Akadémia Policajného zboru v Bratislave
Katedra informatiky a manažmentu

Bezpečnosť elektronickej komunikácie

Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou

Bratislava
2022

AKADÉMIA POLICAJNÉHO ZBORU V BRATISLAVE
Katedra informatiky a manažmentu

BEZPEČNOSŤ ELEKTRONICKEJ KOMUNIKÁCIE

zborník príspevkov

z vedeckej konferencie s medzinárodnou účasťou

konanej dňa 05.05.2022

pod záštitou rektorky Akadémie Policajného zboru v Bratislave
Dr. h. c. doc. JUDr. Lucie Kurilovskej, PhD.
a s podporou Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

Bratislava 2022

Vedecký výbor konferencie:

Dr. h. c. prof. JUDr. Lucia KURILOVSKÁ, PhD. (Akadémia PZ v Bratislave)

doc. Ing. Stanislav ŠIŠULÁK, PhD. (Akadémia PZ v Bratislave)

prof. Ing. Antonín KORAUŠ, PhD., LL.M., MBA (Akadémia PZ v Bratislave)

Ing. Martin FLORIÁN, PhD. (Ministerstvo investícií, regionálneho rozvoja a informatizácie SR)

Ing. Mgr. Jana TKÁČIKOVÁ (Prezídium PZ)

Ing. Ferdinand VAVRÍK, PhD. (Vládna jednotka CSIRT.SK)

PhDr. Peter VESELÝ, PhD., MBA (Fakulta manažmentu, UK Bratislava)

doc. RNDr. Ľudmila GREGUŠOVÁ, CsC.

prof. Ing. Roman RAK, Ph.D.

doc. RNDr. Tatiana HAJDÚKOVÁ, PhD.

plk. JUDr. Stanislav ŠPANKO (poverený riadením Národnej centrály osobitných druhov kriminality P PZ)

kpt. v z. JUDr. Dagmar KOPENCOVÁ, PhD. (Ambis Vysoká škola, katedra Bezpečnosti a práva)

plk. Ing. František VLACH, Ph.D., MBA, LL.M., Ing-Paed (IGIP Akademie vězeňské služby, Česká republika)

Organizačný výbor konferencie:

Členovia Katedry informatiky a manažmentu Akadémie PZ v Bratislave

Ing. Edita LUKÁČIKOVÁ

Mgr. Vladimíra HUDECOVÁ

Ing. Martin KUCHTA, PhD., MBA (Obchodná fakulta, EUBA)

Recenzenti:

Zostavila:

JUDr. Jana ZACHAR KUCHTOVÁ

Za odbornú a jazykovú stránku príspevkov zodpovedajú autori. Rukopis neprešiel jazykovou úpravou.

ISBN 978 – 80 – 8054 – 968 - 8
EAN 9788080549688

Obsah

Úvod ku konferencii „Bezpečnosť elektronickej komunikácie“

Elektronizácia služieb a pracovných činností naprieč celou spoločnosťou vedie ku zvýšenej intenzite toku dát a s tým spojenými problémami v oblasti zabezpečenia bezpečnosti pri ich prenose, spracovaní či uchovávaní. Dňa 26. januára 2022 Európska komisia navrhla medziinštitucionálne vyhlásenie o digitálnych právach a zásadách digitálneho desaťročia, v ktorom ľudia stoja v centre pozornosti. Digitálne technológie by mali chrániť práva ľudí, podporovať demokraciu a zabezpečovať, aby všetci aktéri v digitálnej oblasti konali zodpovedne a bezpečne, pritom. EÚ má snahu tieto hodnoty presadzovať na celom svete. Predstava je, aby každý mal prístup k internetu, digitálnym zručnostiam, digitálnym verejným službám a spravodlivým pracovným podmienkam. Občania by mali mať možnosť zapojiť sa do demokratického procesu na všetkých úrovniach a mať kontrolu nad svojimi vlastnými údajmi. Náročnou výzvou je, aby digitálne prostredie bolo bezpečné a chránené, k čomu smeroval aj obsah problematiky riešenej v rámci vedeckej konferencie s medzinárodnou účasťou, nad ktorou prevzala záštitu rektorka APZ v Bratislave Dr. h. c. doc. JUDr. Lucia Kurilovská, PhD.. Všetci používatelia by od detstva až po starobu mali požívať posilnené postavenie a byť chránení pred nezákonným a škodlivým obsahom a mať posilnené postavenie pri interakcii s novými a vyvíjajúcimi sa technológiami. Digitálne práva a zásady uvedené vo vyhlásení Eutópskej komisie poskytujú občanom referenčný rámec v oblasti ich digitálnych práv, ako aj usmernenie pre členské štáty EÚ a spoločnosti pre prácu s novými technológiami. Majú slúžiť na to, aby bol každý v EÚ schopný vyťažiť z digitálnej transformácie čo najviac. Tento fenomén si vyžaduje zvýšenie úsilia v prevencii a v boji proti nemu na všetkých úrovniach spoločnosti, vrátane vedy a vzdelávania ,

Predložený zborník je výsledkom vedeckej činnosti pracovníkov z viacerých slovenských a českých vysokých škôl, ako aj odborníkov z praxe. Rôzne aspekty problematiky bezpečnosti elektronickej komunikácie obsiahnuté v zborníku umožnili vnorenie do zložitosti sledovanej témy ako aj poukázali na ďalšie výzvy, ktorí sú s ňou spojené.

organizátori konferencie

Tematické zameranie konferencie

Hackli ma! Čo teraz?

Digitálna identita

Ako sa chrániť pred útokmi na internete?

Ako sa správať bezpečne na sociálnych sieťach?

Dezinformácie a hoaxy – aký vplyv majú na dnešnú spoločnosť

Vzdelávanie a budovanie bezpečnostného povedomia v

oblasti elektronickej komunikácie.

Program konferencie

8.00 - 8.30 PREZENTÁCIA ÚČASTNÍKOV

8.30 - 8.50 OTVORENIE KONFERENCIE

HLAVNÝ PROGRAM

8.50 - 9.20 Rozdielnosť reakcií na hacknutie v prípade fyzickej osoby vs štátna inštitúcia.

Prednášajúci: Ferdinand VAVRÍK, Vládna jednotka CSIRT.SK

9.20 - 9.40 Bezpečne a spoľahlivo na internete.

Prednášajúci: Robert Drako, Vládna jednotka CSIRT.SK

9.40 - 10.00 Krotitelia sociálnych sietí

Prednášajúci: Ondrej Bittner, Vládna jednotka CSIRT.SK

10.00 - 10.20 Najväčšie hrozby kybernetickej bezpečnosti.

Prednášajúci: Ondrej Bittner, Róbert Drako, Vládna jednotka CSIRT.SK

10.20 - 10.50 PRESTÁVKA NA KÁVU

10.50 - 11.10 Štandardné problémy pri riešení kybernetických útokov

Prednášajúci: Lukáš HLAVIČKA, IstroSec s.r.o

11.10 - 11.30 Virtuálne dezinformačné mlyny

Prednášajúci: Peter Bíro, SK-NIC, a. s.

11.30 - 11.50 Mapa zraniteľností ako nebezpečná pomôcka bezpečnosti

Prednášajúci Peter Veselý, Fakulta manažmentu UK Bratislava

11.50 - 12.10 Podvodné systémy v kybernetickej bezpečnosti

Prednášajúci: Pavol Sokol, CSIRT UPJŠ

12.10 - 13.00 PRESTÁVKA NA OBED

13.00 - 13.20 Problematika kvality dat: Využití VINdekodéru v kritických aplikacích typu eCALL

Prednášajúci: Roman Rak, VŠ Ambis Praha

13.20 - 13.40 Praktický pohľad na tréningy a cvičenia

Prednášajúci: Matej Šalmík Národné centrum kybernetickej bezpečnosti SK-CERT

13.40 - 14.00 Stav riešenia požiadaviek na bezpečnosť a aktuálnosť a dostupnosť informácií o schválených a realizovaných projektoch financovaných z fondov EU

Prednášajúci: Bystrík Bindas, FIIT STU Bratislava

14.00 - 14.20 Aktuálne trendy – phishing a vishing

Prednášajúci: Eva Marková, UPJŠ

14.20 - 14.40 PRESTÁVKA NA KÁVU

SEKCIA A

14.20 - 14.40 Falošné správy - hrozba pre súčasnú spoločnosť

Prednášajúci: Radoslav Ivančík, Katedra informatiky a manažmentu, A PZ v Bratislave

SEKCIA B

14.20 - 14.40 Dezinformácie z pohľadu študentov bezpečnostných odborov

Prednášajúci: Marek Čandík, Ph. D. Policejní akademie České republiky v Praze

14.40 - 15.00 Riziká komunikácie na sociálnych sieťach

Prednášajúci: Tatiana Hajdúková, Katedra informatiky a manažmentu, A PZ v Bratislave

15.20 - 15.40 Bezpečne na internete

Prednášajúci: Jana Kuchtová, Katedra informatiky a manažmentu, A PZ v Bratislave

SEKCIA C

14.20 - 14.40 Instant messengery a kybernetická bezpečnosť

Prednášajúci : Ondrej Čupka, Ester Federlová, Vincent Karovič ml.

14.40 - 15.00 Participatívne procesy v samospráve a KB

Prednášajúci : Martina Repíková, Michal Greguš st.

15.00 - 15.20 Hackerské útoky na MS EXCHANGE

Prednášajúci : Vincent Karovič ml., Peter Veselý, Matúš Rybanský

15.20 - 15.40 Vplyv kybernetickej kriminality na HDP

Prednášajúci : Lucia Klapáčová, Loretta Pinke, Peter Veselý

15.40 - 16.00 Kybernetická bezpečnosť pri online vzdelávaní

Prednášajúci : Alica Kačmariková, Marián Mikolášik, Silvia Treľová

16.00 - 16.20 Medzinárodný dopad kybernetickej kriminality

Prednášajúci : René Pawera, Peter Veselý

Informácie v bezpečnostnom systéme

Vladimír Andrassy

Abstract: The security system is described as a complex system with defined technical, personnel, communication and operational capabilities. It is a modular system integrating real-life elements that create a tool to ensure security in given space and time. Its priority role is to minimize existing threats and risks through the interaction of interconnected subsystems so that we are able to provide the required protection of a protected object or a protected interest. The basis for the functioning of the system is the need to work with relevant and credible information, the collection, transmission, processing, display and storage of which is provided by the information system.

Key Words: security system, information processes, security system subjects.

Úvod

Súčasný dynamický a turbulentný vývoj ľudskej spoločnosti so sebou prináša mnohé pozitívne, ale zároveň aj negatívne skutočnosti, ktoré sa prejavujú v rôznych oblastiach života človeka i celej ľudskej civilizácie. Dôkazom toho sú početné pôvodné i novo sa objavujúce bezpečnostné hrozby a riziká, ktoré oprávnene stavajú otázky bezpečnosti na popredné miesto.[1] Bezpečnosť totiž tvorí základnú a nevyhnutnú podmienku rozvoja každej spoločnosti a dnes, v ére prehlbujúcej sa globalizácie, už neexistuje oblasť spoločenského života, ktorá by s ňou nebola spojená.[2] Aj preto sa snažia všetky štáty, organizácie či akékoľvek iné entity zaistiť svoju bezpečnosť na čo najvyššej úrovni prostredníctvom efektívneho, účelného a najmä funkčného bezpečnostného systému.[3]

Efektívnosť navrhnutého a vytvoreného bezpečnostného systému je závislá od možnosti získavania, prenosu, spracovania, vyhodnotenia, uchovania a odovzdania relevantných údajov, správ a informácií na miesto ich využitia vo vhodnom čase, potrebnom rozsahu a požadovanej forme. Pri skúmaní bezpečnostného systému ako celku pozostávajúceho z autonómnych častí si musíme uvedomiť, že sa vyznačujú určitou samostatnosťou, ktorá závisí od ich kvalitatívnych charakteristík. Každá samostatná časť má vplyv na podstatu, kvalitu a jeho komplexný rozvoj. Súčasťou bezpečnostného systému je aj informačný systém zabezpečujúci informačné procesy v rámci jednotlivých autonómnych častí. Informačný systém by mal byť otvoreným dynamickým systémom so sústavou vnútorných a vonkajších väzieb medzi jeho

[1] IVANČÍK, R, Bezpečnosť. Teoreticko-metodologické východiská. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022.
[2] IVANČÍK, R., Security Theory: Security as a Multidimensional Phenomenon. Vojenské reflexie, 2021.
[3] NEČAS, P., IVANČÍK, R.: Aktuálny vývoj v oblasti zaisťovania kybernetickej bezpečnosti a ochrany informácií na národnej a nadnárodnej úrovni. Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek). Bratislava, 2019.

jednotlivými časťami. Mal by integrovať funkcie zabezpečenia, ochrany, vyrozumenia, zabezpečenia zásahu a mnohé iné.

Informácie v bezpečnostnom systéme

Informáciou sa v rámci informačných tokov bezpečnostného systému rozumie správa, hodnota alebo iné oznámenie prijaté príjemcom, na základe ktorého realizuje určitú špecifickú činnosť. Je to správa, ktorá vyjadruje istý stav, pre prijímateľa predstavuje niečo nové, slúži definovanému cieľu alebo vyvoláva odpovedajúcu akciu/reakciu. Informácia je merateľná a má stanoveného adresáta.

Správa je skutočnosť, ktorá sa prenáša informačným systémom. Skladá sa z viacerých údajov. Správa sa stáva informáciou v dôsledku ľudskej interpretácie alebo tým, že je spracovaná na základe algoritmov a uloží sa k ďalšiemu využitiu.

V bezpečnostnom systéme bude informáciou každá správa, každé oznámenie medzi jednotlivými subsystémami vo vnútri systému i subsystémami navzájom o tom, že nastal, nastáva, alebo má nastať určitý stav (alebo množina stavov) ako prejav zmeny. Bude to každá správa určená k následnému spracovaniu a využiteľná pre zamýšľaný účel, ktorá napomôže odstrániť alebo zmenšiť neistotu alebo neurčitosť systému, rozšíri vedomosti o stave bezpečnosti, alebo iným spôsobom ovplyvní správanie bezpečnostného systému.

Systém na zabezpečenie informácií potrebných na riadenie, ich zber, zhromažďovanie, prenos, uchovanie, transformáciu, výber a distribúciu na ďalšie využitie pre potreby riadenia a pre prípravu a realizáciu rozhodnutí popisujeme pojmom informačný systém. Je to súhrn procedúr, činností, ľudí a technológií majúcich za cieľ zabezpečiť dostatok relevantných, správnych a presných informácii v požadovanej forme a časovom intervale pre potreby spracovania riadiacim subjektom. Úlohu informačného systému ako neoddeliteľnej súčasti bezpečnostného systému nemôžeme redukovať len na systém spracovania údajov. Jednotlivými prvkami informačného systému sú miesta zberu, spracovania, prenosu, archivácie správ, miesta prípravy a realizácie rozhodnutí a vzájomné väzby medzi nimi zabezpečujúce smery ich tokov.

Odovzdávanie správ, údajov, hodnôt, faktov, oznámení o určitej udalosti, jave, činnosti alebo iných dát medzi autonómnymi časťami alebo medzi systémom a okolím s využitím vytvorených komunikačných kanálov (prenosových ciest) definujeme ako vzájomnú komunikáciu.

Komunikačné spôsobilosti bezpečnostného systému sú viazané na jeho schopnosť efektívne využívať informačné zdroje a informačné nástroje na prepojenie technických, prevádzkových a personálnych spôsobilostí. Je to súbor metód, programov, postupov a aktivít,

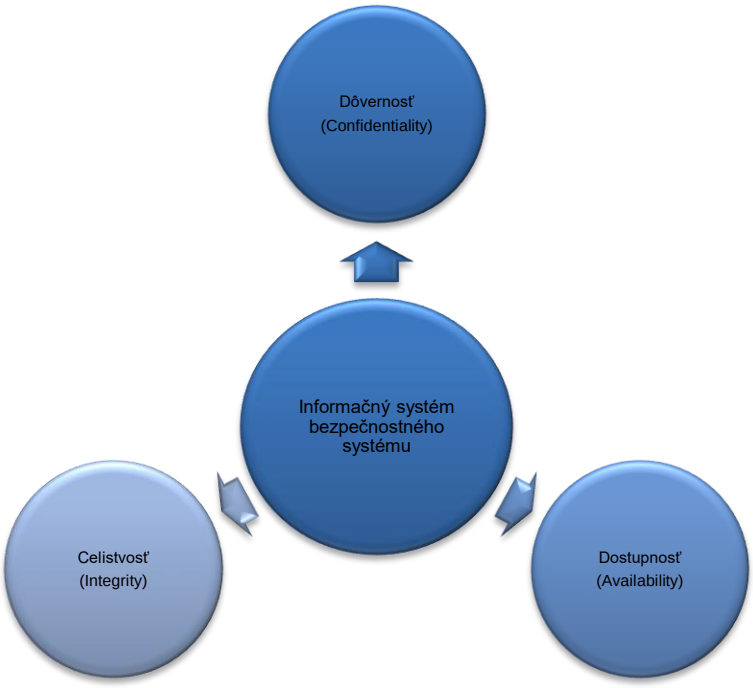
ktorými sa realizuje maximálne využitie informácii získaných zberom, zaznamenávaním a výmenou (spätnou väzbou) s cieľom nájdenia optimálneho riešenia vzniknutého bezpečnostného problému. Vo všeobecnosti je to prijímanie a odovzdávanie správ, údajov, hodnôt, faktov, oznámení o určitej udalosti, jave, činnosti alebo iných dát medzi subsystémami alebo medzi systémom a okolím s využitím vytvorených komunikačných kanálov resp. prenosových ciest.

Existujúci bezpečnostný systém musí zabezpečovať efektívne využívanie informácií v rámci vytvoreného informačného systému na základe identifikácie informačných potrieb, ktoré súvisia s procesom získavania informácií, ich prvotným spracovaním a následnou distribúciou. Umožňujú spoločné spájanie, zhromažďovanie a vyhodnocovanie získaných údajov z jednotlivých rozptýlených autonómnych častí bezpečnostného systému koncipovaných ako samostatné integrované komponenty. Pri koncipovaní je potrebné dbať na požadovanú úroveň bezpečnosti informačného systému (B_{IS}), ktorú je možné definovať troma základnými požiadavkami:

a) dôvernosť (Confidentiality) – ochrana pred prezradením informácie,

b) celistvosť (Integrity) – ochrana pred neoprávnenou modifikáciou,

c) dostupnosť (Availability) – ochrana pred neschopnosťou poskytnúť informáciu.



Obrázok 1 Základné požiadavky na bezpečnosť informačného systému
(zdroj: vlastné spracovanie)

Uvedené požiadavky transformované na charakteristické vlastnosti bezpečnostného systému je možné zhrnúť do nasledujúcich bodov:

a) Výstupom informačných procesov informačného systému musia byť informácie. Vstupné dáta je potrebné zozbierať, spracovať a analyzovať v súlade s potrebami a záujmom zabezpečenia ochrany osôb a majetku.

b) Zber a zhromažďovanie údajov musí byť relevantné pre účel, na ktorý majú byť použité, musia spĺňať základné atribúty a kľúčové podmienky, musia byť zhromažďované s ohľadom na vopred stanovené ciele.

c) Vytvorený bezpečnostný systém by mal byť zrozumiteľný a prehľadný, mal by integrovať jednotlivé autonómne časti a zložky.

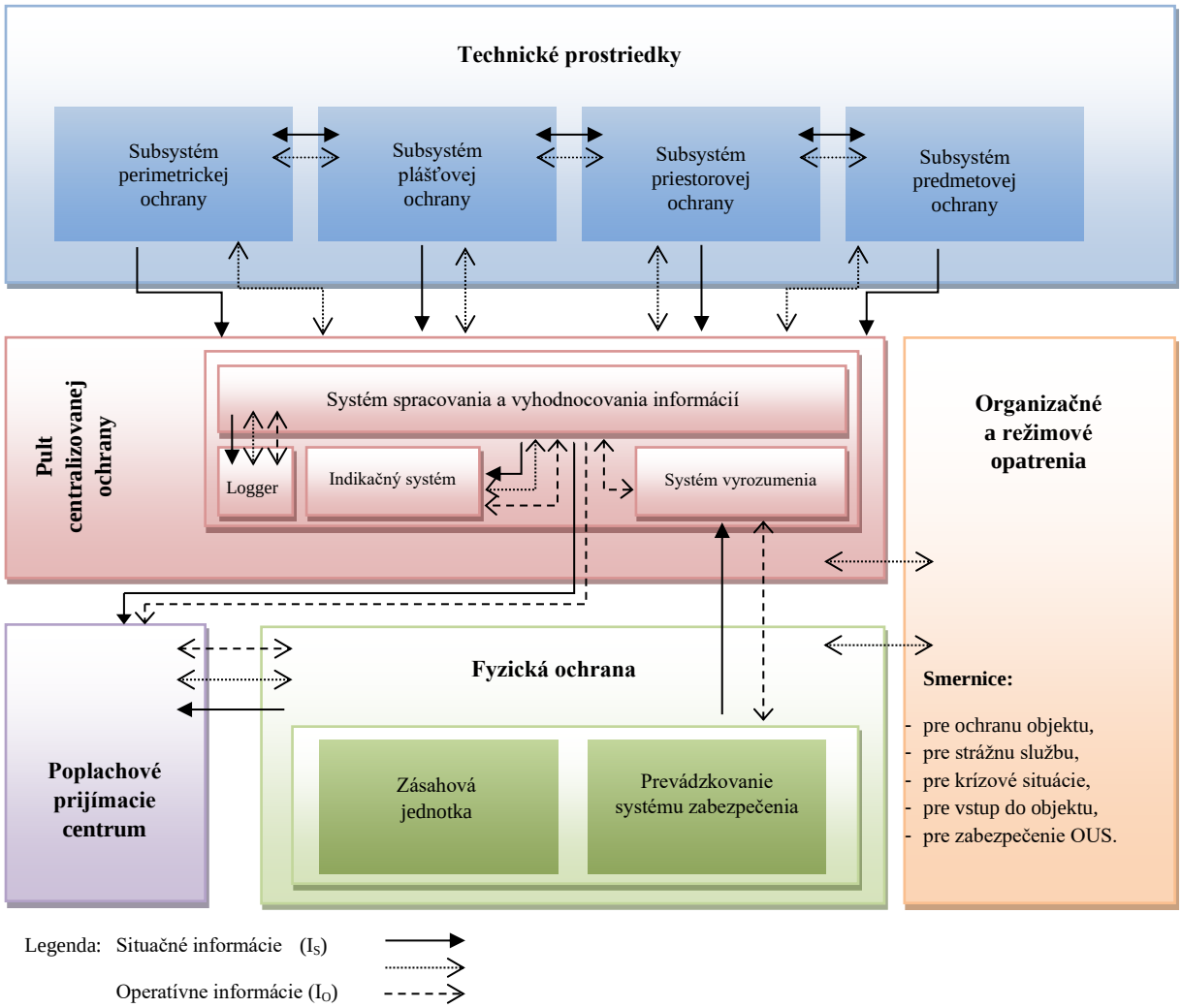
d) Údaje musia byť dodané včas a musia byť k dispozícii pred prijatím rozhodnutí a vykonaním opatrení.

e) Údaje by mali byť orientované na nasledujúcu činnosť, mali by mať podobu takej syntézy, ktorá uľahčí proces rozhodovania a následného konania.

f) Spracovávané údaje by mali poskytovať relevantné a pravdivé indikátory, ktoré možno vyhodnotiť, porovnať a prijať adekvátne opatrenia.

g) Realizácia informačného systému v rámci bezpečnostného systému zabezpečujúceho ochranu chráneného záujmu musí zabezpečiť maximálnu mieru efektívnosti.

Z uvedenej štruktúry informačných tokov v rámci bezpečnostného systému jednoznačne vyplýva, že zdrojom informácií sú jednotlivé samostatné subsystémy tvorené technickými zariadeniami a personálom. Zabezpečujú zber potrebných údajov, ich transformáciu a prenos do pultu centralizovanej ochrany. Ten je tvorený systémom spracovania a vyhodnotenia informácií a následne indikačným a signalizačným systémom zabezpečujúcim svetelnú, zvukovú alebo inú indikáciu stavu narušenia. Systém vyrozumenia aktivuje prvky fyzickej ochrany alebo zásahovú jednotku. Logger, tvoriaci neoddeliteľnú súčasť pultu centralizovanej ochrany, je špecifické zariadenie slúžiace na archiváciu a zálohovanie požadovaných informácií.



Obrázok 2 Schéma štruktúry informačných tokov v rámci bezpečnostného systému (zdroj: vlastné spracovanie)

Na základe zobrazenia je zrejmé, že informačný systém nemožno stotožňovať len so systémom spracovania údajov. Je to systém pozostávajúci z:

a) obsluhy,

b) technických a programových prostriedkov zabezpečujúcich zber, prenos, spracovanie, výber, ukladanie, distribúciu a prezentáciu informácií pre potrebu rozhodovania,

c) jednotky zabezpečujúcej zásah,

d) spracovanej riadiacej a vyhodnocovacej dokumentácie.

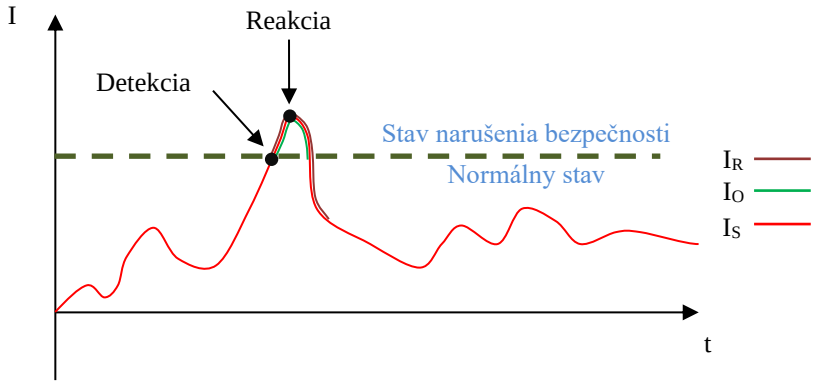
Základnou úlohou bezpečnostného systému je zabezpečenie dostatku relevantných, správnych a presných informácií v požadovanej forme. Z hľadiska obsahu prenášaných dát

v rámci informačných tokov jednotlivých subsystémov je prenášané informácie možné rozdeliť na :

a) situačné informácie (I_S) – poskytujúce prehľad o situácii v chránenom objekte alebo subsystéme (bežia stále),

b) operatívne informácie (I_O) – vznikajúce ako bezprostredná reakcia na vytvárajúcu sa situáciu a sú určené na operatívne riadenie bezpečnostného systému napr. indikácia stavu snímačov, smernice, plány,

c) riadiace informácie (I_R) – ktorých vydanie pokračuje činnosťou napr. poplachové informácie, povely, príkazy, nariadenia.



Graf 1 Rozdelenie informácií v informačnom systéme

(zdroj: vlastné spracovanie)

Vzájomné vzťahy situačných (I_S), operačných (I_O) a riadiacich (I_R) informácií pre riadenie činností v bezpečnostnom systéme vieme popísať grafom (Graf 2).[4] Na základe uvedeného grafu je možné informačný systém charakterizovať ako:

a) informačný systém homeostatický pre $I_R = I_S$, $I_R > 0$, $I_S > 0$,

b) informačný systém riadiaci so spätnou väzbou pre $I_R > I_S$, $I_S > 0$,

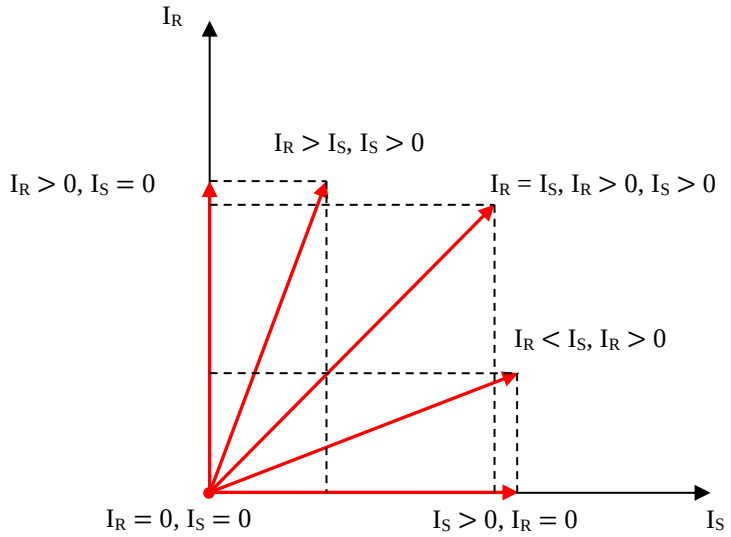
c) informačný systém riadiaci bez spätnej väzby pre $I_R > 0$, $I_S = 0$,

d) informačný systém spravodajský s riadiacou väzbou pre $I_R < I_S$, $I_R > 0$,

e) informačný systém spravodajský pre $I_S > 0$, $I_R = 0$,

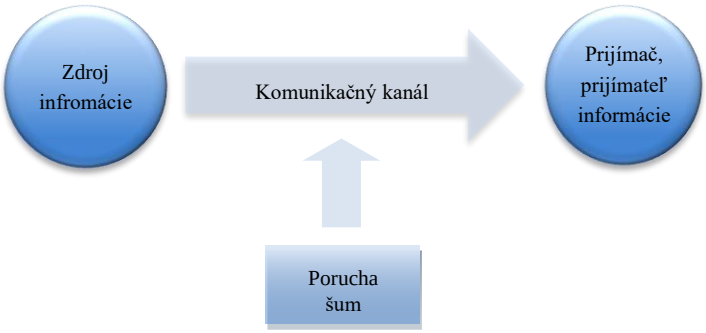
f) informačný systém rozvrátený (deštruovaný) pre $I_R = 0$, $I_S = 0$.

[4] HOFREITER, L., Securitológia., Liptovský Mikuláš, 2006



Graf 2 Stavy informačného systému
(zdroj: Hofreiter, L., 2006)

Na zabezpečenie informačného procesu počínajúc zberom údajov a končiac odovzdaním informácie a prijatím rozhodnutia k minimalizácii hroziaceho ohrozenia sa vytvára informačný systém bezpečnostného systému. Je tvorený súborom informačných systémov jednotlivých subsystémov bezpečnostného systému s vzájomnými vzťahmi a väzbami zabezpečujúci požadované informácie. Spravidla sa skladá z informačného zdroja, komunikačného kanála resp. prenosovej cesty a z prijímača alebo prijímateľa informácie. Ako typický príklad zobrazenia komunikácie v rámci bezpečnostného systému je možné využiť komunikačný model Shannona – Weavera hlavne z pohľadu jednoduchosti, všeobecnosti a merateľnosti.



Obrázok 3 Komunikačný model informačného systému
(zdroj: vlastné spracovanie)

Zdrojom informácie môže byť ľubovoľný fyzikálny systém (technické zariadenie, človek) zameraný na zber a zhromažďovanie údajov. Je to miesto, odkiaľ sa informácia čerpá, získava, pričom všetky existujúce javy, procesy, deje sú vo svojej podstate zdrojom informácie. Pôsobia na svoje okolie rôznymi druhmi signálov, pohybom, energiou a podobne. Vstupné údaje je potrebné zbierať nepretržite, aby bolo možné sledovať prebiehajúce zmeny napr. postup narušiteľa v chránenom objekte. Získaná informácia sa prenáša komunikačným kanálom resp. prenosovou cestou spravidla pomocou premenných parametrov – informačných signálov.

Komunikačný kanál resp. prenosovú cestu charakterizujeme ako komunikačnú cestu používanú pre prenos informácie. Je to fyzické médium, ktoré zabezpečuje prenos informačných signálov medzi zdrojom a prijímačom (adresátom), alebo na miesto uschovania. Počas prenosu pôsobia na signál rušivé vplyvy – poruchy a šumy, ktorých zdrojom sú náhodné procesy, tzv. fluktuačné poruchy, prechodné javy alebo systematicky sa vyskytujúce nenáhodné signály. Vplyvom týchto porúch sa na vstup prijímacieho zariadenia dostáva viac neurčitosti, a teda menej informácií ako zdroj vyslal. Získané informácie sa preto triedia a upravujú tak, aby boli vhodné na zobrazovanie a zaznamenávanie prijímateľom, technickým zariadením alebo človekom. Komunikačným kanálom nie je možné bezchybne preniesť ľubovoľné množstvo informácií za jednotku času. Informačná kapacita C charakterizuje maximálne množstvo informácií, ktoré môžeme preniesť komunikačným kanálom v_f so šírkou pásma B_{vf} pri pôsobení porúch a šumov s nulovou chybovosťou.

$$C = B_{vf} \log_2 \left(1 + \frac{P}{N}\right)$$

kde:

P - je stredný výkon signálu na vstupe prijímača,

N - je stredný výkon šumu.

Komunikačný kanál je tvorený rôznym fyzikálnym prostredím (prenosovým médiom), ktoré je schopné informáciu preniesť bez veľkých strát a skreslenia. Medzi najbežnejšie prenosové média zaraďujeme elektrický vodič (koaxiálne káble, krútená dvojlinka), optické vlákno, vzduch (bezdrôtový prenos). Základné charakteristiky prenosového média sú:

a) odolnosť proti vonkajšiemu elektromagnetickému rušeniu (EMI) - náhodná energia z vonkajších zdrojov, ktorá môže interferovať so signálmi prenášanými metalickým káblom,

b) šírka pásma - určuje maximálnu frekvenciu nosného signálu, udáva sa v Hz,

c) útlm - strata intenzity signálu na médiu so vzdialenosťou, udáva sa v dB na dĺžku média,

d) impedancia - veľkosť odporu vodiča striedavému elektrickému prúdu, ktorá pomáha určiť útlmové vlastnosti vodiča, udáva sa v Ω,

e) presluch medzi vodičmi - rušenie signálom so susedného vodiča, udáva sa v dB.

Prijímač alebo prijímateľ (adresát) informácie je vo všeobecnosti technické zariadenie, ktoré môže byť obsluhované človekom a skladá sa z nasledujúcich podsystémov:

a) podsystém výberu a spracovania dát zameraných na aktualizáciu predchádzajúcich údajov, agregáciu a výpočty tak, aby bol dosiahnutý požadovaný výsledok smerujúci k indikácii reálneho stavu bezpečnostného systému,

b) podsystém uchovania informácií a zaznamenania údajov, ktoré vstúpili do systému a budú systémom spracovávané a poskytované tak, aby bol umožnený ich výber v prípade potreby,

c) podsystém zobrazenia stavov smerujúcich k optickej alebo akustickej indikácii a prezentácii spracovaných údajov a výstupných stavov jednotlivých subsystémov,

d) podsystém distribúcie vyhodnotených a informácii k ďalšiemu spracovaniu.

Proces spracovávania informácií môžeme definovať ako logický, analyticko – syntetický spôsob prevodu správ človekom alebo technickým zariadením na požadovaný výstupný tvar. V tomto procese spracovávania informácií je základným problémom skutočnosť, že správy vznikajú na jednom mieste (zdroj), komunikačným kanálom resp. prenosovou cestou sú prenášané a na inom mieste sústavy (prijímateľ) sú reprodukované. Prenášaná správa sa musí vyznačovať tým, že obsahuje dáta, správu alebo informáciu. Aby v systéme nezanikla, musí obsahovať aj redundanciu (nadbytočnosť), ktorá vždy zväčšuje objem správ bez zvýšenia jej informačného obsahu. Spracovávaním sa množstvo informácií síce zmenšuje, ale kvalita a informačný obsah o danej situácii znižujúci alebo odstraňujúci neurčitosť pred prijatím správy charakterizovaný hodnotnosťou informácie sa zvyšuje. Množstvo informácie (I_x) získané prijatím správy, ktorá sa vyskytuje s určitou pravdepodobnosťou (p_x) bude tým väčšie, čím bude táto správa nepravdepodobnejšia.

$$I_x = \log_2 \left(\frac{1}{p_x}\right)$$

Z matematického hľadiska je informácia (I) funkcia údajov (D), ich štruktúry (S) a časového intervalu (t), v ktorom komunikácia prebieha. [5]

[5] HOFREITER, L., Securitológia., Liptovský Mikuláš, 2006

$$I = f(D, S, t)$$

Každá informácia má dve stránky:

a) kvantitatívnu (syntaktickú), ktorá vyjadruje zloženie správy z jednotlivých znakov umožňujúcich prenos,

b) kvalitatívnu (sémantickú), ktorá vyjadruje primeranosť zobrazenia skutočnosti a užitočnosť informácie v súvislostiach, vo vzťahu k určitej činnosti.

Kvalitatívne a kvantitatívne parametre určujú hodnotu informácie (H) charakterizujúcu mieru odstránenia neurčitosti, alebo úspešnej činnosti, zásahu. Určenú mieru odstránenia neurčitosti resp. úspešnej činnosti je možné matematicky vyjadriť pomocou vzťahu: [6,7]

$$H = \log \frac{p_2}{p_1}$$

kde:

H - je hodnota informácie, ktorá môže byť:

$H > 0$, ak $p_2 > p_1$,

$H < 0$, ak $p_2 < p_1$,

p_1 - je pravdepodobnosť odstránenia neurčitosti pred prijatím informácie,

p_2 - je pravdepodobnosť odstránenia neurčitosti po prijatí informácie.

Pre uľahčenie kvantifikovania hodnoty informácie je možné identifikovať nasledujúce atribúty informácie:

a) relevantnosť – významnosť, dôležitosť z hľadiska účelu,

b) presnosť – miera objektívnosti obsahu informácie,

c) úplnosť – obsahuje všetko podstatné z hľadiska účelu,

d) správnosť a pravdivosť – vhodne vyjadrená z hľadiska obsahu, overená,

e) koncíznosť a primeraná podrobnosť – dostatočne primeraná, vecná, nezahltená,

f) zrozumiteľnosť – vyjadrená vhodnými prostriedkami,

g) konzistentnosť – kompaktnosť obsahu, súvislosť údajov,

h) včasnosť a časovosť – je k dispozícii v čase použitia s vyjadrenou dobou platnosti.

[6] HOFREITER, L., Securitológia., Liptovský Mikuláš, 2006

[7] REITŠPÍS, J. a kol.., Manažérstvo bezpečnostných rizík, Žilina, 2004.

Záver

Bezpečnostný systém umožňujúci realizáciu špecifických funkcií zabezpečenia pre konkrétny chránený záujem je tvorený informačným systémom zabezpečujúcim požadované atribúty informácie v nadväznosti na kľúčové podmienky v rámci bezpečnostného systému. Je možné charakterizovať ho ako prienik technických, programových, organizačných a personálnych subsystémov s dôrazom na hodnotenie cieľovej funkcie systému s prioritami a kvalitami ochrany. Môžeme ho posudzovať z dvoch hľadísk, ktoré sú v interakcii:

a) hľadisko technických prostriedkov - deterministický systém, v ktorom sú vzájomné vzťahy subsystémov informačného systému pevne definované,

b) hľadisko subjektov - stochastický systém, charakterizovaný spracovaním, prípravou a realizáciou rozhodnutí využívajúcich a aktualizujúcich informácie v rámci informačných procesov riadenia bezpečnostných služieb s dôrazom na pôsobenie ľudského faktora.

Flexibilita riešenia bezpečnostného systému sa dosahuje vhodnou voľbou a kombináciou jednotlivých subsystémov s ich vzájomným prepojením. V každom vytvorenom bezpečnostnom systéme je však potrebné zvážiť možnosti a potrebu technických prostriedkov a personálu s dôrazom na získavanie, prenos a vyhodnotenie informácií v rámci existujúceho informačného systému. K tomu je potrebné prispôsobiť štruktúru zdrojov, informačných kanálov, indikačných a signalizačných zariadení prepojených na personálom obsluhované pracovisko. Musíme si uvedomiť, že je potrebná nielen spoľahlivá detekcia narušenia, ale aj rýchla, správna, adekvátna a vyvážená reakcia osôb na získané, spracované a vyhodnotené informácie. Výsledná úroveň bezpečnosti bude vždy závislá od stupňa zabezpečenia relevantnými prostriedkami poskytujúcimi ochranu.[8,9] Vytvorený bezpečnostný systém tak plní úlohu nielen priamej, bezprostrednej ochrany, ale aj prevencie a poskytovania informácií.

Zoznam použitej literatúry

ANDRASSY, V., GREGA, M.: Didaktické postupy riešenia úloh v oblasti krízového manažmentu. Liptovský Mikuláš, Akadémia ozbrojených síl generála M. R. Štefánika, 2013. ISBN 978-80-8040-484-0.

FAY J., J.: Encyklopedia for Security Management. Burlington, MA: Elsevier Inc., 2007. ISBN 978-0-12-370860-1.

[8] HOFREITER, L., Securitológia., Liptovský Mikuláš, 2006

[9] REITŠPÍS, J. a kol.., Manažérstvo bezpečnostných rizík, Žilina, 2004.

HOFREITER, L.: Securitológia. Liptovský Mikuláš: AOS gen. M. R. Štefánika, 2006. ISBN 978-80-8040-310-2.

HOFREITER, L., KRIŽOVSKÝ, S.: Manažérstvo bezpečnostných systémov. Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, 2007. ISBN 978-80-89282-16-6.

HOFREITER, L., VEĽAS, A., KALUŽA, F.: Systémy prenosu informácií v bezpečnostných aplikáciách. Žilina: Žilinská univerzita v Žiline, 2008. ISBN 978-80-8070-823-8.

IVANČÍK, R. 2022. Bezpečnosť. Teoreticko-metodologické východiská. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2022. 240 s. ISBN 978-80-7380-873-0.

IVANČÍK, R. 2021. Security Theory: Security as a Multidimensional Phenomenon. In Vojenské reflexie, 2021, roč. 16, č. 3, s. 32-53. ISSN 1336-9202.

LOVEČEK, T.: Bezpečnostné systémy. Bezpečnosť informačných systémov. Žilina: Žilinská univerzita v Žiline, 2007. ISBN 8080707675.

NEČAS, P., IVANČÍK, R. 2019. Aktuálny vývoj v oblasti zaisťovania kybernetickej bezpečnosti a ochrany informácií na národnej a nadnárodnej úrovni. In Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2019. s. 125-137. ISBN 978-80-8040-819-3.

REITŠPÍS, J. a kol.: Manažérstvo bezpečnostných rizík. Žilina: Žilinská univerzita v Žiline, 2004. ISBN 80-8070-328-0.

SMULDERS, A., HINTZBERGEN, J., BAARS, H.: Foundations of IT Security. Van Haren Publishing, 2010. ISBN 978-90-8753-568-1.

Kontaktné údaje

doc. Ing. Vladimír ANDRASSY, PhD.

Akadémia ozbrojených síl gen. M. R. Štefánika

Demänová 393, 031 01 Liptovský Mikuláš

e-mail: vladimir.andrassy@aos.sk

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing. Paed-IGIP

PhDr. Peter Veselý, PhD.

Stav riešenia požiadaviek na bezpečnosť a aktuálnosť a dostupnosť informácií o schválených a realizovaných projektoch financovaných z fondov EU

Bystrík Bindas

Abstrakt: Článok pojednáva o celkovej existencii a dodržiavaní nariadení pre kybernetickú alebo informačnú bezpečnosť v projektoch schválených v rámci Operačný program integrovaná infraštruktúra na náhodne vybranej vzorke.

Kľúčové slová: projekt, bezpečnosť, informačná bezpečnosť, kybernetická bezpečnosť, štúdia uskutočniteľnosti, projektový zámer, metainformácia

Abstract: The article deals with the overall existence and compliance with regulations for cyber or information security in projects approved under the Integrated Infrastructure Operational Program for randomly selected projects.

Keywords: project, security, information security, cyber security, feasibility study, business plan, metainformation

Úvod

Kybernetická bezpečnosť je významným predpokladom efektívnemu predchádzaniu problémov v akomkoľvek systéme. Zvlášť by na ňu malo byť dbané v prípade, že sa jedná o systém zabezpečujúci služby štátnej a verejnej správy, komunikáciu štátnych inštitúcií s občanom. Aká je však skutočnosť na Slovensku? Je v projektoch financovaných z fondov Európskej únie kybernetická bezpečnosť vyžadovaná, či povinná? Je táto skutočnosť jasne deklarovaná vo vyhláške, ktorou sa riadi príprava projektov pod gesciou MIRRI? A sú na základe dokumentov povinne zverejňovaných na stránkach inštitúcií ľahko dohľadateľné dokumenty viažúce sa k implementácii kybernetickej bezpečnosti, teda že bola realizovaná v projektoch?

Nasledujúci príspevok sa snaží odpovedať na položené otázky. Je pochopiteľné, že neobsahuje úplné štatistiky projektov, ktoré boli realizované, ale vzorku. Dôležité je, že vychádza z verejne dostupných a všeobecne zverejnených dokumentov, ktoré by mali obsahovať reálne informácie o stave implementácie kybernetickej bezpečnosti vo verejnej správe. A prináša pohľad zo strany bežného používateľa, ktorý sa snaží získať relevantné informácie.

Východiská zodpovednosti

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej aj ako MIRRI) je ústredným orgánom štátnej správy pre riadenie, koordináciu a dohľad nad využívaním finančných prostriedkov z fondov Európskej únie a oblasť informatizácie spoločnosti. [2] Je teda zodpovedné aj za stav informácií, ktoré súvisia s prípravou projektov, ich obsahom, aktuálnosťou a určite aj dostupnosťou a prehľadnosťou. Nezainteresovaná osoba mimo verejnej správy, ktorá môže, ale zároveň nemusí byť expertom, by však na základe vyhľadávania mala dostať presnú a aktuálnu informáciu.

Legislatívny rámec prípravy projektov

V Slovenskej republike máme niekoľko záväzných predpisov pre riadenie a implementáciu projektov, životný cyklus projektov. Zameriame sa na najpodstatnejšie, cielene spájané s prípravou projektu a budeme hľadať väzbu s bezpečnosťou a kybernetickou bezpečnosťou. Ak sa na webových portáloch štátnych inštuitúcií nchádzajú informácie o platných právnych predpisoch, referujú sa na portál https://www.slov-lex.sk/ . [4]

- ✓ Vyhláška 179/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu z. 22. júna 2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

Komplexná vyhláška, ktorá sa priamo venuje bezpečnosti.

- ✓ Vyhláška 85/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu zo 14. apríla 2020, o riadení projektov

Vyhláška sa, ako udáva jej názov priamo dotýka systému riadenia a prípravy projektov realizovaných zo zdrojov EU. Vyhláška sa dotýka pri prvkoch riadenia otázky bezpečnosti kybernetickej aj informačnej v súvislosti s prípravou a riadením projektu. V § 2 Vymedzenie základných pojmov aj definuje pracovnú pozíciu člena projektového tímu manažéra kybernetickej a informačnej bezpečnosti, ktorej význam však v § 6 Prípravná fáza projektu, bode 3. e) dávajú do pozície nie vyžadovanej. Znenie hovorí: “ určenie vhodných kandidátov na pozície členov projektového tímu, pričom je potrebné zabezpečiť obsadenie týchto projektových rolí: … 2g. manažér kybernetickej a informačnej bezpečnosti, ak je to potrebné”. [3] Reálne si vieme predstaviť, že by projekt, ktorý nevyžaduje spomínaného manažéra, mohol vzniknúť. Skôr je otázkou, prečo vyhláška vyžaduje výstup projektu s názvom Bezpečnostná

architektúra až v realizačnej fáze projektu, teda až po jeho schválení. U žiadateľa o projekt to môže vyvolať dojem, že o samotnú bezpečnosť sa v príprave projektu nemusí zaujímať, nemusí počítať s nákladmi spojenými so zabezpečením bezpečnosti, či o bezpečnosť sa má zaujímať, až keď je projekt postavený. V každom prípade však vyhláška veľmi jasne počíta so skutočnosťou, že projekty pomocou nej realizované musia s kybernetickou a informačnou bezpečnosťou rátať.

Vyhlášky postačujú na to, aby bola v navrhovaných a realizovaných projektoch riešená otázka IT bezpečnosti.

Dokument Projektový zámer a štúdie uskutočniteľnosti....

Tento dokument v zmysle Vyhlášky 85/2020 Z. z. nahradil v príprave projektov dokument štúdia uskutočniteľnosti dovtedy vyžadovaný. Medzi jeho uplatňovaním a samotným používaním bolo stanovené prechodné obdobie. Predloha projektového zámeru ako aj zvyšné vzťahujúce sa dokumenty sú dostupné online na stránkach projektovej kancelárie MIRRI.

Samotný obsah dokumentu v sebe kombinuje systém riadenia projektov, už nie iba v zmysle metodiky PRINCE 2, prvky obchodného zámeru, až po návrh systému v zmysle prvkov štandardnej otvorenej architektúry TOGAF globálneho konzorcia The Open Group [5]. Samotný dokument je doplnený nápovedou a je pre prípravnú a iniciačnú fázu projektu. Bezpochyby je užitočný, aj keď v sebe kombinuje nielen projektovo-manažérske, ale aj dizajnovo implementačné prvky. A samozrejme CBA – Cost Business Analyses.

Zmienku o bezpečnosti v ňom však nájdete len veľmi ťažko. Tvorcovia sa nezamerali na prepojenie tohoto dokumentu s Vyhláškou 179/2020 Z. z., pritom ide o dokument, ktorý je základom schvaľovacieho procesu pre projekty a na základe jeho schválenia sa projektom prideľujú financie. K požiadavkam na bezpečnosť sa v tomto dokumente dá dopátrať iba cez spojenia vyhlášky 85/2020 Z.z. a následne akousi referenciou na vyhlášku 179/2020 Z.z. Náznaky riešenia bezpečnosti sa dajú nájsť pri spomienke na architektúru navrhovaného systému, čo zrejme vyplýva zo skutočnosti, že dokument vychádza z princípov TOGAF. Lenže bezpečnostná architektúra nie je natívnou súčasťou TOGAF. Informačná bezpečnosť je samostatná projektová disciplína izolovaná od Enterprise Architecture, teda podnikovej architektúry.[5] V kontexte návrhu však obsahuje informácie, ktoré ovplyvňujú podnikovú architektúru. Pre prijímateľa projektu to môže znamenať nejednoznačnosť pri príprave

projektu, nepríjemné prekvapenie pri jeho realizácii, či komplikáciu, ktorú raz bude musieť vyriešiť.

Z uvedeného môže vyplývať predpoklad, že projektové zámery, či predtým štúdie uskutočniteľnosti nemusia obsahovať informácie o stave a spôsobe riešenia informačnej a kybernetickej bezpečnosti. Či tomu v skutočnosti tak aj je si predstavíme v kapitole „Stav riešenia kybernetickej bezpečnosti vo vybraných schválených projektoch“.

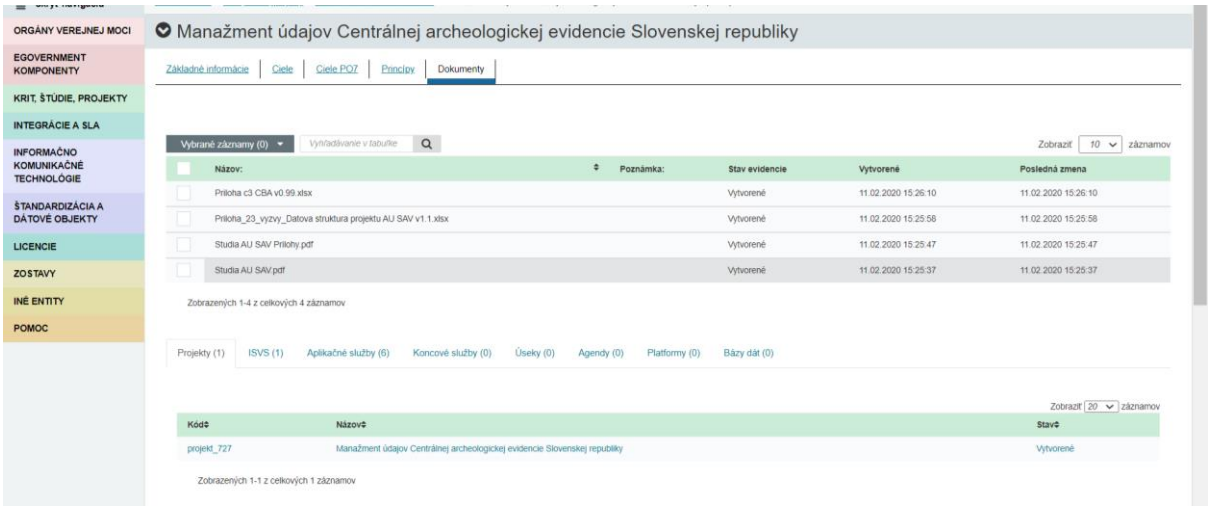
ISVS: Centrálny metainformačný systém verejnej správy

Centrálny metainformačný systém verejnej správy je, ako uvádza aj samotná webová stránka – portál systému: “Je najmä evidenčným portálom, ktorý obsahuje údaje a správu životného cyklu údajov o službách, informačných systémoch, číselníkoch, referenčných registroch a referencovateľných identifikátoroch, licenciách ako aj ďalších komponentoch eGovernmentu na Slovensku. Účelom systému je správnosť, kompletnosť a dostupnosť aktuálnych informácií.” [1] Z predpokladu poslednej vety budeme vychádzať aj tomto dokumente. Je totiž informáciou, keď nie deklaráciou, že zverejnené informácie sú správne, aktuálne a kompletné.

Metainformácia je informáciou o informácii. Takýmto naväzovaním informácií je možné vytvoriť hierarchický systém, v ktorom by malo byť možné prechodom cez súvisiace informácie získať minimálne kontextuálne náväznosti sledovaných objektov.

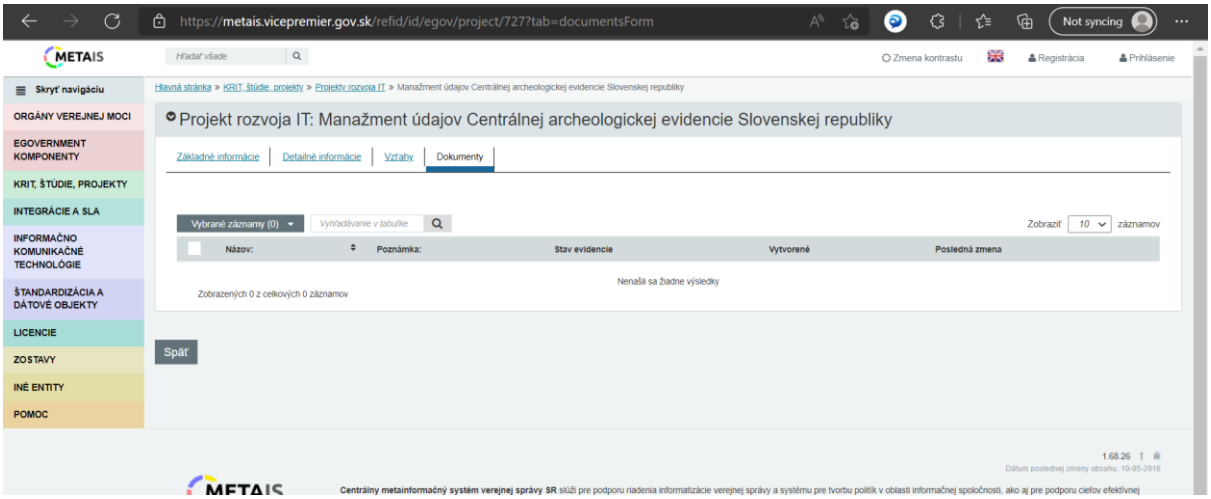
Otázne ale je, či samotný MetaIS je navrhnutý tak, aby poskytoval komfortný spôsob vyhľadávania najmä pre používateľov, ktorý ho nevyužívajú dennodenne. Užívateľsky je systém neprehľadný, neriešený korektne, môže viesť až k zavádzaniu o informáciách pre konkrétny projekt. Príkladom môže byť projekt Manažment údajov Centrálnej archeologickej evidencie Slovenskej republiky, ktorý je schválený, takže v MetaIS má existovať štúdia uskutočniteľnosti (alebo projektový zámer) k danému projektu.

Používateľ sa k nej aj dostane, ale len ak použije základné vyhľadávanie cez Projekty (Obr. 1). Na tej istej vyhľadanej stránke sa má možnosť zvoliť záložku „Základné informácie“, kde je uvedený takzvaný Referencovateľný identifikátor pre priamy prístup k projektu.



Obr. 1 – Vyhľadávanie štúdie uskutočniteľnosti – úspešné

Keď však použije tento identifikátor a pokúsi sa v rovnako pomenovanej záložke „Dokumenty“ vyhľadať už nájdenú štúdiu uskutočniteľnosti k projektu, nenájde žiadny dokument. (Obr. 2). Je predpokladateľné, že zmysel metainformácie nie je v systéme dotiahnutý do konca, respektíve, že oddeľuje typologicky informácie týkajúce sa určitých fáz projektu. Overením tohto predpokladu bolo u iných náhodne vybraných projektov zistené, že tomu tak nie je. Mapovanie tohto stavu, však nie je prioritou zisťovania skutočností v tomto dokumente. Môžeme iba konštatovať, že nastávajú stavy úspešného aj neúspešného vyhľadávania.



Obr. 2 – Vyhľadávanie štúdie uskutočniteľnosti – neúspešné

Nesporne dôležitým predpokladom dopátrania sa aktuálnych a pravdivých informácií je získanie overenej, pravdivej a súčasnej informácie z portálu akéhokoľvek informačného systému. Najmä ak sa jedná o informačný systém verejnej správy. Je preto minimálne divné, že

MetaIS v časti venovanej “Štandardizačným dokumentom” síce malými písmenami poukazuje na stránky http://informatizacia.sk/standardy-is-vs , s komplexnými informáciami o štandardoch, ale na hlavnej stránke má priamy odkaz na Metodický pokyn k výnosu o štandardoch, ktorý priamo poukazuje na 2 roky neplatný a nahradený výnos 55/2014 Z.z. (Obr. 3).

Obr. 3 - Otázka aktuálnosti MetaIS

Stav riešenia kybernetickej bezpečnosti vo vybraných schválených projektoch

Pozrime sa teraz, ako sa preniesli požiadavky vyžiadavky podporené legislatívou do praxe pri vybraných shválených projektoch. Bohužial nemáme priestor, aby sme sa podrobnejšie pozreli na všetky projekty, môžeme si iba stanoviť základné kritériá a pri zhode vybrať náhodne projekty.

Minimálne požiadavky na výber sú:

a) Projekt musí pochádzať z obdobia medzi rokmi 2019 až 2022
b) Výška požadovanej investície, náklady na projekt musia byť nad 1 000 000 EUR
c) Projekt musí byť minimálne v stave „schválený“
d) Operačný program projektu je Operačný program integrovaná infraštruktúra
e) Projekt sa týka informatiky a informačných technológií
f) Projekty majú v metainformačnom systéme zverejnené dokumenty k projektu
g) Názov projektu priamo nepoukazuje na riešenie bezpečnosti

Z výsledkov vyhľadávania boli vybrané nasledovné 4 projekty. Projekty spĺňali základné kritériá, rozdelenie na schválené a realizované bolo už iba na základe dodatočného uváženia, rovnako ako aj výber samotných prijímateľov.

Stav schválený:

1. Manažment údajov Centrálnej archeologickej evidencie Slovenskej republiky, prijímateľ: Archeologický ústav Slovenskej akadémie vied, verejná výskumná inštitúcia
2. Certification Authority, prijímateľ Národná agentúra pre sieťové a elektronické služby

Stav realizovaný:

1. Riešenie konsolidácie registrov OVM, organizácií, fariem a zahraničného obchodu, prijímateľa Štatistický úrad Slovenskej republiky
2. Projekt rozvoja IS pre elektronické služby RÚ, prijímateľa Úrad pre reguláciu elektronických komunikácií a poštových služieb

Na základe zistení priamo z MetaIS mohla vzniknúť nasledovná tabuľka:

Projekt / Hľadaný parameter	**Projekt rozvoja IT: Manažment údajov Centrálnej archeologickej evidencie Slovenskej**	**Certification Authority**	**Riešenie konsolidácie registrov OVM, organizácií, fariem a zahraničného obchodu**	**Projekt rozvoja IS pre elektronické služby RÚ**
V MetaIS je zverejnená štúdia uskutočniteľnosti, či projektový zámer	áno	áno	áno	nie
Náklady na projekt v EUR (plánovaný alebo schválený podľa stavu projektu)	2 139 663	5 259 391,36	2 998 728	8 441 935
Dostupnosť iných projektových dokumentov v MetaIS	áno	áno	áno	áno
Informačná alebo kybernetická bezpečnosť priamo spomenutá v štúdiu uskutočniteľnost, či projektovam zámere	áno	nie	áno	ŠU nie je v MetaIS
Nachádzal sa v MetaIS iný zdroj, ktorý by poukazoval na	Áno, projekt je iba v stave achválený, v rozpočte však už počíta s pozíciou	áno aj...	áno	áno

riešenie bezpečnosti v projektoch?	bezepčnostného špecialistu			
Bola súčasťou štúdie uskutočniteľnosti, alebo projektového zámeru projektov aj bezpečnostná architektúra?	Je spomenutá, ale nie je znázornená	nie	Je spomenutá, ale nie je znázornená	ŠU nie je v MetaIS
Bola súčasťou štúdie uskutočniteľnosti, alebo projektového zámeru samostatná kapitola venovaná bezpečnosti?	áno	nie	áno	ŠU nie je v MetaIS

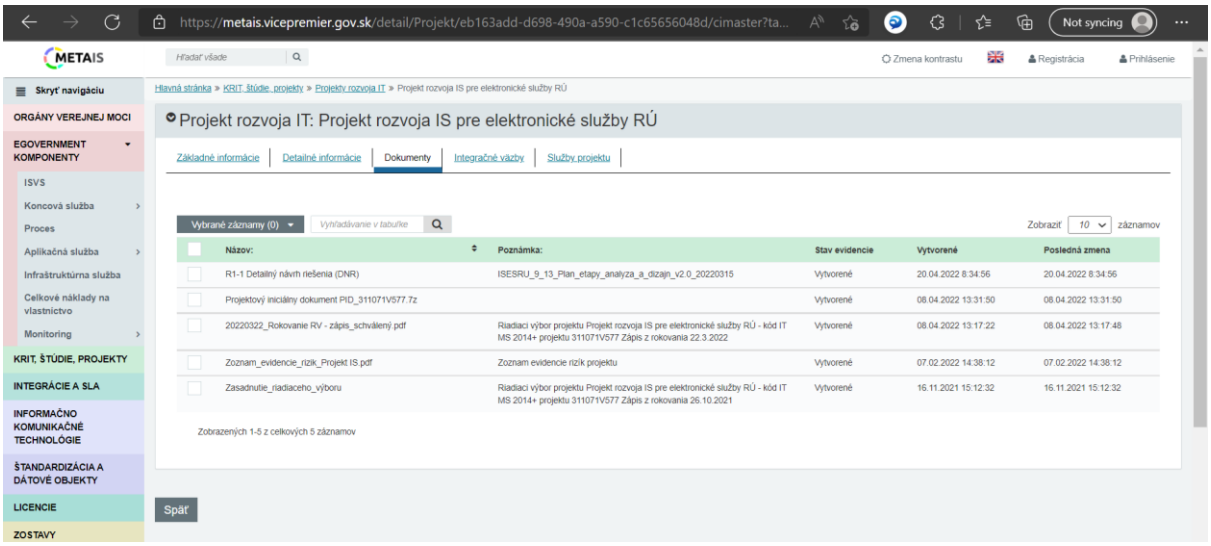
Tab.1 – Porovnanie projektov

Projekt Manažment údajov Centrálnej archeologickej evidencie Slovenskej, aj keď sa nachádza iba v stave schválenia bol príjemným prekvapením. Nielen stavom prepracovanosti predložených dokumentov, ale tým, že sa zaoberal riešením IT bezpečnosti. Aj existencia pracovnej pozície v projekte priamo viazanej na IT bezpečnosť naznačuje, že tento projekt splní všetky kritériá vyplývajúce z našej legislatívy.

Schválený projekt Certification Authority, ktorý ako už vyplýva z názvu mal byť preplnený IT bezpečnosťou je z tohto pohľadu sklamaním. Áno, počíta s odborníkom na predmetnú problematiku, ale to všetko. Tam, kde by mali byť, nie detailné, ale informácie týkajúce sa bezpečnosti - chýbajú. Nedá sa vylúčiť, že autor štúdie vychádzal aj z faktu, že certifikačná autorita musí zahŕňať IT bezpečnosť samotnú, ale nevenovať sa problematike nie je pri takomto projekte ospravedlniteľné.

V projekte Riešenie konsolidácie registrov OVM, organizácií, fariem a zahraničného obchodu je venovaná bezpečnostnej problematike primeraná pozornosť. Aj zastúpením pozície špecialistu pre riešenie IT bezpečnosti, ako aj rozobratím problematiky bezpečnosti ešte pre prípravnú a iniciačnú fázu.

Napriek snahe získať štúdiu uskutočniteľnosti, či projektový zámer projektu Projekt rozvoja IS pre elektronické služby RÚ sa to nepodarilo (Obr. 4). Takýto stav by nemal nastať, už vôbec nie v projekte, ktorý je v realizačnej fáze. Vďaka tejto skutočnosti sme však mohli zistiť, že výstupom projektu má byť návrh bezpečnostnej architektúry. Minimálne podľa dokumentu „Projekt rozvoja IS pre elektronické služby RÚ“, ktorý je dostupný na MetaIS.



Obr. 4 – Dokumenty dostupné pre projekt Projekt rozvoja IS pre elektronické služby RÚ v MetaIS

Záver

Z predložených informácií získaných na základe prehľadania verejne dostupných zdrojov, ktoré pojednávajú o téme verejných projektov financovaných zo zdrojov EU, systémoch verejnej správy, ktoré by mali obsahovať komplexné, úplné a pravdivé informácie a legislatívy k téme kybernetickej bezpečnosti môžeme minimálne povedať:

- Vyhľadávanie aktuálnych a úplných informácií o spôsoboch, formách a povinnostiach v oblasti kybernetickej bezpečnosti v Slovenskej republike je pre bežného, aj keď v príslušnej oblasti vzdelaného používateľa problematické, neprehľadné a mätúce
- Slovenská republika má legislatívne predpisy, ktoré definujú rámec kybernetickej bezpečnosti v inštitúciách
- Vyhláška 85/2020 Z. z. sa kybernetickej a informačnej bezpečnosti dotýka, v celkovom kontexte znenia však dôraz na túto oblasť pôsobí skôr nejednoznačne, akoby sa autor snažil do opisov vložiť všetko, čoho by sa mohol dotýkať TOGAF
- Hodnotenie ISVS: Centrálny metainformačný systém verejnej správy nebolo predmetom článku, ale pri dihľadaní informácií o projektoch sa tento systém ukázal ako kľúčový, nie však jednoducho použiteľný. Jeho komplikovanosť a neprehľadnosť mohla a vnášala nejednoznačnosť a pochybnosti pri zisťovaní zdrojov o projektoch, ktoré by odkazovali na skutočnosť, že informačná a kybernetická bezpečnosť je jednoznačnou zložkou všetkých schválených projektov.

- Napriek malej vzorke posudzovaných dokumentov je jasné, že kvalita schválených projektov je veľmi rozdielna. V prípade jedného projektu sa dokonca zistil stav, ktorý nemal nikdy nastať – zistila sa neexistencia štúdie uskutočniteľnosti v MetaIS
- Napriek nejednoznačnostiam v dokumentoch spojených s prípravnou a iniciačnou fázou projektov sa projekty realizujú s prvkami informačnej a kybernetickej bezpečnosti. Je zrejmé, že v priebehu realizácie sa táto požiadavka riešiť musí

Na základe malej vzorky vybraných projektov sa dá konštatovať, že otázkam kybernetickej a informačnej bezpečnosti je v našich projektoch súvisiacich s rozvojom informačných technológií venovaná pozornosť. Kvalita spracovania témy však značne kolíše, dokonca aj v projektoch, kde by ju nezávislý pozorovať vyslovene očakával. Aj v kvalitatívne dobre pripravených projektoch sa tvorcovia vyhýbajú grafickému znáorneniu bezpečnostnej architektúry. Môže to súvisieť aj so spomínanou skutočnosťou, že bezpečnostná architektúra nie je natívnou súčasťou TOGAF, čo prirodzene predpokladá inú špecializáciu autora predlohy. Aj nedostatok odborníkov, či ich vyťaženosť je možná.

Celkovo však, až na jednu výnimku, dopadlo porovnanie uspokojivo. Je teda predpoklad, že k naplneniu realizácie otázok IT bezpečnosti bude v implementovanom projekte dodržané.

Zoznam použitej literatúry

ISVS: Centrálny metainformačný systém verejnej správy, https://metais.vicepremier.gov.sk/ , dostupné online, naposledy navštívené 25.4.2022

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky, https://www.mirri.gov.sk/ministerstvo/ , dostupné online, naposledy navštívené 24.4.2022

Vyhláška 85/2020 Z.z. Úradu odpredsedu vlády Slovenskej republiky pre investíciea informatizáciu zo 14.apríla 2020, o riadení projektov

Portál Slov-Lex, právny informačný portál, https://www.slov-lex.sk/ , dostupný online, naposledy navštívený 17.4.2022

The Open Group, https://www.opengroup.org/about-us , dostupný online, naposledy navštívený 24.4.2022

Vyhláška 179/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu z. 22. júna 2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

Kontaktné údaje

Bystrík Bindas

FIIT STU Bratislava

E-mail: bystrik.bindas@stuba.sk

Recenzenti: doc. RNDr. Tatiana Hajdúková, PhD.

PhDr. Peter Veselý, PhD.

Hoax – prostriedok elektronickej komunikácie

Alena Buzová

Abstrakt: Elektronická komunikácia je najvýznamnejší vynález modernej spoločnosti. Najmä kvôli výhodám si ju ľudia veľmi obľúbili. Prostredníctvom elektronickej komunikácie si množstvo ľudí tak vymieňa informácie. Avšak okrem dôležitých informácií sa stretávane aj so správami, ktoré sú nám zbytočné, ba až otravné a nebezpečné.

Kľúčové slová: hoax, internet, elektronická komunikácia, správa

Abstract: Electronic communication removes the barriers of time and distance and it allows us efficient, fast and even convient communication.On daily basis the users of electronic communication also come into contact with a number of advertising messages, sending funny e- mails, but also warnings of danger, viruses and malicous softwarw. These messages we can consider to be unsolicited content. In this category, we can include hoax too, which spreads due to peoples lack of information. The aim is to point out the alarm messages – hoax whitch are spread in the enviroment of electronic communication.

Key words: hoax, internet, electronic communitacion, report

Internet

Internet je verejne dostupná celosvetová sieť navzájom prepojených počítačov. Prepojenie počítačov je realizované rôznymi spôsobmi. Dáta sa šíria káblami, vzduchom alebo telefónnymi linkami. Sieť pozostáva z menších komerčných, akademických, vládnych a vojenských sietí. Slúži ako prenosové médium pre rôzne informácie a služby ako napr. www, elektronická pošta a iné.[1]

Službou, ktorú poskytuje internet je elektronické pošta, ktorá je jednou z foriem elektronickej komunikácie.

Elektronická komunikácia

Pod pojmom elektronická komunikácia rozumieme akúkoľvek komunikáciu, čiže spôsob dorozumievania sa medzi ľuďmi, pri ktorej strany medzi sebou komunikujú prostredníctvom dátových správ, čím sa myslí informácia vytváraná, posielaná ale aj prijímaná a uchovávaná

[1] KRUCOVČIN,I. 2015. *Počítačová sieť* [on-line][cit. 2022-03-15]

pomocou elektronických, magnetických optických či podobných prostriedkov vrátane vzájomnej výmeny elektronických dát, elektronického mailu a pod.[2]

Definujeme tieto formy elektronickej komunikácie:

- Elektronická pošta – email
- Internetová telefónia VoIP
- Instat messaging IM

Špecifickým druhom elektronickej komunikácie sú sociálne siete, kde sú používané a kombinované rôzne druhy elektronickej komunikácie

Rozoznávame dva spôsoby elektronickej komunikácie:

1 synchrónny

2. asynchrónny

Synchrónny spôsob nám nahrádza reálnu komunikáciu medzi ľuďmi. Účastníci spolu komunikujú bezprostredne a medzi ich správami nie je žiadny výrazný časový rozdiel. K synchrónnej komunikácií patrí chat , ICQ Skype

Pri asynchrónnom spôsobe nie je nutná okamžitá odozva, a zaraďujeme tu diskusné fóra, ale najmä najpoužívanejší prostriedok a to email.[3]

Elektronická pošta

V roku 1965 sa prvý krát využila. Len čo bolo možné spojiť dva počítačové terminály, ľudia začali robiť niečo, čo po tisícročia hnalo našu civilizáciu vpred a to navzájom komunikovať.

Elektronická pošta : e-mail je obdobou pošty klasickej a je to spôsob písania, posielania a prijímania správ v elektronických komunikačných systémoch.[4]

Internetová telefónia

Internetová technológia nám umožňuje prenos digitalizovaného hlasu v rámci počítačovej siete a je založená na internetovom protokole IP. IP protokol je najpoužívanejší protokol pre

[2] TUŚEROVÁ,L. 2006. *Elektronická komunikace versus elektronické komunikace*. In: epravo.cz
[3] HOSZOWSKI,R. 2013. *Základy informatiky a teorie informacie* [on line][cit.2022-04-10]
[4] KRUCOVČIN,I. 2015. *Počítačová sieť* [on-line][cit. 2022-03-15]

komunikáciu počítačových sietí na internete a je to teda množina popisujúcich prenos dát prostredníctvom siete. Príkladom programu je služba Skype. Aj keď internetovú telefóniu označujeme ako „ telefonovanie zadarmo„ vyžaduje si vstupnú investíciu a to počítač so zvukovou kartou, mikrofón, reproduktor, slúchadlá, prístup do internetu a softvér.

Instatnt Messaging

Služba, ktorá umožňuje online komunikáciu medzi používateľmi, zasielanie správ, chatovanie. Komunikácia tu prebieha v reálnom čase. V porovnaní s VoIP používateľ vie zistiť, či druhá strana je momentálne k dispozícií. Instant messaging teda definujeme ako synchrónny spôsob elektronickej komunikácie.

Sociálne siete

Sociálna sieť je služba založená na webovej platforme, ktorá jednotlivcovi umožňuje konštruovať verejný profil, komunikovať s používateľmi, s ktorými zdieľa pripojenie

K svetovo najpoužívanejším sociálnym sieťam patrí:

- Facebook
- Twitter
- My-Space
- Google
- Linkedln

Spam

Pojem spam uvádza, že označuje rozosielanú nevyžiadanú elektronickú poštu. Ide teda o email, ktorý si príjemca nevyžiadal no napriek tomu mu bol zaslaný. Veľkú časť spamu tvoria reklamné správy, výhodné ponuky na nákupy ale aj ponuky pornografických stránok

HOAX

Elektronická komunikácia patrí medzi najvýznamnejšie vynálezy modernej spoločnosti, no prostredníctvom takejto komunikácie používatelia prijímajú aj množstvo nevyžiadaného obsahu. Okrem spamu, vírusov a reklamy je to hoax a to v rôznych podobách.

Anglické slovo houks znamená v preklade : podvod, fáma, alebo aj falošná správa.

V počítačovom svete ho najčastejšie označujeme ako poplašnú správu, ktorá varuje pred neexistujúcim nebezpečným vírusom. Hoaxom označujeme tiež šírenú správu, ktorá obsahuje nepresné, skresľujúce informácie, účelovo upravené polopravdy alebo zmes poloprávd a lží Takéto správy kolujú na internete roky a postupne sa prekladajú do rôznych jazykov a aj keď je ich obsah absurdný, vždy sa nájdu používatelia, ktorí správu rozpošlú ďalej.

Hoaxové správy sú určitým typom spamu a zároveň môžu byť spojené s ďalšími nepríjemnými malverovými funkciami.[5]

Dôvody vzniku hoaxu

Internet otvoril dvere nielen slušným ľudom, ale je prístupný aj osobám, ktoré využívajú naivitu ľudí alebo len svojou kreativitou vedia využiť situáciu.

Podľa portálu Hoax.sk, ktorý sa venuje internetovým podvodom a klamstvám , hoax vzniká:

- Keď si určité indivíduum uvedomuje svoju zbytočnosť vo virtuálnom svete, cíti svoju slabosť a takýmto spôsobom si chce niečo dokázať
- Keď autor dostane nápad vytvorit klamstvo a tým vyvolá davovú psychózu
- Keď omylom, pri zlom preklade alebo aj nesprávnom pochopení danej veci v rámci témy a nasledovnom očarení závažnosťou faktov, pokračuje v pomýlenej rovine

Autori kvalitných hoaxov využívajú princípy mediálnej komunikácie v kombinácií s pôsobením na city používateľa. Hoaxy pracujú s predstavou o probléme, sú podopreté osobnými dôkazmi a logickými argumentami. Tvrdenia autora sú často doplnené aj obrázkami ako sú napr. obete autonehôd, nebezpečné zvieratá a pod. [10]

Základné znaky

Hoax má špecifickú skladbu textu a taktiež svoje typické základné vlastnosti. Na jeho rozpoznanie je postačujúce riadiť sa niekoľkými pravidlami. Pri opise vírusu alebo pri varovaní pred nebezpečenstvom nesie hoax vo väčšine prípadov rovnaké znaky. Správa sa obvykle

[5] BIRO,P.2014. Hoax. In: informatizacia.sk

začína slovami ako sú pozor, varovanie, nebezpečenstvo. Dôležitosť sa často zvyšuje aj nadmerným použitím výkričníkov a iných znakov, ktoré pútajú pozornosť. [11]

Poplašné správy delíme do týchto znakov:

- Varovanie od dôveryhodného zdroja
- Popis nebezpečenstva
- Ničivé účinky
- Výzva k ďalšiemu rozposlaniu[6]

Varovanie od dôveryhodného zdroja

Autor hoaxu sa snaží presvedčiť, že varovanie prichádza od dôveryhodného zdroja, ako sú napr. štátne orgány, odborníci.

Po prijatí emailu s odkazovaním na dôveryhodné zdroje je skoro isté to , že sa jedná o podvod. Uvádzané autority by nikdy varovania nešírili prostredníctvom reťazových mailov. Veľké firmy ako aj medzinárodné spoločnosti ako hlavnú úlohu varovania volia svoje vlastné internetové stránky, a hlavne masmédia, prostredníctvom ktorých si používateľ môže overiť, či varovanie skutočne pochádza od uvádzaného zdroja.[7]

Možnosťou, ako si overiť pravdivosť prijatej správy , je skopírovanie časti textu do internetového vyhľadávača. Pokiaľ by išlo o hoax, tak vyhľadané predmety budú s najväčšou pravdepodobnosťou odkazovať na stránky HO@X.cz,HOAX.sk a pod. V týchto databázach sa nachádzajú známe hoaxy, ktoré sú popísané a vyvrátené kompetentnými osobami.

Popis nebezpečenstva

V hoaxoch je stručne popísané vymyslené nebezpečenstvo. Text hoaxu obsahuje vymyslený opis údajného nebezpečenstva v podobe nového druhu vírusu alebo zákerného hackera, ktorý preniká do počítačových systémov. Tvorca- autor hoaxu opisuje to, ako sa údajnej hrozbe brániť otvorením správy od vymysleného používateľa, alebo aj neotváraním prílohy s určitým

[6] DŽUBÁK,J. 2015. *Co je hoax*. In: HO@X.cz [online]
[7] URBAN.F. 2013.*Prehľad : Ako HOAX rozpoznať a nenechať sa napáliť*. In: IT News.sk

názvom. Pritom však nemusí ísť len o „ emailovú hrozbu″ ,varovania môžu upozorniť používateľa , aby si nepridával určitého človeka do zoznamu kontaktov v ICQ, Facebooku.[8]

Ničivé účinky

Autori hoaxov pomocou svojej fantázie píšu o účinkoch vírusu . Hoax tak opisuje to, čo sa stane ak čitateľ. Používateľ nepočúvne, pričom uvedie údajné ničivé účinky vírusu. Poplašná správa sa vždy snaží o nebezpečne pôsobiace varovanie a to napr. že dôjde k zmazaniu všetkých súborov na pevnom disku PC, alebo znefunkčnenie operačného systému či odovzdaniu všetkých emailov neznámemu útočníkovi.[9] Hoax sa končí výzvou na ďalšie rozposlanie, pričom drvivá väčšina hoaxov je rozpoznateľná na základe tohto znaku.

Džubák uvádza, že ak správa obsahuje výzvu k hromadnému rozposielaniu na ďalšie adresy, je to podozrivé a s veľkou pravdepodobnosťou ide o hoax

Škodlivosť hoaxov

nám uvádzajú hlavné dôvody škodlivosti hoaxu:

- Nebezpečné rady
- Obťažovanie príjemcov
- Zaťažovanie liniek a serverov
- Strata dôveryhodnosti odosielateľa
- Prezradenie dôverných informácií
- Poškodzovanie cudzej osoby
- Poškodzovanie spoločnosti
- Psychická manipulácia
- Posilňovanie poverčivosti

Šírenie hoaxov a prevencia

Podľa Kopeckého(2010) šíreniu hoaxov napomáha:

- Nekritický príjem informácií
- Vierohodnosť opretá o vedecké fakty
- Vyhrážky a sľuby v hoaxoch
- Dobrý úmysel
- Materinský jazyk

[8] KOPECKÝ,K. 2010.*Hoax*.In: E- bezpečí .cz[on-line]
[9] URBAN.F.2013. Prehľad : *Ako HOAX rozpoznať a nenechať sa napáliť*. In: IT News.sk

Pri prijatí správy, ktorá je podozrivá sa odporúča veriť si jej pravdivosť na niektorom zo serverov s databázami hoaxov. Spôsob ako robiť osvetu atak zastaviť šírenie poplašných správ je kontaktovanie odosielateľa a vysvetlenie mu, čo je zlé a prečo a svoje tvrdenia podoprieť odkazmi na databázy hoaxov.[10]

Poplašnými správami sa okrem databáz zaoberajú aj články v prostredí internetu, ktoré upozorňujú na najnovšie alebo aj opakujúce sa hoaxy.

Podľa Džubáka (2015) poznáme tieto typy hoaxov:

- Varovania pred vírusmi a útokmi na počítač
- Popis nereálneho nebezpečenstva, rôzne varovania či fámy
- Falošné prosby o pomoc
- Hoaxy, ktoré sa týkajú sociálnych sietí
- Urban legends
- Petície či výzvy
- Pyramídové hry
- Žartovné správy, podvodné lotérie

Medzi ďalšie formy hoaxov patria Scamming, Phishing

Vizualizácia najčastejších hoaxov

Slovný mrak je množina slov zadaného textu, kde sú slová usporiadané podľa frekvencie v texte. Frekvencia slova v zadanom texte je vyjadrená veľkosťou alebo farbou, čo znamená čim väčšie slovo, tým vyššia frekvencia výskytu slova. Táto množina je usporiadaná do podoby fiktívnych marakov, z čoho je na pohľad jasné, aké slová hrajú kľúčovú úlohu v texte. Slovné mraky boli použité v rámci internetového portálu, ktoré je zamerané na zdieľanie fotografií.[11]

Tag cloud je vytvorený z 50 hoaxov v slovenskom ale aj českom jazyku

Postup pri spracovaní hoaxov do MRAKU TAGOV

1. Odstránenie stop – slov : slová, ktoré tvoria veľkú časť dokumentov v prirodzenom jazyku, ale neovplyvňujú význam textu. Sú to nevýznamové slová ako sú predložky, spojky
2. Prepis českých slov na slovenské ekvivalenty

[10] ZMEKO,M. 2013. *Základy bezpečnosti na internete*. In: BudOnline.sk[online]
[11] KOPECKÝ,K. 2010.*Hoax*.In: E- Bezpečí.cz[online]

3. Lematizácia : prevod slova na základný tvar, pričom sa každé slovo prepíše na svoj slovníkový tvar
4. Vylúčenie slov s nízkou frekvenciu výskytu
5. Odstránenie slov, ktoré nemajú žiadnu výpovednú hodnotu

Záver

V súčasnosti elektronická komunikácia sa značne podieľa na vývoji modernej spoločnosti. Avšak okrem dôležitých a užitočných informácií sa šíria aj rôzne spôsoby komunikácie nevyžiadaného obsahu, medzi ktoré patrí aj fenomén zvaná hoax.

Keďže hoax je prostriedkom elektronickej komunikácie všade vo svete je aktuálnym problémom a jedným zo spôsobov ako šírenie hoaxov zastaviť je naučiť sa kriticky myslieť. Je preto dôležité, aby sa ľudia naučili rozlišovať aké správy sú pre nich užitočné a ktoré zo správ sú zbytočné. Je dôležité robiť osvetu medi používateľmi elektronickej komunikácie. Pri obdŕžaní podvodnej správy sa odporúča upozorniť odosielateľa ,že takáto správa je hoax. K takémuto upozorneniu by bolo vhodné priložiť odkaz na databázu, kde si používateľ prečíta informácie o danom hoaxe a taktiež aj vyjadrenie odborníkov, ktoré takúto správu vyvracajú.

Súhrn

Elektronická komunikácia nám odstraňuje bariéry času a vzdialenosti a umožňuje nám tak efektívnu, rýchlu ba aj pohodlnú komunikáciu . Používatelia elektronickej komunikácie prichádzajú denne do styku aj s množstvom reklamných správ, preposielaných vtipných emailov, ale aj varovaní pred nebezpečenstvami, vírusmi čo škodlivým softvérom. Tieto správy môžeme považovať za nevyžiadaný obsah. Do tejto kategórie zaradujeme aj hoax, ktorí sa šíri vďaka neinformovanosti ľudí. Cieľom je poukázať na písomne sa prenášajúce poplašné správy-hoaxy, ktoré sa šíria v prostredí elektronickej komunikácie.

Zoznam použitej literatúry

BÍRO,P. 2014. Hoax. In : informatizácia.sk [online].[cit.2022-04-01]. Dostupné na internete: http://www.informatizacia.sk/vdok_simple_hoax

DŽUBÁK,J. 2015. Co je hoax. In: HO@X.cz [online].[cit.2022-04-03]. Dostupné na internete: http://eee.hoax.cz/hoax/co-je to-hoax

HOSZOWSKI,R. 2013. Základy informatiky a teorie informacie[online].[cit. 2022-04-01].Dostupné na internete: http://www.sslch.cz/files/120/ict-hranice.pdf

KOPECKÝ,K. 2010. Hoax. In: E- Bezpečí.cz[online].[cit.2022-04-04]. Dostupné na internete: http:www.e-bezpeci.cz/index.php/ke-stazeni/doc_downolad/5

MACH,M. 2013. Elektronická komunikace [online].[cit.2022-04-11]. Dostupné na internete: http://www.szscb.wz.cz/info/projekty/it3/vy_32_inovace-20.pdf

TUŠEROVÁ,L.2006. Elektronická komunikace versus elektronické komunikace. In: epravo.cz[online]. [cit. 2022-04-11]. Dostupné na internete: http://www.epravo.cz/top/clanky/elektronicka - komunikace-39898html.

URBAN,F.2013. Prehľad: Ako HOAX rozpoznať a nenechať sa napáliť? In: IT News.sk[online] Digital Visions, spol. s.r.o. [cit. 2022-04-03]. Dostupné na internete: http: // www.itnews.sk/tituly/pc-revue/2013

ZMEKO,M. 2013.Základy bezpečnosti na internete. In: BudOnline.sk [online].[cit. 2022-04-04]. Dostupné na internete: http://www.budon-line.sk/storage/files

Kontaktné údaje

Ing. Alena Buzová, MBA

Vysoká škola bezpečnostného manažérstva v Košiciach

Košťova 1, 040 01 Košice

alena.buzova@vsbm.sk

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

doc. RNDr. Tatiana Hajdúková, PhD.

Dezinformace z pohledu studentů bezpečnostních odborů

Marek Čandík

Abstrakt

Článek prezentuje výsledky výzkumu zaměřeného na problematiku dezinformací, který se uskutečnil počátkem roku 2022 na Policejní akademii České republiky v Praze. Do výzkumu se zapojilo 315 respondentů - studentů bezpečnostních oborů PA ČR. Výsledky výzkumu byly zpracované pomocí metod deskriptivní statistiky a statistického zpracování získaných dat.

Klíčová slova: dezinformace, výzkum, statistické zpracování.

Abstract

The paper presents the results of research focused on the issue of disinformation, which took place at the beginning of 2022 at the Police Academy of the Czech Republic in Prague. 315 respondents participated in the research - students of the security fields of PA CR. The research results were processed using the methods of descriptive statistics and statistical processing of the obtained data.

Keywords: disinformation, research, statistical processing.

Úvod

Se zvyšujícím se množstvím informací, jejich snadnou dostupností a rychlostí šíření rostou také rizika, které s nimi souvisí. Problematika vnímání/percepce pravdivých a nepravdivých informací v prostředí internetu se postupně začleňuje do obsahu vzdělávání v rámci tzv. mediální výchovy. Proto je v současné době velmi aktuálním problémem vnímání dezinformací. Dezinformacemi jsou lživé, klamné, nepravdivé informace, které mají za cíl ovlivnit úsudek a názor jedince, více osob či celé společnosti, tak aby vyvolala zdání důvěryhodnosti a pravosti. Někdy je cílem jen zpochybnit původní informaci nebo její pravdivostní hodnotu předstíráním, že existuje jakási alternativní pravda. Rozlišují se dezinformace pasivní, kdy dochází k manipulaci již existující informace, ve smyslu jejího zpoždění, zatajení či likvidace. Druhou skupinou jsou dezinformace aktivní, které jsou vyráběny či záměrně pozměňovány.

Článek prezentuje výsledky výzkumu zaměřeného na problematiku dezinformací, který se uskutečnil počátkem roku 2022 na Policejní akademii České republiky v Praze. Do výzkumu se zapojilo 315 respondentů - studentů bezpečnostních oborů PA ČR.

Metodika výzkumu

Cílem provedeného výzkumu bylo zmapovat, jak vnímají studenti bezpečnostních oborů problematiku dezinformací. Výsledky výzkumu byly následně interpretované pomocí metod deskriptivní statistiky a statistického zpracování získaných dat.

Na základě kvalitativní analýzy odborné literatury byl navržený nestandardizovaný (originální) dotazník. Tento dotazník byl ověřovaný pilotní studii v roce 2022 (leden, únor) a následně byl korigovaný z hlediska validity (přeformulování některých nejasných otázek, vynechání otázek, ve kterých všichni respondenti deklarovali pouze souhlasný, resp. nesouhlasný postoj, atd.).

Získání dat pomocí dotazníkového šetření jsme preferovali z důvodu výhod této efektivní techniky sběru dat. Dotazníkový formulář byl administrovaný ve vytištěné (papírové) podobě (2 listy A4, oboustranně). Dotazníkový formulář byl komponovaný do tří částí. První část obsahovala identifikační znaky respondentů (pohlaví, bydliště, forma studia).

Druhá část dotazníkového formuláře byla tvořena tabulkou znázorňující způsob vyplňování dotazníku (5-bodová Likertova škála; od respondenta se požaduje, aby vyjádřil stupeň souhlasu či nesouhlasu s různými výroky, které se týkají určitého postoje).

Tab. 1. Použitá škála dotazníkového šetření (vlastní výzkum)

5	4	3	2	1
Souhlasím	Částečně souhlasím	Neumím posoudit/ neutrální postoj	Částečně nesouhlasím	Nesouhlasím

Třetí část dotazníkového formuláře představovala zjišťovací část dotazníkového šetření.

Zjišťovací část se skládala ze čtyř okruhů výzkumného šetření:

1. První okruh otázek byl obsahově zaměřený na **znalosti a dovednosti při práci s dezinformacemi.** Tento okruh testování byl tvořený pomocí 6 otázek.

2. Druhý okruh otázek byl obsahově zaměřený na **postoje k dezinformacím.** Tento okruh otázek byl dotazován pomocí 5 otázek.

3. Třetí okruh otázek se zaměřil na **kvalitu vzdělávání v oblasti dezinformací.** Tento okruh otázek byl dotazován pomocí 5 otázek.

4. Čtvrtý okruh otázek se zaměřil na **postoje ke svobodnému šíření informací** a byl dotazován pomocí 4 otázek.

Objekt výzkumu: Dezinformace.

Předmět výzkumu: Postoje studentů bezpečnostních oborů k problematice dezinformací.

Označený základní soubor: Všichni studenti bezpečnostních oborů studující na Policejní akademii České republiky v Praze. V rámci výzkumu byl proveden výběr na základě dostupnosti.

Respondenti: Studenti prezenční a kombinované formy, kteří studují na PA ČR.

Metoda výzkumu: Dotazníkové šetření, s následným matematicko-statistickým vyhodnocením.

Výzkumná otázka: Jak vnímají studenti bezpečnostních oborů problematiku dezinformací?

Výzkumné předpoklady:

VP1: Předpokládáme, že u hodnocení **znalosti a dovednosti při práci s dezinformacemi** nebudou statisticky významné rozdíly **v závislosti na pohlaví**. Vzdělávací systémy nerozlišují pohlaví při systému vzdělávání, proto nelze předpokládat rozdíly statisticky významného charakteru.

VP2: Předpokládáme, že u hodnocení **znalosti a dovednosti při práci s dezinformacemi** nebudou statisticky významné rozdíly **v závislosti na místě bydliště**. Charakter venkova se svým způsobem života velmi přiblížil životu ve městě, vzdělávací systém je unifikovaný, navíc testovaná skupina respondentů má vztah k oblasti bezpečnosti (která s problematikou dezinformací souvisí), nelze proto předpokládat rozdíly statisticky významného charakteru.

VP3: Předpokládáme, že u hodnocení **znalosti a dovednosti při práci s dezinformacemi** nebudou statisticky významné rozdíly **v závislosti na typu vzdělávání.** Obsah vzdělávání prezenčního studia a obsah vzdělávání kombinovaného studia je identický, proto nelze předpokládat rozdíly statisticky významného charakteru.

VP4: Předpokládáme, že u hodnocení **postojů k dezinformacím** nebudou statisticky významné rozdíly **v závislosti na pohlaví.**

VP5: Předpokládáme, že u hodnocení **postojů k dezinformacím** nebudou statisticky významné rozdíly **v závislosti na místě bydliště.**

VP6: Předpokládáme, že u hodnocení **postojů k dezinformacím** nebudou statisticky významné rozdíly **v závislosti na typu vzdělávání.**

VP7: Předpokládáme, že u hodnocení **kvality vzdělávání v oblasti dezinformací** nebudou statisticky významné rozdíly **v závislosti na pohlaví.**

VP8: Předpokládáme, že u hodnocení **kvality vzdělávání v oblasti dezinformací** nebudou statisticky významné rozdíly **v závislosti na místě bydliště.**

VP9: Předpokládáme, že u hodnocení **kvality vzdělávání v oblasti dezinformací** nebudou statisticky významné rozdíly **v závislosti na typu vzdělávání.**

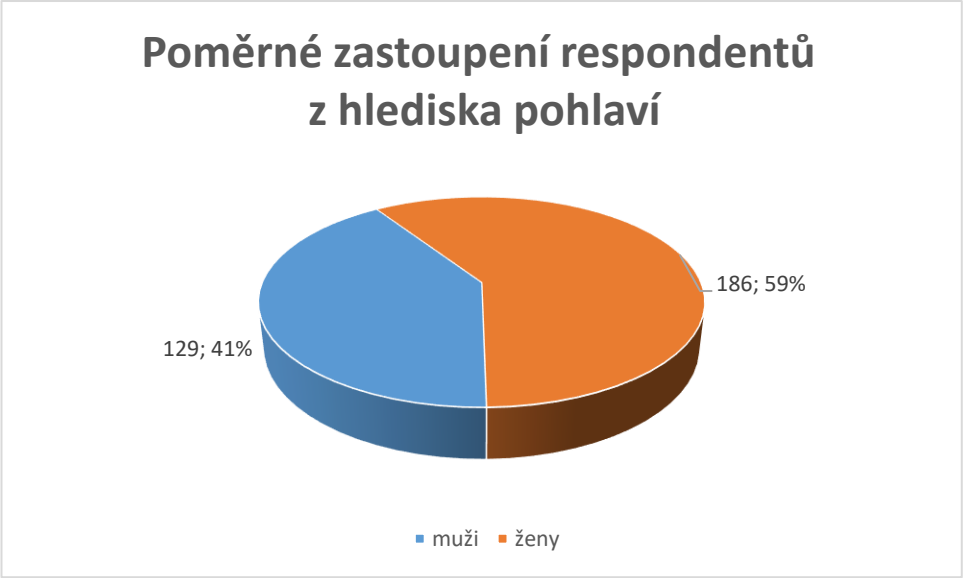
VP10: Předpokládáme, že u hodnocení **postojů ke svobodnému šíření informací** nebudou statisticky významné rozdíly **v závislosti na pohlaví.**

VP11: Předpokládáme, že u hodnocení **postojů ke svobodnému šíření informací** nebudou statisticky významné rozdíly **v závislosti na místě bydliště.**

VP12: Předpokládáme, že u hodnocení **postojů ke svobodnému šíření informací** nebudou statisticky významné rozdíly **v závislosti na typu vzdělávání.**

Pro statistické zpracování jsme data získaná z dotazníkového šetření vložili v numerické podobě do programu MS Excel 2016 a vytvořili jsme základní deskriptivní statistické ukazatele, včetně příslušných grafů. Základní demografické údaje byly analyzovány standardními nástroji deskriptivní statistky. Data jsme následně importovali do softwarového prostředí Statistica v.10, které jsme následně vytěžovali použitím zvolených statistických metod. Ke zpracování dat byly využity adekvátní matematicko-statistické procedury, které jsou obsahem tohoto softwarového prostředí.

Respondenty tvořili studenti Policejní akademie ČR studující bezpečnostní obory. Celkový počet respondentů byl 315. Zkoumaný vzorek tvořili ze 40,95 % muži (129 osob) a ze 59,05 % ženy (186 osob). Zastoupení respondentů z **hlediska pohlaví** znázorňuje níže uvedený obr. 1.



Obr. 1. Struktura respondentů z hlediska pohlaví (vlastní výzkum)

Z hlediska věku se dotazníkového šetření zúčastnili respondenti od 19 do 54 let, průměrný věk respondentů byl 24,77 roků, mediánová hodnota věku byla 23 roky. Nejčetnější skupinou respondentů byli 20-letí studenti (hodnota modusu). Přehled popisných charakteristik respondentů z hlediska věku ukazuje následující tab. 2.

Tab. 2. Popisné charakteristiky respondentů z hlediska věku (vlastní výzkum)

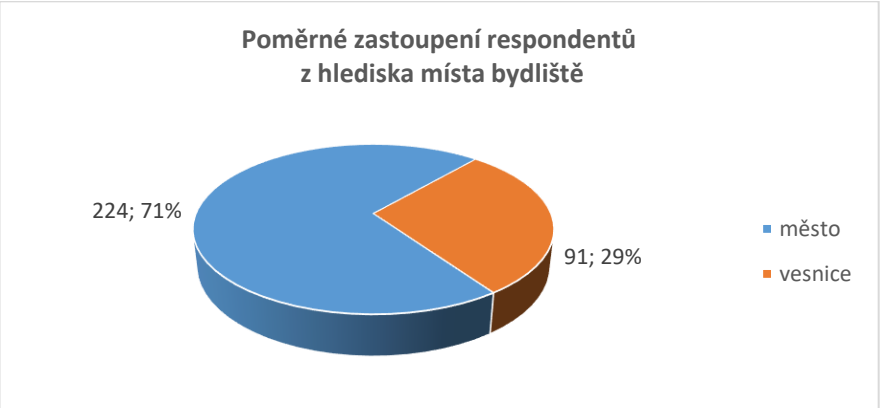
Věk (v letech):	
Minimum	19
Maximum	54
směrodatná odchylka	7,19
Průměr	24,77
Medián	23
Modus	20

U skupiny respondentů mužského pohlaví (186 respondentek, 59 %) se věk pohyboval v intervalu od 19 let (minimum) po 54 roky (maximum), průměrná hodnota věku mužů – respondentů byla 25,85 let, mediánová hodnota dosahovala hodnoty 23 roky, nejčastěji se objevovali respondenti – muži s věkem 20 let (modus).

U skupiny respondentek ženského pohlaví (129 respondentů, 41 %) se věk pohyboval v intervalu od 19 let (minimum) po 52 roky (maximum), průměrná hodnota věku žen –

respondentek byla 24 roky, mediánová hodnota dosahovala hodnoty 22,5 roku, nejčastěji se objevovaly respondentky – ženy s věkem 20 let (modus).

Z hlediska místa bydliště počet respondentů žijících ve městech tvořilo 71,11% (224 respondentů), 28,89 % respondentů žije na venkově (91 respondentů). Zastoupení respondentů z hlediska místa bydliště znázorňuje obr. 2.

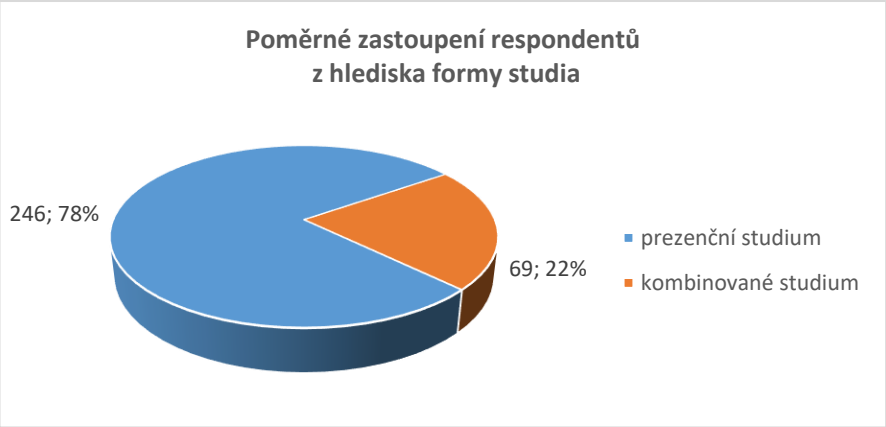


Obr. 2. Struktura respondentů z hlediska místa bydliště (vlastní výzkum)

Skupina respondentů žijících ve městech (71 %, 224 respondentů) dosahovala průměrného věku 24,80 roky, mediánová hodnota jejich věku činila 23 roky, nejčastěji se objevovali respondenti žijící ve městech s věkem 20 let, věkový interval této skupiny respondentů je ohraničen intervalem 19 let (minimum) až 52 let (maximum).

Skupina respondentů žijících na venkově - ve vesnicích (29 %, 91 respondentů) dosahovala průměrného věku 24,68 roky, mediánová hodnota jejich věku činila 22 roky, nejčastěji se objevovali respondenti žijící na venkově s věkem 20 let, věkový interval této skupiny respondentů je ohraničen intervalem 19 let (minimum) až 54 let (maximum).

Z hlediska formy studia počet respondentů studujících v prezenční (denní) formě studia tvořilo 78,10 % (246 respondentů), 21,9 % respondentů studuje v kombinované (dálkové) formě studia (69 respondentů). Zastoupení respondentů z hlediska formy studia znázorňuje obr. 3.



Skupina respondentů studujících v prezenčním (denním) studiu je tvořena 246 respondenty (78 %). Tato skupina dosahovala průměrného věku 21,81 rok, mediánová hodnota jejich věku činila 21 rok, největší věkové zastoupení dosahovali respondenti v prezenčním studiu s věkem 20 let (modus), věkový interval této skupiny respondentů je ohraničen intervalem 19 let (minimum) až 35 let (maximum).

Skupina respondentů studujících v kombinovaném (dálkovém) studiu je tvořena 69 respondenty (22 %). Tato skupina dosahovala průměrného věku 35,3 let, mediánová hodnota jejich věku činila 34 roky, největší věkové zastoupení dosahovali respondenti v kombinovaném studiu s věkem 28 let (modus), věkový interval této skupiny respondentů je ohraničen intervalem 20 let (minimum) až 54 let (maximum).

Ke statistickému vyhodnocení jsme uskutečnili výpočet souhrnů u všech čtyř sledovaných atributů (znalosti a dovednosti při práci s dezinformacemi, postoje k dezinformacím, vzdělávání v oblasti dezinformací, postoje ke svobodnému šíření informací). Protože považujeme každý atribut v hodnocení za stejně důležitý, bylo potřeba, abychom výsledky získaných souhrnů normovali.

Při statistické analýze dat jsme ověřovali podmínky použití statistických testů, a to normalitu a homoskedasticitu/heteroskedasticitu. Normalita byla ověřovaná pomocí Shapiro-Wilksova W-test normality, který byl publikovaný v roce 1965 a je doporučován normou ČSN 01 0225.

Výsledky testu ověření normality uvádí tab. 3.

Tab. 3. Ověření normality základních atributů (vlastní výzkum)

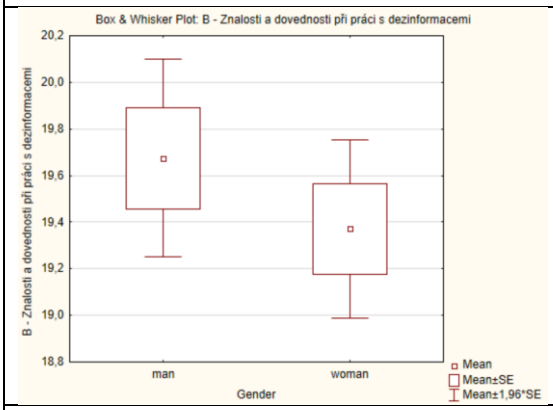
	Shapiro-Wilk		Normalita
znalosti a dovednosti při práci s dezinformacemi	W=,97367	p=,00002	**Zamítnuta**
postoje k dezinformacím	W=,97415	p=,00002	**Zamítnuta**
vzdělávání v oblasti dezinformací	W=,96978	p=,00000	**Zamítnuta**
postoje ke svobodnému šíření informací	W=,96379	p=,00000	**Zamítnuta**

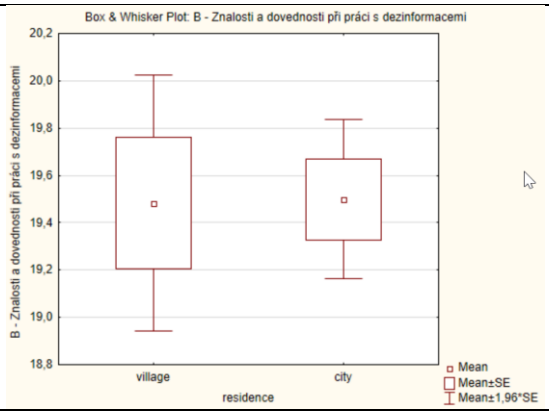
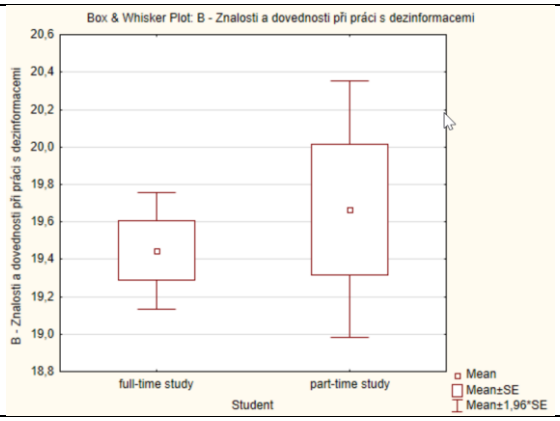
Vzhledem k nesplnění podmínek pro použití parametrických metod testování budou data podrobena analýze pomocí neparametrického Mann-Whitneyova U-testu. Jedná se o neparametrickou obdobu Studentova t-testu pro případ, kdy nejsou splněné podmínky normality a slouží k porovnání mediánů dvou nezávislých proměnných.

Pro každý výzkumný předpoklad (**VP1** – **VP12**) byly stanovené pracovní hypotézy (**H01 - H012** formulované jako shoda testovaného atributu u srovnávaných skupin dle stanoveného kritéria, resp. jejich alternativní hypotézy (HA_1 - HA_{12}) poukazující na odlišnosti mezi testovanými skupinami.

Dosažené výsledky hodnocení znalosti a dovednosti při práci s dezinformacemi dle pohlaví, místa bydliště i formy studia uvádí následující tabulka Tab. 4.

Tab. 4. Dosažené výsledky hodnocení znalosti a dovednosti při práci s dezinformacemi dle pohlaví, místa bydliště i formy studia.

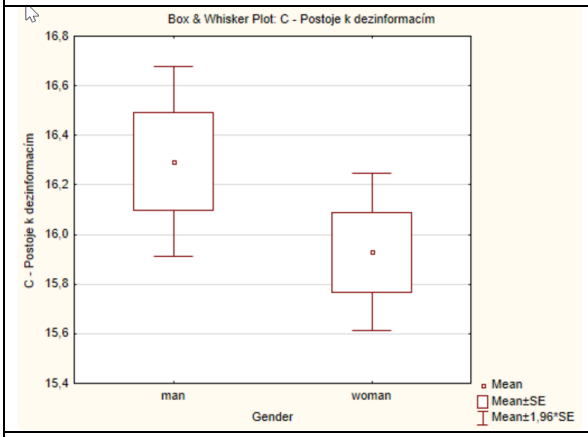
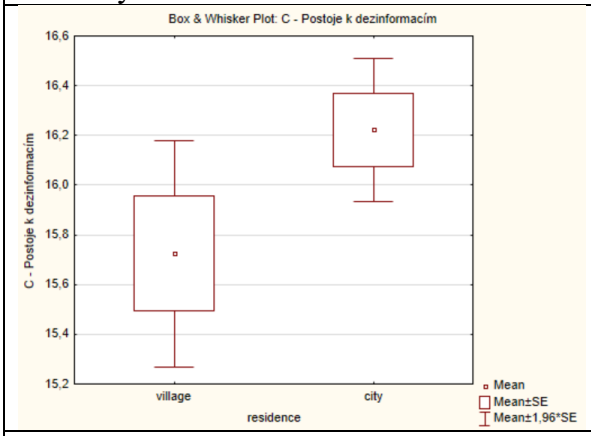
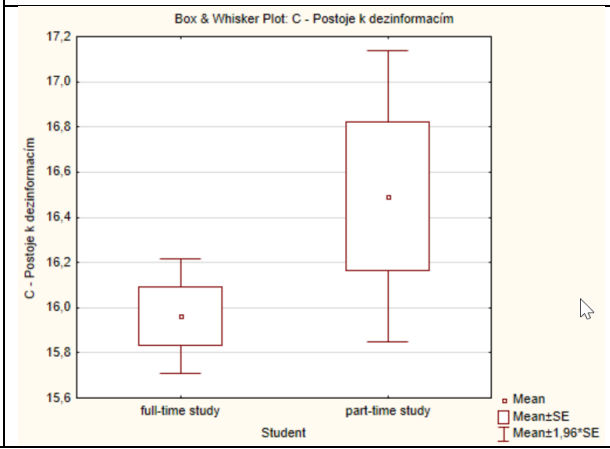
znalosti a dovednosti při práci s dezinformacemi	Pohlaví	
		U=10876,00
		Z=1,409638
		P=0,158648
	Místo bydliště	
		U=10131,00
		Z=-0,082577

		P=0,934188
	Forma studia	
		U=7815,500 Z=-1,00264 P=0,315553

Z grafů prezentovaných v této tabulce je vidět, že znalosti a dovednosti při práci s dezinformacemi dosahují u sledovaných skupin rozdíly (jejich celková míra, případně míra rozptylu ve sledované skupině), které ale **nejsou na 5 % hladině významnosti statisticky významné.**

Výsledky provedeného výzkumu z hlediska vnímání celkového postoje k dezinformacím uvádí Tab. 5.

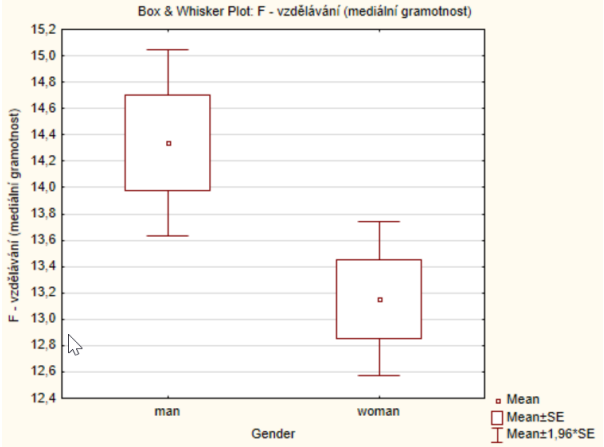
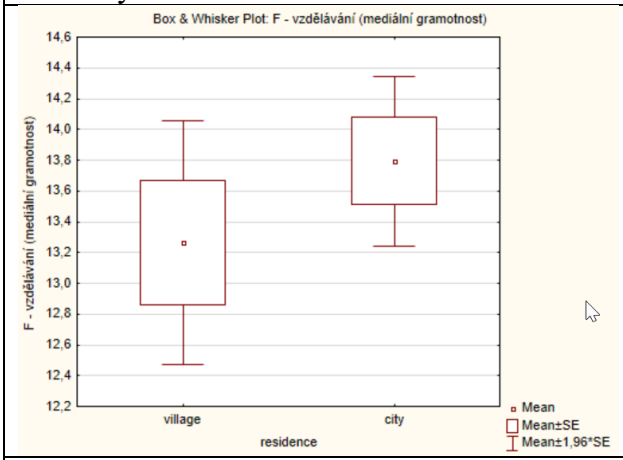
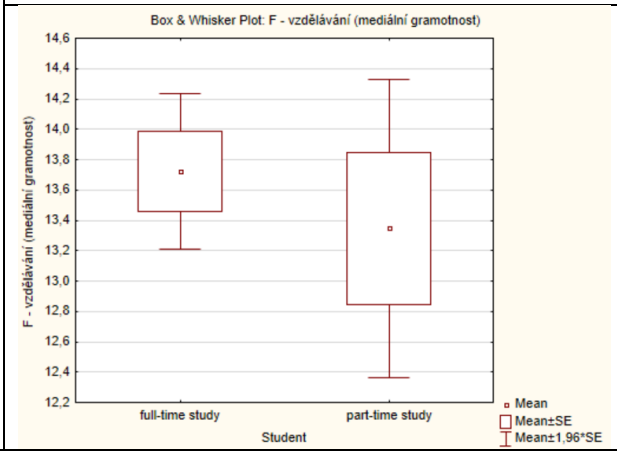
Tab. 5. Dosažené výsledky hodnocení celkového postoje k dezinformacím dle pohlaví, místa bydliště i formy studia.

postoje k dezinformacím	Pohlaví	
		U=10842,50 Z=1,451783 P=0,1451783
	Místo bydliště	
		U=9000,500 Z=-1,62560 P=0,104035
	Forma studia	
		U=7404,000 Z=-1,61913 P=0,105419

Prezentované výsledky v Tab. 5 ukazují, že odlišnosti celkového postoje k dezinformacím ve sledovaných skupinách jsou pozorovatelné, jejich velikost ale **nedosahuje 5 % hladinu statistické významnosti.**

Výsledky provedeného výzkumu z hlediska vnímání kvality vzdělávání v oblasti dezinformací uvádí Tab. 6.

Tab. 6. Dosažené výsledky hodnocení provedeného výzkumu z hlediska vnímání kvality vzdělávání v oblasti dezinformací

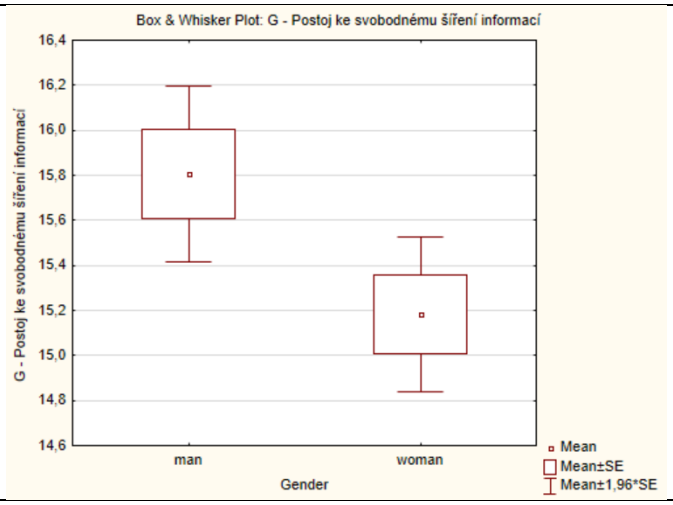
kvalita vzdělávání v oblasti dezinformací	Pohlaví	
		U=10182,00 **Z=2,282720** **P=0,022447**
	Místo bydliště	
		U=9555,000 Z=-0,868762 P=0,384978
	Forma studia	
		U=7965,000 Z=0,780026 P=0,435376

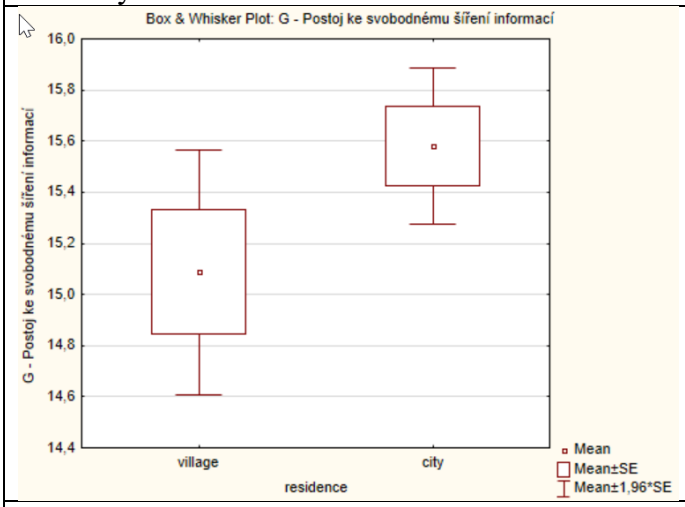
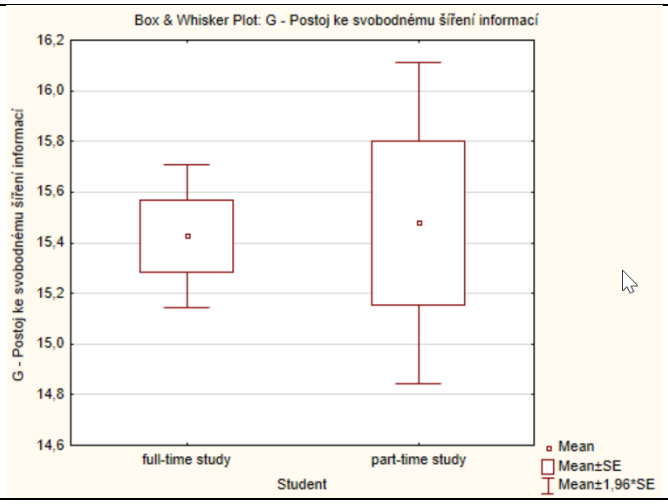
Výsledky Mann-Whitneyova U-testu hodnocení kvality vzdělávání v oblasti dezinformací interpretuje tabulka Tab. 6. Box-ploty naznačují rozdíly *ve vztahu k pohlaví* (Muži hodnotí sledovanou kvalitu vzdělávání lépe než ženy). Neparametrický test (Mann-Whitney) shodu

postojů v závislosti na pohlaví zamítá (na 5 % hladině významnosti), proto zamítáme pracovní hypotézu H07 (která je vztažena k výzkumnému předpokladu VP7: Předpokládáme, že u hodnocení kvality vzdělávání v oblasti dezinformací nebudou statisticky významné rozdíly v závislosti na pohlaví) a přijímáme alternativní hypotézu HA7.(Hodnocení kvality vzdělávání v oblasti dezinformací se liší v závislosti na pohlaví). U proměnných *místo bydliště* a *forma studia* sice krabicové grafy naznačují odlišnosti mezi sledovanými skupinami, výsledky Mannova-Whitneyova U-testu, tyto rozdíly na 5 % hladině významnosti nepotvrdily. Proto pracovní hypotézy o shodě postojů $H0_8$ a $H0_9$, vztahující se k výzkumným předpokladům VP_8 (hodnocení kvality vzdělávání v oblasti dezinformací nebudou statisticky významné rozdíly v závislosti na místě bydliště) a VP_9 (hodnocení kvality vzdělávání v oblasti dezinformací nebudou statisticky významné rozdíly v závislosti na typu vzdělávání) nemůžeme zamítnout na 5 % hladině významnosti.

Výsledky provedeného výzkumu z hlediska vnímání celkového postoje ke svobodnému šíření informací k dezinformacím uvádí Tab. 7.

Tab. 7. Dosažené výsledky vnímání celkového postoje ke svobodnému šíření informací k dezinformacím

<table>
<tr><td rowspan="2">postoje ke svobodnému šíření</td><td>Pohlaví</td><td rowspan="2">U=10000,500
Z=2,511055
P=0,012038</td></tr>
<tr><td> 
</td></tr>
</table>

	Místo bydliště	
		U=8986,000 Z=-1,64539 P=0,099890
	Forma studia	
		U=8100,500 Z=-0,577354 P=0,563701

Shrnutí výsledků ve vztahu k výzkumným předpokladům

Realizovaný výzkum ukázal, že (na 5 % hladině významnosti) existují rozdíly vnímání kvality vzdělávání v oblasti dezinformací z hlediska pohlaví.

Muži hodnotí kvalitu vzdělávání v oblasti dezinformací lépe, než ženy.

Realizovaný výzkum také ukázal, že (na 5 % hladině významnosti) existují rozdíly v celkovém postoji ke svobodnému šíření informací v závislosti na pohlaví.

Muži preferují svobodnější , otevřenější přístup k informacím, než ženy.

Použitá literatura

Cramér, H. (1999). *Mathematical Methods of Statistics*. Princeton University Press. ISBN 978-0691005478.

Meloun, M., Militký, J. (2013). *Kompendium statistického zpracování dat*. Praha: Karolinum. 984 s. ISBN 9788024621968.

Meloun, M., Militký, J. (2012). *Interaktivní statistická analýza dat.* Praha: Karolinum. 960 s. ISBN 9788024621739.

MLEZIVA, Emil: Diktatura informací. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2004. 133 stran. ISBN 80-86898-12-1

MLEZIVA, Emil: Encyklopedie lži, podvádění a klamání. 1. vydání. Praha: Vyšehrad, 2000. 238 stran. ISBN 80-7021-391-4

Kontaktní údaje

Bc. Ing. Marek ČANDÍK, Ph.D., MBA

Katedra managementu a informatiky

Fakulta bezpečnostního managementu

Policejní akademie ČR v Praze Česká republika

e-mail: candik@polac.cz

Recenzenti: doc. RNDr. Tatiana Hajdúková, PhD.

PhDr. Peter Veselý, PhD.

Instant messengery a kybernetická bezpečnosť

Ester Federlová - Ondrej Čupka - Vincent Karovič ml.

Abstrakt: Kybernetická bezpečnosť je jednou z najvýznamnejších tém v oblasti managementu a to oprávnene. Legislatívne zmeny, rastúca kybernetická kriminalita, nízka stíhateľnosť zločincov, škody počítané v miliardách eur, rastúce požiadavky verejnosti o zachovanie súkromia dát sú všetko faktory, ktoré urobili kybernetickú bezpečnosť jednou z ústredných tém manažmentu. Hlavným cieľom bolo oboznámiť čitateľa o kybernetických hrozbách pri používaní instantných messengeroch a vyhodnotiť úroveň zabezpečenia najpoužívanejších aplikácií na posielanie správ na trhu. Tento cieľ bol dosiahnutý skúmaním relevantnej literatúry z verejného a súkromného sektora. V príspevku vytvárame úvod do problematiky v oblasti kybernetickej bezpečnosti, popisujeme štyri vybrané aplikácie na posielanie správ. Na záver sme definovali päť odporúčaní ako chrániť bezpečnosť aplikácie.

Kľúčové slová: Instantné messengery, kybernetická bezpečnosť, bezpečnosť dát

Abstract: Cyber security is one of the most important management topics, and rightly so. Legislative changes, growing cybercrime, low criminal prosecution, billions of euros in damages, growing public demands for data privacy are all factors that have made cyber security one of the central topics of management. The main goal was to acquaint the reader with cyber threats when using instant messengers and to evaluate the level of security of the most used messaging applications on the market. This goal was achieved by examining the relevant public and private sector literature. In this article we create an introduction to issues in the field of cyber security, we describe four selected applications for messaging. Finally, we defined five recommendations on how to protect the security of the application.

Key words: Instant messengers, cybersecurity, data security

Úvod

Instantné messengery umožňujú efektívnu komunikáciu, ktorá umožňuje okamžité prijatie a odosielanie správ. Používateľom umožňuje nielen komunikovať, ale aj vysoko efektívnym spôsobom spolupracovať prostredníctvom množstva funkcií, ktoré presahujú len odosielanie a prijímanie správ, ale zahrňujú posielanie fotografií a videí. Nie je preto prekvapením, že instantné messengery majú miliardy používateľov na celom svete a nachádzajú sa na takmer každom osobnom zariadení. Avšak nesú so sebou bezpečnostné riziká. Prostredníctvom týchto aplikácií možno spáchať takmer akúkoľvek formu narušenia bezpečnosti alebo počítačovej kriminality. Preto je dôležité zabezpečiť, aby bolo zariadenie pred týmito útokmi chránené, a tiež aby sa všetci používatelia programov na odosielanie okamžitých správ dozvedeli o nebezpečenstvách ich používania.

Čo je kybernetická bezpečnosť

Kybernetická bezpečnosť je slovenským zákonom 69/2018 Z. z. v §3 ods. g) definovaná, ako „stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov“.[1]

Čím sa čiastočne odlišuje od definície, z ktorej vychádzajú firmy poskytujúce kybernetickú bezpečnosť a antivírovú ochranu, ktoré definujú kybernetickú bezpečnosť ako súbor postupov alebo prax, nie ako stav.[2] Lepšie povedané, zatiaľ čo zákon Slovenskej republiky vníma kybernetickú bezpečnosť ako statickú, podniky poskytujúce kybernetickú ochranu ju pokladajú za dynamickú a aktívnu. Vzhľadom na povahu kybernetických hrozieb, ktoré sa neustále menia v intenzite a úrovni sofistikovanosti, sa prikláňame k definícii zdôrazňujúcej dynamickosť kybernetickej bezpečnosti, ktorá ju vníma skôr ako proces.

Kybernetická bezpečnosť sa týka troch oblastí, technológie, procesov a ľudí.[3]

- *Technológia* – týka as všetkých technologických riešení, ktoré slúžia ochrane dát, siete, počítačov, serverov, cloudu alebo mobilných zariadení. Bežná ochrana zahŕňa využívanie firewallov, DNS filtrovanie, ochrana pred malwarom, antivírový program alebo systémy ochrany elektronickej komunikácie.[4] Ale aj prvky fyzickej ochrany, ako kamerové systémy, kartové čítačky obmedzujúce vstup ku kľúčovej sieťovej infraštruktúre alebo aj systém zabezpečenia v prípade výpadku energie.
- *Procesy* - sú súborom všetkých aktivít a postupov týkajúcich sa technologických zariadení. Cieľom kybernetickej bezpečnosti je ich upraviť tak, aby sa minimalizovalo riziko.[5] Napríklad častou zmenou hesla, systémom autentifikácie zariadení a zamestnancov, zostavením postupov pri odhalení pokusu o kybernetický útok a iné.
- *Ľudia* - predstavujú ten najmenej predvídateľný článok pri zabezpečení kybernetickej bezpečnosti a súčasne aj najčastejším cieľom pri kybernetických

[1] Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
[2] CISCO: *What Is Cybersecurity?* [online] [cit. 28.04.2022]. Dostupné na internete: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
[3] CISCO: *What Is Cybersecurity?* [online] [cit. 28.04.2022]. Dostupné na internete: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
[4] Tamtiež
[5] Tamtiež

útokoch. Preto je vzdelávanie užívateľov kľúčová pre zabezpečenie systémov. Cieľom je, aby užívatelia rešpektovali bezpečnostné pokyny, používali silné heslá, vymazali podozrivé emaily, nesťahovali nepovolené softvéry a súbory a nepripájali neznáme zariadenia, ako USB nosiče.[6]

Význam kybernetickej bezpečnosti

V súčasnosti je ťažké si predstaviť svet bez elektronických zariadení, čo je nepopierateľným znakom ich užitočnosti, pohodlnosti používania a globálneho významu. Zatiaľ čo bolo evidovaných v roku 2000 približne 738 mil. aktívnych mobilných zariadení, dnes to je viac ako 8 miliárd.[7] Ale asi ešte významnejší, ako elektronické zariadenia, je systém, ktorý väčšinu z nich spája, internet. V roku 2000 ho používalo iba 6,5% globálnej populácie, dnes to je viac ako 50% alebo viac ako 3,5 miliardy ľudí.[8] Táto široká dostupnosť, prepojenosť a štandardizácia má nepochybné benefity pre efektivitu komunikácie, pracovnú produktivitu, ekonomickú aktivitu a iné. Avšak vlastnosti, ktoré robia tieto systémy tak užitočné a cenné, ich robia súčasne aj zraniteľné. Široká dostupnosť a pohodlnosť používania spôsobuje, že sú používane aj úplnými laikmi, ktorí nie sú oboznámení s hrozbami, ktoré pri používaní môžu nastať alebo ako ich minimalizovať. Prepojenosť, najmä prostredníctvom internetu, spôsobujú, že hrozby môžu pochádzať od ľudí z akejkoľvek krajiny, čím sa umožňuje medzinárodná kybernetická kriminalita, ktorá sa len ťažko môže právne stíhať. Štandardizácia znamená, že je len otázkou času, kým budú zraniteľnosti systému odhalené a zneužité tretími stranami.

Dáta vážnosť tejto situácie iba potvrdzujú. V roku 2018 bolo zaznamenaných 812 mil. útokov na systémy pomocou malwaru, z ktorých viac ako 90% bolo uskutočnených prostredníctvom emailu.[9] V rovnakom roku bolo zaznamenaných 204 mil. útokov pomocou ransomware.[10] Priemerná škoda takéto útoku predstavovala približne 133 tis. USD. Očakáva sa, že v roku 2021 bude takto globálne napadnutá jedna organizácia každých 11 sekúnd.[11]

[6] KASPERSKY. What is Cyber Security? In: *www.kaspersky.com* [online] [cit. 17.04.2022]. Dostupné na internete: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
[7] SVETOVÁ BANKA. Mobile cellular subscriptions. In: [cit. 02.05.2022]. Dostupné na internete: https://data.worldbank.org/indicator/IT.CEL.SETS
[8] SVETOVÁ BANKA. Individuals using the Internet (% of population) | Data. In: [cit. 02.05.2022]. Dostupné na internete: https://data.worldbank.org/indicator/it.net.user.zs
[9] PURPLESEC. 2019 Cyber Security Statistics Trends & Data. [online] [cit. 03.05.2022]. Dotupné na internete: https://purplesec.us/resources/cyber-security-statistics/
[10] STATISTA. Number of ransomware attacks per year 2019. In: *Statista* [online] [cit. 03.05.2022]. Dostupné na internete: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/
[11] PURPLESEC. 2019 Cyber Security Statistics Trends & Data. [online] [cit. 03.05.2022]. Dotupné na internete: https://purplesec.us/resources/cyber-security-statistics/

Očakáva sa, že celkové ekonomické škody kybernetickej kriminality dosiahnu v tomto roku 6 biliónov USD.[12] Pritom je iba približne 5% kybernetických zločincov zadržaných policajnými zložkami[13] a z nich je iba približne 1% odsúdených.[14]

Vysoké ekonomické škody spôsobené kybernetickou kriminalitou a nevymáhateľnosť práva robia silnú a aktívnu kybernetickú bezpečnosť kľúčovú, ak nie nevyhnutnú, pre každú organizáciu.

Zásady kybernetickej bezpečnosti

Problematika kybernetická bezpečnosti má mimoriadne veľkú šírku a hĺbku. Zabezpečenie technológií, procesov a ľudí, ako aj detailné charakterizovanie zdrojov rizika, ktoré každý prvok v organizácií môže vyvolať, predstavujú veľkú výzvu pre každú organizáciu. Avšak dlhoročnými skúsenosťami existuje súbor osvedčených postupov, ktoré môže každá organizácia rýchlo aplikovať pre zníženie rizika úspešných útokov na jej systémy.

- *Ochrana dát* – Veľká časť našich životov sa presunula do kybernetického sveta, ktorý v jeho užívateľoch vytvára pocit bezpečia a súkromia. V súčasnosti je bežné zadávať pre najrôznejšie dôvody svoje osobné údaje do systémov, delenie sa o zážitky pomocou fotiek a videí online alebo písanie si súkromných správ aj s osobami, ktoré sme nikdy osobne nevideli. Tento falošný pocit dôvery spôsobuje, že užívatelia sa delia o dáta, ktoré by osobne nikomu nedali. Pritom je možné z videí a fotiek nepozorných zamestnancov získať utajené informácie z obrazoviek alebo tabúľ v pozadí alebo dokonca vytvoriť kópiu preukazu, za určitých okolností aj kľúčov. Tie potom môžu byť spojené s údajmi zo sociálnych sietí alebo s údajmi zadanými na falošných webových stránkach a útočník má všetky potrebné údaje pre účinný útok „social engineeringu“. Takto môžu vzniknúť vysoké škody pre zamestnanca a firmu. Nestačí len ochrana dát zo strany softvéru alebo hardvéru, ale

[12] HERJAVEC. The 2020 Official Annual Cybercrime Report. In: *Herjavec Group* [online] [cit. 03.05.2022]. Dostupné na internete: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/
[13] STRAWBRIDGE, G. How Do Hackers Normally Get Caught? In: *MetaCompliance* [online] [cit. 03.05.2022]. Dostupné na internete: https://www.metacompliance.com/blog/how-do-hackers-normally-get-caught/
[14] GRIMES, R.A. Why it’s so hard to prosecute cyber criminals. In: *CSO Online* [online] [cit. 03.05.2022]. Dostupné na internete: https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html

aj potrebná ostražitosť v kybernetickom priestore a to v pracovnom aj súkromnom živote.[15]

- *Vyhýbanie sa podozrivým odkazom, súborom a emailom* – Pomocou phishing, wishing a smishing sa najčastejšie vykonávajú útoky social engineeringu. Prostredníctvom falošných emailov, telefonátov alebo správ SMS. Neraz sú používané, aby získali údaje od obetí týchto útokov, ale najmä v prípade phishingu je cieľom dostať do systému malware. Toto môže útočník dosiahnuť tým, že užívateľ otvorí súbor, klikne na odkaz alebo reklamu. Potom, v závislosti od útoku a prístupov, ktoré má zariadenie, tak je možné napadnúť nie len dané zariadenie, ale systémy organizácie. Autentifikácia a filtrácia emailov, vytvorenie white- alebo blacklistov webových stránok, obmedzenie prístupov na nevyhnutnú úroveň a vzdelanie zamestnancov sú základom, pri prevencií pred takými útokmi.[16]
- *Silné heslá a autentifikácia* – Heslá sú vstupnými dverami do väčšiny systémov a predstavujú preto najväčšiu zraniteľnosť. Nie je náhodou, že vo väčšine veľkých útokov na systémy organizácie bolo významným prvkom slabé heslo. Jednoduché, ľahko uhádnuteľné a krátke heslá všetky spadajú do kategórie slabých hesiel. Je preto potrebné, aby užívatelia vytvárali komplikované heslá s použitím aspoň 8 znakov, čísel, malých a veľkých písmen a s použitím špeciálnych znakov. Taktiež je potrebné myslieť aj na uhádnuteľnosť. Heslo ako „Heslo.123“ spĺňa tieto podmienky, ale bolo by aj jedno z prvých, ktoré by útočník skúšal. Databáza by preto mala tiež obsahovať zoznam najčastejších hesiel, ktoré sa nesmú používať.[17] Avšak týmto vzniká ďalší problém, tzv. „password fatigue“, kedy sú užívatelia unavený z počtu ťažko zapamätateľných hesiel. Toto neraz vedie k tomu, že sú heslá nevhodným spôsobom ukladané v súboroch na počítači alebo jednoducho napísané na papier v blízkosti zariadenia. Užívatelia by mali byť medzi iným aj učení prečo a ako správne uchovávať a tvoriť heslá.[18] Dodatočným spôsobom ochrany, najmä pre kľúčové systémy, je multifaktorová autentifikácia, kedy užívateľ nezadáva iba heslo, ale napríklad kód, ktorý mu bol odoslaný na mobilné

[15] FEDERAL COMMUNICATIONS COMMISSION USA. Cybersecurity for Small Business. In: *Federal Communications Commission* [online] [cit. 14.04.2022]. Dostupné na internete: https://www.fcc.gov/general/cybersecurity-small-business

[16] NORTON. 10 Cybersecurity Best Practices that Every Employee Should Know. In: [cit. 14.04.2022]. Dostupné na internete: https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html

[17] CHAUHAN, S., PANDA, N.K. Online Security. In: CHAUHAN, S., PANDA, N.K. eds. *Hacking Web Intelligence* [online]. Boston: Syngress, 2015 [cit. 14.02.2021]. DOI: 10.1016/B978-0-12-801867-5.00011-2

[18] TOMKINS, B. Dealing With Password Fatigue. In: *Forbes* [online] [cit. 14.04.2022]. Dostupné na internete: https://www.forbes.com/2009/04/24/single-sign-on-entrepreneurs-technology-bmighty.html

zariadenie v SMS správe. Útočník pravdepodobne nebude mať prístup k obom heslám súčasne, čím sa môže útoku zabrániť.[19]

- *Bezpečné internetové pripojenie* – Útoky typu „man-in-the-middle“, kedy všetka dátová komunikácia medzi zariadením a internetom prechádza cez zariadenie útočníka, hrozia v prípade nezabezpečených pripojení. Týmto útokom sa dá zabrániť káblovým pripojením alebo zabezpečenou a skrytou wifi v organizácií. Avšak ani tie nemusia dostatočne ochrániť systémy a neponúkajú nutnú flexibilitu pre zamestnancov pracujúcich mimo pracoviska. Tieto opatrenia je nutné doplniť šifrovaním dát a používaním VPN pripojenia, ak zamestnanci pracujú mimo pracoviska.[20]
- *Ochrana firewallom a antivírusom* – Firewall je prvou ochrannou líniou väčšiny systémov. Bráni nepovoleným užívateľom získať prístup na webové stránky, emailové služby a iné zdroje informácií. Firewall by mal byť preto vždy aktívny a vhodne nastavený.[21] Antivírus je softvér, ktorý odhaľuje prítomnosť vírusov na zariadení a odstraňuje ich. Takýmto spôsobom sa firewall a antivírus dobre dopĺňajú. Antivírusy v súčasnosti ponúkajú aj doplnkové služby, ako blokovanie nebezpečných webových stránok, kontrola emailovej komunikácie alebo bezpečné skartovanie súborov.[22]
- *Časté aktualizácie softvéru a zálohovanie údajov* – Softvér je tvorený ľuďmi a pre ľudí, preto sa v nich nachádzajú chyby a zraniteľné miesta, ktoré môže útočník využiť. Z toho dôvodu je pre bezpečnosť systémov dôležité ich často aktualizovať, aby mohli byť tieto chyby napravené.[23] Kybernetické útoky sa často sústreďujú na dáta, ktoré sú kradnuté, znehodnocované, mazané alebo zneprístupnené. Zálohovanie kľúčových dát môže byť záchranou pre danú organizáciu. Treba však podotknúť, že by mali byť zálohované offline na externých pevných diskoch alebo v cloude.[24]

[19] FEDERAL COMMUNICATIONS COMMISSION USA, Cybersecurity for Small Business [online] [cit. 14.04.2022]. Dostupné na internete: https://www.fcc.gov/general/cybersecurity-small-business
[20] NORTON, 10 Cybersecurity Best Practices that Every Employee Should Know [online] [cit. 14.04.2022]. Dostupné na internete: https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html
[21] Tamtiež
[22] CHAUHAN, PANDA, Online Security [online] [cit. 14.04.2022]. DOI: 10.1016/B978-0-12-801867-5.00011-2
[23] Tamtiež
[24] NORTON, 10 Cybersecurity Best Practices that Every Employee Should Know [online] [cit. 14.04.2022]. Dostupné na internete: https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html

- *Kontakt s IT oddelením* – Je pochopiteľné, že nie každý v organizácií dôkladne rozumie, ako jednotlivé časti digitálneho systému organizácie fungujú alebo ako sú medzi sebou prepojené a na seba pôsobia alebo ako riešiť komplikovanejšie problémy. Častý kontakt a dôvera k IT oddeleniu dokáže predísť vzniku vážnej hrozby pre integritu systému a vyriešiť problémy, než dôjde vážnejším problémom.[25]
- *Kontrola tretích strán* – Úniky dát nastávajú často vo vnútri organizácie a nie počas externých útokov hackerov. Takéto úniky nastávajú najčastejšie zo strany tretích strán, ktoré majú alebo nadobudnú neoprávnený prístup k dátam. Tieto tretie strany môžu byť externý konzultanti, poskytovatelia softvéru, bývalý zamestnanci, ktorým nebol odobraný prístup a pod. Tretie strany by mali byť preto vždy kontrolované a ich prístup limitovaný.[26]
- *Vzdelávanie* – Žiadna z vyššie menovaných zásad a opatrení nebude fungovať bez znalosti a ochoty zamestnancov ich dodržiavať. Tréning zamestnancov by mal byť preto prioritou pre organizácie. Výsledkom takého tréningu je bezpečnejšia organizácia, ktorá predchádza škodám pre organizáciu a jej klientov a má nižšie náklady na vedenie technickej podpory.[27]

Instantné messengery a pandémia Covid-19

Pandémia Covid-19 zmenila asi všetky oblasti ľudského života na celej planéte a ani oblasť kybernetickej bezpečnosti sa nevyhla zmenám. Zatváranie ekonomík a zákaz vychádzania spôsobil bezprecedentné množstvo zamestnancov pracujúcich z domu. Dá sa predpokladať, že zhoršujúca ekonomická situácia tiež viedla väčší počet ľudí ku kybernetickej kriminalite. Za rok 2020 bol takto zaznamenaný až šesťnásobný nárast prípadov kybernetickej kriminality, najmä prostredníctvom phishingových útokov.[28]

Presun pracovného a súkromného života do kybernetického priestoru a výrazný nárast útokov predstavujú skutočnú výzvu pre kybernetickú bezpečnosť. Súčasťou problému je

[25] NORTON, 10 Cybersecurity Best Practices that Every Employee Should Know [online] [cit. 14.04.2022]. Dostupné na internete: https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html
[26] Tamtiež
[27] Tamtiež
[28] PURPLESEC. 2019 Cyber Security Statistics Trends & Data. [online] [cit. 03.05.2022]. Dotupné na internete: https://purplesec.us/resources/cyber-security-statistics/

mazanie hraníc medzi osobným a pracovným časom. Keď používatelia pracujú z domu, môže byť ťažké držať sa jednej aplikácie na odosielanie správ pre osobné aj pracovné správy. Niektorí zamestnanci a dokonca aj celé tímy si teda vyvinuli svoje vlastné kanály na odosielanie správ – v niektorých prípadoch bez vedomia IT oddelení ich spoločnosti.[29]

Instantný messenger

Instantný messenger je aplikácia pre odosielanie rýchlych/okamžitých správ, skr. IM, ktorý je systémom alebo spôsobom na komunikáciu prostredníctvom textových správ, ktoré sa posielajú prostredníctvom počítačovej siete v reálnom čase. Hlavným problémom bezpečnosti aplikácií na odosielanie správ je rozsah, v akom môžu tretie strany potenciálne čítať súkromné správy, spoločnosti stojace za aplikáciami alebo dokonca vlády, ktoré zhromažďujú údaje o svojich občanoch.[30]

Pri hodnotení zabezpečenia aplikácie na odosielanie správ je potrebné vziať do úvahy:[31]

1. End-to-end šifrovanie - End-to-end šifrovanie zakóduje vaše súkromné chatové správy a iba odosielateľ a príjemca správ majú „kľúče“ na ich čítanie.

2. Otvorený zdrojový kód - Otvorený zdrojový kód znamená, že aplikácia je otvorená externej zodpovednosti a auditu zo strany odborníkov, čo môže byť užitočný spôsob, ako upozorniť na akékoľvek slabé miesta alebo zraniteľné miesta v kóde.

3. Miznúce správy - Miznúce správy zmiznú po uplynutí nastaveného času v závislosti od zvolených nastavení.

4. Použitie údajov - Aj keď mnohé aplikácie na bezpečné odosielanie správ používajú šifrovanie typu end-to-end, stále môžu o vás zhromažďovať údaje, ktoré sa nazývajú metadáta. Patria sem informácie, ako napríklad s kým hovoríte, ako dlho, na akom zariadení, vaša IP adresa a telefónne číslo.

[29]https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/messaging-apps-pose-security-issues.aspx
[30] KASPERSKY.Messaging app security: Which are the best apps for privacy? In: www.kaspersky.com [online] [cit. 17.04.2022]. Dostupné na internete: https:// www.kaspersky.com/ resource-center/preemptive-safety/messaging-app-security
[31] KASPERSKY.Messaging app security: Which are the best apps for privacy? In: www.kaspersky.com [online] [cit. 17.04.2022]. Dostupné na internete: https:// www.kaspersky.com/ resource-center/preemptive-safety/messaging-app-security

Facebook Messenger

Facebook Messenger je bezplatná mobilná aplikácia, ktorá umožňuje chat, hlasovú a video komunikáciu medzi komunikačnými službami webovej stránky Facebooku a smartfónom. Messenger je dostupný pre zariadenia so systémom iOS, Android, Windows a Blackberry a môže sa pripojiť cez Wi-Fi alebo mobilné dáta. Messenger má stovky miliónov používateľov po celom svete[32]

Messenger predstavuje aj po niekoľkých rokoch verejných prísľubov na zlepšenie bezpečnosti jednou z málo bezpečných instantných messengerov na trhu. Asi najväčším problémom aplikácie je, že iba čiastočne ponúka šifrovanie end-to-end. To znamená, že akékoľvek dáta posielané cez túto aplikáciu môžu byť bez akéhokoľvek úsilia prečítané, ak by boli odchytené po celej trase z odosielajúceho zariadenia po cieľové zariadenie. Existuje možnosť konkrétne konverzácie šifrovať, ale iba po nastavení užívateľom a nie automaticky. Väčšina používateľov nemá znalosti o tejto funkcií. Avšak aj v prípade šifrovania je šifrovací kľúč v rukách spoločnosti, čím sa nemôže garantovať rešpektovanie súkromia organizáciou a kýmkoľvek s prístupom k šifrovaciemu kľúču.[33] Facebook v minulosti priznal, že skenuje správy všetkých užívateľov, ktoré obsahujú fotky alebo odkazy, či dodržiavajú pravidlá používania. Avšak je otázne, či rovnaký systém nie je využívaný aj na iné účely.[34] Zdrojový kód aplikácie nie je verejný a tak nie je možné overiť z nezávislých zdrojov jej bezpečnosť. Správy sú trvalo zálohované.[35]

Ako sme naznačovali, hrozba prichádza aj zo strany spoločnosti Facebook, v súčasnosti Meta. Hlavným zdrojom príjmov z prevádzky sociálnych služieb sú príjmy z reklamy a predaja užívateľských dát. To znamená, že samotný architektúra služby je postavená na sledovaní, zbieraní, vyhodnocovaní, predaji a využívaní dát jej používateľov. Čo ponúka mnoho príležitostí na zneužitie, či už oficiálnym alebo neoficiálnym spôsobom. Ako príklad môže slúžiť škandál z roku 2018 so spoločnosťou Cambridge Analytica, ktorá zneužila rovnaké

[32] WIGMORE, I. What is Facebook Messenger? In: *WhatIs.com* [online] [cit. 12.05.2022]. Dostupné na internete: https://www.techtarget.com/whatis/definition/Facebook-Messenger
[33] DOFFMAN, Z. Why You Should Stop Using Facebook Messenger. In: *Forbes* [online] [cit. 12.05.2022]. Dostupné na internete: https://www.forbes.com/sites/zakdoffman/2020/07/25/why-you-should-stop-using-facebook-messenger-encryption-whatsapp-update-twitter-hack/
[34] FRIER, S. Facebook Scans the Photos and Links You Send on Messenger. In: *Bloomberg.com* [online]. 2018 [cit. 12.05.2022]. Dostupné na internete: https://www.bloomberg.com/news/articles/2018-04-04/facebook-scans-what-you-send-to-other-people-on-messenger-app
[35] DOFFMAN, Why You Should Stop Using Facebook Messenger [online] [cit. 12.05.2022]. Dostupné na internete: https://www.forbes.com/sites/zakdoffman/2020/07/25/why-you-should-stop-using-facebook-messenger-encryption-whatsapp-update-twitter-hack/

metódy, aké využíva Facebook, aby získala osobné údaje miliónov jeho používateľov. Tieto dáta následne zneužívala v prospech politických kampaní.[36] Alebo zverejnenie interných dokumentov a štúdií Facebooku, tzv. Facebook Papers, bývalou zamestnankyňou Frances Haugenovou koncom roka 2021. Tá označila toto sociálne médium za hrozbu pre demokraciu, miesto radikalizujúce spoločnosť, kde beztrestne operuje kriminalita a existuje značná skupina používateľov, na ktorých sa žiadne pravidlá nevzťahujú a ktorej členstvo je určené množstvom generovaných príjmov. Pričom zverejnené dokumenty dokazujú znalosť Facebooku o týchto skutočnostiach.[37] Aj z týchto dôvodov nepokladáme za vhodné vkladať dôveru do služieb tejto spoločnosti.

Whatsapp

WhatsApp je bezplatná mobilná aplikácia a aplikácia na odosielanie správ, ktorú vlastní Facebook. WhatsApp sa používa na odosielanie šifrovaných videí, hlasových hovorov a textových správ po celom svete, na ktoré stačí Wi-Fi pripojenie. Aplikácia bola spustená v roku 2009, ale skutočný nárast počtu používateľov nastal, keď ho v roku 2014 kúpil Facebook. Dnes je WhatsApp celosvetovo najpopulárnejšou aplikáciou na odosielanie správ s viac ako 2 miliardami používateľov na celom svete.[38]

Správy posielané prostredníctvom Whatsapp sú, na rozdiel od Facebook Messenger, šifrované end-to-end, čím je z tohto hľadiska bezpečnejší. Avšak rovnako, ako Facebook Messenger, nie je zdrojový kód aplikácie Whatsapp verejný, čím sa nedajú tvrdenia o bezpečnosti užívateľských dát overiť nezávislými stranami. Taktiež nie je šifrovací kľúč ukladaný výlučne na zariadeniach používateľov, ako pri Signale. Zálohovanie správ je možné nastaviť používateľom, avšak preferencia je daná na trvalé ukladanie. Aplikácia však napriek

[36] WONG, J.C. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. In: *The Guardian* [online]. 2019 [cit. 12.05.2022]. Dostupné na internete: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

[37] MILMO, D. Frances Haugen: 'I never wanted to be a whistleblower. But lives were in danger'. In: *The Observer* [online]. 2021 [cit. 12.05.2022]. Dostupné na internete: https://www.theguardian.com/technology/2021/oct/24/frances-haugen-i-never-wanted-to-be-a-whistleblower-but-lives-were-in-danger

[38] DOFFMAN, Z. Yes, You Can Still Use WhatsApp—But Change These 3 Critical Settings First. In: *Forbes* [online] [cit. 13.05.2022]. Dostupné na internete: https://www.forbes.com/sites/zakdoffman/2021/01/12/you-can-use-whatsapp-after-facebook-apple-imessage-and-signal-backlash-but-change-this/

end-to-end šifrovaniu zbiera dáta od svojich používateľov a existujú rovnaké otázky dôveryhodnosti spoločnosti, ktorá ju prevádzkuje, ako pri Facebook Messengeri.[39]

Signal

Signal sa považuje za jednu z najbezpečnejších aplikácií na odosielanie správ na trhu. Používateľská skúsenosť je podobná ako v iných populárnych chatovacích aplikáciách, ako sú WhatsApp a Messenger. Signal existuje od roku 2013, ale v rokoch 2020 a 2021 sa jeho popularita rýchlo zvýšila. Signal je open-source projekt podporený grantmi a darmi. To znamená, že neexistujú žiadne reklamy a ani tie pridružené. Konverzácie na signáli sú end-to-end šifrované. To znamená, že ich môžu vidieť iba ľudia v konverzácii a nikto iný (dokonca ani vlastníci Signalu). Iné aplikácie na odosielanie správ ponúkajú šifrovanie typu end-to-end ako možnosť, ale v systéme Signal je to predvolené nastavenie. Signal ponúka samodeštrukčné, miznúce správy, ktoré sa po uplynutí nastaveného času automaticky odstránia. Signal sa snaží nezbierať príliš veľa údajov o svojich užívateľoch. Všetko vo vašej aplikácii vrátane správ, obrázkov a súborov, je uložené lokálne vo vašom telefóne.[40]

Telegram

Telegram bol založený v roku 2013. Základná funkcia Telegramu je rovnaká ako väčšina ostatných aplikácií na odosielanie správ: môžete posielať správy ostatným používateľom telegramu, vytvárať skupinové konverzácie, telefonovať kontakty a odosielať súbory a nálepky. Telegram vyzval hackerov, aby sa pokúsili prelomiť ich šifrovanie a dešifrovať správy. Telegram má program odmeňovania za chyby, ktorý zostáva otvorený a nabáda bezpečnostných výskumníkov, aby predložili akékoľvek bezpečnostné problémy v aplikáciách alebo protokole Telegramu. Podania, ktoré vedú k zmene na konci telegramu, môžu vyhrať odmeny v rozmedzí od 500 do 100 000 USD. Súťaže a programy, ako je tento, pomáhajú zabezpečiť, aby sa našli a opravili všetky potenciálne slabé miesta. Telegram tiež používa end-to-end šifrovanie. Šifrovanie telegramu bráni komukoľvek mimo obojsmernej konverzácie – či

[39] DOFFMAN, Yes, You Can Still Use WhatsApp—But Change These 3 Critical Settings First [online] [cit. 13.05.2022]. Dostupné na internete: https://www.forbes.com/sites/zakdoffman/2021/01/12/you-can-use-whatsapp-after-facebook-apple-imessage-and-signal-backlash-but-change-this/

[40] KASPERSKY.Messaging app security: Which are the best apps for privacy? In: www.kaspersky.com [online] [cit. 17.04.2022]. Dostupné na internete: https:// www.kaspersky.com/ resource-center/preemptive-safety/messaging-app-security

už spoločnosti, vláde, hackerom alebo niekomu inému – vidieť, čo bolo odoslané. Telegram však toto šifrovanie používa iba pri hovoroch a svojej funkcii „tajných rozhovorov“, nie pri bežných rozhovoroch. Ide iba o šifrovaný klient na server. Existuje možnosť samo deštrukcie správ, súborov, fotografií a videí v určitom čase po ich odoslaní a prijatí. Po prijatí správy zostane v chate nastavenú dobu. Môžete si vybrať časy od jednej sekundy do jedného týždňa. Keď bude váš účet určitý čas neaktívny (predvolená hodnota je šesť mesiacov), účet sa automaticky zničí a úplne vymaže vaše správy a médiá.[41]

Obrázok 1 Dáta, ktoré sú zbierané a viazané na užívateľa pri Facebook Messenger, WhatsApp a Signal[42]

Odporúčania, ako chrániť bezpečnosť aplikácie

Okrem zabezpečenia samotných aplikácií, tipy, ako zostať v bezpečí online pri odosielaní správ ostatným, zahŕňajú:[43]

[41] KASPERSKY.Messaging app security: Which are the best apps for privacy? In: www.kaspersky.com [online] [cit. 17.04.2022]. Dostupné na internete: https:// www.kaspersky.com/ resource-center/preemptive-safety/messaging-app-security

[42] LOVEJOY, B. App privacy labels show stark contrasts among messaging apps. In: *9to5Mac* [online] [cit. 13.05.2022]. Dostupné na internete: https://9to5mac.com/2021/01/04/app-privacy-labels-messaging-apps/

[43] ROBB, Drew. Messaging Apps Pose Security Issues. In SHRM [online] [cit. 04.05.2022]. Dostupné na internete: https://www.shrm.org/resourcesandtools/hr-topics/ technology/pages/ messaging-apps-pose-security-issues.aspx

1. Vyhnite sa používaniu verejných Wi-Fi sietí bez VPN. Pre mnohých je neoceniteľná, ale môže predstavovať bezpečnostné problémy. Keďže verejné siete zvyčajne používa veľa ľudí, môžu byť hlavným cieľom hackerov. Hackeri môžu ľahko snímať údaje, ako sú fotografie, správy, heslá, používateľské mená a bankové informácie odoslané cez Wi-Fi. Používanie siete VPN vás môže chrániť pred akýmkoľvek narušením bezpečnosti.

2. Vyhnite sa odosielaniu citlivých informácií prostredníctvom chatovacích aplikácií alebo prostredníctvom textových správ.

3. Vyhnite sa poskytovaniu hesiel, informácií o kreditných kartách alebo iných súkromných údajov prostredníctvom správ. Buďte opatrní pri prezrádzaní akýchkoľvek osobných údajov cudzincovi, s ktorým sa stretnete, prostredníctvom okamžitých správ. Dokonca aj zdanlivo nevinné informácie, ako je meno vášho zamestnávateľa, môžu byť zneužité proti vám podvodníkmi.

4. Dávajte si pozor na to, na aké odkazy pri chatovaní klikáte. Nikdy neklikajte na odkazy, ktoré dostanete prostredníctvom správ od ľudí, ktorých nepoznáte, ktorým nedôverujete a v skutočnom živote ste ich nikdy nestretli, aby ste sa nestali obeťou phishingového podvodu.

5. Chráňte svoj telefón pomocou bezpečnostného softvéru. Okrem zabezpečenia svojho zariadenia heslom alebo kódom PIN sa uistite, že ste chránení bezpečnostným softvérom.

Záver

Okamžité správy umožňujú používateľom pohodlne komunikovať medzi sebou. Ide o typ online chatu, vďaka ktorému používateľ komunikuje v reálnom čase pomocou textových správ. Počet používateľov instantných messengerov sa zvyšuje, pretože vďaka tomu je konverzácia veľmi spontánna a pohodlná. Existuje množstvo aplikácií na odosielanie okamžitých správ, pomocou ktorých môžu používatelia jednoducho odosielať a prijímať textové správy okamžite. V príspevku sme sa venovali kybernetickej bezpečnosti, zásadám kybernetickej bezpečnosti, aplikáciám na posielanie okamžitých správ a ich úrovni zabezpečenia. Na záver sme zadefinovali päť odporúčaní pre bezpečné používanie instantných messengerov. Medzi odporúčania sme zaradili uprednostňovanie súkromných internetových sietí pred verejnými. Pri používaní verejných sietí by používatelia mali mať zabezpečené pripojenie pomocou VPN. Používatelia by sa mali vyhnúť odosielaniu citlivých informácií cez

instantné messengery. Užívatelia by mali byť opatrní pri klikaní na odkazy. A posledným odporúčaním je zabezpečiť zariadenie aj pomocou kódu a bezpečnostného softvéru.

Zoznam použitej literatúry

CISCO. What Is Cybersecurity? In: *Cisco* [online] [cit. 28.04.2022]. Dostupné na internete: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

DOFFMAN, Zak. Why You Should Stop Using Facebook Messenger. In: *Forbes* [online] [cit. 12.05.2022]. Dostupné na internete: https://www.forbes.com/sites/zakdoffman/2020/07/25/why-you-should-stop-using-facebook-messenger-encryption-whatsapp-update-twitter-hack/

DOFFMAN, Zak. Yes, You Can Still Use WhatsApp—But Change These 3 Critical Settings First. In: *Forbes* [online] [cit. 13.05.2022]. Dostupné na internete: https://www.forbes.com/sites/zakdoffman/2021/01/12/you-can-use-whatsapp-after-facebook-apple-imessage-and-signal-backlash-but-change-this/

FEDERAL COMMUNICATIONS COMMISSION USA. Cybersecurity for Small Business. In: *Federal Communications Commission* [online] [cit. 14.02.2021]. Dostupné na internete: https://www.fcc.gov/general/cybersecurity-small-business

FRIER, Sarah. Facebook Scans the Photos and Links You Send on Messenger. In: *Bloomberg.com* [online]. 2018 [cit. 12.05.2022]. Dostupné na internete: https://www.bloomberg.com/news/articles/2018-04-04/facebook-scans-what-you-send-to-other-people-on-messenger-app

GRIMES, Roger A. Why it's so hard to prosecute cyber criminals. In: *CSO Online* [online] [cit. 03.05.2021]. Dostupné na internete: https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html

HERJAVEC. The 2020 Official Annual Cybercrime Report. In: *Herjavec Group* [online] [cit. 03.05.2022]. Dostupné na internete: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

CHAUHAN, Sudhanshu, PANDA, Nutan Kumar. Online Security. In: CHAUHAN, Sudhanshu, PANDA, Nutan Kumar. eds. *Hacking Web Intelligence* [online]. Boston: Syngress, 2015, s. 203-216 [cit. 14.04.2022]. ISBN 978-0-12-801867-5. DOI: 10.1016/B978-0-12-801867-5.00011-2

KASPERSKY. Messaging app security: Which are the best apps for privacy? In: *www.kaspersky.com* [online] [cit. 17.04.2022]. Dostupné na internete: https:// www.kaspersky.com/ resource-center/preemptive-safety/messaging-app-security

KASPERSKY. What is Cyber Security? In: *www.kaspersky.com* [online] [cit. 17.04.2022]. Dostupné na internete: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

MILMO, Dan. Frances Haugen: 'I never wanted to be a whistleblower. But lives were in danger'. In: *The Observer* [online]. 2021 [cit. 12.05.2022]. ISSN 0029-7712. Dostupné na internete: https://www.theguardian.com/technology/2021/oct/24/frances-haugen-i-never-wanted-to-be-a-whistleblower-but-lives-were-in-danger

NORTON. 10 Cybersecurity Best Practices that Every Employee Should Know. In: [cit. 14.04.2022]. Dostupné na internete: https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html

PURPLESEC. 2019 Cyber Security Statistics Trends & Data. [online] [cit. 03.05.2022]. Dotupné na internete: https://purplesec.us/resources/cyber-security-statistics/

ROBB, Drew. Messaging Apps Pose Security Issues. In SHRM [online] [cit. 04.05.2022]. Dostupné na internete: https://www.shrm.org/resourcesandtools/hr-topics/ technology/pages/ messaging-apps-pose-security-issues.aspx

STATISTA. Number of ransomware attacks per year 2019. In: *Statista* [online] [cit. 03.05.2022]. Dostupné na internete: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

STRAWBRIDGE, Geraldine. How Do Hackers Normally Get Caught? In: *MetaCompliance* [online] [cit. 03.05.2022]. Dostupné na internete: https://www.metacompliance.com/blog/how-do-hackers-normally-get-caught/

SVETOVÁ BANKA. Individuals using the Internet (% of population) | Data. In: [cit. 02.05.2022]. Dostupné na internete: https://data.worldbank.org/indicator/it.net.user.zs

SVETOVÁ BANKA. Mobile cellular subscriptions. In: [cit. 02.05.2022]. Dostupné na internete: https://data.worldbank.org/indicator/IT.CEL.SETS

TOMKINS, Benjamin. Dealing With Password Fatigue. In: *Forbes* [online] [cit. 14.04.2022]. Dostupné na internete: https://www.forbes.com/2009/04/24/single-sign-on-entrepreneurs-technology-bmighty.html

WIGMORE, Ivy. What is Facebook Messenger? In: *WhatIs.com* [online] [cit. 12.05.2022]. Dostupné na internete: https://www.techtarget.com/whatis/definition/Facebook-Messenger

WONG, Julia Carrie. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. In: *The Guardian* [online]. 2019 [cit. 12.05.2022]. ISSN 0261-3077. Dostupné na internete: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

Kontaktné údaje

Univerzita Komenského

Fakulta managementu, Katedra informačných systémov

Odbojárov 10

P.O.BOX 95
820 05 Bratislava 25

Ester Federlová
federlova2@uniba.sk
Orcid ID: 0000-0001-5745-5282

Ondrej Čupka
cupka9@uniba.sk
Orcid ID: 0000-0002-7857-6355

Vincent Karovič ml.
vincent.karovic6@fm.uniba.sk
Orcid ID: 0000-0001-9946-7329

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP
doc. RNDr. Tatiana Hajdúková, PhD.

Zneužívanie elektronických služieb na sexuálne zneužívanie detí

Tatiana Hajdúková

Abstrakt: Technológiami sprostredkovaná vzdialená komunikácia prináša okrem nesporných výhod aj negatíva, akými sú páchanie trestnej činnosti alebo spoločensky nevhodného správania. Cieľom príspevku je poukázať na prítomnosť problému distribúcie materiálov sexuálneho zneužívania a vykorisťovania detí (CSAM), ktorých výskyt v čase pandémie COVID 19 signifikantne vzrástol. Zverejňovania alebo šírenia nevhodných videí alebo obrázkov detí sú výrazným spôsobom porušované ich práva na zdravý a harmonický vývoj. V digitálnom svete bez hraníc má sexuálne zneužívanie detí globálne dôsledky, s čím je nutné primerane zvyšovať úsilie na boj proti nemu koordinovane s intenzívnou medzinárodnou spoluprácou. V obsahu príspevku konkretizujeme nástroje, ktoré slúžia na elimináciu výskytu tohto javu, jeho odhaľovanie a dokazovanie.

Kľúčové slová: internet, elektronické služby, materiál sexuálneho zneužívania detí, odhaľovanie, dokazovanie, medzinárodná spolupráca

Abstract: In addition to indisputable advantages, remote communication mediated by technologies also brings negatives, such as the commission of criminal activity or socially inappropriate behavior. The aim of the paper is to highlight the presence of the problem of distribution of child sexual abuse and exploitation materials (CSAM), the occurrence of which has increased significantly during the COVID 19 pandemic. Publishing or spreading inappropriate videos or pictures of children is a significant violation of their rights to healthy and harmonious development. In a digital world without borders, sexual abuse of children has global consequences, with which it is necessary to increase the efforts to combat it in coordination with intensive international cooperation. In the content of the contribution, we specify the tools that serve to eliminate the occurrence of this phenomenon, its detection and proof.

Key words: internet, electronic services, child sexual abuse material, detection, evidence, international cooperation

Úvod

Násilné správanie je častý spôsob presadzovania vlastnej vôle voči inému jedincovi, hoci aj proti jeho vôli. Ochrana pred násilím patrí k pilierom ľudských práv a slobôd vyspelej demokratickej spoločnosti, pretože je to jediný možný spôsob, ako nepristúpiť na vynucovanie osobných záujmov na úkor iných. Pocit bezpečnosti a stability je nevyhnutný predpoklad akéhokoľvek rozvoja, či už osobnostného, ako aj spoločnosti.[44] Zabezpečenie ochrany pred násilím predstavuje komplexnú úlohu riešiteľnú jedine systematickou participáciou viacerých subjektov spoločnosti, medzi dotknuté patria napríklad orgány útvary Policajného zboru,

[44] LISOŇ, M., FIDLER, Ľ. 2022. Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb. In Policajná teória a prax : časopis Akadémie Policajného zboru v Bratislave, ISSN 1335-1370. s. 47.

prokuratúry, súdov, neziskových organizácií, obcí a samosprávnych krajov na národnej aj medzinárodnej úrovni. Násilník si obvykle nevyberá seberovného protivníka, pretože si pri ňom nemôže byť istý svojím víťazstvom. V prípade presadzovania sa založenom na fyzickej prevahe je obvyklým násilníkom muž voči deťom alebo žene.[45] Deti sú na prejavy násilia, zneužívania a vykorisťovania oveľa jednoduchšia korisť ako dospelé osoby. Ich väčšia zraniteľnosť vyplýva z prebiehajúceho fyzického a psychického vývoja, z čoho pramení ich nezrelosť, prirodzená zvedavosť, dôverčivosť, naivnosť, nevedomosť a túžba po zakázanom, byť výnimočný. Jednou zo základných povinností spoločnosti je autoritatívne zabezpečiť podmienky na ochranu detí pred negatívnymi vplyvmi okolia, kým nedospejú. Za týmto účelom okrem vyššie spomenutých subjektov spoločnosti participujú aj orgány sociálnoprávnej ochrany detí a sociálnej kurately, školy, zdravotnícke zariadenia, resocializačné zariadenia a v neposlednom rade rodina. Dieťa nemusí byť v bezpečí ani zatvorené za dverami detskej izby v byte plnom ľudí. Každý rodič by mal mať primárny záujem poskytnúť svojim deťom čo najväčší pocit ochrany a bezpečia.

Kontaktné a bezkontaktné formy násilia

Formy násilia, miera ich ubližovania a následkov sú rôzne.[46] Najčastejšie praktizovaná klasická prevaha dosahovaná fyzickou silou je podmienená osobnou prítomnosťou dotknutých osôb a obvykle sa u detí deklaruje ako vychovávanie či trestanie. Podobný, v mnohých prípadoch deštrukčnejší následok na psychike dieťaťa môže byť dosahovaný verbálnym spôsobom ako je nadávanie, ponižovanie, zastrašovanie, vydieranie. Verbálne násilie sa dá tlmočiť aj na diaľku napríklad v online prostredí, kde sa pocity zahanbenia a poníženia umocňujú veľkým počtom zdieľaní s inými osobami. Popularita online prostredia medzi mladými ľuďmi sa zakladá v ich širokom vplyve na ostatných ľudí, čo súčasne poskytuje priaznivejšie príležitosti pre šírenie fám, klebiet, dezinformácií a v neposlednom rade bezkontaktného násilia. Vďaka pôsobeniu viacerých faktorov sme na internete otvorenejší, dokážeme hovoriť o intímnejších veciach a to aj častokrát s ľuďmi, ktorých poznáme len krátky čas, alebo len online. Dôležité je zaujať, dostať sa do centra pozornosti,. V skutočnosti to nie sú reálne úspechy ktoré by budovali zdravé sebavedomie, je to len zdanie úspechu, ktoré rýchlo vyprchá. Teraz, keď vo väčšine krajín viac ako polovica všetkých detí používa stránky

[45] F. VLACH, R.. RAK. Czech prison staff training and enhancement in the times of pandemic. In L. Gómez Chova, A. López Martínez, I. Candel Torres. EDULEARN21 Proceedings. 13th International Conference on Education and New Learning Technologies. Spain. Published by IATED Academy, 2021. 4887 p. ISBN 978-84-09-31267-2. doi:10.21125/edulearn.2021.1007. https://library.iated.org/view/VLACH2021CZE

[46] KIŠŠOVÁ, M. 2022. Násilná kriminalita a s ňou súvisiace fenomény. In Policajná teória a prax : časopis Akadémie Policajného zboru v Bratislave, ISSN 1335-1370. s. 20.

sociálnych sietí aspoň raz týždenne, je možno ešte pozoruhodnejšie, že nie všetky deti tak robia: polovica španielskych detí a niečo vyše 40 % detí vo Francúzsku, Nemecko a Malta nikdy alebo takmer vôbec nenavštevujú stránku sociálnej siete.[47]

Na základe Health Behaviour in School-aged Children“ viac ako 15 % teenegerov súhlasilo s tým, že je pre nich jednoduchšie na internete hovoriť o tajomstvách, vnútorných pocitoch a obavách v porovnaní so stretnutím tvárou v tvár.[48] Podľa štúdie Eu Kids Online viac ako štvrtina teenegerov považuje za jednoduchšie byť samým sebou v online priestore.[49] Tento fenomén pomenoval profesor Suler ako **disinhibičný efekt**.[50] Pojem disinhibícia znamená zbavenie sa zábran a následné vyjadrovanie sa bez obmedzenia vnímaného počas osobného stretnutia. Napriek väčšiemu pocitu bezpečia plynúcemu z anonymity a neviditeľnosti, môže práve z tohto dôvodu dochádzať u detí a mladých ľudí, ktorí ešte nemajú v takej miere vyvinuté kritické myslenie, k ohrozeniu a rýchlemu nadviazaniu dôverného vzťahu s niekým, koho cieľom je zneužitie ich dôvery. Prehnanú otvorenosť alebo intimitu vo verejnej komunikácii treba vnímať ako škodlivú predovšetkým pre samotného autora, ktorý tým vytvára podmienky pre svoje budúce zneužitie.

Negatívne aspekty využívania sociálnych sieti

Hlavný dôvod všeobecnej obľúbenosti elektronických sociálnych médií je, že dokážu užívateľsky jednoduchým spôsobom v prostredí internetu rozvíjať komunikáciu medzi ľuďmi, budovať komunity a podporovať podnikanie. Výmena správ, hlasových a video hovorov je bežne a nepretržite prístupná bez ohľadu na fyzickú spôsobilosť a geografickú polohu užívateľa, politické a ekonomické podmienky v krajine a to obvykle bez priamych poplatkov.

[47] SMAHELl, D , MACHAČKOVÁ, H., MASHERONI, D. at all. 2020. EU Kids online 2020 – Survey results from 19 coutries. ISSN 2045-256X, online https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf [cit. 8. marec 2022]

[48] BAKALÁR, P, at al. Health Behaviour in School-aged Children. 2019. “Sociálne determinanty zdravia školákov” ISBN: 978-80-7159-242-6, p. 382. Retrieved from URL https://hbscslovakia.files.wordpress.com/2019/06/nar-sprava-zdravie-11_lq.pdf

[49] SMAHELl, D , MACHAČKOVÁ, H., MASHERONI, D. at all. 2020. EU Kids online 2020 – Survey results from 19 coutries. ISSN 2045-256X, online https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf [cit. 8. marec 2022]

[50] Suller, J.,. “The Online Disinhibition Effect”, CYBERPSYCHOLOGY & BEHAVIOR, Volume 7, Number 3, 2004, p. 321-326

Obzvlášť deti a mladí ľudia vzhľadom na ich vek majú zvýšenú potrebu socializovať sa, tvoriť nové priateľstvá a vzťahy, čo je primárny účel použitia sociálnych sietí.

Kuchynský nôž je s každodennou pravidelnosťou využívaný pri príprave alebo konzumácii jedál. Z užitočného pomocníka sa bez akejkoľvek úpravy veľmi jednoducho môže stať útočná zbraň, ktorou je možné zraniť, dokonca usmrtiť. Procesom výroby nie je možné jednoznačne rozhodnúť o účele použitia daného predmetu, rozhoduje o tom až používateľ v momente použitia. Moderné komunikačné technológie sú primárne určené a veľmi úspešne slúžia na sprostredkovávanie vzdialenej komunikácie. Podobne ako nôž, aj moderné technológie okrem mnohých užitočných účelov pre ktoré sú prevádzkované, môžu byť a aj sú vedome zneužívané na škodlivé správanie voči iným. V online prostredí prevažne nevzniká nový druh trestnej činnosti, častejšie sa jedná o modifikáciu už existujúcej klasickej kriminality, ktorá využíva nové techniky. Páchatelia trestnej činnosti sa od dávna vyskytovali a uprednostňovali miesta so zvýšenou koncentráciou osôb. Dôvody sú prosté, primárne veľa príležitostí nájsť vhodné obete. Vďaka digitálnym technológiám sa páchatelia môžu dostať k deťom prostredníctvom webových kamier, v chatovacích miestnostiach na sociálnych sieťach a vo videohrách. A vďaka technológiám ako proxy serverm cloud computing a dark web môžu zostať v anonymite, čo pre orgány presadzujúce právo komplikuje odhaľovanie a dokazovanie protiprávneho konania. Oba dôvody sú platné a príznačné pre online prostredie, pre ktoré je charakteristická jednak anonymita používateľov a že stopy vznikajú prevažne v digitálnej podobe.

Jedným z negatívnych aspektov vzdialenej komunikácie je možnosť jej zneužitia napríklad na nebezpečné prenasledovanie tzv. kyberstalking, poškodzovanie cudzích práv, výrobu (rozširovanie, prechovávanie) detskej pornografie, nátlak, kyberšikanovanie atď.

Veľmi častý je výskyt rôznych foriem vydierania, napríklad sextortion: keď páchatelia nútia alebo podvádzajú svoje obete, aby zdieľali citlivé osobné obrázky alebo videá, ktoré sú následne použité na ich vydieranie. Podľa štatistík kriminality sa síce evidovaná sexuálna aktivita mladistvých do 15 rokov znižuje, čo sa s vysokou pravdepodobnosťou nedá povedať o digitálnej sexuálnej aktivite. Do policajnej evidencie z digitálnej sexuálnej aktivity sa dostávajú len ojedinelé prípady, celkovo sa táto činnosť vyznačuje vysokou mierou latencie. Obeťou sextortion sa ľahšie stanú mladiství, ktorí vedome prijímajú, odosielajú alebo zverejňujú sexuálne ladené správy, fotografie a videá, t. j. praktizujú sexting, Samostatne generovaný obsah, v ktorom je detská obeť upravená a donútená k tomu, aby vytvorila obrázky a videá

svojho zneužívania, sa výrazne rozrástla najmä počas pandémie COVID 19, kedy sa nestíhala venovať pozornosť primeraná ich nebezpečnosti.

Sexuálne zneužívanie detí online

World Health Organization definuje týranie a zneužívanie detí ako "používanie akýchkoľvek foriem fyzického alebo psychického *násilia, poškodenia alebo zneužitia, zanedbávania alebo nedbalého zaobchádzania, obchodného, sexuálneho a iného vykorisťovania, pričom dochádza k priamemu alebo potenciálnemu ublížení na zdraví dieťaťa, ohrozeniu života a narušeniu rozvoja alebo ľudskej dôstojnosti zneužijúc zodpovednosť, dôveru alebo moc, ktorú zneužívajúci v danom vzťahu má.* Dokument Child Protection Policy definuje sexuálne zneužívanie detí ako kontakt dieťaťa a staršej alebo vyspelejšej osoby, kedy je dieťa zneužité ako objekt sexuálneho uspokojenia staršej alebo vyspelejšej osoby. Zo strany páchateľa môže byť toto správanie vynucované silou, vydieraním, vyhrážaním alebo iným typom nátlaku.[51] Rozlišujeme dve základné formy sexuálneho zneužívania **dotykové a nedotykové**. Páchateľmi kontaktného zneužívania detí sú často osoby pre dieťa známe z blízkeho okolia, príbuzní, pedagogický pracovníci.

Bezdotykové sexuálne zneužívanie môže zahŕňať aktivity, kde nedochádza k telesnému kontaktu ako napríklad nútenie do odhaľovania častí tela, zasielanie odhalených fotografií, nútené sledovanie pornografie, atď. aj prostredníctvom elektronických komunikačných služieb. Napriek rozdeleniu sexuálneho zneužívania na niekoľko typov ostáva faktom, že každá z foriem vedie u dieťaťa k citovému chaosu, ktorého následkom môžu byť vážne psychické problémy.

Podľa Child Exploitation and Online Protection Command sú hlavnými obeťami sexuálneho vykorisťovania a groomingu dievčatá bieleho etnického pôvodu vo veku 11 až 14 rokov . Hlavnými obeťami detskej pornografie na webových stránkach sú tiež dievčatá s oveľa nižším vekom. (Internet Watch Foundation (IWF)

[51] Children of Slovakia Foundation. 2018. Child Protection Policy Retrieved from URL https://www.nds.sk/wp-content/uploads/2018/11/zmena_eng_2.pdf. [cit. 21. jún 2022]

Child sexual abuse material (CSAM)

Podľa Lanzarotského výboru (2017) je "sextingom" označené zdieľanie sexuálne explicitných správ, fotiek, videí alebo so sexuálnym obsahom pomocou technológií Sexting a jeho negatívne dôsledky sú sociálne nevhodný spôsob prezentovania sa predovšetkým u mladých ľudí. S témou sextingu úzko súvisí oblasť detskej pornografie zaznamenanej vo forme obrázkov, videí alebo zvukových záznamov. Niekedy sa materiál CSAM nesprávne označuje ako detská pornografia. Výrazu „detská pornografia" by sme sa však mali vyhnúť z nasledujúcich dôvodov: Výraz detská pornografia nepopisuje skutočnú povahu materiálu a podkopáva závažnosť zneužívania z pohľadu dieťaťa. Pornografia je termín, ktorý sa primárne používa na opis materiálu zobrazujúceho dospelých zapojených do dobrovoľných sexuálnych aktov distribuovaných na účely sexuálneho potešenia. Používanie tohto pojmu v kontexte detí riskuje normalizáciu, bagatelizovanie a dokonca legitimizáciu sexuálneho zneužívania a vykorisťovania detí. Detská pornografia znamená súhlas a dieťa nemôže legálne dať súhlas. Pojem detská pornografia sa v niektorých krajinách stále používa v legislatíve. Z tohto dôvodu sa CSAM niekedy na právne účely označuje ako detská pornografia. V neprávnom kontexte, ako napríklad v mediálnych publikáciách, by sa mal používať termín materiál sexuálneho zneužívania detí (CSAM).

Child Sexual abuse Materials (CSAM) zahŕňa zobrazovanie, výrobu, šírenie a používanie materiálu, ktorý zobrazuje dieťa pri sexuálnej činnosti (nezáleží na tom, či je skutočná alebo simulovaná), zobrazuje pohlavné orgány dieťaťa za účelom sexuálneho uspokojenia sledovateľa. Zvuková pornografia taktiež zahŕňa výrobu, rozširovanie alebo používanie materiálu so záznamom detského hlasu (skutočného alebo simulovaného) s cieľom sexuálneho uspokojenia. Podľa výročnej správy Nadácie Internet Watch (IWF) sa poskytovatelia internetových služieb v Európe stali najväčším hostiteľom materiálu o sexuálnom zneužívaní detí na svete.

Rozdiely definície sexuálneho zneužívania detí v krajinách

Materiál sexuálneho zneužívania detí (CSAM) má v rôznych krajinách rôzne právne definície. Minimálna verzia definuje bezkontaktné sexuálne zneužívanie detí ako snímky alebo videá, ktoré zobrazujú osobu, ktorá je dieťaťom a zapája sa do explicitnej sexuálnej aktivity alebo je zobrazovaná ako osoba, ktorá sa dopúšťa explicitnej sexuálnej aktivity.

- Líši sa vek, v ktorom sa v jednotlivých krajinách jednotlivec považuje za dieťa.
- Legislatíva sa tiež líši, pokiaľ ide o obrázky detí, ktoré boli poučené, aby pózovali sexualizovaným spôsobom.
- V mnohých krajinách sú obrázky a videá detí, ktoré sú úplne alebo čiastočne vyzlečené a v sexualizovaných pózach, a obrázky zamerané na pohlavné orgány detí nezákonné a mali by byť nahlásené na národnej horúcej linke.
- Ďalšou oblasťou, v ktorej sa legislatíva líši, je to, či na obrázku musí byť zobrazené skutočné dieťa, alebo či umelo vytvorené obrázky predstavujú CSAM.
- V neposlednom rade právne sankcie za výrobu, distribúciu a držbu CSAM sa tiež v jednotlivých krajinách líšia.

Mimoriadne škodlivý je materiál zdieľaný prostredníctvom online platforiem alebo sietí, kde sa nachádzajú obrázky interakcie páchateľa s obeťou. Nápodobe živé vysielanie sexuálneho vykorisťovania detí za úplatu tiež zaznamenalo v posledných rokoch nárast. Na uvedomenie si závažnosti problému je potrebné nezabúdať, že obrázky sexuálneho zneužívania detí nájdené na webe nie sú virtuálne; sú zločinom, ktorý zahŕňa skutočné deti a ich skutočné poníženie a utrpenie. Podľa Centra pre detské zneužívanie a online ochranu vo Veľkej Británii (CEOP) v online priestore môže byť ohrozený ktokoľvek bez ohľadu na vek, pohlavie, vierovyznanie, etnický a rasový pôvod, povolanie, Zmena a vývin technológií mení aj ľudskú komunikáciu a interakciu, vrátane sexuality.

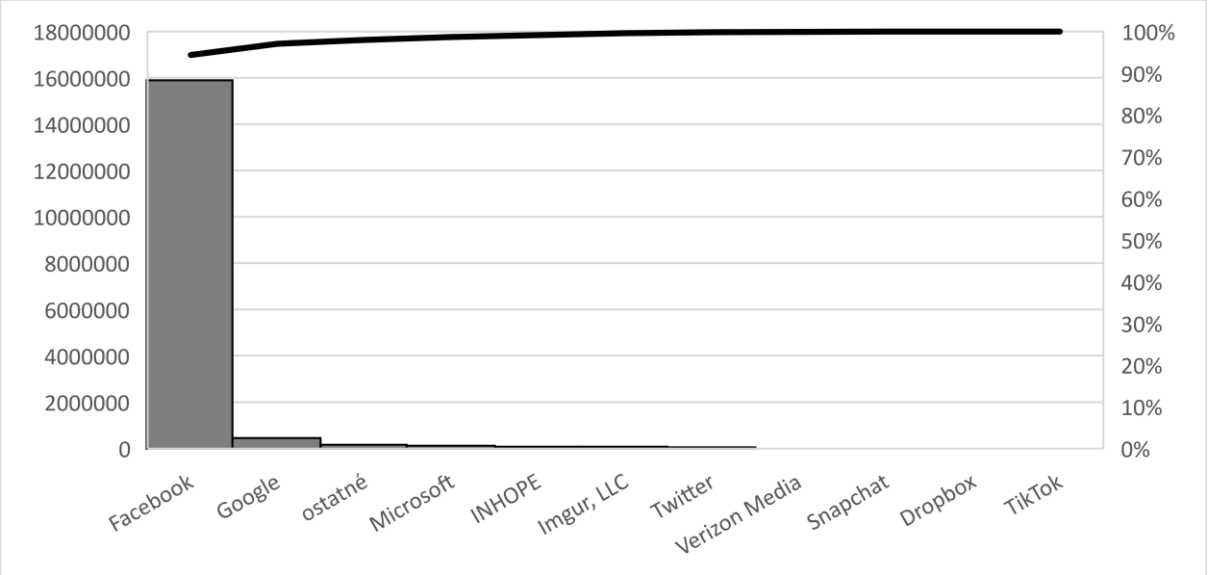
V oblasti sexuality je podľa štatistík z USA približne jedno z troch detí vo veku od 10 do 17 rokov vystavené sexuálnemu materiálu online a jedno zo siedmich bolo sexuálne obťažované. V Spojenom kráľovstve sa zistilo, že z dopytovaných 60% mladých ľudí potvrdilo, že boli niekedy požiadaní o fotografiu alebo video so sexuálnym obsahom.

Množstvo CSAM, ktoré už bolo online, bolo ohromujúce a počas pandémie sa naďalej zvyšovalo, pričom štatistiky naznačujú, že množstvo materiálu sa v niektorých krajinách zvýšilo prudko.[52]

Miera koncentrácie evidovaného nevhodného CSAM podľa poskytovateľov elektronických služieb

[52] EUROPOL, 2020. "Expoilting Isolation: Offenders and victims of online child sexual abuse during the Covid-19 pandemic" Retrieved from URL :///C:/Users/defaultuser0/Downloads/ europol_covid_report-cse_jun2020v.3_0%20(1).pdf. [cit. 17. máj 2022]

Nasledovným Paretovým grafom č. 1 ilustrujeme mieru koncentrácie evidovaného nevhodného CSAM podľa Electronic Servive Provider. Hlavná os vľavo slúži na zobrazenie absolútneho počtu sledovaných materiálov a vedľajšia os vpravo relatívny kumulatívny podiel týchto materiálov za rok 2019. Sledované subjekty na vodorovnej osi sú usporiadané zostupne od najpočetnejších po najmenej početné.



Graph 1 Paretov graf evidovaných CSAM podľa Electronic Servive Provider za rok 2019

Source of data: National center for missing &exploited children

S obrovskou dominanciou na úrovni 90 % bolo najviac sledovaných materiálov zaregistrovaných na sociálnych sieťach spoločnosti Facebook. Ako sme v teoretickej časti uviedli, jedná sa o dominantného prevádzkovateľa sociálnych sietí, čo sa odráža aj vysokom počte užívateľov. Navyše v rámci svojej politiky Facebook vyhlasuje nulovú toleranciu voči zneužívaniu detí, čomu môže nasvedčovať aj vysoká miera evidencie tohto materiálu. Na predchádzanie, odhaľovanie, odstraňovanie a nahlasovanie porušení bezpečnostných zásad využíva najmodernejšie technológie, ktoré dokážu byť vysoko efektívne pri automatizovaných činnostiach. Detekcia nevhodného obsahu sa uskutočňuje na základe automatizovaných postupov, ktoré kombinuje s participáciou s užívateľmi, ktorí môžu jednoduchým spôsobom nahlasovať potenciálne škodlivé správanie. Všetky ostatné subjekty sledované na graph N. 1v sumáre zaznamenali 10 % evidovaných CSAM.

Zvýšenú pozornosť treba venovať providerom s najväčším nárastom škodlivého materiálu za posledné dva roky, t. j. Snapchat a TikTok. Snapchat je relatívne nová komunikačná sieť zameraná predovšetkým na teenagerov. Zakladá si na tvorbe podmienok na rýchlu, efektívnu a zábavnú osobnú prezentáciu používateľov. Aplikácia poskytuje zdieľanie materiálov ako sú fotky a videá, ktoré nemjú mať trvalú hodnotu. Správy majú stačiť na krátkodobé pobavenie, pretože sú po 24 hodinách automaticky vymazané, pokiaľ nie sú vedome archivované do albumu. Momentky vtipne komentované priateľmi vytvárajú uvoľnenú atmosféru, ktorá môže priveľmi strhnúť zábrany sebakontroly. Mnohí užívatelia si neuvedomujú, že v online prostredí pojem vymazané neplatí absolútne, nakoľko ani pri jednorazovom zobrazení sa nedá zabrániť vytvoreniu ‚kópie", nad ktorou už autor stráca akúkoľvek kontrolu.Ďalším rizikom aplikácie je mapa Snap, ktorá priateľom umožňuje navzájom viedieť poluhu.

TikTok je aplikácia a sociálna sieť určená podobne ako Snapchat na zdieľanie krátkych videí a videoklipov Expanziu do celého sveta uľahčuje ľahká dostupnosť obsahu, nakoľko na vzhliadnutie obsahu nie je potrebná žiadna registrácia. Okrem samotného obsahu aplikácia predstavuje riziko z hľadiska ochrany osobných údajov užívateľov, ktorých počet enormne narastá.

Legislatívne opatrenia na boj proti šíreniu CSAM

Koncentrovali sme argumenty o znepokojivo zvyšujúcom sa výskyte škodlivého materiálu v online prostredí. Riešením problému je lepšie zosúladenie a doplnenie už existujúcich legislatívnych opatrení predovšetkým na medzinárodnej úrovni. Dohovor Rady Európy o ochrane detí pred sexuálnym vykorisťovaním a sexuálnym zneužívaním bol prijatý v Lanzarote už 25. 10. 2007. Odvtedy vstúpilo do platnosti viacero viac či menej účinných právnych aktov, ktoré doposiaľ nepriniesli trvalo uspokojivé riešenie. Prísne pravidlá vyplývajúce zo európskej smernice e-privacy z decembra 2020 spôsobili, že metódy používané na odhaľovanie zneužívania detí na internete možnosťou získania údajov jednoznačne určujúcich páchateľa a aj použité zariadenie sa zo dňa na deň stali nezákonné. Odvtedy bol zaznamenaný enormný pokles odhalených prípadov zneužívania detí v online svete, a to až o 58% napriek tomu, že množstvo verejne dostupného materiálu výrazne stúpol (Europol). Vzhľadom na kombinované faktory veku, pohlavia, súkromia, súhlasu, právnych predpisov a prevládajúcich sociálnych noriem, neexistuje univerzálne riešenie na aktiváciu regulácie spôsobom, ktorý by na jednej strane nezasahoval do súkromia používateľa a uplatňoval pravidlá

o dôvernosti elektronickej komunikácie a údajov o prenose dát zakotvených v smernici EÚ z roku 2002 a na druhej by zaručil jeho ochranu pred zdieľaním alebo inými nebezpečenstvami. Dňa 7. júla 2021 Európska komisia prijala dočasnú legislatívnu úpravu, ktorou sa ustanovuje výnimka na dobrovoľné systémy poskytovateľov internetových služieb pri odhaľovaní detskej pornografie a celkovo nahlasovaní materiálov obsahujúcich sexuálne zneužívanie detí z online prostredia. Prax ukazuje, že trestné stíhanie pokrýva iba zlomok prípadov, kedy by mal byť závadný obsah odstránený.[53] Smernicou by sa mala vyvážiť na jednej strane povinnosť ochrániť deti a na strane druhej, zachovať legitimitu smernice o elektronickom súkromí a tak naďalej chrániť právo jedinca na súkromie.

Legislatívna úprava umožní spoločnostiam cieľavedome sledovať na svojich platformách pomocou skenovacích technológií explicitný materiál bez obáv z porušenia európskych zákonov o ochrane súkromia. Navyše budú môcť prijímať opatrenia proti kybernetickému nadväzovaniu kontaktov na sexuálne účely a oznamovať domnelé sexuálne zneužívanie detí online príslušným orgánom presadzovania práva a justičným orgánom či organizáciám konajúcim vo verejnom záujme proti sexuálnemu zneužívaniu detí. Skenovania sa musí vykonávať tak, aby čo najmenej zasahovalo do súkromia a nesmie byť schopné pochopiť podstatu obsahu, ale len odhaliť vzorce. Viacerí európski zákonodarcovia v tejto súvislosti upozornili, že pravidlá sú „právne chybné“ a môžu sa stať pred súdom neobhájiteľné. Nariadenie bude platiť dovtedy, kým sa podarí dohodnúť adekvátne dlhodobé pravidlá maximálne však môže ísť o 3 roky.

Odhaľovanie a dokazovanie sexuálneho zneužívania detí

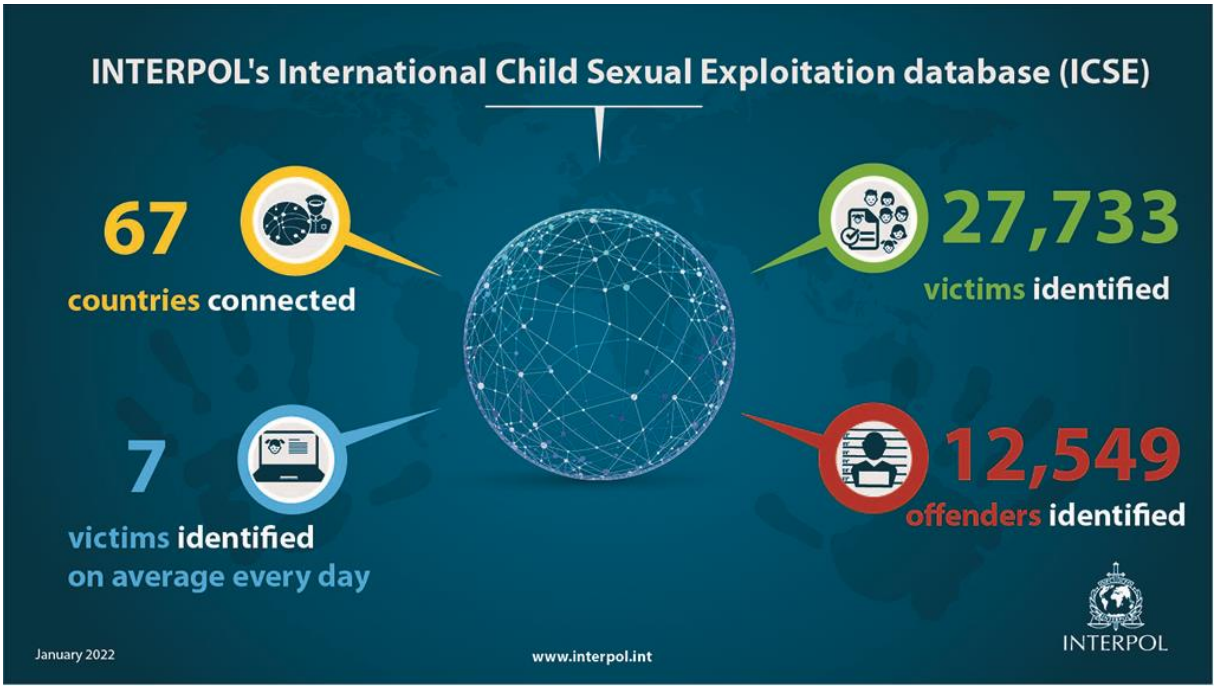
Významným nástrojom na boj proti sexuálnemu zneužívaniu detí je sieť liniek Inhope. Medzinárodná globálna sieť Inhope pozostáva z 50 hotline v 46 krajinách, ktoré poskytujú verejnosti možnosť anonymne nahlásiť podozrenie zo nezákonného obsahu na internete so zameraním na sexuálne zneužívanie detí. Cieľom jej činnosti je boj proti materiálom zobrazujúcim sexuálne zneužívanie detí na internete zapojením širokej verejnosti, ich rýchlou identifikáciou a odstraňovaním prostredníctvom pripravených formulárov. Ministerstvo práce, sociálnych vecí a rodiny SR v máji 2022 verejne iniciovalo snahu pripojiť sa ku tejto sieti, do

[53] KORDÍK, M., DRAŽOVÁ, P. “Efektivita postihu počítačovej kriminality” In: *Efektívnosť prípravného konania - jej skúmanie, výzvy a perspektívy*. Bratislava: Faculty of law UK, 2020. ISBN 978-80-7160-577-5. – s. 51

ktorej Slovensko ako jediná krajina Európskej únie nebolo zapojené a tým dobehnúť rozbehnutý vlak. Za rok 2021 bolo na Slovensku vznesené obvinenie viac ako 270 osobám, právoplatne bolo odsúdených 212 osôb. Relevantné informácie z hotline dostávajú aj orgány činné v trestnom konaní, aby sa páchatelia vedeli čo najrýchlejšie identifikovať a obete ochrániť.

Medzinárodná databáza sexuálneho zneužívania detí (ICSE - International Child Sexual Exploitation) INTERPOL-u poskytuje globálnu platformu, ktorá má za cieľ pomáhať špecialistom na identifikáciu obetí z viac ako 64 krajín na celom svete analyzovať a porovnávať obrázky sexuálneho zneužívania detí. Databáza obrázkov a videí ICSE je spravodajský a vyšetrovací nástroj, ktorý umožňuje špecializovaným vyšetrovateľom zdieľať údaje o prípadoch sexuálneho zneužívania detí. Databáza sa vyhýba duplicite úsilia a šetrí drahocenný čas tým, že dáva vyšetrovateľom vedieť, či už séria obrázkov bola objavená alebo identifikovaná v inej krajine, alebo či má podobné vlastnosti ako iné obrázky. Analýzou digitálneho, vizuálneho a zvukového obsahu fotografií a videí môžu odborníci na identifikáciu obetí získať stopy, identifikovať akékoľvek prekrývanie prípadov a spojiť svoje úsilie pri hľadaní obetí sexuálneho zneužívania detí.

Indikátorom intenzity výskytu škodlivého materiáli a miery závažnosti tohto problému je prehľad z medzinárodnej databázy sexuálneho zneužívania detí Interpolu, obrázok č. 1.



Obrázok 2 Štatistika databázy Interpolu z materiálov o sexuálnom zneužívaní detí

Zdroj: Interpol https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database. [cit. 18. máj 2022]

Databáza Interpolu o sexuálnom zneužívaní detí obsahuje viac ako 2,7 milióna obrázkov a videí a pomocou nej bolo identifikovaných 23 564 obetí na celom svete, v priemere sedem obetí zneužívania detí je identifikovaných denne, od svojho vytvorenia pomohla identifikovať a zdokumentovať viac ako 12 500 páchateľov.

Identifikácia obetí zahŕňa podrobnú analýzu obrázkov a videí s cieľom nájsť a zachrániť obete sexuálneho zneužívania detí. Online sexuálne zneužívanie detí je jednou z mála oblastí kriminality, kde policajti začínajú s dôkazmi a postupujú späť na miesto činu. Obrázky možno objaviť buď prostredníctvom: vyšetrovania zneužívania detí alebo proaktívne monitorovaním online platforiem; Forenzná analýza sa realizuje na zaistených mobilných telefónoch, notebookoch, digitálnych pamäťových jednotkách atď. Po nájdení fotografií a videí prevezmú kontrolu nad riešeným prípadom špecialisti na identifikáciu obetí.

Prevažná väčšina prípadov sexuálneho zneužívania detí nie je zdokumentovaná, väčšinou sa odohráva za zatvorenými dverami v súkromnom prostredí. Keď je však zneužívanie zaznamenané alebo odfotografované, to, čo sa skutočne dokumentuje, je dôkazom závažného zločinu. Zneužívatelia často používajú obrázky na budúce sexuálne uspokojenie alebo na predaj a zdieľanie s inými násilníkmi.

Identifikácia obetí kombinuje podrobnú analýzu obrazu a tradičné vyšetrovacie metódy. Skúmaním digitálneho, vizuálneho a zvukového obsahu fotografií a filmov môžu policajti nájsť stopy identifikujúce miesto alebo obeť. Stopy môžu pochádzať z mnohých miest a v mnohých podobách – je na špecialistoch na identifikáciu obetí, aby ich spojili pomocou radu špecializovaných nástrojov.

Okrem medzinárodnej databázy obrázkov a videí je dôležitým nástrojom softvér na porovnávanie obrázkov, ktorý pomáha špecialistom na identifikáciu obetí porovnávať a vymieňať si informácie o materiáloch a aktívnych vyšetrovaniach. Vzhľadom na svoju povahu je identifikácia obetí náročná práca, ktorá si vyžaduje špecialistov z rôznych oblastí. Príslušníci orgánov činných v trestnom konaní často úzko spolupracujú s autorizovanými civilnými analytikmi, aby určili pôvod série obrázkov alebo videa. Špecialisti na identifikáciu obetí úzko spolupracujú so svojimi kolegami na celom svete, aby jedinečné, typické alebo ľahko rozpoznateľné stopy v jednej krajine, iná krajina neprehliadne. Často krát len jedna stopa delí

od prerušenia prípadu. Na vytvorenie kľúčového spojenia stačí správna osoba so správnymi nástrojmi a zručnosťami.

Záver

Internet je mimoriadne rýchlo sa rozvíjajúca a expandujúca platforma poskytujúca svojim užívateľom obrovské množstvo príležitostí.54 Nakoľko neustále dochádza k rozvoju nových technologických oblastí, odborníci strácajú schopnosť reagovať v takom rozsahu a dostatočnou rýchlosťou, ako by bolo potrebné, či už výskumne, intervenčne alebo preventívne. V kombinácii so zväčšovaním kapacity mobilných telefónov a obrovskej rozmanitosti využiteľnosti mobilných telefónov. nedokážeme mať plnú moc a kontrolu nad činnosťou ľudí v online priestore.

Pre zákonodarcu znamená enormná dynamika činností v online priestore náročnú výzvu. Nastavenie právnych noriem dostatočne univerzálne, aby dokázali zabrániť nežiaducim činnostiam na internete je podstatne náročnejšie ako v klasickom trojdimenzionálnom priestore. Funkčné nastavenie nelegálnosti nežiadúcich činností predstavuje zložitú, avšak najúčinnejšiu prevenciu vo všeobecnosti, nielen pred vznikom a zdieľaním nevhodného zvukového alebo obrazového materiálu CSAM. Ďalším faktorom, ktorým dokážeme riziko zneužívania detí v online priestore veľmi znížiť je vzdelávanie, rešpektovanie a dodržiavanie základných bezpečnostných pravidiel užívateľmi. Uvedomelé správanie, pocit zodpovednosti a kritického myslenia, ktorými môžu užívateľ výrazne prispieť k svojmu bezpečiu je potrebné budovať skôr, ako začnú komunikačné technológie využívať, Na základe merateľných ukazovateľovi sme v príspevku poukázali na niektoré komunikačné kanály, kde je zvýšená miera výskytu škodlivého materiálu CSAM a kde je žiaduce byť ostražitejší, prípadne zintenzívniť kontrolu. Zlepšenie automatickej detekcie online materiálu súvisiaceho so sexuálnym zneužívaním detí by sa mohlo dosiahnuť takzvanými hašovacími technológiami a zapojením umelej inteligencie. Z hľadiska celospoločenských úloh je dôležitá synergia zainteresovaných subjektov, aby sa nevhodný materiál na internete minimalizoval. Prevencia a všeobecná kontrola ideálne uvedomelá každým používateľom internetu je perspektíva, ktorá by mohla byť úspešná aj v tak rušnom prostredí ako je internet.

[54] KOPENCOVÁ, D., RAK. R. Distance forensic learning during the Covid 19 pandemic and ITS specification. In In L. Gómez Chova, A. López Martínez, I. Candel Torres. EDULEARN21 Proceedings. 13th International Conference on Education and New Learning Technologies. Spain. Published by IATED Academy, 2021. 2828 p. ISBN 978-84-09-31267-2. doi:10.21125/edulearn.2021.0612. https://library.iated.org/…DIS

Poďakovanie

Príspevok vznikol v rámci projektu VVÚ Metódy spracovania policajne relevantných informácií – Výsk. 161 na Akadémii Policajného zboru v Bratislave.

Zoznam použitej literatúry

BAKALÁR, P. at al. Health Behaviour in School-aged Children. 2019. "Sociálne determinanty zdravia školákov" ISBN: 978-80-7159-242-6, p. 382. Retrieved from URL

https://hbscslovakia.files.wordpress.com/2019/06/nar-sprava-zdravie-11_lq.pdf.

KIŠŠOVÁ, M. 2022. Násilná kriminalita a s ňou súvisiace fenomény. In Policajná teória a prax : časopis Akadémie Policajného zboru v Bratislave, ISSN 1335-1370. Bratislava, 2022, roč. 30, č. 2, s. 20.

KOPENCOVÁ, D., RAK. R. Distance forensic learning during the Covid 19 pandemic and ITS specification. In In L. Gómez Chova, A. López Martínez, I. Candel Torres. EDULEARN21 Proceedings. 13th International Conference on Education and New Learning Technologies. Spain. Published by IATED Academy, 2021. pp. 2826-2832. ISBN 978-84-09-31267-2. doi:10.21125/edulearn.2021.0612. https://library.iated.org/…DIS

KORDÍK, M., DRAŽOVÁ, P.. 2020 Efektivita postihu počítačovej kriminality In: Efektívnosť prípravného konania - jej skúmanie, výzvy a perspektívy. Bratislava : Právnická fakulta UK, 2020. ISBN 978-80-7160-577-5. – s. 48-61

LISOŇ, M., FIDLER, Ľ. 2022. Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb. In Policajná teória a prax : časopis Akadémie Policajného zboru v Bratislave, ISSN 1335-1370. Bratislava, 2022, roč. 30, č. 2, s. 47.

J.SULLER, , 2004. The Online Disinhibition Effect, CYBERPSYCHOLOGY & BEHAVIOR, Volume 7, Number 3, 2004, p. 321-326

F. VLACH, R.. RAK. Czech prison staff training and enhancement in the times of pandemic. In L. Gómez Chova, A. López Martínez, I. Candel Torres. EDULEARN21 Proceedings. 13th International Conference on Education and New Learning Technologies. Spain. Published by IATED Academy, 2021. pp. 4880-4889. ISBN 978-84-09-31267-2. doi:10.21125/edulearn.2021.1007. https://library.iated.org/view/VLACH2021CZE

Children of Slovakia Foundation. 2018. Child Protection Policy Retrieved from URL https://www.nds.sk/wp-content/uploads/2018/11/zmena_eng_2.pdf

SMAHELl, D., MACHAČKOVÁ, H., MASHERONI, D. at all. 2020. EU Kids online 2020 – Survey results from 19 coutries. ISSN 2045-256X, online https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf

SULLER, J.,. "The Online Disinhibition Effect", CYBERPSYCHOLOGY & BEHAVIOR, Volume 7, Number 3, 2004, p. 321-326

EUROPOL, 2020. Expoilting Isolation: Offenders and victims of online child sexual abuse during the Covid-19 pandemic online file:///C:/Users/defaultuser0/Downloads/europol_covid_report-cse_jun2020v.3_0%20(1).pdf

Health Behaviour in School-aged Children. 2019. Sociálne determinanty zdravia školákov ISBN: 978-80-7159-242-6, p. 382. online https://hbscslovakia.files.wordpress.com/2019/06/nar-sprava-zdravie-11_lq.pdf

Children of Slovakia Foundation. 2018. Child Protection Policy Retrieved from URL

https://www.nds.sk/wp-content/uploads/2018/11/zmena_eng_2.pdf

Kontaktné údaje

doc. RNDr. Tatiana Hajdúková, PhD.

Katedra informatiky a manažmentu

Akadémia Policajného zboru v Bratislave

Sklabinská 1, 835 17 Bratislava

E-mail: tatiana.hajdukova@akademiapz.sk

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

PhDr. Peter Veselý, PhD.

Falošné správy – hrozba pre súčasnú spoločnosť

Radoslav Ivančík

Abstrakt: V súčasnosti, keď môžeme naplno využívať výhody modernej informačnej spoločnosti a výdobytky modernej vedy a techniky, keď sa môžeme vďaka rýchlemu internetu dostať v priebehu niekoľkých sekúnd k mnohým potrebným a dôležitým informáciám, ku ktorým by sme sa ešte pred pár rokmi vôbec nedostali, alebo by to trvalo veľmi dlho, žiaľ, žijeme aj v ére falošných správ. Tak, ako rýchlo je dnes možné vyhľadávať a šíriť množstvo cenných a zaujímavých informácií, tak rýchlo je dnes možné šíriť aj množstvo falošných správ. Mnohé falošné mediálne webové stránky sú vytvorené tak, aby pripomínali legitímne médiá, pričom cieľom ich tvorcov je práve šírenie falošných správ, dezinformácií a propagandy rôzneho druhu, napríklad v rámci rôznych dezinformačných kampaní. Ich šírenie a zdieľanie mnohokrát ohrozuje ľudské zdravie, spoločnosť, demokraciu a národnú bezpečnosť. Aj preto sa autor v rámci kvalitatívneho teoretického výskumu, s využitím viacerých analyticko-syntetických prístupov a metód, vo svojom príspevku zaoberá problematikou falošných správ ako hrozby pre súčasnú spoločnosť.

Kľúčové slová: Falošné správy, demokracia, spoločnosť, bezpečnosť, hrozba.

Abstract: Nowadays, when we can take full advantage of the modern information society and the achievements of modern science and technology, when we can, thanks to fast internet, have access to a lot of necessary and important information in a few seconds that we would not have at all a few years ago, because it would have taken a very long time, unfortunately, we are also living in an era of fake news. As fast as it is possible to search for and disseminate a lot of valuable and interesting information today, so fast it is possible to spread a lot of fake news today. Many false media websites are designed to resemble legitimate media, and their creators aim to spread fake news, disinformation, and propaganda of various kinds, for example in various disinformation campaigns. Their dissemination and sharing can often threaten human health, society, democracy, and national security. That is why the author, in the framework of qualitative theoretical research, using several analytical-synthetic approaches and methods, in his contribution deals with the issue of fake news as threat to contemporary society.

Keywords: Fake news, democracy, society, security, threat.

Úvod

Falošné správy, tzv. „fake news“ je súslovie, ktoré je považované za jednu z najväčších hrozieb pre súčasnú spoločnosť. Collins Dictionary dokonca vyhlásili „fake news“ za pojem roku 2017.[1] Ide o fenomén, ktorý najmä v posledných rokoch až príliš často zvyšuje napätie v spoločnosti, čo sme mohli vidieť napríklad počas amerických prezidentských volieb v rokoch 2016 a 2020, alebo ešte predtým počas referenda o vystúpení Veľkej Británie z Európskej únie, či najnovšie počas obdobia tzv. koronakrízy. Kým v prvom prípade proti sebe stáli prívrženci

[1] CD. 2018. Word of the Year 2017 is Fake News. In *Collins Dictionary*, 2018

a odporcovia Donalda Trumpa, v druhom prípade tí, ktorí podporovali Brexit, a tí, ktorí proti nemu bojovali, a v treťom prípade zasa zástancovia a odporcovia očkovania proti koronavírusu SARS-CoV-2 spôsobujúcemu ochorenie Covid-19. Z nich najmä pandémia koronavírusu priniesla široké spektrum najrôznejších falošných správ, ktoré pritiahli pozornosť ľudí, médií aj inštitúcií. Patria sem napríklad tie, ktoré tvrdia, že technológie 5G potláčajú imunitný systém ľudí, a tým ich robia zraniteľnejšími voči koronavírusu,[2] alebo tie, ktoré tvrdia, že vakcíny proti koronavírusu spôsobujú autizmus a navyše obsahujú nanočipy, prostredníctvom ktorých budú zaočkovaní ľudia všade sledovaní a monitorovaní.[3] Samozrejme, podobných prípadov, kedy falošné správy doslova rozoštvali proti sebe skupiny ľudí, by sme našli oveľa viac.

Problémom je, že v ostatných rokoch sa s dynamickým nástupom nových médií, prudkým rozvojom a masívnym využívaním informačných a komunikačných technológií[4], systémov, prostriedkov a zariadení[5], objavila aj nová škála možností ako najrôznejšie správy, zvesti, novinky či teórie prijímať, vyhľadávať, ale aj šíriť. Zároveň sa však objavila aj nová škála možností ako moderné technológie a zariadenia zneužiť[6] a šíriť prostredníctvom nich klamlivé, zavádzajúce a skreslené informácie s cieľom ovplyvniť konanie ľudí. Šírenie rôznych falošných správ, ktoré reagujú na rôzne významné udalosti odohrávajúce sa okolo nás, tak predstavuje veľmi nebezpečnú hrozbu, ktorá môže mať pre jednotlivcov, organizácie i celú ľudskú spoločnosť veľmi nepriaznivé dôsledky.

Pred objavením sa internetu bolo šírenie informácií oveľa nákladnejšie. Na vybudovanie dôvery boli potrebné celé roky. Kedysi existovali tiež menej zložité vysvetlenia definujúce

[2] WASSIM, A. a kol. Four Experts Investigate How the 5G Coronavirus Conspiracy Theory Began. In *The Conversation*, 2020

[3] PLIEŠOVSKÝ, R. Videli ste už schému nanočipu z vakcíny Pfizer? In *Techbox*, 2021; REITER, M. Chcú nás začipovať? A môže za to Pfizer a 5G? In *TouchIT*, 2021

[4] V úvodných dvoch dekádach nového tisícročia sa v súvislosti so šírením a stále intenzívnejším využívaním IKT výrazne zmenil spôsob života a charakter ľudskej spoločnosti, ako aj fungovanie všetkých jej oblastí (FRIANOVÁ, 2020, s. 17).

[5] S rozvojom informačných a komunikačných technológii zaznamenávame masívne rozšírenie mobilného pripojenia na internet (GPRS, UMTS, LTE, WiFi), pričom čoraz viacej používateľov sa na internet pripája prostredníctvom rôznych mobilných zariadení (HAJDÚKOVÁ, HRUŠKA, 2018, s. 133).

[6] Bližšie pozri: KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98; ZACHAR, Š. 2018. Anonymizácia komunikácie zmenou IP adresy ako metóda bezpečného prehliadania internetu. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie*. Bratislava : A PZ, 2018, s. 217-224; KOSTREC, M. 2020. Nebezpečné hrozby v digitálnom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie*. Bratislava : Akadémia Policajného zboru, 2020, s. 78-87; KORAUŠ, A. – KELEMEN P. 2018. Protection of persons and property in terms of cybersecurity. In *Ekonomické, politické a právne otázky medzinárodných vzťahov 2018 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Vydavateľstvo Ekonóm, 2018; RÉVESZOVÁ, L. 2018. Počítačová kriminalita a dynamika jej vývoja v rokoch 2014 - 2017. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie*. Bratislava : A PZ, 2018, s. 161-173; alebo TOMÁŠEK, R. – TOMÁŠEKOVÁ, L. 2020. Kybernetické hrozby a kybernetický terorizmus. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie*. Bratislava : A PZ, 2020, s. 146-152.

pojmy ako správy a médiá. To rozhodne uľahčilo reguláciu aj samoreguláciu. Masívny nárast využívania sociálnych sietí však doslova zničil množstvo hraníc, ktoré predtým bránili šíreniu falošných správ v demokratických krajinách. Dnes rôzne chytré, tzv. „smart zariadenia“ spolu s internetom a sociálnymi sieťami umožňujú takmer každému jednotlivcovi produkovať a distribuovať množstvo najrôznejších informácií, včítane informácií klamlivých, skreslených, nepravdivých. Zdieľanie správ, fotiek, obrázkov, videí a pod. prostredníctvom rôznych sociálnych sietí ako sú napríklad Facebook, Twitter, Instagram, You Tube, Tik Tok, Massenger, WhatsApp, Viber, Telegram a ďalších, ako aj množstva najrôznejších aplikácií, nikdy nebolo také jednoduché ako dnes. Publikačné platformy, ako je napríklad WordPress, navyše umožňujú každému ľahko vytvoriť neustále sa meniaci web. Stručne povedané, prekážky brániace vytváraniu a šíreniu falošných správ boli odstránené.

Čo sú to vlastne falošné správy?

Napriek tomu, že sa ľudia s nimi stretávajú už veľmi dlhú dobu, stále neexistuje presná definícia falošných správ, na ktorej by sa dokázala odborná verejnosť zhodnúť, a ani sa to očakávať nedá. Existuje niekoľko verzií, ktoré sa od seba viac či menej líšia, predovšetkým tým, aké druhy zavádzajúcich správ považujú za falošné. Je dôležité pozrieť sa na niekoľko definícií a porovnať ich pre pochopenie toho, v čom sa odlišujú a v čom majú spoločné znaky.[7]

Niektoré zo všeobecne uznávaných definícií hovoria, že falošné správy sú spravodajské články, ktoré prezentujú v nich obsiahnuté informácie ako fakty, hoci vôbec nie sú na faktoch založené. Z tejto definície vyplýva, že falošné správy obsahujú informácie, ktorých pravdivosť je možné objektívne overiť. Iné definície sú vo vymedzení falošných správ menej prísne, pretože zahŕňajú všetky druhy zavádzajúcich, klamlivých správ, ako sú fámy, hoaxy a satirické články. Fámy obsahujú informácie, ktorých pravdivosť nemožno potvrdiť alebo vyvrátiť, hoaxy slúžia na oklamanie človeka prostredníctvom nepravdivých informácií a satirické články majú za úlohu pobaviť čitateľov predkladaním vymyslených informácií.

Mnohé z takýchto zavádzajúcich správ nie sú priamo zámerne falošné a ani písané s úmyslom čitateľa zmiasť alebo presvedčiť o nepravde. Satirické články nemajú v úmysle ľudí oklamať, ale zabaviť. Hoaxy často obsahujú informácie, ktoré nemožno overiť, preto sa nechcú prezentovať ako nepravdivé informácie, fakty a fámy, ktoré nevychádzajú zo spravodajských udalostí. Pri všetkých týchto falošných správach je ťažké ich overiť a ešte ťažšie preukázať ich vyslovený úmysel oklamať čitateľov, nakoľko sa môžu viesť dohady o tom, či ide skutočne

[7] McQUAIL, D. 2009. *Úvod do teorie masové komunikace*. Praha : Portál, 2009, s. 342-344

o falošné správy. Z toho dôvodu sa za falošné správy dajú považovať len tie články, u ktorých sú úmysel a nepravdivosť informácií jasne preukázateľné.[8]

Pre lepšiu ilustráciu vyššie uvedených informácií uvádzame aspoň dva príklady definícií falošných správ, jednu zo zahraničného a jednu z domáceho prostredia. Allcott a Gentzkow definujú falošné správy ako „*spravodajské príspevky, ktoré sú zámerne a overiteľne klamlivé a môžu čitateľa zavádzať*“.[9] Podľa Gregora ide o „*chytľavé súslovie, ktoré označuje úmyselne nepravdivé alebo zavádzajúce informácie, ktoré sa objavujú v médiách alebo na sociálnych sieťach*“.[10]

Jedným z problémov preukázania toho, že naozaj ide o falošné správy je to, že môžu existovať v mnohých rozličných formách, so všestrannými motívmi, od rôznych autorov a bez obmedzenia na:

- komerčne senzačný obsah;
- správy, ktoré nie sú ideologicky motivované, ktorých hlavným cieľom je stimulovať návštevnosť webu a generovať príjmy z reklamy;
- štátom podporované dezinformácie, ktorých cieľom nie sú príjmy, ale vplyv; môžu vytvárať a šíriť obsah, ktorý otrasie verejnou mienkou a vyvolá zmeny v podpore, preferenciách verejnosti; môžu podporovať určitého kandidáta, stranu alebo myšlienky, ktoré môžu ovplyvniť verejnú mienku, rozhodovanie voličov a pod.; produkované falošné správy a dezinformácie správy pritom môžu byť kombinované s pravdivými, originálnymi informáciami;
- silné guerillové spravodajské weby, ktoré dokážu kombinovať fakty a názory tak, aby podporili určité politické hľadisko, stranu alebo svoju pozíciu ako alternatívu k mainstreamovým médiám;
- sociálne siete.[11]

Claire Wardle, expertka na sociálne médiá, obsah vytváraný používateľmi a overovanie, identifikovala sedem typov falošných správ:

- satira alebo paródia, ktorá má potenciál oklamať publikum, ale nemá v úmysle spôsobiť mu škodu;

[8] FORGAS, J. P. – BAUMEISTER, R. 2019. *The Social Psychology of Gullibility: Conspiracy Theories, Fake News and Irrational Beliefs*. London : Routledge, 2019, s. 63-65.
[9] ALLCOTT, H. – GENTZKOW, M. Social Media and Fake News in the 2016 Election. In *Journal of Economic Perspectives*, 2017, roč. 31, č. 2, s. 213
[10] GREGOR, M. a kol. *Nejlepší kniha o Fake News, dezinformacích a manipulacích!!!* Brno: CPress, 2018, s. 7
[11] TITCOMB, J. – CARSON, J. 2018. Fake news: What exactly is it – and how can you spot it? In *The Telegraph*, 2018

- falošné spojenie, kde sa nadpisy, titulky alebo vizuály používajú spôsobom, ktorý nepodporuje skutočný obsah;
- zavádzajúci obsah, v ktorom sa informácie používajú zavádzajúcim spôsobom s cieľom ohraničiť niečo alebo niekoho;
- falošný kontext, v ktorom je samotný obsah pravý, ale je vytrhnutý z kontextu a umiestnený do iného;
- podvádzajúci obsah, v ktorom falošné a vymyslené zdroje napodobňujú pravé zdroje a ako také ich zobrazujú s cieľom oklamať publikum (t. j. maskované ako legitímne mainstreamové médiá);
- zmanipulovaný obsah, pri ktorom sa pravý obsah, ako sú obrázky, mení s cieľom klamať.
- vymyslený obsah, kde je všetok obsah falošný a vytvorený so škodlivým úmyslom.[12]

Zatiaľ čo niektoré falošné správy sa javia ako falošné, príbehy falošných správ sú čoraz sofistikovanejšie. Jednou z bežne používaných metód je zmazať hranicu medzi pravdou a do očí bijúcimi klamstvami. Jedným z príkladov takýchto sofistikovaných falošných správ sú „deepfakes“ – fiktívne videá alebo obrázky, na ktorých dobre známi alebo vymyslení ľudia robia alebo hovoria veci, ktoré nie sú skutočné. Sú vytvorené pomocou umelej inteligencie a strojového učenia.

Falošné správy a bezpečnosť

Žiaľ, ako je už naznačené vyššie, v súčasnej dobe žijeme okrem iného aj v ére falošných správ, v ktorej ich tvorcovia – kyberzločinci využívajú tento fenomén a robia si z neho pomerne lukratívny biznis. Ceny za ich služby sa zdajú byť dostupné, pretože sú, ako sa zdá, široko využívané. Napríklad falošné a vymyslené mediálne webové stránky sú vytvorené tak, aby pripomínali legitímne médiá. Niektorí zločinci používajú metódy, ako je úprava legitímnych dokumentov a ich distribúcia, napríklad v rámci rôznych dezinformačných kampaní. Odborníci na informačnú a kybernetickú bezpečnosť a odhaľovanie falošných správ, dezinformácií a hoaxov identifikovali takmer 2 800 miest „živej fikcie“, ktorá sa dosahuje jednoducho len zmenou jediného písmena vo webovej adrese, čím sa vytvorí falošný „klon“ na skutočnej spravodajskej webovej stránke.[13]

Hoci sa používanie rozličných techník v rôznych, prevažne politických, ale aj konkurenčných obchodných kampaniach, stalo zdrojom vážnych obáv, rovnaké metódy možno

[12] ARKVIK, I. 2021. What is fake news? In VISMA, 2021
[13] KHAN, M. K. 2020. Sifting truth from fiction: enhanced protection from fake news. In *G20 Insights*, 2020

použiť aj na zisk. Jednoduchý prístup k príslušným nástrojom poukazuje na takmer úplný nedostatok prekážok. Podľa Ricka Hollanda, viceprezidenta pre stratégiu spoločnosti Digital Shadows, sú „súpravy nástrojov" dostupné na dočasné použitie len za 7 dolárov na ovládanie robotov v sociálnych médiách. Mnohé z týchto služieb sú inzerované v Dark Net, kde je ťažké identifikovať používateľov. Niektoré sú však otvorene propagované ako marketingové nástroje. Holland v tomto kontexte zdôrazňuje, že zavádzajúce, klamlivé, vymyslené informácie síce existujú už dlho, ale dnes je novinkou v digitálnom svete rýchlosť, akou sa takéto techniky šíria po celom svete.[14]

Pozornosť bezpečnostných expertov priťahujú falošné správy aj preto, že sa používajú na distribúciu malvéru. Podľa viacerých odborníkov, napríklad Scotta Nelsona, viceprezidenta SecureSet, sú falošné správy najnovšou líniou sociálneho inžinierstva a hackingu. Rovnako ako phishingové útoky, existuje veľa možností ich využívania. Na druhej strane, nie každý podozrivý odkaz na Facebooku alebo inej sociálnej sieti musí byť považovaný za falošný. Ani automatizované riešenia na ich odhalenie nedokážu vždy identifikovať podozrivú alebo nepravdivú správu. V každom prípade, používanie falošných správ na distribúciu malvéru prostredníctvom sociálnych sietí je relatívne nový prístup.[15]

Falošné správy a Európska únia

Do boja proti falošným správam sa aktívne zapája aj Európska únia. Európska komisia v tejto súvislosti vytvorila expertnú skupinu[16], ktorá sa zaoberá viacerými oblasťami , v ktorých sa najvýraznejšie prejavujú falošné správy a dezinformácie negatívne ovplyvňujúce európsku spoločnosť, jej občanov, ako aj bezpečnosť a demokraciu v členských krajinách Európskej únie (zahraničné zasahovanie do volieb a vnútorných záležitostí EÚ[17], pandémia koronavírusu[18], propaganda namierená proti EÚ[19] atď.). Tento vážny problém nie je neznámy ani Slovensku a preto príslušné inštitúcie a orgány prijímajú náležité opatrenia. Napríklad z opatrenia uloženého v Akčnom pláne digitálnej transformácie Slovenska[20], ktorého cieľom je predovšetkým nastavenie inštitucionálneho zabezpečenia odolnosti voči prvkom informačných

[14] FERRARO, M. F. – CHIPMAN, J. C. 2019. Fake news threatens our businesses, not just our politics. In *The Washington Post*, 2019
[15] FERRARO, M. F. – CHIPMAN, J. C. 2019. Fake news threatens our businesses, not just our politics. In *The Washington Post*, 2019
[16] Bližšie pozri: EP. *Boj proti dezinformáciám*. In Európsky parlament, 2022
[17] Bližšie pozri: EP. EÚ musí aktívnejšie bojovať proti dezinformáciám a zahraničnému zasahovaniu do volieb. In *Európsky parlament*, 2022
[18] Bližšie pozri: EP. Koronavírus, EÚ a vyvracanie dezinformácií. In *Európsky parlament*, 2022
[19] Bližšie pozri: EP. Propaganda namierená proti EÚ je čoraz sofistikovanejšia. In *Európsky parlament*, 2019
[20] Bližšie pozri: MIRRI SR. Akčný plán digitálnej transformácie Slovenska na roky 2019-2022. In *Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky*, 2019.

operácií, bola zriadená medzirezortná pracovná skupina s cieľom vytvoriť koordinovaný mechanizmus na boj proti falošným správam, dezinformáciám, hoaxom a propagande. Účelom je vytvoriť mechanizmus reakcie voči zámernému, systematickému a rozsiahlemu šíreniu falošných, nepravdivých, skreslených informácií, čo pre európske demokracie a spoločnosti predstavuje jednu z najvážnejších a najaktuálnejších výziev. Vláda Slovenskej republiky a jednotlivé rezorty okrem toho prijímajú aj ďalšie opatrenia na boj s falošnými správami.[21]

Lavína nových technologických riešení a tempo, akým sa zvyšujú výpočtové schopnosti systémov, donedávna robili teoretické riziká a hrozby celkom reálne a hmatateľné. Nájsť falošné správy totiž nie je jednoduché. Viaceré výskumy v ostatných rokoch ukázali, že ľudia sú extrémne slabí v rozlišovaní medzi rôznymi typmi online vecí, bez ohľadu na to, či sú platené, falošné alebo zákonné. V tejto súvislosti komisárka EÚ pre digitálnu ekonomiku a spoločnosť Mariya Gabriel založila pravidelnú verejnú konferenciu o falošných správach a vyhlásila zriadenie expertnej skupiny na úrovni EÚ s cieľom analyzovať, do akej miery problém spojený s falošnými správami ohrozuje EÚ.[22]

Falošné správy sa v súčasnosti šíria alarmujúcou rýchlosťou a podľa eurokomisárky Gabrielovej ohrozujú blaho ľudí, spoločnosti a demokracie. V tejto súvislosti zároveň dodáva, že falošné správy dusia okrem spoločnosti i médiá. Preto presadzuje analýzu na úrovni EÚ s cieľom posúdiť mieru, do akej miery falošné správy ohrozujú Úniu, a navrhnúť, či je pravdepodobné, že sa nájde možné riešenie tohto javu. Hlavnou výzvou je definovať falošné správy a dobré novinárske praktiky.[23] Problém je v tom, že médiá sú v ťažkej situácii pokiaľ ide o dôveru médií, pretože sociálne siete postupne získavajú stále väčšiu popularitu a ľudia viac veria tomu, s čím sa stretávajú na Facebooku, Twitteri alebo Instagrame, ako informáciám, ktoré sa nachádzajú v odborných médiách.[24]

Irina Nedeva, predsedníčka Asociácie európskych novinárov, v tomto kontexte poukazuje na falošné správy ako na hlavnú výzvu, ktorej súčasní novinári čelia. Čo je však podľa nej znepokojujúce, je riziko uchyľovania sa k nadmernej regulácii, ktorá môže byť použitá na potlačenie slobody prejavu. Je preto veľkou výzvou rozlíšiť fakty od poloprávd, klamstiev a výmyslov. Asociácia a jej partneri z toho dôvodu v súčasnosti zvažujú, ako posilniť

[21] Bližšie pozri: SLIZ, M. Vláda v boji s dezinformáciami. In Aktuality, 2020; JURÁŠEK, D. Vláda vyhlásila veľký boj proti dezinformáciám a hoaxom. Aké sú jej prvé kroky? In HrotInfo, 2020; alebo SLIZ, M. Štát sa pokúsi predbehnúť dezinformátorov. Naď s Mikulcom zriaďujú tímy na boj s hybridnými hrozbami. In Aktuality, 2022

[22] Bližšie pozri: STUPP, C. Gabriel leading Commission effort against fake news 'disease'. In *Euractive.com,* 2017; alebo STUPP, C. Gabriel to start EU expert group on fake news. In *Euractive.com,* 2017.

[23] NIELSEN, N. EU Commission to target fake news. In *EU Observer*, 2017

[24] AEJ. 2017. European Commissioner Mariya Gabriel: Fake news stifle the media and society. In *Association of European Journalists*, 2017

úlohu profesionálnej žurnalistiky, zvýšiť mediálnu gramotnosť a zriadiť jednotky na vyhľadávanie faktov v spravodajských médiách. Na prekonanie tohto javu je zároveň potrebné zabezpečiť transparentnosť a rôzne vysokokvalitné informácie a lepšie pochopiť mechanizmy ich šírenia a taktiež finančné toky.[25]

K dnešnému dňu je už síce definovaný nelegálny obsah (nenávistné prejavy), falošné správy sú však väčšinou legálne a v ich prípade nejde o trestný čin. Sloboda prejavu, ako aj právo na prístup k informáciám sú nedotknuteľné a nikto nemôže ani nemá v úmysle nútiť ľudí, aby verili konkrétnej informácii. Ak sa však neprijmú adekvátne opatrenia proti vytváraniu a šíreniu falošných správ na európskej úrovni, je vysoko pravdepodobné, že situácia nebude lepšia ani na národnej úrovni a falošné správy budú aj naďalej predstavovať hrozbu pre súčasnú spoločnosť.

Záver

V dnešnej modernej dobe široko dostupného rýchleho internetu a najrozličnejších vysoko výkonných „smart“ zariadení sa ľudia dokážu dostať k veľkému množstvu informácií veľmi rýchlo a jednoducho. Najnovšie správy či údaje sú ľahko dostupné prostredníctvom internetových webových stránok, spravodajských portálov alebo sociálnych sietí, ktoré na ne odkazujú. S narastajúcim množstvom informácií sa zvyšuje aj množstvo falošných správ. Ich cieľom je zapôsobiť na čitateľov tak, aby uverili informáciám, ktoré sú v nich prezentované ako fakty, hoci tieto správy sú falošné, skreslené či nepravdivé (alebo aspoň z časti nepravdivé). Ukazuje sa, že falošné správy ovplyvňujú mienku a názory ľudí oveľa viac, než by sa na prvý pohľad mohlo zdať.

Jedným z dôvodov prečo majú taký vplyv a zároveň jedným z najväčších problémov je ich ľahká dostupnosť pre všetkých a rýchlosť šírenia. K obom týmto atribútom prispel najmä internet a rozmach sociálnych sietí, kde predovšetkým mladí ľudia trávia až príliš veľa času a kde môže ktokoľvek rýchlo, jednoducho a zadarmo takéto správy vytvárať a šíriť. Pre nich je potom často oveľa pohodlnejšie získavať informácie zo sociálnych sietí ako z klasických spravodajských portálov, čo tiež prispieva k prehlbovaniu tohto problému. Ďalším problémom je fakt (existujú o tom mnohé svedectvá a dôkazy), že množstvo priaznivcov prostredníctvom internetu a sociálnych sietí priťahujú a získavajú na svoju činnosť radikálne organizácie, ktoré šíria rôzne falošné správy, dezinformácie a propagandu.

[25] AEJ. 2018. Fake news undermines democratic freedoms: the AEJ’s road-map for the right responses. In *Association of European Journalists,* 2018

Medzi najzraniteľnejšie z hľadiska týchto rizík patria demokratické štáty. Európska únia i jej členské štáty už prijímajú praktické opatrenia na neutralizáciu falošných správ, ale pre každý členský štát je dôležité mať aj vlastnú transparentnú a konkrétnu politiku, prípadne viac politík, stratégií alebo koncepcií zameraných na boj proti falošným správam. Zvýšenie povedomia o falošných správach, zlepšenie schopnosti rozoznávať a odhaľovať ich, ako aj eliminovať ich šírenie v čo najväčšej miere by určite znamenalo menej príležitostí napríklad pre populizmus, radikalizmus, extrémizmus, xenofóbiu či akékoľvek ovplyvňovanie alebo rozdeľovanie spoločnosti práve na základe posúvania klamlivých a zavádzajúcich informácií. Angažovanie relevantných európskych inštitúcií, ako aj inštitúcií demokratických štátov v tejto problematike je z toho dôvodu nielen žiaduce, ale dokonca nevyhnutné. Na druhej strane si všetci musíme uvedomiť, že ich možnosti nie sú nekonečné, nie všetko za nás vyrieši štát, a tak je nutné, aby sme aj my sami prispeli k potláčaniu množstva, sily a vplyvu dezinformácií a ich šíriteľov na naše konanie.

Zoznam použitej literatúry

AEJ. 2017. European Commissioner Mariya Gabriel: Fake news stifle the media and society. In *Association of European Journalists*, 2017. [online] [Cit. 03.04.2022] Dostupné na: <https://aej-bulgaria.org/en/european-commissioner-mariya-gabriel-fake-news-stifle-the-media-and-society/>.

AEJ. 2018. Fake news undermines democratic freedoms: the AEJ's road-map for the right responses. In *Association of European Journalists*, 2018. [online] [Cit. 03.04.2022] Dostupné na: <https://aej-belgium.eu/fake-news-undermines-democratic-freedoms-aejs-road-map-right-responses/>.

ALLCOTT, H. – GENTZKOW, M. Social Media and Fake News in the 2016 Election. In *Journal of Economic Perspectives*, 2017, roč. 31, č. 2, s. 211–236. ISSN 0895-3309.

ANDRASSY, V. – GREGA, M. 2015. Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In *Košická bezpečnostná revue*, 2015, roč. 5, č. 2, s. 11-18. ISSN 1338-4880.

ARKVIK, I. 2021. What is fake news? In *VISMA*, 2021. [online] [Cit. 03.04.2022] Dostupné na: <https://www.visma.com/blog/what-is-fake-news/>.

CD. 2018. Word of the Year 2017 is Fake News. In *Collins Dictionary*, 2018. [online] [Cit. 01.04.2022] Dostupné na: <https://www.collinsdictionary.com/woty>.

EP. 2019. Propaganda namierená proti EÚ je čoraz sofistikovanejšia. In *Európsky parlament*, 2019. Dostupné na: <https://www.europarl.europa.eu/news/sk/headlines/priorities/fake-news/20190130STO24604/propaganda-namierena-proti-eu-je-coraz-sofistikovanejsia-rozhovor>.

EP. 2022. *Boj proti dezinformáciám*. In *Európsky parlament*, 2022. [online] [Cit. 03.04.2022] Dostupné na: <https://www.europarl.europa.eu/news/sk/headlines/priorities/fake-news>.

EP. 2022. EÚ musí aktívnejšie bojovať proti dezinformáciám a zahraničnému zasahovaniu do volieb. In *Európsky parlament*, 2022. [online] [Cit. 03.04.2022] Dostupné na: <https://www.europarl.europa.eu/news/sk/headlines/priorities/fake-news/20191007IPR63550/eu-musi-aktivnejsie-bojovat-proti-dezinformaciam-a-zahranicnemu-zasahovaniu>.

EP. 2022. Koronavírus, EÚ a vyvracanie dezinformácií. In *Európsky parlament*, 2022. [online] [Cit. 03.04.2022] Dostupné na: <https://www.europarl.europa.eu/news/sk/headlines/priorities/fake-news/20200618STO81510/koronavirus-eu-a-vyvracanie-dezinformacii>.

FERRARO, M. F. – CHIPMAN, J. C. 2019. Fake news threatens our businesses, not just our politics. In *The Washington Post*, 2019. [online] [Cit. 01.04.2022] Dostupné na: <https://www.washingtonpost.com/outlook/fake-news-threatens-our-businesses-not-just-our-politics/2019/02/08/f669b62c-2b1f-11e9-984d-9b8fba003e81_story.html>.

FORGAS, J. P. – BAUMEISTER, R. 2019. *The Social Psychology of Gullibility: Conspiracy Theories, Fake News and Irrational Beliefs*. London : Routledge, 2019. 352 s. ISBN 978-0-429-51219-3.

FRIANOVÁ, V. 2020. Kybernetická bezpečnosť ako jeden z „vedľajších produktov“ investovania štátu do obrany, ľudských zdrojov, výskumu a vývoja In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 17-22. ISBN 978-80-8040-819-3.

GREGOR, M. a kol. *Nejlepší kniha o Fake News, dezinformacích a manipulacích!!!* Brno : CPress, 2018. 143 s. ISBN 978-80-264-1805-4.

JURÁŠEK, D. 2020. Vláda vyhlásila veľký boj proti dezinformáciám a hoaxom. Aké sú jej prvé kroky? In *HrotInfo*, 2020. [online] [Cit. 03.04.2022] Dostupné na: <https://hrot.info/sloboda-prejavu/2640-vlada-vyhlasila-velky-boj-proti-dezinformaciam-a-hoaxom-ake-su-jej-prve-kroky>.

HAJDÚKOVÁ, T. – HRUŠKA, P. 2018. Prínos siete Internet pre rozvoj spoločnosti a jeho možnosti využitia v činnosti Policajného zboru. In Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním. Bratislava : Akadémia Policajného zboru v Bratislave, 2018, s. 131-142. ISBN 78-80-8054-768-4.

KHAN, M. K. 2020. Sifting truth from fiction: enhanced protection from fake news. In *G20 Insights*, 2020. [online] [Cit. 02.04.2022] Dostupné na: <https://www.g20-insights.org/policy_briefs/sifting-truth-from-fiction-enhanced-protection-from-fake-news/>.

KORAUŠ, A. – KELEMEN P. 2018. Protection of persons and property in terms of cybersecurity. In *Ekonomické, politické a právne otázky medzinárodných vzťahov 2018 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Vydavateľstvo Ekonóm, 2018. ISBN 978-80-225-4506-8.

KOSTREC, M. 2020. Nebezpečné hrozby v digitálnom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti: zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : A PZ, 2020, s. 78-87. ISBN 978-80-8040-819-3.

KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98. ISBN 978-80-8054-773-8.

McQUAIL, D. 2009. *Úvod do teorie masové komunikace*. Praha : Portál, 2009. 447 s. ISBN 978-80-7367-338-3.

MIRRI SR. 2019. Akčný plán digitálnej transformácie Slovenska na roky 2019-2022. In *Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky*, 2019. [online] [Cit. 03.04.2022] Dostupné na: <https://www.mirri.gov.sk/wp-content/uploads/ 2019/07/Akcny-plan-DTS_2019 -2022.pdf>.

NIELSEN, N. 2017. EU Commission to target fake news. In *EU Observer*, 2017. [online] [Cit. 03.04.2022] Dostupné na: <https://euobserver.com/justice/139850>.

PLIEŠOVSKÝ, R. 2021. Videli ste už schému nanočipu z vakcíny Pfizer? In *Techbox*, 2021. [online] [cit. 01.04.2022] Dostupné na internete: <https://techbox.dennikn.sk/ temy/videli-ste-schemu-nanocipu-z-vakciny-pfizer/>

REITER, M. 2021 Chcú nás začipovať? A môže za to Pfizer a 5G? In *TouchIT*, 2021. [online] [cit. 01.04.2022] Dostupné na internete: <https://touchit.sk/chcu-nas-zacipovat-a-moze-za-to-pfizer-a-5g-tu-su-nase-odpovede/357432>

RÉVESZOVÁ, L. 2018. Počítačová kriminalita a dynamika jej vývoja v rokoch 2014 - 2017. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : A PZ, 2018, s. 161-173. ISBN 978-80-8054-773-8.

SLIZ, M. 2020. Vláda v boji s dezinformáciami: nové technológie, nové tresty aj zmena vzdelávania. In *Aktuality*, 2020. [online] [Cit. 03.04.2022] Dostupné na: <https://www. aktuality.sk/clanok/784303/vlada-v-boji-s-dezinformaciami-nove-technologie-nove-tresty-aj-zmena-vzdelavania/>.

SLIZ, M. 2022. Štát sa pokúsi predbehnúť dezinformátorov. Naď s Mikulcom zriaďujú tímy na boj s hybridnými hrozbami. In *Aktuality*, 2022. [online] [Cit. 03.04.2022] Dostupné na: <https://www.aktuality.sk/clanok/ 17g4nez/stat-sa-pokusi-predbehnut-dezinformatorov-nad-s-mikulcom-zriaduju-timy-na-boj-s-hybridnymi-hrozbami/>.

STUPP, C. 2017. Gabriel leading Commission effort against fake news 'disease'. In *Euractive.com*, 2017. [online] [Cit. 03.04.2022] Dostupné na: <https://www.euractiv.com/ section/digital/news/gabriel-leading-commission-effort-against-fake-news-disease/>.

STUPP, C. 2017. Gabriel to start EU expert group on fake news. In *Euractive.com*, 2017. [online] [Cit. 03.04.2022] Dostupné na: <https://www.euractiv.com/section/digital/news/ gabriel-to-start-eu-expert-group-on-fake-news/>.

TITCOMB, J. – CARSON, J. 2018. Fake news: What exactly is it – and how can you spot it? In *The Telegraph, 2018*. [online] [Cit. 02.04.2022] Dostupné na: <https://www.telegraph.co.uk/ technology/0/fake-news-exactly-has-really-hadinfluence/>.

TOMÁŠEK, R. – TOMÁŠEKOVÁ, L. 2020. Kybernetické hrozby a kybernetický terorizmus. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : A PZ, 2020, s. 146-152. ISBN 978-80-8040-819-3.

WASSIM, A. a kol. 2020. Four Experts Investigate How the 5G Coronavirus Conspiracy Theory Began. In *The Conversation*, 2020. [online] [cit. 01.04.2022] Dostupné na: <https://theconversation.com/four-experts-investigate-how-the-5gcoronavirus-conspiracy-theory-began-139137>

ZACHAR, Š. 2018. Anonymizácia komunikácie zmenou IP adresy ako metóda bezpečného prehliadania internetu. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : A PZ, 2018, s. 217-224. ISBN 978-80-8054-773-8.

Kontaktné údaje

plk. gšt. v. z. doc. Ing. Radoslav Ivančík, PhD. et PhD., MBA, MSc.

Katedra informatiky a manažmentu

Akadémia Policajného zboru v Bratislave

Sklabinská 1, 835 17 Bratislava

e-mail: radoslav.ivancik@akademiapz.sk

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

PhDr. Peter Veselý, PhD.

O bezpečnosti v kontexte DDoS útokov[26]

Rastislav Kazanský - Nina Mijoč

Abstrakt: Na začiatku tretieho desaťročia 21. storočia predstavuje kyberterorizmus jednu z najvážnejších bezpečnostných hrozieb pre verejný a súkromný sektor. Žiadna krajina, spoločnosť ani spoločnosť nie je v dnešnej dobe imúnna voči kybernetickým aktivitám. Kybernetické útoky sa vykonávajú takmer vo všetkých regiónoch sveta a predstavujú každodennú hrozbu pre veľké množstvo ľudí, úradov a inštitúcií v mnohých krajinách. Žiaľ, v súčasnosti, v informačnom veku, môžu kybernetické útoky zasiahnuť takmer každého, kdekoľvek a kedykoľvek. Zároveň môžu spôsobiť obrovské osobné a organizačné problémy a obrovské materiálne a finančné škody. A to sú dôvody, prečo kybernetická bezpečnosť nadobúda stále väčší význam. Jeden z najzávažnejších a najúčinnejších kybernetických útokov predstavujú DDoS útoky.

Kľúčové slová: Bezpečnosť, komunikačné a informačné technológie, útoky typu Distributed Denial of Service, kybernetická bezpečnosť.

Abstract: At the beginning of the third decade of the 21st century, cyberterrorism represents one of the most serious security threats for the public and private sector. No country, society or company is immune to cyber activities in these days. Cyberattacks are performed nearly in all regions of the world and present daily menace for a large number of people, offices and institutions in many countries. Unfortunately, at present, at the information age, cyberattacks can hit almost anyone, anywhere and anytime. Simultaneously, they can cause enormous personal and organisational problems, and tremendous material and financial damages. And those are the reasons why cyber security gains still more and more significance. One of the most serious and effective cyberattacks on society represent DDoS attacks.

Keywords: Security, communication and information technologies, Distributed Denial of Service attacks, cyber security.

Úvod

V súčasnosti je čoraz širšia škála procesov a aktivít vo všetkých oblastiach nášho každodenného života v súčasnej modernej spoločnosti založená na integrácii komunikačných a informačných technológií (ďalej len „KIT“) a počítačových systémov, prepojených sieťami a internetom.[27] Masívne využívanie počítačov, nástup internetu, vznik celosvetovej komunikačnej a informačnej siete, digitálne spracovanie informácií a obchodovanie s nimi, ako aj prenos dát a informácií prostredníctvom sietí na veľké vzdialenosti vedú k prehlbujúcej sa

[26] Príspevok bol spracovaný v rámci riešenia projektu APVV-20-0334 „Nie je to pravda, ale mohla by byť.“ Konšpiračné teórie a hoaxy v modernom vývoji Slovenska v európskom kontexte.

[27] IVANČÍK, R. – BARIČIČOVÁ. Ľ. 2019. Kybernetické hrozby ako súčasť asymetrických bezpečnostných hrozieb v 21. storočí. In *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019, s. 35

závislosti vyspelých štátov sveta a ich ekonomík na KIT, k zvyšovaniu ich vzájomnej prepojenosti i závislosti, a zároveň k "zmenšovaniu" vzdialeností medzi nimi.[28] Technologický pokrok však neprináša len nové príležitosti, výzvy a prosperitu, ale aj nové bezpečnostné riziká a hrozby. Preto sa čoraz dôležitejšou a naliehavejšou stáva ochrana kybernetického priestoru a kritickej informačnej infraštruktúry, čiže zaistenie kybernetickej bezpečnosti.[29]

Zvyšujúca sa závislosť spoločnosti na KIT vedie ku vzniku nových foriem bezpečnostných hrozieb, ktorým musia štáty čeliť,[30] a to bez ohľadu na to, či ide o hrozby úmyselné, zapríčinené človekom, alebo hrozby náhodné, vyplývajúce napríklad z bežnej poruchy, zlyhania systému alebo živelnej pohromy. Tieto hrozby však čoraz častejšie ohrozujú kybernetickú národnú i medzinárodnú bezpečnosť. Kybernetické hrozby vychádzajú z rôznych zdrojov, prejavujú sa rozvratnou a rušivou činnosťou namierenou proti jednotlivcom, verejným a súkromným inštitúciám, národnej infraštruktúre, podnikateľským subjektom i vláde krajiny. Vyznačujú sa viacerými špecifickými črtami, ako napríklad ich nadnárodným charakterom, rozptýlenosťou, nejednoznačnosťou, anonymitou útočníkov, nízkymi vstupnými nákladmi a taktiež možnosťou zaútočiť z veľkej vzdialenosti bez priameho kontaktu s cieľom.[31] Aktérmi môžu byť štáty, jednotlivci, alebo neštátni aktéri. Hlavnými hrozbami, ktorým musia v súčasnosti štáty a organizácie čeliť, sú najmä hacking, kybernetická kriminalita, kybernetický terorizmus, politický a ideologický extrémizmus, kybernetická špionáž alebo aj niektorými štátmi sponzorované kybernetické útoky a agresia, kybernetický boj.

Kybernetická bezpečnosť

So vzrastajúcim počtom kybernetických útokov na verejné i súkromné počítačové siete a rastom prípadov kybernetickej kriminality vzrastajú vo verejnom aj súkromnom sektore obavy týkajúce sa zraniteľnosti komunikačných a informačných systémov (ďalej len „KIS"), ktoré pramenia predovšetkým zo skutočnosti, že jednotlivé informačné infraštruktúry sú navzájom prepojené a na sebe závislé. So vzrastajúcimi obavami zároveň rastú požiadavky na zaistenie kybernetickej bezpečnosti. Preto jednotliví aktéri pristupujú k zavádzaniu rôznych

[28] NEČAS, P. – IVANČÍK, R. 2019. Aktuálny vývoj v oblasti zaisťovania kybernetickej bezpečnosti a ochrany informácií na národnej a nadnárodnej úrovni. In Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2019. s. 125

[29] IVANČÍK, R. 2012. *Kybernetická bezpečnosť – neoddeliteľná súčasť národnej a medzinárodnej bezpečnosti.* In *Národná a medzinárodná bezpečnosť 2012 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála Milana Rastislava Štefánika. 2012. s. 173

[30] TUNGAL, A. T. 2022. What is a Cyber Threat? In *UpGuard*, 2022

[31] IVANČÍK, R. 2019. Kybernetický boj ako jeden z nekonvenčných spôsobov boja. In *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek) – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019, s. 26

politík a opatrení, ktoré by prehĺbili ochranu kybernetického priestoru a kritickej informačnej infraštruktúry a reagovali tak na nevyhnutnosť ochrany utajovaných informácií, počítačových sietí a zavádzania efektívneho dodržiavania bezpečnostných štandardov. Cieľom kybernetickej bezpečnosti je vybudovanie dôvery v spoľahlivosť kritickej informačnej infraštruktúry a istoty, že bude plniť svoje funkcie a úlohy a slúžiť národným záujmom aj v prípade kybernetického útoku.[32]

Aj preto možno kybernetickú bezpečnosť chápať ako schopnosť siete alebo informačného systému odolávať náhodným udalostiam aj škodlivým aktivitám, ktoré môžu negatívne ovplyvniť dostupnosť, celistvosť, dôvernosť a hodnovernosť uložených a prenášaných dát a informačných služieb zaisťovaných prostredníctvom siete alebo informačného systému.[33] Predstavuje teda a) zaistenie dostupnosti služieb a dát, b) zamedzenie rozvrátenia a narušenia siete a neoprávneného odpočúvania komunikácie, c) potvrdenie, že dáta, ktoré boli poslané, prijaté alebo uložené, sú kompletné a nezmenené, d) zaistenie dôvernosti dát, ochrany informačných systémov proti neoprávnenému prístupu k nim a proti útokom zahŕňajúcim škodlivý softvér a e) zabezpečenie hodnovernej autentifikácie.[34] Pod pojmom kybernetická bezpečnosť možno zároveň chápať fyzické mechanizmy, definované politiky alebo procesy, ktorých úlohou je chrániť systémy, dáta alebo všeobecne majetok pred hrozbou alebo útokom. Každá ochrana sa vyznačuje určitými zraniteľnosťami, ktoré predstavujú slabé miesta ochrany alebo jej úplnú absenciu.[35]

Základom kybernetickej bezpečnosti je zaistenie ochrany kybernetického priestoru na národnej úrovni. Vysporiadať sa s výzvami, ktoré ohrozujú spoločenský a sociálno-ekonomický poriadok a univerzálne práva jednotlivcov je zodpovednosťou a povinnosťou štátu. Môže to byť dosiahnuté prostredníctvom a) implementácie príslušných stratégií, politík a bezpečnostných opatrení týkajúcich sa celého spektra kybernetických hrozieb a zraniteľností, b) vytvorením jasného legislatívneho rámca, ktorý špecifikuje kompetencie, oprávnenia a povinnosti relevantných inštitúcií v prípade kybernetických útokov, c) vymedzením oblasti pôsobnosti, kompetencií a povinností jednotlivých aktérov na národnej úrovni s cieľom zaistiť

[32] ITU. 2011. *International Telecommunication Union – National Cybersecurity Strategy Guide*, s. 37
[33] CoEC. 2001. Commission of the European Communities. *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for A European Policy Approach*.
[34] EC. 2002. *European Council Resolution of 28 January 2002 on a Common Approach and Specific Actions in the Area of Network and Information Security*.
[35] JIROVSKÝ, V. 2007. *Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, 2007, s. 10

účinné a efektívne zvládnutie bezpečnostných incidentov a udalostí a posilniť vzájomnú spoluprácu.

V tejto súvislosti je nevyhnutné si uvedomiť, že schopnosť vysporiadať sa a zvládnuť riziká spojené s používaním KIT nespočíva len na vláde a verejnom sektore, ale na vzájomnej spolupráci verejného sektora so súkromným sektorom, ktorý v súčasnosti vlastní, riadi alebo spravuje väčšinu národnej kritickej informačnej infraštruktúry. Aktérmi kybernetickej bezpečnosti sa tak stávajú nielen vládne inštitúcie zodpovedné za zaistenie bezpečnosti kritických informačných infraštruktúr na národnej úrovni, ale aj aktéri zodpovední za informačnú bezpečnosť a nepretržitú prevádzku KIS na úrovni súkromného sektoru a samotní individuálni užívatelia. Zaistenie kybernetickej bezpečnosti preto musí spočívať v posilnení siete vzájomnej spolupráce medzi súkromným a verejným sektorom ako na národnej, tak aj na medzinárodnej úrovni a na vytvorení stavu rovnováhy medzi národnými a medzinárodnými reakciami na aktuálne výzvy.

K základným oblastiam kybernetickej bezpečnosti možno priradiť a) správu internetu a všeobecnú bezpečnosť siete, b) ochranu kritickej informačnej infraštruktúry, c) kybernetický boj a reakciu na kybernetický útok, d) kybernetickú kriminalitu, kybernetický terorizmus a využívanie internetu na teroristické účely, e) bezpečnosť elektronického obchodu, f) ochranu osobných údajov a súkromia a aj g) ochranu pred nevyžiadanou elektronickou poštou. Od týchto oblastí sa odvíjajú jednotlivé úrovne pripravenosti v rámci kybernetickej bezpečnosti, t. z. každodenné uplatňovanie kybernetickej bezpečnosti, pripravenosť na kybernetickú kriminalitu a na kybernetické útoky, zvlášť na také útoky, ktoré by mohli ohroziť národnú bezpečnosť.[36]

DDoS útoky

DDoS (Distributed Denial of Service) útoky predstavujú vyšší vývojový stupeň tzv. DoS (Denial of Service) útokov, ktoré sú známe od 80. rokov minulého storočia. Základný rozdiel medzi týmito typmi útokov spočíva v tom, že DDoS útoky sú vo svojej podstate distribuované útoky, to znamená že pochádzajú z viac ako jedného zdroja, čím sú zároveň efektívnejšie a nebezpečnejšie.[37] DoS aj DDoS útoky pritom možno charakterizovať ako útoky na internetové služby alebo webové stránky, pri ktorých dochádza k ich zahlteniu požiadavkami

[36] TIKK, E. 2010. Global Cyber Security - Thinking About The Niche for NATO. In *The SAIS Review of International Affairs*, 2010, s. 72
[37] INCAPSULA, Inc. 2017. *Denial of Service Attacks*.

a k pádu alebo nefunkčnosti a nedostupnosti systému pre ostatných užívateľov, a to útokom z mnohých vektorov. DDoS útoky sa snažia o vyradenie a zneprístupnenie cieľovej služby.[38]

Ak zhrnieme samotnú podstatu DDoS útokov, možno povedať, že ide o útoky, ktoré sa zasielaním enormného počtu požiadaviek na cieľový server obete snažia o vyčerpanie kapacity zdroja. Tieto aktivity majú za následok nielen zneprístupnenie príslušnej služby až na niekoľko hodín, v dôsledku čoho môže dochádzať k značným, najmä finančným stratám, ale sprevádzať ho môže tiež napríklad pozmeňovanie dát, a to vďaka sprístupneniu siete.[39]

Jedným z najzásadnejších rysov DDoS útokov je ich distribuovaná povaha. K distribuovaným útokom sú útočníkmi využívané siete označované ako botnety. Tie predstavujú sieť infikovaných počítačov, ktoré sú zneužiteľné na páchanie kriminálnych aktivít vo veľkom meradle, a to vďaka prístupu k výpočtovému výkonu mnohých tisícov strojov súčasne. Botnety sú útočníkmi kontrolované, diaľkovo riadené, pričom ide o rozsiahlu a organizovanú sieť počítačov, ktoré sú naprogramované tak, aby súčasne a nepretržite vysielali veľké množstvo požiadaviek na cieľový systém. Tisíce infikovaných počítačov následne vykonáva bez vedomia používateľov počítača naprogramovanú úlohu, napríklad zahltia a zablokujú koordinovaným útokom zvolenú webovú stránku, hromadne zasielajú spam a podobne.

Cieľový systém je potom pod vplyvom DDoS útokov výrazne spomalený alebo dochádza k jeho kompletnému zrútenia.[40] Vytváranie botnetov je väčšinou automatická činnosť, ktorá prebieha cez skenovanie hľadajúce bezpečnostné diery a zraniteľnosť jednotlivých počítačov, väčšinou náhodných používateľov, ktoré sú následne infikované a využité k útoku alebo k ďalšiemu automatizovanému vyhľadávaniu iných zariadení, ktoré môžu byť ďalej zapojené do botnetu.[41] Botnety bývajú najčastejšie vytvorené napadnutím počítačov prostredníctvom techník ako je napríklad trójsky kôň, počítačovými vírusmi alebo napríklad metódou zadných vrátok.[42] Väčšina užívateľov, ktorí sa stanú súčasťou počítačovej siete hackerov, si svojho zapojenia do takéhoto typu útokov nie je vôbec vedomá.[43]

---

[38] MIRKOVIC, J. – REIHER, P. 2014. A taxonomy of DDoS attack and DDoS defense mechanisms. In *ACM SIGCOMM Computer Communications Review*, 2014, roč. 34, č. 2, s. 39

[39] GUPTA, M. – GOPALAKRISHNAN, G. – SHARMAN, R. 2017. *Counter-measures against Distributed Denial of Service*.

[40] CHANG, R. K. C. 2012. Defending against flooding-based distributed denial of service attacks. In *Computer journal of IEEE Communications Magazine*, 2012, roč. 40, č. 10, s. 45

[41] MIRKOVIC, J. – REIHER, P. 2014. A taxonomy of DDoS attack and DDoS defense mechanisms. In *ACM SIGCOMM Computer Communications Review*, 2014, roč. 34, č. 2, s. 41

[42] ZARGAR, S. T. – JOSHI, J. – TIPPER, D. 2013. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. In *Communica-tions Surveys & Tutorials*, 2013, roč. 15, č. 4, s. 2049

[43] INCAPSULA, Inc. 2017. *Denial of Service Attacks*.

Vzhľadom na vysoký počet charakteristických vlastností je veľmi ťažké prísť iba s jednou ucelenou typológiou DDoS útokov, ktorých medzi jednotlivými autormi existuje nespočetné množstvo a vyskytujú sa podľa rôznych úrovní a kritérií. Vzhľadom na obmedzený priestor príspevku preto vyberáme iba základné delenie DDoS útokov a ich typy, ktoré sú popísané v rozsahu, ktorý je relevantný cieľu tohto príspevku.

Základná typológia DDoS útokov rozdeľuje útoky do celkom troch skupín, a to na základe charakteru obete – to znamená podľa toho, či sú obeťou útoku a) siete, b) servery alebo c) aplikácie.

Prvým typom DDoS útokov sú útoky na siete, tiež označované ako objemové (volumetrické) útoky. Tento typ útoku využíva techniku tzv. záplavy pomocou paketov. Počas útoku na sieť útočník využíva celé dostupné prenosové pásmo cieľového servera a jeho pripojenie k internetu. Cieľom objemového útoku je spôsobiť všeobecné preťaženie infraštruktúry hrubou silou tak, že dôjde k vyčerpaniu dostupných zdrojov na cielených serveroch.[44] Výsledkom, resp. dôsledkom útoku je, že používateľ, ktorý sa k danej službe snaží dostať, sa stretne buď s veľmi pomalou odpoveďou alebo je mu prístup k službe úplne odmietnutý.

Druhým typom DDoS útoku podľa obete sú útoky vedené na servery. Tieto útoky sú vedené tak, aby došlo k vyčerpaniu procesora alebo pamäte cielených serverov a tie potom odmietli prístup k službe legitímnemu užívateľovi. K tomuto typu DDoS útoku je využitá niektorá zistená zraniteľnosť cieleného servera alebo zraniteľný návrh komunikačných protokolov, pričom napadnutý nemusí byť len server, ale tento postup môže byť aplikovaný aj na ďalšie týmto spôsobom zraniteľné ciele.[45]

V treťom prípade môžu DDoS útoky cieliť na aplikácie, pričom sa zameriavajú najmä na ich zraniteľnosť a využívajú vlastnosti aplikácií alebo protokolov (napr. HTTP, DNS, SMTP), ktoré sú vhodné pre spôsobenie odmietnutia služby. Aplikačné útoky sú sofistikovanejšie ako je tomu u predchádzajúcich dvoch typov. V porovnaní s objemovými útokmi je ich veľkou prednosťou najmä to, že nevyžadujú toľko zdrojov pre útok. Z hľadiska objemu dát totiž nie sú aplikačné útoky natoľko významné.[46] Tento typ útokov je tiež veľmi

[44] ZARGAR, S. T. – JOSHI, J. – TIPPER, D. 2013. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. In *Communica-tions Surveys & Tutorials*, 2013, roč. 15, č. 4, s. 2050
[45] KENIG,R. – MANOR, D. – GADOT, Z. – TRAUNER,. D. 2013. *DDoS Survival Handbook*.
[46] MINAŘÍK, P. 2015. *Metody ochrany před útoky typu DDoS v podniku a na páteřní síti*.

nebezpečný kvôli tomu, že ľahko splýva s bežnou prevádzkou. Bez cielenej analýzy paketov je potom veľmi ťažké útok odhaliť, na rozdiel od objemových útokov na sieť.[47]

Záver

V súvislosti s vyššie uvedenými informáciami možno v závere príspevku skonštatovať, že dosiahnuť absolútnu bezpečnosť je v súčasnosti pre štát, organizáciu alebo jednotlivca chimérou z dôvodu prítomnosti veľkého počtu možných ohrození – či už bezpečnostných, politických, spoločenských, ekonomických, environmentálnych alebo kybernetických. Vzhľadom na často nadnárodný charakter útokov, dochádza k stieraniu štátnych hraníc, ako aj hraníc medzi domácim a zahraničným, ako aj medzi verejným a súkromným. Geografické hranice, tak ako sú historicky definované medzi jednotlivými národmi, strácajú v prípade kybernetických hrozieb v kybernetickom priestore na význame. Zaistenie národnej bezpečnosti už nie je len vnútornou záležitosťou jedného štátu alebo jedného subjektu, ale naopak, stáva sa záležitosťou kolektívnej medzinárodnej spolupráce a koordinácie.

V súčasnej dobe prehlbujúcej sa globalizácie, ktorá prináša nielen množstvo pozitív, ale aj viacero negatív, napríklad v podobe kyberterorizmu, kybernetickej kriminality a kybernetických útokov na verejné či súkromné informačné siete, sa môže stať každý prvok národnej informačnej infraštruktúry potenciálnym cieľom, a preto je nevyhnutné starostlivo preskúmať a zhodnotiť nové bezpečnostné hrozby a riziká (a nielen v oblasti KIT, KII alebo KIS) a následne vyvodiť efektívne protiopatrenia v súvislosti s možnými útokmi využívajúcimi zraniteľnosti KIS a rastúcu závislosť národných inštitúcií a kritickej infraštruktúry na KIT.

Kybernetická bezpečnosť už dlho nie je len záležitosťou ochrany počítačov. Postupne sa stáva nevyhnutnou súčasťou národných politík, keďže nezákonné správanie sa v kybernetickom priestore ohrozuje národnú bezpečnosť, obranu jeho slobody, nezávislosti a suverenity, základné činnosti štátu, verejné služby, atď. Z toho dôvodu sú národní lídri a vedúci predstavitelia štátu zodpovední za zaistenie kybernetickej bezpečnosti, ktorá v súčasnosti predstavuje jednu zo základných podmienok fungovania štátu, výkonu jeho funkcií a poskytovania verejných služieb.

Efektívna a účinná obrana a ochrana v kybernetickom priestore si však vyžadujú spojenie viacerých oblastí, akými sú stratégie, doktríny a politiky, legislatíva a efektívny výkon práva, národná bezpečnosť, ochrana práva na súkromie, inštitucionálny rámec a stanovenie kompetencií, oblastí pôsobnosti a pravidiel angažovania sa jednotlivých orgánov a subjektov,

[47] ZARGAR, S. T. – JOSHI, J. – TIPPER, D. 2013. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. In *Communica-tions Surveys & Tutorials*, 2013, roč. 15, č. 4, s. 2050

technické štandardy a bezpečnostné technológie, bezpečnostné opatrenia a protiopatrenia, zvyšovanie povedomia a zdieľanie informácií, identifikácia hrozieb a rizík spojených s používaním KIT a KIS. Vytvorenie obrannej štruktúry v tejto oblasti si preto vyžaduje vysporiadať sa s organizačnými, politickými, ekonomickými, právnymi a ďalšími výzvami. Aj preto pristupujú vlády jednotlivých štátov v čoraz väčšej miere k prijímaniu veľkého množstva rôznych bezpečnostných opatrení za účelom zvýšenia kybernetickej bezpečnosti.

Zoznam použitej literatúry

AMOROSO, G. E. 2012. *Cyber Attacks. Protecting National Infrastructure*. New York : Elsevier, 2012. 336 s. ISBN 978-0-12391-867-3.

CNSS. 2010. *Committee on National Security Systems – National Information Assurance Glossary*. [online] [cit. 22.04.2022] Dostupné na: <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>.

CoEC. 2001. Commission of the European Communities. *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for A European Policy Approach*. [online] [cit. 21.04.2022] Dostupné na: <http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf>.

EC. 2002. *European Council Resolution of 28 January 2002 on a Common Approach and Specific Actions in the Area of Network and Information Security*. [online] [cit. 21.04.2022] Dostupné na: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002G0216(02):EN:HTML>

GUPTA, M. – GOPALAKRISHNAN, G. – SHARMAN, R. 2017. *Counter-measures against Distributed Denial of Service*. [online] [cit. 22.04.2022] Dostupné na: <https://www.albany.edu/iasymposium/proceedings/2016/ASIA2016_Proceedings_Final.pdf>

HALPIN, E. F. – TREVORROW, P. – WEBB, D – WRIGHT, S. 2006. *Cyberwar, Netwar and the Revolution in Military Affairs*. New York : Palgrave Macmillan. 304 s. ISBN 978-1-40398-717-4.

CHANG, R. K. C. 2012. Defending against flooding-based distributed denial of service attacks. In *Computer journal of IEEE Communications Magazine*, 2012, roč. 40, č. 10, s. 42-51. ISSN 0163-6804.

INCAPSULA, Inc. 2017. *Denial of Service Attacks*. [online] [cit. 22.04.2022] Dostupné na: <http://www.incapsula.com/ddos/ddosattacks/denial-of-service.html>.

ITU. 2010. International Telecommunication Union – Sample Legislative Language for Cyber Crime. In *Frameworks for International Cyber Security*. Tallinn: CCD COE Publications. [online] [cit. 22.04.2022] Dostupné na: <www.ccdcoe.org>.

ITU. 2011. *International Telecommunication Union – National Cybersecurity Strategy Guide*. [online] [cit. 22.04.2022] Dostupné na: <www.itu.int/ITUD/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf>.

IVANČÍK, R. – BARIČIČOVÁ. Ľ. 2019. Kybernetické hrozby ako súčasť asymetrických bezpečnostných hrozieb v 21. storočí. In *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek) – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019, s. 35-47. ISBN 978-80-8040-819-3.

IVANČÍK, R. 2012. *Kybernetická bezpečnosť – neoddeliteľná súčasť národnej a medzinárodnej bezpečnosti.* In *Národná a medzinárodná bezpečnosť 2012 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála Milana Rastislava Štefánika. 2012. s. 173-182. ISBN 978-80-8040-450-5.

IVANČÍK, R. 2019. Kybernetický boj ako jeden z nekonvenčných spôsobov boja. In *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek) – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019, s. 25-34. ISBN 978-80-8040-819-3.

JIROVSKÝ, V. 2007. *Kybernetická kriminalita - nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, a.s., 2007. 284 s. ISBN 978-80-2471-561-2.

KENIG,R. – MANOR, D. – GADOT, Z. – TRAUNER,. D. 2013. *DDoS Survival Handbook*. [online] [cit. 23.04.2022] Dostupné na: <https://www.scribd.com/document/17427 4499/DoS-Handbook>.

MINAŘÍK, P. 2015. *Metody ochrany před útoky typu DDoS v podniku a na páteřní síti*. [online] [cit. 23.04.2022] Dostupné na: <https://www.systemonline.cz/clanky/metody-ochrany-pred-utoky-typuddos.htm>

MIRKOVIC, J. – REIHER, P. 2014. A taxonomy of DDoS attack and DDoS defense mechanisms. In *ACM SIGCOMM Computer Communications Review*, 2014, roč. 34, č. 2, s. 39-53. ISSN 0146-4833.

NEČAS, P. – IVANČÍK, R. 2019. Aktuálny vývoj v oblasti zaisťovania kybernetickej bezpečnosti a ochrany informácií na národnej a nadnárodnej úrovni. In *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek) – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019. s. 125-137. ISBN 978-80-8040-819-3.

TIKK, E. 2010. Global Cyber Security - Thinking About The Niche for NATO. In *The SAIS Review of International Affairs*, 2010, č. 2. [online] [cit. 22.04.2022] Dostupné na: <http://www.ccdcoe.org/205.html>.

TUNGAL, A. T. 2022. What is a Cyber Threat? In *UpGuard*, 2022. [online] [cit. 22.04.2022] Dostupné na: <https://www.upguard.com/blog/cyber-threat>.

ZARGAR, S. T. – JOSHI, J. – TIPPER, D. 2013. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. In *Communications Surveys & Tutorials*, 2013, roč. 15, č. 4, s. 2046 – 2069. ISSN 2046-2069.

Kontaktné údaje

doc. PhDr. Rastislav Kazanský, PhD., MBA

Katedra bezpečnostných štúdií

Fakulta politických vied a medzinárodných vzťahov

Univerzita Mateja Bela

Krčméryho 1, 974 01 Banská Bystrica

E-mail: rastislav.kazansky@umb.sk

Mag.rel.publ. Nina Mijoč

doktorand

Katedra bezpečnostných štúdií

Fakulta politických vied a medzinárodných vzťahov

Univerzita Mateja Bela

Kuzmányho 1, 974 01 Banská Bystrica

E-mail: nina.mijoc.soccer@gmail.com

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

doc. RNDr. Tatiana Hajdúková, PhD.

Elektronická komunikácia v súčasnosti

Michaela Kiššová

Abstrakt: V úvode príspevku sa zameriavame na charakterizovanie ľudskej komunikácie a vybraných druhov komunikácie z hľadiska viacerých klasifikačných znakov. Definujeme charakteristické rysy osobnej a elektronickej komunikácie. Zameriavame sa aj na viaceré prípady zneužitia elektronickej komunikácie z pohľadu vybraných prípadov, ktoré boli spáchané v Slovenskej republike. V závere opisujeme preventívne projekty v tejto oblasti v Slovenskej republike.

Kľúčové slová: komunikácia, elektronická komunikácia, osobná komunikácia, prípady, prevencia.

Abstract: In the introduction we focus on the characterization of human communication and selected types of communication in terms of several classification features. We define the charateritics of personal and electronic communication. We also focus on several cases of misuse of electronic communication in terms of selected cases that were committed in the Slovak Republic. Finally,we describe preventive projects in this area in the Slovak Republic.

Key words: communication, electronic communication, personal communication, cases, prevention.

Úvod

V súčasnosti svet ponúka veľké množstvo spôsobov ako môžu ľudia medzi sebou komunikovať. Podstatou komunikácie je prenos rôznorodého informačného obsahu prostredníctvom jazyka a reči. Za základnú schému komunikácie je považovaný model, ktorý vypracoval americký politológ a teoretik komunikácie H.D. Lasswell tzv. Lasswellov model komunikácie (prípadne Lasawellov komunikačný model). Daný model opisuje akt komunikácie prostredníctvom definovania piatich prvkov. Prvým prvkom je definovanie osoby, ktorá oznámi určitú informáciu. Druhým prvkom je charakterizovanie informácie, ktorá bola povedaná. Tretím prvkom je vymedzenie akým komunikačným kanálom bola oznámená daná informácia. Štvrtým prvom je definovanie komu bola informácia povedaná a piatym prvkom je vymedzenie s akým účinkom bola informácia prijatá. Viacerí odborníci daný model považujú za jeden z prvých a zároveň z najvplyvnejších modelov sociálnej komunikácie. Na základe uvedeného môžeme povedať, že komunikáciou sa rozumie proces oznamovania, zmeny a distribúcie informácií medzi dvoma alebo viacerými ľuďmi v sociálnych vzťahoch a v rámci sociálneho správania.[48]

[48] HALADA, J. 2015. *Marketingová komunikace a public relations (výklad pojmů a teorie oboru*), s. 54.

K primárnym funkciám komunikovania môžeme zaradiť informovanie (odovzdanie správy, oznámenie informácie či vyhlásenie), inštruovanie (navedenie na niečo, naučenie niečo či zasvätenie do niečoho), presvedčenie (o zmene či pozmenení názoru na niečo, získanie niekoho na svoju stranu, ovplyvnenie či zmanipulovanie adresáta), vyjadrenie či dohodnutie sa (riešenie či vyriešenie určitého problému, dospetie k dohode), pobavenie (rozveselenie adresáta), kontaktovanie sa (zažitie blízkosti s osobou, sebapotvrdenie) či predvedenie sa (prezentovanie sa a vyvolanie dojmu).[49]

Odborná literatúra rozlišuje niekoľko foriem medziľudskej komunikácie, ktoré sa rozdeľujú podľa viacerých klasifikačných znakov. Prvým znakom je z hľadiska komunikačných prostriedkov. Na jeho základe sa komunikácia delí na verbálnu a neverbálnu. Verbálnou komunikáciou sa rozumie použitie slovnej komunikácie, ktorá sa uskutočňuje prostredníctvom jazyka, jazykových znakov a významov na nich viazanými a to prostredníctvom hovorenej a písanej reči. V ľudskej komunikácii práve verbálna komunikácia zohráva kľúčovú úlohu. Neverbálna (mimoslovná či nepojmová) komunikácia obsahuje všetky neslovné prejavy komunikácie ako napríklad mimika, kinezika, gestika, haptika, posturológia, proxemika, komunikácia prostredníctvom očí, komunikácia prostredníctvom telesných modifikácií a artefaktov spojených s ľudským telom, komunikácia kultúrnymi artefaktmi, komunikácia farbami, komunikácia čuchovými a chuťovými signálmi, symbolická komunikácia, obrazová komunikácia a pod. Druhým znakom je z hľadiska početnosti komunikujúcich subjektov. V tomto delení sa rozlišuje intrapersonálna komunikácia (vnútorná komunikácia - rozhovor so sebou samým), interpersonálna komunikácia (komunikácia medzi dvoma osobami), skupinová komunikácia (komunikácia medzi viac ako dvoma osobami), inštitucionálna komunikácia (komunikácia medzi záujmovými skupinami napríklad o mocenských a politických otázkach), verejná komunikácia (komunikácia oznamovaná a prenášaná k početným skupinám osôb), masová komunikácia (komunikácia zameraná na početné, anonymné, časovo a priestorovo rozptýlené publikum osôb s využitím informačných prostriedkov a médií). Tretím znakom je priamosť komunikácie, ktorú klasifikujeme na priamu komunikáciu (komunikácia v tvárou v tvár) a nepriamu komunikáciu (komunikáciu sprostredkovanú prostredníctvom rozličných prostriedkov). Štvrtým znakom je z hľadiska smerovania komunikácie a rozlišujeme jednostrannú komunikáciu (monológ osoby) a obojstrannú komunikáciu (dialóg medzi osobami). Piatym znakom je z hľadiska formálnosti. Na základe tohto rozlišovacieho znaku komunikáciu delíme na formálnu komunikáciu

[49] BYTEŠNÍKOVÁ, I. 2012. *Komunikace dětí předškolního věku*, s. 11.

(komunikácia nejakým spôsobom kontrolovaná či predpísaná) a neformálnu komunikáciu (komunikácia voľná bez pravidiel). Šiestym znakom je z hľadiska usmerňovania komunikácie a rozlišujeme riadenú komunikáciu (komunikácia ovplyvnená vôľou so stanoveným cieľom) a spontánnu komunikáciu (komunikácia neriadená vôľou a vyplýva z prirodzenej potreby sociálnej interakcie aktéra/ov).[50] Obsahovo sa zameriame iba na vybrané aspekty charakterizovanej komunikácie v predchádzajúcej časti príspevku.

Osobná a elektronická komunikácia. Prevencia javov vyplývajúcich z elektronickej komunikácie.

V komunikácii vystupujú viaceré prvky a to konkrétne komunikátor (osoba, ktorá oznamuje informácie adresátovi), adresát (osoba, ktorá prijíma oznamované informácie), komuniké (obsah oznamovanej informácie), komunikačný kanál (spôsob, akým je informácie oznamovaná), dekódovanie (pochopenie informácie, ktorú komunikátor oznámil), zakódovanie (premena informácie na vecnú podobu), komunikačný jazyk (sústava vyjadrovacích znakových prostriedkov), komunikačné prostredie (priestor, v ktorom komunikácia prebieha), kontext komunikácie (situácia, v ktorej sa komunikácia uskutočňuje) a spätná väzba (reakcia osoby na oznamovanú informáciu druhou osobou). Dané prvky sa vzájomne do väčšej či menšej miery ovplyvňujú v závislosti od formy a cesty medziľudskej komunikácie.

Cesty komunikácie môžme rozdeliť do šiestich druhov. Prvým druhom je písomná komunikácia, v ktorej sa informácie prenášajú vo forme písaného textu. Tento druh prebieha medzi komunikátorom a adresátom nekontaktnou formou. Z daného vyplýva, že ide o komunikáciu na diaľku a absentuje v nej neverbálna komunikácia. Druhým druhom je telefonická komunikácia, ktorá je čiastočne nepriama komunikácia. Taktiež v nej do istej miery absentuje neverbálna komunikácia, okrem paralingvistiky (napríklad sila hlasu, tón hlasu a pod.). Tretím druhom je osobná komunikácia, ktorá prebieha priamo medzi komunikátorom a adresátom. Daný druh v sebe spája verbálnu aj neverbálnu komunikáciu. Štvrtým druhom je elektronická komunikácia, ktorá je sprostredkovaná prostredníctvom elektronických médií (napríklad formou emailovej pošty, internetových stránok, diskusných fór na internete a pod.). Piatym druhom je audiovizuálna komunikácia, ktorá prebieha prostredníctvom médií (napríklad televízie, rozhlasu, novín, časopisov a pod.). Daný druh je jednosmerný a rozlišujeme písomnú audiovizuálnu komunikáciu, obrazovú audiovizuálnu komunikáciu

[50] URBAN, L., DUBSKÝ, J., MURDZA, K. 2011. *Masová komunikace a veřejné mínění,* s. 25 - 26, s. 30 - 31.

a sluchovú audiovizuálnu komunikáciu. Tento druh komunikácie je nekontaktnou formou. Šiestym druhom je sprostredkovaná komunikácia, ktorá je prenášaná prostredníctvom ďalšej osoby - sprostrekovateľa.[51]

Následne porovnáme a poukážeme na viaceré znaky, ktoré odlišujú osobnú komunikáciu od elektronickej komunikácie z hľadiska vymedzených prvkov, ktoré sa objavujú v priebehu komunikácie.

Prvým porovnávaným prvkom je komunikátor a adresát. V osobnej komunikácii je na prvý pohľad vidieť s akou osobou sa komunikuje, napríklad z hľadiska veku, pohlavia, výzoru a pod. V elektronickej komunikácii je výrazná anonymita užívateľov a z tohto dôvodu nie je možné spoľahlivo určiť s akou osobou sa komunikuje, aj keď sa osoba môže predstaviť, popísať, prípadne ukázať na webkamere. Negatívnosť anonymity počas elektronickej komunikácie môžeme vidieť aj na nasledujúcom reálnom prípade, v ktorom 54 ročná žena bola „*oslovená prostredníctvom sociálnej siete neznámym mužom, ktorý sa predstavil ako lekár pracujúci vo vojnovej zóne v Sýrii. Pod zámienkou, že ho chcú presťahovať do iného mesta si u nej chcel uchovať peniaze a dokumenty, ktoré jej mal zaslať poštou do úschovy. Pod zámienkou zaplatenia potrebných poplatkov týkajúcich sa balíka, mu žena zaslala na účet 53,850 eur. Po zaplatení tejto sumy ju „lekár" požiadal o ďalšie peniaze, ale následne žena začala mať podozrenie, že ide o podvod a kontaktovala políciu. Vyšetrovateľ začal v tomto prípade trestné stíhanie vo veci zločinu podvodu*."[52] Otázkou je či by daná žena takto jednoducho poskytla dané finančné prostriedky aj osobe, ak by ju oslovila s podobným príbehom počas osobnej komunikácie? Z nášho pohľadu práve daná anonymnosť elektronickej komunikácie poskytuje páchateľom výhodu, že jednoduchšie môžu páchať rôzne druhy podvodov aj súčasne na viacerých osobách.

Druhým porovnávaným prvkom je komunikačný kanál. V osobnej komunikácii si komunikátor a adresát priamo podávajú informácie o niečom. Daná skutočnosť sa následne odzrkadľuje aj v rýchlosti a priamosti spätnej väzby druhej osoby na danú informáciu. Pri osobnej komunikácii sa využíva vo vzťahu komunikátor a adresát aj sluchové, zrakové, hmatové a proxemické pôsobenie. Ich vplyv pôsobí aj na celkovú úroveň komunikácie a interakcie. V porovnaní s priamou komunikáciou elektronická komunikácia vkladá medzi komunikátora a adresáta „sprostredkovateľa" (napríklad sociálnu sieť, elektronickú poštu,

[51] HASANOVÁ, L., PORUBČANOVÁ, D., BILČÍK, A. 2020. *Vybrané kapitoly z pedagogickej komunikácie v odbornom vzdelávaní*, s. 40 - 41.
[52] Prevencia.kriminality. 2020. *Žena doplatila na svoju dôverčivosť. Emotívny príbeh podvodníka ju stál viac ako 50 000 eur.* [cit. 2022-03-22]. [online]. Dostupné na internete: https://m.facebook.com/prevenciakriminality/.

internetové komunikačné programy). Z čoho vyplýva, že táto komunikácia neumožňuje takú priamu spätnú väzbu ako osobná komunikácia. Vo vzťahu komunikátor a adresát je v elektronickej komunikácii využívané najčastejšie zrakové pôsobenie, aj keď pri grafike a videách je využívané aj sluchové a zrakové pôsobenie. V danom prípade interakcia osoby je oveľa pomalšia a oneskorenejšia ako v prípade priamej komunikácie a danú skutočnosť vnímame ako negatívny faktor elektronickej komunikácie. Taktiež pri elektronickej komunikácii absentuje aj priama emocionálna zložka.

Tretím a štvrtým porovnávaným prvkom je dekódovanie a zakódovanie. Nesprávne kódovanie a zakódovanie informácie môže rovnako prebiehať aj pri osobnej komunikácii, ako aj pri elektronickej komunikácii.

Piatym porovnávaným prvkom je komunikačný jazyk. V osobnej komunikácii sa prejavujú verbálne schopnosti komunikátora a adresáta. Negatívom osobnej komunikácie sú problémy s výstižným formulovaním myšlienok, alebo aj skákanie do reči či chybne interpretujúci význam slov. Taktiež sa môže objaviť aj chybne interpretovaná neverbálna komunikácia komunikátora a adresáta. V prípade elektronickej komunikácie môže dochádzať k nesprávnej interpretácii informácie alebo správy, aj napriek tomu, že osoby komunikujú rovnakým jazykom. Pri osobnej aj elektronickej komunikácii sa môže objaviť aj nevhodne zvolený slovník medzi komunikátorom a adresátom, ako napríklad používanie slangu, žargónu, ako aj vulgarizmov či moralizovanie alebo vyhrážanie sa osobe. V prípade elektronickej komunikácie sa môžu objaviť aj nenávistné prejavy a extrémizmus. Celoslovenský prieskum verejnej mienky zameraný na subjektívne vnímanie bezpečia obyvateľmi Slovenskej republiky poukázal na to, že „*dve tretiny respondentov sa na internete, sociálnych sieťach alebo on-line hráčskych platformách stretáva veľmi často, často alebo občas s násilným, zosmiešňujúcim alebo inak znevažujúcim obsahom. Mladší ľudia pritom citlivejšie vnímajú pocit ohrozenia extrémizmom, nárast nenávisti a nenávistných prejavov, a zároveň poznajú najviac jednotlivcov s extrémistickou motiváciou vo svojom okolí*.“[53] Na základe uvedeného môžeme vidieť aj prejavy ďalších sociálno-patologických javov, ktoré sa objavujú aj v elektronickej komunikácii.

Šiestym a siedmym porovnávaným prvkom je komunikačné prostredie a kontext komunikácie. V osobnej komunikácii je komunikátor a adresát priamo na spoločnom mieste a v reálnom čase. Komunikácia je medzi nimi synchronizovaná. V elektronickej komunikácii

[53] PREVENCIA KRIMINALITY, 2022. *Ohrození extrémizmom sa cítia predovšetkým mladší obyvatelia Slovenska*. [cit. 2022-05-11]. [online]. Dostupné na internete: https://prevenciakriminality.sk/clanok/3-extremizmus/274-ohrozeni-extremizmom-sa-citia-predovsetkym-mladsi-obyvatelia-slovenska.

je komunikátor a adresát od seba vzdialený nielen z hľadiska územia (priestoru), ale aj z hľadiska času, ktorý nemusí byť zhodný s reálnym časom. V danom prípade je vytvorená voľba načasovania odpovede, ktorú si osoba individuálne zvolí. V elektronickej komunikácii môže byť komunikácia synchronizovaná (napríklad v chate), ale taktiež aj asynchronálna, kedy si osoby informácie vymieňajú v rôznych časoch (napríklad v prípade e-mailovej komunikácie).[54] Osoby vystupujúce v elektronickej komunikácii sa nemusia nikdy v živote ani fyzicky stretnúť, ale napriek tomu, môžu spolu neustále komunikovať. Nevýhoda elektronickej komunikácie je neustála dostupnosť osoby. V elektronickej komunikácii sa môže objaviť aj nízka miera existencie reálnych medziľudských vzťahov a v častejších prípadoch dochádza k zneužitiu zistených informácií o osobe napríklad aj prostredníctvom uvedeným informácií na sociálnych sieťach danej osoby, alebo jej priateľov či rodinných príslušníkov. Taktiež dochádza k šíreniu nepravdivých, neúplných či zavádzajúcich informácií a správ. V rámci negatívnych javov vyskytujúcich sa v elektronickej komunikácii môžeme vidieť napríklad aj kyberšikanovanie, kybergrooming, kyberstalking a pod. K negatívam elektronickej komunikácie môžeme zaradiť aj reagovanie vlastným správaním na určité druhy výzviev na konanie určitého správania, ktoré nie sú priamo doručené či určené kontrétnej osobe, ale osoba sa s nimi dostane nepriamo do kontaktu napríklad keď si to prečíta danú informáciu, alebo ju vidí priamo na profile svojho priateľa či známeho. Takéto konanie sa vyskytlo v Slovenskej republike napríklad ako forme nebezpečnej internetovej výzvy, ktorá bola zaznamená v apríli 2022 - „*výzva nabádala deti a mladistvých na intoxikáciu voľne predajnými liekmi a zúčastnení mali zaznamenať priebeh intoxikácie a len v Bratislave sa počas daného mesiaca objavilo dvanásť prípadov otravy detí a mladistvých, ktoré pravdepodobne s touto výzvou súvisia*.“[55] Na danom prípade je vidieť, že práve maloleté a mladistvé osoby sú oveľa ľahšie ovplyvniteľné aj elektronickou komunikáciou ako dospelé osoby.

Ôsmym porovnávaným prvkom je spätná väzba. V elektronickej komunikácií sa môže pod vplyvom veľkého množstva správ určených adresátovi objaviť psychická únava či iné psychické problémy. Tatiež „*viaceré výskumy konštatujú, že počas interakcií vo virtuálnom prostredí majú užívatelia moderných informačných a komunikačných technológií zvýšené súkromné a znížené verejné uvedomenie. Okrem toho majú užívatelia komunikačných technológií tendenciu správať sa a reagovať sociálne menej žiaducim spôsobom vo virtuálnom prostredí v porovnaní s reálnym životom. Z toho vyplýva aj šírenie neprimeraného agresívneho*

[54] DeVito, A. J. 2008. *Základy mezilidské komunikace*, s. 40.
[55] PREVENCIA KRIMINALITY, 2022. *Rodičia, pozor na nebezpečnú internetovú výzvu.* [cit. 2022-05-01]. [online]. Dostupné na internete: https://www.facebook.com/prevenciakriminality/.

správania, čo vzhľadom na veľký počet používateľov súčasne, zvyšuje nebezpečnosť dôsledkov. Zlyhanie životného zmyslu prejavujúce sa agresívnym brojením voči druhým má vo virtuálnom prostredí vytvorenejšie priaznivejšie predpoklady ako v realite, navyše s menším rizikom potrestania. Efektívna kontrola je prakticky nemožná."[56] Podľa nášho názoru kontrolu môžeme najefektívnejšie vykonávať prostredníctom realizovania viacerých preventívnych aktivít.

Bezpečnosť elektronickej komunikácie sa v poslednom období stala kľúčovou prioritou v oblasti vypracovania preventívnych projektov najmä z dôvodu, že na internete hrozí viacero nástrah a to nielen pre neskúsené a vekovo nezrelé osoby, ale aj pre dospelé a skúsené osoby. Hlavným cieľom preventívnych aktivít je predchádzanie, aby sa maloleté a mladistvé osoby nestali obeťami a nebol narušený ich psychosociálny vývoj. Zároveň aby sa osoby všetkých vekových kategórií naučili či zvýšili si zručnosti na bezpečné používanie internetu ako nástroja na získavanie hodnoverných a využiteľných informácií vo svojich životoch a nenechali sa podvodnými spôsobmi oklamať. Taktiež aby pri týchto osobách nevznikali obavy vedúce ku následnému skresľovaniu pravdivých informácií pod vplyvom negatívnej skúsenosti z elektronickej komunikácie.

V Slovenskej republike sú realizované viaceré preventívne aktivity a následne sme vybrali tri, ktoré sú vypracované MV SR. Prvou preventívnou aktivitou je preventívna brožúra pod názvom „Nenávistné prejavy". Cieľom tejto preventívnej brožúry je predchádzať nenávistným prejavom a extrémizmu a ich páchaniu aj prostredníctvom internetu a sociálnych sietí. Daná brožúra sa skladá z viacerých častí. Prvá časť brožúry charakterizuje pojem - nenávistné prejavy. Druhá časť brožúry vymedzuje ciele a páchateľov nenávistných prejavov a poukazuje na slobodu prejavu. Tretia časť brožúry sa zameriava na osobnosť obete nenávistných prejavov. Štvrtá časť brožúry vymedzuje prevenciu týchto javov a to konkrétne prostredníctvom uvedenia kontaktov, ktoré poskytujú pomoc obetiam v jednotlivých krajoch v Slovenskej republike.[57]

Druhou preventívnou aktivitou je preventívna brožúra zameraná na kyberšikovanie a jej podoby v kyberpriestore. Daná brožúra charakterizuje pojem kyberšikanovanie, hlavné znaky kyberšikanovania, rozdiely medzi kyberšikanovaním a šikanovaním, ako aj najčastejšie podoby kyberšikanovania vyskytujúce sa v spoločnosti. Následne poukazuje na trestnoprávne hľadisko kyberšikanovania v Slovenskej republike. V preventívnej brožúre je charakterizovaná

[56] HAJDÚKOVÁ, T., BACIGÁL, I. 2015. *Ochrana detí vo virtuálnom prostredí*, s. 15.
[57] MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY, *Nenávistné prejavy*. [cit. 2022-05-03]. [online]. Dostupné na internete: https://www.minv.sk/?brozury-a-letaky.

aj obeť kyberšikanovania a ako aj rady ako sa nestať obeťou kyberšikanovania. Taktiež sú v nej uvedené aj kontakty na pomoc obetiam kyberšikanovania v Slovenskej republike.[58]

Treťou preventívnou aktvitou je aktívne poskytovanie rád prostredníctvom preventívnych aktitív zameraných na kyberšikanovanie a nástrahy internetového sveta. Realizácia je vo forme prednášok, besied a prezentácii preventívneho filmu. Cieľom preventívneho projektu je „*zvýšenie informovanosti a právneho vedomia maloletých, na úseku bezpečného používania moderných informačných a komunikačných technológií s dôrazom na riziká spojené s používaním internetu*.“[59]

Komunikácia je základnou súčasťou získavania informácií a pod ich vplyvom sa formuje individualita každého jedinca. V súčasnosti má komunikácia viacero aspektov, ktoré sa odrážajú aj v rizikách, ktoré z nej vyplývajú či sa jedná o osobnú alebo o elektronickú komunikáciu. Rozšírenie možností komunikácie so sebou prináša aj isté riziká, ktoré hrozia každému z nás, ale osobitne maloletým a mladistvým osobám. Na základe tohto predpokladu je potrebné realizovať a rozvíjať preventívne aktivity zamerané aj na túto oblasť pre široké spektrum adresátov preventívnych aktivít v Slovenskej republike ako aj v ostatných krajinách vo svete.

Zoznam použitej literatúry

BYTEŠNÍKOVÁ, I. 2012. *Komunikace dětí předškolního věku*. Praha: Grada Publishing, a.s., 2012, 236 s. ISBN 978-80-247-3008-0.

DeVito, A. J. 2008. *Základy mezilidské komunikace*. Praha: Grada Publishing, a.s., 2008, 512 s. ISBN 978-80-247-2018-0.

HALADA, J. 2015. *Marketingová komunikace a public relations (výklad pojmů a teorie oboru)*. Praha: Karolinum, 2015, 123 s. ISBN 978-80-246-3075-5.

HAJDÚKOVÁ, T., BACIGÁL, I. 2015. *Ochrana detí vo virtuálnom prostredí.* Bratislava: Akadémia Policajného zboru v Bratislave, 2015, 115 s. ISBN 978-80-8054-654-0.

HASANOVÁ, L., PORUBČANOVÁ, D., BILČÍK, A. 2020. *Vybrané kapitoly z pedagogickej komunikácie v odbornom vzdelávaní*. Dubnica nad Váhom: Vysoká škola DTI, 2020, 198 s. ISBN 978-80-8222-015-8.

[58] MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY, *Kyberšikanovanie*[cit. 2022-05-03]. [online]. Dostupné na internete: https://www.minv.sk/?brozury-a-letaky.

[59] MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY, *Preventívne projekty a aktvitiy pre deti a mládež.* [cit. 2022-05-05]. [online]. Dostupné na internete: https://www.minv.sk/?preventivne-projekty-a-aktivity-pre-deti-a-mladez.

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY, *Nenávistné prejavy*. [cit. 2022-05-03]. [online]. Dostupné na internete: https://www.minv.sk/?brozury-a-letaky

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY, *Kyberšikanovanie.* [cit. 2022-05-03]. [online]. Dostupné na internete: https://www.minv.sk/?brozury-a-letaky.

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY, *Preventívne projekty a aktvitiy pre deti a mládež.* [cit. 2022-05-05]. [online]. Dostupné na internete: https://www.minv.sk/?preventivne-projekty-a-aktivity-pre-deti-a-mladez.

PREVENCIA KRIMINALITY, 2022. *Ohrození extrémizmom sa cítia predovšetkým mladší obyvatelia Slovenska*. [cit. 2022-05-11]. [online]. Dostupné na internete: https://prevenciakriminality.sk/clanok/3-extremizmus/274-ohrozeni-extremizmom-sa-citia-predovsetkym-mladsi-obyvatelia-slovenska.

PREVENCIA KRIMINALITY, 2022. *Rodičia, pozor na nebezpečnú internetovú výzvu.* [cit. 2022-05-01]. [online]. Dostupné na internete: https://www.facebook.com/prevenciakriminality/.

Prevencia.kriminality. 2020. *Žena doplatila na svoju dôverčivosť. Emotívny príbeh podvodníka ju stál viac ako 50 000 eur.* [cit. 2022-03-22]. [online]. Dostupné na internete:.https://m.facebook.com/prevenciakriminality/.

URBAN, L., DUBSKÝ, J., MURDZA, K. 2011. *Masová komunikace a veřejné mínění*. Praha: Grada Publishing, 2011, 240 s. ISBN 978-80-247-3563-4.

Kontaktné údaje

Mgr. Michaela Kiššová, PhD.

Akadémia Policajného zboru v Bratislave

Sklabinská 1, 835 17 Bratislava

e-mail: michaela.kissova@akademiapz.sk

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

PhDr. Peter Veselý, PhD.

Vplyv kybernetickej kriminality na HDP

Lucia Klapáčová - Loretta Pinke - Peter Veselý

Abstrakt

Cieľom práce je posúdenie aspektov kybernetickej kriminality. V práci venujeme priestor histórii kybernetickej kriminality a jej definícii z právneho hľadiska. Definujeme kybernetickú kriminalitu a jej všeobecné aspekty v rámci informačnej spoločnosti a jej vplyv na ekonomiku krajiny. V závere práce uvádzame možné východiská a spôsoby, ako zabezpečiť efektívne vyšetrovanie tohto novodobého typu trestnej činnosti Pozornosť venujeme aj novým trendom a rozvíjajúcim sa druhom kybernetickej kriminality.

Kľúčové slová: kybernetická kriminalita, ekonomika, hrubý domáci produkt,

Kľúčové slová v anglickom jazyku: cybercrime, economy, gross domestic product

Úvod

Výpočtová technika prešla v posledných rokoch veľmi rýchlym vývojom, ktorý by len málokto dokázal predpovedať. Je súčasťou bežného života a využívajú ju ľudia všetkých vekových kategórií. Hrozba zneužívania tejto techniky súčasnosti na páchanie trestnej činnosti je aktuálnejšia ako kedykoľvek predtým. S rýchlym vývojom výpočtovej techniky súvisia aj otázky boja s rozvíjajúcou sa kyberkriminalitou a reflektovanie technologického vývoja právnymi poriadkami jednotlivých krajín. Z teoretického hľadiska sa zavádza množstvo nových pojmov, z pohľadu kriminalistiky zas možno badať profilovanie nového druhu páchateľov trestných činov a zvyšujúce sa požiadavky na kvalifikovanosť vyšetrovateľov. Táto téma je veľmi zaujímavá pre svoju spoločenskú aktuálnosť. Zároveň z právneho hľadiska môžeme vidieť veľké možnosti rozširovania právnej vedy v súvislosti s ďalším rozvojom výpočtovej techniky.

Vývoj kybernetickej kriminality

Nečakane rýchly vývoj počítačov a počítačových sietí bol zdrojom vzniku ďalších mnohých technológií, ktoré ľuďom čoraz viac uľahčovali komunikáciu. Len ťažko by sme mohli rýchly technologický vývoj komunikačných technológií za posledné rokx prirovnať k niečomu podobnému.

Štatistický úrad Slovenskej republiky uskutočňuje každý rok zisťovania o informačných a komunikačných technológiách (IKT) v podnikoch a domácnostiach. V roku 2006 sa podľa

prieskumu Štatistického úradu Slovenskej republiky[1] nachádzal aspoň jeden osobný počítač celkovo v 50,1 % všetkých domácností na Slovensku. Práve po tomto roku nastáva výrazný rast a v roku 2010 má podľa meraní Štatistického úradu Slovenskej republiky aspoň jeden osobný počítač 72,2 % všetkých domácností. Toto číslo však stále rastie, v roku 2012 má podľa rovnakej analýzy Štatistického úradu Slovenskej republiky aspoň jeden osobný počítač až 78,8 % z celkového počtu domácností.

Začína sa meniť aj celkový pohľad na duševné vlastníctvo. Veľmi často dochádza ku kopírovaniu obsahu, jeho kradnutiu a nedovolenému používaniu. Získava sa prospech z neoprávneného šírenia programov a to aj na bežnej používateľskej úrovni. Kým pred 15 rokmi bola bežná distribúcia softvéru len prostredníctvom diskiet a CD, dnes už prevažuje digitálna distribúcia programov, čím získavajú napríklad aj licenčné zmluvy programov novú podobu.

Spolu s technologickým vybavovaním domácností súvisí aj šírenie internetového pripojenia, ktoré pre málo skúseného používateľa môže predstavovať viacero hrozieb. Po roku 2000 zažíva internet prvé výrazne rozširovanie, na Slovensku sa zároveň objavuje stále viac poskytovateľov pripojenia. Od roku 2004 začína výrazný nárast domácností s pripojením na internet. V roku 2012 už má už pripojenie na internet viac než tri štvrtiny všetkých domácností.[2] Najmarkantnejší nárast počtu pripojení môžeme sledovať práve v rokoch 2006, 2007 a 2008. Na štatistických údajov zároveň vidno, že ľudia začali internet považovať za bežnú súčasť života a zároveň počítač bez aktívneho pripojenia na internet už je v domácnostiach skôr raritou.[3]

Bolo by však povrchné brať internet iba ako jeden zo spôsobov komunikácie či prostriedkov zábavy. Stále častejšie na internete dochádza k uzatváraniu zmlúv na diaľku, vykonávaniu právnych úkonov. Internet už dávno nie je anonymným miestom pre pár nadšencov. Práve tieto aspekty sú dôvodom vzniku nových právnych predpisov reflektujúcich rýchly technologický vývoj a rozvoj počítačového práva na Slovensku.

[1] Štatistický úrad Slovenskej republiky. [online]. [cit.12.5.2022]. Dostupné na internete: <portal.statistics.sk/files/Sekcie/sek...IKT/publikacia_ikt_sr_2012.pdf>.
[2] Štatistický úrad Slovenskej republiky. [online]. [cit.12.5.2022]. Dostupné na internete: <portal.statistics.sk/files/Sekcie/sek...IKT/publikacia_ikt_sr_2012.pdf>
[3] Štatistický úrad Slovenskej republiky. [online]. [cit.12.5.2022]. Dostupné na internete: <portal.statistics.sk/files/Sekcie/sek...IKT/publikacia_ikt_sr_2012.pdf>

Právne zmeny v súvislosti s kybernetickou kriminalitou

Po roku 2000 zaznamenávame v slovenskom právnom poriadku viacero zmien, ktoré sa týkajú rozličných úprav v súvislosti s rozširujúcim sa využívaním výpočtovej techniky. Jedným z najzásadnejších bol v tomto ohľade zákon č. 618/2003 Z. z. o autorskom práve s účinnosťou od 1. januára 2004, v ktorom nájdeme úpravu ochrany počítačového programu ako výsledku tvorivej duševnej činnosti programátora. Okrem toho prináša tento zákon vymedzenie pojmu „počítačový program“, pričom pod tento pojem môžeme subsumovať aj samotné podklady a materiály potrebné na prípravu programu.[4]

Nemalú súvislosť s počítačovou kriminalitou a autorským právom nájdeme aj priamo v Trestnom zákone v § 283 Porušenie autorského práva. Objektom trestného činu sú v tomto prípade diela, na ktoré sa vzťahujú autorské práva a ktoré sú chránené pred neoprávnením nakladaním s nimi. Takéto ustanovenie sa samozrejme vzťahuje aj na počítačové programy a databázy.[5]

Rozširovanie platieb prostredníctvom platobných kariet predstavovalo ešte v 90. rokoch minulého storočia veľkú zmenu v platení, no zároveň bolo vidieť aj pomerne veľkú nedôverčivosť ľudí voči tomuto spôsobu platenia. V súčasnosti to už však neplatí. S postupným technologickým vývojom a vývojom ochranných prvkov sa však vyvíjala aj technologická úroveň páchateľov trestných činov súvisiacich s falšovaním a zneužívaním tohto platobného prostriedku. Na vývoj v tejto oblasti reflektuje § 219 Trestného zákona – Neoprávnené vyrobenie a používanie platobného prostriedku, elektronických peňazí alebo inej platobnej karty.

Napriek značnému rozvoju v oblasti výpočtovej techniky nie je v žiadnom našom právnom predpise presne vymedzený pojem „Počítačová kriminalita“. Tento výraz však možno vnímať veľmi široko a je otázne, či by to vzhľadom k stále veľmi rýchlemu technologickému vývoju bolo vôbec účelné. V súčasnosti môžeme v jednotlivých zákonoch nachádzať viacero spomínaných ustanovení vzťahujúcich sa na činy, ktoré môžeme jednoznačne označiť za kyberkriminalitu.

[4] Zákon č. 618/2003 Z. z. o autorskom práve
[5] Zákon č. 300/2005 Z. z. v znení neskorších predpisov

Spôsoby na efektívne zabezpečenie vyšetrenia novodobého typu tresnej činnosti

Jedným z najdôležitejších právnych aktov z pohľadu medzinárodného práva je Dohovor o počítačovej kriminalite otvorený na podpis v Budapešti 23. novembra 2001. Slovenskou republikou bol dohovor ratifikovaný v roku 2007 a platnosť nadobudol 1. mája 2008.

Jedným z hlavných cieľov Dohovoru o počítačovej kriminalite je spoločné hľadanie možností boja proti kybernetickej trestnej činnosti, uznáva zároveň, že pre účinný boj proti počítačovej kriminalite je mimoriadne dôležitá rýchly a spoľahlivá medzinárodná spolupráca a zároveň spolupráca so súkromným sektorom. Dohovor obsahuje základné vymedzenie pojmov súvisiacich s počítačovými systémami, údajmi a poskytovateľmi služieb. Zároveň sú v Dohovore uvedené jednotlivé trestné činy, ich hmotnoprávne hľadisko a opatrenia, ktoré je potrebné prijať na vnútroštátnej úrovni.

Dohovor sa stal dôležitým rámcom pre ďalšie úpravy vnútroštátnych poriadkov, určil jednoznačné ciele a niekoľko opatrení, ktoré na medzinárodnej úrovni pomáhajú potláčať počítačovú kriminalitu. Dohovor Rady Európy o počítačovej kriminalite sa stal zároveň podkladom aj pre právne zmeny na Slovensku, ktoré sa prejavili predovšetkým ustanoveniami Trestného zákona č. 300/2005 Z. z.[6]

Hrozby

Za jeden z najzásadnejších problémov kyberkriminality je považované samotné definovanie základných hrozieb. Všeobecne by sme mohli povedať, že objektom kybernetického útoku býva spravidla hardvér, softvér, dáta a osoby spracujúce informačné systémy. V súčasnosti sa medzi veľmi časté hrozby zaraďuje aj krádež identity osoby a jej zneužitie, či vážne porušenie súkromia osôb, sledovanie a neoprávnené zhromažďovanie údajov. Viac ako kedykoľvek predtým sú ohrození bežní používatelia internetu a počítačov.

Útoky smerované voči informačným systémom sa môžu prejaviť rôznymi spôsobmi. V tých lepších prípadoch ide o menšie nepríjemnosti pre užívateľov v podobe pomalšieho prístupu k údajom, či krátkodobých výpadkov. V horších prípadoch môžeme hovoriť o dlhodobých výpadkoch dôležitých systémov, či krádeži citlivých údajov, pričom v prípade rozsiahleho a úspešného útoku možno hovoriť aj o značných finančných škodách. Medzi základné hrozby mierené proti informačným systémom môžeme zaradiť: únik informácií, narušenie integrity,

[6] Dohovor o počítačovej kriminalite otvorený na podpis 23.11.2001 v Budapešti [cit.13.5.2022]. Dostupné na internete: < http://www.ucps.sk/Dohovor_o_pocitacovej_kriminalite>

nelegitímne použitie služby (neadekvátnym spôsobom alebo neoprávnenou osobou), zabránenie prístupu ku službe.

V tomto prípade teda vystupuje otázka adekvátneho zabezpečenia informačných systémov, ktoré predstavuje celý komplex rôznych bezpečnostných a preventívnych opatrení. V tejto súvislosti však treba pripomenúť, že účinné zabezpečenie býva finančne nákladnou záležitosťou bez okamžite viditeľného efektu. Bezpečnosť systémov býva pomerne často zo strany správcov podceňovaná. Spolu s uvedomením si týchto hrozieb je potrebné myslieť aj na to, že cena chránených dát nemusí byť rovnaká pre ich vlastníka a pre útočníka. Pri určovaní bezpečnostných štandardov je preto dobré uvedomiť si hodnotu chránených aktív. Na druhej strane, absolútnu bezpečnosť informačných systémov je prakticky nemožné dosiahnuť.[7]

Ďalší zo základných problémov kybernetických trestných činov je ich legislatívne vyjadrenie a spôsoby. Ako sme už spomínali v predchádzajúcich častiach, základným problémom je už samotná definícia kyberkriminality. Tento typ trestnej činnosti prechádza ešte stále mimoriadne rýchlym vývojom a preto nie je celkom možné kyberkriminalitu presne charakterizovať a vymedziť. Vzhľadom k extrémne rýchlemu vývoju, platné právne normy nie sú schopné tieto činy taxatívne vymedziť, čo vyúsťuje do celej rady problémov v aplikačnej praxi. Stretávame sa najmä s problémami vyplývajúcimi z vágnosti samotných ustanovení. Jedným z mála možných účinných riešení sa ukazuje využívanie analógie, teda aplikovania právnych noriem na delikty podľa podobných charakteristík.

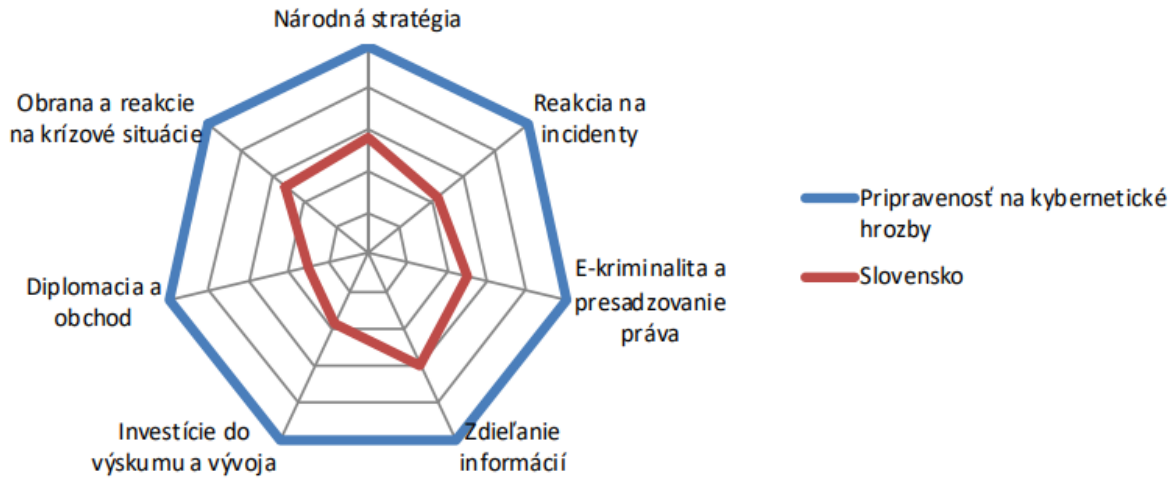
Slovensko a kybernetická bezpečnosť

Na Slovensku za kybernetickú bezpečnosť a priority týkajúce sa schopnosti krajiny odolávať kybernetickým hrozbám zodpovedá Národný bezpečnostný úrad. Vojenské spravodajstvo Slovenskej republiky prevezme zodpovednosti v prípade vážneho celonárodného kybernetického incidentu a bude reagovať s použitím technických prostriedkov Centra pre kybernetickú obranu.

Index pripravenosti na kybernetické hrozby (Cyber Readiness Index – CRI) bol použitý na vyhodnotenie aktuálnej úrovne pripravenosti Slovenska na kybernetické riziká. Poskytuje

[7] Jirovský, V. Kybernetická kriminalita: *Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. - 1. vyd. - Praha: GRADA Publishing, 2007 str. 21 ISBN 978-80-247-1561-2

informácie využiteľné v praxi, na základe ktorých môže Slovensko vyhodnotiť svoju pripravenosť na zaplnenie prázdneho miesta medzi svojou aktuálnou pozíciou v oblasti kybernetickej bezpečnosti a technickými prostriedkami na národnej úrovni potrebnými na podporu digitálnej budúcnosti.



Obrázok 3 Hodnotenie pripravenosti Slovenskej republiky na kybernetické hrozby[8]

Kybernetická kriminalita a jej vplyv na ekonomiku

Kybernetický kriminalita zasahuje výrazne do ekonomík jednotlivých krajín. Rok 2020 bol poznamenaný pandémiou Covid-19. Zločinci využili pandémiu na spustenie podvodov a phishingových útokov na sociálnych médiách, lekárskych a výskumných inštitúciách.

Spoločnosť McAfee vyhlásila, že v roku 2020 zaznamenala incidenty v oblasti počítačovej kriminality, ktoré mohli stáť ekonomiku takmer 1 bilión amerických dolárov. Pre porovnanie, v roku 2018 náklady spojené s kybernetickou kriminalitou predstavovali 600 miliárd dolárov. Spoločnosť tiež uviedla, že ročné náklady na počítačovú kriminalitu predstavujú viac ako 1 % celosvetového hrubého domáceho produktu.[9]

[8] Hathaway, M: Slovenská republika kybernetická pripravenosť v kocke.[cit.20.5.2022]. Dostupné na internete: < https://www.globsec.org/wp-content/uploads/2019/04/CRI_Slovakia_SK.pdf>

[9] Saroha, A: *The year that lost 1% of global GDP to cybercrime*. [cit.20.5.2022]. Dostupné na internete: < https://www.thehindu.com/sci-tech/technology/the-year-that-lost-1-of-global-gdp-to-cybercrime/article33430555.ece>

Ďalší z negatívnych vplyvov kybernetickej kriminality nachádzame v kryptomenách. Analýza spoločnosti Elliptic, ktorá sa zaoberá dodržiavaním kryptomien, ukázala, že podvodníci dostali v roku 2020 viac ako 400 platieb v bitcoinoch v celkovej hodnote 121 000 dolárov.[10]

Aká je teda budúcnosť kybernetickej kriminality ? Podľa najnovších odhadov v roku 2025 dosiahnu globálne náklady na počítačovú kriminalitu výšku takmer 10,5 bilióna amerických dolárov, čo predstavuje nárast o 15 % ročne.[11]

Téma využívania výpočtovej techniky na páchanie trestnej činnosti je veľmi rôznorodá a prináša množstvo aspektov, na ktoré spoločnosť ešte nedokáže adekvátne reagovať. Uplatňovaním nových zásad prispôsobených dynamike technologického vývoja uľahčí byť boj proti kybernetickej kriminalite.

Záver

Pojem kybernetická kriminalita môže byť predmetom veľmi širokého výkladu rôznych činností, ktoré prebiehajú buď v kybernetickom priestore, alebo činností, pri ktorých prostriedky výpočtovej techniky zohrávajú nezastupiteľnú úlohu. Aj keď tento pojem nemá presné vymedzenie, za posledné roky prichádza k zaujímavému posunu od zaužívaného pojmu "počítačová kriminalita" k pojmu "kybernetická kriminalita". Práve pod druhý, a v súčasnosti používanejší pojem, môžeme zaradiť rozličné skutky páchané predovšetkým v rámci internetu a iných sietí, či infraštruktúr. Rýchlo napredujúci vývoj prináša nové trendy a narastá tak tlak na medzinárodné spolupráce vzhľadom na charakter súvisiacich problémov.

Zoznam použitej literatúry

Štatistický úrad Slovenskej republiky.[online].[cit.12.5.2022].Dostupné na internete: <portal.statistics.sk/files/Sekcie/sek...IKT/publikacia_ikt_sr_2012.pdf>

Zákon č. 618/2003 Z. z. o autorskom práve

[10] Saroha, A: *The year that lost 1% of global GDP to cybercrime*. [cit.20.5.2022]. Dostupné na internete: < https://www.thehindu.com/sci-tech/technology/the-year-that-lost-1-of-global-gdp-to-cybercrime/article33430555.ece>

[11] Calif, S.: Cybercrime to cost the world $10.5 Trillion Annually By 2025. [cit.20.5.2022]. Dostupné na internete: < https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

Zákon č. 300/2005 Z. z. v znení neskorších predpisov

Dohovor o počítačovej kriminalite otvorený na podpis 23.11.2001 v Budapešti [cit.13.5.2022]. Dostupné na internete: < http://www.ucps.sk/Dohovor_o_pocitacovej_kriminalite>

Jirovský, V. Kybernetická kriminalita: *Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. - 1. vyd. - Praha: GRADA Publishing, 2007 str. 21 ISBN 978-80-247-1561-2

Hathaway, M: Slovenská republika kybernetická pripravenosť v kocke.[cit.20.5.2022]. Dostupné na internete: < https://www.globsec.org/wp-content/uploads/2019/04/CRI_Slovakia_SK.pdf>

Saroha, A: *The year that lost 1% of global GDP to cybercrime*. [cit.20.5.2022]. Dostupné na internete: < https://www.thehindu.com/sci-tech/technology/the-year-that-lost-1-of-global-gdp-to-cybercrime/article33430555.ece>

Calif, S.: Cybercrime to cost the world $10.5 Trillion Annually By 2025. [cit.20.5.2022]. Dostupné na internete: < https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

doc. RNDr. Tatiana Hajdúková, PhD.

Digitální identifikace vozidla v současné kriminalistice a forenzních vědách

Dagmar Kopencová - Roman Rak - Vladimíra Hudecová

Abstrakt: *Individuální identifikace objektu je výchozím nebo konečným stavem každé forenzní analýzy či dokumentace. Příspěvek se zaměřuje ve své první části na základní a doplňkové zásady forenzní identifikace objektů. Jsou popsány 4 základní a 2 doplňkové zásady. Ve druhé části se příspěvek zaměřuje na individuální identifikaci vozidla. Zásadní akcent je dán na nový způsob určení identity vozidla pomocí digitálně uloženého VIN (Vehicle Identification Number) do různých elektronických komponent moderního vozidla. Je popsán způsob, jak pomocí tzv. „VIN čtečky" lze jednotným způsobem u automobilů různých továrních značek vyčítat VIN nebo další objektové identifikátory z významných komponent vozidla, u kterých jsou digitálně ukládána rozmanitá data. Příspěvek seznamuje čtenáře s novou metodou identifikace vozidla, pomocí které lze nalézt odcizená vozidla, neodborně zaměněné klíčové komponenty vozidla, které mohou pocházet i z trestné činnosti.*

Klíčová slova: *Vozidlo, digitální data, identifikace, forenzní, kriminalistika.*

Abstract: *Individual object identification is the initial or final state of any forensic analysis or documentation. In its first part, the paper focuses on the basic and supplementary principles of forensic identification of objects. 4 basic and 2 supplementary principles are described. In the second part, the paper focuses on individual vehicle identification. The main emphasis is on a new way of determining the identity of a vehicle using a digitally stored VIN (Vehicle Identification Number) in various electronic components of a modern vehicle. It describes how to use the so-called "VIN reader" to read VIN or other object identifiers from important vehicle components, in which various data are digitally stored, in a uniform way for cars of various brands. The article acquaints the reader with a new method of vehicle identification, which can be used to find stolen vehicles, unprofessionally confused key components of the vehicle, which can also come from crime.*

Keywords: *Vehicle, digital data, identification, forensic, criminalistics.*

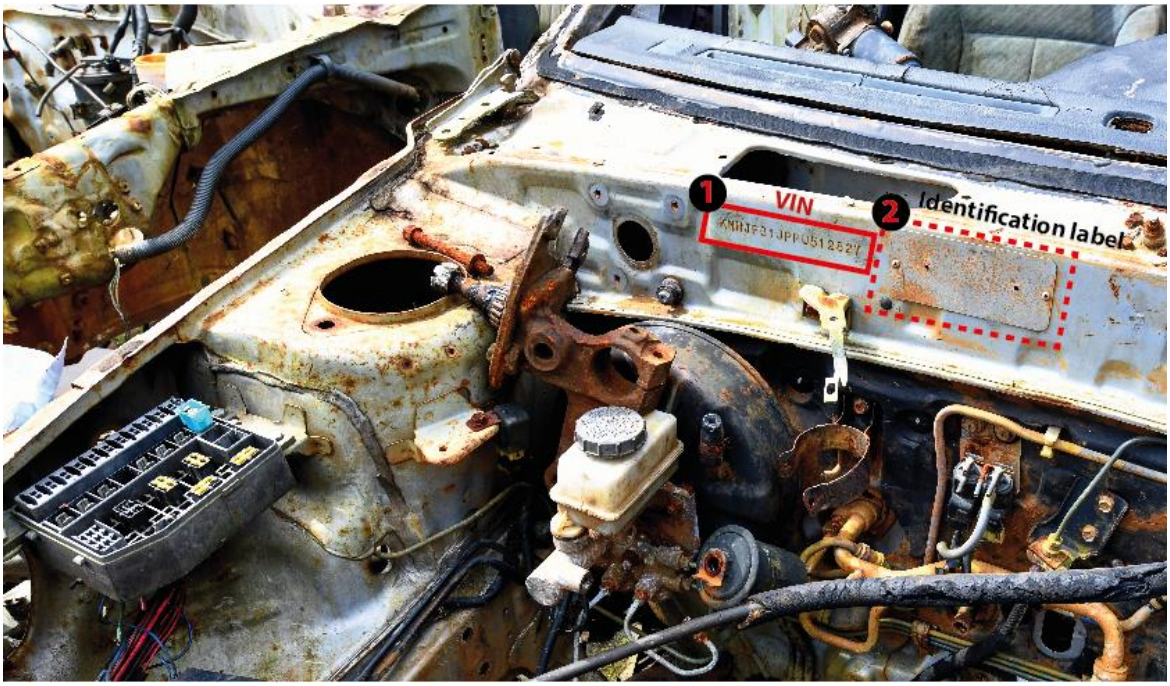
Úvod

Pro možnost využití individuální identifikace jakýchkoliv objektů (osob, živých i neživých objektů, artefaktů, které vytvořila příroda nebo člověk) ve forenzních disciplínách (včetně kriminalistiky) potřebujeme naplnit několik teoretických i ryze praktických základních zásad. Jedná se o zásady nezbytně nutné a zásady doplňkové [16].

Zásady nezbytně nutné:

1) **Identifikační charakteristiky** (vlastnosti) předmětného objektu musí být v určitém zkoumaném prostoru **jedinečné, unikátní**. V době celosvětové globalizace je zkoumaným prostorem celá planeta země, tj. objekt musí mít takové charakteristiky, které zajistí jeho celosvětovou jedinečnost, unikátnost, neopakovatelnost [6].

2) **Identifikační charakteristiky** objektu musí být **relativně neměnné**. Mohou se tedy v určitém rozsahu měnit, ale nesmí být porušena předchozí zásada. Změny jsou tedy malé, pro identifikační proces, zaručující jednoznačnou, unikátní shodu mezi srovnávanými objekty, nepodstatné. Otisk prstu malého dítěte i téhož dospělého člověka má sice jiné rozměry, ale identifikační znaky (tzv. markanty) jsou neměnné. Relativní neměnnost lze vysvětlit i jako určitou stálost, neměnnost v čase.
3) **Identifikační charakteristiky** musí být **od** daného **objektu neoddělitelné**, tj. musí být jeho nerozlučnou částí. Jinými slovy, pokud nějaký objekt např. označíme ve výrobním procesu určitým unikátním identifikačním, výrobním číslem, tento identifikátor musí být jeho přirozenou součástí. Pokud např. identifikátor vyrazíme do kovu karosérie vozidla, do dílu či části, nelze jej nijak dále oddělit. Pokud identifikátor ale vyhotovíme v podobě určitého štítku (kovového, plastového či papírového), tento identifikátor je od svého s ním spojeného objektu oddělitelný, poškoditelný či zničitelný (provozem objektu v době jeho životnosti), požárem, působením různých látek prostředí nebo účelovým zájmem identifikátor zničit či vyměnit za jiný. Zásada číslo 3 je logicky spojená se zásadou č. 2 a dále ji doplňuje. Identifikátor v podobě štítku nebo nálepky je sice jedinečný, unikátní a relativně neměnný (zásada č. 1 a 2), ale pokud jej od identifikovaného objektu oddělíme, objekt tyto identifikační charakteristiky okamžitě ztratí, tj. nelze jej identifikovat. Zásada č. 3 je důležitá pro identifikaci přírodních objektů i objektů vytvořených člověkem (tzv. artefaktů).
4) **Identifikační charakteristiky** musí být **technologicky zpracovatelné, vyhodnotitelné**. Musí tedy existovat určité procesy, metodiky, nástroje, poznatkové fondy apod., abychom identifikační charakteristiky dokázaly vůbec nalézt, „zviditelnit“ pro smyslové orgány člověka, zpracovat, analyzovat, dokumentovat a vyhodnotit. Ideálně ještě takovým způsobem, aby tento proces byl v čase opakovatelný se stejným výsledkem. Identifikace na základě DNA nebyla ještě nedávno možná, protože nebyly známé identifikační charakteristiky, tedy podstata celého identifikačního procesu. Jakmile tento fakt byl teoreticky zvládnut, čekalo se ještě na samotnou technologii pro praktické vyhodnocení a srovnání biologických vzorků obsahujících DNA.



Obr. 1 Ukázka rozdílu časové neměnnosti identifikátoru VIN[12] vozidla. (1) – primární identifikace a hliníkového homologačního štítku (2) - sekundární identifikace. Hliníkový materiál v agresivních klimatických podmínkách velice rychle koroduje a ztrácí svůj identifikační obsah. Autor: Roman Rak

Výše uvedené zásady nezbytně nutné jsou důležité pro forenzní identifikaci, která je základem každého začátku forenzního zkoumání [4, 10]. Zde v mnoha případech nezáleží až tak na rychlosti a nákladech na zpracování (byť v praxi stále usilujeme o vylepšení uvedených dvou faktorů). Důležitá je ale především skutečnost naplnění právní podstaty procesu a spravedlivosti, tj. například při objasňování vraždy nebo jiné závažné trestné činnosti je společnost vždy ochotna vynaložit i nemalé prostředky pro zajištění práva a spravedlnosti.

Pokud ale identifikace objektů (osob, živých neživých výtvorů přírody, lidské výtvory – různé artefakty) má sloužit pro preventivní účely, zamezení nebo podstatné omezené určitého typu kriminality, je potřeba kontrolovat pomocí identifikace velké množství objektů v rozsáhlém prostoru a v krátkém čase. V těchto případech je pak opodstatněné definovat další **dvě doplňkové zásady** pro identifikační procesy. Identifikační charakteristiky musí být „průmyslově“, technologicky zpracovatelné s následujícími **doplňkovými zásadami:**

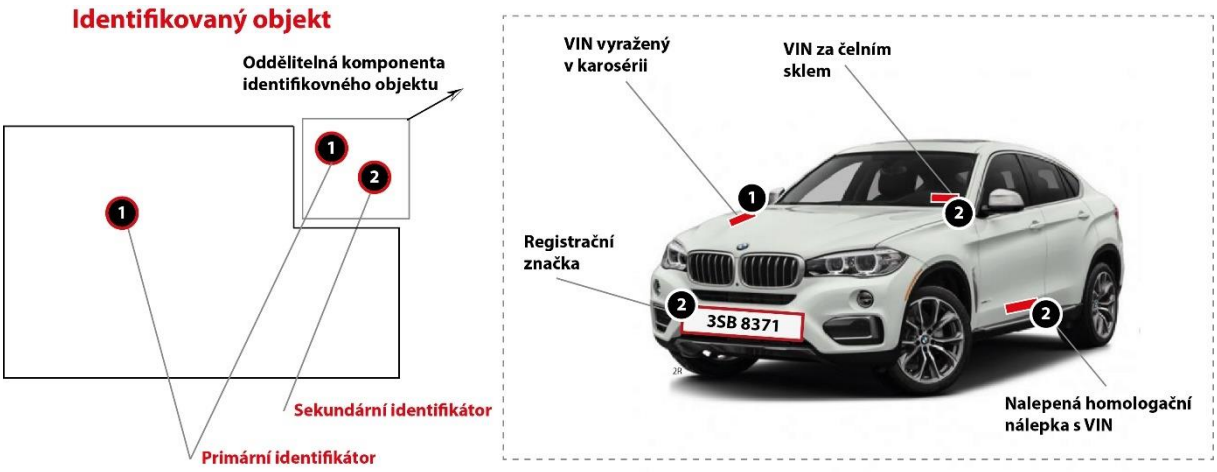
5) **Identifikační charakteristiky** musí být **zpracovatelné veřejně dostupnými technologiemi**, které jsou pro danou oblast průmyslově, informačně **standardizované**

[12] VIN – Vehicle Identification Number

v mezinárodním měřítku. Pro digitální vyčtení VIN z řídících jednotek by mělo být použitelné standardní zařízení, rozhraní, které je využitelné pro všechny modely vozidel všech továrních značek od určitého data výroby či ustanovení platnosti identifikačních kontrol. V současnosti každý výrobce v oblasti digitální identity vozidla používá jiné, často odlišné standardy a je nutné pořídit proprietární systém pro jejich forenzní či jiné zpracování. V praxi není pak možné pro preventivní účely provozovat desítky či stovky technologií, používaných různými výrobci vozidel. Takovýto přístup je prostorově, časově, metodicky a finančně náročný.

6) **Identifikační charakteristiky** musí být **zpracovatelné automaticky, v reálném čase, s minimálním podílem lidského faktoru,** s možností objektivní kontroly tzv. „čtyř očí“. Jedině tak je možné zajistit objektivnost, rychlost a nezávislost celého procesu.

U přírodních objektů (lidé, zvířata, rostliny atd.) je jednoznačná, unikátní a primární identita daná v zásadě především jejich přírodním, nativním původem, tj. biologickými vlastnostmi (otisk prstů, DNA, pach, vzhled tváře atd.).



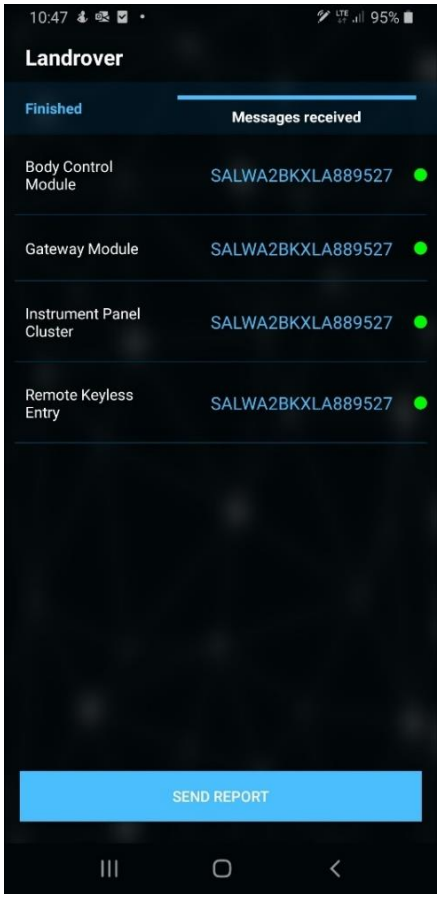
Obr. 2 Primární a sekundární identifikace vozidla. Autor: Roman Rak

Unikátní, jednoznačné identifikátory můžeme rozdělovat na **primární unikátní identifikátory** a **sekundární unikátní identifikátory** [15].

Primární unikátní identifikátory vznikají zpravidla při zrodu (narození/vytvoření) živého nebo neživého přírodního objektu nebo vytvoření umělého objektu člověkem (tj. vytvoření artefaktu).

- **Primární unikátní identifikátory** jsou časově relativně neměnné a s objektem trvale spojeny a i v případě, že od objektu je oddělena jeho část, tato část je obvykle v ideálním případě schopná identifikovat původní objekt. Příkladem může být DNA, pach apod. Primární unikátní identifikátory nalezneme vždy u všech objektů stejné kategorie po celém světě (tj. všechny osoby mají DNA, otisk prstu, svou tvář, vozidla vyrobená po roce 1986 VIN - *Vehicle Identification Number*).
- **Sekundární unikátní identifikátory** vznikají v průběhu určitého procesu, v průběhu „života" objektu. Jsou sice individuální, ale nemusí být vždy nalezeny u všech objektů dané kategorie. Pokud osoby mají např. unikátní, jednoznačné tetování, unikátní vlastnosti chrupu po ošetření dentistou apod., neznamená to ale automaticky, že to platí pro všechny lidi na planetě Země. Sekundární identifikátory pomáhají jednoznačné identifikaci v případě, že existují; nazývají se často pomocnými unikátními identifikátory. Protože sekundární identifikátory často vznikají dodatečně, člověk jimi označuje různé vytvořené umělé artefakty, nemusí být zaručeno jejich trvalé spojení s objektem od samého začátku až po konec jeho existence. Sekundární identifikátory mohou být z objektu určitými technologiemi odstranitelné.

U artefaktů se v praxi spíše používá sekundární identifikace, která je uměle vytvořená člověkem – zejména různá výrobní, evidenční, administrativní, úřední čísla apod. Mohou mít podobu papíru ale i počítačových čipů. Ale i artefakty mají vlastnosti, které jsou dány primárně v procesu jejich výroby (tedy zrodu) – určitá napětí v materiálu, specifické materiálové složení či charakteristiky atd. Pokud tyto vlastnosti artefaktů jsou trvalé a relativně neměnné a mají charakter unikátních identifikátorů, lze je využít jako primární unikátní identifikátory.



***Obr.** 3 Vlevo: Detail umístění OBD[13] konektoru se zasunutou čtecí jednotkou VIN pro odečítání identifikátoru VIN z jednotlivých komponent vozidla. Vpravo: seznam vyčtených identifikátorů VIN z různých komponent vozidla. Pokud s vozidlem nebylo po technické stránce manipulovány, identifikátor VIN musí být ve všech vozidlových komponentách shodný. V opačném přístupu se může jednat o případy, kdy do vozidla byl neautorizovaně namontován díl z jiného vozidla, které mohlo pocházet i z trestné činnosti (krádeže vozidla na náhradní díly apod.). Zelená tečka označuje, že identifikátor VIN není v pátrání a komponenta tedy nepochází z vozidla pochybného původu. Autor: Roman Rak*

Digitální VIN a další identifikátory

Pro identifikaci vozidla dle mezinárodně platných standardů se používá VIN – **Vehicle Identification Number**. Tento identifikátor se dle standardu fyzicky razí do neoddělitelné části vozidla – do karosérie nebo do rámu vozidla specifickým fontem a technologií konkrétního

[13] OBD – On Board Diagnostic

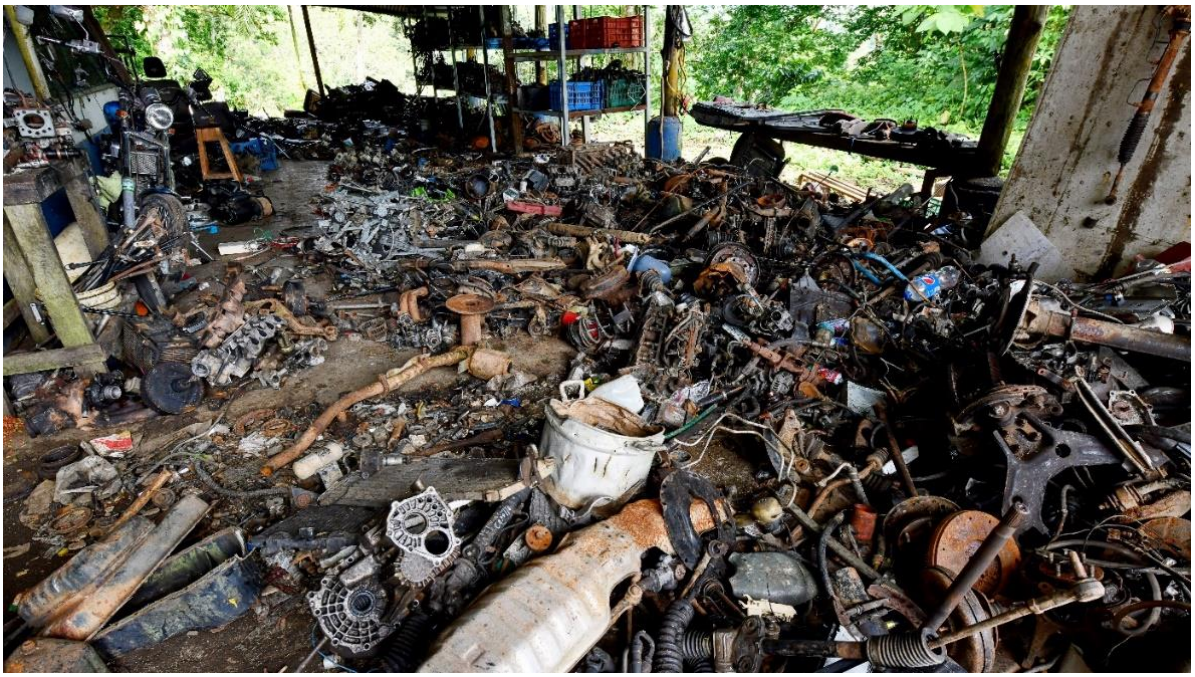
výrobce. Jedná se o primární identifikaci podle prvních tří výše uvedených zásad. Kromě toho se vozidlo označuje dle mezinárodních standardů tzv. homologačními štítky z různých materiálů (kov, plast, plastová nálepka, papír) a s různými způsoby připevněná štítku k vozidlu. Jedná se o sekundární, administrativní identifikací vozidla. Štítky obsahují sice u drahých vozidel sofistikované ochranné znaky, ale štítky jsou v podstatě oddělitelné od vozidla a pokud by identifikace vozidla byla založena pouze na nich, v případě zájmu pachatele trestné činnosti s vozidlem jsou lehce odstranitelné a tedy identifikace bude nespolehlivá.

Výše uvedené způsoby lze označit za mechanické technologie. Současná doba ale umožňuje ukládat identifikátor VIN vozidla v elektronické podobě do různých komponent vozidla. Digitální VIN se používá minimálně posledních deset let a neustále jej jednotliví výrobci zdokonalují. Tato skutečnost je velmi pozitivní, protože se jedná o další způsob zajištění identity vozidla a její technologické, automatizované zpracování. Negativní moment je ta skutečnost, že není nikterak systémově řešena skutečnost, jak tento VIN z vodidel efektivně vyčítat, aby byly naplněny výše uvedené zásady č. 5 a č. 6.

Obr. 4 Ukázková situace, kde je nutná identifikace vozidla pro nalezení vozidel či náhradních dílů pocházejících z trestné činnosti. Autor: Roman Rak

Neexistuje žádná obecná norma, jak a kam digitální VIN do vozidla ukládat, aby to bylo povinné pro všechny výrobce a vozidla byla označována standardizovaným způsobem. Abychom mohli vyčítat digitální VIN z vozidla, musíme dnes vlastnit několik rozdílných

zařízení od různých výrobců, které zpravidla pokrývají jen výrobce určitých koncernů, uskupení – jinak musíme postupovat u vozidel japonských, asijských, amerických, evropských (koncern VW, BMW apod.) apod. [2]. Toto v praxi přináší problémy finanční, spojené s nákupem nestandardizovaných technologií, které jsou rozdílné, metodické – spojené s používáním jednotek schopných vyčítat VIN (obsluha musí umět používat všechny technologie), s místem, kam všechna zařízení umístit a v neposlední řadě spojené s rychlostí a efektivitou. Navíc výše uvedený přístup pak znamená i silné zapojení lidského faktoru, který může mít a má pak zásadní vliv na chybovost takto načítaných či prověřovaných VIN. Všechny výše uvedené nedostatky, potíže spojené s praktickým použitím pramení z nedodržení již výše uvedených zásad č. 5 a č. 6.



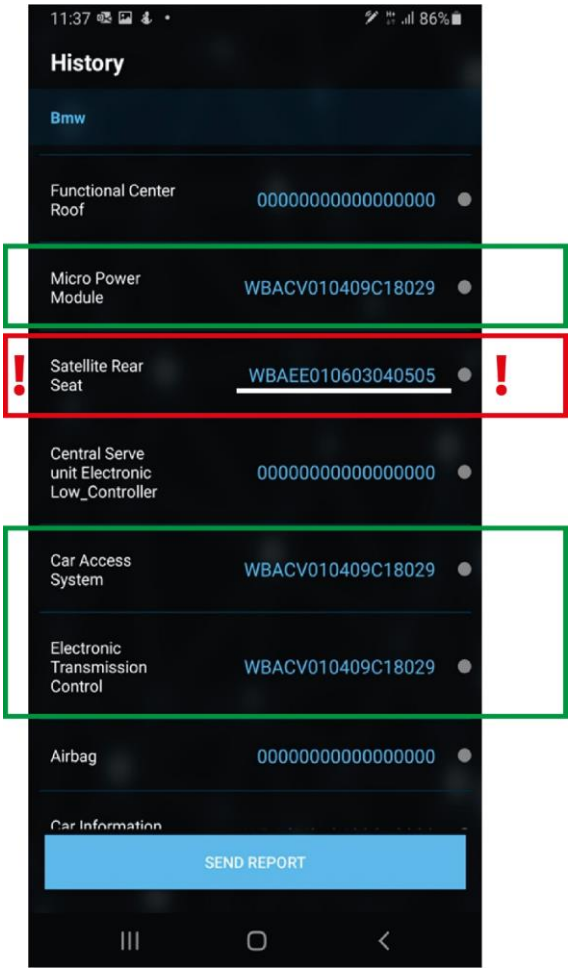
Obr. 5 Sklad s použitými díly vozidel. Identifikátor VIN nebo identifikační štítky se nacházejí na vozidle jen na několika místech. Abychom mohli identifikovat jednotlivé významné komponenty vozidla, musí být taktéž označeny vhodným způsobem - buď mechanicky nebo v dnešní době elektronicky. Autor: Roman Rak

Digitální identifikace vozidla je velmi perspektivní a vkládají se do ní i velká očekávání. Nejedná se jen o zájmy forenzní, ale především i o zájmy komerční. Jednotlivé tovární značky jsou motivovány i tím, abych servis jejich vozidel byl prováděn profesionálně s patřičným dílenským a diagnostickým vybavením, pomocí standardních postupů, metodicky správně proškolených profesionálních osob. Servisované vozidlo by mělo splňovat všechny nároky, včetně zaručení postupů, které se promítají především do bezpečného provozu vozidla.

Z pohledů výrobců není žádoucí, aby se vozidla opravovala „na koleně“, a při tom docházelo k výměně komponent z jiných vozidel, včetně těch havarovaných nebo pocházejících z trestné činnosti. Tohoto lze dosáhnou digitálním označováním klíčových komponent a příslušným softwarem, který neumožní ko-existenci neoficiálních náhradních dílů ve vozidle. Bohužel tento zájem je primárně zájmem výrobce a jeho servisní sítě a není ze strany výrobců snaha o standardizaci digitálních technologií pro digitální rozpoznávání komponent napříč výrobci, což by pomohlo pak následně i státním orgánům a institucím, včetně forenzních, se zapojit do boje s trestnou činností spojenou s motorovými vozidly, včetně preventivních opatření. Identifikaci vozidla lze chápat rovněž i jako objektovou záležitost [9], kde každý objekt je nutné primárně nebo sekundárně identifikovat. Identifikace na nejobecnější úrovni patří do bezpečnostních věd [14], do analýzy a řízení rizik. V oblasti identifikace se stále ve větší míře uplatňuje i umělá inteligence, informatika, digitalizace apod. [3], [18]. Identifikace vozidla má i své dopady na bezpečnost silničního provozu [2, 5].

ČTEČKA DIGITÁLNÍHO VIN

V rámci řešené vědecko-výzkumného úkolu č. 245 *Moderní technologie v páchání, odhalování, dokumentování, dokazování a prevenci trestné činnosti* vytýčeného na Akademii Policajného zboru v Bratislavě, Slovenská republika je řešena právě i otázka standardizovaných technologií pro snímání digitálního VIN, nalezení vhodné komerční, běžně dostupné technologie a vyhodnocení výsledků, které byly pomocí ní získány na dostatečném množství vzorku dat.



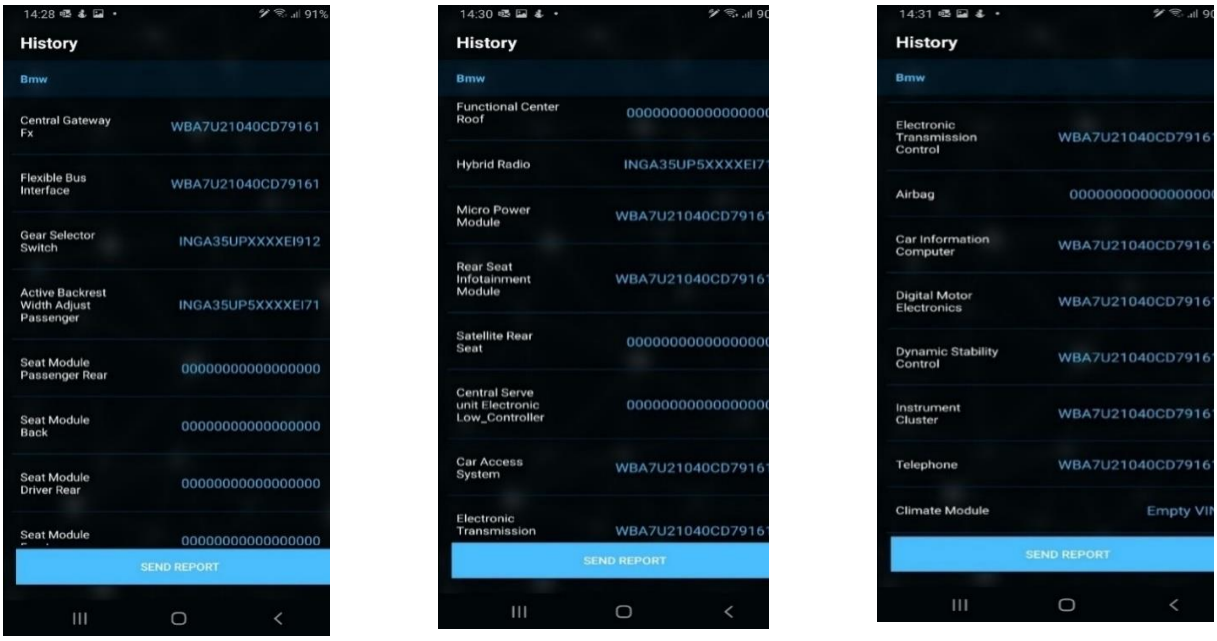
Obr. 6. Ukázka načtených hodnot u vozidla BMW X5 typ G05/G5X. Všechny hodnoty VIN by měly být shodné a žádná z nich by neměla pocházet ze závadového vozidla (vozidlo pohřešované, odcizené, sešrotované apod.). V uvedeném přehledu komponenta „Satellite Rear Seat" pochází z jiného vozidla. Autor: Roman Rak

V rámci řešené vědecko-výzkumné úlohy v minulých letech bylo vyzkoušeno nemalé množství různých diagnostických jednotek, které ale neposkytovaly možnosti vyčítat digitální VIN různých výrobců. Jako nejlépe v praxi použitelné se v praxi ukázala jednoduchá čtečka VIN, která se napojuje na OBD jednotku vozidla. Předpokladem, aby zařízení bezchybně fungovalo, je nainstalování příslušné aplikace do chytrého telefonu, aktualizace datového fondu firmwaru a v neposlední řadě palubní přístroje vozidla pod napětím a zapnutý klíček zapalování. Poslední je vhodné vždy dodržet, protože u některých továrních značek při vypnutém zapalování nejsou vyčteny všechny kódy VIN (u jiných továrních značek tento proces funguje bezchybně i při vypnutém zapalování).

Jak již bylo řečeno, čtečka VIN je jednoúčelové zařízení, které se připojuje k OBD konektoru vozidla. Načtené umístění jednotlivých identifikátorů komponent vozidla s jejich hodnotami jsou pomocí technologie Bluetooth přeneseny a zobrazeny do smart mobilního telefonu, kam se před tím jednorázově nahraje příslušná aplikace, pracující v operačním systému Android nebo Apple. Z mobilního telefonu je možné odeslat report o výsledku

kontroly nebo data pro pozdější zpracování archivovat. Zároveň je možné porovnávat, zda nalezený VIN není v pátrání po odcizených vozidlech.

Při analýze bylo kontrolováno přibližně 220 vozidel různých (odlišných i shodných modelů) vyráběných v posledních cca 10ti letech od více jak 35 továrních značek.



Obr. 7 Ukázka identifikátorů vozidla BMW 750Li (typ G12/7L), pořízená OBD čtečkou VIN. Položky v seznamu (levý sloupec obrázku mobilní aplikace) obsahují různé hodnoty. Nalezneme zde identifikátor vozidla VIN (WBA7U21040CD79161), konstanty s řetězcem 17 ti nul (které mohou být výrobcem vyplněny konkrétní hodnotou), nevyplněné položky (Empty VIN) a kódy INGA – typová identifikace, opakující se u různých vozidel, i různých modelů.

Aplikace, postupně jak je nachází, vypisuje na obrazovku seznam komponent a k nim odpovídající hodnoty identifikátorů, jež jsou v nich digitálně uloženy. Názvy komponent, označených digitálním identifikátorem jsou definovány výrobcem, a mezi výrobci se terminologicky liší, byť z názvu lze usoudit, že se jedná o stejnou komponentu (např. *Remote Keyless Entry*). Chybí zde standardizace. Pokud vypracujeme přehled názvů komponent, zjistíme, že v určitém roce výroby výrobce ale označuje komponenty pro svá vozidla obvykle stejně (v různých letech se ale názvy jedné a té samé komponenty mohou měnit, tak jak se problematika vyvíjí). Stejně tak se mění i vyplňované hodnoty. V prvních letech se u jednoho modelu vozidla mohou jako hodnoty objevovat samé nuly (nebo jiné kódy), v následujících letech se pak důsledně vyplňuje jako hodnota identifikátor VIN.

Komponenty mohou tedy nabývat těchto hodnot:

a) prázdná hodnota (prázdný textový řetězec, v IT pojetí zřejmě hodnota NULL);
b) řetězec 17ti nul („00000000000000000“), tedy stejná délka řetězce jako má identifikátor VIN);
c) hodnota konkrétního VIN vozidla např. „JHMRW2760LX203795“, „WBAFF01020L322951“ apod.
d) textový řetězec „Empty VIN“;
e) individuální kód komponenty, odvozený od VIN, resp. poslední znaky VIN v podobě sériového výrobního čísla (V.I.S.) např. „L322951
f) individuální kód komponenty, odlišný od VIN, mající délku kratší než 17 pozic;
g) individuální kód komponenty, odlišný od VIN, mající délku 17 pozic, např. „L INGA35UP5XXXXEI71“;
h) směs netisknutelných znaků, nebo znaků odlišných od alfabetického charakteru. Tedy jiné znaky, než jsou písmena základní národní abecedy (A až Z) a číslice 1 až 9.

Tab. 1. Závislost vyplňování digitálních hodnot identifikátorů jednotlivých komponent vozidel BMW na modelu vozidla. Čím je vozidlo modernější, více vybavené technologiemi (včetně těmi volitelnými zákazníky), komfortnější, tím více digitálních identifikátorů ve vozidle nalezneme. Zdroj: autoři.

Tab. 1. Dependence of filling in digital values of identifiers of individual components of BMW vehicles on the vehicle model. The more modern the vehicle, the more equipped with technology (including those optional customers), the more comfortable, the more digital identifiers we will find in the vehicle. Source: Authors.

	M8 Gran Coupé	X5	X6	M4 Coupé	X3	serie 3	X1	serie 6 (640i)	serie 1 (118d)	serie 7 (750Li)	serie 2 Gran Coupé	M2 (CS)
Počet digitálních VIN ve vozidle		1	0		0	0				1	0	
Central Gateway Fx												
Flexible Bus Interface				0				0	0			0
Seat Module Front	0	0	0	0	0	0		0		0	0	
Seat Module Back	0	0	0	0				0		0		

	M8 Gran Coupé	X5	X6	M4 Coupé	X3	serie 3	X1	serie 6 (640i)	serie 1 (118d)	serie 7 (750Li)	serie 2 Gran Coupé	M2 (CS)
Seat Module Driver Rear												
Seat Module Passanger Rear												
Gear Selector Switch	E	E	E	0	C	E		C	E	C	E	0
Active Backrest Width Adjust Passanger										C		
Trailer Module		E	E		E	E		E				
Functional Center Roof	0	0	0	0	0	0		0		0	E	C
Hybrid Radio			C					C		C		
Micro Power Modul	V	V	V	0	V	V		0		V		
Rear Seat Infotainment Module										V		
Satellite Rear Seat	0	V	0		0	0		0	0	0		
Central Serve unit Electronic Low_Controller	0	0	0	0	0	0		0	0	0	0	0
Car Access System	V	V	V	V	V	V	V	V	V	V	V	V
Electronic Transmission Control	V	V	V	V	V	V		V	V	V	V	V
Base Body Module				E					0			E
Airbag	0	0	0	0	0	0		0		0	0	0
Car Information Computer	0	V	V	V	V	V		V	V	V	V	V
Digital Motor Electronics	V	V	V	V	V	V		V	V	V	V	V
Dynamic Stability Control	V	V	V	0	V	V		E	V	V	V	0
Electronic Power Steering												
Instrument Cluster	V	V	V	0	V	V		0	V	V	V	E
Telephone	V	V	V	0	V	V		0	0	V	V	0
Climate Module	E	E	E	0	E	E		E	E	E	E	0

Legenda:

V – v položce je digitálně zapsán VIN daného vozidla, např. WBSGV01050CE68914

E – v položce je uvedena hodnota „Empty VIN“

0 – v položce je digitálně uveden řetězec „0000000000000000“, 17x znak 0 (nula)

C – v položce je uveden jiný výrobní kód, než VIN, označující určitý typ zařízení (stejný kód se může vyskytovat i u jiný ch modulů daného výrobce. Příklad: INGA35UP5XXXXEI71, INGA35UPXXXXEI912 apod (kód má 17 pozic).

Závěr

Oblast zkoumání digitálních dat souvisejících s provozem motorových vozidel (*Vehicle Digital Forensics*) patří do širšího oboru analýzy digitálních dat (stop), který bývá označován jako *Digital Forensic* nebo *Computer Forensics* [1]. Zkoumání dat, digitálních stop vzniklých používáním počítačů, mobilních telefonů a dalších komponent osazených procesorovými jednotkami je dnes již poměrně ustálený obor, který si prošel svou ne zrovna lehkou historií. Tyto disciplíny se rovněž postupně rozvíjejí v ČR i SR [12], [13].

Zkoumání digitálních dat ve vozidle je v kriminalistické a forenzní praxi (včetně soudního inženýrství) využitelné zejména v následujících základních oblastech:

- **Identifikace vozidla a jednotlivých komponent** – účelem je boj s automobilovou trestnou činností (krádeže vozidel, podvody a další trestné činy spojené s vozidly, nelegální obchod s komponentami vozidel apod.). Korektní identifikace vozidla je rovněž prvotním úkonem pro jakékoliv další, následné forenzní aktivity.
- **Vyčítání digitálních dat** pro analytické účely (podvody se stáčenými kilometry, neoprávněné jízdy, provoz, údržba vozidla apod.).
- **Analýzy chování vozidla v průběhu standardních i nestandardních situacích** (nehody, kybernetické útoky apod.).
- **Chování vozidla a jeho posádky využitelné pro operativní činnost nebo vyšetřování orgánů činných v trestním řízení** (geografický pohyb vozidla, vystupování a nastupování osob, telefonní a datový provoz jednotlivých členů osádky během jejich pobytu ve vozidle apod.).

Vehicle Digital Forensics je obor, který teprve vzniká a na své rozsáhlé využití teprve čeká. Klíčovými otázkami je standardizace datových rozhraní, záznamových jednotek [20], ukládaných dat ve vozidlech na straně jedné, jejich využití a uplatnění ve forenzní činnosti na straně druhé. Bezesporu bude nutná existence dostupných, dostatečně obecných, certifikovaných forenzních technologií [11], které bude možné poměrně lehce využívat při

forenzním zkoumání, stejně tak adekvátní forenzní metody a metodologie. Tyto aktivity budou úzce spojené s výchovou zcela nového druhu specialistů, forenzních inženýrů, bezpečnostních manažérů [17] a forenzních pracovišť [8, 19], jejichž oborová náplň bude velmi multidimenzionální [7].

Seznam citované literatúry

BATES, E. A. Digital Vehicle Forensics [online, cit, 2019-11-17], Dostupné z: https://abforensics.com/wp-content/uploads/2019/02/INTERPOL-4N6-PULSE-IssueIV-BATES.pdf

BÖHM, K., KUBJATKO, T., PAULA, D., SCHWEIGER, H.-G. (2020). New developments on EDR (Event Data Recorder) for automated vehicles**.** *Open Engineering*, 10(1), pp. 140–146 ISSN: 23915439, DOI: 10.1515/eng-2020-0007

ČERMÁK, M., ŠULC, V. (2022). Scams Committed Solely Through Computer Technology, Internet and E-Mail. In: Tušer, I., Hošková-Mayerová, Š. (eds) Trends and Future Directions in Security and Emergency Management. Lecture Notes in Networks and Systems, vol 257. Springer, Cham. https://doi.org/10.1007/978-3-030-88907-4_17 https://link.springer.com/chapter/10.1007/978-3-030-88907-4_17

DIRNBACH, I., KUBJATKO, T., KOLLA, E., ONDRUŠ, J., ŠARIĆ, Z. (2020). Methodology designed to evaluate accidents at intersection crossings with respect to forensic purposes and transport sustainability**.** *Sustainability (Switzerland)*, 12(5), 1972 ISSN: 20711050, DOI: 10.3390/su12051972

HUDECOVA ,V. (2021), Road Safety from the Perspective of European Union. In Kavan, Š. (eds.) International Conference Safe and Secure Society 2021. Conference proceeding. České Budějovice: College of European and Regional Studies, Czech Republic, 2021. pp. 15 – 23. DOI: 10.36682/SSS_2021. ISBN 978-80-7556-097-1, ISSN 2533-6223.

FELCAN, M., KOPENCOVÁ, D., RAK, R. *Objekty a systémy – základní analytické prvky bezpečnosti*. Zborník ze 14. mezinárodního sympózia konaného dne 14.3.2020 v rámci mezinárodního veletrhu Security Bratislava 2019, Akademie policejního zboru v Bratislavě, Bratislava, 212 s, ISBN 978-80-8054-795-0, s. 41–55.

HAJDUKOVÁ, T. *Metodológia výzkumu*, In: Aplikácia vedeckých metód na prípady z policajnej praxe. 2018, ISBN 978-80-8054-766-0.

JŮZL M., VLACH F., (2022). Modern Approaches in Czech Prison Staff Education and Training Against a Background of Comenius' Thoughts. In: Tušer I., Hošková-Mayerová Š. (eds) Trends and Future Directions in Security and Emergency Management. *Lecture Notes in Networks and Systems*, vol 257. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-88907-4_24

KOPENCOVA D., FELCAN M., RAK R. (2021) Equilibrium and Limit States in Technical and Social Disciplines as Part of Risk Analysis and Management. In: Abdel Wahab M. (eds) Proceedings of 1st International Conference on Structural Damage Modelling and Assessment. Lecture Notes in Civil Engineering, vol 110. Springer, Singapore. ISBN 978-981-15-9120-4. https://doi.org/10.1007/978-981-15-9121-1_22

KUBJATKO, T.,GÖRTZ, M., MACUROVA, L.,BALLAY, M. (2018). Synergy of forensic and security engineering in relation to the model of deformation energies on vehicles after

traffic accidents (Conference Paper) Transport Means - Proceedings of the International ConferenceVolume 2018-October, 2018, pp, 1342-1348, *22nd International Scientific on Conference Transport Means 2018*; Trasalis - Trakai Resort and SPAGedimino str. 26, Trakai; Lithuania; 3 October 2018 through 5 October 2018; Code 140271. ISSN 1822296X

MANSOR, H., MARKANTONAKIS, K., AKRAM, R. N., MAYES, K., GURULIAN, I.: *Log your car: The non-invasive vehicle forensics*. 2016 IEEE International Conference Trustcom/BigDataSE/ISPA, Trust, Security and Privacy in Computing and Communications, [online, cit, 2019-11-26], Dostupné z: https://ieeexplore.ieee.org/document/7847047/authors#authors

ODLEROVÁ, M. Postavenie bezpečnostných zložiek v Slovenskej republike z hľadiska ich vplyvu na verejný poriadok a bezpečnosť. In: *QUAERE 2020*. Hradec Králové: Magnanimitas akademické sdružení, 2020. ISBN 978-80-87952-32-0, s. 1422-1431.

ODLEROVÁ, M., HAJDÚKOVÁ, T. Komparácia právnej úpravy a skúseností s použitím zbrane príslušníkmi Policajného zboru a príslušníkmi Polície Českej republiky. In: *Policajná teória a prax*. ISSN 1335-1370. - Roč. 28, č. 2, 2020, s. 61-81.

RAK, R.; SULC, V.; KOPENCOVA, D.; VLACH, F.; HUDECOVA, V., (2022). Crisis Development and its management, *Entrepreneurship and Sustainability Issues* 9(3): 414-428. https://doi.org/10.9770/jesi.2022.9.3(25) , http://jssidoi.org/jesi/article/957

RAK, R., KOPENCOVA D. AND M. FELCAN, (2021). Digital vehicle identity – Digital VIN in forensic and technical practice, *Forensic Science International: Digital Investigation*, Elsevier, Volume 39, 2021, 301307, ISSN 2666-2817, https://doi.org/10.1016/j.fsidi.2021.301307, https://www.sciencedirect.com/science/article/pii/S2666281721002328

RAK, R., FELCAN, M. AND KOPENCOVA, D., (2021). Digital identification of vehicles not only for investigative and forensic purpose, *2021 5th International Conference on Vision, Image and Signal Processing (ICVISP)*, 2021, pp. 18-26, doi: 10.1109/ICVISP54630.2021.00013.

ŠULC, V., JEDIŇÁK, P., (2019). Role manažera kybernetické bezpečnosti v procesu řízení technických zranitelností. In: Sborník příspěvků z konference „*Human potential development*" konané dne 28. – 30. 5. 2019. Poland, universita of Lodz. Str. 107-115. ISBN 978-83-65766-25-0.

ŠULC, V., ZELINKA, I., CONG, T., PLUCAR, J., ČANDÍK, M., (2019). Umělá inteligence a kybernetická bezpečnost. In: *Sborník příspěvků ze čtvrté Mezinárodní konference o umělé inteligenci a evolučních výpočtech v inženýrských systémech*.

VLACH, F. Akademie Vězeňské služby ČR jako učící se organizace. In Jůzl, M. a kol. *Současné vzdělávací trendy v českém vězeňství,* s. 203–228. Praha: UJAK Praha, 2020. ISBN 978-80-7452-148-5.

Event Data Recorders (US National Higway Traffic Safety Administration regulation) (NHTSA), 2018 edition, updated as of May 29, 2018, The Law Library, printed by Amazon, ISBN 9781729754900.

Kontaktné údaje
JUDr. Dagmar Kopencová, PhD.
Katedra bezpečnosti a práva
AMBIS Vysoká škola
Dagmar.Kopencova@ambis.cz

prof. Ing. Roman Rak, PhD.
Katedra bezpečnosti a práva
AMBIS Vysoká škola
Roman.Rak@ambis.cz

PhDr. Vladimíra Hudecová
Odbor dokladov a evidencií
Prezídium Policajného zboru
vladimira.hudecova2@minv.sk

Recenzenti: doc. RNDr. Tatiana Hajdúková, PhD.
PhDr. Peter Veselý, PhD.

Aktuálne hrozby interakcií vo virtuálnom svete[1]

Patrícia Krásná

Abstrakt: Virtuálny priestor, resp. svet prináša pri svojich pozitívach i negatíva, s ktorými je potrebné sa adekvátne vysporiadať a dbať na to, aby nespôsobili nežiadúce účinky. V aktuálnej dobe je internet a virtuálny svet súčasťou každodenného života takmer každého človeka. Bez moderných elektronických zariadení, ktoré majú okamžitú možnosť pripojenie sa na internet je pre nás každodenné bytie často až závislé. Práve i z tohto dôvodu je potrebné neustále vnímať a hľadať možné riziká, ktoré vo virtuálnom svete vznikajú. Predkladaný vedecký článok dbá na dané a predkladá čitateľovi i charakteristiky vybraných hrozieb, ktoré sú viac, či menej v spoločnosti známe a ohrozujú vo zvýšenej miere každého užívateľa internetu. Vedecký článok reflektuje na aktuálne virtuálne hrozby, ktoré v spoločnosti vznikajú a poskytuje predpoklad pre efektívnu činnosť i orgánov činných v trestnom konaní aj v rámci prípravného konania.

Kľúčové slová: hrozba, virtuálny svet, počítačový vírus, bezpečnostný incident, prevencia, efektívnosť

Abstract: Virtual space, or the world brings its positives as well as negatives, with which it is necessary to deal adequately and to ensure that they do not cause unwanted effects. Nowadays, the Internet and the virtual world are part of the daily life of almost every person. Without modern electronic devices, which have an immediate possibility to connect to the Internet, our everyday life is often even dependent. Precisely for this reason, it is necessary to constantly perceive and look for possible risks that arise in the virtual world. The presented scientific article pays attention to the data and presents to the reader the characteristics of selected threats that are more or less known in society and increasingly threaten every Internet user. The scientific article reflects on the current virtual threats that arise in society and provides a prerequisite for the effective activity of law enforcement agencies as well as in the framework of preliminary proceedings.

Key words: threat, virtual world, computer virus, security incident, prevention, efficiency

Úvod

Kvalita trestnoprávnej ochrany spoločenských vzťahov je významným ukazovateľom funkčnosti každého demokratického a právneho štátu. Vývoj spoločnosti je okrem pozitívnych zmien spojených predovšetkým s používaním moderných technológií sprevádzaný aj novými formami protispoločenskej činnosti, na čo je nútený právny systém dynamicky reagovať.[2] Medzi tieto formy protispoločenskej činnosti, dovolíme si uviesť, s určitosťou patria aj hrozby interakcií v virtuálnom svete.

[1] „Táto práca bola podporená Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-19-0102.“

[2] KURILOVSKÁ, L., HAJDÚKOVÁ, T. 2021. *Hodnotenie efektívnosti prípravného konania pri prečinoch v kontexte objasnenosti a regionálnych disparít na území Slovenskej republiky*. In ČENTÉŠ, J. (ed.) a kol.: „Efektívnosť prípravného konania – jej skúmanie, výzvy a perspektívy“, Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2020, s. 74-85.

Hrozbu je možné identifikovať ako akýkoľvek fenomén, ktorý má potenciálnu schopnosť poškodiť záujmy a hodnoty chránené, či už jednotlivcom alebo napr. aj štátom. Miera hrozby je daná veľkosťou možnej škody a časovou vzdialenosťou, vyjadrenou obvykle pravdepodobnosťou, čiže rizikom, možného uplatnenia tejto hrozby.[3] Je opodstatnené, že aktuálne hrozby interakcií hrozia vo veľkej miere vo virtuálnom svete práve z dôvodu zvýšených aktivít, ktoré ľudia n internete realizujú. Vzájomné ovplyvňovanie relevantných prvkov, ktoré vo virtuálnom svete existujú a ovplyvňujú sa sú odrazom nespočetného množstva aktivít, ktoré je možné vo virtuálnom svete vykonávať. Virtuálny priestor nám poskytuje neobmedzený priestor a takmer neobmedzené možnosti či už pri práci, hľadaní nových informácií alebo i pri komunikácii medzi priateľmi a rodinou.

Hrozby, ktoré vnímame v najvyššej miere na internete je možné zaradiť medzi často známe riziká, ale na čo je potrebné reflektovať sú aj hrozby, ktoré širokej verejnosti nie sú až také známe. Predkladaný vedecký článok reflektuje aj na dané a preto poukazuje i na hrozby, o ktorých nie je tak často hovorené. Naša pozornosť bude smerovať k počítačovým vírusom, malwaru, phishingu, botnetu, Distributed Denial of Service (DDoS) - teda distribuovanému odmietnutiu služby, SQL Injection Attack, rootkitu, Rogue Security Software a APT Threats.

Virtuálne prostredie, virtuálny svet, je možné ponímať ako počítačom simulované prostredie. Do určitej miery sa stal tento pojem synonymom pre interaktívne 3D virtuálne prostredia, kde majú používatelia rôzne podoby a môžu navzájom medzi sebou komunikovať.[4] Samozrejme, ako synonymum k danému je možné, podľa nášho názoru, vnímať aj prostredie internetu a virtuálnych možností. Pri zamyslení sa nad skutočnosťou existencie internetu je opodstatnené domnievať sa, že akákoľvek aktivita, ktorá prebieha prostredníctvom internetu je virtuálna agilita, ktorá v konečnom dôsledku prinesie výsledok. Je veľmi podstatné vnímať tieto virtuálne agility i so zamyslením sa nad skutočnosťou ich priebehu a v konečnom dôsledku aj výsledku. Pri bežnej činnosti mimo online priestoru vnímame postup, potrebnú aktivitu, jednotlivé potrebné kroky, ktoré je potrebné vykonať pre získanie požadovaného stavu. Pri realizácií činnosti vo virtuálnom svete vnímame často iba počiatočný impulz a následne konečný výsledok. Medzi začiatočným podnetom a rezultátom nám veľmi často vzniká neznáme vákuum. Práve i z tohto dôvodu považujeme za dôležité venovať sa tejto téme a poukázať na hrozby, ktoré vznikajú pri interakcii na internete, resp.

[3] Bezpečnostní strategie Českej republiky. 2003. [online]. [cit.2022.05.22.]. Dostupné na internete: https://mocr.army.cz/images/Bilakniha/CSD/2003%20Bezpecnostni%20strategie%20CR.pdf.

[4] IGI GLOBAL. 2015. [online]. [cit.2022.05.22.]. Dostupné na internete: https://www.igi-global.com/chapter/internet-identity-and-the-right-to-be-forgotten/131357.

vo virtuálnom svete. Je zrejmé, že v súčasnosti sa kybernetické zločiny odhaľujú oveľa rýchlejšie ako v minulosti, ale vždy existuje obmedzená schopnosť určiť, kto je za tým a aký je jeho zámer. To platí najmä pre hackerov, či skupiny kyberzločincov, ktorí pracujú relatívne beztrestne, mimo tradičného trestného systému krajiny a fyzických hraníc.[5]

Cieľom vedeckého článku je prostredníctvom analýzy, syntézy a rešerše odbornej literatúry uviesť charakteristiky a princípy hrozieb, ktoré vznikajú vo virtuálnom svete a napomôcť tak prevencii, ale i represii pri každodenných vznikajúcich nejasnostiach v aplikačnej praxi. Tiež je cieľom reflektovať na potrebu upovedomenia o vystihnutí podstaty počítačového bezpečnostného incidentu a legislatíve informačnej bezpečnosti v Slovenskej republike a v Európskej únii. Považujeme to za dôležité, pretože pri našej vedecko-výskumnej činnosti i v rámci projektu sa stretávame s častými dotazmi z aplikačnej praxe k daným súvislostiam z dôvodu zvyšujúceho sa počtu ohrození našich občanov pri ich interakciách práve vo virtuálnom prostredí.

Bezpečnostné hrozby vo virtuálnom svete

Kybernetické hrozby a útoky sú takmer každodennou súčasťou virtuálneho sveta. Ich hrozba je nepredvídateľná a ich následky sú veľmi často enormné. Dôležité a cenné dáta, ktoré sú pri týchto hrozbách „odcudzené“ vlastníkom predstavujú často vysokú hodnotu. Preto sú povedomie, znalosti a informácie o týchto skutočnostiach kľúčové i pre odborníkov, ale i pre širokú verejnosť. Popularizácia, prezentovanie a reflektovanie na aktuálne vznikajúce riziká sú podstatne dôležité. Preto je tiež významná aj spoľahlivá počítačová bezpečnosť, ktorá je už v súčasnosti nevyhnutnosťou. Techniky používané kyberzločincami sa v priebehu rokov stali čoraz sofistikovanejšími a pre obete čoraz ťažšie spozorovateľnými. K zvýšeniu nárastu hrozieb interakcií vo virtuálnom svete, dovolíme si s určitosťou tvrdiť, prispela aj pandémia COVID-19, ktorá posunula svet smerom k zvýšeniu technologických inovácií a online spolupráce.

Okrem kyberzločinu môžu byť kybernetické útoky spojené aj s kybernetickou vojnou alebo kyberterorizmom.[6] Z čoho vyplýva, že motivácia pri ohrozeniach vo virtuálnom prostredí je rôzna. Dovolíme si konštatovať, že najčastejšie dochádza k motivácii z troch hlavných dôvodov - kriminálna, politická a osobná. Kriminálne motivovaní útočníci sa snažia

[5] ROGERS, M. K. 2011. *The psyche of Cybercriminals: A Psycho-Social Perspective.* In Ghosh, S., Turrini, E. (eds.), Cybercrimes: A multidisciplinary Analysis. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13547-7_14.

[6] IBM. 2022. [online]. [cit.2022.05.20.]. Dostupné na internete:https://www.ibm.com/topics/cyber-attack.

získať finančný zisk prostredníctvom krádeže peňazí, krádeže údajov alebo narušenia podnikateľskej činnosti. Takto motivovaní útočníci žiadajú najčastejšie finančnú odplatu. Sociálno-politicky motivovaní útočníci hľadajú pozornosť a chcú zaujať širokú verejnosť. Výsledkom je teda, že o svojich útokoch informujú verejnosť, dané môžeme označiť i pojmom „hacktivizmus“.[7]

Počítačové vírusy

Následne si dovolíme prejsť k samotnej charakterizácii jednotlivých, nami vybraných, bezpečnostných hrozieb, ktoré sú v súčasnosti identifikované. Počítačové vírusy sú tými najbežnejšími medzi internetovými bezpečnostnými hrozbami. Vírusy „vstupujú“ do elektronických zariadení pripojením k určitému hostiteľskému súboru alebo systému. Dôležité je uvedomiť si, že v prípade ak preniknú do zariadenia môžu okamžite spôsobiť poškodenie alebo naopak ostať úplne nečinné. V prípade ich nečinnosti je veľmi pravdepodobné, že ich cieľom nie je iba jedno zariadenie, ale práve naopak majú tendenciu vstúpiť i do iných zariadení a tak vytvoriť ideálne podmienky pre získanie potrebných informácií, údajov, či skutočností. Ich zámerom je „infikovať“ ďalšie počítače a sieťové systémy. Počítačový vírus je typ malvéru, ktorý sa pripojí k inému programu (napríklad k dokumentu), ktorý sa môže replikovať a šíriť. Jeho rozširovanie nastáva vtedy, keď ho osoba prvýkrát spustí vo svojom systéme. Môže ísť, napr. o e-mail so škodlivou prílohou. Vírusy môžu získať údaje o heslách, zničiť údaje, spomaliť systémové prostriedky, spamovať e-mailové kontakty a dokonca, napríklad aj zaznamenávať stlačenia klávesov. Kyberzločinci nevytvárajú stále nové vírusy, namiesto toho zameriavajú svoje úsilie na sofistikovanejšie hrozby. Pre lepšie ozrejmenie uvádzame tiež, že počítačový vírus je typ škodlivého kódu alebo programu vytvoreného s cieľom zmeniť spôsob fungovania počítača a je navrhnutý tak, aby sa šíril z jedného počítača do druhého. Útok počítačového vírusu sa môže prejavovať prostredníctvom rôznych príznakov. Dovolíme si uviesť najčastejšie z nich: časté vyskakovacie okná, zmeny na domovskej stránke, nemožnosť resetovať počítač, hromadné e-maily odosielané z e-mailového účtu. Vírus tiež môže spôsobiť veľké škody na pevnom disku elektronického zariadenia. Môže to spôsobiť zamrznutie alebo zlyhanie zariadenia, neobvykle pomalý výkon zariadenia a pod.

Malware

Ďalšou bežnou bezpečnostnou hrozbou, ktorá je veľmi často identifikovaná v kontexte virtuálneho prostredia je malvér alebo ransomvér. Malvér útočí na súbory, ktoré sa

[7] MANSFIELD-DEVINE, S. 2011. *Hacktivism: assessing the damage.* In Network Security Volume 2011, Issue 8, August 2011, s. 5-13.

nachádzajú, napr. v počítači. Rôzne štúdie ukazujú, že malvér postihuje 32 % všetkých počítačov na svete.[8] Útok začína infikovaním databázových systémov. Z týchto databázových systémov následne zašifruje získané údaje a predstavuje hrozbu zmazania všetkých existujúcich súborov v zariadení.

Z dôvodu častého zamieňania pojmov „vírus“ a „malware“(malvér) si dovolíme v stručnosti uviesť ich diferenciu. Počítačový vírus je typ malvéru, ale naopak nie každý malvér je počítačový vírus. Najjednoduchší spôsob, ako odlíšiť počítačové vírusy od iných foriem škodlivého softvéru, je premýšľať o daných vírusoch optikou biológie.

Najelementárnejšie pochopenie je zjavné pri víruse chrípky. Chrípka si vyžaduje určitý druh interakcie medzi dvoma ľuďmi - napríklad potrasenie rukou, bozk alebo dotyk niečoho, čoho sa infikovaná osoba dotkla. Akonáhle sa vírus chrípky dostane do ľudského systému, naviaže sa na zdravé ľudské bunky a pomocou týchto buniek vytvorí viac vírusových buniek. Počítačový vírus funguje veľmi podobne: počítačový vírus vyžaduje hostiteľský program, vyžaduje na prenos z jedného systému do druhého akciu používateľa a následne pripája kúsky vlastného škodlivého kódu k iným súborom alebo súbory priamo nahrádza svojimi kópiami. Z daného vyplýva aj skutočnosť, že vírusy sa nemôžu šíriť bez nejakej akcie používateľa, ako je napríklad otvorenie infikovaného dokumentu programu Word. Malvér sa na druhej strane dokáže šíriť v systémoch a sieťach sám, čo ich robí oveľa rozšírenejšími a nebezpečnejšími. Je známe, že ransomvérový červ WannaCry z roku 2017 sa rozšíril po celom svete, zlikvidoval tisíce systémov Windows a nazbieral značné množstvo nevystopovateľného bitcoinového výkupného za údajných severokórejských útočníkov.[9]

V súčasnosti je možné detegovať aj malvér novej generácie. Tento môže spustiť viac deštruktívnych útokov ako to bolo spozorované v minulosti. Je samozrejmé, že i vývoj samotných malvérov napreduje aby tak získal v rámci jedného útoku čo najviac prospešných údajov. Následne si v stručnosti dovolíme zhrnúť v priloženej tabuľke porovnanie tradičného malvéru a malvéru „novej generácie“.

[8] VELECOR. 2022. [online]. [cit.2022.05.15.]. Dostupné na internete: https://mocr.army.cz/images/Bilakniha/CSD/2003%20Bezpecnostni%20strategie%20CR.pdf.https://velecor.com/10-common-internet-security-threats-and-how-to-avoid-them/.

[9] MALWAREBYTES. 2022. [online]. [cit.2022.05.15.]. Dostupné na internete: https://www.malwarebytes.com/computer-virus.

Tabuľka 1 Porovnanie tradičného malvéru a malvéru novej generácie.

Porovnávací parameter	*Tradičný malvér*	*Malvér novej generácie*
Implementačná úroveň	jednoduchý kód	zložitý kód
Správanie	statické	dynamické
Šírenie	kópie sú podobné	kópie sú odlišné
Prostredie šírenia	časovo ohraničené	trvalé
Stálosť v systéme	jednotlivé procesy	komplexné procesy
Využívanie krycích techník	nie	áno
Čas útoku	všeobecný	cielený
Obranná výzva	jednoduchá	náročná
Cieľové zariadenia	všeobecné zariadenia	konkrétne zariadenia

Zdroj: vlastné spracovanie podľa ÖMER, A., REFIK, S.[10]

Z daného opäť vyplýva skutočnosť, že inovácie sa dotýkajú aj samotných útokov a ich sofistikovanosti.

Phishing

Pojmu „phishing“ sa venovala pozornosť v rámci diskusií odborníkov, výskumníkov, ale aj inštitúcií zaoberajúcich sa kybernetickou bezpečnosťou. V súčasnosti však konštatujeme, že neexistuje žiadna ustálená definícia tohto pojmu. Vybrané definície označujú webové stránky ako jediné možné médium na vykonávanie útokov prostredníctvom phishingu. Phishing je identifikovaný ako „podvodná činnosť, ktorá zahŕňa vytvorenie repliky existujúcej webovej stránky s cieľom oklamať používateľa, aby odoslal osobné, finančné alebo údaje o heslách“.[11] Charakteristika typická pre phishing hovorí aj o skutočnosti, že phishing je formou online krádeže identity, ktorej cieľom je ukradnúť používateľom citlivé informácie, ako sú napr. heslá online bankovníctva a informácie o kreditných kartách.[12] Niektoré definície tiež zdôrazňujú používanie kombinovaných sociálnych a technických zručností. Napríklad APWG[13] definuje phishing ako „zločinecký mechanizmus využívajúci

[10] ÖMER, A., REFIK, S. 2020. *A Comprehensive Review on Malware Detection Approaches.* In IEEE Access, Volume: 8, 2020, s. 6249-6271.

[11] MERWE, A., MARIANNE, L., MAREK, D. 2005. *Characteristics and responsibilities involved in a Phishing attack.* In WISICT ’05: proceedings of the 4th international symposium on information and communication technologies. Trinity College Dublin, s. 249-254.

[12] KIRDA, E., KRUEGEL, C. 2005. *Protecting users against phishing attacks with AntiPhish.* Proc. - Int. Comput. Softw. Appl. Conf. 1, s. 517-524.

[13] Poznámka autora: Anti-Phishing Working Group je medzinárodné konzorcium, ktoré sa pokúša eliminovať podvody a krádeže identity spôsobené phishingom a súvisiacimi incidentmi.

sociálne inžinierstvo aj technické triky na odcudzenie osobných údajov spotrebiteľov a poverení finančného účtu“.[14]

Phishing zvyčajne začína podvodným e-mailom, ktorý je navrhnutý tak, aby prilákal obeť. Štúdie ukázali, že podvodník môže použiť ľudské kognitívne a behaviorálne atribúty na navrhovanie svojich trikov a následne tak na oklamanie obetí. Napríklad podvodník môže poslať falošný e-mail, ktorý vyzerá, že pochádza z legitímneho zdroja a prostredníctvom neho využiť slabosť obete.[15] Môžu napríklad požiadať príjemcu, aby klikol na webový odkaz a vyhral cenu. Postoj niektorých ľudí, ktorí riskujú alebo sú jednoducho zvedaví smeruje na kliknutie odkazu, čím sa otvorí phishingová stránka. Podvodníci veľmi často používajú psychologické triky, ktoré vedia, že obete navedú ku kliknutiu na škodlivý odkaz. Typickými znakmi phishingu, resp. phishingových e-mailov, sú všeobecné alebo neformálne oslovenia. V prípade e-mailu napr. chýba osobnejší prístup - obsahuje všeobecné oslovenie, ale nie je to pravidlom. Dobrá organizácia útoku môže zabezpečiť okrem konkrétneho oslovenia aj logo hodnovernej organizácie, ktoré podporí dôveru voči danému e-mailu. Takéto e-maily sú charakteristické žiadosťou o osobné informácie. V minulosti bol phishing jednoduchšie rozpoznateľný vďaka zlej štylizácii slov, či viet. V súčasnosti to už, vo väčšine prípadov, neplatí. Útočníci dnes už často využívajú služby profesionálnych prekladateľov. Ďalším veľmi častým znakom phishingu je vytvorenie pocitu naliehavosti. Takéto správy sa často svojím obsahom pokúšajú o to, aby obeť konala rýchlo a neuvážene. Phishingové správy či falošné webové stránky vyzerajú čoraz legitímnejšie. Preto je potrebné, aby si jednotlivec všímal doménu v adrese odosielateľa. V prípade, ak dôjde k presmerovaniu na externú webovú adresu je potrebné sledovať, či stránka obsahuje https:// protokol a ikonu bezpečnostného zámku (ten je možné nájsť v okienku s URL adresou).[16] Pre názornú ukážku si dovolíme poukázať na phishingové e-maily, ktoré veľmi často prichádzajú i do našej služobnej pošty. Je to dôkazom toho, že hrozby virtuálneho sveta neobchádzajú ani rezort Ministerstva vnútra Slovenskej republiky.

[14] APWG. 2018. *Phishing activity trends report 3rd quarter*. 2018, s. 1-11.
[15] ABROSHAN, H., DEVOS, J., POELS, G., LAERMANS, E. 2017. *Phishing attacks root causes*. Proc. Int. Conf. Risks Secur. Internet Syst., s. 187-202.
[16] ESET. 2022. [online]. [cit.2022.05.16.]. Dostupné na internete: https://www.eset.com/sk/blog/domaca-it-bezpecnost/ako-rozpoznat-phishing/.

Obrázok 1 Phishingový e-mail

Zdroj: vlastné spracovanie z e-mailovej adresy.

Botnet

Nepriateľské internetové roboty, tzv. botnety, predstavujú rastúcu hrozbu pre bezpečné používanie internetu a interakciu vo virtuálnom svete. Napriek značnému rozsahu výskumov detekcie a ochrany pred botnetmi,[17] ich útoky sú vážnym problémom, ktorý sa rýchlo vyvíja. Útočníci neustále vytvárajú nové typy útokov so zvýšenou úrovňou prepracovanosti na skrytie identít každého jednotlivého robota. Pri útokoch spameri používajú hostiteľov (botnetov) na registráciu miliónov používateľských účtov (označovaných ako používatelia botov alebo účty botov) od veľkých bezplatných poskytovateľov webových e-mailových služieb, ako sú, napr. Gmail, Hotmail a Yahoo. Charakteristika bot-u alebo webového robota je typická škodlivým programom, ktorý prechádza cez sieťové adresy a infikuje nechránené počítače, zariadenia. Hackeri takto môžu prevziať kontrolu nad viacerými počítačmi v tom istom čase a zmeniť ich na botov. Hackeri väčšinou používajú botov na infikovanie veľkej skupiny zariadení (televízny prijímač, router, detské video pestúnky s pripojením na internet alebo IP kamery), ktoré vytvoria sieť alebo tiež botnet. Akonáhle je zariadenie používateľa v sieti botnet, môže byť použité na šírenie DDoS útokov[18], proxy[19] a tiež môže byť použitý na vykonávanie automatizovaných úloh cez internet bez toho, aby o tom požívateľ vedel. Je možné v tejto súvislosti hovoriť o posielaní nevyžiadanej pošty, vírusov alebo na ukradnutie súkromných informácií (prihlasovacie údaje do internet

[17] ZHANG, G. Gu, J., BOTSNIFFER, W. Lee, 2008. *Detecting botnet command and control channels in network traffic*. In NDSS, 2008.

[18] Poznámka autora: Distributed Denial of Service - ide o istú formu "odmietnutia služby". Server, na ktorý je útok vykonávaný po čase naozaj odmietne poskytovať svoje služby. Navonok sa to prejaví jednoducho tak, že na server sa nemôžete dostať. Prvé písmenko "D" potom predstavuje skratku od slova Distributed, čiže "distribuovaný". V jednoduchosti rozložený na väčšie množstvo užívateľov.

[19] Poznámka autora: Server proxy alebo proxy server je server počítačovej siete, ktorý umožňuje klientom nepriame pripojenie k inému serveru. Proxy server funguje ako sprostredkovateľ medzi klientom a cieľovým serverom, prekladá požiadavky klienta a oproti cieľovému serveru vystupuje ako klient.

bankingu, čísla kreditných kariet).[20] V momente, keď je zariadenie napadnuté botom začína pracovať prakticky autonómne a užívateľ zariadenia o ňom nemá ani tušenie. Infikovaný bot v zariadení vytvorí spojenie s centrálnym uzlom (C&C server), od ktorého vyžiadava inštrukcie ku svojej práci. Ak nedostane hneď potrebné inštrukcie, prepne sa do čakacieho módu a snaží sa nevzbudzovať pozornosť užívateľa zariadenia.

Najčastejším cieľom botnetových útokov je, ako bolo nami už uvedené, finančný sektor. Útočníci získavajú vzdialenú kontrolu nad počítačmi obetí a zbierajú osobné údaje či prihlasovacie heslá, inštalujú a šíria ďalšie typy malvéru. Botnety nastupujú pri DDoS útokoch, v ťažbe kryptomien aj pri ransomvérovej ofenzíve.[21]

Distributed Denial of Service (DDoS)

Distribuovaný útok odmietnutia služby (DDoS) je špeciálny typ útoku odmietnutia služby, ktorý zahltí cieľ alebo súvisiacu infraštruktúru škodlivou prevádzkou. Dosiahnutie je podmienené existenciou robotov, siete počítačov a iných zariadení napadnutých škodlivým softvérom cez vzdialené ovládanie útočníka. Dané vážne obmedzuje šírku pásma a konektivitu, čo vedie k prerušeniu všetkých služieb v sieti.[22] Podstatnou hrozbou sú nadmieru zasiahnuté Cloudové ekosystémy, ktoré trpia maximálnymi stratami v dôsledku úplného odmietnutia služby a degradácie služieb. Primárnym cieľom DDoS útoku je dostupnosť zdrojov pre skutočných používateľov. Škodlivé napadnutia preťažujú sieť, prekračujú jej možnosti šírky pásma a narúšajú služby. Cieľový rozsah sa líši od finančných inštitúcií, poskytovateľov zdravotnej starostlivosti a vládnych agentúr až po nízke kľúčové verejné siete.[23]

DDoS útok je nebezpečný práve z dôvodu, že je ho kvôli jeho podobnosti s legitímnou prevádzkou veľmi náročné rozpoznať. Škodlivý útok z malého počtu uzlov je ľahšie odhaliť a zmierniť. DDoS používa ale často výrazne veľký počet uzlov a kolektívne správanie drasticky prerušuje akúkoľvek šancu na obsluhovanie nezávadných požiadaviek. Kompromitované zariadenia prenášajú veľké množstvo paketov bez akýchkoľvek prestávok cez sieť, čím obeť zavádzajú a snažia sa, aby ich identifikovala ako legitímny prenos. DDoS útoky možno klasifikovať ako útoky hrubou silou, spoofingové útoky a záplavové útoky.

[20] INTERNET BEZPEČNE. 2022. [online]. [cit.2022.05.15.]. Dostupné na internete: https://www.internetembezpecne.cz/internetem-bezpecne/malware/botnet/.
ALISON-GROUP. 2022. [online]. [cit.2022.05.15.]. Dostupné na internete: https://www.alison-group.sk/report-bezpecnosti/botnet-je-tradicny-brutalny-a-funkcny-utok-preco-sa-mu-bude-darit.

[22] AGRAWAL, N., TAPASWI, S. 2019. *Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges.* IEEE Commun. Surv. Tutorials 2019, 21, s. 3769-3795.

[23] BANITALEBI DEHKORDI, A., SOLTANAGHAEI, M. R., BOROUJENI, F. Z. 2020. *The DDoS attacks detection through machine learning and statistical methods in SDN.* J. Supercomput. 2020, s. 1-33.

Záplavové útoky sú z týchto troch najnebezpečnejšie a najzávažnejšie, pretože bránia šírke pásma siete a blokujú všetky legitímne požiadavky. Prístupy prežitia sa zameriavajú na obete jedného cieľa a vyžadujú, aby obete odhalili a zvládli útok samy. Záplava v celej sieti si však vyžaduje zmierňujúce prístupy skôr, ako sa dostane k obetiam, vďaka čomu je vhodná na viacúčelový útok. DDoS nie je možné úplne zablokovať alebo mu úplne zabrániť inštaláciou softvérových opráv a nasadením zariadení. Poskytovatelia internetových služieb preto buď využívajú scrubbingové služby, alebo poskytujú svoje siete.[24]

SQL Injection Attack

SQL je skratka pre Structured Query Language, teda štruktúrovaný jazyk používaný v databázach pre prácu s dátami. SQL príkazy sú používané pre vykonanie príkazov, ktoré menia databázu. Môžu napríklad aktualizovať, získavať alebo pridávať dáta do databázy. Medzi rôzne databázové systémy patria: Oracle, Sybase, Microsoft SQL Server, Access, Ingres a iné. Väčšina SQL príkazov sa skladá zo štandardných príkazov SELECT, INSERT, UPDATE, DELETE, CREATE, ALTER a DROP, ktoré môžu byť použité na každom z vyššie uvedených systémov.[25] „Injekčný útok“ je prvou z 10 najzávažnejších bezpečnostných hrozieb oznámených OWASP[26]. Vďaka rôznym typom a rýchlym variáciám môže „injekcia“ SQL spôsobiť veľké škody siete, čo vedie k úniku údajov a paralýze webových stránok. Kvôli heterogenite zaťaženia útokov, rozmanitosti metód útoku a rôznym režimom útoku je detekcia SQL injekcie stále náročným problémom pretože využíva dizajnové chyby v zle navrhnutých webových aplikáciách. Typy útokov, ktoré je možné vykonať pomocou SQL sa líšia v závislosti od typu databázového zdroja. Útok funguje na dynamických príkazoch SQL. Na vykonanie útoku musí útočník najprv nájsť zraniteľné vstupy používateľov na webovej stránke alebo vo webovej aplikácii. Práve webová stránka alebo webová aplikácia, ktorá má chybu zabezpečenia je úplne najvhodnejšou pre SQL útok. Útočník tak môže vytvárať vstupný obsah. Takýto obsah sa často nazýva škodlivý vklad a je kľúčovou súčasťou útoku. Po odoslaní tohto obsahu útočníkom sa v databáze vykonajú škodlivé príkazy SQL. Dovolíme si poukázať ešte na skutočnosť, že SQL je vyhľadávací jazyk, ktorý bol navrhnutý na správu údajov uložených v relačných databázach a môže sa použiť na prístup, úpravu a vymazanie

[24] KHOOI, X. Z., CSIKOR, L., DIVAKARAN, D. M., KANG, M. S. DIDA. 2020. *Distributed in-Network Defense Architecture against Amplified Reflection DDoS Attacks.* In Proceedings of the 2020 IEEE Conference on Network Softwarization: Bridging the Gap Between AI and Network Softwarization (NetSoft), Ghent, Belgium, 29 June-3 July 2020, s. 277-281.

[25] TECHTARGET. 2022. [online]. [cit.2022.05.15.]. Dostupné na internete: https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

[26] Poznámka autora: OWASP je projekt, ktorý sa zameriava na bezpečnosť webových aplikácií.

údajov. Mnoho webových aplikácií a webových stránok ukladá všetky údaje v databázach SQL. Preto úspešný SQL útok môže mať veľmi vážne následky.

Rootkit

Termín „rootkit“ pozostáva z dvoch nemeckých slov „root“ - najvyšší adresár v systéme súborov, používateľ so všetkými právami správcu a „kit“ - sada. Rootkit je úplne neutrálna zbierka softvérových aplikácií, ktoré môžu používať práva správcu. Keď sa však tieto práva použijú na opätovné načítanie škodlivého softvéru, samotný rootkit sa stane malvérom. Rootkity sú zvyčajne klasifikované podľa hĺbky, v akej pôsobia v súborovom systéme príslušného počítača. Rozoznávame viacero druhov rootkitov. Rootkity používateľského režimu ovplyvňujú hlavne účet správcu v počítači. Malvér má všetky výhody správcovského prístupu k súborom alebo programom a môže napríklad meniť nastavenia zabezpečenia. Rootkity sa automaticky spustia pri každom reštarte počítača. Rootkity modelu jadra fungujú priamo na úrovni operačného systému a majú tak možnosť manipulácie so všetkými oblasťami operačného systému. Aj skenovanie vírusových skenerov môže priniesť nesprávne výsledky, ak je infikovaný rookitom režim jadra. Rootkity jadra však musia prekonať mnoho prekážok, než sa môžu v jadre „ustáliť“. Virtuálne rootkity sa inštalujú na virtuálny počítač a môžu mať prístup k infikovanému počítaču mimo skutočného operačného systému. To sťažuje detekciu softvéru, ktorý sa využíva na ochranu pred vírusmi. Hybridné rootkity rozdeľujú softvér a sú výhodné pre zločincov, pretože fungujú veľmi stabilne na užívateľskej úrovni a zároveň pôsobia v jadre, teda sú skryté. Rootkit je teda softvér určený na skrytie existencie súvisiacich programov pred kontrolou a detekciou pri zachovaní privilegovaného prístupu k cieľovému zariadeniu. Stojí za zmienku, že moderné malvéry často používajú rootkit techniky na pripojenie sa a odomknutie bez toho, aby boli odhalené, čo spôsobuje značné poškodenie počítačov obetí.

Pre jednoduchšie ozrejmenie si dovolíme uviesť, že rootkit, tak ako už bolo spomenuté, dokáže rozvrátiť bezpečnostné alebo antivírusové programy, ktorých cieľom je nájsť ho a preto je mimoriadne ťažké odhaliť ho. V dôsledku toho zisťovanie a práca s rootkitom sa stáva významnou výzvou. Za bežných okolností má každý operačný systém dva režimy a to používateľský režim a režim jadra . Skutočné kódy sa spúšťajú v režime jadra na vykonávanie základných úloh operačného systému počas používania. Tieto kódy sa vykonávajú nepriamo cez aplikačné programové rozhranie (API). Inými slovami, API sa používa v užívateľskom režime na pomoc pri prístupe do režimu jadra namiesto explicitného

spracovania operácií s jadrom.[27] Rootkit sa bežne skrýva v prístupových procesoch v užívateľskom režime a v režime jadra, tak ako sme už uviedli.

Rogue Security Software

Tento typ hrozby je špecifický tým, že navodzuje pocit bezpečnosti a to tak, že upozorňuje na hrozbu, ktorá sa nachádza v elektronickom zariadení. Vybrané antivírusové produkty – tie neškodlivé informujú obete o vírusoch prostredníctvom kontextových správ, iné – tie škodlivé sú navrhnuté tak, aby zobrazovali falošné vírusové správy. Tento známy, nečestný bezpečnostný softvér je rozšíreným problémom pre podniky aj spotrebiteľov.

Rogue Security Software je forma škodlivého softvéru, ktorý je navrhnutý tak, aby prinútil obete domnievať sa, že ich počítač alebo zariadenie je infikované vírusom. Rovnako ako legitímne antivírusové produkty zobrazuje „vyskakovacie" správy s informáciou pre obeť, že jej počítač alebo zariadenie bolo infikované vírusom. Avšak žiadny vírus v zariadení nie je. Nebezpečenstvo Rogue Security Software spočíva v skutočnosti, že zvyčajne nekradne údaje. Namiesto toho je navrhnutý tak, aby obeť oklamal a aby obeť zaplatila za falošnú službu odstránenia vírusu. Po zobrazení falošnej vírusovej správy bude softvér obsahovať pokyny, ako vyčistiť počítač alebo zariadenie. Rogue Security Software žiada, aby si obeť zaplatila za prémiovú službu alebo nástroj na odstránenie vírusu alebo vírusov.[28]

APT Threats

Táto hrozba virtuálneho priestoru je odlišná od predchádzajúcich. Považujeme však za dôležité upriamiť pozornosť aj na túto, veľmi závažnú, hrozbu, ktorá sa síce týka vo väčšine prípadov veľkých firiem, resp. subjektov, ale v konečnom dôsledku aj každého jednotlivca. Pokročilá pretrvávajúca hrozba (APT) je široký pojem, ktorý sa používa na opis útočnej kampane, v ktorej narušiteľ alebo tím narušiteľov vytvorí nezákonnú a dlhodobú prítomnosť v sieti s cieľom získať vysoko citlivé údaje. Ciele týchto útokov, ktoré sa veľmi starostlivo vyberajú a skúmajú zvyčajne zahŕňajú veľké podniky alebo vládne siete. Dôsledky takýchto prienikov sú rozsiahle a zahŕňajú: krádeže duševného vlastníctva (obchodné tajomstvá alebo patenty), ohrozené citlivé informácie (osobné údaje zamestnancov a používateľov), sabotáž kritických organizačných infraštruktúr (vymazanie databázy), či celkové prevzatia stránok. Vykonanie útoku APT vyžaduje viac zdrojov ako útok štandardnej webovej aplikácie. Páchatelia sú zvyčajne spojení do tímov skúsených kyberzločincov, ktorí majú značné

[27] SAHU, A., TARODIA, A., JAGTAP, S., GUNDLA, M., R. 2021. *A Survey on Rootkit Techniques*. In IJIRSET, Volume 10, Issue 5, May 2021, s. 4242-4246.

[28] LOGIXCONSULTING. 2022. [online]. [cit.2022.05.10.]. Dostupné na internete: https://logixconsulting.com/2020/08/24/what-is-rogue-security-software/.

finančné zabezpečenie. Niektoré útoky APT sú financované vládou a používané ako kybernetické vojnové zbrane.[29]

Úspešný APT útok možno rozdeliť do troch etáp: infiltrácia do siete, rozšírenie prítomnosti útočníka a extrakcia zhromaždených údajov. Infiltrácia zvyčajne prebieha prostredníctvom ohrozenia jedného z troch útočných plôch: webových aktív, sieťových zdrojov alebo autorizovaných ľudských používateľov. Dosahuje sa to buď prostredníctvom škodlivého nahrávania, napr. prostredníctvom spomínaného SQL injection alebo útokmi sociálneho inžinierstva, napr. spear phishing, teda hrozbám, ktorým veľké organizácie pravidelne čelia. Okrem toho môžu „infiltrátori" súčasne vykonať proti svojmu cieľu, už spomínaný, DDoS útok. Ten slúži ako dymová clona na rozptýlenie personálu siete a ako prostriedok na oslabenie bezpečnostného perimetra, čo uľahčuje jeho prelomenie. Po dosiahnutí počiatočného prístupu útočníci rýchlo nainštalujú „backdoor shell", čiže malvér, ktorý poskytuje prístup k sieti a umožňuje vzdialené, utajené operácie. V druhej fáze po vytvorení opory sa útočníci presunú, aby rozšírili svoju prítomnosť v sieti. Zahŕňa to posun v hierarchii organizácie nahor a ohrozenie prístupu zamestnancov k najcitlivejším údajom. Pritom sú schopní zhromažďovať dôležité obchodné informácie vrátane informácií o produktových radoch, údajoch o zamestnancoch a finančných záznamoch. V závislosti od konečného cieľa útoku môžu byť nazhromaždené údaje predané konkurenčnému podniku, pozmenené tak, aby sabotovali produktovú radu spoločnosti alebo použité na zničenie celej organizácie. Ak je motívom sabotáž, táto fáza sa používa na nenápadné získanie kontroly nad viacerými kritickými funkciami a manipuláciu s nimi v špecifickom poradí, aby spôsobili maximálne poškodenie. Útočníci by napríklad mohli vymazať celé databázy v rámci spoločnosti a následne narušiť sieťovú komunikáciu, aby predĺžili proces obnovy. Fáza extrakcie – v čase, kým prebieha udalosť APT ukradnuté informácie sú zvyčajne uložené na bezpečnom mieste vo vnútri napadnutej siete. Po zhromaždení dostatočného množstva údajov ich následne zločinci extrahujú.[30] Po extrakcii ich využijú na vopred naplánované ciele.

Po charakterizácii jednotlivých hrozieb si dovolíme smerovať našu pozornosť na špecifikáciu samotného pojmu „počítačový bezpečnostný incident". Konáme tak z dôvodu, že všetky spomínané hrozby sú počítačovými bezpečnostnými incidentmi a preto je potrebné ich jasne a zreteľne vymedziť. Taktiež aj samotné orgány činné v trestnom konaní sa

[29] IMPERVA. 2022. [online]. [cit.2022.05.10.]. Dostupné na internete: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.

[30] IMPERVA. 2022. [online]. [cit.2022.05.10.]. Dostupné na internete: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.

stretávajú pri svojej každodennej činnosti s týmto pojmom a preto máme za to, že je vhodné poukázať na dané a vymedziť jeho základné atribúty, okrem iného, pre zabezpečenie efektívnosti ich činnosti aj v prípravnom konaní.

Počítačový bezpečnostný incident a legislatíva informačnej bezpečnosti v Slovenskej republike a v Európskej únii

Zásadným pojmom pre oblasť kybernetickej bezpečnosti je „bezpečnostný incident". V zmysle § 3 písm. k) Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov sa kybernetickým bezpečnostným incidentom rozumie akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je: strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby, vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo ohrozenie bezpečnosti informácií. Konštatujeme, že právna úprava v oblasti ochrany osobných údajov explicitne neupravuje definíciu bezpečnostného incidentu, ale poukazuje na nutnosť jeho riešenia. V obsahu Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušila Smernica 95/46/ES sa spomínajú tímy na riešenie bezpečnostných incidentov a ich činnosť ako súčasť zabezpečenia ochrany osobných údajov. Počítačový bezpečnostný incident môžeme definovať aj ako „porušenie alebo bezprostrednú hrozbu porušenia pravidiel počítačovej bezpečnosti, prijateľných zásad používania alebo štandardných bezpečnostných postupov"[31].

Kľúčové faktory, ktoré v jednoznačnej miere ovplyvňujú dopady hrozieb vo virtuálnom prostredí na štruktúry štátov, či v konečnom dôsledku jednotlivcov, sú možnosti ich eliminácie. Medzi tieto možnosti patria určite aj legislatívne podporné piliere, ktoré zabezpečujú jednotný postup a multiinštitucionálny prístup k riešeniu hrozieb. Na národnej úrovni, v rámci kybernetickej bezpečnosti, sú veľmi dôležitými a kľúčovými dokumentmi Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, Národná stratégia a Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na

[31] CICHONSKI P. et al. 2012. *Computer security incident handling guide*. NIST Special Publication, 2012, s. 138-147.

roky 2021 až 2025. Národnú stratégiu kybernetickej bezpečnosti na roky 2021 až 2025 schválila vláda Slovenskej republiky 7. januára 2021 uznesením č. 5/2021. Ide o východiskový strategický dokument, ktorý komplexne určuje strategický prístup Slovenskej republiky k zabezpečeniu kybernetickej bezpečnosti. Národnú stratégiu vypracoval Národný bezpečnostný úrad, na jej príprave sa podieľali aj ostatné zainteresované ministerstvá a ústredné orgány štátnej správy. Dokument ponúka ucelený koncept riadenia informačnej a kybernetickej bezpečnosti. Reflektuje strategické smerovanie štátu v oblasti bezpečnosti, zohľadňuje princípy Bezpečnostnej stratégie SR, vychádza aj zo strategických dokumentov NATO, EÚ, OECD a OSN. Národná stratégia je určená pre všetky subjekty, ktoré sa podieľajú na budovaní systému kybernetickej bezpečnosti. Na základe jasných princípov určuje strategické ciele a má ambíciu moderným spôsobom reagovať na aktuálne a perspektívne bezpečnostné hrozby. V nadväznosti na národnú stratégiu bude nasledovať príprava a predloženie akčného plánu jej realizácie. V ňom budú jasné konkrétne časové, vecné, ale aj finančné kritéria rozvoja kybernetickej bezpečnosti na v Slovenskej republike. Bude obsahovať aj úlohy pre jednotlivé ústredné štátne orgány v medziach ich kompetencií a prípadné vplyvy, ktoré prinesie nová alebo upravená legislatíva.[32]

ISO/IEC normy radu 27000 predstavujú medzinárodné štandardy v oblasti riadenia informačnej bezpečnosti odvodené od britských štandardov radu BS 7799. Samotné normy alebo viac informácií o nich je možné získať na webovom sídle Medzinárodnej organizácie pre štandardizáciu ISO. Európska komisia a Európska služba pre vonkajšiu činnosť v decembri 2020 predstavili nový Document 52013JC0001 Stratégiu kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor. Cieľom tejto stratégie je posilniť odolnosť Európy voči kybernetickým hrozbám a zabezpečiť, aby všetci občania a podniky mohli v plnej miere využívať dôveryhodné a spoľahlivé služby a digitálne nástroje. Nová stratégia obsahuje konkrétne návrhy na zavedenie regulačných, investičných a politických nástrojov.[33]

Rada 22. marca 2021 prijala závery o stratégii kybernetickej bezpečnosti, v ktorých zdôrazňuje, že kybernetická bezpečnosť má zásadný význam pre budovanie odolnej, zelenej a digitálnej Európy. Ministri Európskej únie za kľúčový cieľ stanovili dosiahnuť strategickú autonómiu a zároveň zachovať otvorené hospodárstvo. V rámci toho chce EÚ posilniť svoju

[32] NBÚ. 2021. [online]. [cit.2022.05.12.]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Strategia_kybernetickej_bezpecnosti_2021.pdf.

[33] CSIRT. 2022. [online]. [cit.2022.05.12.]. Dostupné na internete: https://www.csirt.gov.sk/prehlad-standardov-iso-iec-27000.html.

schopnosť prijímať autonómne rozhodnutia týkajúce sa kybernetickej bezpečnosti, aby si upevnila vedúce postavenie v digitálnej oblasti a strategické kapacity.[34] Európska únia prijíma opatrenia na riešenie výziev v oblasti kybernetickej bezpečnosti, ktorých cieľom je posilniť kybernetickú odolnosť, bojovať proti počítačovej kriminalite, posilniť diplomaciu v oblasti kybernetickej bezpečnosti, posilniť kybernetickú obranu, posilniť výskum, inováciu a ochrániť kritickú infraštruktúru. Európska únia pracuje v súčasnosti aj na dvoch legislatívnych návrhoch na riešenie súčasných a budúcich „online" a „offline" rizík a to na aktualizácii Smernice na lepšiu ochranu sietí a informačných systémov a novej Smernici o odolnosti kritických subjektov.[35] Uvádzané prepojenie národnej a nadnárodnej legislatívy považujeme za veľmi dôležité pre čo najefektívnejší boj s aktuálnymi hrozbami interakcií vo virtuálnom svete.

Záver

Máme za to, že identifikácia hrozieb, skúmanie a reflektovanie na ich inovatívne postupy a snaha o ich elimináciu je kľúčovým postupom boja proti aktuálnym hrozbám interakcií vo virtuálnom svete. I v rámci procesu úkonov a postupov prípravného konania je bezpodmienečne potrebné, aby orgány činné v trestnom konaní mali potrebné znalosti pre uplatnenie čo najefektívnejšieho postupu pri skúmaní, hodnotení kritérií a vplyvu legislatívnych zmien aj v rámci hrozieb vo virtuálnom svete. Dodržiavanie základných ľudských práv a slobôd všetkých subjektov zúčastnených v rámci prípravného konania môžeme taktiež považovať za jeden z jeho najdôležitejších aspektov, ktorý priamo ovplyvňuje nie len zákonnosť získavania dôkazov, ale aj celkovú úspešnosť spravodlivého rozhodnutia v trestnej veci.[36] Preto je poznanie kľúčových synopsií spojených s danou problematikou bezpodmienečne potrebné. Pretože ak chceme skúmať efektívnosť práva alebo akéhokoľvek systému musíme definovať nevyhnutne podmienky (predpoklady), ktoré umožňujú uvažovať o tom, že skúmanie efektivity systému ma vôbec nejaký zmysel.[37]

---

[34] CONSILIUM EUROPA. 2021. [online]. [cit.2022.05.10.]. Dostupné na internete: https://www.consilium.europa.eu/sk/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/.

[35] CONSILIUM EUROPA. 2022. [online]. [cit.2022.05.12.]. Dostupné na internete: https://www.consilium.europa.eu/sk/policies/cybersecurity/.

[36] DRUGDA, J. 2022. Špecifické dôkazné prostriedky ako nevyhnutné zásahy do základných ľudských práv a slobôd. In DRUGDA, J. eds. 2022. *Vyšetrovanie a dokazovanie prostredníctvom špecifických dôkazných prostriedkov.* Bratislava: Akadémia Policajného zboru v Bratislave, s. 43-49.

[37] ČENTÉŠ, J., VOJTUŠ, F. 2021. *Efektívnosť práva a prístupy k jej skúmaniu.* In ČENTÉŠ, J. (ed.) a kol.: „Efektívnosť prípravného konania – jej skúmanie, výzvy a perspektívy", Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2020, s. 28-42.

Zoznam použitej literatúry

ABROSHAN, H., DEVOS, J., POELS, G., LAERMANS, E. 2017. Phishing attacks root causes. Proc. Int. Conf. Risks Secur. Internet Syst., s. 187-202.

AGRAWAL, N., TAPASWI, S. 2019. Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges. IEEE Commun. Surv. Tutorials 2019, 21, s. 3769-3795.

Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025.

ALISON-GROUP. 2022. [online]. [cit.2022.05.15.]. Dostupné na internete:https://www.alison-group.sk/report-bezpecnosti/botnet-je-tradicny-brutalny-a-funkcny-utok-preco-sa-mu-bude-darit.

APWG. 2018. Phishing activity trends report 3rd quarter. 2018, s. 1–11.

BANITALEBI DEHKORDI, A., SOLTANAGHAEI, M. R., BOROUJENI, F. Z.2020. The DDoS attacks detection through machine learning and statistical methods in SDN. J. Supercomput. 2020, s. 1-33.

Bezpečnostní strategie Českej republiky. 2003. [online]. [cit.2022.05.22.]. Dostupné na internete:https://mocr.army.cz/images/Bilakniha/CSD/2003%20Bezpecnostni%20strategie%20CR.pdf.

CICHONSKI P. et al. 2012. Computer security incident handling guide. NIST Special Publication, 2012, s. 138-147.

CONSILIUM EUROPA. 2021.[online]. [cit.2022.05.10.]. Dostupné na internete: https://www.consilium.europa.eu/sk/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/.

CONSILIUM EUROPA. 2022. [online]. [cit.2022.05.12.]. Dostupné na internete: https://www.consilium.europa.eu/sk/policies/cybersecurity/.

CSIRT. 2022. [online]. [cit.2022.05.12.]. Dostupné na internete: https://www.csirt.gov.sk/prehlad-standardov-iso-iec-27000.html.

Document 52013JC0001 Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor.

DRUGDA, J. 2022. Špecifické dôkazné prostriedky ako nevyhnutné zásahy do základných ľudských práv a slobôd. In DRUGDA, J. eds. 2022. Vyšetrovanie a dokazovanie prostredníctvom špecifických dôkazných prostriedkov. Bratislava: Akadémia Policajného zboru v Bratislave, s. 43-49. ISBN 978-80-8054-932-9.

ČENTÉŠ, J., VOJTUŠ, F. 2021. Efektívnosť práva a prístupy k jej skúmaniu. In ČENTÉŠ, J. (ed.) a kol.: „Efektívnosť prípravného konania – jej skúmanie, výzvy a perspektívy“, Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2020, s. 28-42. ISBN 978-80-7160-577-5.

ESET. 2022. [online]. [cit.2022.05.16.]. Dostupné na internete: https://www.eset.com/sk/blog/domaca-it-bezpecnost/ako-rozpoznat-phishing/.

IBM. 2022. [online]. [cit.2022.05.20.]. Dostupné na internete:https://www.ibm.com/topics/cyber-attack.

IGI GLOBAL. 2015. [online]. [cit.2022.05.22.]. Dostupné na internete: https://www.igi-global.com/chapter/internet-identity-and-the-right-to-be-forgotten/131357.

IMPERVA. 2022. [online]. [cit.2022.05.10.]. Dostupné na internete: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.

INTERNET BEZPEČNE. 2022. [online]. [cit.2022.05.15.]. Dostupné na internete: https://www.internetembezpecne.cz/internetem-bezpecne/malware/botnet/.

ISO/IEC normy radu 27000.

KHOOI, X. Z., CSIKOR, L., DIVAKARAN, D. M., KANG, M. S. DIDA. 2020. Distributed in-Network Defense Architecture against Amplified Reflection DDoS Attacks. In Proceedings of the 2020 IEEE Conference on Network Softwarization: Bridging the Gap Between AI and Network Softwarization (NetSoft), Ghent, Belgium, 29 June-3 July 2020, s. 277-281.

KIRDA, E., KRUEGEL, C. 2005. Protecting users against phishing attacks with AntiPhish. Proc. - Int. Comput. Softw. Appl. Conf. 1, s. 517–524.

KURILOVSKÁ, L., HAJDÚKOVÁ, T. 2021. Hodnotenie efektívnosti prípravného konania pri prečinoch v kontexte objasnenosti a regionálnych disparít na území Slovenskej republiky. In ČENTÉŠ, J. (ed.) a kol.: „Efektívnosť prípravného konania – jej skúmanie, výzvy a perspektívy“, Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2020, s. 74-85. ISBN 978-80-7160-577-5.

LOGIXCONSULTING. 2022. [online]. [cit.2022.05.10.]. Dostupné na internete: https://logixconsulting.com/2020/08/24/what-is-rogue-security-software/.

MALWAREBYTES. 2022. [online]. [cit.2022.05.15.]. Dostupné na internete: https://www.malwarebytes.com/computer-virus.

MANSFIELD-DEVINE, S. 2011. Hacktivism: assessing the damage. In Network Security Volume 2011, Issue 8, August 2011, s. 5-13. ISSN: 1353-4858.

MERWE, A., MARIANNE, L., MAREK, D. 2005. Characteristics and responsibilities involved in a Phishing attack. In WISICT ’05: proceedings of the 4th international symposium on information and communication technologies. Trinity College Dublin, s. 249–254.

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov.

Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025.

NBÚ. 2021. [online]. [cit.2022.05.12.]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Strategia_kybernetickej_bezpecnosti_2021.pdf.

ÖMER, A., REFIK,S. 2020. A Comprehensive Review on Malware Detection Approaches. In IEEE Access, Volume: 8, 2020, s. 6249 - 6271. ISSN 2169-3536.

ROGERS, M. K. 2011. The psyche of Cybercriminals: A Psycho-Social Perspective. In Ghosh, S., Turrini, E. (eds.), Cybercrimes: A multidisciplinary Analysis. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13547-7_14.

SAHU, A., TARODIA, A., JAGTAP, S., GUNDLA, M., R. 2021. A Survey on Rootkit Techniques. In IJIRSET, Volume 10, Issue 5, May 2021, s. 4242-4246. e-ISSN 2319-8753.

Smernica 95/46/ES.

TECHTARGET. 2022. [online]. [cit.2022.05.15.]. Dostupné na internete: https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

VELECOR. 2022. [online]. [cit.2022.05.15.]. Dostupné na internete: https://mocr.army.cz/images/Bilakniha/CSD/2003%20Bezpecnostni%20strategie%20CR.pdf.https://velecor.com/10-common-internet-security-threats-and-how-to-avoid-them/.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

ZHANG, G. Gu, J., BOTSNIFFER, W. Lee, 2008. Detecting botnet command and control channels in network traffic. In NDSS, 2008.

Kontaktné údaje

npor. JUDr. Patrícia Krásná, PhD., LL.M.

Katedra vyšetrovania

Akadémia Policajného zboru v Bratislave

patricia.krasna@akademiapz.sk

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

PhDr. Peter Veselý, PhD.

Identifikácia názorových postojov prostredníctvom dostupných vizuálnych prvkov na sociálnej sieti Facebook

Martin Kuchta – Peter Červenka

Abstrakt

Hlavným cieľom príspevku je identifikácia a kvantifikácia reakcií vyjadrených vizuálnym elementom pod článkovými príspevkami vybraného spravodajského média na sociálnej sieti Facebook. V prvom kroku výskumu bolo identifikovaných päť článkov, ktoré za obdobie jedného mesiaca mali spolu najviac reakcií. Druhým krokom bola identifikácia emotikonov a ich charakteristika. Posledným krokom výskumu bola kvantifikácia počtu jednotlivých emotikonov vyjadrených pri analyzovaných článkových príspevkoch. Sledované bolo predovšetkým obsahové zameranie príspevkov a vplyv témy príspevku na počet konkrétnych emotikonov. Výsledky výskumu odhaľujú výrazný vplyv obsahového zamerania príspevku na počet a vzájomný pomer jednotlivých emotikonov a čiastočne identifikujú témy s najsilnejším polarizačným efektom.

Abstract

The main goal of the paper is the identification and quantification of the reactions expressed by the visual element under the article post of the selected news media on the Facebook social network. In the first step of the research, five articles were identified, which together had the most reactions over a period of one month. The second step was the identification of emoticons and their characteristics. The last step of the research was the quantification of the number of individual emoticons expressed in the analyzed article posts. Mainly, the content focus of the posts and the influence of the topic of the post on the number of specific emoticons were monitored. The research results reveal a significant impact of the content focus of the post on the number and mutual ratio of individual emoticons and partially identify the topics with the strongest polarizing effect.

Key words

emotikon, názor, postoj, sociálne siete

Úvod

Neustále rastúca penetrácia internetu a technologický vývoj spôsobili vytvorenie nových podmnožín internetu. Za takúto podmnožinu možno označiť aj sociálne siete, ktoré mali na marketingovú komunikáciu a diverzifikáciu komunikácie firiem minimálne tak významný vplyv ako internet samotný (Europarl, 2021). Jedným z najvýraznejších špecifík sociálnych sietí oproti iným komunikačným kanálom je možnosť používateľa interakcie s obsahom. Expanzia informačno-komunikačných technológií a digitalizácia tradičných typov médií majú signifikantný vplyv na produkciu, šírenie a v konečnom dôsledku celkové vnímanie informácií (Pow & Li, 2015). Internetové prostredie už od svojich počiatkov vyvíja tlak na

producentov obsahu, ktorí sú nútení tvoriť obsah rýchlo a aktuálne, aby prilákali čo najviac čitateľov a monetizovali reklamný mediálny priestor (Berger et al., 2015). Uvedené má za následok pretlak informácií. Tlak na rýchlu tvorbu obsahu médií a snaha používateľov internetu byť stále informovaní spôsobili, že čitatelia konzumujú internetový obsah vo vysokej frekvencii a pravidelne, avšak často bez rozlišovania pôvodu informácie (Vamanu & Zak, 2022). V súčasnej dobe sociálne siete čelia akejsi transformácii používateľského správania. Zatiaľ čo v minulosti používatelia sociálnych sietí ich vnímali ako priestor na sebaprezentáciu, konzumáciu obsahu a komunikáciu v súčasnej dobe ich vnímajú ako priestor na vyjadrenie osobných postojov, názorov, či dokonca ako priestor na presviedčanie o vlastných názoroch a postojoch (Housley et al., 2018). Mnoho používateľov sa postupom času naučilo vytvárať svojimi príspevkami a komentármi náladu, ktorou ovplyvňujú ďalších používateľov, ktorí vytvorený obsah konzumujú (Edwards et al., 2013). Sociálne siete poskytujú hneď niekoľko možností ako vyjadriť názor alebo stotožnenie s konzumovaným obsahom. Napríklad sociálna sieť Facebook umožňuje používateľom interakciu s príspevkom v dvoch formách:

- komentovanie príspevku
- použitie emotikona.

V prvom prípade používateľ napíše pod príspevok na sociálnej sieti textový komentár, ktorý môže obsahovať vizuálne prvky vo forme emotikonov, gif obrázkov, dokonca aj videí. V druhom prípade ide o použitie emotikona, ktorý sa zobrazuje priamo pri príspevku a používateľ ho môže použiť bez nutnosti písania textového komentára (Piliapp, 2021). Emotikony slúžia ako efektívny ukazovateľ emócií používateľa. Je však veľmi dôležité pred dedukciou emócie používateľa dôsledne analyzovať emotikona, pretože smejúci sa emotikon nemusí nutne znamenať dobrú náladu používateľa, avšak môže indikovať výsmech (Brito et al., 2019). Podľa typu použitého emotikona možno odhadnúť náladu používateľa v čase, keď emotikon použil.

Hlavným cieľom tohto príspevku je identifikovať a prostredníctvom kvantifikácie analyzovať reakcie vo forme emotikonov pod článkovými príspevkami vybraného spravodajského média. V prvom kroku výskumu bolo identifikovaných päť článkov, ktoré za obdobie jedného mesiaca mali spolu najviac reakcií. Tieto články boli zaznamenané v prehľadnej tabuľke. Ďalším krokom bola identifikácia emotikonov. V čase výskumu mohli používatelia sociálnej siete Facebook vyjadriť emóciu alebo postoj spojený s článkovým príspevkom

prostredníctvom šiestich emotikonov, ktorí sú uvedení a definovaní ďalej v texte. Posledným krokom výskumu bolo kvantifikovať počet jednotlivých emotikonov vyjadrených pri analyzovaných článkových príspevkoch. Sledované bolo predovšetkým obsahové zameranie príspevkov a vplyv témy príspevku na počet konkrétnych emotikonov.

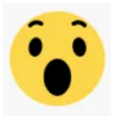
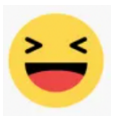
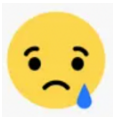
1 Výsledky a diskusia

Na Facebook profile internetového spravodajského média Aktuality.sk, ktorý bol identifikovaný ako predmet výskumu tohto článku, bolo identifikovaných päť spravodajských článkov, ktoré mali v skúmanom období najvyšší počet interakcií. Analýza prebehla na týchto článkových príspevkoch:

- *Článok 1*: Anonymous odstavili televíziu RT, rovnako zasiahli viaceré weby vládnych orgánov.
- Článok 2: Slovenskí hokejisti postupujú do semifinále!
- Článok 3: Výzvy ruského prezidenta Vladimíra Putina na zastavenie vojenskej operácie... .
- Článok 4: Ministar Obrany J. Naď po rokovaní s ministrom obrany USA L. Austinom.
- Článok 5: Drucker vyzýva, aby tí, ktorí zmluvu spochybňujú, ukázali jednu krajinu... .

V realizovanom výskume boli skúmané predovšetkým reakcie na článkové príspevky vo forme emotikonov, ktoré vyjadrujú jednu z vybraných emócií. V čase výskumu bolo dostupných 6 rôznych emotikonov. Pre ilustráciu sú znázornení v nasledujúcej tabuľke.

Tabuľka 1 Ukážka emotikonov, ktorými možno reagovať na príspevky na sociálnej sieti Facebook

					
Palec hore	Srdiečko	Začudovaný	Smejúci sa	Plačlivý	Nahnevaný

Zdroj: vlastné spracovanie podľa Facebook.com

Vysvetlenie emotikonov, ktorými možno reagovať na príspevky na sociálnej sieti Facebook.

- *Pale hore* – jeho použitie označuje súhlasné stanovisko s obsahom príspevku.
- *Srdiečko* – jeho použitie označuje stotožnenie sa s obsahom príspevku.
- *Začudovaný* – jeho použitie označuje prekvapenie alebo pobúrenie vyvolané obsahom príspevku.
- *Smejúci sa* – jeho použitie označuje pobavenie alebo výsmech vyvolaný obsahom príspevku.
- *Plačlivý* – jeho použitie označuje ľútosť alebo sklamanie vyvolané obsahom príspevku.
- *Nahnevaný* – jeho použitie označuje rozhorčenie, pobúrenie alebo nesúhlas vyvolaný obsahom príspevku.

Uvedené emotikony môžu mať niekoľko významov, ktorý môže pri rôznych používateľoch znamenať rôzne emócie. Rámcovo však možno chápať palec hore ako stotožnenie, srdiečko ako súhlas, začudovanie ako rozhorčenie, smiech ako pobavenie, plačlivosť ako sklamanie a nahnevanosť ako pobúrenie. Emotikony tak do veľkej miery dokážu indikovať emočný stav používateľa vyvolaný konzumáciou obsahu príspevku.

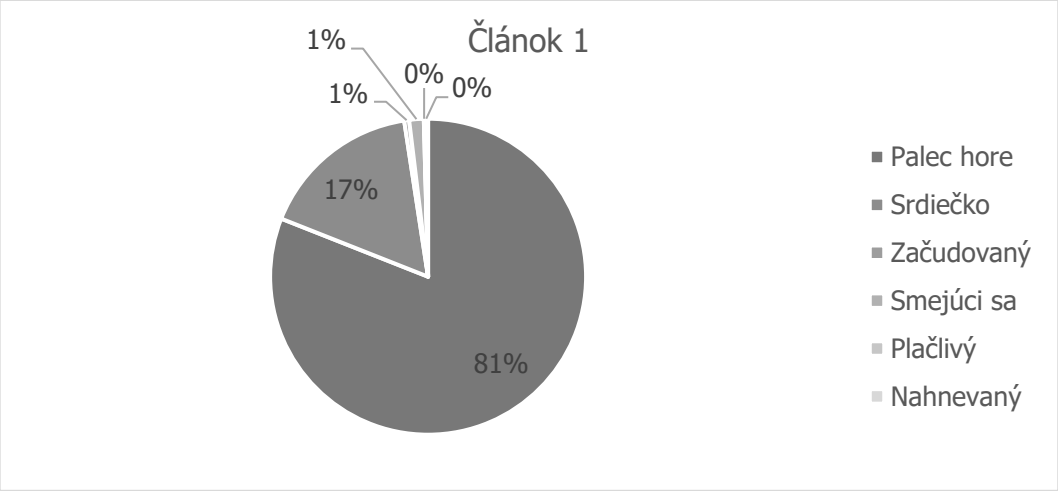
Tabuľka 2 Počet interakcií prostredníctvom emotikona na vybraných článkových príspevkoch na sociálnej sieti Facebook spravodajského média Aktuality.sk

	Článok 1	**Článok 2**	**Článok 3**	**Článok 4**	**Článok 5**
Palec hore	8052	5269	5833	890	2904
Srdiečko	1649	1666	1055	129	106
Začudovaný	50	9	10	47	186
Smejúci sa	148	4	44	682	888
Plačlivý	6	0	4	53	8
Nahnevaný	37	0	2	2701	641
Spolu	**9942**	**6948**	**6948**	**4502**	**4733**

Zdroj: vlastné spracovanie

Uvedená tabuľka skúmala počet identifikovaných a definovaných emotikonov pri analyzovaných článkových príspevkoch na Facebook profile spravodajského portálu Aktuality.sk. Získané údaje sú interpretované vo vizuálnej podobe prostredníctvom koláčových grafov za účelom rýchlejšieho a efektívnejšieho pochopenia dosiahnutých výsledkov.

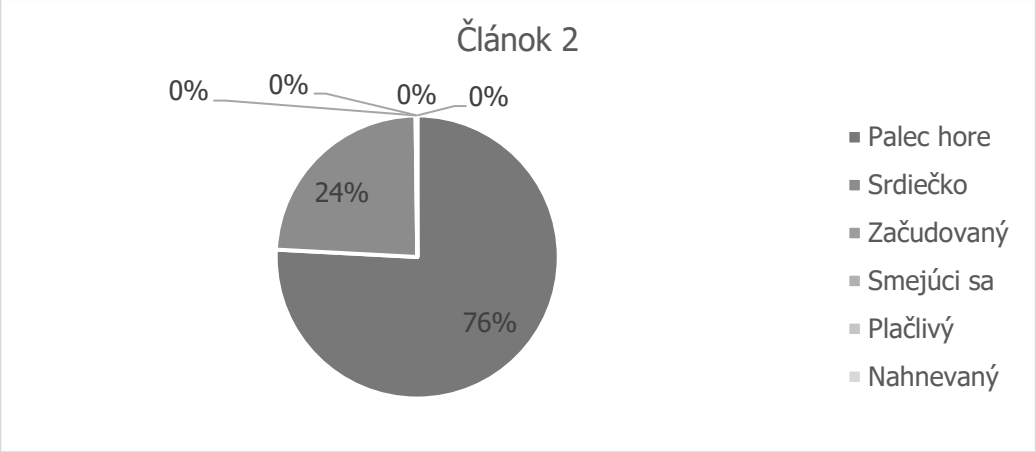
Graf 1 Vizualizácia počtu dosiahnutých interakcií vo forme emotikona na prvom analyzovanom článku na Facebook profile spravodajského média Aktuality.sk



Zdroj: vlastné spracovanie

Prvý analyzovaný článok s názvom „Anonymous odstavili televíziu RT, rovnako zasiahli viaceré weby vládnych orgánov“ získal 8052 palcov hore, 1649 srdiečok, 50 začudovaných, 148 smejúcich sa, 6 plačlivých a 37 nahnevaných emotikonov. Téma článku má spoločenský presah, pojednáva o prebiehajúcom konflikte a reakcie vyjadrené prostredníctvom emotikonov indikujú, že čitatelia so správou súhlasia, stotožňujú sa s ňou a sympatizujú s opísanou aktivitou. Napriek tomu, že prebiehajúci vojnový konflikt je polarizujúca téma získal príspevok takmer výhradne emotikony vyjadrujúce pozitívny postoj k správe a len minimum emotikonov vyjadrujúcich negatívny postoj k správe.

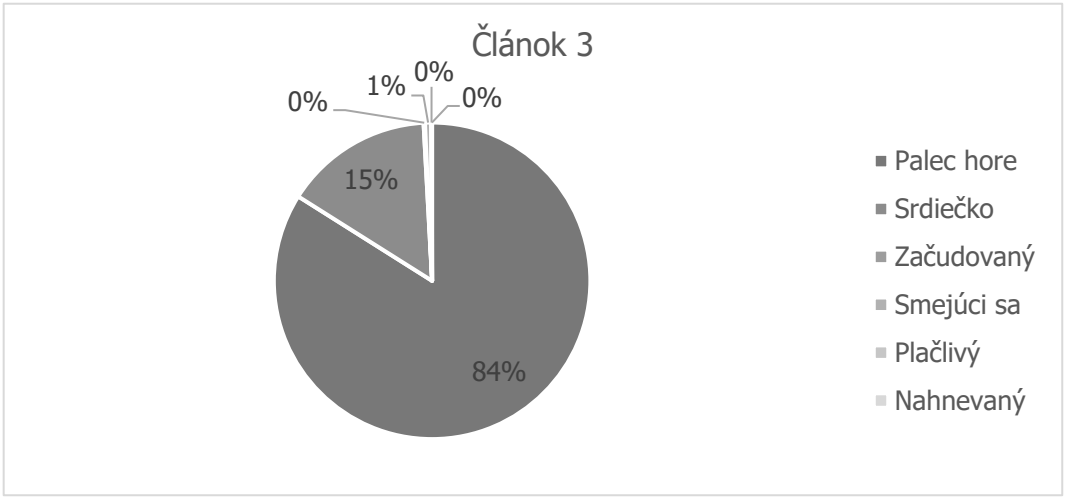
Graf 2 Vizualizácia počtu dosiahnutých interakcií vo forme emotikona na druhom analyzovanom článku na Facebook profile spravodajského média Aktuality.sk



Zdroj: vlastné spracovanie

Druhý analyzovaný článkový príspevok s názvom „Slovenskí hokejisti postupujú do semifinále!“ získal 5269 palcov hore, 1666 srdiečok, 9 začudovaných, 4 smejúcich sa, 0 plačlivých a 0 nahnevaných emotikonov. Článok bol tematický zameraný na šport, konkrétne na hokej. Slovensko ako hokejová krajina má k tejto tematike výrazne pozitívny postoj, čo sa odrazilo aj na skladbe získaných emotikonov, ktorí boli výlučne pozitívneho charakteru.

Graf 3 Vizualizácia počtu dosiahnutých interakcií vo forme emotikona na treťom analyzovanom článku na Facebook profile spravodajského média Aktuality.sk

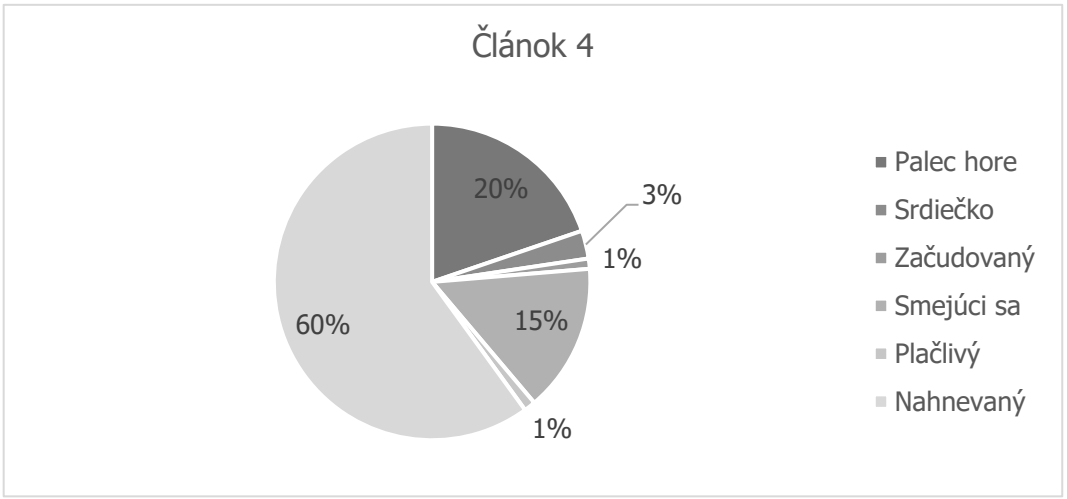


Zdroj: vlastné spracovanie

Tretí analyzovaný článkový príspevok s názvom „Výzvy ruského prezidenta Vladimíra Putina na zastavenie vojenskej operácie..“ získal 5833 palcov hore, 1055 srdiečok, 10 začudovaných,

44 smejúcich sa, 4 plačlivých a 2 nahnevaných emotikonov. Prebiehajúci vojnový konflikt a informácie, ktoré načrtávali jeho ukončenie vyvolávali pozitívne reakcie u používateľov, ku ktorým sa tento príspevok dostal. Používatelia sa s príspevkom a jeho znením stotožňovali a prostredníctvom nepomerne veľkého počtu emotikonov vo forme palca hore a srdiečka vyjadrovali svoj súhlasný postoj s článkom.

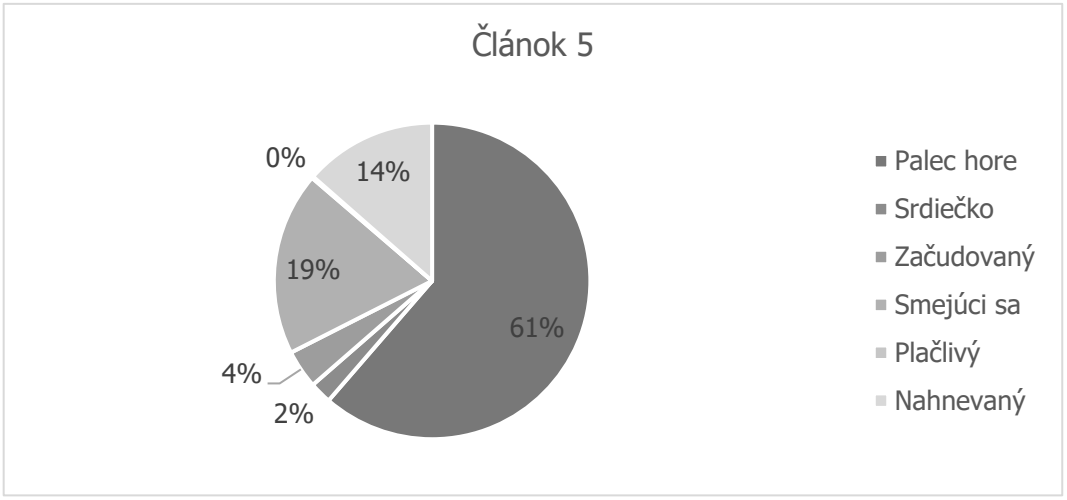
Graf 4 Vizualizácia počtu dosiahnutých interakcií vo forme emotikona na štvrtom analyzovanom článku na Facebook profile spravodajského média Aktuality.sk



Zdroj: vlastné spracovanie

Štvrtý analyzovaný článkový príspevok s názvom „Minister Obrany J. Naď po rokovaní s ministrom obrany USA L. Austi....“ získal 890 palcov hore, 129 srdiečok, 47 začudovaných, 682 smejúcich sa, 53 plačlivých a 2701 nahnevaných emotikonov. Politická téma vyvolala rozporuplné reakcie a polarizovala používateľov, ku ktorým sa článkový príspevok dostal. Polarizácia nebola spôsobená príspevkom samotným ale jeho témou. Existuje predpoklad, že akákoľvek politická téma by vyvolala rovnakú reakciu.

Graf 5 Vizualizácia počtu dosiahnutých interakcií vo forme emotikona na piatom analyzovanom článku na Facebook profile spravodajského média Aktuality.sk



Zdroj: vlastné spracovanie

Piaty analyzovaný článok s názvom „Drucker vyzýva, aby tí, ktorí zmluvu spochybňujú, ukázali jednu krajinu...“ získal 2904 palcov hore, 106 srdiečok, 186 začudovaných, 888 smejúcich sa, 8 plačlivých a 641 nahnevaných emotikonov. Podobne ako pri štvrtok analyzovanom článku aj tento pojednával o politickej téme. To sa prejavilo aj v názorovej polarizácii prijímateľov správy a tento príspevok dosiahol značné množstvo negatívnych emotikonov, ktorý prezentujú rozhorčenie alebo nesúhlas s článkom, alebo s informáciou, ktorú sa čitateľ v článku dozvedel.

Záver

Internet a predovšetkým sociálne siete a diskusné fóra vytvorili priestor pre interakciu s obsahom, ktorý používateľ konzumuje. Formy interakcie sú rôzne avšak najčastejšie využívané sú formou textovej správy alebo formou grafického znázornenia formou emotikonov. Predovšetkým sociálne siete v súčasnej dobe čelia obvineniam, že sa z nich stalo miesto plné nenávisti a šírenia neznášanlivých správ. Internet je zatiaľ regulovaný iba veľmi obmedzene, čo spôsobilo, že jeho používatelia vyjadrujú názor často bez rozmyslu a bez následkov. Používatelia na sociálnych sieťach používajú často vyjadrenia, ktoré by v reálnom svet nikdy nezverejnili. Hlavným cieľom príspevku je identifikovať a prostredníctvom kvantifikácie analyzovať reakcie vo forme emotikonov pod článkovými príspevkami vybraného spravodajského média. Výskumom bolo zistené, že obsahové zameranie príspevku na sociálnej sieti má vplyv na zloženie vyjadrených emotikonov, a že témy alebo oblasti, ktoré

sú politicky orientované majú vyššiu tendenciu polarizovať názory používateľov. Limitáciou príspevku je tematická homogénnosť analyzovaných príspevkov na sociálnej sieti. Analyzované príspevky sú výhradne politického alebo športového charakteru. Ďalšou limitáciou je absencia analýzy vnímania používaných emotikonov. Teoretický rešerš naznačuje, že použitie rovnakého emotikonu môže mať pre rôznych používateľov rôzny význam. Pre budúci výskum odporúčame analyzovať vnímanie jednotlivých emotikonov rôznymi používateľmi, priradiť jednotlivých emotikonom význam a využiť rovnakú metodológiu, avšak aplikovanú na tematicky širšie spektrum príspevkov.

Zoznam použitej literatúry

Berger, B., Matt, C., Steininger, D. M., & Hess, T. (2015). It Is Not Just About Competition with "Free": Differences Between Content Formats in Consumer Preferences and Willingness to Pay. Journal of Management Information Systems, 32(3), 105–128. https://doi.org/10.1080/07421222.2015.1095038

Brito, P. Q., Torres, S., & Fernandes, J. (2019). What kind of emotions do emoticons communicate? Asia Pacific Journal of Marketing and Logistics, 32(7), 1495–1517. https://doi.org/10.1108/APJML-03-2019-0136

Edwards, A., Housley, W., Williams, M., Sloan, L., & Williams, M. (2013). Digital social research, social media and the sociological imagination: surrogacy, augmentation and re-orientation. International Journal of Social Research Methodology, 16(3), 245–260. https://doi.org/10.1080/13645579.2013.774185

Europarl. (2021, April 23). Digitalizácia: dôležitosť, benefity a legislatíva EÚ. https://www.europarl.europa.eu/news/sk/headlines/society/20210414STO02010/digitalizacia-dolezitost-benefity-a-legislativa-eu

Housley, W., Webb, H., Williams, M., Procter, R., Edwards, A., Jirotka, M., Burnap, P., Stahl, B. C., Rana, O., & Williams, M. (2018). Interaction and Transformation on Social Media: The Case of Twitter Campaigns. Social Media + Society, 4(1), 205630511775072. https://doi.org/10.1177/2056305117750721

Piliapp. (2021, January 1). Facebook symbols. https://www.piliapp.com/facebook-symbols/

Pow, J., & Li, S. C. (2015). The effect of students' perceptions of Internet information quality on their use of Internet information in inquiry-based learning. Australasian Journal of Educational Technology, 31(4). https://doi.org/10.14742/ajet.1936

Vamanu, I., & Zak, E. (2022). Information source and content: articulating two key concepts for information evaluation. Information and Learning Sciences, 123(1/2), 65–79. https://doi.org/10.1108/ILS-09-2021-0084

Kontaktné údaje

Ing. Martin Kuchta, PhD., MBA,
University of Economics in Bratislava,
Faculty of Commerce, Department of Marketing,
Dolnozemská cesta 1, 852 35 Bratislava
E-mail: martin.kuchta@euba.sk

Ing. Peter Červenka, PhD.,
University of Economics in Bratislava,
Faculty of Commerce, Department of Marketing,
Dolnozemská cesta 1, 852 35 Bratislava
E-mail: peter.cervenka@euba.sk

Recenzenti: doc. RNDr. Tatiana Hajdúková, PhD.
PhDr. Peter Veselý, PhD.

Od troch krížikov ku elektronickému podpisu

Ivan Makatura - Peter Veselý

Abstrakt

Článok má ambíciu porovnať formy výslovného prejavu vôle v elektronických dokumentoch, najmä zhrnúť dostupné definície všeobecne podpisu a vlastnoručného podpisu, ako aj jednotlivých foriem elektronického podpisu. Zároveň, pre odbornú verejnosť zhrnúť definície jednotlivých foriem elektronického podpisu a poskytnúť základný opis používaných protokolov a formátov. Cieľom je ujasniť terminologické rozdiely medzi vlastnoručným podpisom a elektronickým podpisom, z hľadiska právnych účinkov a zosumarizovať výhody a nevýhody používania elektronického podpisu. Zároveň opísať problémy v slovenskej aplikačnej praxi elektronického podpisu.

Abstract

The article aims to compare forms of explicit expression of will in electronic documents, in particular, to summarize the available definitions of signature and handwritten signature and individual forms of electronic signature. At the same time, for the professional public, translate all definitions of particular forms of electronic signature and provide a basic description of the protocols and formats used. The goal is to clarify the terminological differences between a handwritten signature and an electronic signature, in terms of legal effects, and to summarize the advantages and disadvantages of using an electronic signature. At the same time, describe the problems in the Slovak application practice of electronic signature.

Úvod

Ôsmy september sa považuje za Medzinárodný deň gramotnosti. Jeho vznik iniciovala Organizácia Spojených národov pre výchovu, vedu a kultúru (UNESCO) v roku 1966 a podnet na zavedenie prišiel na prvom svetovom kongrese o boji proti analfabetizmu, v roku 1965 v Teheráne.

Za základný prvok gramotnosti sa odjakživa chápe schopnosť človeka vlastnoručne sa podpísať. Samozrejme, svojim menom – nie tromi krížikmi. Mohli by sme schopnosť podpísať sa elektronicky začať považovať za základný prejav digitálnej gramotnosti?

Mimochodom – v dlhodobom analyticko-monitorovacom projekte „Digitálna gramotnosť na Slovensku“, realizovaný Inštitútom pre verejné otázky, táto kompetencia občanov Slovenska ani nebola predmetom zisťovania.

V nasledujúcom texte sa snažíme zamyslieť nad kompetenciami a vyhliadkami v súvislosti s používaním (a akceptovaním) elektronického podpisu.

Čo je to podpis? /

Zjednodušene povedané: **prejav vôle, ktorým deklarujeme, že sme s nejakým právnym úkonom vôľovo a obsahovo stotožnení**. Vôľa je základným predpokladom každého právneho úkonu. **Právny úkon** je prejav vôle smerujúci najmä k vzniku, zmene alebo zániku práv alebo povinností, ktoré právne predpisy s takýmto prejavom spájajú.

Aby bola vôľa rozpoznateľná a určitá navonok, musí byť vyjadrená spôsobom, aby bola rozpoznateľná a jednoznačná smerom k ostatným účastníkom, alebo vonkajšiemu prostrediu. V právnych vzťahoch sa najčastejšie vyskytuje **výslovný prejav vôle** (t. j. prejav vyjadrený napríklad slovom, písmom alebo kresbou, či konkrétnym potvrditeľným konaním prameniacim z chcenia človeka).

V nasledujúcom texte sa budeme opakovane odkazovať na zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov (ďalej len ako „OZ“). Podľa § 40 ods. 3 OZ „***písomný právny úkon je platný, len ak je podpísaný konajúcou osobou*****“**, čo znamená, že **podpis konajúcej osoby** je výslovným prejavom jej vôle, smerujúci ku vzniku, zmene alebo zániku práv alebo povinností.

Samotný výraz **podpis** alebo **vlastnoručný podpis** (niekedy aj signatúra z latinského „signare“ – označovať) sa chápe ako ručne písané, štylizované napísanie vlastného mena alebo iného identifikačného znaku (napr. prezývky, znaku alebo monogramu) osoby, ktorá podpis napísala. Podpis typicky priestorovo a obsahovo uzatvára listinu i samotný písomný právny úkon. Pre platnosť podpisu sa nevyžaduje uvedenie celého mena a priezviska, stačí, ak je uvedené priezvisko konajúcej osoby. Uvedenie iba krstného mena je spravidla pre identifikáciu osoby nepostačujúce.[1]

Slovenský právny poriadok termín „podpis“ explicitne nedefinuje a neustanovuje žiadne špecifické nároky na jeho obsah, spôsob jeho vykonania alebo na jeho čitateľnosť. Obsah pojmu „podpis“ je považovaný za notorietu (z lat. notorius = známy) t. j. za skutočnosť, ktorú nie je potrebné dokazovať, pretože sa považuje za všeobecne známu.

Čo je to elektronický podpis?

Digitálny podpis je kryptografická konštrukcia používaná na overenie autenticity a overenie integrity digitálnych údajov. Kým **digitálny podpis** je potrebné chápať v odbornej

[1] KRAJČO, J. a kol.: Občiansky zákonník pre prax (komentár). I. Bratislava, 2015, s. 517-518

literatúre ako bezpečnostnú technológiu, výraz **elektronický podpis** predstavuje metódu používania digitálneho podpisu podľa právnych predpisov. Celou vetou vyjadrené, elektronický podpis pomocou technológie digitálneho podpisu.

Ako už názov nepriamo naznačuje, **digitálny podpis sa používa na podpisovanie digitálnych dokumentov**, čo predznačuje, že digitálne nie je možné podpísať papierový dokument. Elektronicky je možné podpísať akýkoľvek digitálny formát dokumentu (PDF, TXT, XML, DOCX, TIFF, alebo iné) a štandardne je potom najčastejším výstupom jeden z týchto formátov digitálne podpísaných dokumentov napr. PDF, XML, CMS, ASiC-S a ASiC-E.

V konečnom dôsledku jestvujú tri najčastejšie používané výstupné formáty digitálne podpísaných dokumentov: **CAdES** (CMS Advanced Electronic Signatures), **XAdES** (XML Advanced Electronic Signatures) a **PAdES** (PDF Advanced Electronic Signatures), resp. kontajnery typu **ASiC-S**, **ASiC-E**.

Digitálny podpis má v porovnaní s klasickým podpisom niekoľko špecifických vlastností:

- jeho forma závisí, sa odvodzuje aj s ohľadom na podpisovaný dokument,
- používateľ môže efektívne vytvoriť digitálny podpis ku konkrétnemu dokumentu,
- ktokoľvek môže overiť platnosť digitálneho podpisu.

Súčasne pre digitálny podpis platí, že nikto nemôže vytvoriť digitálny podpis iného používateľa, t. j. že nie je možné:

- použiť digitálny podpis z dokumentu A a pripojiť ho k dokumentu B (pretože digitálny podpis A je nerozlučne spätý z podpísaným digitálnym dokumentom A),

- zmeniť podpísaný dokument tak, aby zostala zachovaná platnosť pôvodného digitálneho podpisu (týka sa bezpečnostného atribútu „integrita“),
- poprieť vlastný digitálny podpis (týka sa bezpečnostného atribútu „nepopierateľnosť“).

Na čo je digitálny podpis použiteľný? Primárne na tie isté úkony, na ktoré je používaný aj klasický vlastnoručný podpis. Digitálny podpis má však niekoľko nepopierateľných výhod navyše. Na rozdiel od klasického vlastnoručného podpisu dokáže elektronickému dokumentu zabezpečiť:

- **autenticitu** – t. j. overiť totožnosť používateľa a zistiť, či deklarovaná identita používateľa je skutočná a pravá, čo klasický podpis neumožňuje. V prípade spornej totožnosti dokáže pravosť klasického podpisu overiť len znalec – grafológ.
- **integritu** – t. j. zaručiť, že po podpísaní digitálneho dokumentu už nedošlo k žiadnej zmene jeho obsahu – či už úmyselne alebo neúmyselne. Toto klasický podpis vôbec neumožňuje, o čom svedčia prípady falšovania podpísaných listín.
- **nepopierateľnosť** (angl. „non-repudiation“) – t. j. zaručiť, že právny úkon bol skutočne podpísaný konajúcou osobou a že táto nebude môcť dodatočne poprieť svoj výslovný prejav vôle, vykonaný podpisom elektronického dokumentu. To klasický podpis vyčerpávajúcim spôsobom neumožňuje. Sú až príliš časté prípady popierania vlastného podpisu podpísaných listín – po príklady ani nemusíme chodiť ďaleko.

Terminologické rozdiely medzi podpisom a elektronickým podpisom

Podľa § 40. ods. 4 OZ je písomná forma právneho úkonu zachovaná vždy, ak právny úkon urobený elektronickými prostriedkami je podpísaný zaručeným elektronickým podpisom alebo zaručenou elektronickou pečaťou. Tu niekde začína príbeh elektronického popisu.

Aby nedošlo k omylu, zdôrazňujem, že výrazy „zaručený elektronický podpis“ a „zaručená elektronická pečať“ vychádzajú ešte z pôvodnej terminológie, ktorá bola následne zmenená Nariadením EÚ č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (tzv. eIDAS), resp. zákonom č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu (zákon o dôveryhodných službách) v znení neskorších predpisov.

Podľa § 17 ods. 2 písm. a) zákona o dôveryhodných službách, „Ak sa vo všeobecne záväzných právnych predpisoch používa pojem zaručený elektronický podpis, rozumie sa tým kvalifikovaný elektronický podpis.“. Takže, aby to bolo jednoznačné, **medzi kvalifikovaným elektronickým podpisom a zaručeným elektronickým podpisom nie je absolútne žiaden rozdiel. Oba pojmy označujú to isté**, len slovo „zaručený“ bolo nahradené slovom „kvalifikovaný“. Formát elektronického podpisu označovaný v slovenskej legislatíve pred nadobudnutím účinnosti nariadenia 910/2014 (eIDAS) ako zaručený elektronický podpis bol mierne rozdielny od toho ako je kvalifikovaný elektronický podpis definovaný v nariadení eIDAS. Nakoniec sa však zjednodušene dá povedať, že §17 ods. 2 zákona c. 272/2016 Z. z. len zharmonizoval našu legislatívu s požiadavkami nariadenia eIDAS. Používala sa aj skratka ZEP, ktorá bola nahradená skratkou KEP (v angličtine QES z „Qualified Electronic Signature“).

Ale aby som sa vrátil ku nadpisu tejto časti – aký je rozdiel medzi podpisom a elektronickým podpisom? Začnime tým, že rozlíšime k podpisu sa vzťahujúcu rôznu terminológiu:

Podpis konajúcej osoby – je výslovným prejavom vôle, smerujúci ku vzniku, zmene alebo zániku práv alebo povinností (v prenesenom význame jedinečný prejav súhlasu osoby s obsahom konkrétneho dokumentu).

Vlastnoručný podpis – je ručne písané, štylizované napísanie vlastného mena alebo iného identifikačného znaku konajúcej osoby.

Osvedčenie podpisu – je úkon v zmysle zákona č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok), v ktorom notár, alebo ním poverený zamestnanec osvedčuje, že osoba, ktorej podpis má byť osvedčený v jeho prítomnosti, listinu vlastnoručne podpísala alebo podpis na listine uznala pred ním za vlastný. Osvedčenie podpisu je možné aj podľa zákona č. 599/2001 Z. z. o osvedčovaní listín a podpisov na listinách okresnými úradmi a obcami.

Elektronický podpis – sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie. To je typicky používané ako všeobecný pojem.

Zdokonalený elektronický podpis – je elektronický podpis, ktorý je jedinečne spojený s podpisovateľom, umožňuje určenie totožnosti podpisovateľa, je vyhotovený pomocou údajov na vyhotovenie elektronického podpisu, ktoré môže podpisovateľ s vysokou mierou

dôveryhodnosti používať pod svojou výlučnou kontrolou a je prepojený s údajmi, ktoré sa ním podpisujú takým spôsobom, že každú dodatočnú zmenu údajov možno zistiť.

Kvalifikované zariadenie na vyhotovenie elektronického podpisu – je zariadenie na vyhotovenie elektronického podpisu (skratka QSCD z anglického Qualified Electronic Signature Creation Devices). Podľa ETSI EN 319412-5: QSCD Qualified electronic Signature/Seal Creation Device. Zrejme najdôležitejšia vlastnosť QSCD je tá, že zariadenie nesmie umožniť vytváranie kópií certifikátov a kľúčov na ňom uložených.

Kvalifikovaný elektronický podpis – je zdokonalený elektronický podpis, vyhotovený s použitím kvalifikovaného zariadenia na vyhotovenie elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy. V elektronickom vyhotovení dokumentov má rovnocenný právny účinok ako použitie vlastnoručného podpisu. To znamená, že ak je elektronický dokument podpísaný kvalifikovaným elektronickým podpisom, má rovnaké právne účinky, ako keď bude písomný dokument podpísaný vlastnoručným podpisom.

Kvalifikovaná elektronická pečať – je zdokonalená elektronická pečať, vyhotovená pomocou kvalifikovaného zariadenia na vyhotovenie elektronickej pečate a založená na kvalifikovanom certifikáte pre elektronickú pečať, pričom „certifikát pre elektronickú pečať“ je elektronické osvedčenie, ktoré spája údaje na validáciu elektronickej pečate s právnickou osobou a potvrdzuje jej názov. V podstate si elektronickú pečať môžeme stotožniť s pečiatkou organizácie, avšak s výhodou zaručenia autentickosti a integrity elektronického dokumentu.

Rozdiely z hľadiska právnych účinkov

Ako sme už uviedli vyššie, podľa § 40 ods. 4 OZ: „písomná forma je zachovaná vždy, ak právny úkon, urobený elektronickými prostriedkami, je podpísaný zaručeným elektronickým podpisom.“ (t. j. kvalifikovaným elektronickým podpisom).

Zároveň platí, že digitálny dokument, opatrený kvalifikovaným elektronickým podpisom a časovou pečiatkou, sa považuje za osvedčený vlastnoručný podpis, pretože v zmysle § 40. ods. 5 OZ sa „*na právne úkony uskutočnené elektronickými prostriedkami, podpísané zaručeným elektronickým podpisom alebo zaručenou elektronickou pečaťou a opatrené časovou pečiatkou osvedčenie pravosti podpisu nevyžaduje*“.

Niektorí čitatelia by mohli namietať, že nevidia rozdiel medzi zdokonaleným elektronickým podpisom a kvalifikovaným elektronickým podpisom. To by však bol omyl. Jednotlivé typy digitálneho podpisu, spôsoby použitia, sme zhrnuli v tabuľke nižšie, kde je

možné si pozrieť a porovnať právne následky resp. právne účinky jednotlivých typov digitálneho podpisu:

Typ digitálneho podpisu	Právny účinok	Podmienka QESCD	Úroveň zabezpečenia	Spôsob použitia
Zdokonalený elektronický podpis	výslovný prejav vôle, identifikácia osoby	Nie	nízka	určenie totožnosti podpisovateľa
KEP	vlastnoručný podpis osoby	Áno	pokročilá	právne úkony, pre ktoré **nie je požadované** osvedčenie podpisu
KEP + časová pečiatka	osvedčený vlastnoručný podpis osoby	Áno	vysoká	právne úkony, pre ktoré **je požadované** osvedčenie podpisu

Nad to všetko platí, že právny účinok elektronického podpisu a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z toho dôvodu, že má elektronickú formu alebo že nespĺňa požiadavky pre kvalifikované elektronické podpisy. Zároveň kvalifikovaný elektronický podpis založený na kvalifikovanom certifikáte vydanom v jednom členskom štáte sa uznáva ako kvalifikovaný elektronický podpis vo všetkých ostatných členských štátoch.

Pre prostriedky elektronickej identifikácie, vydávané v rámci príslušnej schémy v zmysle Nariadenia eIDAS, sa určuje špecifikácia úrovní zabezpečenia – konkrétne „nízka“, „pokročilá“ a/alebo „vysoká“, ktoré spĺňajú nasledujúce kritériá:

- **obmedzený** stupeň dôveryhodnosti, pokiaľ ide o údajnú alebo uvádzanú totožnosť osoby, charakterizovaný odkazom na technické špecifikácie, normy a postupy, ktorých účelom je **znížiť riziko zneužitia alebo pozmenenia totožnosti,**
- **pokročilý** stupeň dôveryhodnosti, pokiaľ ide o údajnú alebo uvádzanú totožnosť osoby, charakterizovaný odkazom na technické špecifikácie, normy a postupy, ktorých účelom je **podstatne znížiť riziko zneužitia alebo pozmenenia totožnosti,**
- **vyšší** stupeň dôveryhodnosti, ako prostriedok elektronickej identifikácie s úrovňou zabezpečenia „pokročilá“, pokiaľ ide o údajnú alebo uvádzanú totožnosť osoby, charakterizovaný odkazom na technické špecifikácie, normy a postupy, ktorých účelom je **zabrániť zneužitiu alebo pozmeneniu totožnosti**.

Výhody a nevýhody elektronického podpisu v praxi

Čitateľ neznalý problematiky sa môže spýtať – kde všade môžem použiť elektronický podpis a akú výhodu mi to prinesie?

Predovšetkým získa zjednodušený prístup k elektronickým službám štátu. Ponechajme teraz bokom kvalitu týchto služieb, alebo ich množstvo. Zostávame optimisti.

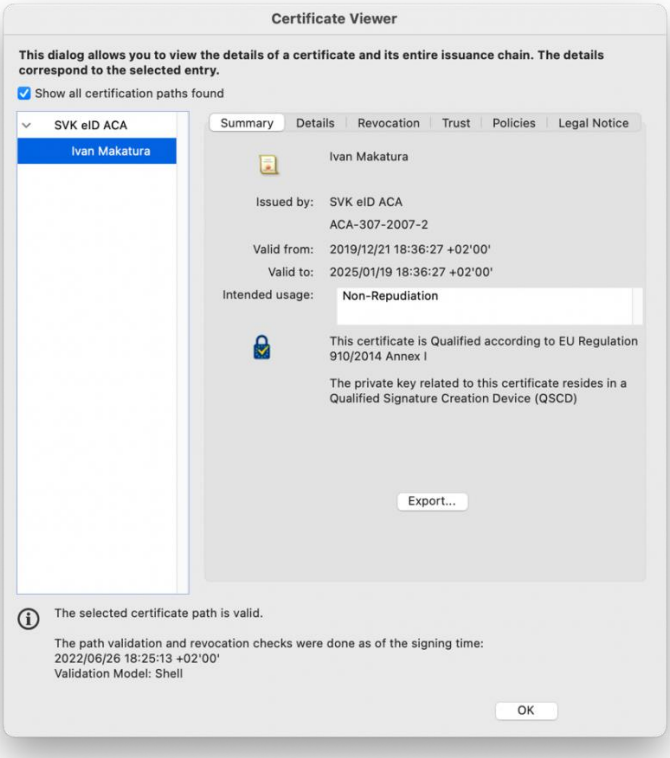
V každom prípade, v rámci riešenia rôznych životných situácií, sa komunikácii so štátom vyhnúť nedá. Potom je už len otázkou osobného rozhodnutia, či jednotlivé právne úkony riešiť obiehaním po úradoch, návštevou notárov, podpisovaním a overovaním podpisov, alebo či nie je hodnejšie skúsiť využiť elektronické služby štátu. Týmto elektronickým službám sa hovorí eGovernment a upravuje ich zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente).

Elektronicky sa dá právny úkon vykonať z akéhokoľvek miesta, zvyčajne aj bez časového obmedzenia, za dodržania prípadnej zákonom stanovenej lehoty na vykonanie úkonu. Nie je to ani raketová veda – postačí eID karta, čítačka kariet, počítač a prístup na internet.

Hlasujeme jednoznačne za elektronickú komunikáciu.

Nie je v možnostiach jedného článku vykonať recenziu všetkých existujúcich elektronických služieb štátu. Stačí vedieť, že aktivovaná eID karta je nový typ občianskeho preukazu s elektronickým čipom, ktorý sa vydáva od roku 2013. Vo fyzickom svete, tak ako to u bolo doteraz, slúži občiansky preukaz na preukazovanie totožnosti pri osobnom styku s inštitúciami. Na elektronickom čipe sú však nahraté špeciálne dáta, ktoré slúžia predovšetkým na vyhotovenie digitálneho podpisu, najmä tzv. **certifikát verejného kľúča**, a **súkromný kľúč**. Certifikát je elektronické osvedčenie, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený verejný kľúč patrí konkrétnej fyzickej osobe, ktorej identita je uvedená v

tele certifikátu. Obsahuje informáciu o verejnom kľúči, informáciu o totožnosti jeho držiteľa a elektronický podpis vydavateľa, ktorý overil obsah certifikátu.



Súkromný kľúč je zásadne uložený v QSCD a prístup k nemu je chránený heslom. Bežnému používateľovi o obsahu čipu na eID karte viac vedieť netreba.

Na elektronickom čipe sú uložené aj ďalšie dáta umožňujúce vytvoriť elektronický podpis (kryptografické kľúče + certifikát), ktoré môžu byť následne používané v zložitých kryptografických protokoloch, okrem samotného elektronického podpisu, najmä na nasledovné procesy:

- **Identifikácia** – predstavuje procedúru, v ktorej používateľ potvrdzuje svoju totožnosť, „predstavuje“ sa systému, identifikuje sa ako platný používateľ. Elektronická identifikácia je proces používania osobných identifikačných údajov v elektronickej forme, ktoré jedinečne reprezentujú fyzickú osobu alebo právnickú osobu alebo fyzickú osobu zastupujúcu právnickú osobu.
- **Autentizácia** – je následný proces overenia totožnosti používateľa. Je to zisťovanie, či deklarovaná identita používateľa je skutočná a pravá.

- **Autorizácia** – je pridelenie alebo preukázanie príslušných oprávnení na vykonanie právneho úkonu, systémovej zmeny, alebo elektronickej transakcie.

Často sa chybne zamieňajú pojmy autorizácia a autentizácia, avšak autorizácia má vždy využívať výsledky autentizácie na pridelenie príslušných oprávnení v systéme, alebo na potvrdenie elektronickej transakcie, či preukázanie oprávnenia. To napokon vyplýva aj z § 23 ods. 2 Zákona č. 305/2013 Z. z. o e-Governmente, ktorý zdôrazňuje nutnosť identifikácie a autentizácie osoby, ktorá má byť autorizovaná k príslušnému právnemu úkonu: „*Uznaný spôsob autorizácie je taký spôsob autorizácie, ktorý zabezpečuje spoľahlivú identifikáciu osoby, ktorá autorizáciu vykonala, a spoľahlivé zachytenie obsahu právneho úkonu, ktorý autorizovala, ako aj zhodu medzi autorizovaným právnym úkonom a právnym úkonom, ktorý osoba autorizovala*.“ Rovnako tak sa zamieňajú aj pojmy autorizácia a podpis. Skutočne to nie je rovnaký úkon (viď. vyššie).

Elektronický podpis a vyššie uvedené tri procedúry, súvisiace s manažmentom identít, sú de facto všetky bezpečnostné mechanizmy súvisiace s eID, ktoré sú potrebné na to, aby fyzická osoba mohla vykonávať právne úkony elektronicky.

Slovenské aplikačné problémy elektronického podpisu

Tie aktuálne sa odvíjajú od prípadu z roku 2017. Vtedy českí výskumníci z Masarykovej univerzity identifikovali zraniteľnosť v knižnici od nemeckej firmy Infineon, ktorá sa nachádza aj na čipe slovenských elektronických občianskych preukazov. Zraniteľnosť umožňuje útočníkovi vygenerovať súkromný kľúč len za pomoci verejného kľúča. Útočníci by potom dokázali elektronicky podpisovať dokumenty v mene vlastníka získaného kľúča, alebo dešifrovať citlivé dáta. Bolo by však neférové, ak by sme zodpovednosť za túto zraniteľnosť pripisovali štátu, keď ju spôsobil výrobca. Preto číslovanie začína až nasledujúcim prípadom.

Problém č. 1:

Štát vtedy po určitom úvodnom váhaní čiastočne ošetril vzniknuté riziko tým, že rozšíril dĺžku používaného kľúča z 2048-bitového na 3072-bitový, ktorý je voči zistenej zraniteľnosti približne 500 násobne odolnejší. Zároveň však certifikácia zariadenia ako QSCD končí práve 31.12.2022 a preto NBÚ oznámil vydavateľom certifikátov, že sú povinní k 31.12.2022 zrušiť všetky vydané na eID s CardOSv5.0 z dôvodu, že v nich bude uvedená nepravdivá informácia, že ide o QCSD zariadenie. Pre elektronické občianske preukazy vydané do 20. júna 2021 tým fakticky končí platnosť certifikátu 1. januára 2023. Následky asi

nie je potrebné opisovať. Keďže asi pol milióna právnických osôb je povinných komunikovať so štátom výlučne elektronicky, ich štatutárni zástupcovia vezmú klientske centrá koncom roka útokom.

Problém č. 2:

Spočíva v tom, že štát stále nedokázal dokončiť verejné obstarávanie na elektronické občianske preukazy novej generácie s NFC čipom a biometrickými údajmi. Ministerstvo má na sklade množstvo nepoužitých plastov. Tie však vzhľadom na nové európske pravidlá pre eID budú mať tiež obmedzenú platnosť a preto do niekoľkých rokov si všetci budú musieť ísť po elektronický občiansky preukaz aj po tretí krát.

Problém č. 3:

Od negramotného používania troch krížikov v stredoveku sme sa prepracovali do stavu, v ktorom štát vyžaduje kvalifikovaný elektronický podpis aj tam, kde by vôbec nemusel. Tým odrádza používateľov od používania elektronických služieb štátu. Pretrváva príliš extenzívne presadzovanie používania kvalifikovaného elektronického podpisu aj v takých právnych úkonoch, pre ktoré by výslovný prejav vôle konajúcej osoby mohol byť deklarovaný aj jednoduchšou formou. Napríklad použitím zdokonaleného elektronického podpisu. Alebo autorizáciou právneho úkonu iným prostriedkom, za dodržania pravidiel identifikácie konajúcej osoby.

Problém č. 4:

Elektronická pečať nie je to isté, čo elektronický podpis. Keďže kvalifikovaný elektronický podpis je ekvivalentom vlastnoručného podpisu, certifikát kvalifikovaného elektronického podpisu možno vydať iba fyzickej, nie však právnickej osobe. To je logické, pretože v mene každej právnickej osoby vždy koná konkrétna fyzická osoba. Slovenská duša je však vynaliezavá a tak sa tu rozmohol taký nešvár, že na „elektronický podpis“ sa používajú certifikáty elektronickej pečate. Problém vznikol tým, že zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) označil za ekvivalent vlastnoručného podpisu aj „kvalifikovanú elektronickú pečať“ , čo je právny nezmysel, keďže tým vytvára precedens, že právnická osoba môže niečo „podpisovať“.

Problém č. 5:

Aj keď to nie je akútny a bezprostredný problém, ale začínajú sa tu rozmáhať snahy o presadenie takých technologických riešení, ktoré by v eGovernmente ako výslovný prejav vôle konajúcej osoby umožnili používať rôzne formy pseudoidentifikácie. „Kliknutie“ nie je „podpis“, ale autorizácia. Mobilný token tiež nie je „podpis“, ale autentizácia... a podobne. Väčšina týchto snáh je však, našťastie, stále ešte v rovine terminologickej diskusie.

Problémy sú riešiteľné

Pri posudzovaní výslovných prejavov vôle v elektronických dokumentoch je samozrejme potrebné vychádzať z osobitných predpisov. Podľa teórie práva platí princíp, že „zákon osobitný ruší zákon všeobecný", t. j. ak je jedna skutková situácia upravená dvomi normami tej istej právnej sily odlišne, potom prednostne (ako prvú) treba aplikovať tú z nich, ktorá je konkrétnejšia, ktorá na daný skutkový stav prilieha tesnejšie.[2]

Preto napríklad, ak osobitný predpis vyžaduje, aby bol určitý písomný dokument podpísaný vlastnoručným podpisom a tento dokument je v jeho elektronickom vyhotovení podpísaný kvalifikovaným elektronickým podpisom osoby, ktorá prejavuje podpísaním tohto dokumentu svoju vôľu, je potrebné na takýto prejav vôle hľadieť ako na platný. Na druhej strane ak osobitný predpis vyžaduje, aby bol určitý písomný dokument podpísaný vlastnoručným podpisom a dokument v jeho elektronickom vyhotovení je podpísaný kvalifikovaným elektronickým podpisom s časovou pečiatkou (t. j. ekvivalentom osvedčeného podpisu), takýto prejav vôle by bol samozrejme taktiež platný, avšak použitá úroveň zabezpečenia elektronického podpisu je nadbytočná. S takouto rigidnou aplikáciou úrovne zabezpečenia elektronického podpisu je totiž spojené nenulové množstvo rizík. Čo s tým?

Na ceste za porozumením konfliktných požiadaviek na výslovný prejav vôle v písomných dokumentoch a výslovný prejav vôle v elektronických dokumentoch pre rovnaké právne úkony sa pokúsme vymenovať aspoň niektoré z nich, vrátane implikácií:

Scenár 1: písomný dokument má byť **podpísaný osvedčeným vlastnoručným podpisom** a dokument v jeho elektronickom vyhotovení má byť **podpísaný kvalifikovaným elektronickým podpisom s časovou pečiatkou** (t. j. ekvivalentom osvedčeného podpisu).

[2] KÁČER, M., PROCHÁZKA, R. In PROCHÁZKA, R., KÁČER, M. Teória práva. 2. vyd. Bratislava: C. H. Beck, 2019, s. 138.

V tomto scenári je bezpodmienečne nutné použiť QESCD, kvalifikovaný certifikát elektronického podpisu a časovú pečiatku.

Scenár 2: písomný dokument má byť **podpísaný vlastnoručným podpisom** a dokument v jeho elektronickom vyhotovení má byť **podpísaný kvalifikovaným elektronickým podpisom**. V tomto scenári je bezpodmienečne nutné použiť QSCD a kvalifikovaný certifikát elektronického podpisu, i keď bez časovej pečiatky.

Scenár 3: písomný dokument má byť **podpísaný** a dokument v jeho elektronickom vyhotovení má byť **podpísaný kvalifikovaným elektronickým podpisom** a zákon neustanovuje iný spôsob autorizácie alebo je podľa osobitného predpisu náležitosťou podania **vlastnoručný podpis**. V tomto scenári nie je nutné použiť QSCD ani kvalifikovaný certifikát elektronického podpisu, ani časovú pečiatku. Keďže nie je určené, že podpis na písomnom dokumente má byť vlastnoručný podpis, na elektronické podanie bude v zmysle § 23 ods. 2 Zákona č. 305/2013 Z. z. o e-Governmente postačovať uznaný spôsob autorizácie, t. j. taký spôsob autorizácie, ktorý zabezpečí spoľahlivú identifikáciu osoby, ktorá autorizáciu vykonala a spoľahlivé zachytenie obsahu právneho úkonu, ktorý autorizovala, ako aj zhodu medzi autorizovaným právnym úkonom a právnym úkonom, ktorý osoba autorizovala.

Scenár 4: písomný dokument má byť **podpísaný** a dokument v jeho elektronickom vyhotovení má byť **podaný prostredníctvom elektronickej podateľne** (bez určenia úrovne identifikácie alebo typu elektronického podpisu). Platia podmienky pre scenár č. 3.

Scenár 5: písomný dokument má byť **podpísaný** a dokument v jeho elektronickom vyhotovení má byť **podaný prostredníctvom elektronickej podateľne ústredného portálu verejnej správy** (bez určenia úrovne identifikácie alebo typu elektronického podpisu). V tomto scenári je „chyták“, pretože – elektronická podateľňa ústredného portálu verejnej správy donedávna neumožňovala použiť na autentizáciu iný autentizačný nástroj než eID (t. j. QSCD zariadenie). Toto už našťastie niekoľko týždňov neplatí, pretože na autentizáciu je už možné použiť aj autentizačným token, konkrétne aplikáciu názvom „Slovensko v mobile“. Či je však skutočne možné vykonať aj samotné podanie, to už záleží aj na použitom XML formulári na ÚPVS (bez detailnejšej analýzy si dovolíme tvrdiť, že väčšina formulárov je závislá na použití kvalifikovaného elektronického podpisu).

Záver

Pokiaľ by čo najväčšie množstvo elektronických služieb štátu umožňovalo použitie prostriedkov elektronickej identifikácie na úrovni zabezpečenia nižšej, než „vysoká“ (napr. zdokonaleného elektronického podpisu, alebo MobileID), odstránilo by to mnohé bariéry a rozšírili by sa možnosti použitia elektronického podpisu pre väčšie množstvo občanov.

Bolo by nanajvýš vhodné vykonať revíziu relevantných právnych predpisov s cieľom uistiť sa, že ak pre právny úkon v písomnej forme nie je explicitne vyžadovaný vlastnoručný podpis, nebude ani pre ekvivalentný právny úkon v elektronickom vyhotovení dokumentu vyžadované použitie kvalifikovaného elektronického podpisu. Za všetky príklady je možné uviesť ustanovenie § 13 ods. 5 Zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov Daňového poriadku, podľa ktorého: „*Podanie urobené elektronickými prostriedkami sa podáva prostredníctvom elektronickej podateľne alebo prostredníctvom elektronickej podateľne ústredného portálu verejnej správy a* ***musí byť podpísané zaručeným elektronickým podpisom*** *osoby, ktorá ho podáva.“* Podľa § 13 ods. 2: „*Písomné podanie musí byť podpísané osobou, ktorá ho podáva*.“ V tomto ustanovení nie je zmienka o tom, že by podpis konajúcej osoby na písomnom podaní mal byť vlastnoručný podpis a už vôbec nie, že by to mal byť vlastnoručný podpis osvedčený notárom. V elektronickom vyhotovení dokumentu by bolo použitie zdokonaleného elektronického podpisu dostatočne dôveryhodným výslovným prejavom vôle, ktorým by identifikovaná konajúca osoba na písomnom podaní deklarovala, že je s právnym úkonom vôľovo a obsahovo stotožnená. A dalo by sa súhlasiť aj s diskutovaným názorom, že dostatočne dôveryhodným spôsobom výslovného prejavu vôle by mohol byť aj uznaný spôsob autorizácie v zmysle § 23 ods. 2 Zákona č. 305/2013 Z. z. o e-Governmente, t. j. taký spôsob autorizácie, ktorý zabezpečí spoľahlivú identifikáciu osoby, ktorá autorizáciu vykonala a spoľahlivé zachytenie obsahu právneho úkonu, ktorý autorizovala, ako aj zhodu medzi autorizovaným právnym úkonom a právnym úkonom, ktorý osoba autorizovala.

V mnohých prípadoch môže mať použitie zdokonaleného elektronického podpisu rovnocenný právny účinok ako použitie kvalifikovaného elektronického podpisu. To by umožnilo zachovať reálny kryptografický a teda dostatočne dôveryhodný charakter identifikácie a autentizácie konajúcej osoby. Ale zároveň aj virtualizáciu úložísk pre certifikáty verejného kľúča. Čím by sa dalo **vyhnúť použitiu QSCD zariadení**, ktoré sú pre kvalifikovaný elektronický podpis a pre kvalifikovaný elektronický podpis s časovou pečiatkou povinné. Benefitom vyhnutia sa použitiu QSCD zariadení by bol fakt, že by sa dali

vyvinúť rôzne mobilné riešenia umožňujúce efektívnu a dostatočne bezpečnú elektronickú komunikáciu so štátom.

Tu vstupuje do hry aj pripravované nariadenie eIDAS2 a pripravovaný koncept peňaženky digitálnej identity (Digital ID Wallet). Stručne povedané, do roku 2023 musí každý členský štát EÚ sprístupniť peňaženku digitálnej identity každému občanovi, ktorý o ňu požiada. To bude predstavovať novú generáciu Mobile ID, ktorá vytvorí bezpečné úložisko na smartfónoch pre údaje o digitálnej identite občanov EÚ.

Ak chceme zotrvať na najvyššej úrovni zabezpečenia pre prostriedky elektronickej identifikácie podľa špecifikácie v nariadení eIDAS, jednou z možností je aj **vytvorenie tzv. kvalifikovanej dôveryhodnej služby** v rámci infraštruktúry Národnej agentúry pre sieťové a elektronické služby (NASES). Výraz kvalifikovaná dôveryhodná služba nie je pre laickú verejnosť celkom známy. Zjednodušene to znamená, že štát by mohol čiastočne nahradiť čipy elektronických občianskych preukazov aj automatizovaným riešením, ktorého základom sú tzv. zariadenia HSM. Hardvérový bezpečnostný modul (HSM) je kryptografický procesor, ktorý je špeciálne navrhnutý na zabezpečenie kryptografických kľúčov a automatizovanú podporu služieb šifrovania, dešifrovania, autentifikácie a elektronického podpisovania pre širokú škálu aplikácií.

Všetky z vyššie uvedených možností by rozšírili možnosti použitia elektronického podpisu pre väčšinu občanov.

Na začiatok by však bolo nanajvýš vhodné vykonať revíziu dotknutých právnych predpisov s cieľom uistiť sa, že ak pre právny úkon v písomnej forme nie je vyslovene vyžadovaný vlastnoručný podpis, nebude vyžadovaný kvalifikovaný elektronický podpis ani pre ten istý právny úkon v elektronickom vyhotovení dokumentu.

V mnohých prípadoch by mohlo mať **použitie zjednodušených foriem elektronického podpisu rovnocenný právny účinok ako použitie kvalifikovaného elektronického podpisu**. To by umožnilo zachovať reálny kryptografický charakter identifikácie a autentizácie konajúcej osoby.

Odbornou verejnosťou obchádzaným paradoxom je, že aj všetky vyššie uvedené zjednodušené formy elektronickej identifikácie by aj naďalej zachovali vyššiu úroveň zaručenia požiadaviek na autenticitu, integritu a nepopierateľnosť v porovnaní s vlastnoručným podpisom.

Zoznam použitej literatúry

KRAJČO, J. a kol.: Občiansky zákonník pre prax (komentár). I. Bratislava, 2015, s. 517-518

KÁČER, M., PROCHÁZKA, R. In PROCHÁZKA, R., KÁČER, M. Teória práva. 2. vyd. Bratislava: C. H. Beck, 2019, s. 138.

Kontaktné údaje

Ing. Bc. Ivan Makatura, CRISC, CDPSE, CCNA

Univerzita Komenského

Fakulta managementu, Katedra informačných systémov

doktorand

Odbojárov 10

P.O.BOX 95

820 05 Bratislava 25

PhDr. Peter Veselý, PhD., MBA

Univerzita Komenského

Fakulta managementu, Katedra informačných systémov

Odbojárov 10

P.O.BOX 95

820 05 Bratislava 25

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

doc. RNDr. Tatiana Hajdúková, PhD.

Ransomvérové skupiny, ransomvérové útoky a exfiltrácia údajov

Martin Mišota

Abstrakt: Ransomvérové útoky a exfiltrácia údajov je hrozbou pre jednotlivcov, vládne organizácia či veľké nadnárodné korporácie. Ochrana informačných aktív, korporátnej siete a pravidelné zálohovanie údajov a konfigurácie systémov je dôležité až takmer nevyhnutné. Odborný článok sa orientuje na ransomvérové útoky, analyzuje súčasné trendy ransomvérových útokov a popisuje vybrané techniky ransomvérových skupín vo svete.

Abstract: Ransomware attacks and data exfiltration is a threat to individuals, government organizations or large multinational corporations. Protecting information assets, corporate networks and regular data backups and systems configuration is important to the point of being essential. This expert article focuses on ransomware attacks, analyzes current trends of ransomware attacks and describes selected techniques of ransomware groups in the world.

Kľúčové slová: ransomvér, ransomvérové útoky, techniky vydierania, exfiltrácia údajov, zraniteľnosti

Key words: ransomware, ransomware attacks, extortion techniques, data exfiltration, vulnerabilities

Úvod

Ransomvér (Ransomware) alebo ransomvérový útok je typ počítačového útoku, ktorý využíva malvér, ktorý zničí a zašifruje všetky súbory obete z cieľom zamedziť obeti k prístupu k jej predmetným údajom pokým nezaplatí výkupné (ransom) zvyčajne v kryptomene Bitcoin alebo Monero) výmenou za dešifrovací kľúč – dekryptor na odomknutie zašifrovaných údajov.[1] Ransomvér, podobne ako akýkoľvek iný škodlivý softvér, môže získať prístup do systémov organizácie viacerými rôznymi spôsobmi. Viac ako 90 % počítačových útokov preniká do organizácie prostredníctvom e-mailu. Podľa FBI sa počet phishingových útokov od začiatku pandémiu v roku 2020 medziročne zvýšil o 400 %. V roku 2021 bol zaznamenaný 50 % nárast celkového počtu počítačových útokov na podnikové siete za týždeň v porovnaní s rokom 2020[2]. Ransomvéroví útočníci v počiatočnej fáze útoku často používajú techniky sociálneho inžinierstva. Dobre prepracované, cielené, legitímne vyzerajúce phishingové e-maily sú zamerané na zamestnancov a snažia sa vyvolať ich reakciu: kliknutie na odkaz, otvorenie prílohy alebo ich presvedčiť, aby prezradili svoje prihlasovacie údaje alebo iné citlivé informácie. Veľa ransomvérových útokov využíva protokol RDP ako vstupný vektor. Ide o súčasť širšieho trendu "Living off the Land": používanie legitímnych hotových nástrojov

[1] Ransomware nezamieňať z tzv. sextortion, čiže digitálne podvodné vydieranie ktoré požaduje platbu vo virtuálnej mene Bitcoin za to, že potencionálny počítačový podvodník alebo doxxer vydiera obeť, že zverejní citlivé údaje o obeti, ku ktorým má akože prístup.

[2] https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/

(zneužívanie protokolu RDP, protokolu SMB1 alebo rôznych nástrojov príkazového riadka CMD.exe, WMI alebo Powershell) na zamaskovanie detekcie, ktoré umožňuje ich splynutie s typickou činnosťou správcu. Techniky Living off the Land (LotL), ktoré využívajú legitímny softvér a funkcie v systéme na vykonávanie škodlivých akcií v operačnom systéme. Používanie legitímnych nástrojov s menšou pravdepodobnosťou vyvolá podozrenie a útočníci sa tak môžu vyhnúť mnohým metódam detekcie, ako sú hashovacie hodnoty, identifikátory IOC a signatúry.

Cobalt Strike, Mimikatz, MSHTA.exe, Net.exe a psExec boli najčastejšie zneužívané nástroje ransomvérovými kyberzločincami pri vykonávaní počítačových útokov. Keďže tieto legitímne nástroje sú zvyčajne zaradené na biely zoznam pravidiel bezpečnostných operačných centier (SOC), akákoľvek ich aktivita je často ignorovaná. Taktika Living off the Land (LotL) umožňuje útočníkom obmedziť používanie škodlivého softvéru až do oveľa neskorších fáz útočného reťazca, ako je to v prípade ransomvéru, pričom napadnutej organizácii zostáva len málo času na reakciu alebo žiadny čas. Skupiny ransomvérových útočníkov sa vo všeobecnosti identifikujú podľa malvéru, ktorý používajú, pričom sofistikované skupiny kybernetického zločinu a hackeri podporovaní štátom tzv. APT skupiny často používajú vlastný malvér, čo uľahčuje ich identifikáciu, či stoja za určitou činnosťou. Ak sa však ransomvérový útok vykoná pomocou nástrojov LotL a iných ako použitím vlastného malvéru, je oveľa ťažšie určiť, kto by za takýmto útokom mohol stáť.[3]

Na základe udalostí v treťom štvrťroku 2021 spoločnosť Trellix[4] identifikovala trend v nástrojoch používaných protivníkmi, ktorí sa snažia zostať neodhalení. Zatiaľ čo štátom sponzorované ATP skupiny a väčšie kriminálne ATP skupiny majú zdroje na vlastný vývoj nástrojov, mnohé z nich často využívajú binárne súbory a administratívne nainštalovaný softvér, ktorý už môže byť prítomný v cieľovom systéme na vykonanie jednotlivých fáz ransomvérového útoku. Na identifikáciu pôvodných binárnych súborov alebo administratívne používaného softvéru počas fázy prieskumu vysokopostaveného cieľa môžu počítačoví útočníci získať informácie o používaných technológiách z pracovných ponúk, referencií zákazníkov inzerovaných dodávateľmi alebo od vnútorného komplica. V roku 2022 sa objavili nové skupiny ransomvéru BlackCat (alias AlphaVM, AlphaV), Spook, Sabbath, Lockbit 3.0, Pandora Leaks, Night Sky[5], ktoré fungujú systémom ransomvér ako služba – Ransomware as

[3] https://res.armor.com/resources/threat-intelligence/living-off-the-land-attacks
[4] https://www.trellix.com/en-us/assets/docs/threat-reports/trellix-atr-report-apr-2022.pdf
[5] https://blog.malwarebytes.com/ransomware/2022/01/night-sky-the-new-corporate-ransomware-demanding-a-sky-high-ransom/

a Service (RaaS). RaaS znamená, že kybernetickí zločinci zložia zálohu finančných aktív v kryptomene výmenou za použitie vlastných počítačových útokov "na prenájom". Väčšina ransomvérových skupín prechádza od používania programovacieho jazyka C, Visual C++ na nové netradičné programovacie jazyky Rust, GO a Nim.[6] Skupina ransomvéru Pandora Leaks je pravdepodobne rebrandom značky ransomvéru ROOK.[7] Ransomvér Pandora infikuje a zašifruje súbory, aby si ich obeť nemohla otvoriť, po spustení do každého priečinka počítača obete vloží poznámkuo výkupnom s názvom "Restore_My_Files.txt.". Po zašifrovaní sa súbor premenuje na súbor s príponou ".Pandora". Skupina Night Sky a aj ďalšie ransomvérové skupiny začali zneužívať zraniteľnosti v Log4j2. Keďže takmer každý systém sieťového zabezpečenia beží na nejakom procese protokolovania (pričom najpopulárnejšou knižnicou na protokolovanie je Log4j2), Log4Shell bol a stále je pre organizácie používajúce tento softvér vážnym problémom.[8] Milióny aplikácií používajú Log4j2, a ak útočník by získal prístup do aplikácie Log4j2, mohol by ju kompromitovať zaznamenávaním špeciálneho reťazca znakov. S Log4Shell boli nakoniec spojené tri zraniteľnosti (CVE-221-44228, CVE-2021-4104 a CVE-2021-45046) a ransomvérové skupiny Night Sky.[9][10] Ransomvérové skupiny ako LockBit hromadne zneužívajú od roku 2021 známu zraniteĺnosť Log4Shell v systémoch VMware Horizon a **používajú techniky tzv. "sideloading" - postranného zavádzania knižníc DLL na exfiltráciu a zašifrovanie údajov.**[11] Ransomvérové skupiny Pysa, Hades, LockBit, Nefilim, Conti, BlackCat/ALPHV využívajú na exfiltráciu dát a údajov zo siete obetí synchronizačný nástroj **MegaSync**, ktorý umožňuje nahrávať súbory do cloudového úložiska s end-to-end šifrovaním MEGA v systémoch Windows, Mac, Linux, Android a iOS. [12] Ransomvérová skupina Sabbath podobne ako v minulosti skupina Avaddon či Blackbyte na rozdiel od iných partnerských programov typu RaaS poskytuje svojim pridruženým partnerom vopred nakonfigurovaný nástroj Cobalt Strike BEACON. Tento

[6] https://www.bankinfosecurity.com/ransomware-groups-such-as-blackcat-are-turning-to-rust-a-18507

[7] ROOK a Pandora majú podobný kód. Aj VirusTotal (detekcia vírusov spoločnosti Google) deteguje Pandoru ako ROOK, odvodený od ransomvéru Babuk, ktorý je založený na uniknutom zdrojovom kóde. Variant ransomvéru ROOK bol podozrivý z toho, že je najnovším potomkom ransomvérovej rodiny Babuk, pretože súbor pravidiel YARA spojený s ROOK, pochádza z Babuku. Okrem toho analýza od spoločnosti Virus Total uviedla, že ide o generický kód ransomvéru Babuk. Babuk je v súčasnosti nefunkčný ransomvér ako služba.

[8] https://www.eset.com/sk/o-nas/press-centrum/eset-tlacove-spravy/kriticka-zranitelnost-log4shell-ohrozuje-aj-slovenske-firmy-eset-zablokoval-tisicky-pokusov-o-utok/

[9] https://www.avertium.com/resources/threat-reports/everything-you-need-to-know-about-night-sky-ransomware

[10] Ransomvér Night Sky je odnožou rodiny ransomvéru s názvom Rook, ktorý bol tiež vytvorený z uniknutého zdrojového kódu ransomvéru Babuk

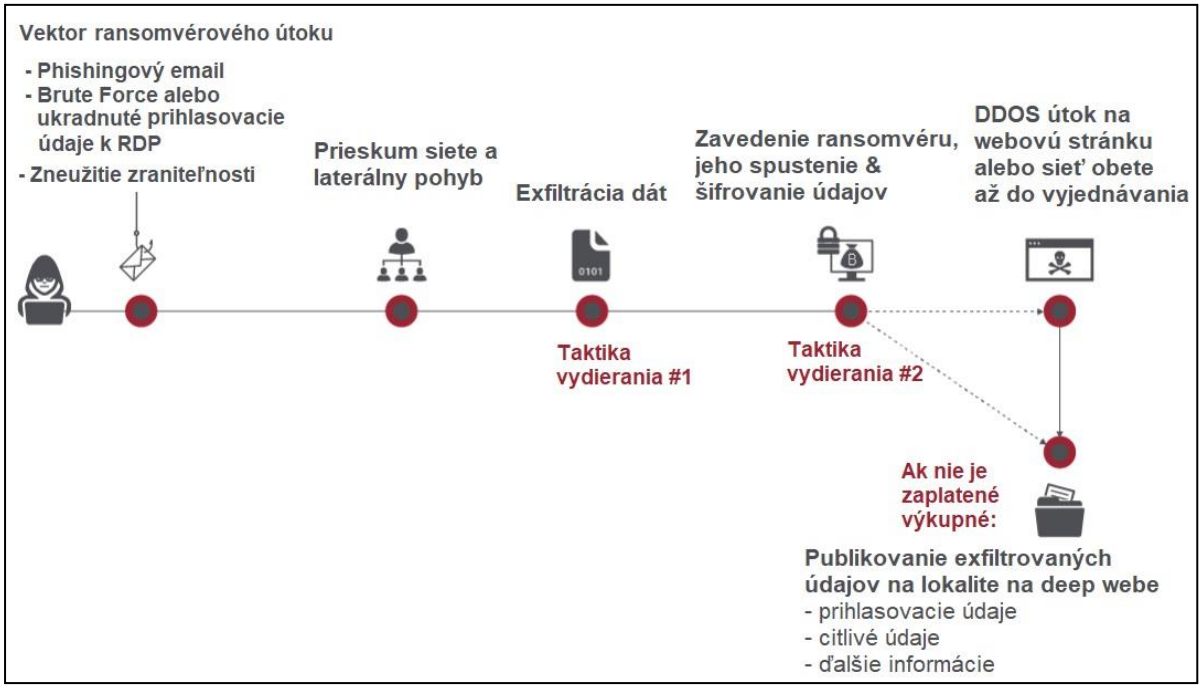
[11] https://www.hivepro.com/deep-panda-deploys-new-rootkit-fire-chili-by-exploiting-log4shell-in-vmware-horizon/

[12] https://mega.io

komerčný program Cobalt Strike BEACON vedie k lukratívnym a efektívnym počítačovým útokom, aj keď ich využívajú menšie a neznáme skupiny. Používanie nástroja Cobalt Strike BEACON na nasadenie ransomvéru nie je pre ransomvérové gangy ničím výnimočným. Neobvyklý je však prevádzkovateľ programu pre výkupné, ktorý poskytuje prostredníctvom nástroja Cobalt Strike BEACON. To predstavuje výzvu pre firmy a organizácie pre úsilie o jeho identifikáciu a zároveň ponúka ďalšie možnosti na odhalenie ransomvérových skupín. V niektorých prípadoch to, čo sa môže javiť ako útok ransomvéru, je v skutočnosti deštruktívny počítačový útok, ktorého cieľom je zničiť digitálne aktíva a údaje namiesto toho, aby ich nakoniec uvoľnili ich právoplatným vlastníkom. Pri deštruktívnych útokoch sa na vymazanie systémových komponentov používa škodlivý softvér s cieľom poškodiť údaje a znefunkčniť podnikové zariadenia. Po odcudzení citlivých údajov sa ransomvérové gangy ako Sabbath či Blackbyte následne pokúšajú zničiť zálohy.[13] Aj napriek Rusko-ukrajinského konfliktu z februára 2022 boli identifikované vnútorné rozpory medzi jednotlivými členmi ransomvérového kartelu Conti, čo viedlo k zverejneniu a následnému odhaleniu ich konverzácií, zdrojového kódu ransomvéru Conti a vnútornej štruktúry ransomvérovej skupiny Conti, jej taktiky, spoločných techník a postupov[14] [15] Uniknutý zdrojový kód ransomvéru Conti t.j. encryptor, decryptor a builder je dostupný od 1. marca 2022 na online trhovisku v najväčšej zbierke a agregovaných zdrojových kódov malvéru, vzoriek a dokumentov na internete.[16] Uniknuté dokumenty obsahujú okrem iného aj školiace materiály vrátane videí online kurzov v ruštine, ako aj návod na použitie z vybraných kategórií ako Cobalt Strike, Metasploit, powershell pre pentesterov, útoky na WMI a obrana[17][18], Active Directory a iné. Predmetné znalosti implementácie adresárových služieb LDAP vyvinuté firmou Microsoft na použitie v operačných systémoch Microsoft Window, ktoré umožňuje administrátorom firiem a organizácií nastavovať bezpečnostnú politiku, inštalovať programy na viacero počítačov alebo aplikovať kritické aktualizácie v celej organizačnej štruktúre umožňujú kyberzločincom pri počítačových útokoch správne nasadenie ransomvéru do infraštruktúry napadnutej obete, tak aby boli všetky súbory zašifrované. Cieľom ransomvérových skupín je získať účet administrátora respektíve vytvoriť konto s administrátorským povolením, aby boli schopný získať všetky systémové práva predtým, ako použijú stratégiu na zmapovanie a infikovanie

[13] https://www.picussecurity.com/resource/ttps-used-by-blackbyte-ransomware-targeting-critical-infrastructure
[14] https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member/
[15] https://twitter.com/vxunderground/status/1498060366445613056
[16] https://share.vx-underground.org/Conti/
[17] https://www.varonis.com/blog/wmi-windows-management-instrumentation
[18] https://www.sans.org/blog/investigating-wmi-attacks/

infraštruktúry siete svojej obete. Po spustení skriptu PowerShell sa ransomvér rozšíri do počítačov obete. V niektorých prípadoch môže byť škodlivý súbor, ktorý skript PowerShell stiahol, zamaskovaný ako obrázok PNG. Verejný kľúč použitý na tento účel je trvalo uložený v module škodlivého kódu.



Obrázok č.1 Grafická vizualizácia z priebehu ransomvérového útoku

Ransomvérové skupiny zneužívajú väčšinou aj niekoľko zraniteľností v Microsoft Exchange Server a to tak, že skenujú a kontrolujú sieť ich potencionálnych cieľov na prítomnosť zraniteľností: CVE-2021-34473, CVE-2021-34523 a CVE-2021-31207. Následne zneužívajú zraniteľnosti ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) nájdené v serveri Microsoft Exchange Server na získanie počiatočného prístupu do cieľovej siete. Po získaní privilegovaných prístupov a prístupových hesiel ransomvéroví útočníci prenesú Cobalt Strike Beacon do počítača obete za pomoci webshellu. Akonáhle je tzv. beacon umiestnený, do počítača obete sa stiahne aplikácia AnyDesk alebo iná, ktorá umožňuje vzdialené ovládanie počítača. [19] Spoločnosť Intel 471 začiatkom roka 2022 identifikovala ďalšie ransomvérové skupiny - BlackByte a Karakurt - ktoré sa podobne výrazne prekrývajú s ransomvérovými útokmi Conti a v skutočnosti môžu byť jednoducho rebrandovanými operáciami ransomvérovej skupiny Conti. [20]Okrem toho niektoré partnerské skupiny a

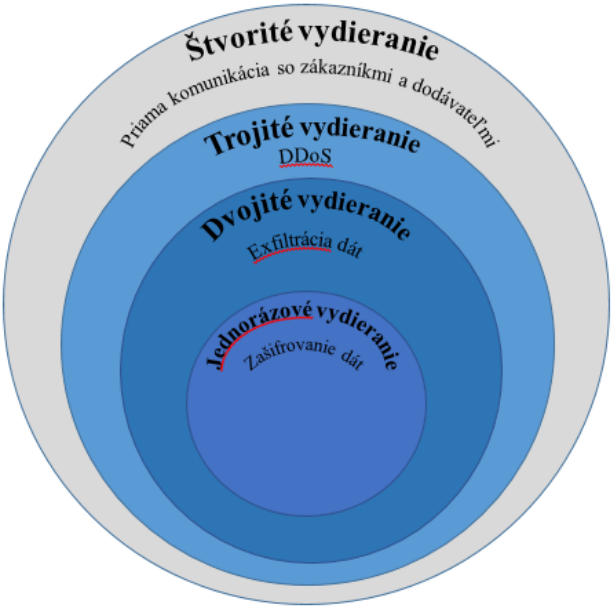
[19] Beaconing - beaconing je prípad, keď malvér pravidelne kontaktuje útočníkov server C2, aby získal ďalšie pokyny na vykonanie úloh na počítači obete. Frekvenciu, s akou sa malvér hlási a metódy používané na komunikáciu konfiguruje útočník

[20] https://intel471.com/resources/whitepapers/ransomware-variants

vývojári ransomvérovej skupiny Conti uzavreli spojenectvá s inými ransomvérovými skupinami vrátane Ryuk, Maze, LockBit 2.0, BlackCat, Hive a HelloKitty alias FiveHands. V máji 2022 uzavreli ďalšie partnerské skupiny ransomvéru CONTI uzavreli spojenectvo s ďalšími aktívnymi ransomvérovými skupinami typu RaaS: ALPHV alias BlackCat; AvosLocker a Hive.

Pokračujúcim trendom vydierania ransomvérovými skupinami je aj naďalej tzv .dvojité vydieranie, známe aj ako "zaplaťte teraz, alebo budete vyplatení", a stáva sa čoraz častejšie neoddeliteľnou súčasťou stratégie ransomvéru, pretože ransomvérové gangy využívajú tieto metódy na zmiešané útoky na kritickú infraštruktúru po celom svete. (Obrázok č.2).

Útočníci najprv exfiltrujú veľké množstvo súkromných informácií a potom zašifrujú súbory obete. Po zašifrovaní útočníci hrozia zverejnením údajov, ak sa nezaplatí výkupné. Mnohé organizácie nie sú na tieto druhy ransomvérových útokov pripravené, čo ich po infiltrácii ich podnikového prostredia núti zamyslieť sa nad svojimi bezpečnostnými opatreniami. Techniky dvojitého vydierania ransomvérom expandovali do taktiky viacnásobného vydierania. Pri tomto typu útoku útočníci nielen zašifrujú a exfiltrujú súbory organizácie, ale aj pomenujú firmy/organizácie, ohrozia reputáciu firmy/organizácie tlačovou správou s oznamom o tom, že firma/organizácia bola napadnutá a/alebo sa vyhrážajú ďalšími počítačovými útokmi (napr. distribuovaným odmietnutím služby DDoS prípadne telefonicky kontaktujú zákazníkov a dodávateľov obetí). Po zašifrovaní útočníci hrozia zverejnením údajov, ak sa nezaplatí výkupné. Útočníci niekedy aj napriek zaplateniu výkupného môžu exfiltrované údaje obete dať dražbu na lokality s licitáciou takýchto uniknutých údajov). Prípadne môžu žiadosť opätovné výkupné za nezverejnenie exfiltrovaných údajov resp. stiahnutie oznamu o exfiltrovaných údajoch z dražby tzv. „happyblogs“. Takto napadnuté obete sa zvyčajne dostávajú do pozície rukojemníkov viacerých škodlivých počítačových útokov. Tieto nátlakové taktiky môžu na organizáciu uvaliť obrovský tlak, pretože prichádzajú nielen o údaje, peniaze ale aj o svoju reputáciu.



Obrázok č.2 Techniky viacnásobného vydierania ransomvérom

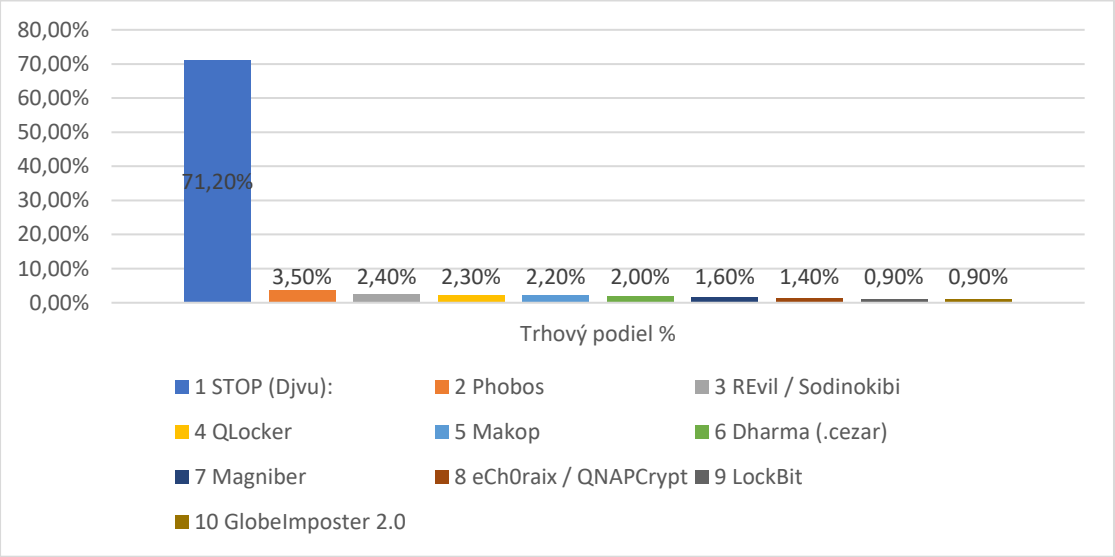
V roku 2021 boli na stránkach s únikom ransomvéru verejne zverejnené mená a dôkazy o kompromitácii 2 566 obetí, čo predstavuje 85 % nárast v porovnaní s rokom 2020. Jednotlivé ransomvérové gangy využívajú tieto viaceré taktiky ako nátlak na obete, aby zaplatili viac, rýchlejšie, hoci účinnosť tejto stratégie nátlaku a vydierania čiastočne závisí od toho, aké citlivé sú skutočne ukradnuté údaje. V roku 2021 sa objavilo 35 nových ransomvérových skupín, ktoré používali techniky dvojitého vydierania, čo znamená, že požadovali výkupné a potom informovali obete, že v prípade nezaplatenia výkupného verejne zverejnia ukradnuté údaje. (Obrázok č. 3)[21]

Obrázok č.3 Náhľad mirrorovaných stránok ransomvéru LockBIT 3.0

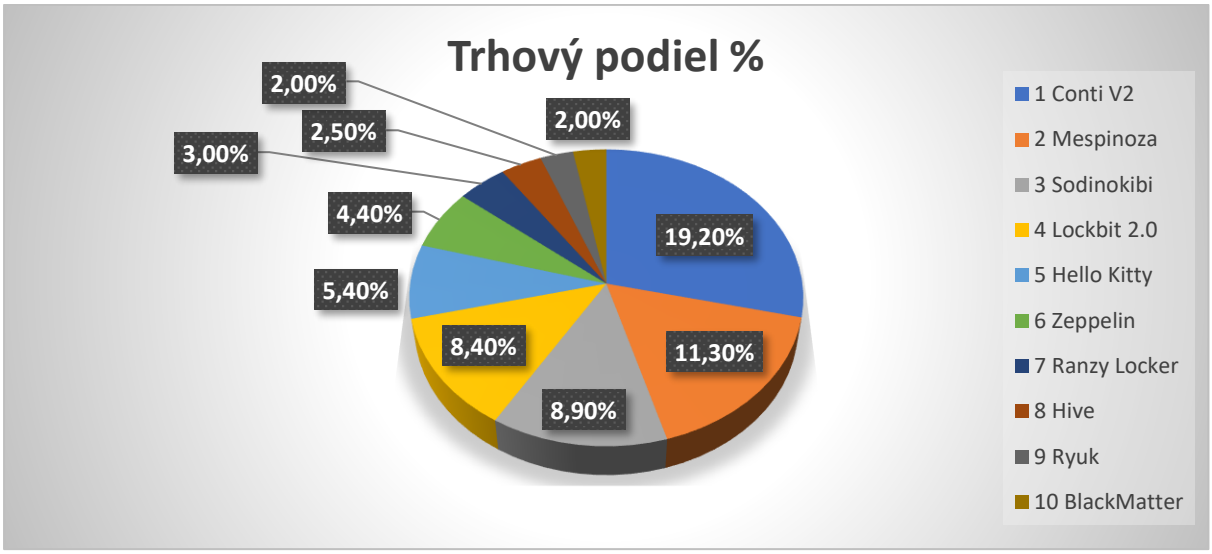
Viaceré ransomvérové skupiny ako napríklad LockBit a iné, používajú na zverejňovanie exfiltrovaných údajov z napadnutých serverov svojich ransomvérových obetí tzv. blogy alebo

[21] https://unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights

aukčné stránky so zverejneným zoznamom napadnutých firiem a organizácií s uvedením vydieračskej sumy a času, ktorý zostáva do zverejnenia exfiltrovaných údajov. Tento obsah je chránený Anti-DDOS ochranou voči DDOS útokom a je viacnásobne zrkadlený na viacerých onionových stránkach.



Graf 1 Najbežnejšie varianty ransomvéru Q2/2021



Graf 2 Najbežnejšie varianty ransomvéru Q3/2021

Percentuálna sadzba partnerského programu je 20 % z ceny výkupného, ktorú zaplatí obeť napadnutá ransomvérom LOCKBIT. Platby za výkupné pri tomto type ransomvéru ako služba pridružení partneri a členovia ransomvérovej skupiny LOCKBIT dostávajú do svojich

osobných virtuálnych peňaženiek v akejkoľvek vhodnej mene a až potom prevádzajú podiel LOCKBIT partnerský program.

Obrázok 4 Náhľad z prístupu do webového panelu ransomvéru LockBIT

Pre zaujímavosť pri výkupných sumách nad 500-tisíc dolárov však napadnutá spoločnosť uhrádza výkupné na 2 peňaženky - jedna je pridruženého partnera ransomvérovej skupiny, na ktorú obeť prevedie 80 % z ceny výkupného, a druhá kryptopeňaženka na ktorú prevedie zvyšnú časť platby 20 %, z ceny výkupného je vlastnená vývojármi ransomvéru, čím je vývojár ransomvéru poskytujúci ransomvér ako službu chránení pred podvodom od pridruženého partnera. Ransomvérové skupiny používajú väčšinou na svoju komunikáciu end-to-end šifrovaný protokol XMPP/Jabber alebo peer-to-peer protokol TOX [22]pre okamžité správy a videohovory, ktorý ponúka tiež end-to-end šifrovanie. (E2EE). Predmetný ransomvérový kit ponúkaný partnerským členom ransomvérových skupín formou RaaS služby má možnosť vytvárať súkromné chaty na tajnú komunikáciu s firmami zaoberajúcimi sa obnovou zašifrovaných údajov, čo zachováva súkromie korešpondencie a zabraňuje narušeniu vyjednávacích rokovaní pri zaplatení výkupného. Na zabezpečenie dešifrovania je garantovaná vývojármi ransomvéru maximálna ochrana dešifrovacích zariadení, aby napadnutá obeť nedešifrovala zašifrované súbory zadarmo v dôsledku akýchkoľvek zraniteľností vo webovom paneli.

[22]https://tox.chat/

Obrázok č.5 Vybrané ransomvérové skupiny používajúce techniky viacnásobného vydierania Zdroj: https://unit42.paloaltonetworks.com/wp-content/uploads/2022/03/word-image-1.jpeg

Záver

Ransomvérové skupiny naďalej predstavujú vážnu hrozbu pre firmy aj jednotlivcov. Firmy a organizácie musia okrem zavádzania potrebných osvedčených bezpečnostných postupov a bezpečnostných kontrolných mechanizmov udržiavať náskok pred technikami používanými ransomvérovými skupinami, ktoré sa snažia finančne profitovať zo zneužitia zraniteľností a krádeže intelektuálnych, organizačných a iných kritických informácií tak, aby si ochránili svoje citlivé informácie, infraštruktúru a cenné informačné aktíva. Obetiam ransomvéru hrozí, že v dôsledku takýchto útokov prídu o cenné údaje ich zašifrovaním, čo má za následok finančné straty a stratu produktivity. Ak obeť nie je schopná alebo ochotná zaplatiť výkupné, ransomvérové skupiny môžu tieto údaje exfiltrovať alebo predať online na aukcii údajov, čím ohrozia citlivé údaje používateľov z firiem, organizácií a jednotlivcov

a spôsobia stratu reputácie napadnutej firme. Dôležité je, aby boli údaje firiem a organizácií pravidelne zálohované, predmetné zálohy logovacích prístupov izolované, konfigurácie systémov zabezpečené a systémy pravidelne updatované - je potrebná detekcia každej anomálnej akcie v reálnom čase. V priebehu rokov 2021 a začiatkom roka 2022 bola identifikovaná rekordná úroveň aktivity ransomvérových skupín aj napriek prebiehajúcemu konfliktu Rusko/Ukrajina. Novou taktikou je spolupráca a spájanie jednotlivých ransomvérových skupín do kartelov, či tzv. rebrandovanie existujúcich ransomvérových skupín, ktoré používajú predmetné ransomvérové kartely za sťaženie ich identifikácie a takisto nábor nových členov či preberanie jednotlivých členov z iných ransomvérových gangov.

Zoznam použitej literatúry

ARMOR. 2021. Almer Elsad [online]. © 2021 [zverejnené 2021-11-11]. Dostupné na URL:

https://res.armor.com/resources/threat-intelligence/living-off-the-land-attacks

BANKINFOSECURITY.2022. [online]. © 2022 [zverejnené 2022-02-14]. Dostupné na URL: https://www.bankinfosecurity.com/ransomware-groups-such-as-blackcat-are-turning-to-rust-a-18507

ESET.2021. Soumik Ghosh [online]. © 2021 [zverejnené 2021-12-16]. Dostupné na URL: https://www.eset.com/sk/o-nas/press-centrum/eset-tlacove-spravy/kriticka-zranitelnost-log4shell-ohrozuje-aj-slovenske-firmy-eset-zablokoval-tisicky-pokusov-o-utok/

HIVE PRO. 2022. [online]. © 2022 [zverejnené 2022-04-05]. Dostupné na URL: https://www.hivepro.com/deep-panda-deploys-new-rootkit-fire-chili-by-exploiting-log4shell-in-vmware-horizon/

CHECKPOINT.2022. [online]. © 2022 [zverejnené 2022-01-21]. Checkpoint Sofware 2022 Security Report: Global Cyber Pandemic Magnitude Revealed. Dostupné na URL: https://pages.checkpoint/cyber-security-report-2022.html

INTEL 471.2022. [online]. © 2022 [zverejnené 2022-03-14]. Ransomware Variant. Dostupné na URL: https://intel471.com/resources/whitepapers/ransomware-variants

MALWAREBYTES.2022. [online]. © 2022 [zverejnené 2022-01-11]. Dostupné na URL: https://blog.malwarebytes.com/ransomware/2022/01/night-sky-the-new-corporate-ransomware-demanding-a-sky-high-ransom/

PICUS SECURITY INC.2022. [online]. [zverejnené 2022-02-21]. Dostupné na URL:

https://www.picussecurity.com/resource/ttps-used-by-blackbyte-ransomware-targeting-critical-infrastructure

SANS Institute.2019 © 2019[online]. [zverejnené 2019-02-09]. Dostupné na URL: https://www.sans.org/blog/investigating-wmi-attacks/

THE RECORD.2022. Catalin Cimpanu [online]. [zverejnené 2022-02-27]. Dostupné na URL: https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member/

TRELLIX.2022. [online]. © 2022 [zverejnené 2022-04-27]. Trellix Threat Labs Research Report April 2022. Dostupné na URL: https://www.trellix.com/en-us/assets/docs/threat-reports/trellix-atr-report-apr-2022.pdf

Unit 42.2022. [online]. © 2022 [zverejnené 2022-03-24]. Unit 42 Ransomware Threat Report Highlights: Ransomware Remains a Headliner. Dostupné na URL: https://unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights

VARONIS. 2020. [online]. © 2022 [zverejnené 2020-08-12]. Dostupné na URL:

https://www.varonis.com/blog/wmi-windows-management-instrumentation

VX-UNDERGROUND.2022 [online]. [zverejnené 2022-02-27]. Dostupné na URL: https://twitter.com/vxunderground/status/1498060366445613056

Kontaktné údaje

mjr. Mgr. Martin Mišota

Odbor počítačovej kriminality,

Národná centrála osobitných druhov kriminality,

Prezídium Policajného zboru

E-mail: martin.misota@minv.sk

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

PhDr. Peter Veselý, PhD.

Vybrané techniky detekcie deepfake obsahu

Marek Petrik

Abstrakt:

Príspevok sa zaoberá fenoménom syntetických médií deepfake v online prostredí. Analyzuje techniky a postupy, prostredníctvom ktorých môžu byť používatelia schopní detegovať deepfake, a tiež nástroje, ktoré môžu byť využité na automatickú detekciu. Autor v závere príspevku poukazuje aj na možné pozitívne využitie technológií, ktoré súvisia s deepfake. Predmetná problematika je spracovaná v súvislosti s témou autorovej dizertačnej práce s názvom „Ochrana pred pokročilými kybernetickými útokmi“, ktorá je súčasťou riešenia medzinárodnej vedeckovýskumnej úlohy „Metódy spracovania policajne relevantných informácií - Výsk. 161“ na Katedre informatiky a manažmentu Akadémie PZ v Bratislave.

Kľúčové slová:

deepfake, umelá inteligencia, neurónové siete

Abstract:

The paper deals with the phenomenon of deepfake synthetic media in the online environment. It analyses the techniques and procedures through which users may be able to detect deepfakes, as well as the tools that can be used for automated detection. At the end of the article, the author points out the possible positive use of technologies related to deepfake. The present issue is treated in the context of the author's dissertation topic entitled „Protection against advanced cyber attacks”, which is part of the international scientific research project „Methods of processing police-relevant information - Research 161” at the Department of Informatics and Management of the Academy of the Police Force in Bratislava.

Keywords:

deepfake, artificial intelligence, neural networks

Úvod

Fenomén deepfake sa stáva čoraz väčším problémom a hrozbou v modernom online svete. Falošné a upravené videá s výrokmi známych politikov a osobností, či fotografie alebo rôzne videá s tvárami celebrít sa objavujú na internete stále častejšie. Odlíšiť kvalitne spracovaný deepfake obsah od reality môže byť neraz značne zložité. Deepfake médiá vznikajú prostredníctvom pokročilých technológií, ktoré boli v minulosti pre bežného používateľa internetu a digitálnych technológií len ťažko dostupné. Ide o technológie ako napríklad mapovanie tváre a umelá inteligencia, ktoré dokážu zamieňať tvár digitálne zobrazenej osoby za tvár inej osoby. Dnes už však existujú aplikácie a webové platformy, ktoré sú bežne dostupné a ich používateľské rozhranie je veľmi intuitívne a jednoduché. Deepfake obsah je ťažké odhaliť, pretože pri jeho tvorbe sú využité aj skutočné zábery, môže mať autenticky znejúci zvuk a v mnohých prípadoch je svojím obsahom optimalizovaný na rýchle šírenie sa na

sociálnych sieťach.[1] Mnoho používateľov tak automaticky predpokladá, že obsah, ktorý sledujú, zodpovedá realite. V príspevku sa budeme venovať vybraným technikám, ako odhaliť deepfake obsah.

Pojem deepfake

Pojem deepfake vznikol slovným spojením termínov „deep“ a „fake“. Slovo „deep“ v tomto prípade vychádza z podoblasti strojového učenia, ktorá sa nazýva „deep learning“, v preklade „hlboké učenie“, ktoré je na tvorbu syntetických médií deepfake používané.[2] Strojové učenie je podoblasťou kategórie s názvom umelá inteligencia. Deepfake je druh syntetického média predstavujúci obrazový, zvukový alebo obrazovo-zvukový obsah, ktorý je buď manipulovaný, alebo úplne generovaný umelou inteligenciou s cieľom využiť ho na dezinformačné účely.[3] Väčšina autorov vo svojich štúdiách používa termíny deepfake a syntetické médiá ako synonymá. Pojmy deepfake a syntetické médiá však nie je vhodné zamieňať. Hlavným rozdielom medzi deepfake a syntetickými médiami je zámer tvorcu. Deepfake obsah je vytváraný so škodlivým zámerom, ako napríklad zavádzanie, šikanovanie, šírenie falošných správ a podobne.[4]

Detekcia používateľom

Vznik technológie deepfake a najmä hrozby, ktoré deepfake obsah predstavuje, zdôrazňujú naliehavú potrebu využívania vhodných a efektívnych metód ich detekcie. Jednou zo základných techník odhaľovania deepfake obsahu je nepochybne vzdelávanie používateľov s cieľom, aby dokázali účinne rozlíšiť reálny obsah od falošného. Medzi ďalšie techniky patrí využívanie softvérových nástrojov pre automatickú strojovú detekciu. V nasledujúcej časti analyzujeme techniky a postupy, prostredníctvom ktorých môžu byť používatelia schopní detegovať deepfake, a tiež nástroje, ktoré môžu byť využité na automatickú detekciu.

V súvislosti so syntetickými médiami, ktoré boli upravené alebo vytvorené umelou inteligenciou, neexistujú žiadne zaručené znaky, podľa ktorých by bolo možné s určitosťou odhaliť deepfake. Rozpoznanie deepfake obsahu je pre bežného používateľa pomerne zložité, najmä ak ide o kvalitný a prepracovaný deepfake. Vzhľadom na neustále dynamické

[1] WESTERLUND, M., 2019. *The Emergence of Deepfake Technology: A Review*. [online] [cit. 14.05.2022]. Dostupné na internete: <https://www.researchgate.net/publication/337644519_The_Emergence_of_Deepfake_Technology_A_Review>
[2] VRABEC, N. – PIEŠ, L., 2021. *Spoločenské ohrozenia v dôsledku fenoménu deepfakes*. s. 120.
[3] MESARČÍK, M., – ZIMEN, O., 2019. *Deep Fakes a ochrana súkromia.* [online] [cit. 10.05.2022]. Dostupné na internete: <*https://afi.flaw.uniba.sk/index.php/AFI/article/ download/51/44/87*>
[4] VRABEC, N. – PIEŠ, L., 2021. *Spoločenské ohrozenia v dôsledku fenoménu deepfakes*. s. 120.

zdokonaľovanie technológií a umelej inteligencie, tak v budúcnosti bude pre bežného používateľa čoraz zložitejšie odhaliť uvedený falošný obsah. Pri menej kvalitnom deepfake je však možné zamerať sa na nasledujúce aspekty:

Rysy tváre

- **Oči a ich pohyb** – jedným z indikátorov deepfake videa môže byť nežmurkanie alebo nadmerné, prípadne neprirodzené žmurkanie zobrazenej osoby. Druhým ukazovateľom je samotný pohyb očí. Napríklad v prípade, keď oči majú tendenciu neprerušene sledovať osobu, s ktorou sa hovorí. Je potrebné zamerať sa aj na nekonzistentné osvetlenie a odrazy na dúhovke očí.
- **Obočie** – ide najmä o neprirodzený pohyb obočia a nesprávne zobrazenie jeho tieňov.
- **Okuliare** – odlesky v okuliaroch a zlyhávanie fyziky odrazov svetla.
- **Výrazy tváre** – predovšetkým tie neprirodzené, ako napríklad nos smerujúci iným smerom ako hlava, nevyjadrovanie alebo prehnané vyjadrovanie emócií.
- **Vlasy a ochlpenie** – najmä ich nereálny pohyb a vykreslenie jemných detailov.
- **Koža** – odtieň kože niektorých častí nemusí zodpovedať zvyšku tváre alebo dokonca tela. Ďalej je to neprirodzené vykreslenie starnutia kože a vrások, ktoré nemusí korešpondovať so zdanlivým vekom vlasov, očí alebo zobrazenej osoby všeobecne. Zvýšenú pozornosť je potrebné venovať aj drobným kožným znakom, ako sú materské znamienka alebo tetovania.
- **Pery** – veľkosť a farba pier nemusí zodpovedať zvyšku tváre zobrazenej osoby.
- **Zuby** – niektoré algoritmy na tvorbu deepfake obsahu nie sú schopné generovať presné obrysy jednotlivých zubov.[5]

Rysy tela

- **Poloha tela alebo držanie tela** – neprirodzene vyzerajúce držanie tela, prípadne nekonzistentné umiestnenie hlavy voči telu.
- **Pohyb tela** – pohyby zobrazené v deepfake videách môžu byť skreslené, najmä v prípadoch, keď zobrazená osoba pohybuje hlavou.[6]

[5] GROH, M., 2020. *Detect DeepFakes: How to counteract misinformation created by AI.* [online] [cit. 14.05.2022]. Dostupné na internete:<https://www.media.mit.edu/projects/detect-fakes/overview/>
[6] JOHANSEN, A., 2020. *What are deepfakes and how to spot them.* [online] [cit. 14.05.2022]. Dostupné na internete: <https://us.norton.com/internetsecurity-emerging-threats-what-are-deepfakes.html>

Hlasové charakteristiky

- **Neobvyklé tempo** – neprimerané tempo reči môže spôsobiť, že reč neznie ako ľudská.
- **Konce slov** – odhaliť syntetizovanú reč môžu pomôcť aj konce slov, ktoré môžu vykazovať anomálie v porovnaní s bežnou ľudskou rečou.[7]

Všeobecné aspekty

- **Rozmazanie alebo nesprávne zarovnanie okrajov** – viditeľné najmä na rozhraniach a okrajoch vizuálnych štruktúr, napríklad na rozhraní tváre a zvyšku tela.
- **Nekonzistentný šum alebo zvuk** – v tejto súvislosti ide najmä o zlú synchronizáciu pier so zvukom, robotické hlasy, podivnú výslovnosť alebo dokonca úplnú absenciu niektorých zvukov.[8]

Na uľahčenie odhalenia deepfake obsahu pomocou niektorých vyššie uvedených tipov je možné používateľmi využiť napríklad aj akýkoľvek softvér na úpravu videa, ktorý je schopný spomaliť rýchlosť prehrávaného obsahu. Predmetný softvér tak poskytne lepšie podmienky na skúmanie videa, napríklad pri spomalení pohybov očí alebo pier, čím je možné odhaliť nezrovnalosti naznačujúce, že s obsahom bolo manipulované. Na uvedené účely sú využiteľné aj internetové vyhľadávače, ako napríklad Google, pomocou ktorého je možné spätne nájsť pôvodný obsah. Odhaliť kvalitne spracovaný deepfake nie je jednoduché, ale praxou si používatelia môžu vybudovať určitú mieru intuície pre posúdenie toho, čo je falošné a čo skutočné.[9]

Strojová detekcia

V súčasnosti existuje množstvo softvérových nástrojov na detekciu deepfake obsahu, ktoré sa líšia v sofistikovanosti, miere presnosti a ich dostupnosti pre bežných používateľov. Jednou z hlavných myšlienok týchto nástrojov je poskytnúť spoľahlivú detekčnú techniku odborníkom aj bežným používateľom s cieľom predchádzať hrozbám ako sú napríklad masové dezinformácie. Niektoré z nich pracujú s kontrolou metadát a obsah kontrolujú po jednotlivých bajtoch. Sofistikovanejšie nástroje hľadajú neobvyklé spektrálne korelácie v hlasoch

[7] JOHNSON, D., 2020. *Audio Deepfakes: Can Anyone Tell If They're Fake?* [online] [cit. 14.05.2022]. Dostupné na internete: <https://www.howtogeek.com/682865/audio-deepfakes-can-anyone-tell-if-they-are-fake/>
[8] JOHANSEN, A., 2020. *What are deepfakes and how to spot them.* [online] [cit. 14.05.2022]. Dostupné na internete: <https://us.norton.com/internetsecurity-emerging-threats-what-are-deepfakes.html>
[9] GROH, M., 2020. *Detect DeepFakes: How to counteract misinformation created by AI.* [online] [cit. 14.05.2022]. Dostupné na internete:<https://www.media.mit.edu/projects/detect-fakes/overview/>

generovaných hlbokými neurónovými sieťami (DNN)[10]. Neustály vývoj a zlepšovanie v oblasti tvorby deepfake obsahu tiež vytvára tlak aj na vývoj a zdokonaľovanie detekčných nástrojov.

Väčšinu metód detekcie deepfake obrázkov nemožno použiť na detekciu deepfake videa z dôvodu značného zhoršenia kvality jednotlivých snímok (frames) v dôsledku kompresie. Videá tiež majú aj časové charakteristiky, ktoré sa medzi jednotlivými skupinami snímok líšia. Na základe uvedeného je možné rozlišovať dve hlavné skupiny nástrojov na detekciu deepfake videí a to nástroje, ktoré skúmajú časové vlastnosti a nástroje, ktoré skúmajú vizuálne artefakty.

Metódy využívajúce časové prvky skúmajú vizuálne artefakty a ich výskyt v rámci snímok videa. Pri manipulácii s jednotlivými snímkami v nástrojoch na vytváranie deepfake obsahu vznikajú nekonzistentnosti medzi snímkami, ktoré možno využiť na detekciu deepfake videa. Ďalšia metóda využívajúca časové prvky sa zameriava na analýzu rôznych fyziologických znakov, ako napríklad frekvencia žmurkania očí.[11]

Druhou skupinou sú metódy detekcie založené na vizuálnych artefaktoch. Predmetná metóda spočíva v tom, že video je rozložené na jednotlivé snímky, z ktorých sa extrahujú rôzne vlastnosti slúžiace na odlíšenie skutočných a falošných snímok. Predmetná metóda vychádza zo skutočnosti, že deepfake videá sú zvyčajne vytvorené s nižším rozlíšením, čo spôsobuje rôzne deformácie zobrazovanej tváre. Uvedený postup vytvára artefakty, ako napríklad nesúlad rozlíšenia medzi deformovanou oblasťou a zobrazovaným okolím.[12] Predmetné artefakty možno odhaliť pomocou konvolučných neurónových sietí.[13]

Online detekčné nástroje

Jedným z najznámejších online nástrojov na detekciu deepfake obsahu je platforma spoločnosti Sensity, ktorá bola sprístupnená verejnosti v januári 2021. Predmetný nástroj na odhaľovanie deepfake obsahu využíva kombináciu algoritmov hlbokého učenia a automatizácie. Používateľ má možnosť v intuitívnom prostredí jednoducho a rýchlo odhaliť falošné fotografie a videá z kategórie deepfake. Analyzovať je možné video formáty .mp4, .mov a fotografie vo formátoch .png, .jpeg, .jfif a .tiff. Podozrivý obsah je potrebné nahrať do web

[10] Hlboké neurónové siete (Deep Neural Networks – DNN) sú veľmi výkonné modely strojového učenia, ktoré sú určené na riešenie zložitých problémov, ako je rozpoznávanie reči či vizuálnych objektov.
[11] NGUYEN, T. et al., 2019. *Deep Learning for Deepfakes Creation and Detection: A Survey.* [online] [cit. 13.05.2022]. Dostupné na internete: <https://www.researchgate.net/publication/336055871_Deep_Learning_for_Deepfakes_Creation_and_Detection_A_Survey>
[12] ALMARS, A., 2021. Deepfakes Detection Techniques Using Deep Learning: A Survey. [online] [cit. 10.05.2022]. Dostupné na internete: <https://www.researchgate.net/publication/336055871_Deep_Learning_for_Deepfakes_Creation_and_Detection_A_Survey>
[13] V hlbokom učení (deep learning) je konvolučná neurónová sieť (CNN alebo ConvNet) triedou umelej neurónovej siete, ktorá sa najčastejšie používa na analýzu vizuálnych snímok.

rozhrania a následne spustiť analýzu. Stránka tiež obsahuje zoznam celebrít a ľudí, ktorých tváre sú v deepfake videách zneužívané najčastejšie. Pri samotných videách tento nástroj analyzuje tzv. „face swap“, teda výmenu tváre osoby na videu. Nástroj sa učí postupne aj s pribúdajúcimi príkladmi deepfake obsahu. Používateľ môže skontrolovať deepfake video aj len na základe URL adresy. Analýza videa trvá nanajvýš pár minút, no bežne dokáže deepfake odhaliť už za pár sekúnd. Kontrola deepfake fotografií prebieha obdobne, kde nástroj kontroluje a overuje „face swap“, no navyše aj generované „GAN“ obrázky. Technológia GAN (Generative Adversarial Networks) bola predstavená ešte v roku 2014. Ide o novú neurónovú sieť, ktorá dokáže s využitím umelej inteligencie vytvárať komplexné obrazové výstupy. Tento nástroj však môže byť zneužitý aj na vytváranie deepfake fotiek. GAN proti sebe stavia dva algoritmy umelej inteligencie. Prvému algoritmu, známemu ako generátor, sa podáva náhodný šum, ktorý sa postupne premení na obraz. Uvedený syntetický obraz sa potom pridá k množstvu skutočných obrazov, napríklad celebrít, ktoré sa vložia do druhého algoritmu, známeho ako diskriminátor. Spočiatku sa syntetické obrazy vôbec nepodobajú tváram. Pri dostatočnom počte cyklov a spätnej väzbe začne generátor vytvárať úplne realistické tváre úplne neexistujúcich osobností. A práve takéto úpravy pomocou GAN analyzuje aj zverejnený nástroj od startupu Sensity, ktorý dokáže vyhodnotiť, či fotografia prešla týmto procesom úpravy. K výsledku celej analýzy má používateľ prístup hneď pod fotografiou alebo videom, pričom dostane aj percentuálny výsledok, ktorý vypovedá o tom, do akej miery si je nástroj istý, že ide o deepfake obsah. Správa o analýze je následne odoslaná aj na email.

Medzi ďalšie známe softvérové nástroje na odhalenie deepfake obsahu patrí napríklad open-source forenzný nástroj Deepware Scanner, Microsoft Video Authenticator, DeepDetector & DeepfakeProof from DuckDuckGoose, Reality Defender alebo online platforma Deepfake-o-Meter.

Záver

Na účinnú detekciu deepfake obsahu je nevyhnutné neustále vzdelávanie, mediálna gramotnosť a kritické myslenie používateľov internetu. Bežní používatelia internetu si musia uvedomiť, že technológie na tvorbu falošného vizuálneho obsahu sú už dnes bežne dostupné a nástroje na výmenu tvárí sú jednoducho použiteľné. Vytváranie realistického a bezchybného deepfake multimediálneho obsahu si však vyžaduje hlbšie znalosti a profesionálny softvér. Súčasné spôsoby regulácie šírenia deepfake obsahu je možné považovať za nedostatočné a ani nástroje na detegovanie deepfake médií nezaručujú úplnú presnosť odhalenia každého podvrhnutého obsahu. Používatelia digitálnych technológií by mali kriticky pristupovať k

mediálnemu obsahu a overovať si pravosť obsahu videa, obrázka či zvuku pred ďalším jeho šírením. Vzhľadom na povahu siete internet, ktorá umožňuje, aby sa akýkoľvek online obsah mohol okamžite šíriť, sa tak deepfake prostredníctvom internetu môže dostať k cieľovej skupine ešte pred jeho včasnou detekciou.

Využívanie umelej inteligencie a technológií, na ktorých deepfake stojí, v budúcnosti nepochybne prinesie aj množstvo pozitívnych vplyvov. Technika strojového učenia GAN môže nájsť uplatnenie napríklad pri anonymizácii videí s cieľom skryť identitu skutočných ľudí, ktorí sú zobrazení vo videách alebo na fotografiách a ktorí z rôznych dôvodov nemajú byť poznaní. Pomocou GAN tak bude možné vytvoriť úplne novú tvár s rovnakým výrazom a pridať ju do pôvodnej fotografie či videa, pričom ostane zachované rovnaké pozadie. Výraz tváre (aj keď inej), ktorý je často na videu či fotografii to najvýznamnejšie, tak môže ostať do určite miery zachovaný. Anonymizácia tváre je v súčasnosti využívaná napríklad na ochranu identity osoby, ktorá je zachytená na fotografiách či video záznamoch a vystupuje napríklad ako poškodený alebo oznamovateľ trestného činu. Tradičné techniky, ako je rozmazanie alebo začernenie tváre, v sebe zahŕňajú riziko, že výsledok bude neúplný alebo nedokonalý, čím môže dôjsť k prezradeniu identity zobrazenej osoby. Tradičné techniky anonymizácie tváre tiež úplne odstraňujú výraz a emócie zobrazené v tvári, ktoré môžu byť dôležité pre kontext daného videa alebo fotografie. Vzhľadom na to, že GAN vôbec nepoužíva pôvodnú tvár osoby, sú uvedené nedostatky tradičnej anonymizácie tváre eliminované. Technológiu GAN tiež možno efektívne použiť aj na anonymizáciu hlasov.

Zoznam použitej literatúry

ALMARS, A., 2021. *Deepfakes Detection Techniques Using Deep Learning: A Survey*. [online] [cit. 10.05.2022]. Dostupné na internete: <https://www.researchgate.net/publication/336055871_Deep_Learning_for_Deepfakes_Creation_and_Detection_A_Survey>

BULAKH, A., 2021. *Synthetic Media and Deepfakes – Where Can Fun Turn Into Harm?* [online] [cit. 13.05.2022]. Dostupné na internete: <https://blog.reface.ai/synthetic-media-and-deepfakes/>

GROH, M., 2020. *Detect DeepFakes: How to counteract misinformation created by AI.* [online] [cit. 14.05.2022]. Dostupné na internete: <https://www.media.mit.edu/projects/detect-fakes/overview/>

GÜERA, D. – DELP, E., 2018. *Deepfake Video Detection Using Recurrent Neural Networks.* [online] [cit. 14.05.2022]. Dostupné na internete: <https://gangw.web.illinois.edu/class/cs598/papers/AVSS18-deepfake.pdf>

JOHANSEN, A., 2020. *What are deepfakes and how to spot them.* [online] [cit. 14.05.2022]. Dostupné na internete: <https://us.norton.com/internetsecurity-emerging-threats-what-are-deepfakes.html>

JOHNSON, D., 2020. *Audio Deepfakes: Can Anyone Tell If They're Fake?* [online] [cit. 14.05.2022]. Dostupné na internete: <https://www.howtogeek.com/682865/audio-deepfakes-can-anyone-tell-if-they-are-fake/>

MESARČÍK, M. – ZIMEN, O., 2019. *Deep Fakes a ochrana súkromia.* [online] [cit. 10.05.2022]. Dostupné na internete: *<https://afi.flaw.uniba.sk/index.php/AFI/article/download/51/44/87>*

NASU, H., 2022. *Deepfake Technology in the Age of Information Warfare*. [online] [cit. 10.05.2022]. Dostupné na internete: <https://lieber.westpoint.edu/deepfake-technology-age-information-warfare/>

NGUYEN, T. et al., 2019. *Deep Learning for Deepfakes Creation and Detection: A Survey.* [online] [cit. 13.05.2022]. Dostupné na internete: <https://www.researchgate.net/publication/336055871_Deep_Learning_for_Deepfakes_Creation_and_Detection_A_Survey>

VRABEC, N. – PIEŠ, L., 2021. *Spoločenské ohrozenia v dôsledku fenoménu deepfakes*. In: Marketing identity 2021: Nové zmeny, nové šance: Zborník z medzinárodnej vedeckej konferencie. Trnava: UCM, 2021. s. 119 – 125. ISBN 978-80-572-0219-6.

WESTERLUND, M., 2019. *The Emergence of Deepfake Technology: A Review*. [online] [cit. 14.05.2022]. Dostupné na internete: https://www.researchgate.net/publication/337644519_The_Emergence_of_Deepfake_Technology_A_Review

Kontaktné údaje

npor. JUDr. Marek Petrik

Katedra informatiky a manažmentu – externý doktorand

Akadémia Policajného zboru v Bratislave

e-mail: marek.petrik4@minv.sk

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

PhDr. Peter Veselý, PhD.

Bezpečné zálohovanie dát pomocou technického vybavenia

Zuzana Sochuľáková - Zlatica Geročová

Anotácia:

Článok sa zaoberá bezpečným zálohovaním údajov prostredníctvom technických zálohovacích zariadení. V prvej kapitole si stručne rozoberieme čo predstavuje slovné spojenie záloha údajov a aké dôležité je pravidelné zálohovanie dát, aby sme predišli ich strate. V druhej kapitole sa zameriavame na technické vybavenie zálohovacích zariadení a v poslednej tretej kapitole sme urobili dotazník, v ktorom sme sa pýtali účastníkov, aké technické zálohovacie zariadenia preferujú a porovnáme a analyzujeme si parametre dvoch zariadení, ktoré získali najvyšší počet hlasov.

Kľúčové slová: informácia, bezpečnosť, zálohovanie, informačná bezpečnosť

Abstract: The introductory part of the article draws attention to the study field of security sciences and draws attention to the possibilities of studying this field in Slovakia. In the next part we deal with the issue of promotion of an educational institution operating in the field of security on the internet. The main goal is to propose solutions to bring to the attention of the general public the opportunity to study the Department of Security Science at USM. To obtain the goal we used the method of observation and experiment where in the end we proposed the possibilities of promotion together with the implementation schedule using a table according to the framework See Think Do Care.

Keywords: information, security, backup, information security

Úvod

Záloha dát je v dnešnej dobe veľmi dôležitá a je potrebné poznať spôsoby zálohovania dát, a to hlavne z dôvodu, aby sme predišli strate dôležitých súborov. Takmer každý v súčasnosti vlastní určité súbory o ktoré by nechcel prísť. Jedná sa predovšetkým o vlastnoručne vytvorené súbory, ktoré sú samé o sebe originálne a nie je možné ich získať z iných zdrojov. Reč je hlavne o rôznych pracovných textoch, tabuľkových dokumentoch, vzácnych fotografiách, alebo iných multimediálnych súboroch, ktoré sú spravidla výsledkom našej dlhodobej práce. S rýchlym rozvojom informačných technológií sa rozvíjajú aj zariadenia, prípadne programy, na ktoré si ukladáme naše dôležité súbory.

Najlepšou prevenciou pred stratou dát, je práve ich časté a pravidelné zálohovanie. V dnešnej dobe existuje niekoľko možností, ako si dáta vieme zálohovať a tak zabezpečiť, aby sme k ním neskôr mali taktiež prístup.

Bezpečné zálohovanie

Záloha je kópia údajov, ktoré sú vytvorené v určitom časovom bode. Táto kópia je uchovávaná počas jej doby použiteľnosti vo formáte, ktorý je bežne používaný. Vytvorené záložné súbory bývajú zvyčajne uložené nezávisle na inom mieste, než ich zdrojové údaje. [1]

Zálohovanie je proces vytvorenia kópie údajov, ktorá môže byť fyzicky umiestnená kdekoľvek mimo pôvodného miesta, ktorú môžeme ďalej používať a ku ktorej sa v prípade potreby môžeme zakaždým vrátiť. Cieľom zálohovania je mať údaje k dispozícii bez zbytočného oneskorenia v prípade problémov s primárnym médiom. Proces zálohovania je vykonávaný hlavne z dôvodu bezpečnosti, a to ako ochrana pred trvalou stratou údajov a z tohto dôvodu by malo byť zálohovanie súčasťou každodennej práce s dôležitými údajmi. Po vytvorení alebo akejkoľvek úprave súboru, by v optimálnom prípade mala byť vytvorená aj jeho záložná kópia. Záložná kópia slúži na obnovenie aktuálnych dát v prípade, že došlo k ich poškodeniu alebo zničeniu. [1]

Zálohovaniu je potrebné venovať veľkú pozornosť, keďže nedostupnosť dát môže byť nepredvídateľná a neočakávaná. Existuje veľa faktorov, ktoré môžu mať za následok zlyhanie, stratu alebo nedostupnosť dát, napríklad vírusy, zlyhanie aplikácií alebo systémov, ľudské používateľské alebo operátorské chyby, respektíve zámerné útoky s vymazaním či poškodením dát.

Pre ochranu dát pred zneužitím sú známe dva základné spôsoby. Prvým z nich je dostatočné zabezpečenie protokolu, ktorý dokáže dáta šifrovať, bráni rôznym útokom a zaisťuje integritu dát. Ďalšou metódou je archivácia a zálohovanie. [1]

Pre zálohovanie údajov môžeme využiť technické vybavenie zálohovacích zariadení alebo programové vybavenie zálohovacích zariadení. Zálohovanie pomocou technického vybavenia bude bližšie popísané a porovnané v nasledujúcej kapitole článku.

Technické vybavenie zálohovacích zariadení

Pod pojmom technické vybavenie zálohovacích zariadení si môžeme predstaviť všetky hmotné zariadenia, na ktoré sa dajú ukladať údaje. Technické vybavenie spadá pod „HARDWARE“. Pod pojmom „HARDWARE“ rozumieme technické vybavenie počítača. [2]

Z pohľadu zálohovania medzi technické vybavenie zaraďujeme magnetické pásky, diskové pole, Data Domain, flash disk, pamäťové karty, CD, DVD, USB kľúč, externý disk HDD alebo externý disk SSD alebo inteligentné dátové úložiská (NAS).

Diskové pole

Diskové pole predstavuje hardvér, ktorý pozostáva z väčšieho počtu pevných diskov, ktoré pracujú ako jeden celok. Tieto disky sú následne riadené centrálnou jednotkou, ktorá zabezpečuje distribúciu úloh na jednotlivé disky a tým pádom zvyšuje rýchlosť prístupu k dátam. Diskové polia sa využívajú práve v spoločnostiach, ktoré hľadajú technológie na úschovu dôležitých informácií, ktoré musia byť neustále dostupné. Diskové polia prešli postupom času mnohými zmenami a ich dnešný redundantný dizajn eliminoval najpodstatnejší problém z minulosti – vysokú citlivosť komponentov na chod zariadenia. Zdvojený napájací zdroj, zdvojená riadiaca jednotka, alebo zavedenie technológie RAID priniesli maximálnu bezpečnosť dát a minimálne výpadky prevádzky. [1]

Data Domian

Zálohovacie zariadenia Data Domain predstavuje diskové pole spojené s deduplikačnou technológiou. Obsahuje integrovaný operačný systém, ktorý je prispôsobený na účely zálohovania. Kombinácia deduplikácie a jednoduchej správy uložených dát predstavuje akýsi optimálny štandard dnešných potrieb korporácií. Technológiu deduplikácie používa väčšina súčasných diskových polí, avšak pri zariadení Data Domain prebieha v reálnom čase priamo pri vstupe dát. Toto riešenie predstavuje podstatné šetrenie úložným priestorom a v konečnom dôsledku aj menej vynaložených finančných prostriedkov na úschovu dát. Špeciálna architektúra riadiacej jednotky je prispôsobená na spracovanie vstupných informácií v reálnom čase, čo v princípe znamená, že žiadne dáta sa nezapíšu na disk viac krát. V prvej fáze sú údaje rozkúskované na malé časti, ktoré sú následne porovnávané s databázou uložených dát. Ak sa vstupný údaj už na diskoch nachádza, vytvorí sa namiesto zápisu iba odkaz a pokračuje sa v porovnávaní nasledujúcich častí. Týmto spôsobom dokážeme v praxi ušetriť miesto. [1]

USB Flash disky a pamäťové karty

Pamäťové karty a flash disky sú v súčasnosti masívne využívaným médiom. Slúžia predovšetkým na uchovávanie a prenos informácií medzi počítačmi a inými elektronickými zariadeniami. Pre potreby dlhodobého zálohovania však nie sú najvhodnejším médiom, pretože

majú obmedzenú životnosť. Negatívne na nich pôsobí statická elektrina a vďaka ich malej veľkosti sa môžu ľahko stratiť. Navyše cena za 1GB kapacity je u flash diskov vyššia, ako u väčšiny optických alebo pevných diskov. Nevýhoda teda je, že pomer cena a kvalita nie je ideálny. Výhodou je, že nie je potreba žiadnych napájacích káblov. Môžeme teda povedať, že flash disky sú relatívne spoľahlivé zálohovacie média, ktoré sú vhodné na zálohovanie predovšetkým malých súborov na krátkodobé účely. [1]

CD a DVD

CD a DVD sa stále používajú na zálohu dát hlavne kvôli výhodám, ktoré tieto média majú. Medzi ich výhody patrí dlhá životnosť. Spoločnosť Verbatim uvádza až 100 rokov, ktorá je dosiahnuteľná vtedy, keď zachádzame s nimi opatrne a skladujeme ich v podmienkach, ktoré im vyhovujú. Ďalšou výhodou je, že si môžeme nahrať zálohované súbory na viacero diskov, ktoré následne môžeme uložiť na viacerých miestach a tým zabrániť strate údajov v prípade požiaru alebo vykradnutia budovy. Najväčšou nevýhodou je ich kapacita a fakt, že v dnešnej dobe už veľa nových PC nemá CD/DVD mechaniku. [1]

Sieťové úložiská NAS

Pripojením k sieti vzniká možnosť ukladať dáta z viacerých počítačov, dokonca naraz a zároveň možnosť prístupu k dátam odkiaľkoľvek zo sveta pomocou internetu, ako v prípade cloudu. Často sa tiež NASu hovorí súkromný cloud, pretože poskytuje podobné možnosti, ale dáta sú u používateľa v byte alebo v kancelárii, nie niekde v dátovom centre na Aljaške.
Pevných diskov je možné použiť viac a nastaviť pomocou prehľadného a rýchleho sprievodcu zálohovaním tak, aby v prípade fyzického poškodenia alebo zlyhania jedného z pevných diskov došlo nielen k upozorneniu majiteľa na tento problém, ale hlavne aby boli dáta v poriadku. NAS majú tiež stovky ďalších možností ako napríklad prehrávanie filmov rovno na TV, zdieľanie tlačiarne alebo zapojenie kamerového systému pre kancelárie alebo byt. Dnes ide o jednu z najobľúbenejších možností ako zdieľať a zálohovať dáta.

NAS server a jeho hlavné výhody

Inteligentné dátové úložiská sú obľúbené pre svoje hlavné benefity:

- Ideálne riešenie pre automatické zálohovanie dôležitých dát (zrkadlenie v diskových poliach RAID).

- Prístup z viacerých počítačov alebo inteligentných zariadení doma aj v rozsiahlej firme so stovkami zariadení.
- Spoločné úložisko pre dokumenty, filmy, hudbu a ďalší multimediálny obsah s možnosťou rozšírenia.
- NAS úložisko dát podporuje veľa pokročilých funkcií (Web server, iTunes server, BitTorrent a ďalšie).
- Oproti klasickým serverom oveľa nižšia energetická spotreba, ale tiež minimálna hlučnosť.
- Vďaka USB portom môžete pripojiť externé pevné disky a ešte viac tak rozšíriť celkovú kapacitu dátového úložiska. [1]

Externý disk HDD a SSD

Externý disk je druhou najrozšírenejšou formou zálohy a má veľa spoločných znakov s flash diskom. Rýchlosť je veľmi podobná flash disku, kapacita v radoch TB je samozrejmosťou. Pevné disky je možné ľahko prenášať a zálohovať na nich tak aj väčšie množstvo počítačov. Používatelia tiež ocenia jednoduché použitie disku na odkladanie dát, ktoré na notebooku už nechcú, ako napríklad staré fotografie, filmy či dokumenty z minulých rokov.

Pevné disky v dnešnej dobe nahrádzajú aj HDD a SSD, takže ide o najrýchlejšiu možnosť zálohy, kedy je možné kopírovať dáta rýchlosťami okolo 500MB/s, čo žiadny flash disk nevie. Odolné pevné disky sú navyše použiteľné aj na cestách, kde hrozí napríklad pád, alebo vplyv prostredia, ako vlhkosť a prach. Moderné pevné disky HDD a SSD sú na tieto hrozby vo väčšine prípadov pripravené. Niektoré disky tiež ponúkajú automatický software, ktorý zálohu nastaví a užívateľ si tak nemusí pamätať, že musí kopírovať dáta.

Rozdiel medzi HDD a SSD je v tom, že SSD majú o čosi vyššiu cenu, HDD obsahujú pohyblivé časti, ktoré sú náchylné k poškodeniu napríklad vplyvom pádu na zem a SSD nemajú pohyblivé časti a teda sú o čosi odolnejšie. [1]

Druhý počítač

Využitie ďalších počítačov v kancelárii alebo starého PC doma sa rovnako používa na zálohovanie dát. Hoci sa toto riešenie zdá ako najlepšie z pohľadu nulových vstupných nákladov, je toto riešenie najmenej vhodné. Pokiaľ druhý počítač napadne vírus, dáta sú v podstate nepoužiteľné a nie je možné sa na zálohu spoľahnúť.

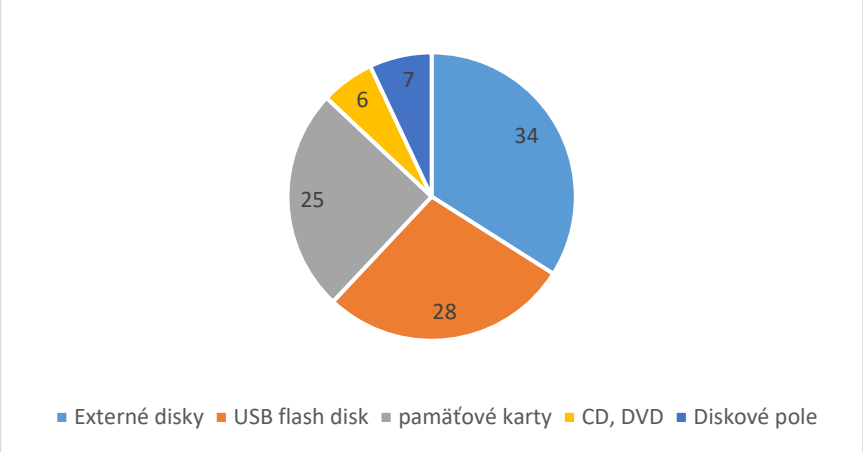
Veľkou nevýhodou je potreba starať sa o ďalšie aktualizácie a riešenia možných hardwarových problémov. Výhodné je naopak to, že je možné zdieľať dáta pre viac PC a kapacita je v podstate neobmedzená, pretože do počítača je možné pridať ďalšie disky, alebo pripojiť externé. Možné je tiež nastavenie, kedy sa jednotlivé počítače zálohujú na všetky ostatné počítače v sieti, čo znamená niekoľkonásobnú zálohu. Samozrejme pri vyššom počte PC je toto riešenie neefektívne. [1]

Prieskum obľúbenosti a porovnanie výsledkov

Cieľom prieskumu využívania zálohovacích zariadení bolo prostredníctvom ankety na sociálnej sieti Facebook zistiť, ktoré zariadenia na zálohovanie sú u respondentov najviac využívané. Ankety sa zúčastnilo presne 100 respondentov, pričom mali na výber z piatich možností a to: externé disky, USB flash disky, pamäťové karty, CD, DVD a diskové pole, pričom mohli označiť len jednu odpoveď.

V prvej časti prieskumu sme sa na sociálnej sieti Facebook opýtali 100 ľudí otázku: „Ktoré zálohovacie zariadenie využívate najčastejšie?". Z prieskumu vyplýva, že najobľúbenejším zálohovacím zariadením je externý disk (HDD alebo SSD), za ktorý hlasovalo až 34 používateľov, na druhom mieste skončili USB flash disky, ktoré používa 28 opýtaných, tretie miesto obsadili pamäťové karty, ktoré sú obľúbené u 25 hlasujúcich a posledné miesta získali CD, DVD a diskové pole, ktoré získali dokopy 13 hlasov.

Podľa výsledkov budeme ďalej porovnávať parametre dvoch najobľúbenejších zálohovacích zariadení, ktorými sú externé disky HDD a SSD a USB flash disky. V tabuľke budeme porovnávať zariadenia s rovnakou kapacitou úložiska a to 1 TB.



Graf 1 – Ktoré zálohovacie zariadenie využívate najčastejšie?

1.1.Porovnanie externých diskov HDD a SSD s USB flash diskami

Z výsledkov prieskumu vyplýva, že ľudia najčastejšie na zálohovanie využívajú práve externé disky a USB flash disky. V ďalšej časti si porovnáme parametre u oboch zariadení. Konkrétny typ zariadenia sme vyberali podľa rovnakej kapacity úložiska.

Tab. 1 Porovnanie parametrov u externých diskov a USB flash diskov

	Kapacita úložiska	Rozhranie	Rýchlosť čítania	Cena
Externý disk	1 TB	USB 3.0	5000 MB/s	46€ - 107€
USB flash disk	1 TB	USB 3.0	150 MB/s	132€ - 264€

1.1.1. Externé disky HDD a SSD

Externý disk je jednou z najrozšírenejších foriem zálohy. Pevné disky je možné ľahko prenášať a zálohovať na nich aj väčšie množstvo dát.

Môžeme povedať, že pevné externé disky HDD a SSD v dnešnej dobe predstavujú najrýchlejšiu možnosť zálohy, kedy je možné kopírovať dáta rýchlosťami okolo 500MB/s. Odolné pevné disky sú navyše použiteľné aj na cestách, kde hrozí napríklad pád, alebo vplyv prostredia, ako vlhkosť a prach. Moderné pevné disky HDD a SSD sú na tieto hrozby vo väčšine prípadov pripravené. Niektoré disky tiež ponúkajú automatický software, ktorý zálohu nastaví a užívateľ si tak nemusí pamätať, že musí kopírovať dáta.

Rozdiel medzi HDD a SSD je v tom, že SSD majú o čosi vyššiu cenu, HDD obsahujú pohyblivé časti, ktoré sú náchylné k poškodeniu napríklad vplyvom pádu na zem a SSD nemajú pohyblivé časti a teda sú o čosi odolnejšie. [1,3]

Obr. 1 Externý pevný disk Western Digital Elements Portable 1 TB

Zdroj: https://www.datart.sk [3]

USB flash disk

Flash disky sú v súčasnosti masívne využívaným médiom. Slúžia predovšetkým na uchovávanie a prenos informácií medzi počítačmi a inými elektronickými zariadeniami. Pre potreby dlhodobého zálohovania však nie sú najvhodnejším médiom, pretože majú obmedzenú životnosť. Negatívne na nich pôsobí statická elektrina a vďaka ich malej veľkosti sa môžu ľahko stratiť. Navyše cena za 1GB kapacity je u flash diskov vyššia, ako u väčšiny optických alebo pevných diskov. Nevýhoda teda je, že pomer cena a kvalita nie je ideálny. Výhodou je, že nie je potreba žiadnych napájacích káblov. Môžeme teda povedať, že flash disky sú relatívne spoľahlivé zálohovacie média, ktoré sú vhodné na zálohovanie predovšetkým malých súborov na krátkodobé účely. [1,4]

Obr. 2 - SanDisk Ultra Dual Drive Luxe 1 TB
Zdroj: https://www.visiongadgetry.com [4]

Záver

Vývoj v oblasti zálohovania dát napreduje obrovskou rýchlosťou. V súčasnosti máme niekoľko desiatok možností ako ochrániť naše dáta pred stratou, zničením alebo iným znehodnotením

K strate dát môže dôjsť viacerými spôsobmi, môže to byť napríklad dôsledok náhodného vymazania užívateľom alebo dôsledkom infiltrácie vírusu do systému, kedy vírus môže dáta prepísať, alebo zrušiť celý systém, no najčastejšie k strate dát dochádza v dôsledku hardwarovej chyby a jediný spôsob ako tomu predchádzať je práve pravidelné zálohovanie. V dnešnej dobe existuje mnoho odborníkov, ktorí sa zaoberajú práve zálohovaním a vymýšľajú nové metódy a spôsoby aby zálohovanie v budúcnosti bolo ešte viac efektívnejšie a bezpečnejšie.

Z prieskumu práce sme zistili, že najviac preferované metódy zálohovania údajov sú práve prostredníctvom externých diskov a USB flash diskov. V porovnaní týchto dvoch zariadení vyplýva, že v pomere cena a výkon, sú viac vyhovujúce práve externé disky, ktoré okrem iného sa môžu pýšiť aj dlhšou životnosťou a vyššou rýchlosťou čítania MB/s.

Zoznam použitej literatúry

[1] MUDROŇ, M. , 2017: *5 spôsobov ako zálohovať dáta , [online] [cit 25-03-2022]dostupné na internete:* https://www.mojwindows.sk/2017/09/5-sposobov-ako-zalohovat-data/

[2] MELCOMP, 2017: *Základné pojmy operačných systémov, [online] [cit 30-03-2022] dostupné na internete:* https://melisko.webnode.sk/news/software-a-zakladne-pojmy-operacnych-systemov/

[3] ELEKTROSPED, 2022: *Externý pevný disk Western Digital Elements Portable 1TB (WDBUZG0010BBK-WESN), čierny [online] [cit 02-04-2022] dostupné na internete:* https://www.datart.sk/Externy-pevny-disk-WESTERN-DIGITAL-HDD-2-5-1TB-Elements.html

[4] VISION GADGETRY, 2022: *SANDISK ULTRA DUAL DRIVE LUXE TYPE-C OTG USB 3.1 DC4 FLASH DRIVE 150MB/S 1TB, [online] [cit 02-04-2022] dostupné na internete:* https://www.visiongadgetry.com/sandisk-ultra-dual-drive-luxe-type-c-otg-usb-3-1-dc4-flash-drive-150mb-s-1tb

Kontaktné údaje

[1]Ing. Zuzana Sochuľáková

Ústav humanitných a technologických vied na Vysokej škole bezpečnostného manažérstva v Košiciach,

Turčiansky Peter 103, 03841, Slovenská republika,

e-mail: zuzana.sochulakova@vsbm.sk

[1]Ing. Zlatica Geročová, MBA

Ústav humanitných a technologických vied na Vysokej škole bezpečnostného manažérstva v Košiciach, Obišovce 147, 044 81 Kysak, Slovenská republika,

E-mail: gerocovazlatica@gmail.com

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

doc. RNDr. Tatiana Hajdúková, PhD.

Bezpečnosť e-mailovej komunikácie ženskej populácie Slovenskej republiky

Kristína Staňová

Abstrakt: Príspevok sa zaoberá bezpečnosťou elektronickej komunikácie so zameraním na e-mailovú komunikáciu. Kvôli neustále narastajúcej elektronizácii a informatizácii a veľkému množstvu e-mailových užívateľov je nevyhnutné neustále zabezpečovať a zvyšovať úroveň bezpečnosti a bezpečnostného povedomia ľudí a následne informovať o možných rizikách a z nich vyplývajúcich opatreniach pri elektronickej komunikácii. Primárnym cieľom štúdie je na základe metódy prieskumu zistiť na akej úrovni je bezpečnostné povedomie žien v oblasti e-mailovej komunikácie. Zároveň bolo dôležité identifikovať a charakterizovať základné riziká a následné opatrenia, ktoré môžu ovplyvňovať e-mailovú komunikáciu. Komparáciou týchto údajov a vyhodnotením prostredníctvom grafov boli v závere príspevku znázornené výsledky prieskumu.

Kľúčové slová: elektronická komunikácia, e-mail, bezpečnosť, riziká, opatrenia, povedomie.

Úvod

Elektronická komunikácia patrí k významným objavom v informačnej a komunikačnej oblasti života každého z nás. Pokrok niekoľkých posledných desaťročí nás posunul vpred a otvoril nám cestu k obrovskej zbierke informácií, no predovšetkým nás spojil s celým svetom v rámci komunikácie prostredníctvom internetu.

Najviac využívaným komunikačným kanálom je elektronické pošta, tzn. e-mail. Elektronická doba, v ktorej žijeme zvyšuje počet internetových a e-mailových užívateľov na pravidelnej báze. Z toho dôvodu je dôležité klásť čoraz väčší dôraz na zvyšovanie úrovne jej bezpečnosti a zároveň vzdelanosti jej používateľov.

Prvá časť príspevku sa zaoberá základnými aspektami bezpečnosti e-mailovej komunikácie so zameraním na riziká, ktoré najčastejšie ohrozujú elektronickú komunikáciu. Tieto riziká môžu ohroziť nie len chod veľkých organizácií, ale môžu do značnej miery znepríjemniť život každého z nás a v horšom prípade môžu zneužiť, znehodnotiť alebo ukradnúť naše súkromné informácie alebo osobné údaje.

Ďalšia časť príspevku poukazuje na základné formy preventívnych opatrení slúžiacich na predchádzanie pred hrozbami a rizikami, ktoré môžu vyplývať z elektronickej komunikácie.

Hlavným cieľom, spracovaným v druhej časti príspevku, bolo na základe vedeckej metódy prieskumu prostredníctvom dotazníka zistiť názory žien na bezpečnosť e-mailovej komunikácie a zvýšiť povedomie o zabezpečení elektronických poštových schránok s poukázaním na základné bezpečnostné opatrenia .

Bezpečnosť e-mailovej komunikácie

Vznik e-mailovej komunikácie patril medzi významné medzníky histórie. Tento typ komunikácie bol navrhnutý na doručovanie správ a bezpečnosť takejto komunikácie bol neznámym pojmom.

E-mailová komunikácia sa patrí v rámci digitálnej komunikácie k neoddeliteľnej časti každodenného života a je prakticky súčasťou všetkých odvetví spoločnosti, hlavne vďaka svojej jednoduchosti, všestrannosti a užitočnosti. Na základe prieskumu bolo zistené, že v roku 2020 sa vymenilo zhruba 306,4 miliardy e-mailov každý deň, ktoré boli využité na pracovné a súkromné účely. Budúce predpoklady hovoria, že v roku 2024 môže toto číslo vzrásť na 361,6 miliardy odoslaných e-mailov denne. Práve kvôli obľúbenosti a neustále vzrastajúcej popularite sa e-mailová komunikácia stáva žiadaným cieľom kybernetických útokov, ktorých počet sa každý rok zvyšuje.[1]

E-mailová bezpečnosť hovorí o zabezpečení prostredníctvom rôznych spôsobov a s využitím technických vymožeností, ktorých úlohou je dbať na bezpečnosť e-mailových účtov a ich obsahu na ochranu proti nelegálnemu prístupu alebo krádeži a zneužívaniu údajov. Jej súčasťou sú taktiež zákonitosti nevyhnutné na zabezpečenie pripojenia vlastníka daného účtu, šifrovanie komunikácie, ochranu pred podvodnými e-mailmi a filtrovanie nevyžiadanej pošty. Práve kvôli týmto faktorom, je dôležité dbať na vzdelávanie a zvyšovanie povedomia o bezpečnosti elektronickej komunikácie nie len zamestnancov vo firmách ale aj bežných užívateľov, predovšetkým pri spracovávaní prichádzajúcej a odchádzajúcej pošty.

[1] Soare, B., Petcu, A. and Din, A., 2019. What Is Email Security?. [online] Heimdal Security Blog.

Riziká e-mailovej komunikácie

V súčasnej dobe rozsiahlej elektronizácie a informatizácie je ochrana a zabezpečenie kybernetickej bezpečnosti e-mailových schánok a serverov jednou z najdôležitejších úloch pre správne fungovanie spoločnosti.

Medzi najčastejšie riziká, ktoré môžu ohroziť správne fungovanie e-mailovej komunikácie patria:

- **Počítačový vírus**

Je typ škodlivého softvéru alebo malvéru, ktorý sa šíri medzi počítačmi a spôsobuje poškodenie základných častí počítača a osobých údajov. Jeho úlohou je narušiť systémy a spôsobiť znehodnotenie, stratu alebo krádež informácií. Vírusy sa najčastejšie pripájajú k spustiteľnému súboru hostiteľa, ktorý je pri otvorení vypustený. Bežné znaky počítačového vírusu sú spomalenie systému, vyskakovacie okná, odosielanie hromadných e-mailov, samospúšťajúce programy.

- **Taktika sociálneho inžinierstva**

Patrí k najnebezpečnejším a najefektívnejším spôsobom získavania citlivých údajov, ktorá nevyžaduje špeciálne technické vzdelanie, no je schopná napadnúť zabezpečené informačné systémy. Je to manipulačná technika využívajúca chybu ľudského faktora a neznalosť obete, kedy sa útočník snaží vyvolať emócie, zneistiť a zároveň vzbudiť dôveru, naliehať a vyžadovať okamžitú pozornosť alebo využíva podvodné e-mailové prílohy, ktoré by mohli obeť zaujať.

- **Phising**

Phishing je forma útoku s využitím metód sociálneho inžinierstva, pri ktorom sa zločinec vydáva za dôveryhodnú osobu alebo inštitúciu s cieľom získať od obete citlivé informácie. Na používateľa využíva manipulačné techniky so zámerom zistiť údaje o platobných kartách, prihlasovacích údajoch alebo je schopná napadnúť samotný počítač. Takýto spôsob útoku pri e-mailovej komunikácii využíva dôverihodnosť a pretvárku, že odosielateľmi sú bankové inštitúcie, poisťovne, doručovacie spoločnosti alebo ďalšie organizácie, pri ktorých útočník predpokladá, že budú mať s obeťou vzťah.[2]

[2] Csirt. 2021. *Sociálne inžinierstvo* | CSIRT.SK.

- **Spoločenské hrozby**

Súčasná situácia a hrozby spoločnosti, ktoré majú meniacu a stúpajúcu tendenciu ohrozujú chod spoločnosti a zabezpečenie elektronickej komunikácie. Pandemická, ekonomická a vojnová kríza zvýšila počet internetových užívateľov a s tým aj počet internetových podvodov a hackerských útokov. Mimoriadne spoločenské situácie predstavujú impulz a prostriedok na tvorbu nápadov na sofistikovanejšie ciele a metódy internetových podvodníkov.

Opatrenia pre zabezpečenie e-mailu

Ochrana osobných údajov sa stala dôležitým aspektom bezpečnosti, na ktorú sa kladie veľký dôraz, aby sa predchádzalo kyberútokom, neoprávneným prístupom k súkromným informáciám a ich zneužitím.

Medzi základné opatrenia patria:

- **Viacfaktorová kontrola prístupu**

Online účty sú bezpečnejšie, keď sú na ich ochranu použité viaceré druhy hesiel. Viacfaktorová autentifikácia pridáva ďalšie úrovne na overenie identity používateľa po prihlásení do účtu. Tieto úrovne môžu obsahovať biometrické údaje, ako je odtlačok prsta alebo rozpoznávanie tváre, alebo dočasné prístupové kódy odoslané prostredníctvom textovej správy.

- **Kontrola hlavičiek správ**

Prvotná kontrola prichádzajúcich správ by mala spočívať v kontrole hlavičiek a samotného tvaru e-mailovej adresy odosielateľa. Podľa týchto faktorov je možné určiť podozrivo vyzerajúce e-maily. E-mailový program, akým je napríklad Gmail, má vo svojom systéme zabudovanú automatickú kontrolu prichádzajúcich správ, pri ktorých používa bezpečnostné označenia, akými môžu byť výstražné otázniky alebo výkričníky, ktorými opozorňuje svojich užívateľov na podozrivý obsah.

- **Kontrola obsahu správ**

Pri otváraní e-mailovej komunikácie je dôležité si všímať varovné signály, ktoré používateľov môžu upozorniť na podozrivý a škodlivý obsah správ. Medzi takéto signály patrí samotná forma správy, jazyk a gramatika použitá vo vetách, odseky, písmo, meno

odosielateľa alebo cudzia a nezvyčajná forma internetových odkazov a príloh. Hoci existujú rôzne spamové filtre alebo antivírusové programy, je dôležité predovšetkým vnímať, nebyť neprítomný a príliž zvedavý, pretože práve tieto faktory vedú častokrát k chybnému identifikovaniu škodlivého e-mailu.[3]

- **Silné heslá**

Jedným z prvých krokov pri vytváraní osobného ale ja pracovného účtu je vytvorenie prihlasovacieho mena a hesla. Základný postup pre tvorbu silných hesiel spočíva vo využívaní veľkých a malých písmen, čísel, znakov a prípadne aj medzier, pri ktorých platí, že čím sú dlhšie tým je ochrana väčšia.

- **Zdieľať len nevyhnutné/žiadne množstvo osobných údajov**

Je dôležité uchovávať a zabezpečovať osobné údaje, ktoré by nemali byť viditeľné pre tretie strany, pretože každá informácia, zdieľaná prostredníctvom elektronickej komunikácie, môže byť odcudzená a zneužitá.[4]

- **Využívanie VPN siete**

Virtuálna privátna sieť (VPN) prináša internetové pripojenie iba overeným a identifikovaným používateľom súkromnej siete, ktorá využíva šifrovanie a kontrolu pre odosielané a prijímané dáta. Takýmto spôsobom je možné chrániť aj staršie typy aplikácii a zvýšiť tým odolnosť systémov voči prípadným útokom.[5]

- **Použitie ochranných softvérov**

V prvom rade netreba zabúdať na aktualizovanú verziu operačných systémov a aplikácií, ktoré využívajú aj vlastné systémy bezpečnosti údajov. Ďalšími systémami sú antivírusové programy, ktoré netreba podceňovať, pretože škodlivé kódy sa môžu nadzádzať všade, aj v prílohách e-mailovej správy a infikovanej reklamy. Hoci internetové stránky častokrát ponúkajú testovacie verzie antivírusových programov, je výhodnejšie a bezpečnejšie kúpiť si plnú verziu systému, ktorá obsahuje širokú škálu ochranných prostriedkov, pre dostatočné zabezpečenie nie len elektronickej komunikácie.[6]

- **Nepoužívať verejné wi-fi pripojenie**

Veľké množstvo podnikov a budov ponúka pripojenie do svojich verejných internetových sietí, ktoré predstavujú pre kyberzločincov ľahkú cestu na sledovanie

[3] Mukherjee, L., 2020. *Email Security: 10 Steps for How to Secure Your Email Communication* – InfoSec Insights.
[4] Alton, L., 2017. *4 Most Secure Forms of Online Communication* | ISACA Blog.
[5] Qubit Academy. 2021. *Bezpečná komunikácia*.
[6] Koliba, J., 2018. Ako bezpečne komunikovať na internete? Pozrite si niekoľko tipov.

potenciálnych obetí a zachytávanie údajov prenášaných internetom. Takýmto spôsom je ľahké získať prístup k bankovým údajom, heslám účtov a iným informáciám. Je dôležité skontrolovať samotný názov siete, do ktorej je možný prístup a pri práci so súkromným zariadením sa vyhnúť prihlasovaniu do stránok s dôležitým obsahom pre používateľa.

- **Vzdelávanie a zvyšovanie povedomia**

Jedným z najlepších spôsobov ako sa chrániť pred rôznymi rizikami je poznať ich a vedieť ich odhaliť. Z toho dôvodu je dôležité budovať a zvyšovať povedomie ľudí o môžných útokoch a podvodoch, ktorým môžu čeliť a rozprávať o technikách sociálneho inžinierstva.

Výskumná časť príspevku bezpečnosti e-mailovej komunikácie

Výskumnú časť príspevku tvorí zisťovanie povedomia o bezpečnosti e-mailovej komunikácie a zabezpečení e-mailových účtoch žien ako používateliek elektronických poštových schránok. Základ príspevku spočíva vo forme prieskumu tvoreného dotazníkom, prostredníctvom ktorého možno ľahko interpretovať a vyhodnotiť zistené poznatky a výsledky.

Dotazník bol vyhodnotený na základe informácii zozbieraných na internetovej stránke https://www.survio.com/sk/, ktorá bola vhodná pre respondentov vďaka ľahkej a prehľadnej manipulácii pri vypĺňaní. Získané výsledky boli následne zaznamenané v grafoch s prehľadným zoznamom odpovedí a ich číselným vyjadrením v percentách.

Prieskum a vyhodnotenie výskumu

Prieskum bol realizovaný prostredníctvom internetu a sociálnych sietí a distribuovaný respondentkám vo veku 20-50 rokov, ktorých odpovede boli anonymné. Otázky boli zamerané na zisťovanie úrovne zabezpečenia e-mailových schránok používateliek a ich celkového povedomia o rizikách a ochranných opatreniach pri spracovávaní e-mailovej komunikácie.

Znenie a vyhodnotenie otázok bolo nasledovné:

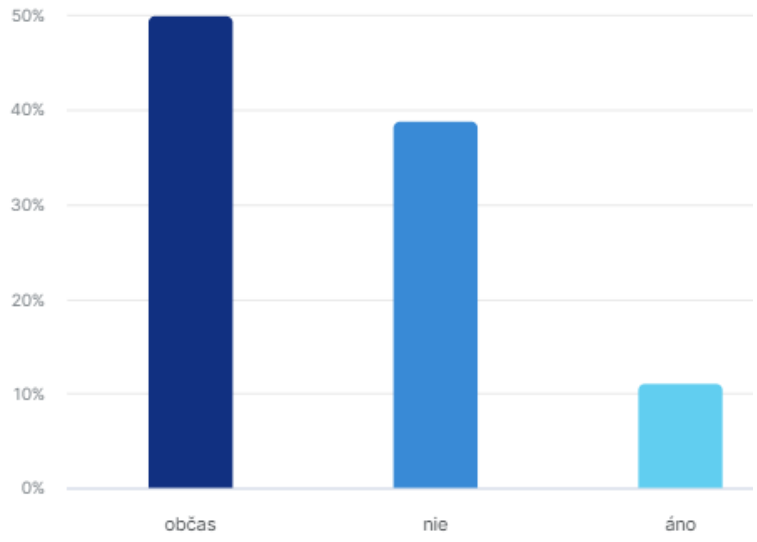
- Úvodné otázky boli zamerané na zistenie počtu e-mailových účtov, ktoré respondenti vlastnia, pričom približne polovica respondentov uviedla že vlastní 1-2 účty a druhá

polovica 3-5 e-mailových účtov. Ďalšou odpoveďou, ktorú označilo 58% bolo zistenie, že viac ako polovica respondentov používa svoj e-mailový účet na dennej báze.

- **Myslíte si, že heslo, ktoré používate do svojho emailového účtu je dostatočne silné?** - odpovede v tejto otázke pozostávali zo štyroch častí a respondenti mali na výber z možností „áno, asi áno, asi nie, nie“. Najväčšia časť výsledku, ktorá bola viac ako 60 % zodpovedala odpovedi „asi áno“. Druhú najčastejšiu odpoveď „asi nie“ označilo viac ako 20 % respondentiek.

- **Ako často si v priemere meníte heslo do e-mailového účtu?** - respondentky mali pri tejto otázke na výber z troch možností, pričom výsledky jasne preukázali že necelých 70 % žien si heslo do svojho e-mailového účtu nemení nikdy.

- **Používate verejné Wi-Fi siete pri spracovávaní e-mailov? –** výsledky tejto otázky poukazujú na fakt, že 50 % ľudí uviedlo, že sa „občas“ pripájajú do verejných internetových sietí pri spracovávaní e-mailovej komunikácie a necelých 40 % respondentov uviedlo, že sa nepripája k verejným internetovým sieťam.

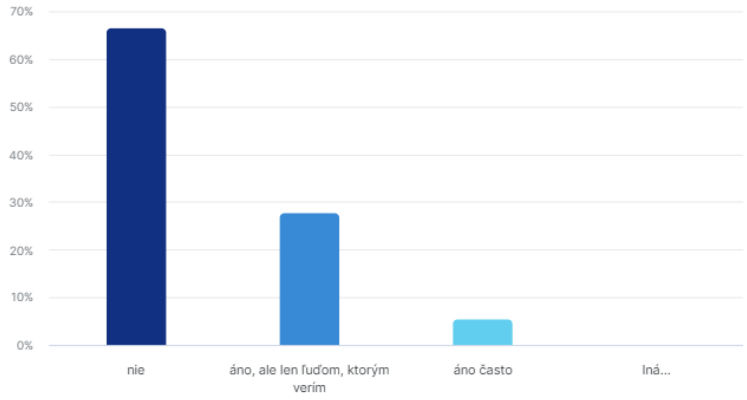


Graf č. 1- Používate verejné Wi-Fi siete pri spracovávaní e-mailov?

Zdroj: www.my.survio.com

- **Posielate prostredníctvom e-mailovej komunikácie hektické alebo súkromné informácie? -** výsledky prieskumu preukázali, že najvyššie percento ľudí až 66,7 %

neposiela prostredníctvom elektronickej komunikácie súkromné informácie. Na druhej strane 27,8 % odpovedí hovorí o tom, že respondentky posielajú súkromný obsah len ľuďom, ktorým veria a 5,6 % posiela osobné informácie často.

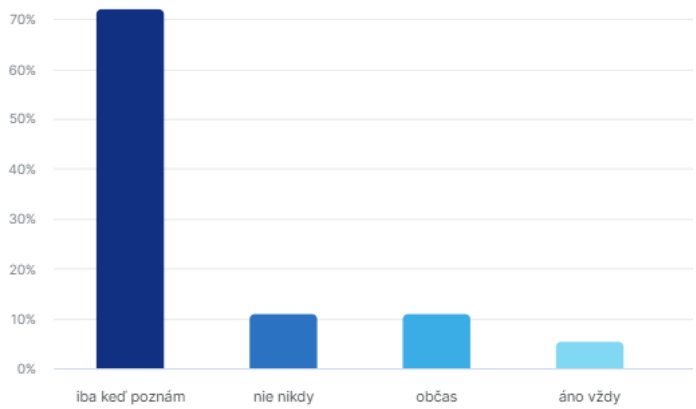


Graf č. 2- Posielate prostredníctvom e-mailovej komunikácie hektické alebo súkromné informácie?

Zdroj: www.my.survio.com

- **Kontrolujete e-mailovú adresu prichádzajúcich e-mailov?** - odpovede na túto otázku pozostávali z troch možností- áno, nie, občas. Výsledky preukázali percentuálnu rovnosť odpovedí, pričom menšiu, respektíve zvýšenú odchýlku zaznamenala odpoveď „občas“.

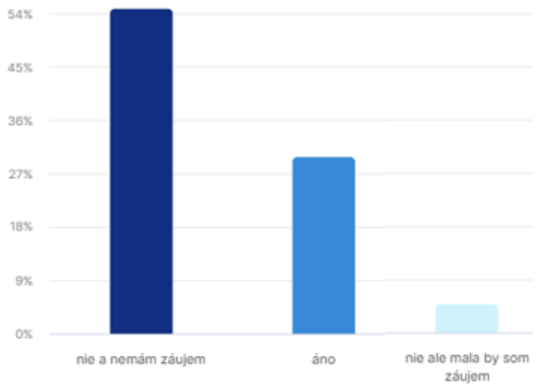
- **Otvárate odkazy uvedené v prichádzajúcich e-mailoch?** - táto otázka bola zameraná na zistenie správania respondentov v prípade, ak sa nachádza v prichádzajúcom e-maily ďalší odkaz na internetovú stránku. Najviac respondentov sa priklonilo k odpovedi „iba keď poznám odosielateľa“, ktorú označilo viac ako 70 % opýtaných. Ďalšie odpovede „nie nikdy, občas“ označilo len 11 % opýtaných a „áno vždy“ necelých 6 % ľudí, čo bola najmenej označovaná odpoveď.



Graf č. 3- Otvárate odkazy uvedené v prichádzajúcich e-mailoch?

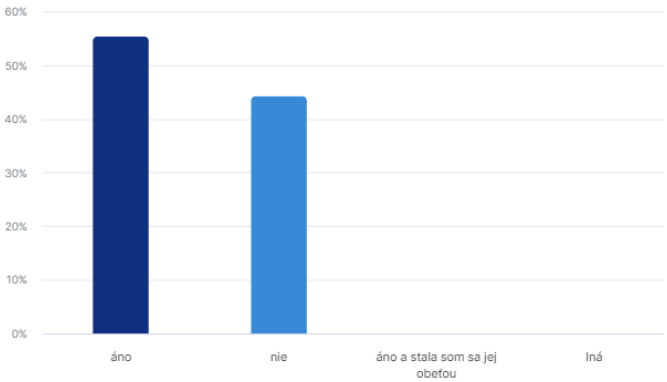
Zdroj: www.my.survio.com

- **Zúčastnili ste sa niekedy kurzu/školenia/webináru alebo iného vzdelávacieho programu týkajúceho sa bezpečnosti elektronickej komunikácie?** - odpovede v tejto otázke pozostávali z troch častí a respondenti mali na výber z možností „nie a nemám záujem, áno, neviem, nie ale mala by som záujem“. Najväčšia časť výsledku 55 % zodpovedala odpovedi „nie a nemám záujem“, 30 % respondentov sa zúčastnilo podobného vzdelávacieho programu a 5 % by v budúcnosti malo záujem zúčastniť sa vzdelávania v oblasti elektronickej komunikácie.



Graf č. 4- Zúčastnili ste sa niekedy kurzu/školenia/webináru alebo iného vzdelávacieho programu týkajúceho sa bezpečnosti elektronickej komunikácie? Zdroj: www.my.survio.com

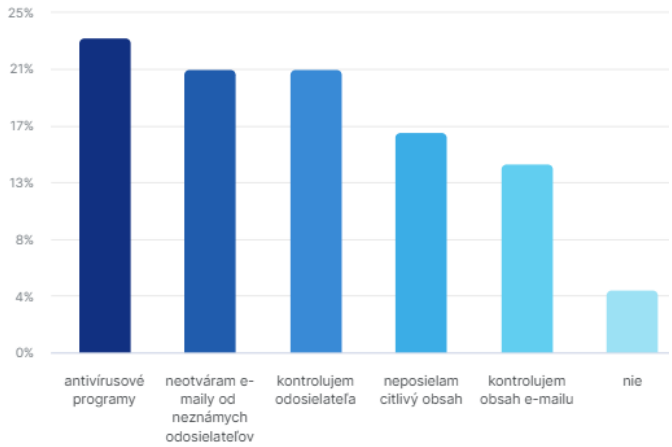
- **Stretli ste sa s podvodnou metódou PHISING, kedy sa zločinec vydáva za dôveryhodnú osobu alebo inštitúciu s cieľom získať od obete citlivé informácie?** - výsledky tohto prieskumu poukázali že, že viac ako polovica opýtaných mala už skúsenosť a podobným druhom e-mailov a menšia polovica opýtaných nemala s takýmto druhom správ ešte žiadne skúsenosti.



Graf č. 5- Stretli ste sa s podvodnou metódou PHISING, kedy sa zločinec vydáva za dôveryhodnú osobu alebo inštitúciu s cieľom získať od obete citlivé informácie? Zdroj: www.my.survio.com

- **Stali ste sa obeťou podvodu prostredníctvom e-mailovej komunikácie?** - táto otázka bola zameraná na zistenie subjektívneho postoja opýtaných, v ktorej mohol každý napísať svoju skúsenosť podvodných situácií. Výsledky poukázali, že väčšina respondentov sa snaží na základe opatrnosti a všímavosti predchádzať takémuto druhu podvodu a byť informovaný o možných spôsoboch a rizikových prípadoch elektronických podvodov.

- **Používate nejaké opatrenia na ochranu Vašej e-mailovej komunikácie?** - súčasťou tejto otázky bolo šesť odpovedí pozostávajúcich z rôznych možností ochrany elektronickej komunikácie, využívaných v bežnom režime. Respondenti si z nich mohli vybrať viac alternatív podľa toho, ktorý z nich využívajú. Z výsledku sme zistili, že najviac respondentov používa antivírusové systémy, ďalej je to kontrola odosielateľa alebo samotného obsahu e-mailu. Medzi odpoveďami sa objavili aj názory ľudí, ktorý nepoužívajú žiadne formy ochrany e-mailovej komunikácie.



Graf č. 6- Používate nejaké opatrenia na ochranu Vašej e-mailovej komunikácie? Zdroj: www.my.survio.com

- **Ďalšie názory respondentov na bezpečnosť e-mailovej komunikácie** - záverečná časť dotazníkového prieskumu sa týkala samotného postoja a názoru respondentiek na bezpečnosť e-mailovej komunikácie. Veľké množstvo opýtaných zastáva názor, že je nevyhnutné neustále pracovať na zlepšovaní a zvyšovaní úrovne bezpečnosti, pretože šikovnosť a vynaliezavosť hackerov stále rastie. Zároveň je nevyhnutné zvyšovať povedomie, rozprávať a informovať o možnostiach a typoch útokov, ktoré sa stávajú a zároveň vzdelávať používateľov elektronických poštových schránok o možnostiach obrany a ochrany svojich účtov. Respondenti takisto zastávajú názor, že pokiaľ je človek

chránený dobrým a silným heslom a nereaguje na podozrivé a podvodné e-maily, tak je v relatívnom bezpečí.

3.2 Zhrnutie dotazníkového prieskumu

Na základe zrealizovaného výskumu je možné skonštatovať, že výpovede žien, na ktoré bol prieskum zameraný, boli realizované na základe ich vlastných názorov a skúseností.

Prvá fáza dotazníka bola venovaná základným otázkam o používaní elektronickej pošty a prvotnej ochrany pri prihlasovaní. Ďalej bolo dôležité zistiť samotný spôsob používania elektronickej komunikácie a to konkrétne či respondentky používajú svoje účty aj na posielanie súkromných informácií, hoci väčšina opýtaných neposiela takéto údaje, stále existujú ľudia, ktorý neriešia obsah alebo formu informácií, ktoré zdieľajú prostredníctvom internetových stránok.

Nasledujúca časť sa týkala kontroly prichádzajúcej pošty. Výsledky tejto časti majú znepokojivý charakter, pretože pomerne veľká časť opýtaných nekontroluje e-mailovú adresu odosielateľa, ktorá môže viesť práve k „PHISINGOVÉMU“ typu útoku, zameranému na osobné informácie používateľa, kedy sa odosielateľ môže vydávať za známu osobu.

Výsledky časti týkajúcej sa zisťovania povedomia o najbežnejšom a najčastejšie používanom type útoku „PHISING“, možno pokladať za očakávané, nakoľko približne polovica opýtaných túto metódu pozná a polovica sa s ňou ešte nestretla.

Za prekvapujúcu časť prieskumu možno považovať informácie získané z otázky, týkajúcej sa účasti respondentov na vzdelávacích programoch zameraných na elektronickú komunikáciu, pretože viac ako polovica opýtaných nemá do budúcna záujem zúčastniť sa podobného typu vzdelávania.

Je dôležité zhrnúť aj názory a postoje ľudí, ktorý sa o svoju bezpečnosť starajú vo zvýšenej miere, upriamujú svoju pozornosť aj na kontrolu samotných e-mailov a ich obsahu, používajú a poznajú rôzne servery na ochranu svojich účtov, zaujímajú sa o zvyšovanie povedomia a boli súčasťou rôznych foriem vzdelávania v rámci bezpečnosti elektronickej komunikácie.

Záver

V súčasnej dobe, v ktorej čelíme rôznym zdravotným ale aj vojnovým a ekonomickým krízam, sa začala častejšie využívať práca z domu. Tieto aspekty výrazne ovplyvnili množstvo a formu útokov na elektronickú komunikáciu. Z toho dôvodu sa zameranie príspevku týkalo bezpečnosti e-mailovej komunikácie so zameraním na zisťovanie názorov a povedomia žien na úroveň zabezpečenia.

Prvá polovica príspevku poukázala na základné druhy rizík s ktorými sa ľudia najčastejšie stretávajú a o ktorých je nevyhnutné neustále zvyšovať povedomie. S nimi súvisia aj opatrenia, o ktorých je dôležité neustále hovoriť a pripomínať ich nevyhnutnosť.

Forma dotazníkového prieskumu priniesla zaujímavé výsledky v oblasti elektronickej komunikácie, ktoré môžu prispieť k väčšej informovanosti a priniesť väčší prehľad o tom, čím by sa mala spoločnosť viac zaoberať a na čo klásť dôraz. Aj vďaka takémuto prieskumu si respondenti často začnú uvedomovať dôležitosť ochrany informácií a začnú si dávať väčší pozor na to, ako zabezpečujú svoje internetové účty. Hoci je možné povedať, že veľká časť opýtaných dbá na bezpečnosť svojej elektronickej komunikácie, stále existuje množstvo ľudí, ktorý berú túto problematiku na ľahkú váhu, nemajú o nej dostatok informácií alebo sa o ňu nezaujímajú.

Ochrana pred rôznymi typmi útokov začína vzdelávaním. Neustále prehlbovanie a zvyšovanie úrovne poznatkov môže do budúcna prispieť k lepším výsledkom zabezpečenia a k znižovaniu počtu obetí kybernetických podvodov a útokov.

Je potrebné si uvedomiť, že každý ochranný systém má svoje slabé miesta a preto je dôležité zaviesť maximálne možné množstvo zabezpečovacích prvkov, tým eliminovať hroziace riziká a v závere byť vždy o krok vpred.

Zoznam použitej literatúry

Alton, L., 2017. *4 Most Secure Forms of Online Communication | ISACA Blog*. [online] ISACA. Available at: <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/the-4-most-secure-forms-of-online-communication>.

Csirt. 2021. *Sociálne inžinierstvo | CSIRT.SK*. [online] CSIRT. Available at: <https://www.csirt.gov.sk/socialne-inzinierstvo.html>.

Hrehová, 2016. Bezpečnosť a komunikácia na internete | *Digital Science Magazine*. [online] Digital Science Magazine. Available at: <https://www.digitalmag.sk/bezpecnost-komunikacia-na-internete/>.

Johansen, A., 2020. *What Is A Computer Virus?*. [online] Us.norton.com. Available at: <https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html>.

Kaliňák, V., 2022. *Sociálne inžinierstvo a princípy presviedčania | Preventista*. [online] Preventista.sk. Available at: <https://preventista.sk/info/socialne-inzinierstvo-a-principy-presviedcania/>.

Koliba, J., 2018. *Ako bezpečne komunikovať na internete? Pozrite si niekoľko tipov*. [online] Živé.sk. Available at: <https://zive.aktuality.sk/clanok/124083/ako-bezpecne-komunikovat-na-internete-pozrite-si-niekolko-tipov/>.

Mukherjee, L., 2020. Email Security: *10 Steps for How to Secure Your Email Communication*. [online] InfoSec Insights. Available at: <https://sectigostore.com/blog/email-security-how-to-secure-email-communication/>.

Qubit Academy. 2021. *Bezpečná komunikácia.* [online] Qubit Academy. Available at: <https://qubitacademy.com/sk/2021/02/03/bezpecna-komunikacia/>.

Soare, B., Petcu, A. and Din, A., 2019. *What Is Email Security?*. [online] Heimdal Security Blog. Available at: <https://heimdalsecurity.com/blog/email-security/> [Accessed 2021].

Keywords: electronic communication, e-mail, security, risk, measures, awareness.

Summary

The article deals with the security of electronic communication with a focus on e-mail communication. Due to the ever-increasing electronic and informatization and the large number of e-mail users, it is necessary to constantly ensure and increase the level of security and safety awareness of people and subsequently inform about possible risks and resulting measures in electronic communication. The primary goal of the study is to find out at the level of the survey the level of security awareness of women in the field of e-mail communication. At the same time, it was important to identify and characterize the underlying risks and follow-up measures that can affect e-mail communication. By comparing these data and evaluating them through graphs, the results of the survey were presented at the end of the paper.

Kontaktné údaje

Ing. Kristína Staňová

Vysoká škola bezpečnostného manažérstva v Košiciach

Košťova 1

040 01 Košice

e-mail: kristina.stanova@vsbm.sk

Recenzenti: doc. RNDr. Tatiana Hajdúková, PhD.

PhDr. Peter Veselý, PhD.

Kybernetické útoky na infrastrukturu státu

Vladimír Šulc

Abstrakt: Kybernetická bezpečnost je v současné době jedním z nejvíce diskutovaných témat v oblasti bezpečnosti. Stále narůstající závislost nejen soukromých subjektů, ale také orgánů veřejné moci na informačních technologiích staví digitální terorismus do popředí, jako metodu vytváření a šíření strachu cestou digitálních dezinformačních hrozeb. Naléhavou otázkou je zabezpečení informační infrastruktury a uložených, často velice citlivých dat.

Klíčová slova: Kybernetická bezpečnost, kybernetické útoky, kritická infrastruktura státu, DDoS útoky.

Abstract: Cyber security is currently one of the most discussed topics in the field of security. The growing dependence of not only private actors but also public authorities on information technology puts digital terrorism at the forefront, as a method of creating and spreading fear through digital disinformation threats. The urgent issue is securing the information infrastructure and stored, often very sensitive data.

Keywords: Cyber security, cyber attacks, critical state infrastructure, DDoS attacks.

Úvod

V posledních dnech jsme zaznamenali několik poměrně závažných kybernetických útoků vedených na státní i soukromý sektor. Tyto útoky bývají vedeny jak ze strany cizím státem sponzorovaných organizací, tak mezi konkurencí v určitém odvětví, kde za nimi stojí nejen organizované skupiny, ale i jednotlivci.[1] Motiv těchto útočníků je ovšem různý. U státem sponzorovaných skupin se jedná o demonstraci síly a snahu narušit informační systémy a kritickou informační infrastrukturu státu, se kterým je daný stát v kybernetické válce, a tím destabilizovat jeho hospodářství. U organizovaných skupin je to zpravidla finanční motiv a snaha dostat se k penězům a vyvést je z bankovního oběhu. U jednotlivců je to spíš touha po uznání a získání respektu v kyberprostoru, nezanedbatelný je ale také finanční motiv[2].

Počet a razance těchto kybernetických útoků v čase roste a koreluje i s počtem zařízení a uživatelů připojených do internetu, kteří zpravidla vytváří ten nejslabší článek celého systému. Na tyto uživatele, kteří bezpečnost prakticky neřeší, je nejsnazší vést útok. Útočníci se pokouší získat citlivé informace, pozměnit je nebo je zcela zničit. Za tímto účelem se snaží narušit fungování informačních systémů a infrastruktury popřípadě tyto systémy ovládnout

1 ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018.
2 SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015.

a začlenit je do botnetu (což je síť infikovaných počítačů pod kontrolou útočníka, která může být zneužita ať už k plošným nebo cíleným kybernetickým útokům na další cíle v kyberprostoru).[3]

Pokud jde o výnosy z těchto kybernetických útoků, podle některých odhadů už celosvětově převýšily výnosy z klasické trestné činnosti a škody jdou až do miliard dolarů. Nemůžeme si rovněž nevšimnout, že vzdálenost mezi útočníkem a obětí se stále prodlužuje. Útočníci využívají zdánlivě anonymního prostředí internetu k vedení kybernetických útoků, kdy své útoky vedou prakticky z jakéhokoliv místa na zemi. Úspěšnost dopadení pachatelů, kteří páchají kyberkriminalitu, je totiž ve srovnání s ostatními typy trestné činnosti dlouhodobě nejnižší[4].

DDoS útoky

Při dosud největším kybernetickém útoku na ukrajinské státní banky a weby, kdy se odehrál největší DDoS útok na vládní weby a bankovní sektor v dějinách Ukrajiny, byly použity IP adresy z Ruska, Číny, Uzbekistánu a České republiky[5]. Všechny orgány, které mají na starosti počítačovou bezpečnost a služby počítačové bezpečnosti v bankovních institucích pracovaly na tom, aby čelily těmto útokům a co nejrychleji je zlikvidovaly. Skutečně tento útok byl bezprecedentní. Je jasné, že byl předem připraven a že klíčovým cílem byla destabilizace a vyvolání paniky a chaosu.

Cílem DDoS útoků, jak už tato zkratka napovídá, je odepření služby (Distributed Denial of Service) a to zahlcením cíle množstvím požadavků. V zásadě rozlišujeme dva typy DDoS útoků a to volumetrické a aplikační[6]. Útok na daný cíl však může být veden v podstatě na všech vrstvách ISO/OSI modelu a zahlcen tak může být i prvek, který je cíli předřazen (například firewall). Nezapomínejte, že typická infrastruktura se skládá zpravidla z těchto prvků: hraniční router, firewall, load balancer, DNS server, reverzní proxy a teprve až poté webové, aplikační a databázové servery[7].

---

[3] BRADSHAW, Samantha. *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*. Global Commission on Internet Governance. [online]. 2015.

[4] POLČÁK, Radim, Jakub HARAŠTA a Václav STUPKA. *Právní problémy kybernetické bezpečnosti*. Brno: Masarykova univerzita, 2016.

[5] DRATVA Pavel. *Při dosud největším kybernetickém útoku na ukrajinské weby byly použity IP adresy z Česka*. Newsbox. [online]. 2022.

[6] SARKHEL Aritra. *Tools for DDoS attacks available for free online*. The Economic Times, tech. [online]. 2017.

[7] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007.

Byť je dnešní aplikace obvykle vícevrstvá a jednotlivé její vrstvy (minimálně webová, aplikační a databázová) bývají často od sebe odděleny firewally, tak může dojít k situaci, že určitý prvek se DDoS útoku sice ubrání, ovšem začne intenzivně komunikovat s jiným prvkem a to na stejné nebo nižší vrstvě a ten zahltí. Uživateli takového systému se pak bude daná služba jevit jako nefunkční nebo nedostupná.

DDoS útok je na rozdíl od ostatních už od samého začátku velice přesně cílený. v zásadě jde o to, že si útočník nebo zájemce tento útok zaplatí a následně jsou z botnetu (což jsou kompromitované počítače, tzv. zombie, které jsou za úplatu pronajímány) otevírány spojení/realizovány dotazy na server či web. Pod obrovským množstvím požadavků se pak cílový systém zpomalí nebo úplně zhroutí.

Realizovat DDoS útok je poměrně snadné, stačí si jen pronajmout dostatečně velký botnet. V současné době nejnižší ceny za pronájem botnetu požadují Rusové a nabízejí, že za vás provedou i samotný DDoS útok. Pronajmout si můžete botnet čítající 1.000 až 10.000 zombií, přičemž takový botnet o 1.000 zombiích rozesetých po celém světě pořídíte již za pouhých 25 USD na den[8], což je v přepočtu nějakých 500 Kč. Pokud byste chtěli botnet nacházející se v Evropě, zaplatíte jednou tolik. Pořád je to ale taková cena, za kterou si může pronajmout botnet v podstatě každý. Součástí těchto botnetů nejsou jen počítače, ale i jednoúčelová zařízení s Linuxem, Androidem či jiným neaktualizovaným systémem. Když se zamyslíme nad následky, které firmám těmito útoky hrozí, může sem zařadit například:

- **přímou finanční ztrátu**, která vznikne, pokud by neproběhly určité obchody, protože klient by je nemohl v důsledku nedostupnosti systému realizovat[9];
- **sankce**, které mohou být uplatňovány nejen po subjektu, který danou službu poskytuje, ale i po subjektu, který danou službu využívá a spoléhá, že bude funkční, a v důsledku její nedostupnosti není schopen dostát závazkům, které vyplývají ze smlouvy (smlouvy jsou ale většinou koncipovány tak, že v případě působení vyšší moci či útoků není možné sankci za nedostupnost uplatnit);
- **negativní publicitu**, která hrozí, pokud by se prokázalo, že k nedostupnosti služby dochází opakovaně a dlouhodobě z důvodu špatného zabezpečení (firma může být v médiích popotahována za neschopnost s tím něco dělat);

[8] KRAMER Franklin D., Stuart STARR a Larry K. WENTZ. *Cyberpower and national security*. Washington DC: Center for Technology and National Security Policy, 2009.
[9] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018.

- **ztrátu produktivity**, která může nastat jak na straně organizace, která danou službu poskytuje, tak i na straně subjektu, který danou službu užívá, a to proto, že vznikají náklady v souvislosti s reakcí na útok.

DDoS útoky mohou být vedeny na organizace a subjekty podnikající v různém odvětví a každý z nich může mít DDoS různý dopad[10]:

- **Vyhledávače a zpravodajské weby** – Nedostupnost těchto portálů vede přímo k poklesu počtu návštěvníků, zobrazených stránek a reklamních bannerů a tím dochází i k poklesům příjmů z reklamy. Nejde však pouze o zisk, nedostupnost určitých informací může vést k odložení některých rozhodnutí.
- **Webové prezentace bank** – v případě nedostupnosti webové prezentace samotné banky se může část návštěvníků rozhodnout pořídit daný bankovní produkt u konkurence, jejíž web byl v danou dobu dostupný. Ztráta banky by pak vyplývala z peněžního toku, který by ji mohl takový klient generovat.
- **Internetové bankovnictví** – Nedostupnost internetového bankovnictví může způsobit, že klient nebude moci zaplatit za zboží, které měl v úmyslu koupit a od jeho koupě ustoupí a banka přijde o provizi. Stejně tak se může stát, že neproběhnou určité platby.
- **Portály mobilních operátorů** – Klient, jenž na stránkách mobilního operátora vyhledává informace či chce prostřednictvím formuláře realizovat objednávku, ji provede spíše později, než že by ji neprovedl vůbec či šel na web konkurence.
- **Weby organizačních složek státu** – Tyto weby nejsou povětšinou zřizovány za účelem dosahování zisku, takže jejich nedostupnost způsobí jen to, že je občan navštíví později.
- **E-shopy** – Klient nerealizuje na e-shopu, který je nedostupný, nákup a obrátí se na konkurenci. Stejně tak ale může počkat a nákup uskutečnit později.

Útoky na kritickou infrastrukturu

Nebude překvapením, že jedním z prvních zmíněných útoků budy útoky z roku 2007 v Estonsku. Tyto útoky nejenže byly mediálně velmi sledované, ale jednalo se i o jeden z prvních kybernetických útoků na stát, který nebyl ve válečném konfliktu. Jejich důležitost

[10] ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018.

tkví také v tom, že poukázaly na některé velké nedostatky týkající se kybernetické bezpečnosti, které byly dosud opomíjeny. Události v Estonsku například vedly k přehodnocení bezpečnostních politik a zákonů vztahujících se ke kybernetické bezpečnosti ve strukturách NATO, EU ale i jednotlivých státech po celé zemi.

Útoky na různé prvky kritické infrastruktury (dále jen KI) Estonska propukly 27. dubna 2007 v návaznosti na spor mezi estonským parlamentem a Ruskem o přemístění vojenského památníku v podobě bronzové sochy sovětského vojáka na vojenský hřbitov na kraji města[11]. Útoky proběhly ve dvou fázích a ačkoliv se jednalo o několik druhů (mimo DDoS také o defacement webových stránek, nárůst nevyžádané pošty s propagandistickým obsahem aj.), které se prolínaly, ve většině případů šlo právě o útoky typu DDoS (celkem proběhlo na 128 DDoS útoků), které dočasně paralyzovaly téměř celou KI Estonska .V první fázi (zhruba od 27. do 29. dubna) docházelo hlavně k emocionálně motivovaným útokům neznámých jedinců, které nebyly příliš dobře koordinovány a nezpůsobovaly tak takové škody jako útoky v druhé fázi. Vážnější útoky pak probíhaly ve fázi od 30. dubna do 18. května, a to díky jejich výrazně intenzivnější povaze (docházelo k zapojení více botnetových sítí s daleko větší silou) a lepší koordinaci útoků, do kterých byly ve velké míře zapojeni již profesionální hackeři. V období nejsilnějších útoků byly servery přehlcovány až 400 násobným počtem požadavků oproti běžnému provozu. Většina útoků trvala pouze několik desítek minut, avšak nejdelší výpadek byl zaznamenán až na 10 hodin. Jednotlivé počítačové sítě, které se staly součástí botnetů, se nacházely celkem ve 128 zemích s nejvyšším zastoupením USA, Brazílie, Kanady, Egypta, Peru a Vietnamu, což velmi znesnadňovalo jakoukoliv lokalizaci, identifikaci či dopadení útočníků[12].

Cílem útoků byly především webové stránky státních institucí a vládních úřadů, on-line zpravodajské servery, klíčové servery internetové infrastruktury, jednotliví poskytovatelé internetového připojení a také webové stránky hlavních estonských bank zajišťující služby elektronického bankovnictví. Zasaženy byly také mnohé další servery provozované soukromými společnostmi i veřejnými institucemi. Nedošlo k žádným škodám na fyzickém majetku ani na zdraví či životech obyvatel. Většina škod byla finančních, což se týkalo zejména sektoru bankovnictví a soukromých společností, které prodělaly tím, že nebyly schopny poskytovat danou službu (například Hansabank údajně odhadla ztrátu převyšující 1 milion

[11] GEVA, M., HERZBERG, A., GEV, Y. (2014): *Bandwidth Distributed Denial of Service: Attacks and Defense*. IEEE Security & Privacy, 12, 54–61.

[12] LANDLER, M., MARKOFF, J. *Digital Fears Emerge After Data Siege in Estonia*. NYTimes.com. [online]. 2007.

USD). Škodu však utrpěl také veřejný sektor, a to především ve formě ztráty důvěry v zajišťování bezpečnosti a kritických služeb ze strany svých občanů.[13]

Závěr

V souvislosti s globálním nárůstem využívání kybernetického prostoru se neustále rozšiřuje nejen okruh jeho uživatelů, ale rovněž množství nových a sofistikovanějších způsobů páchání kybernetické trestné činnosti, která se tak stává stále větším problémem. Jedním z nejdůležitějších prvků v rámci účinného boje proti kybernetické kriminalitě je bezpochyby též preventivní předcházení nežádoucím jevům souvisejícím s využíváním kybernetického prostoru ke každodenním aktivitám lidské společnosti. Při zohlednění současných trendů vývoje a distribuce informačních systémů lze do budoucna očekávat nárůst kybernetické kriminality zejména v oblastech tzv. internetu věcí, cloudových úložišť či dalších nastupujících moderních technologií a služeb.

Cílem tohoto příspěvku bylo identifikovat rizika spjatá s hrozbou DDoS útoků, které jsou mířeny na prvky KI. V rámci analýzy bylo definováno celkem 5 významných rizik plynoucích z DDoS útoků, které ohrožují KI. Jedná se o riziko vysokých finančních ztrát jako následek DDoS útoků, riziko vyřazení zranitelných systémů se závažným dopadem na bezpečnost, zdraví a chod společnosti, riziko stále intenzivnějšího rozvoje technických možností DDoS útoků, riziko užití DDoS útoků novými aktéry a riziko podcenění připravenosti systémů KI proti DDoS útokům. Detekování IP adres z konkrétní země v podobném masivním útoku nelze nikdy zcela vyloučit. Napadená zařízení, která jsou prostřednictvím botnetové sítě zapojena do útoku, mohou být z jakékoli části světa, včetně České republiky, a koncoví uživatelé zpravidla ani nevědí, že je jejich počítač nebo chytrý telefon či nějaké chytré zařízení do útoku zapojeno.

Poznatky spojené s hrozbou DDoS útoků, které jsou přímo mířeny na prvky kritické infrastruktury, uvedené v tomto příspěvku, poskytují stručné vymezení této rozsáhlé oblasti, díky čemuž může příspěvek posloužit také jako stručný přehled dané problematiky v méně technickém jazyce, než je obvyklé. Cílem tohoto příspěvku bylo vědeckými metodami vyjádřit kybernetický pohled na systémové pojetí DDoS útoků, které jsou mířeny na prvky kritické infrastruktury státu.

[13] SPOUSTOVÁ, Michaela. *DDos útoky jako hrozba pro kritickou infrastrukturu*. Diplomová práce, 2015. Masarykova univerzita fakulta sociálních studií.

Použitá literatura

BRADSHAW, Samatha *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*. Global Commission on Internet Governance. [online]. 2017 [cit. 02. 04. 2022]. Dostupné z: https://www.cigionline.org/sites/default/files/gcig_no23web_0.pdf

DRATVA Pavel. *Při dosud největším kybernetickém útoku na ukrajinské weby byly použity IP adresy z Česka*. Newsbox. [online]. 2022 [cit. 02. 04. 2022]. Dostupné z: https://newsbox.cz/zpravy/pri-dosud-nejvetsim-kybernetickem-utoku-na-ukrajinske-weby-byly-pouzity-ip-adresy-z-ceska-dk6r7x2x.

GEVA, M., HERZBERG, A., GEV, Y. (2014): *Bandwidth Distributed Denial of Service: Attacks and Defense*. IEEE Security & Privacy, 12, 54–61.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007.

KRAMER Franklin D., Stuart STARR a Larry K. WENTZ. *Cyberpower and national security*. Washington DC: Center for Technology and National Security Policy, 2009.

LANDLER, M., MARKOFF, J. *Digital Fears Emerge After Data Siege in Estonia*. NYTimes.com. [online]. 2007 [cit. 02. 04. 2022]. Dostupné z: http://www.nytimes.com/2007/05/29/technology/29estonia.html

POLČÁK, Radim, Jakub HARAŠTA a Václav STUPKA. *Právní problémy kybernetické bezpečnosti*. Brno: Masarykova univerzita, 2016.

SARKHEL Aritra. *Tools for DDoS attacks available for free online*. The Economic Times, tech. [online]. 2017 [cit. 02. 04. 2022]. Dostupné z: https://economictimes.indiatimes.com/technology/tools-for-ddos-attacks-available-for-free-online/articleshow/56297496.cms

SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015.

SPOUSTOVÁ, Michaela. *DDos útoky jako hrozba pro kritickou infrastrukturu.* Diplomová práce, 2015. Masarykova univerzita fakulta sociálních studií.

ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018.

Kontaktní údaje

Ing. Vladimír Šulc Ph.D.

AMBIS vysoká škola, a.s.

Katedra Bezpečnosti a práva

Šujanovo náměstí 356/1, 602 00 Brno

vladimir.sulc@ambis.cz

Tel.: +420 605 714 895

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

PaeDr. Peter Veselý, PhD.

Bezpečnosť na sociálnych sieťach

Jana Zachar Kuchtová

Abstrakt: Sociálne siete umožňujú používateľom interaktívnu formu vytvárania a zdieľania obsahu, ktoré je realizované prostredníctvom vytvoreného účtu. Takýto účet tvorí súčasť digitálnej identity, čo je jedným z hlavných dôvodov, prečo sa páchatelia kybernetickej kriminality snažia ostať anonymní. Cieľom tohto príspevku je poukázať na vybrané aspekty súvisiace s bezpečnosťou na sociálnych sieťach a to najmä na najväčšej sociálnej sieti Facebook. S tým súvisí vyhľadávanie a posudzovanie informácií a odlišovanie relevantných informácií od dezinformácií a hoaxov a odhaľovanie falošných profilov na sociálnych sieťach. CSAM

Kľúčové slová: bezpečnosť, internet, sociálne siete

Abstract: Social networks allow users an interactive form of content creation and sharing, which is realized through the created account. Such an account forms part of a digital identity, which is one of the main reasons why cybercriminals try to remain anonymous. The aim of this post is to highlight selected aspects related to security on social networks, especially on the largest social network, Facebook. Related to this is finding and assessing information and distinguishing relevant information from misinformation and hoaxes and detecting fake profiles on social networks.

Key words: security, internet, social networks

Úvod

Internet umožňuje jeho používateľom spájať sa kdekoľvek na svete, či už za účelom práce, zábavy alebo voľného času. Prenos správ a ďalšieho obsahu umožňujú počítačové siete, prostredníctvom ktorých je možná komunikácia na diaľku. V súčasnosti je jedným z najžiadanejších spôsobov komunikácie a zdieľania dát využívanie sociálnych sietí. Aj napriek tomu, že internet možno považovať za významný míľnik ľudstva je okrem všetkých pozitív nutné brať do úvahy aj druhý, nemenej významný faktor – bezpečnosť. Cieľom tohto príspevku je poukázať na bezpečné používanie sociálnych sietí, na ktorých je umožnená registrácia prakticky komukoľvek. Každý používateľ môže mať viacero účtov, pri registrácii stačí vyplniť e-mail, dátum narodenia a pohlavie. Aj napriek tomu, že sociálne siete obmedzujú minimálny vek používateľa[1], po zadaní falošných údajov týkajúcich sa dátumu narodenia sa dokážu registrovať aj osoby, ktoré sú mladšie ako stanovený vekový limit. *„Komunikácia z domova v kombinácii s anonymitou virtuálneho priestoru vytvára najmä u deti zdanlivý pocit bezpečia a povzbudzuje ich, aby sa komunikácia rýchlejšie otvorila a odložili zábrany. Rizikom je, že nie*

[1] Minimálny vek pre vytvorenie účtu na sociálnej sieti Facebook je 13 rokov.

vždy, či dokonca nikdy si nemôžeme byť istí, kto je osoba na druhej strane. Ilúzia dokáže zmiasť aj dospelého človeka a ešte väčší zmätok narobí s detskou zraniteľnejšou a dôverčivejšou mysľou, ale s oveľa horšími následkami. Mládež nemá zábrany sprostredkúvať ani svoje intímne zážitky, čo ľuďom s nie najlepšími úmyslami dáva do rúk zbrane, ktoré potrebujú na ceste ku svojej potenciálnej obeti.“ [2]

Základné zásady bezpečného používania internetu

Súčasný dynamický a turbulentný vývoj ľudskej spoločnosti so sebou prináša mnohé bezpečnostné hrozby a riziká, ktoré oprávnene stavajú otázky bezpečnosti na popredné miesto.[3] Bezpečnosť totiž tvorí základnú a nevyhnutnú podmienku rozvoja každej spoločnosti a dnes, v ére prehlbujúcej sa globalizácie, už neexistuje oblasť spoločenského života, ktorá by s ňou nebola spojená a v ktorej by nebolo potrebné prijímať opatrenia a dodržiavať zásady zamerané na elimináciu reálnych i potenciálnych bezpečnostných hrozieb a rizík.[4]

Bezpečnosť používateľov internetu zvyšuje dodržiavanie určitých zásad, ktorých realizácia pôsobí preventívne, aj keď nikdy nemožno hovoriť o stopercentne účinnej ochrane. V prvom rade by mal byť **každý** používateľ dostatočne informovaný, ako je potrebné bezpečne na internete vyhľadávať, aké sú dôveryhodné zdroje a informácie, ako si ich overiť, aký obsah si možno bezpečne stiahnuť do svojho zariadenia a ako zamedziť tomu aby sa používateľovi nevedomky sťahoval do zariadenia neželaný obsah, prípadne ho sám nedistribuoval.

Bezpečné vyhľadávanie na internete zaručujú dôveryhodné vyhľadávacie nástroje, ktoré boli do zariadenia stiahnuté priamo od overených výrobcov. Počas vyhľadávania sa neodporúča navštevovať neznáme webové stránky a ak už používateľ niektorú navštívil, nemal by z nej sťahovať žiaden obsah do svojho zariadenia.

Za dôveryhodné zdroje a informácie možno považovať tie, ktoré sú všeobecne známym faktom, boli overené, sú vedecky alebo faktologicky podložené a pod. V súčasnosti je internet plný rôzneho obsahu, ktorého relevantnosť nie je často krát známa. Používatelia si často krát nevedia overiť ich pravdivosť čo má za následok ďalšie šírenie neoverených informácií, hoaxov a dezinformácii.

[2] HAJDÚKOVÁ, T, BACIGÁL, I.. Hrozby kybernetického priestoru pre deti v období dospievania. *In: Policajná teória a prax, Roč. 22, č. 3 (2014), s. 5-19*
[3] IVANČÍK, R. 2022. *Bezpečnosť. Teoreticko-metodologické východiská*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2022, s. 7
[4] IVANČÍK, R. 2021. Security Theory: Security as a Multidimensional Phenomenon. In *Vojenské reflexie*, 2021, roč. 16, č. 3, s. 33

- Informovanosť

Základom akejkoľvek bezpečnosti je informovanosť, ktorá umožňuje používateľovi identifikovať hrozby. V zásade platí, že čím väčšia je informovanosť, tým vyššia je šanca nepodľahnúť útočníkom. Najbežnejšie sú prípady súvisiace s hromadnými útokmi zameranými na kvantitu, napríklad nigerijské listy[5], ktoré páchateľ rozošle čo najväčšej skupine ľudí alebo na kvalitu, v zmysle budovania si pomyselného vzťahu s vybranou obeťou.

- Vzdelanie

Vzdelanie v oblasti bezpečnosti a bezpečného správania sa na internete by mala byť neodmysliteľnou súčasťou nie len vo vzdelávaní mládeže ale aj ďalších rizikových skupín; seniorov a nových používateľov internetu a sociálnych sietí.

- Poznanie a predchádzanie útokom

Okrem všeobecného vzdelania z oblasti bezpečného správania sa na internete a sociálnych sietí je hlbšie poznanie problematiky zásadným atribútom k ochrane používateľa pred širokou škálou hroziacich útokov.

- Antivírus a iné bezpečnostné programy

Kvalitná antivírusová ochrana by mala byť súčasťou nie len stolných počítačov a notebookov ale všetkých smart zariadení. Internet veci (IoT) spočíva v prepojení inteligentných zariadení v domácnosti. Slabý článok v takejto štruktúre zariadení tvorí významné bezpečnostné riziko.[6] Rovnako by mali byť zabezpečené aj smartfóny, kde používatelia častokrát nemajú žiadnu alebo len minimálnu ochranu.

Bezpečnosť sociálnej siete Facebook

[5] Nigerijské listy sú správy, ktoré obsahujú dojímavý alebo zdanlivo pre obeť finančne prospešný príbeh. Ide o nevyžiadané telefonáty, emaily, pop-up reklamy (vyskakovacie okná), či presmerovanie na falošný web alebo e-shop. Ich cieľom je získať prístup k vašim osobným údajom.

[6] Domáce bezpečnostné systémy Ring, ktoré vlastní Amazon, sa dostali do celoštátnych titulkov, keď sa koncom roka 2019 objavilo video, na ktorom sa muž rozprával s osemročným dievčaťom cez zariadenie Ring v jej izbe, kde jej povedal „Som tvoj najlepší priateľ“. ROUHANDEH, A. How Cyber Thieves Use Your Smart Fridge As Door to Your Data. [online] [cit. 2022-05-09]Dostupné na internete https://www.newsweek.com/how-cyber-thieves-use-your-smart-fridge-door-your-data-1603488

Spoločnosť Meta Platforms Ireland Limited, ktorá poskytuje aplikáciu Facebook, v svojich podmienkach a službách používania deklaruje nasledovné: *„Bojujeme proti škodlivému správaniu, chránime a podporujeme našu komunitu: Ľudia budú v Produktoch Meta budovať komunitu iba vtedy, ak sa budú cítiť bezpečne. Po celom svete zamestnávame špecializované tímy a vyvíjame pokročilé technické systémy na zisťovanie zneužitia našich Produktov, škodlivého správania voči iným a identifikovanie situácií, v ktorých by sme mohli napomôcť podpore a ochrane našej komunity. Ak sa dozvieme o takomto obsahu alebo správaní, podnikneme príslušné kroky – môžeme napríklad ponúknuť pomoc, odstrániť obsah, zablokovať prístup k určitým funkciám, zablokovať účet alebo kontaktovať orgány presadzovania práva. Keď zistíme zneužitie alebo škodlivé správanie zo strany niekoho, kto používa niektorý z našich Produktov, údaje zdieľame s ďalšími Spoločnosťami Meta.“*. Zároveň vymedzuje, že Produkty Meta je možné používať len pokiaľ nedochádza k porušovaniu ich noriem a zásad a zároveň zakazuje nezákonné, zavádzajúce, diskriminačné alebo podvodné správanie používateľov. V prípade, že dôjde k zisteniu, že používateľ koná v rozpore s pravidlami, môže byť jeho účet odstránený alebo zablokovaný.

Efektívne odhaľovanie falošných profilov na sociálnej sieti Facebook

V súčasnosti je na sociálnej sieti Facebook aktívnych cca 2,9 miliardy používateľov.[7] Z toho je podľa dostupných štatistík 16% profilov falošných alebo duplicitných. Facebook vydáva štvrťročnú správu, ktorej obsahom sú aj aktualizované informácie o podiele falošných účtov. Odhaduje sa, že podiel duplicitných účtov tvorí 11% mesačne aktívnych používateľov, čo tvorí okolo 275 miliónov profilov. Podiel „falošných“ – nesprávne klasifikovaných a „nežiaducich“ – účtov sa pohybuje okolo 5% v prvom kvartály roku 2022 (čo tvorí cca 1,6 miliónov používateľských profilov). Vzhľadom na to, že metóda detekcie falošných a duplicitných účtov sa neustále vyvíja, nie je v súčasnosti možné štatisticky zaznamenávať ich nárast alebo pokles.[8] Zástupcovia sociálnej siete Facebook tvrdia, že cieľom je odstrániť čo najviac falošných účtov, pričom uprednostňované sú tie, ktoré sa snažia spôsobiť škodu prostredníctvom spamu alebo finančnej motivácie.[9]

[7] Essential Facebook statistics and trends for 2022. [online] [cit. 2022-05-10]. Dostupné na https://datareportal.com/essential-facebook-stats
[8] ARMSTRONG, M. 16% of All Facebook Accounts Are Fake or Duplicates. [online] [cit. 2022-05-10]. Dostupné na https://www.statista.com/chart/20685/duplicate-and-false-facebook-accounts/
[9] WARWICK, S. Facebook removed 1.6 billion fake accounts in just three months. [online] [cit. 2022-05-10]. Dostupné na https://www.imore.com/facebook-removed-16-billion-fake-accounts-just-three-months

Znalosť odhaľovania falošných profilov na sociálnej sieti Facebook je významná pre bezpečnosť používateľa na sociálnych sieťach.

Spôsob odhaľovania falošných účtov na sociálnej sieti Facebook

Prvým stretom s falošným profilom na sociálnej sieti Facebook spočíva v tom, že sa takýto používateľ snaží o interakciu. To znamená, že iniciuje prvý kontakt alebo žiada iných používateľov o priateľstvo. Základom bezpečného správania sa je nepotvrdzovať takéto žiadosti neznámym osobám, ktoré by z profilu používateľa mohli vyčítať citlivé informácie a následne by ich mohli zneužiť. Medzi takéto informácie, ktoré používateľ o sebe zverejňuje patrí napríklad pracovisko, vyštudované školy, mesto narodenia a aktuálne mesto, v ktorom používateľ žije. Tiež sem patria rôzne životné udalosti, fotografie, videá a v neposlednom rade samotný zoznam priateľov. Tieto informácie sú zneužívané na sociálne inžinierstvo, ktoré spočíva vo vybudovaní si dôvery so svojou obeťou a následnou snahou o získanie ďalších citlivých informácií, peňazí a pod. Ďalšou s hrozieb je kyberšikana, ktorá môže súvisieť so zverejnenými informáciami na sociálnej sieti, krádež identity, stalking a mnoho ďalšieho.

Pre falošný profil je typická absencia akejkoľvek profilovej fotografie. Ak už fotografia prítomná je, tá nie je reálna a nepatrí danej osobe. Väčšinou ide o fotografie známych alebo atraktívnych ľudí aby si získali pozornosť. Existuje základný spôsob, akým je možné fotografiu overiť prostredníctvom webovej stránky www.google.sk. Najprv je potrebné profilovú fotografiu stiahnuť do svojho zariadenia. Následne na stránke www.google.sk zvoliť v pravom hornom rohu ikonu fotoaparátu. Stiahnutú fotografiu je potrebné nahrať zo zariadenia, následne sa zobrazí ponuka najlepšej zhody, medzi ktorou sa častokrát objaví aj pravý majiteľ fotografie. Vo väčšine prípadov ide o verejne dostupné profily, z ktorých je možné fotografie ľahko získať a zneužívať ich na vytváranie falošných profilov. Vzhľadom na to, že falošne profily pozostávajú z cudzích fotografií, veľakrát ich je v profile zverejnených málo, prípadne sú dopĺňané o fotografie iných osôb, ktoré sú podobné alebo odfotené z nerozpoznateľných uhlov od profilovej fotky.

Informácie zverejňované vo falošných profiloch sú vytvárané účelovo tak, aby pôsobili čo najatraktívnejšie a najzaujímavejšie. Môže ísť napríklad o vydávanie sa za vojaka, lekára, modelku a pod. Informácie o takomto používateľovi buď absentujú alebo pozostávajú z najznámejších alebo najnavštevovanejších lokalít, zo známych škôl a zamestnaní. Tvorcovia takýchto profilov nezachádzajú do detailov. Zároveň sa na nástenke takého používateľa

spravidla nachádza len veľmi málo príspevkov a reakcií na nich. Ak ide o profil vytvorený za účelom propagácie, príspevky budú zamerané na túto oblasť a budú sa opakovať.

Dôležitým ukazovateľom je zoznam priateľov. Falošný profil má buď veľmi nízky počet priateľov alebo naopak, najmä ak sú na vytvorenie takého profilu zneužité fotky atraktívnej ženy, resp. žien, bude počet priateľov veľmi vysoký. Ide však o ľudí z rôznych častí štátu alebo sveta, ktorí medzi sebou nemajú žiadne väzby a aj napriek snahe o interakciu v komentároch nedochádza k žiadnej reakcii zo strany falošného profilu.

Medzi posledný ukazovateľ patrí dátum registrácie na sociálnej sieti. Falošné profily pôsobia na sociálnej sieti väčšinou krátku dobu, preto ide skôr o nových používateľov. Tento jav je spôsobený najmä tým, že na sociálnej sieti Facebook existujú skupiny, ktoré zdieľajú a nahlasujú takéto falošné profily, ktoré sú následne odstraňované. Ak je používateľ takýmto falošným účtom kontaktovaný, má možnosť nahlásiť a blokovať takýto profil.

Motivácii na vytváranie takýchto profilov je mnoho, avšak spoločným ukazovateľom je snaha o čo najväčšiu anonymitu. Môže ísť o:

- internetových trollov, ktorých účelom je vytvárať provokatívne komentáre s cieľom získavania interakcií alebo odkláňania od pôvodných tém. Väčšinou platí, že obsahom nie sú vlastné príspevky ale skôr príspevky či stránky, ktoré sú populárne a navštevuje alebo komentuje ich veľa používateľov. Rozpoznanie internetového trolla vyznačujú okrem provokatívnych komentárov aj spôsob jeho reakcií, ktorých snahou je pokračovať v konverzácii čo najdlhšie. Najzásadnejším ukazovateľom je denný počet príspevkov, ktorý je u takýchto používateľov spravidla výrazne vyšší.
- Spam týkajúci sa pridružených odkazov, na ktoré používateľ s falošným profilom odkazuje v komentároch a skupinách. Častokrát ide o lákavé ponuky lacných vecí, odkazy na šokujúce správy, ľahké zarábanie prostredníctvom internetu a mnoho iného, ktoré majú spoločnú podstatu, ktorá spočíva v linku na ktorý keď používatelia kliknú, prípadne sa niekde registrujú, z čoho majú jednotlivci alebo spoločnosti finančný profit. Ide o takzvané clickbaity alebo affiliate marketing.
    - Clickbaity sú založené na princípe zaujatia čo najväčšieho počtu používateľov, ktorých upútava zaujímavý, šokujúci názov, prípadne obrázok. Následne keď si používateľ otvorí článok, obsah je úplne iný alebo len čiastočne taký, na aký odkazovala upútavka. Cieľom je zvýšenie návštevnosti webovej stránky za účelom

zobrazovania reklám alebo ponuky produktov, zdieľanie materiálov alebo šírenia škodlivých kódov.

- Affiliate marketing spočíva v predaji produktov alebo služieb prostredníctvom sprostredkovateľov. Sprostredkovateľom môže byť ktokoľvek, často ide o známe osobnosti, ktoré zdieľajú ponuku s určitou zľavou. Pokiaľ používateľ použije kód alebo link takej osoby, tá dostáva percentuálnu časť z predaja. Vzhľadom na to, že cieľom je sprostredkovávať predaj sa častokrát za týmto účelom využívajú falosné profily na sociálnych sieťach, ktoré zdieľajú odkazy.

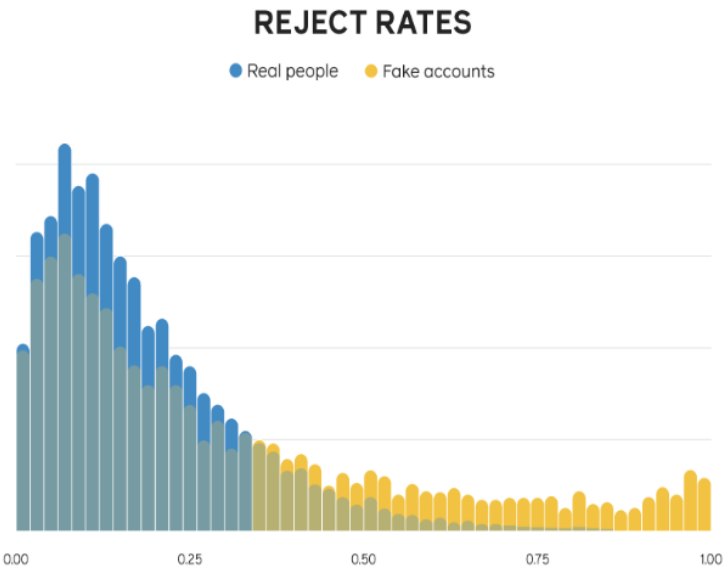
- Šírenie malware, ktorého distribúcia prostredníctvom sociálnych sietí je na vzostupe. Útočníci zdieľajú odkazy prostredníctvom falošných účtov, na ktoré keď používatelia kliknú, hrozí stiahnutie malware do zariadenia, prípadne sa nevedome stanú sami jeho šíriteľmi.
- Phishing prostredníctvom ktorého sa útočníci snažia získať citlivé informácie od používateľov, ktoré následne zneužívajú vo svoj prospech alebo v prospech spoločností na marketingové účely.
- Podvody pri ktorých si útočníci vytvárajú falošné profily na sociálnych sieťach a oslovujú opačné pohlavie s cieľom vytvoriť si s nimi pomyselný vzťah založený na citoch. Cieľom je následne získavať peniaze, častokrát s prísľubom vrátenia alebo príchodu za podvedenou osobou.

Algoritmus SybilEdge

Algoritmus SybilEdge slúži na odhaľovanie nových falošných účtov, ktoré sa dokážu vyhýbať klasifikátorom podľa času registrácie ale zároveň ešte nemajú dostatočné prepojenia na porušovanie podmienok a pravidiel sociálnej siete Facebook. SybilEdge sa zamierava na účty, ktoré dokážu obchádzať obrany. Ide o nové účty ihneď po ich vytvorení, napr. pomocou podozrivej e-mailovej adresy alebo adresy IP, ktoré sú v počiatočných štádiách svojej aktivity na platforme, prípadne ešte predtým, než sa prejaví ich zneužitie. Včasným odhalením falošných účtov sa obmedzuje schopnosť zneužívania iných používateľov.

Z týchto dôvodov bol navrhnutý a vytvorený algoritmus s názvom SybilEdge, ktorý spracováva spôsob, akým si noví používatelia pridávajú priateľov do svojich sociálnych sietí. Pri pohľade na výber cieľov žiadostí o priateľstvo a zodpovedajúcich prijatých a zamietnutých žiadostí SybilEdge presne deteguje falošné účty, na čo stačí už 20 žiadostí o priateľstvo.

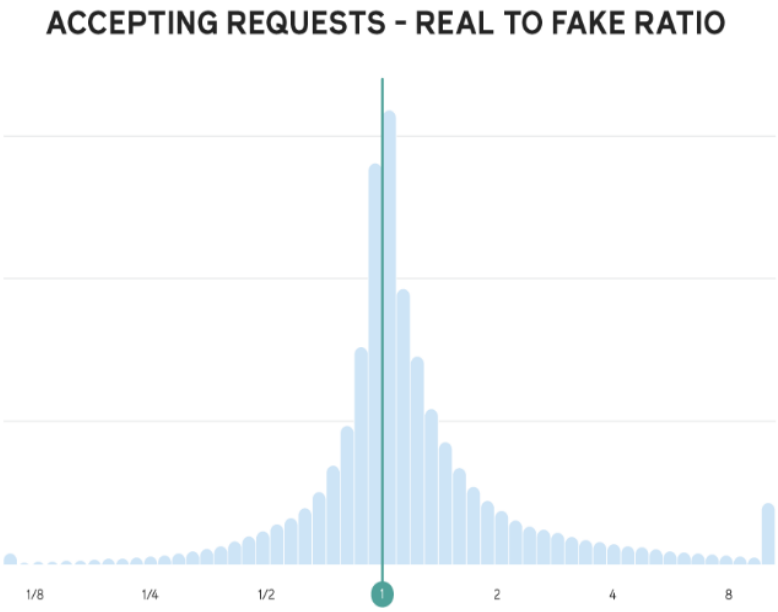
Používatelia si po vytvorení falošného účtu najprv musia nájsť ciele, následne im poslať žiadosť o priateľstvo a nakoniec si nechať túto žiadosť schváliť. Vývojári algoritmu SybilEdge zistili, že výber potenciálnych priateľov ako aj schvaľovanie žiadostí o priateľstvo sa výrazne líši v skupine bežných používateľov a v skupine používateľov s falošnými účtami.



Graf 4 Počet zamietnutých žiadostí z celkového počtu žiadostí o priateľstvo
Zdroj: https://research.facebook.com/blog/2020/04/detecting-fake-accounts-on-social-networks-with-sybiledge/

Na prvom grafe je rozdelená miera odmietnutí (počet zamietnutých žiadostí z celkového počtu žiadostí o priateľstvo). Miera odmietnutia falošných účtov je vychýlená doprava, čo znamená, že ich žiadosti sú zamietnuté častejšie ako žiadosti skutočných používateľov. Vychádza sa najmä z toho, že ľudia sú ostražití a je pravdepodobnejšie, že odmietnu žiadosti prichádzajúce z falošných účtov (ktoré pravdepodobne nepoznajú) ako od skutočných ľudí (ktorých s väčšou pravdepodobnosťou poznajú). Ako však ukazuje graf 1, niekedy sú odmietnuté žiadosti aj od skutočných ľudí a zároveň nie sú vždy odmietnutí falošní používatelia.

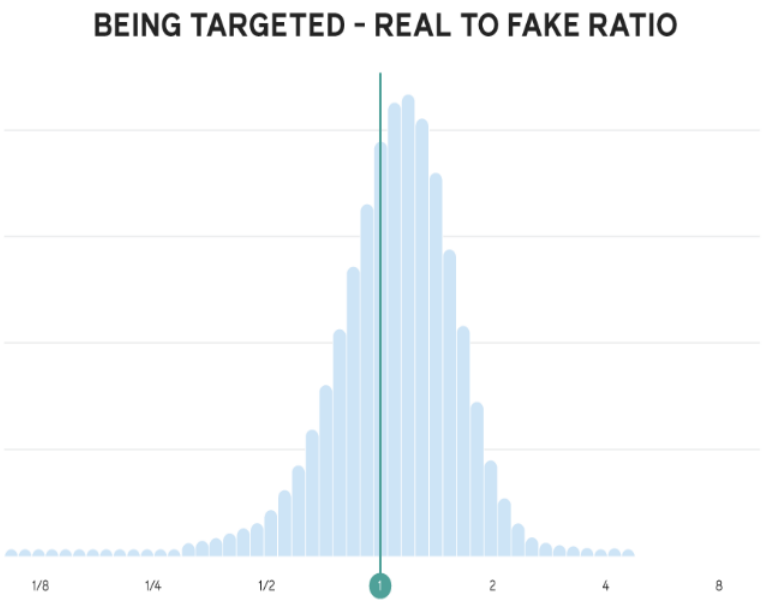
Nasledujúci graf zobrazuje pomer medzi akceptovaním žiadosti o priateľstvo od skutočných a falošných účtov. Hodnota 1 označuje ľudí, ktorí rovnako pravdepodobne akceptujú falošné účty ako skutočných ľudí. Ak je hodnota väčšia ako 1, znamená to prijatie väčšieho počtu žiadostí od skutočných ľudí ako od falošných účtov. Ak je hodnota menej ako 1, znamená to prijatie väčšieho počtu žiadostí, ktoré prijímajú používatelia z falošných účtov.



Graf 5 Pomer medzi akceptovaním skutočných a falošných účtov
Zdroj: https://research.facebook.com/blog/2020/04/detecting-fake-accounts-on-social-networks-with-sybiledge/

Používatelia pod hodnotou 1 s väčšou pravdepodobnosťou dostanú požiadavky od skutočných používateľov, zatiaľ čo používatelia nad hodtnotou 1 s väčšou pravdepodobnosťou dostanú požiadavky od falošných používateľov. Vďaka tomu je možné na základe cieľa žiadateľa zvýšiť pravdepodobnosť, či je žiadateľ falošný alebo skutočný.

Tieto pozorovania zapadajú do pravdepodobnostného rámca, kde je určovaná pravdepodobnosť, či používateľ bude falošný. To je možné na základe pozorovania množiny cieľov (ľudí, ktorým boli odoslané žiadosti o priateľstvo) a ich zodpovedajúcich odpovedí (prijatie alebo odmietnutie).



Graf 6 Pomer medzi žiadosťami o priateľstvo medzi skutočnými a falošnými účtami
Zdroj: https://research.facebook.com/blog/2020/04/detecting-fake-accounts-on-social-networks-with-sybiledge/

Model SybilEdge funguje v dvoch fázach:

1. Pozorovanie údajov za určité časové obdobie a využívanie výstupov z iných klasifikátorov; klasifikátory správania a obsahu, ktoré na základe skutočného zneužitia označia účet ako zneužívajúci.
2. Spustenie modelu v reálnom čase pre každú žiadosť o priateľstvo a odpoveď (prijatie alebo odmietnutie) a aktualizácia pravdepodobnosti, že žiadateľ bude falošný.

Záver

Bezpečnosť na sociálnych sieťach tvorí významnú oblasť, ktorou je potrebné sa zaoberať. Vzhľadom na veľký počet používateľov a interaktívny obsah, zdieľané osobné údaje a anonymitu komunikácie sa vytvoril ďalší priestor, v ktorom sa páchatelia realizujú a ohrozujú tým bezpečnosť používateľov. Sociálne siete nemusia slúžiť len ako distribútor škodlivých kódov a informácií ale zároveň sa v nich dokážu priamo tvoriť. Najčastejšími príkladmi sú dezinformácie, hoaxy, sociálne inžinierstvo, kyberšikanovanie, grooming, sexting a mnoho ďalšieho, pričom páchatelia v záujme uchovania svojej anonymity na túto činnosť zneužívajú falošné profily. Cieľom príspevku bolo poukázať na možnosti odhaľovania falošných profilov

na sociálnej sieti Facebook, zároveň popísať aktuálne vyvíjaný, testovaný a používaný algoritmus SybilEdge ako nástroj ochrany proti falošným účtom na sociálnej sieti Facebook. Tento a mnoho ďalších obdobných nástrojov možno považovať za nevyhnutnú súčasť budúcnosti internetu.

Zoznam použitej literatúry

ARMSTRONG, M. 16% of All Facebook Accounts Are Fake or Duplicates. [online] [cit. 2022-05-10]. Dostupné na https://www.statista.com/chart/20685/duplicate-and-false-facebook-accounts/

Essential Facebook statistics and trends for 2022. [online] [cit. 2022-05-10]. Dostupné na https://datareportal.com/essential-facebook-stats

HAJDÚKOVÁ, T, BACIGÁL, I.. Hrozby kybernetického priestoru pre deti v období dospievania. *In: Policajná teória a prax, Roč. 22, č. 3 (2014), s. 5-19,* ISSN 1335-1370

IVANČÍK, R. 2021. Security Theory: Security as a Multidimensional Phenomenon. In *Vojenské reflexie*, 2021, roč. 16, č. 3, s. 33

IVANČÍK, R. 2022. *Bezpečnosť. Teoreticko-metodologické východiská*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2022, s. 7

ROUHANDEH, A. How Cyber Thieves Use Your Smart Fridge As Door to Your Data. [online] [cit. 2022-05-09]Dostupné na internete https://www.newsweek.com/how-cyber-thieves-use-your-smart-fridge-door-your-data-1603488

WARWICK, S. Facebook removed 1.6 billion fake accounts in just three months. [online] [cit. 2022-05-10]. Dostupné na https://www.imore.com/facebook-removed-16-billion-fake-accounts-just-three-months

Kontaktné údaje

npor. JUDr. Jana Zachar Kuchtová

Katedra informatiky a manažmentu

Akadémia PZ v Bratislave

Sklabinská 1, 83517 Bratislava

E-mail: jana.kuchtova@akademiapz.sk

Recenzenti: doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP

PaeDr. Peter Veselý, PhD.

Názov: ***Bezpečnosť elektronickej komunikácie***

Recenzenti: doc. RNDr. Tatiana Hajúková, PhD., doc. Ing. Václav Friedrich, PhD. Ing.Paed-IGIP, PaeDr. Peter Veselý, PhD.

Zostavil: JUDr. Jana Zachar Kuchtová

Vydala: Akadémia Policajného zboru v Bratislave

Počet strán: 247

Rok vydania: 2022

Vydanie: 1. vydanie

Jazyková úprava: Rukopis neprešiel jazykovou úpravou

Za obsah publikovaných príspevkov zodpovedajú autori

ISBN 978 – 80 – 8054 – 968 - 8

EAN 9788080549688