KYBERTERORIZMUS AKO SKUTOČNÝ PROBLÉM PRE MODERNÚ SPOLOČNOSŤ

npor. JUDr. Milan **KUSÁK**, LL.M.

ÚVOD

V posledných rokoch sa kybernetický svet stáva čoraz zložitejším a s tým sa zvyšuje aj počet hrozieb, ktoré nové technológie prinášajú. Zatiaľ čo technologický pokrok prináša mnoho výhod a možností, je dôležité si uvedomiť aj tienisté stránky, ktoré sú s ním spojené. Jednou z najvážnejších hrozieb, ktorej dnes čelíme v kybernetickom priestore, je kyberterorizmus.

Doposiaľ neexistuje jednotná univerzálna definícia pojmu terorizmus, a taktiež ani jednotná univerzálna definícia kyberterorizmu. Ak sa vychádza z definície, podľa ktorej „*terorizmus predstavuje násilie, resp. vyhrážanie sa násilím a zastrašovanie uplatňované proti odporcovi až do jeho fyzického zničenia*," tak potom „*kyberterorizmus tvorí zhodnú činnosť, avšak realizovanú v priestore informačných systémov*". [1]) Preto je možné kyberterorizmus vnímať ako využívanie informačných technológií, najmä internetu, na vykonávanie teroristických činov. Zámerom takýchto činov je vytváranie atmosféry strachu, narušenie kritických infraštruktúr alebo dosiahnutie politických, náboženských či ideologických cieľov prostredníctvom narušenia alebo poškodenia elektronických informačných systémov. [2])

Rozdiel medzi bežným kybernetickým útokom a kyberterorizmom je v zámeroch a výsledkoch. Kým bežný kybernetický útok môže byť motivovaný finančným ziskom, špionážou alebo jednoducho túžbou po narušení, kyberterorizmus je často spojený s väčšími ideologickými alebo politickými cieľmi a má za cieľ vyvolať v spoločnosti masový strach alebo značné škody.

V dnešnom svete je teda nevyhnutné neustále sa vzdelávať a byť pripravení na možné hrozby, ktoré kyberterorizmus môže priniesť.

1 PREHĽAD SÚČASNEJ SITUÁCIE A DÔLEŽITOSŤ TÉMY

S rastom digitálnej éry je dôležité si uvedomiť, že kyberterorizmus predstavuje vážnu hrozbu. Teroristické organizácie získavajú prístup k sofistikovanejším technikám a nástrojom, čo zvyšuje riziko útokov. V minulosti mohli byť kybernetické útoky považované za obťažovanie, ale dnes môžu spôsobiť vážne škody vrátane výpadkov elektriny, finančných problémov alebo ohrozenia zdravotníckych zariadení.

Kyberterorizmus má priame dôsledky nielen pre jednotlivcov a podniky, ale môže mať aj katastrofálne dôsledky pre celé národy. Stratégie strachu z digitálnych systémov, ekonomické straty a dokonca straty na ľudských životoch sú skutočné scenáre, ktorých sa treba obávať. Psychologicky má kyberterorizmus vplyv na spoločnosť a môže spôsobovať obavy z online transakcií a používania sociálnych médií. Preto je nevyhnutné, aby vlády, súkromný sektor a občania spolupracovali na zlepšení obranných mechanizmov a zvýšení povedomia o kybernetických hrozbách. S rastom technológií je potrebné byť o krok dopredu pred potenciálnymi teroristami a ich metódami. Je dôležité investovať do bezpečnosti a vzdelávania, aby sa minimalizovalo riziko kybernetických útokov a ochránili sa naše digitálne systémy a životy.

1) PŘIBYL, T.: *Kyberterorizmus*.
2) IVANČÍK, R. - BARIČIČOVÁ, Ľ.: Kybernetické hrozby ako súčasť asymetrických bezpečnostných hrozieb v 21. storočí, 2019.

2 TYPY ÚTOKOV

2.1 Malware a ransomware

Malware je všeobecný termín, ktorý označuje rôzne formy škodlivého softvéru, ktoré majú často za cieľ poškodiť počítačové zariadenie používateľa. Existuje mnoho názvov pre malwarové programy – vírusy, červy, trojské kone, keyloggery, droppery, scareware, spamery, zadné vrátka, rootkity, spyware, adware, ransomware, skripty, makrá a ďalšie. Každý antivírusový program používa iné označenia pre rovnaké malwarové varianty. Komplexné malwary zahŕňajú rôzne programy a techniky, ktoré sú kombinované s cieľom dosiahnuť úspech útoku. Napríklad trojský kôň môže spolupracovať s červom na šírenie malwaru. Výraz „vírus" sa najčastejšie používa na označenie rôznych typov škodlivého kódu, hoci väčšina malwarov spadá do viacerých kategórií. [3] [4] Vírus sa pripája k programom alebo súborom a môže sa replikovať a infikovať ďalšie počítačové zariadenia. [5] Červy dokážu replikovať samy seba bez akcie používateľa a šíria sa cez počítačové siete. Trójske kone sa vydávajú za legitímne programy, ale v skutočnosti sú škodlivým softvérom. Rootkity skrývajú súbory a procesy pred detekciou a môžu získať vzdialený prístup k systému. Zadné vrátka poskytujú neoprávnený prístup k systému. Boty sú zariadenia, ktoré sú súčasťou botnetov a môžu byť využité na rôzne útoky. Je dôležité chrániť sa pred malwarom a využívať bezpečnostné opatrenia ako sú aktualizácie softvéru, antivírusové programy a informovanosť používateľov. [6]

2.1.1 Skutočné prípady

Conficker (známy tiež ako Downup, Downadup a Kido) je počítačový červ, ktorý sa zameriava na operačný systém Windows a prvýkrát bol objavený v novembri 2008. Jeho pôvodná verzia, Conficker A, sa šírila prostredníctvom zraniteľnosti vo Windows Server Service. Neskôr objavené varianty, Conficker B a C (objavené v decembri 2008 a februári 2009), pridali schopnosť šírenia cez zdieľané súbory Windows so slabými heslami, ako aj cez funkciu „Autorun" na USB zariadení. Ešte novšie varianty Conficker D a E (objavené v marci 2009 a apríli 2009) zahrnovali systém komunikácie peer-to-peer, pričom varianta E stiahla a nainštalovala aj spambot Waledac, ako aj SpyProtect 2009, čo je falošný antivírusový produkt. Vzhľadom na meniaci sa spôsob šírenia Confickeru bolo ťažké odhadnúť počet infekcií počas vrcholu jeho šírenia. Odhaduje sa, že v januári 2009 bol počet infekcií medzi 9 až 15 miliónmi.

Skupina bezpečnostných výskumníkov a spoločností, vrátane Microsoftu, Symantecu a VeriSignu, vytvorila na začiatku roka 2009 Conficker Working Group (CWG) v snahe bojovať proti šíreniu Confickeru a vystopovať hackera alebo hackerov, ktorí ho vytvorili. Od vzniku CWG blokujú servery príkazy a kontroly (C&C) Confickeru registráciou určitých kľúčových doménových mien. Takto sa botnet Conficker stáva pre jeho majiteľov bezcenným. Zastavenie týchto aktivít by mohlo umožniť Confickeru znovu získať kontrolu. Microsoft momentálne ponúka odmenu 250 000 dolárov za informácie vedúce k zatknutiu tvorcov Confickeru.

3) BAILEY, M.: *Complete Guide to Internet Privacy, Anonymity & Security*, 2015.
4) SZOR, P.: *Počítačové viry : analýza útoku a obrana*, 2006.
5) *Types of Malware*, 2012.
6) *Communication from the Commision to the European Parliament...,* 2006.

2.1.2 Ransomware

Ransomware je škodlivý softvér navrhnutý na vykonávanie nelegálnych aktivít, ako je obmedzenie prístupu k osobným údajom alebo požadovanie výkupného. [7]) Výkupné je zvyčajne požadované v kryptomene, čo utajuje identitu útočníka a umožňuje mu uniknúť spravodlivosti. V posledných rokoch došlo k značnému nárastu ransomwarových útokov.

Existujú rôzne formy ransomware vrátane lockeru, crypto a scareware. Scareware zavádza užívateľov pomocou vyskakovacích reklám, aby si mysleli, že musia stiahnuť určitý softvér, a tým si nainštalujú malware. Táto forma ransomwaru je založená skôr na zastrašovaní užívateľov, než na uzamknutí zariadenia alebo šifrovaní údajov. Locker ransomware blokuje základné funkcie počítača ako je napríklad prístup k súborom. Obyčajne je ľahko prekonateľný. Crypto ransomware šifruje citlivé súbory užívateľa a je často nezvratný v dôsledku použitia silných šifrovacích techník.

Pri hybridnom šifrovaní, čo je najťažšie dešifrovateľná forma, sa používajú symetrické aj asymetrické šifrovacie metódy. Ransomware najprv vytvorí náhodný symetrický kľúč, ktorý potom použije na šifrovanie súborov obete. [8]) Následne sú vygenerované verejné a súkromné kľúče zo servera príkazov a kontroly, ku ktorému je ransomware pripojený. Verejný kľúč slúži na šifrovanie symetrického kľúča, zatiaľ čo súkromný kľúč je uložený na serveri C&C. Obete sú následne vyzvané k zaplateniu výkupného, pričom dešifrovací proces sa spustí až po jeho úhrade. Ak je výkupné zaplatené, obeť získa prístup k dešifrovaciemu kľúču a pomocou neho súbory obnoví. [9])

Zvyčajne sa pre každú infekciu generuje unikátny pár verejných a súkromných kľúčov, aby sa obetiam znemožnilo zdieľanie súkromných kľúčov na obnovenie súborov. Ransomware je vážnou hrozbou, ktorá má negatívne dôsledky pre jednotlivcov a podniky.

2.2 DDoS útoky

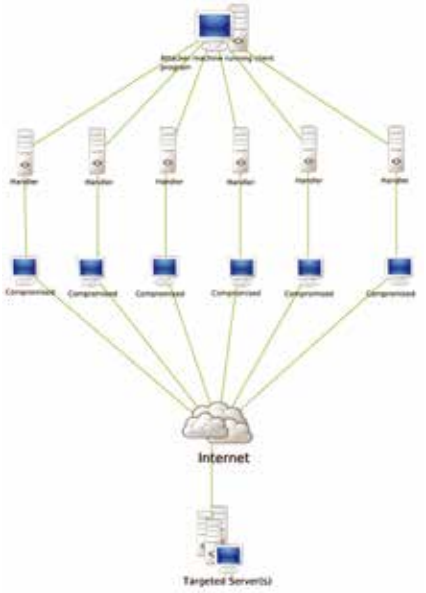
Útoky typu odopretie služby (Denial of Service, skr. DoS) sú druhom kybernetického útoku zameraného na konkrétnu aplikáciu alebo web s cieľom vyčerpať zdroje cieľového systému, čo následne spôsobí, že cieľ bude nedosiahnuteľný alebo neprístupný, čím sa legitímnym používateľom odoprie prístup k službe. Existuje mnoho foriem DoS útokov, ale najbežnejšie sú nasledujúce typy:

1. Preťaženie sieťových zdrojov spotrebuje všetok dostupný hardvér, softvér alebo kapacitu cieľa.
2. Preťaženie zdrojov protokolu spotrebuje dostupné zdroje relácie alebo pripojenia cieľa.
3. Preťaženie zdrojov aplikácie spotrebuje dostupné výpočtové alebo úložné zdroje cieľa. [10])

Útok DoS sa klasifikuje ako útok distribuovaného odopretia služby (Distributed Denial of Service, skr. DDoS), kedy preťažujúca premávka pochádza z viac ako jedného útočiaceho zariadenia (všetky spolupracujú súčasne). Útočníci DDoS často využívajú botnet na vykonávanie útokov veľkého rozsahu, ktoré sa zo strany cieľovej entity zdajú akoby pochádzali od väčšieho množstva rôznych útočníkov. Do botnetu môže patriť široká škála zariadení vrátane zariadení internetu vecí (Internet of Things, skr. IoT). Zariadenia IoT sú pripojené k internetu, často používajú predvolené heslá a chýba im dobrá bezpečnostná politika, čo ich robí zraniteľnými voči kompromitácii a zneužitiu.

7) PETROWSKI, T.: *Bezpečí na internetu pro všechny*, 2014.
8) *Ransomvér CryptoWall 3.0 zarobil stovky miliónov : Jedinej skupine*, 2015.
9) *Internet Security Threats*, 2015.
10) TRIPATHI, N. - MEHTRE, B. M.: *DoS and DDoS Attacks...*, 2013.

Keďže infekcie zariadení IoT často unikajú pozornosti používateľov, útočník môže ľahko zoskupiť stovky tisíc týchto zariadení do silného botnetu schopného vykonávať útok veľkého objemu. Ďalej, po vytvorení botnetu môže kybernetický aktér prenajímať ho iným potenciálnym útočníkom v schéme „útok za nájom", čo umožňuje neskúseným používateľom spúšťať DDoS útoky. [11])



Obrázok 1: Diagram útoku DDoS
(Zdroj: https://en.wikipedia.org)

Hoci dopad DDoS útokov môže byť často zanedbateľný (v závislosti od rozsahu útoku), ale mohol by byť aj vážny a zahŕňať stratu alebo degradáciu kritických služieb, stratu produktivity, rozsiahle náklady na nápravu a akútnu škodu na povesti.

Cieľom DDoS útoku je nemožné vyhnúť sa úplne. Existujú však proaktívne kroky, ktoré môžu organizácie podniknúť, aby zmiernili účinky útoku na dostupnosť ich zdrojov.

2.2.1 BOTNET

BOTNET je výraz, ktorý je odvodený od termínu bot, čo je skrátenie slova robot. Útočníci používajú rôzne trikové techniky na šírenie škodlivého softvéru, ktorý dokáže počítač premieňať na bota alebo zombíka. V situácii, keď počítač nie je ovládaný používateľom, ale ovláda ho hacker, vykonáva počítač na internete niekoľko podozrivých úloh bez vedomia používateľa. Útočníci zvyčajne využívajú boty na infikovanie veľkého počtu počítačov. Tieto počítače tvoria skupinu známu ako BOTNET. Tieto zombíky možno využiť na šírenie nevyžiadaných e-mailov, šírenie vírusov, útoky na servery a páchanie rôznych druhov podvodov a kybernetických trestných činov. Veľkosť BOTNETu je premenná a závisí od sofistikovanosti a zložitosti použitých botov. Veľký BOTNET pozostáva z desiatok až stoviek tisícov zombíkov. Na druhej strane menší BOTNET pozostáva z niekoľko tisíc zombíkov. Majiteľ, ktorého počítač sa stal zombíkom nevie, že postihnutý počítač a všetky jeho zdroje sú na diaľku ovládané, podrobené a zneužívané, a to jedným alebo skupinou prevádzkovateľov škodlivého softvéru, ktorí používajú Internet Relay Chat (IRC) ako podstatný nástroj pre tieto škodlivé útoky. Existuje niekoľko druhov škodlivých softvérov a aplikácií. Veľké boty sa používajú na šírenie vírusov, zatiaľ čo menšie druhy botov takéto schopnosti nemajú.

11) ROSSOW, Ch.: *Amplification Hell*..., 2014.

2.2.2 Detekcia

Detekcia BOTNETov je zložitá a veľmi náročná. Dôvodom je, že boty fungujú v sieti alebo v infikovanom stroji bez predchádzajúceho informovania majiteľa. Existujú však bežné indikátory rutinného fungovania počítača, na základe ktorých môže majiteľ určiť, či je stroj napadnutý alebo nie. Tieto indikácie sú:

1. Využitie Internet Relay Chat (IRC) monitorovaním prevádzky.
2. Časté pokusy o pripojenie k známym C&C serverom.
3. Viacero strojov generuje identické DNS požiadavky.
4. Odchádzajúca SMTP prevádzka je veľmi vysoká.
5. Neočakávané vyskakovacie okná.
6. Pomalá rýchlosť spracovania, využitie procesora je na maxime, keď nie je spustená žiadna ťažká aplikácia.
7. Vysoké a opakujúce sa špičky v dátovom prenose cez sieť. Konkrétne Port 6667 používaný pre IRC. Port 25 obvykle používaný pre nevyžiadané e-maily. Port 1080 používaný proxy servermi.
8. Odchádzajúce správy odoslané používateľom bez jeho vedomia, napríklad v e-mailoch, instantných správach, sociálnych médiách atď.
9. Prístup na internet je bez zjavného dôvodu nedostupný. Webové stránky nie je možné otvoriť. [12])

2.2.3 Obrana

Existuje mnoho metód, techník a opatrení, ktoré môže majiteľ infikovaného zariadenia podniknúť, aby predišiel útokom BOTNET. Hlavným problémom pri premene normálneho stroja na BOTNET je škodlivý softvér. Odporúčané postupy od rôznych poskytovateľov bezpečnosti sietí:

1. inštalácia a povolenie Windows Firewall,
2. zakázaná funkcia Auto-Run,
3. rušenie dôvery v heslá,
4. kompartmentalizácia siete,
5. poskytovanie najmenšieho oprávnenia,
6. inštalácia aplikácie Host-based Intrusion Prevention,
7. zlepšenie monitorovania prevádzky v sieti,
8. filtrovanie odchádzajúcich dát zo siete,
9. použitie proxy serverov,
10. monitorovanie dotazov generovaných DNS.

2.2.4 Skutočný prípad útoku DDoS – Dyn

Dňa 21. októbra 2016 sa odohral najväčší útok typu DDoS, ktorý na väčšinu dňa zastavil fungovanie mnohých častí internetu vrátane služieb ako Twitter, Amazon, GitHub a New York Times.[13])

12) SRINIVASAN, S. - DEEPALAKSHMI, P.: *Enhancing the security in cyber-world*..., 2023.
13) GREENE, T.: *How the Dyn DDoS attack unfolded*, 2016.

Cieľom útoku bola spoločnosť Dyn, ktorá zabezpečuje veľkú časť infraštruktúry systému doménových mien (DNS) na internete. Malvér použitý v útoku využil zariadenia IoT namiesto počítačov, čo viedlo k mimoriadne škodlivému útoku, ktorý bol „približne dvakrát silnejší ako akýkoľvek podobný zaznamenaný útok". [14])

To, čo robilo útok na Dyn jedinečným bola skutočnosť, že páchatelia použili špecifický typ malvéru – „botnet", ktorý infikuje sieť počítačov a koordinuje ich tak, aby sa na konkrétne servery obrátilo obrovské množstvo webovej prevádzky, až kým servery nezlyhajú. Pri útoku na Dyn bol použitý „Mirai botnet", ktorý využíval zariadenia IoT namiesto počítačov. Táto stratégia poskytla hackerom na výber oveľa viac zariadení (medzi 50 000 a 100 000) vrátane domácich smerovačov a video rekordérov. [13])

Páchateľom sa podarilo zariadenia IoT napadnúť tak, že sa do nich hackli. Väčšina zariadení IoT použitých pre Mirai botnet bežala na predvolených povereniach. Po útoku bol online zverejnený zdrojový kód Mirai, ktorý obsahoval predvolené poverenia pre viac ako 60 zariadení. [15])

Tento útok znamenal niekoľko cenných ponaučení o bezpečnosti zariadení IoT:

1. Zariadenia by mali mať vždy možnosť aktualizovať svoj softvér, heslá a firmware. Ak tieto funkcie nie je možné aktualizovať, nemali by sa tieto zariadenia používať, pretože sú príliš náchylné na útoky.
2. Užívateľom by nemalo byť dovolené ponechať si predvolené poverenia.
3. Zariadenia IoT by mali vyžadovať jedinečné heslá pre každé zariadenie.
4. Zariadenia IoT by mali byť vždy aktualizované najnovším softvérom a firmware. [16])

Okrem lekcií o bezpečnosti útok na Dyn ukázal aj potrebu zvýšenej ostražitosti vo vzťahu k zariadeniam IoT. Zariadenia predstavovali nový bod zraniteľnosti pre celý internet.

2.3 Sociálne Inžinierstvo

Phishing je činnosť, pri ktorej sa útočník pokúša získať informácie ako používateľské meno, heslo alebo údaje o kreditnej karte tak, že sa v elektronickej komunikácii predstavuje ako dôveryhodná entita. Phishingové e-maily môžu obsahovať odkazy na webové stránky infikované škodlivým softvérom.

Obrázok 2: Informácie, ktoré útočníci najčastejšie získavajú phishingom
(Zdroj: https://www.esferize.com)

14) WOOLF, N.: *DDoS attack that disrupted internet was largest of its kind in history, experts say*, 2016.
15) LEWIS, D.: *The DDoS Attack Against Dyn One Year Later*, 2017.
16) DUNLAP, T.: *The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History*, 2020.

Phishing je príkladom sociálneho inžinierstva a najčastejšie sa využíva pri hackovaní e-mailov. Pri phishingu cez e-mail hacker pošle používateľovi odkaz napríklad na údaje o banke alebo osobné informácie cez e-mail. Keď používateľ klikne na tento odkaz a vyplní všetky údaje, hacker získa všetky jeho informácie. Phishing v jednotlivých krokoch:

1. útočník pošle e-mail obeti,
2. obeť klikne na e-mail a presmeruje sa na phishingovú webovú stránku,
3. útočník zhromažďuje prihlasovacie údaje obete,
4. útočník použije prihlasovacie údaje obete na prístup k webovej stránke.

Niekedy sa na počítač cieľovej osoby stiahne aj škodlivý softvér.

V oblasti sociálneho inžinierstva môže útok prichádzať rôznymi spôsobmi: cez e-mailovú správu, telefonáty alebo predstieranie dôveryhodnej entity. Telefonát komplikuje overovací proces identity. Z rovnakého dôvodu sa používa e-mail, ktorý tiež zjednodušuje proces predstierania identity. [17])

2.3.1 Návnada

Útočník v tejto forme sociálneho inžinierstva zbiera informácie o záujmoch obete a potom využíva tieto informácie, aby obeť zlákal do pasce, ktorá vedie k odcudzeniu citlivých informácií alebo ohrozeniu počítačov. Návnadový útok sa zakladá na vzbudení zvedavosti a chamtivosti obetí. [18]) Napríklad, ak má obeť záujem o filmy, môže útočník ponúknuť bezplatné sťahovanie filmov, aby obeť zlákal k prezradeniu informácií o sebe. Iný príklad, útočník môže posielať darček obsahujúci flash pamäť so škodlivým malwarom, aby zvýšil zvedavosť obete. Obeť ho otvorí a spustí útok.

2.3.2 Hrozba vytvárania predpokladov (Pretexting)

Útočník v tejto situácii predstiera a vytvára predpoklady na získanie prístupu k obeti, a potom jej ukradne informácie. Najpopulárnejším príkladom pretextingu je, keď zločinecká osoba predstiera, že volá z banky a potrebuje potvrdiť identitu obete. [19]) [20]) Je to umenie, ktorého cieľom je ukradnúť kritické informácie ako sú zdravotné údaje, údaje o platobnej karte, adresa alebo získanie výhod ako sú napríklad peniaze. Útočník obvykle cieli na skupiny ľudí a komunikuje s nimi prostredníctvom mnohých kanálov ako sú e-maily, sociálne médiá, telefonáty a textové správy. [19]) Existuje veľa dôvodov, prečo ľudia môžu byť ľahko zneužití. Je to napríklad nedostatok vedomostí o počítačovej bezpečnosti, vizuálne klamné triky alebo nedostatok záujmu o bezpečnostné indikátory.

Špecifický phishing (spear-phishing) je typ phishingu, pri ktorom útočník cieli na konkrétnu obeť. Keďže tento typ phishingu používa pokročilé metódy, má vyššiu úspešnosť ako tradičný phishing. [19])

Význam vzdelávania a povedomia v oblasti sociálneho inžinierstva je nesmierny. Keďže mnohé útoky sociálneho inžinierstva cielia priamo na ľudský faktor, vedomosti a povedomie zamest-

17) SALAHDINE, F.- KAABOUCH, N.: *Social engineering attacks : A survey*, 2019.
18) PARTHY, P. P. - RAJENDRAN, G.: Identification and prevention..., 2019, s. 89.
19) PARTHY, P. P. - RAJENDRAN, G.: Identification and prevention..., 2019, s. 1-5.
20) HADNAGY, C.: *Social engineering : The art of human hacking*, 2010.

nancov môžu často predstavovať prvú a poslednú obrannú líniu proti týmto hrozbám. Preto je veľmi dôležité neustále sa vzdelávať a trénovať zamestnancov v oblastiach, ako sú:

1. rozpoznávanie pokusov o phishing a iných útokov sociálneho inžinierstva,
2. správne postupy pri nakladaní s citlivými informáciami,
3. postup pri konfrontácii s podozrivou komunikáciou alebo žiadosťou,
4. Dôležitosť zachovávania silných a jedinečných hesiel a pravidelnej zmeny týchto hesiel.

V konečnom dôsledku, keď sú zamestnanci informovaní a vedomí si rizík spojených so sociálnym inžinierstvom, stávajú sa aktívnymi účastníkmi v obrannej stratégii organizácie, čím zvyšujú celkovú bezpečnosť a odolnosť voči útokom.

2.3.3 Obrana proti sociálnemu inžinierstvu

Pre organizáciu je veľmi dôležité mať jasné a presne definované bezpečnostné politiky a protokoly. Tieto pravidlá by mali obsahovať postupy pre príjem, spracovanie a odosielanie citlivých informácií, ako aj pravidlá pre komunikáciu s tretími stranami. Implementáciou týchto pravidiel a protokolov môže organizácia výrazne zredukovať riziko, že jej zamestnanci sa stanú obeťami sociálneho inžinierstva. Pravidelným prehodnocovaním a aktualizáciou týchto politík sa tiež zabezpečí, že organizácia je pripravená na nové hrozby a taktiky, ktoré môžu útočníci využiť.

Niektoré svetové spoločnosti si uvedomujú vážnosť hrozieb sociálneho inžinierstva a investujú do vzdelávania svojich zamestnancov, ako aj zavedenia silných bezpečnostných opatrení. Napríklad Google je známy svojimi rozsiahlymi testami a tréningami, ktoré sú zamerané na ochranu pred phishingovými útokmi. Tieto tréningy často zahŕňajú simulované phishingové útoky na zamestnancov, aby sa overilo, či sú schopní rozpoznať podvodné e-maily a nereagovať na ne. Tiež upozorňujú zamestnancov na najnovšie hrozby a spôsoby ako sa brániť. Vďaka týmto opatreniam dosiahol Google výrazné zníženie úspešnosti phishingových útokov proti svojim zamestnancom.

3 GENERÁLNE PRINCÍPY OBRANY PRED KYBERTERORIZMOM

Generálne princípy obrany pred kyberterorizmom sa zakladajú na prevencii, ktorá je základným kameňom v stratégii ochrany pred kybernetickými hrozbami. Prevencia zahŕňa rôzne opatrenia, ktoré majú za cieľ predchádzať útokom a zabezpečiť digitálne aktíva a informačné systémy. Jedným z dôležitých opatrení je využitie firewalov a bezpečnostných opatrení siete. Firewally slúžia ako prvá línia obrany medzi počítačovými systémami a externými hrozbami z internetu. Sledujú sieťovú premávku a filtrovaním a kontrolovaním pravidiel rozhodujú o pripojení. [21]) Existuje viacero typov firewallov, ktoré zabezpečujú blokovanie neoprávneného prístupu a ochranu sietí a systémov. Ďalším dôležitým opatrením je využitie antivírusových programov. Tieto programy sa zameriavajú na detekciu, karanténu a odstránenie škodlivého softvéru z počítačových systémov. Poskytujú skenovanie systému, funkciu karantény a heuristickú analýzu na zistenie nových hrozieb. Firewally a antivírusové programy tvoria základ kybernetickej bezpečnosti a poskytujú silnú ochranu proti rôznym kybernetickým hrozbám. [22])

21) MITRA, A.: *Digital Security : Cyber Terror and Cyber Security*, 2010.
22) MATEJKA, M.: *Počítačová kriminalita*, 2002.

Okrem týchto opatrení je dôležitá aj pravidelná aktualizácia softvéru. Poskytovatelia softvéru vyhodnocujú svoje produkty, identifikujú ich slabé miesta a vydávajú aktualizácie obsahujúce vylepšenia, opravy chýb a bezpečnostné opravy. Aktualizácie sú nevyhnutné z dôvodu zabezpečenia softvéru pred známymi hrozbami. Rovnako dôležité je aj opravovanie softvéru, ktoré sa vykonáva v prípade identifikácie slabostí. [23]) Automatizované aktualizácie a testovanie pred nasadením zabezpečujú správnu funkčnosť softvéru a minimalizujú riziko útokov. Rýchla reakcia je tiež nevyhnutná pri detekcii a odozve na bezpečnostné hrozby. Systémy detekcie a prevencie (IDS/IPS) monitorujú sieťovú prevádzku a upozorňujú na podozrivé aktivity. Systémy správy informačnej bezpečnosti a udalostí (SIEM) zhromažďujú a analyzujú logovacie dáta z rôznych zdrojov a umožňujú tak identifikáciu potenciálnych hrozieb. Tímy na reakciu na bezpečnostné incidenty sú špecializované skupiny, ktoré majú skúsenosti s riešením kybernetických útokov. Ich úlohou je izolovať postihnuté systémy, analyzovať útok, obnoviť dáta a komunikovať so zainteresovanými stranami. [24])

Pri riešení bezpečnostných incidentov je kľúčové mať pripravený plán reakcie na incidenty, ktorý stanovuje postupy, zodpovednosti a komunikačné kanály. Detekcia a rýchla odozva sú nevyhnutné, aby sa minimalizovalo riziko útokov a škôd spôsobených kybernetickými hrozbami. Forenzná analýza je tiež dôležitá na zistenie príčin incidentov a zabezpečenie, aby sa podobné incidenty neopakovali. Celkovo je dôležité kombinovať rôzne bezpečnostné opatrenia a stratégie pre efektívnu obranu proti kyberterorizmu. Prevencia, využívanie firewallov a antivírusových programov, pravidelné aktualizácie a opravy softvéru sú rozhodujúce pre ochranu digitálnych aktív a informačných systémov. V súčasnom kybernetickom svete je kľúčové mať pripravené opatrenia a tímy na riešenie bezpečnostných incidentov a zabezpečenie vysokého stupňa kybernetickej bezpečnosti. [25])

Monitorovacie systémy sú neoddeliteľnou súčasťou kybernetickej obrany organizácií. Poskytujú prehľad o aktuálnom stave, aktivite a bezpečnosti IT prostredia. Existujú rôzne typy monitorovacích systémov vrátane sieťového monitorovania a SIEM systémov. Sieťové monitorovanie sa zaoberá sledovaním komunikácie v sieti, zatiaľ čo SIEM systémy zhromažďujú a analyzujú logovacie dáta na detekciu potenciálnych hrozieb v reálnom čase. Ochrana organizácie zahŕňa nielen monitorovanie siete, ale aj aplikácií, databáz, koncových zariadení a fyzických aktív. Používanie technológií ako sú kamerové systémy a biometrika pomáhajú zabezpečiť fyzickú ochranu aktív. Incident Response tímy sú nesmierne dôležité pre koordinovanú reakciu na bezpečnostné incidenty. Ich úlohou je identifikovať, izolovať, analyzovať, opraviť a komunikovať o incidentoch. Prítomnosť takýchto tímov pozitívne ovplyvňuje dôveru zákazníkov a partnerov v organizácii, pretože ukazuje, že organizácia je pripravená čeliť a riešiť bezpečnostné problémy. [26])

Pre účinnú ochranu aktív a zabezpečenie dôveryhodnosti organizácie je nevyhnutné kombinovať proaktívnu prevenciu, rýchlu detekciu a efektívnu odozvu. Je dôležité si uvedomiť, že najzraniteľnejším článkom v obrannom reťazci organizácie je ľudský faktor. Preto je školenie a vzdelávanie zamestnancov a partnerov nevyhnutnou súčasťou kybernetickej obrany. Moderné technologické riešenia sú síce kritické pre detekciu a ochranu pred hrozbami, ale často to sú ľudské chyby alebo nedbanlivosť, ktoré umožňujú vniknutie hrozieb. Preto je dôležité zvyšovať povedomie o rôznych

23) ABEYWARDANA, K. - PLUEGEL, E. - TUNNICLIFFE, M.: A layered defense mechanism..., 2016.
24) ABRAMOV, M. - AZAROV, A.: Social engineering attack modeling..., 2016.
25) SOKOL, P. - BAČO, L. - BAJTOŠ, T.: *Digitálna forenzná analýza I.,* 2020.
26) *Use of information technology: Masaryk University Directive No. 10/2017*, 2017.

hrozbách a naučiť zamestnancov bezpečnostné postupy. Kľúčové komponenty účinného školenia v oblasti kybernetickej bezpečnosti zahŕňajú povedomie o rôznych hrozbách, bezpečnostné postupy, simulácie a testovanie a pravidelnú aktualizáciu vzdelávacích materiálov. Je dôležité, aby zamestnanci mali vedomosti ako rozpoznávať a minimalizovať riziká spojené s phishingom, ransomwarom a sociálnym inžinierstvom. Praktické cvičenia a simulované útoky pomáhajú zamestnancom získať skúsenosti s reakciou na hrozby v reálnom prostredí. Aby bolo vzdelávanie účinné, materiály by mali byť pravidelne aktualizované, aby reflektovali nové hrozby.

Ľudský faktor je dôležitý nielen pri kybernetickej bezpečnosti, ale aj pri fyzickej bezpečnosti. Aj keď technologické riešenia chránia informačné systémy, zločinné aktivity sú často smerované na jednotlivcov. Ľudské správanie je rôznorodé a ovplyvnené rôznymi faktormi, preto je nevyhnutné investovať do vzdelávania a školenia ľudí v oblasti kybernetickej bezpečnosti. Keď sú ľudia oboznámení s rizikami a odolnými postupmi, stávajú sa dôležitou súčasťou obranného reťazca organizácie. Okrem digitálnej bezpečnosti je potrebné venovať pozornosť aj fyzickej bezpečnosti. Táto oblasť zabezpečuje ochranu infraštruktúry a kritických aktív pred fyzickými hrozbami a prírodnými katastrofami. Ochrana dátových centier, prístupových bodov a pracovných staníc sú dôležité aspekty fyzickej bezpečnosti. Integrácia fyzickej bezpečnosti s kybernetickým zabezpečením je kľúčová pre komplexný prístup k ochrane informačných aktív. [27])

Celkovo je dôležité kombinovať technologické riešenia s vzdelávaním ľudí pre vytvorenie efektívnej kybernetickej obrannej stratégie. Vzdelávanie zamestnancov a partnerov, povedomie o hrozbách a zlepšovanie bezpečnostných postupov sú kľúčové pre ochranu organizácie pred kybernetickými hrozbami. Fyzická bezpečnosť je neoddeliteľnou súčasťou kybernetickej bezpečnosti a vyžaduje investície a implementáciu opatrení. Je dôležité uvedomiť si, že ľudský faktor je kľúčový pri ochrane pred hrozbami a že technologické riešenia sú len časťou celého obranného reťazca.

4 PRÍKLADY PRÍPADOVÝCH ŠTÚDIÍ ÚSPEŠNEJ OBRANY

4.1 Operácia Aurora a obrana Google

V druhej dekáde 21. storočia sa kybernetická bezpečnosť stala kritickou oblasťou záujmu pre korporácie na celom svete. Jedným z najvýznamnejších príkladov kybernetickej špionáže, ktorý zdôrazňoval túto skutočnosť, bola operácia Aurora, ktorá sa odohrala koncom roka 2009. Cieľom tejto masívnej kampane bol celý rad prominentných technologických spoločností vrátane spoločnosti Google. Útočníci sa zameriavali na získanie prístupu k cenným informáciám, najmä k intelektuálnemu vlastníctvu a osobným údajom. Google, ako jeden z hlavných cieľov tohto útoku, začal okamžite analyzovať neoprávnený zásah do svojich systémov. Rýchle a dôkladné forenzné vyšetrovanie umožnilo spoločnosti identifikovať a porozumieť technikám a nástrojom, ktoré útočníci použili, čo bolo zásadné v boji proti invázii a pri náprave kompromitovaných systémov. [28])

Spoločnosť Google následne aktivovala svoj interný bezpečnostný tím a vytvorila multidisciplinárnu stratégiu na riešenie hrozby. Táto stratégia zahrnovala nielen technické riešenia, ako izoláciu kompromitovaných systémov a odstraňovanie malvérov, ale aj spoluprácu s externými bezpečnostnými spoločnosťami a úradmi na zdieľanie informácií a spoločné úsilie na zastavenie útoku. Rovnako dôležitá bola aj komunikácia spoločnosti s verejnosťou a ostatnými napadnutý-

27) *Global Terrorism Index 2019 : Measuring The Impact Of Terrorism*, 2019.
28) ADHIKARI, R.*: In Google Attack Aftermath, Operation Aurora Keeps On Hacking*, 2012.

mi organizáciami. Transparentnosť Google v tomto období bola významná, pretože informovala ostatné spoločnosti o existujúcich hrozbách a pomáhala vytvárať širšiu spoluprácu v boji proti kybernetickým hrozbám. [29])

Operácia Aurora predstavuje názorný príklad toho, ako možno úspešne čeliť aj dokonca veľmi dobre financovanému a sofistikovanému útoku. Reakcia Google na túto hrozbu zdôrazňuje význam rýchlej detekcie, efektívnej odozvy a transparentnosti vo vzťahu k verejnosti a partnerom počas kybernetického útoku.

4.2 Estónska obrana po kybernetickom útoku v roku 2007

Estónsko sa v roku 2007 stalo cieľom jedného z najväčších a najznámejších kybernetických útokov v histórii, ktorý sa často označuje ako prvý „kybernetický vojnový útok". Útok bol vykonaný formou DDoS a postihol vládne siete, banky, médiá a ďalšie kľúčové infraštruktúry krajiny. Táto kybernetická ofenzíva prišla v čase národného napätia, kedy Estónsko presúvalo sovietsky vojenský pamätník z centra Talinu, čo vyvolalo silné reakcie zo strany Ruska. V dôsledku týchto útokov musela estónska vláda podniknúť rýchle a rozhodné kroky ako reakciu na túto krízu:

1. Izolácia: Estónsko dočasne izolovalo niektoré zo svojich národných webových serverov od medzinárodného internetu, aby obmedzilo dosah útokov a zabezpečilo kontinuitu kritických služieb.
2. Mobilizácia expertov: Estónsko mobilizovalo svojich domácich IT odborníkov a bezpečnostné tímy, aby analyzovali útoky, identifikovali zraniteľné body a implementovali obranné stratégie.
3. Medzinárodná spolupráca: krajina požiadala o pomoc a spoluprácu svojich medzinárodných partnerov vrátane členských štátov NATO, aby im pomohli riešiť situáciu a poskytli expertízu v oblasti kybernetickej obrany. [30])

Estónsko po skončení útokov a stabilizácii situácie uznalo potrebu posilniť svoju kybernetickú obranu na trvalom základe. Krajina investovala do vývoja pokročilých kybernetických obranných kapacít a založila Estónske centrum kybernetickej obrany pri Technickej univerzite v Taline. Okrem toho, v roku 2008 bola v Taline založená NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), čo Estónsku poskytlo príležitosť stať sa svetovým lídrom v oblasti kybernetickej obrany.

5 BUDÚCNOSŤ KYBERTERORIZMU A OBRANA VOČI NEMU

V budúcnosti sú očakávané výrazné zmeny v oblasti kyberterorizmu a obrany proti nemu. Technologický vývoj a nové stratégie obrany budú zohrávať kľúčovú úlohu v boji proti kybernetickým hrozbám. Jedným z možných riešení je kvantová kryptografia, ktorá využíva kvantovú mechaniku na vytváranie spojení, ktoré by boli v teórii nemožné dešifrovať bez odhalenia útočníka. Toto by poskytlo vysokú mieru ochrany voči kybernetickým útokom, ktoré sa sústreďujú na tradičné kryptografické metódy. Ďalším dôležitým faktorom je integrácia umelej inteligencie. [31]) Obranné technológie budú stále viac využívať umelú inteligenciu na identifikáciu a riešenie hrozieb v reálnom čase. S pomocou predchádzajúcich útokov sa tieto technológie budú učiť a prispôsobovať novým stratégiám útočníkov.

29) CUTLER, T.: *The Anatomy of an Advanced Persistent Threat*, 2010.
30) SCHMIDT, A.: *The Estonian Cyberattacks*, 2013.
31) MANJOO, F.: *The case of the missing code...,* 2002.

Zero Trust architektúry sú založené na predpoklade, že v žiadnej sieti nie je žiadne zariadenie, ani používateľ vopred dôveryhodný. Každý prístup musí byť overený a monitorovaný, aby sa minimalizovalo riziko neoprávnenej prítomnosti. Decentralizované siete a technológie ako blockchain môžu tiež prispieť k lepšiemu zabezpečeniu údajov. [32]) Tieto technológie poskytujú nové spôsoby overovania a zabezpečenia, pričom útočníci by museli namiesto jedného centra kompromitovať viacero uzlov v sieti. Biometria a multifaktorová autentifikácia majú potenciál poskytnúť silnejšiu ochranu ako tradičné metódy autentifikácie pomocou hesiel. Napríklad rozpoznávanie tváre alebo odtlačkov prstov môže pridať dodatočnú úroveň bezpečnosti. [33])

Budúcnosť obrany proti kybernetickým hrozbám bude založená na kontinuálnom monitorovaní a adaptácii. Statické riešenia sa budú nahradzovať dynamickými stratégiami, ktoré umožnia rýchlu reakciu na nové hrozby a meniace sa techniky útokov. Nové technológie však prinášajú aj nové hrozby a výzvy. S nástupom kvantových počítačov budú tradičné metódy šifrovania ohrozené. Zneužívanie umelej inteligencie, autonómne zariadenia, rozšírenie IoT, deepfakes a biotechnologické útoky sú ďalšími potenciálnymi hrozbami, ktoré budeme musieť zvládnuť.

Je dôležité, aby spoločnosti, vlády a jednotlivci rýchlo reagovali na tieto nové hrozby a prispôsobili svoje bezpečnostné protokoly. Prevencia a príprava sú kľúčovými opatreniami na úspešnú obranu proti kyberterorizmu. Konštantné hodnotenie a posilňovanie bezpečnosti budú nevyhnutné, aby sme si udržali krok s rýchlo meniacimi sa technologickými krajinami.

6 ZÁVER

Kybernetický priestor sa stal integrovanou súčasťou našej každodennej existencie. Prináša so sebou nielen nové príležitosti, ale aj značné riziká. Predstava, že informačné systémy môžu byť kompromitované, manipulované alebo úplne zničené kyberteroristickými činmi, je alarmujúca. Význam kyberbezpečnosti sa zvyšuje v kontexte globalizovanej ekonomiky, kde kybernetické útoky môžu mať hlboký vplyv nielen na digitálne prostredie, ale aj na fyzický svet. Príklady rozsiahlych porúch služieb, ekonomických strát alebo kompromitácie citlivých údajov sú čoraz častejšie a ukazujú na krehkosť našich systémov.

V snahe čeliť tejto hrozbe je nevyhnutné investovať do robustných a flexibilných obranných riešení. Je potrebné zvyšovať povedomie o rizikách a neustále zlepšovať naše schopnosti detekcie a reakcie na kybernetické hrozby. Týmto spôsobom môžeme minimalizovať potenciálne škody a zabezpečiť, aby technológie, ktoré si tak veľmi ceníme, zostali bezpečné a dôveryhodné. Na konci dňa je dôležité uvedomiť si, že kyberterorizmus nie je len technologický problém, ale aj sociálny, politický a ekonomický. Je to výzva, ktorej čeliť si vyžaduje koordinovanú a integrovanú reakciu na globálnej úrovni. Technologický pokrok môže priniesť nové nástroje a stratégie na obranu, ale musíme si byť vedomí hlavnej zásady – v oblasti kyberbezpečnosti je kľúčová neustála bdelosť.

Článok sa zaoberá definíciou kyberterorizmu, kybernetickými útokmi, prevenciou a ochranou voči nim. Uvedomujeme si, že v boji proti kyberterorizmu ide o neustály zápas medzi útočníkmi a obhajcami, pričom obidve strany sa neustále vyvíjajú a adaptujú. Dôležité je, aby spoločnosti, vlády a jednotlivci boli vždy o krok dopredu v oblasti kyberbezpečnosti. To zahŕňa neustále vzdelávanie a školenie zamestnancov, investície do najnovších bezpečnostných technológií a nástrojov, ako aj aktívnu spoluprácu na medzinárodnej úrovni na zdieľanie informácií a najlepších

32) *Never forget your PIN again : Mastercard creates credit card with fingerprint scanner*, 2017.
33) ŠČUREK, R.: *Biometrické metody identifikace osob v bezpečnostní praxi*, 2008.

postupov. Rovnako dôležité je chápať, že v kontexte kybernetickej bezpečnosti je kolaborácia nevyhnutná. [34]) V súčasnej globálnej kybernetickej krajine je tímovo vypracovaná stratégia tou najlepšou obranou. To znamená budovanie mostov medzi sektorom verejnej a súkromnej sféry, medzi technológmi a politikmi a dokonca aj medzi národmi. Spolupráca a zdieľanie informácií môžu výrazne zvýšiť efektívnosť našich obranných opatrení.

Zatiaľ čo sa technológie neustále vyvíjajú a menia, základné ľudské hodnoty ako sú dôvera, integrita a spolupráca zostávajú konštantné. Budúcnosť kybernetickej bezpečnosti tak závisí nielen od technologických inovácií, ale aj od spôsobu, akým sa ako spoločnosť rozhodneme tieto hodnoty uplatňovať v kontexte ochrany digitálnej budúcnosti.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

ABEYWARDANA, K. - PFLUEGEL, E. - TUNNICLIFFE, M.: A layered defense mechanism for a social engineering aware perimeter. In: *Proceedings of the SAI Computing Conference, London, UK, 13–15 July 2016,* s. 1054-1062. ISBN 978-1-4673-8460-5.

ABRAMOV, M. - AZAROV, A.: Social engineering attack modeling with the use of Bayesian networks. In: *Proceedings of the XIX International Conference on Soft Computing and Measurements, St. Petersburg, Russia, 25–27 May 2016*, s. 58-60. ISBN 978-1-4673-8919-8.

ADHIKARI, R.: *In Google Attack Aftermath, Operation Aurora Keeps On Hacking* [online]. TechNewsWorld, 2012 [cit. 2023-08-12]. Dostupné na internete: <http://www.technewsworld.com/story/76109.html>.

BAILEY, M.: *Complete Guide to Internet Privacy, Anonymity & Security*. 2. vyd. Lexington : A Nerel Publication, 2015, 260 s. ISBN 9783950309348.

Communication from the Commision to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Fighting Spam, Spyware and Malicious Software : COM (2006) 688 final. Brussels : Commision of the European Communities, 2006. 12 s.

CUTLER, T.: *The Anatomy of an Advanced Persistent Threat* [online]. Security Week, 2010 [cit. 2023-08-12]. Dostupné na internete: <http://www.securityweek.com/anatomy-advanced-persistent-threat>.

DUNLAP, T.: *The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History* [online]. IoT for all, 2020 [cit. 2023-08-09]. Dostupné na internete:<https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/>.

Global Terrorism Index 2019 : Measuring The Impact Of Terrorism [online]. Relief Web, 2019 [cit. 2023-08-12]. Dostupné na internete: <https://reliefweb.int/report/world/global-terrorism-index-2019>.

GREENE, T.: *How the Dyn DDoS attack unfolded* [online]. Network World, 2016 [cit. 2023-08-09]. Dostupné na internete: <https://www.networkworld.com/article/3134057/security/how-the-dyn-ddos-attack-unfolded.html>.

HADNAGY, Ch.: *Social engineering : The art of human hacking*. New Jersey : John Wiley & Sons, 2010. 416 s. ISBN 978-0-470-63953-5.

Internet Security Threats [online]. Kaspersky Lab, 2015 [cit. 2023-08-20]. Dostupné na internete: <http://www.kaspersky.com/internet-security-center/threats/all-articles>.

34) SVRČEK, M.: Kriminologické aspekty obetí počítačovej kriminality, 2015.

IVANČÍK, R. - BARIČIČOVÁ, Ľ.: Kybernetické hrozby ako súčasť asymetrických bezpečnostných hrozieb v 21. storočí. In: *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek)*. Bratislava : Akadémia policajného zboru, 2019, s. 35-47. ISBN 978-80-8054-819-3.

LEWIS, D.: *The DDoS Attack Against Dyn One Year Later* [online]. Forbes, 2017 [cit. 2023-08-09]. Dostupné na internete: <https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack--against-dyn-one-year-later/#47df91f41ae9>.

MANJOO, F.: *The case of the missing code : Are al-Qaida terrorists hiding their secrets in eBay photographs?* [online]. Salon, 2002 [cit. 2023-08-12]. Dostupné na internete:<http://goo.gl/xMWh63>.

MATEJKA, M.: *Počítačová kriminalita*. Praha : Computerpress, 2002. 120 s. ISBN 80-7226-419-2.

MITRA, A.: *Digital Security : Cyber Terror and Cyber Security*. 1vyd. New York : Fact on File, Incorporated, 2010. 120 s. ISBN 9780816067916.

Never forget your PIN again : Mastercard creates credit card with fingerprint scanner [online]. The Telegraph, 2017 [cit. 2023-08-12]. Dostupné na internete: <http://www.telegraph.co.uk/technology/2017/04/20/mastercard-creates-credit card-fingerprint-scanner>.

PARTHY, P. P. - RAJENDRAN, G.: Identification and prevention of social engineering attacks on an enterprise [online]. In: *The IEEE 53rd International Carnahan Conference on Security Technology (ICCST), October 1-3, 2019, Anna University, Chenai, India*. IEEE, 2019 [cit. 2023-08-09]. Dostupné na internete: <https://sci-hub.se/10.1109/ccst.2019.8888441>.

PETROWSKI, T.: *Bezpečí na internetu pro všechny*. 1. vyd. Liberec : Dialog, 2014, 243 s. ISBN 978-80-7424-066-9.

PŘIBYL, T.: *Kyberterorizmus* [online]. [cit. 2023-08-03]. Dostupné na internete: <https://www.virusy.sk/clanok.itc?ID=402.html>

Ransomvér CryptoWall 3.0 zarobil stovky miliónov : Jedinej skupine. [online]. Zive.sk, 2015 [cit. 2023-08-20]. Dostupné na internete: <https://www.zive.sk/clanok/109653/ransomver-cryptowall-3-0--zarobil-stovky-milionov-jedinej-skupine>.

ROSSOW, Ch.: *Amplification Hell : Revisiting Network Protocols for DDoS Abuse* [online]. NDSS, 2014 [cit. 2023-08-09]. Dostupné na internete: <https://www.ndss-symposium.org/ndss2014/programme/amplification-hell-revisiting-network-protocols-ddos-abuse/>.

SALAHDINE, F. – KAABOUCH, N.: *Social engineering attacks : A survey* [online]. Future Internet, 2019 [cit. 2023-08-09]. Dostupné na internete: <https://www.researchgate.net/publication/332151597_Social_Engineering_Attacks_A_Survey/link/5ca4c0dda6fdcc12ee8fceca/download>.

SCHMIDT, A.: *The Estonian Cyberattacks* [online]. Atlantic Council, 2013 [cit. 2023-08-12]. Dostupné na internete: <https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks>.

SOKOL, P. - BAČO, L. - BAJTOŠ, T.: *Digitálna forenzná analýza I.* [online]. Košice : UPJŠ, 2020. 99 s. [cit. 2023-08-12]. Dostupné na internete: <https://unibook.upjs.sk/img/cms/2020/pf/digitalna-forenzna-analyza-1.pdf>.

SRINIVASAN, S. - DEEPALAKSHMI, P.: *Enhancing the security in cyber-world by detecting the botnets using ensemble classification based machine learning* [online]. Science Direct, 2023 [cit. 2023-08-09]. Dostupné na internete: <https://www.sciencedirect.com/science/article/pii/S2665917422002586>.

SVRČEK, M.: Kriminologické aspekty obetí počítačovej kriminality [online]. In: *Obete kriminality a ich práva*. 1 vyd. Žilina : Spoločnosť pre trestné právo a kriminológiu, 2015, s. 119-130 [cit. 2023-08-12]. ISBN 978-80-971911-0-8. Dostupné na internete:<http://www.paneurouni.com/wp-content/uploads/2017/03/obete-kriminality-ich-prava-zbornik-zo-seminara-medzinarodnou-ucastou-6-november-2014-1.pdf#page=119>.

SZOR, P.: *Počítačové viry : analýza útoku a obrana*. Brno : Zoner Press, 2006, 608 s. ISBN 80-86815-04-8.

ŠČUREK, R.: *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. VŠB TU Ostrava, 2008 [cit. 2023-08-12]. Dostupné na internete: <http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf>.

TRIPATHI, N. - MEHTRE, B. M.: *DoS and DDoS Attacks : Impact, Analysis and Countermeasures* [online]. Research Gate, 2013 [cit. 2023-08-20]. Dostupné na internete: <https://www.researchgate.net/publication/259941506_DoS_and_DDoS_Attacks_Impact_Analysis_and_Countermeasures>.

Types of Malware [online]. Kaspersky lab, 2012 [cit. 2016-05-14]. Dostupné na internete: <http://www.kaspersky.com/internet-security-center/threats/malware-classifications>.

Use of information technology : Masaryk University Directive No. 10/2017 [online]. MUNI, 2017 [cit. 2023-08-12]. Dostupné na internete: <https://is.muni.cz/do/mu/Uredni_deska/Predpisy_MU/Masarykova_univerzita/Smernice_MU/SM10-17/102278820/MU_Directive_No._10_2017_-_Use_of_Information_Technology.pdf>.

WOOLF, N.: *DDoS attack that disrupted internet was largest of its kind in history, experts say* [online]. The Guardian, 2016 [cit. 2023-08-09]. Dostupné na internete: <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>.

TÉMY NA VEDENIE ZÁVEREČNEJ DISKUSIE

1. Spolupráca medzi verejným a súkromným sektorom: Ako môže spolupráca medzi verejným a súkromným sektorom efektívne čeliť kyberterorizmu? Aké sú hlavné prekážky tejto kolaborácie a ako sa dajú prekonať?
2. Prípadové štúdie: Ktoré konkrétne prípady úspešnej alebo neúspešnej obrany proti kyberterorizmu by mohli slúžiť ako hodnotné lekcie pre budúce stratégie a taktiky? Je možné z týchto prípadov vyvodzovať obecné zásady efektívnej obrany?
3. Budúcnosť kybernetickej bezpečnosti: Aké sú predpoklady a scenáre pre budúci vývoj kyberterorizmu a kybernetickej obrany? Ako sa budú musieť meniť stratégie obrany, aby efektívne čelili budúcim hrozbám?
4. Význam ľudského faktora: Ako môže vzdelávanie a školenie v oblasti kybernetickej bezpečnosti zvýšiť odolnosť proti kyberteroristickým útokom? Aké sú najlepšie prístupy k zvýšeniu povedomia a pripravenosti na individuálnej a organizačnej úrovni?
5. Technologické inovácie ako dvojsečná zbraň: Ako môžu byť nové technológie, napríklad umelá inteligencia a internet vecí, využité na zlepšenie obrany, ale zároveň predstavovať aj nové hrozby? Ako je možné vyvážiť výhody a riziká týchto inovácií?