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

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.

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