KYBERNETICKÉ ÚTOKY AKO SÚČASŤ INFORMAČNÝCH OPERÁCIÍ POČAS HYBRIDNEJ VOJNY

CYBER ATTACKS AS A PART OF INFORMATION OPERATIONS DURING THE HYBRID WARFARE

plk. gšt. v. z. doc. Ing. Radoslav IVANČÍK, PhD. et PhD., MBA, MSc.
Akadémia Policajného zboru v Bratislave, Katedra informatiky a manažmentu,
Sklabinská 1, 835 17 Bratislava, Slovenská republika
radoslav.ivancik@akademiapz.sk

Abstract: Cyber-attacks are a modern way of waging war, in which there is no direct clashes between military units on the battlefield or large human losses caused by destructive firepower. Their goal is to disrupt the information and communication infrastructure of the state, the functioning of state institutions, state administration and self-government bodies, disrupt the economy, destabilize society, demoralize citizens, and generally weaken the influence and power of the enemy. This is one of the reasons why the author deals with cyber-attacks, their types and methods of execution as an important part of information operations conducted within the broader concept of hybrid war, using relevant methods of interdisciplinary scientific research.

Keywords: cyber-attacks, information operations, hybrid warfare.

Abstrakt: Kybernetické útoky predstavujú moderný spôsob vedenia vojny, pri ktorom nedochádza pri nich k priamym stretom vojenských jednotiek na bojovom poli ani k veľkým ľudským stratám spôsobených ničivou palebnou silou. Ich cieľom je narúšať informačnú a komunikačnú infraštruktúru štátu, fungovanie štátnych inštitúcií, orgánov štátnej správy a samosprávy, znefunkčniť ekonomiku, destabilizovať spoločnosť, demoralizovať občanov a celkovo oslabiť vplyv a silu protivníka. Aj preto sa autor v práci s využitím relevantných metód interdisciplinárneho vedeckého výskumu zaoberá kybernetickými útokmi, ich typmi a spôsobmi vykonávania ako dôležitou súčasťou informačných operácií vedených v rámci širšieho konceptu hybridnej vojny.

Kľúčové slová: kybernetické útoky, informačné operácie, hybridná vojna.

ÚVOD

V 21. storočí, vzhľadom na aktuálny vývoj ľudskej spoločnosti a postupne stále väčšiu previazanosť a prepojenosť jednotlivých štátnych i neštátnych aktérov pod vplyvom prehlbujúcej sa globalizácie, ozbrojené konflikty už nepredstavujú ani hlavný nástroj ani

skutočný spôsob riešenia problémov medzi štátmi. Na ich miesto prichádza nový typ konfrontácie – hybridná vojna, ktorej podstata spočíva v tom, že znepriatelené strany neutrpia obrovské ľudské straty v priamom ozbrojenom boji na vojnovom poli a hlavné škody nespôsobí vojenská technika a ničivé zbrane, ale informačná zložka nepriateľského štátu. Predmetom útokov nie sú vojenské jednotky, ale informačné infraštruktúry protivníka, pomocou ktorých je jeho obyvateľstvo dezinformované, verejná mienka ovplyvnená, ekonomika krajiny narušená a funkčnosť štátnej správy a samosprávy obmedzená. Súčasné vojny sa preto už len výnimočne vedú na skutočných bojiskách. Dnes prevažujú tie, ktoré sa vedú informačnom poli a v kybernetickom priestore a víťazstvo získava ten aktér, ktorého kybernetické útoky sú efektívnejšie a účinnejšie, a ten, kto dokáže svoju informačnú infraštruktúru, predovšetkým kritickú informačnú infraštruktúru, brániť a chrániť lepšie ako protivník. Aj preto sa autor, využijúc relevantné metódy interdisciplinárneho vedeckého výskumu (najmä analyticko-syntetickú metódu, obsahovú a kvalitatívnu analýzu, analýzu štúdia dokumentov a pod.) v nadväznosti na predchádzajúce vlastné práce[1] a práce renomovaných zahraničných i domácich autorov zaoberajúcich sa problematikou kybernetickej bezpečnosti a hybridnej vojny (Glenna[2], Hoffmana[3], Van Haastera[4], Sigholma[5], Singera a Friedmana[6], Hromadu[7], Jurčáka[8], Gregu[9], Valucha[10] a ďalších[11]), zaoberá v tomto článku problematikou kybernetických útokov ako súčasťou informačných operácií vedených počas hybridnej vojny.

---

1 IVANČÍK, R. 2016. Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia. In Medzinárodné vzťahy, 2016, roč. 14, č. 2, s. 130-156; IVANČÍK, R. 2020. Analýza prístupov k definovaniu a vymedzeniu hybridnej vojny. In Národná a medzinárodná bezpečnosť 2020 : zborník príspevkov z 11. medzinárodnej vedeckej konferencie. Liptovský Mikuláš : Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2020. s. 174-184.

2 GLENN, R. W. 2009. Thoughts on Hybrid Conflict. In *Small Wars Journal*, 2009.

3 HOFFMAN, F. G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. In *Potomac Institute for Policy Studies*, 2007.

4 Van HAASTER, J. *On cyber: the utility of military cyber operations during armed conflict*. Amsterdam : University of Amsterdam, 2019

5 SIGHOLM, J. Non-State Actors in Cyberspace Operations. In Journal of Military Studies, 2016, roč. 4, č. 1

6 SINGER, P. W. – FRIEDMAN, A. Cybersecurity and Cyberwar (What Everyone Needs to Know®). Oxford : Oxford University Press, 2014

7 HROMADA, M. Kybernetická bezpečnosť. In Lukáš, L. a kol.: *Teória bezpečnosti I*. Zlín : Radim Bačuvčík – VeRBuM, 2017, s. 123-133; VALOUCH, J. – HROMADA, M. 2016. *Bezpečnostní futurologie*. Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2016

8 JURČÁK, V. - TURAC, J. 2018. Hybridné vojny – výzva pre NATO. In Bezpečnostné fórum 2018 : zborník vedeckých prác. Banská Bystrica : Interpolis, 2018. s. 177-184; JURČÁK, V. - SASARÁK, J. 2016. Hybridné hrozby – výzva pre Európsku úniu. In Medzinárodné vzťahy 2016 : aktuálne otázky svetovej ekonomiky a politiky. Bratislava : Vydavateľstvo Ekonóm, 2016, s. 542-550.

9 GREGA, M. – ŽENTEK, M. – NEČAS, P. Security Threats Versus New Areas and Approaches of the Cyber Synthetic Environment. In Fabián, K. - Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in cyberspace*. Krakow : Apeiron University of Public and Individual Security in Kraków, 2020, s. 172-229

10 VALUCH, J. *Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti*. Bratislava: Wolters Kluwer, 2019

11 Bližšie pozri napríklad: ZACHARIDESOVÁ, N. 2021. Moderné spôsoby vedenia vojny. In *Aktuálne bezpečnostné výzvy a medzinárodné právo - zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2021, s. 54-67; HAJDUKOVÁ, S. 2021. Konflikty v šedej zóne a hybridná vojna. In *Aktuálne bezpečnostné výzvy a medzinárodné právo - zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2021, s. 68-82; LUKÁČOVÁ, V. 2020. Hybridné hrozby v kybernetickom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava :

HYBRIDNÉ HROZBY A HYBRIDNÁ VOJNA

Termíny hybridné hrozby a hybridná vojna sú predmetom viacerých publikácií, štúdií alebo článkov, v ktorých sa jednotliví autori[12] zaoberajú hybridnými hrozbami či hybridnou vojnou všeobecne alebo sa zameriavajú vo svojom výskume na ich jednotlivé aspekty. Z toho dôvodu je možné stretnúť sa s ich viacerými definíciami. Jedna z nich hovorí, že *„pojem hybridná hrozba sa vzťahuje na činnosť vykonávanú štátnymi alebo neštátnymi aktérmi, ktorej účelom je podkopať alebo poškodiť cieľ kombináciou otvorených a skrytých vojenských a nevojenských prostriedkov“*.[13]

Glenn definuje hybridné hrozby ako *„nepriateľa, ktorý súčasne a adaptabilne používa rôzne kombinácie politických, ekonomických, sociálnych a informačných prostriedkov a zároveň konvenčné, nepravidelné, katastrofické, teroristické a rozvratné kriminálne metódy vedenia boja“*.[14] Podľa Hoffmana *„hybridné hrozby zahŕňajú celú škálu konvenčných i nekonvenčných spôsobov boja a neregulárnej taktiky, ako aj kriminálne a teroristické činy, ktoré zahŕňajú neobmedzené násilie, nátlak, spoločenské nepokoje a rozvrat“*.[15]

Pod pojmom hybridná vojna možno chápať *„široké spektrum nepriateľských aktivít, v ktorých úloha vojenského komponentu je skôr malá, pretože politický, informačný, ekonomický a psychologický vplyv sa stáva hlavným prostriedkom vedenia boja. Takéto metódy pomáhajú dosiahnuť významné výsledky: teritoriálne, politické a ekonomické straty nepriateľa, chaos a rozvrat systému výkonu štátnej moci a oslabenie morálky spoločnosti“*.[16] Hybridnú vojnu možno tiež chápať ako *„súbor letálnych a neletálnych prostriedkov, ktoré štátny alebo neštátny aktér využíva k presadeniu svojich záujmov proti vôli iného aktéra. Hybridná vojna pritom kombinuje hneď niekoľko spôsobov vedenia boja: klasické vojenské operácie, operácie v kybernetickom priestore alebo kybernetické útoky, špionáž, šírenie nepravdivých informácií s cieľom pôsobiť na verejnú mienku nepriateľa a pod.“*.[17]

Akadémia Policajného zboru, 2020, s. 102-105; 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; JIRÁSKOVÁ, S. 2019. Ekonomická vojna ako jedna z podôb hybridnej vojny. In *Národná a medzinárodná bezpečnosť 2019 – zborník príspevkov z 10. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála Milana Rastislava Štefánika, s. 205-213

[12] Bližšie pozri napríklad: VOERZIO, M. 2021. *Hybrid War: Attack on the West*. Garden City : Babelcube, 2021; DVORAK, J. 2016. *Complexity in Modern War: Examining Hybrid War*. Springfield : Missouri State University, 2016; GRISCIOLI, G. 2016. *Intelligence. The Hybrid War*. Roma : Aracne, 2016; MILLER, M. 2015. *Hybrid Warfare: Preparing for Future Conflict*. Montgomery : Air War College, 2015; alebo MURRAY, W. - MANSOOR, P. R. 2012. *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge : Cambridge University Press, 2012

[13] Hybrid CoE. 2022. Hybrid Threats. In *Hybrid Centre of Excellence*, 2022

[14] GLENN, R. W. 2009. *Thoughts on Hybrid Conflict*. In *Small Wars Journal*, 2009

[15] HOFFMAN, F. G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. In *Potomac Institute for Policy Studies*, 2007.

[16] MANKO, O. - MIKHIEIEV, Y. 2018. Defining the Concept of 'Hybrid Warfare' Based on Analysis of Russian Agression against Ukraine. In *Connections*, 2018, s. 13

[17] DANYK, Y. – MALIARCHUK, T. – BRIGGS, C. 2017. Hybrid War: High-tech, Information and Cyber Conflicts. In *Connections*, 2017

Ďalšia z definícií hovorí, že *„hybridná vojna je ozbrojený konflikt vedený kombináciou nevojenských a vojenských prostriedkov s cieľom ich synergickým efektom prinútiť protivníka k vykonaniu takých krokov, ktoré by sám o sebe nevykonal. Aspoň jednou stranou konfliktu je štát. Hlavnú úlohu pri dosiahnutí cieľov vojny hrajú nevojenské prostriedky v podobe informačných a psychologických operácií, propagandy, ekonomických sankcií, embárg, kriminálnych aktivít, teroristických aktivít a iných subverzívnych aktivít podobného charakteru, ktoré sú vedené proti celej spoločnosti, najmä proti jej politickým štruktúram, orgánom štátnej správy a samosprávy, ekonomike štátu, morálke obyvateľstva a ozbrojeným silám“*.[18]

Jedným zo zámerov hybridnej vojny je ovládnuť informačné prostredie nepriateľa a na dosiahnutie tohto cieľa sa realizujú rôzne informačné operácie, ktorých cieľom sú médiá, informačné a počítačové systémy a strategicky významné sektory života spoločnosti. Okrem informačného prostredia hybridná vojna všetkými dostupnými prostriedkami ovplyvňuje ekonomický a politický život nepriateľského štátu, čím sa dosahuje kontrola nad masovým vedomím ľudí a postupný morálny útlak ich názorov a zásad na život. Výsledkom je, že vláda, ktorá hybridnú vojnu prehrala, už nedokáže vzdorovať a pod tlakom militantného obyvateľstva sa buď zrúti, alebo sa vzdá svojich právomocí, ktoré už môžu otvorene presadzovať nepriateľské ozbrojené sily alebo špeciálne jednotky.

Na dosiahnutie tohto efektu, ako aj na odcudzenie, zmenu alebo vymazanie dôležitých informácií, vedú poprední hackeri kybernetické útoky, ktoré sú súčasťou informačných operácií, zamerané na informačnú štruktúru protivníka. Ich cieľom sú údaje, ktoré by mohli kompromitovať vládnuce kruhy spoločnosti a tým ich prinútiť buď upustiť od akýchkoľvek politických zámerov, alebo šíriť takéto usvedčujúce dôkazy s cieľom narušiť dôveru obyvateľstva vo vládnucu moc. Objavujú sa aj pokusy narúšať ekonomickú či inú interakciu občanov vo verejnej sfére s cieľom vniesť zmätok a nedôveru ľudí v rôzne inštitúcie krajiny, čo následne vedie k destabilizácii politickej a ekonomickej situácie v krajine.[19] Práve kybernetickými útokmi sa často začínajú mnohé konflikty medzi štátmi, ktoré sa potom rozvinú do hybridnej vojny. Pozrime sa teda na ne podrobnejšie.

KYBERNETICKÉ ÚTOKY

V súčasnosti sú hrozby v informačnej sfére čoraz rozsiahlejšie a špeciálne služby a/alebo zložky rôznych štátnych i neštátnych aktérov útočia na informačné systémy nepriateľa. Tieto útoky, ktoré zahŕňajú preniknutie do informačných a počítačových systémov, ako aj krádež, pozmenenie alebo zničenie údajov, sa nazývajú kybernetické útoky. Možno ich definovať ako „*akékoľvek úmyselné konanie útočníka/ov v kybernetickom priestore, ktoré smeruje proti záujmom inej osoby, skupiny, organizácii alebo štátu. Môže to byť útok jedinca*

[18] KŘÍŽ, Z. – SCHEVCUK, Z. – ŠTEVKOV, P. 2015. *Hybridní válka jako fenomén v bezpečnostním prostředí Evropy*. Ostrava : Jagelo 2000, 2015, s. 8

[19] HOFFMAN, F. G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. In *Potomac Institute for Policy Studies*, 2007.

alebo skupiny hackerov, prípadne útok cudzej mocnosti“.[20] Motivácia k nim siaha od snahy dokázať, že nejakú nastavenú úroveň zabezpečenia rôznych on-line systémov možno prelomiť, cez kriminálne činy, až k organizovaným akciám rôznych vlád v rámci vedenia kybernetických operácií.

Kybernetické operácie sú spravidla vedené vojenskými alebo polovojenskými silami, pod velením a/alebo pod kontrolou štátov alebo aj neštátnych aktérov, zamerané na využitie slabých stránok protivníka, jeho zraniteľností, implementáciu rôznych techník narúšania kyberpriestoru, schopnosť preťažiť ťažko dostupné kybernetické ciele a presadzovanie cielených škodlivých kybernetických produktov[21], ktoré pôsobia na nepriateľské sily. V americkej vojenskej doktríne sú definované ako „*operácie v kybernetickom priestore navrhnuté tak, aby premietali silu prostredníctvom použitia síl v kyberpriestore alebo prostredníctvom neho*“.[22]

V súčasnosti existuje aj v nadväznosti na dynamický vývoj v oblasti informačných a komunikačných technológií, systémov, prostriedkov a zariadení viacero spôsobov, metód alebo variantov ako kybernetické útoky realizovať v praxi.[23] Tu sú niektoré z nich:

DDoS útoky

DDoS (Distributed Denial of Service) útok je typ útoku na internetové služby, servery alebo webové stránky, ktorého zámerom je cieľovú službu znefunkčniť a zneprístupniť ostatným užívateľom s využitím veľkého množstva počítačov z rôznych geografických lokalít. Útok s cieľom odmietnutia služby má schopnosť úplne alebo čiastočne zakázať akékoľvek internetové zdroje. Zdrojmi sa tu rozumejú stránky, servery atď. Dnes už takmer žiadny hacker neorganizuje tento typ útoku sám, vo väčšine prípadov používa sieť počítačov infikovaných vírusom. Tento vírus poskytuje útočníkovi potrebný vzdialený prístup k počítaču obete. Počet takýchto počítačov je veľký a vytvára sieť nazývanú ‚botnet‘. Táto sieť nevyhnutne disponuje akýmsi koordinačným serverom, s ktorým hacker interaguje pomocou príkazov a ten zase posiela príkazy dostupným botom na implementáciu škodlivých požiadaviek zo servera.

Tento typ útoku má určité obmedzenia šírky pásma, ktoré sú typické pre všetky sieťové zdroje.[24] Útok DDoS odošle napadnutému webovému zdroju obrovské množstvo požiadaviek, aby prekročil schopnosť stránky spracovať všetky prichádzajúce požiadavky a spôsobil

---

[20] BAŠTA, P. - KOLOUCH, J. CyberSecurity. Praha : CZ.NIC, 2019, s. 82.

[21] SMEETS, M. Organizational integration of offensive cyber capabilities: A primer on the benefits and risks. In *9th International Conference on Cyber Conflict (CyCon)*. Tallinn : IEEE, 2017, s. 6

[22] U.S. DoA. *FM 3-12 Cyberspace and Electonic Warfare Operations*, s. 18

[23] ANDRÁSSY, V. 2022. Informácie v bezpečnostnom systéme. In Bezpečnosť elektronickej komunikácie - zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2022, s. 98-107

[24] KAZANSKÝ, R. - MIJOČ, N. 2022. O bezpečnosti v kontexte DDoS útokov. In *Bezpečnosť elektronickej komunikácie - zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 11

odmietnutie služby. Existuje viacero typov DDoS útokov, ale možno ich podmienečne rozdeliť na dva hlavné typy: na útoky na sieťovú a softvérovú časť servera.

a) Počas útoku na sieťovú časť sa útočník pokúša preťažiť komunikačný kanál servera. Je zodpovedný za množstvo dát, ktoré je server schopný prevziať. Keď je však údajov veľa, server ich nestihne spracovať a niektorí návštevníci nemôžu stránku otvoriť.
b) Počas útoku na softvérovú časť je cieľom útočníka vyčerpať niektoré zo zdrojov servera: výkon procesora, operačnú pamäť počítača, povolený počet procesov alebo databázových pripojení. Keď sa jeden zo zdrojov minie, server sa začne spomaľovať alebo úplne zamrzne.

Na zodpovedanie rôznych požiadaviek je potrebné mať k dispozícii rôzne množstvo zdrojov. Úlohou útočníka je nájsť požadovanú požiadavku, na ktorú server vynaloží najviac zdrojov. Sieťové zdroje, ako sú webové servery, sú obmedzené na súčasné obsluhovanie niekoľkých požiadaviek. Okrem povoleného zaťaženia servera existujú aj obmedzenia týkajúce sa šírky pásma kanála, čo je spojenie medzi serverom a internetom. Keď počet požiadaviek prekročí výkon ktoréhokoľvek komponentu infraštruktúry, môže dôjsť k oneskoreniu odozvy na požiadavky používateľov a k odmietnutiu služby pre všetky požiadavky alebo ich časť.[25]

HTTP DDoS útoky

HTTP (HyperText Transfer Protocol) DDoS (Distributed Denial of Service) útok predstavuje typ útoku zameraný na odmietnutie služby pre HTTP protokol, pričom nezávisle skenuje stránky na internete, aby vytvoril zoznam stránok, ku ktorým je potrebné pristupovať tak, aby sa získali informácie o tom, ktoré stránky sa načítavajú najdlhšie. Po vykonaní týchto operácií sa vykoná výber medzi stránkami, ktorých generovanie trvá dlhšie a následne sa na jednu z vybraných stránok odošle obrovské množstvo HTTP požiadaviek.

Na zodpovedanie každej požiadavky sú na serveri rezervované systémové prostriedky a s prílevom požiadaviek sa jeho zdroje jednoducho vyčerpajú, v dôsledku čoho prestane reagovať na akékoľvek požiadavky zvonku. Pomocou tejto metódy hackeri používajú jednoduché skripty na odosielanie toku požiadaviek počas tohto útoku. Problém je však v tom, že ak stránka obsahuje iba statické stránky HTML, nedôjde k žiadnym konkrétnym výsledkom, ale ak sa dynamické stránky generujú s požiadavkami na databázový server, potom môže takýto HTTP DDoS útok spôsobiť značné poškodenie chráneného systému.[26]

Otrava alebo úprava súborov cookie

Otrava súborov cookie predstavuje snahu neoprávnenej osoby o prístup a kontrolu aspektov údajov v súbore cookie, zvyčajne za účelom odcudzenia totožnosti alebo finančných

[25] W3C. 2019. DDoS Attacks. In *The World Wide Web Security FAQ*, 2019

[26] MAMUNTS, D. a kol. 2017. Models and Algorithms for Estimation and Minimization of the Risks Associated with Dredging. In *Transport and Telecommunication Journal*, 2017, roč. 18, č. 2, s. 141 - 142

informácií niekoho. Mnoho rôznych druhov hackingu, ktoré sa zameriavajú na získavanie údajov zo súborov cookie, sa môže nazývať otrava súbormi cookie, vrátane krádeže hesiel, čísel kreditných kariet alebo iných identifikátorov uložených v súboroch cookie. Položky vo vnútri cookies, ktoré sú predmetom otravy cookie, sa často nazývajú parametre.

Úspešné pokusy otravy súbormi cookie správne identifikujú parametre, ktoré obsahujú použiteľné informácie, napríklad výber čísla kreditnej karty z transakcie, ktorá obsahuje aj položky ako ID relácie, časovú pečiatku a ďalšie informácie o nákupoch. Všeobecný spôsob zabezpečenia údajov proti otrave súborov cookie spočíva v šifrovaní požiadaviek alebo transakcií. Rôzne služby môžu pomôcť klientom a koncovým používateľom šifrovať odoslané údaje, takže už nebudú transparentné pre tých, ktorí môžu na prístup k nim použiť otravu pomocou súborov cookie.[27]

Skriptovanie medzi stránkami

Tento typ útoku je najbežnejší v oblasti webových technológií a zameriava sa na väčšie a všeobecnejšie známe zdroje. Okrem toho môžu byť tieto útoky uskutočnené v dôsledku nezabezpečeného programovania a nedostatku úmyslu zlepšiť bezpečnosť infraštruktúry na internete. Klientske prehliadače majú zvyčajne prednastavené používateľské bezpečnostné nástroje, ktoré zabraňujú prístupu do vyrovnávacej pamäte a cookies komukoľvek inému ako vlastníkovi týchto súborov, teda samotnému používateľovi. V tejto situácii si hackeri vytvoria a vložia do stránky vlastný skript. Tieto skripty sú väčšinou napísané v programovacom jazyku JavaScript a možno ich použiť na úpravu súborov cookie, ukradnutie relácií obete a prenos skriptu do jeho prehliadača, po čom sa s najväčšou pravdepodobnosťou spustí a poškodí počítač používateľa.[28]

SQL útoky

SQL (Structured Query Language) je počítačový jazyk na manipuláciu a definíciu údajov. V súčasnosti je to najpoužívanejší jazyk tohto druhu v relačných systémoch riadenia databáz. SQL injection je technika napadnutia databázovej vrstvy aplikácie, spočívajúca vo vsunutí kódu prostredníctvom neošetreného alebo nesprávne ošetreného vstupu a vykonaní vlastného SQL príkazu. Týka sa tak webových, ako aj všetkých ostatných aplikácií pracujúcich s databázami. V dnešnej dobe sú databázy využívané na všetkých webových portáloch a v tomto prípade webová aplikácia nadviaže spojenie s databázou, odošle do nej požiadavku a prehliadač prijíma dáta z databázy vo formáte webovej stránky. Tieto útoky je možné použiť, ak sú vstupné dáta, ktoré klient posiela do databázy pomocou dotazov, zle filtrované. Potom je možné manipulovať pomocou SQL dotazov a najčastejšie to hackeri robia za účelom vykonania

[27] STONE, M. 2021. Cookie Hijacking: More Dangerous Than it Sounds. In Security Intelligence, 2021

[28] ALLAHVERAN, Z. A. – ELNUR, M. T. 2018. Major types of threats to information security. In *National Security*, 2018, č. 1, s. 16-17

nesprávnych operácií s databázou. Používateľ ale môže využiť aj vlastné SQL dotazy, pomocou ktorých je možné ukradnúť dáta z databázy, alebo ktoré môžu viesť k úplnému vymazaniu dát v databáze.[29]

Kryptografické zneužívanie alebo využívanie slabých miest v kryptografických algoritmoch

Všetky stránky, ktoré sú chránené, používajú technológiu založenú na certifikátoch SSL (Secure Sockets Layer), ktoré sa používajú na šifrovanie údajov a prenos cez sieť. Pomerne veľa aplikácií nešifruje údaje v súboroch cookie o nákupe, takže zostávajú v čistom texte. A aj keď sú prenášané cez sieť a šifrované pomocou SSL, na strane klienta je možné spustiť skript napísaný hackerom, v dôsledku čoho útočník získa prístup k obsahu súboru cookie a môže ukradnúť užívateľské údaje.[30]

Sociálne inžinierstvo

Štatistiky ukazujú, že sociálne inžinierstvo sa dnes v rôznych podobách využíva až pri 97 percentách špeciálne plánovaných kybernetických útokoch, pričom využitie technologických nástrojov sa nepoužíva vôbec alebo sa využíva len minimálne.

Phishing predstavuje pokus o podvodné získanie citlivých informácií, ako sú heslá a/alebo podrobnosti o kreditných kartách, maskovaním sa za dôveryhodnú osobu alebo obchod pri elektronickej komunikácii. Phishing je typickým príkladom techniky sociálneho inžinierstva používanej na oklamanie používateľov, pričom je zameraný hlavne na využitie slabých miest súčasných bezpečnostných technológií (a ich implementácií).

Špeciálnym prípadom phishingu je spear phishing (lovenie harpúnou), ktorý je útokom na úzku skupinu potenciálnych obetí alebo jednotlivcov, väčšinou takých, ktorí majú prístup k citlivým informáciám o organizácii a spravidla sú v organizačnom rebríčku vyššie postavení. Takéto emaily sú úzko zamerané a personalizované. Útočníci sa pri tejto technike zvyčajne spoliehajú na diery v systéme, čiže škodlivé kódy, ktoré využívajú zraniteľnosti softvéru vo vyhliadnutom počítači.

Na podobnom princípe ako phishing sú založené aj ďalšie podvody, keď sa podvodníci snažia vylákať dáta prostredníctvom telefonického phishingu – *Vishingu* (Voice Phishing), cez sms správu s URL odkazom na podvodnú stránku alebo výzvou na odpovedanie na telefónne číslo – *Smishingu* (SMS Phishing), alebo útočníci skúšajú citlivé údaje získať cez zavírený

---

[29] PS. 2022. SQL injection. In *PortSwigger*, 2022

[30] DOINIKOVA, E. 2018. Enhancing attack graphs for cybersecurity monitoring: handling inaccuracies, processing loops, displaying incidents, and automatically selecting defenses. In *SPIIRAS Proceedings Journal*, 2018, roč. 57, č. 2, s. 212

počítač alebo mobilné zariadenie prostredníctvom podvodného presmerovania webových stránok – *Pharmingu*.[31]

Vírus Stuxnet

Stuxnet predstavuje všestranný autonómny priemyselný špionážny nástroj určený na získanie prístupu k operačnému systému, ktorý je zodpovedný za zber a spracovanie údajov, ako aj za prevádzkové dispečerské riadenie priemyselných zariadení. Na rozdiel od väčšiny týchto vírusov však hlavnou aplikáciou nemusí byť krádež dôležitých údajov, ale poškodenie systémov priemyselnej automatizácie. Takéto červy môžu potichu hibernovať v napadnutom systéme a v správnom momente môžu začať vydávať príkazy, ktoré deaktivujú napadnutý systém. Napríklad Win32/Stuxnet je sieťový červ, ktorý infikuje počítače so systémom Windows. Je distribuovaný ako na počítačoch bežných používateľov, tak aj na systémoch priemyselnej automatizácie, pričom môže byť použitý ako prostriedok na kradnutie dát, špionáž alebo sabotáž v rôznych podnikoch, firmách, letiskách, čerpacích staniciach, železničných staniciach a pod.[32]

Vírus Regin

Vírus Regin predstavuje sofistikovanú súpravu malvéru a hackerských nástrojov, ktorú používajú americké a britské vládne bezpečnostné agentúry. Je to v podstate trójsky kôň, ktorý infikuje počítače s operačným systémom Microsoft Windows. Vírus bol prvýkrát detegovaný spoločnosťami Kaspersky Lab a Symantec, ktoré tvrdia, že tento vírus je revolučný a nemá analógiu. Podľa štatistík poskytnutých spoločnosťou Symantec: 28 % obetí tohto vírusu sú telekomunikačné spoločnosti, 24 % sú inštitúcie a úrady spojené s vládou a zvyšných 48 % sú podniky a firmy.[33]

Regin je vírus s modulárnym prístupom, ktorý mu umožňuje načítať funkcie, ktoré sú potrebné na zohľadnenie individuálnych charakteristík počítača obete alebo infikovanej siete. Je postavený tak, aby bolo možné bez prerušenia monitorovať veľké množstvo potrebných objektov. Okrem toho ukladá všetky údaje vo svojom vlastnom súborovom systéme s názvom Encrypting Virtual File System (EVFS) a nie v počítači obete. Tento systém je šifrovaný blokovou šifrou RC5. Regin komunikuje cez internet pomocou protokolu ICMP/Ping, príkazov vložených do HTTP cookies a protokolov TCP a UDP, čím premieňa infikovanú sieť na botnet. Má komplexnú viacstupňovú architektúru, spoľahlivo šifruje stopy svojej práce a má obrovské

---

[31] Bližšie pozri: ESET. 2019. Ako rozpoznať phishing? In *ESET*, 2019; ŽIVÉ. 2019. Spear phishing: Cielený podvod priamo na vás. In *Živé.sk*, 2019; ESET. 2022. Vishing: ako ho rozpoznať a vyhnúť sa tak podvodu? In *Bezpečne na nete*, 2022.

[32] TRELLIX. 2022. What Is Stuxnet? In *Trellix*, 2022.

[33] TCRA. 2019. Cyber Threats: key insights from the best reports. In *The Cyber Rescue Alliance*, 2019

množstvo možností implementovaných počas útoku. Mnohé jeho možnosti sú ale stále neznáme a zložky vírusu sa stále skúmajú.[34]

Agent Tesla Trojan

Agent Tesla Trojan predstavuje vylepšený Remote Access Trojan (RAT), teda trójsky kôň, ktorý je odborníkom na informačnú bezpečnosť známy už od roku 2014. Má schopnosť sledovať a zbierať dáta zadané obeťou z klávesnice alebo získané zo snímok obrazovky. Okrem toho dokáže ukradnúť používateľské prihlasovacie údaje z rôznych programov, napríklad z obľúbeného prehliadača Google Chrome. Jeho nebezpečenstvo spočíva v tom, že ho nie je potrebné opraviť v systéme alebo čakať na ovládací príkaz, aby dokončil svoje úlohy. Keď sa dostane do počítačového systému, okamžite začne zhromažďovať osobné informácie a prenesie ich do počítačového numerického riadenia (CnC). Toto agresívne správanie je trochu podobné správaniu ransomvéru, jediný rozdiel je v tom, že ransomvér nepotrebuje sieťové pripojenie.[35]

Trojan AZORult

AZORult je špeciálny trójsky kôň, ktorý je schopný zhromažďovať rôzne údaje na infikovanom počítači a následne ich odosielať na príkazový a riadiaci server. Tieto údaje môžu zahŕňať históriu prehliadača, prihlasovacie údaje a heslá, súbory cookie, súbory z priečinkov špecifikovaných v príkaze servera príkazu (napríklad všetky súbory s príponou.txt z priečinka Pracovná plocha) atď. Tento škodlivý softvér tiež slúži na stiahnutie iného vírusu. Počas procesu vývoja prešiel AZORult mnohými zmenami súvisiacimi s rozširovaním jeho schopností. Verzia škodlivého programu v C++, ktorá má množstvo nedostatkov, je zároveň oveľa nebezpečnejšia ako jej predchodca vďaka možnosti vzdialeného pripojenia k pracovnej ploche obete.[36]

ZÁVER

V nadväznosti na informácie uvedené v predchádzajúcich kapitolách je možné na záver uviesť, že kybernetické útoky predstavujú v dnešnej dobe veľmi dôležitú súčasť informačných operácií vedených v rámci hybridnej vojny. Samotné informačné operácie zahŕňajú *„integrované využitie elektronického boja, operácií počítačových sietí, psychologických operácií, klamania a bezpečnosti operácií v súlade so špecifikovanými podpornými a súvisiacimi schopnosťami ovplyvňovať, narúšať, korumpovať alebo uzurpovať si ľudské a automatizované rozhodovanie protivníka a zároveň chrániť vlastné“*.[37] Informačné operácie

---

[34] FLYNN, A. 2014. Regin Virus, One Of The Most Powerful Computer Viruses Ever Built. In *VBT News*, 2014

[35] SCROXTON, A. 2021. Agent Tesla trojan finds new ways to sneak past defences. In *ComputerWeekly.com*, 2021; YAAKOBI, O. 2022. What Is Agent Tesla Spyware and How Does It Work? In *Datto*, 2022

[36] MESKAUSKAS, T. 2021. AZORult Trojan. In *PCrisk*, 2021.

[37] U.S. DoD. 2003. *Joint Publication 3-53*. Washington : United States Department of Defense, 2003

sú teda akcie vedené s cieľom ovplyvniť informácie a informačné systémy protivníka pri obrane vlastných informácií a vlastných informačných systémov. Sú, ako už je uvedené vyššie, súčasťou väčšej, viacrozmernej a viacsmernej hybridnej vojny.

Kybernetické útoky ako súčasť informačných operácií spravidla prejdú bez povšimnutia a stanú sa známymi až po nástupe ich následkov. Ich vplyv sa vzťahuje na všetkých občanov a dôsledky sú škodlivé pre všetky oblasti či sféry spoločnosti. Revolúcia v oblasti informačných technológií, ktorá sa začala v roku 2000 a pokračuje dodnes, si vyžaduje vývoj najnovších systémov a technológií na obranu proti kybernetickým útokom. Ako vyplýva z vyššie uvedeného textu, hybridná vojna je veľmi rýchlo sa rozvíjajúci spôsob vedenia vojny, v dôsledku ktorého síce nedochádza k veľkým stratám na životoch, ako v prípade konvenčnej vojny, ale všetko úsilie smeruje k destabilizácii politických, ekonomických a sociálnych sfér nepriateľa. V priebehu hybridnej vojny sa to dosahuje aj vďaka takej zložke, akou sú informačné operácie, ktoré sú schopné spôsobiť obrovské škody na informačných a počítačových systémoch pomocou rôznych kybernetických útokov, ako aj odraziť útoky na ich vlastné systémy. To je v moderných vojnách zásadné, pretože ak je nepriateľ zbavený prenosu informácií, možno bezpečne preniknúť na jeho územie a rýchlo udrieť na jeho systémy riadenia a velenia, ešte skôr ako sa spamätá a podnikne adekvátne protiopatrenia.

Štát pomocou kybernetických útokov v rámci informačných operácií počas vedenia hybridnej vojny sleduje cieľ znefunkčniť, destabilizovať alebo v čo najväčšej miere oslabiť iný štát. Konfrontácia teda prebieha na pomerne vysokej úrovni, pričom bežný občan trpí v takýchto prípadoch následkami vedenia „neviditeľnej“ vojny. Preto je potrebné na tento problém upozorniť a prijímať účinné a efektívne opatrenia na zastavenie takéhoto konanie vo najmä vzťahu k ľuďom, keďže vykonávanie riadených informačných, dezinformačných a propagandistických aktivít negatívne ovplyvňuje psychický aj fyzický stav človeka.

Informačné systémy sa aktualizujú každý deň a stávajú sa čoraz zložitejšími a nebezpečnejšími. Je stále ťažšie do nich preniknúť, ale tiež je stále ťažšie ich chrániť. Práve tieto ťažkosti riešia informačné operácie, ktorých realizátori sa snažia študovať a nachádzať nové spôsoby kybernetických útokov, ako aj vyvíjať technológie, ktoré dokážu obísť spôsoby ochrany nepriateľských systémov a zároveň zabezpečiť, ochrániť tie svoje.

Zoznam použitej literatúry a zdrojov:

ALLAHVERAN, Z. A. – ELNUR, M. T. 2018. Major types of threats to information security. In *National Security*, 2018, č. 1, s. 13 - 18. ISSN 1812-5592.

ANDRÁSSY, V. 2022. Informácie v bezpečnostnom systéme. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022, s. 98-107. ISBN 978-80-8054-968-8.

BAŠTA, P. – KOLOUCH, J. 2019. *CyberSecurity*. Praha : CZ.NIC, 2019. 556 s. ISBN 978-80-88168-34-8.

DOINIKOVA, E. 2018. Enhancing attack graphs for cybersecurity monitoring: handling inaccuracies, processing loops, displaying incidents, and automatically selecting defenses. In *SPIIRAS Proceedings Journal*, 2018, roč. 57, č. 2, s. 211–240. ISSN 2078-9599.

DVORAK, J. 2016. *Complexity in Modern War: Examining Hybrid War*. Springfield : Missouri State University, 2016. 178 s. ISBN 978-1-721-51009-2.

ESET. 2019. Ako rozpoznať phishing? In *ESET*, 2019. [online] [cit. 04.06.2022] Dostupné na: <https://www.eset.com/sk/blog/domaca-it-bezpecnost/ako-rozpoznat-phishing/>.

ESET. 2022. Vishing: ako ho rozpoznať a vyhnúť sa tak podvodu? In *Bezpečne na nete*, 2022. [online] [cit. 04.06.2022] Dostupné na: <https://bezpecnenanete.eset.com/sk/cybernews/vishing-ako-ho-rozpoznat-a-vyhnut-sa-tak-podvodu/>.

FLYNN, A. 2014. Regin Virus, One Of The Most Powerful Computer Viruses Ever Built. In *VBT News*, 2014. [online] [cit. 05.06.2022] Dostupné na: <https://www.vbt.ie/regin-virus-one-powerful-computer-viruses-ever-built-year/>.

GLENN, R. W. 2009. Thoughts on Hybrid Conflict. In *Small Wars Journal*, 2009. [online] [cit. 06.04.2022] Dostupné na: <https://www.smallwarsjournal.com/blog/188-glenn.pdf>.

GREGA, M. – ŽENTEK, M. – NEČAS, P. 2020. Security Threats Versus New Areas and Approaches of the Cyber Synthetic Environment. In Fabián, K. – Beňuška, T. (eds.): *Analysis of Social Network Security. Threats in cyberspace*. 2020, s. 172-229. Krakow: Apeiron University of Public and Individual Security in Kraków. ISBN 978-83-64035-70-8.

GRISCIOLI, G. 2016. *Intelligence. The Hybrid War*. Roma : Aracne, 2016. 108 s. ISBN 978-88-5489-060-2.

HOFFMAN, F. G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. In *Potomac Institute for Policy Studies*, 2007. [online] [cit. 06.04.2022] Dostupné na: <http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf>.

HROMADA, M. 2017. Kybernetická bezpečnosť. In Lukáš, L. a kol.: *Teória bezpečnosti I.* Zlín : Radim Bačuvčík – VeRBuM, 2017, s. 123-133. ISBN 978-80-87500-89-7.

IVANČÍK, R. 2016. Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia. In *Medzinárodné vzťahy*, 2016, roč. 14, č. 2, s. 130-156. ISSN 1339 – 2751. [cit. 06.04.2022] Dostupné na: <https://fmv.euba.sk/www_write/files/dokumenty/veda-vyskum/medzinarodne-vztahy/archiv/2016/2/mv_2016_2_130-156_ivancik.pdf>.

IVANČÍK, R. 2020. Analýza prístupov k definovaniu a vymedzeniu hybridnej vojny. In *Národná a medzinárodná bezpečnosť 2020 : zborník príspevkov z 11. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2020. s. 174-184. ISBN 978-80-8040-589-2.

JURČÁK, V. - SASARÁK, J. 2016. Hybridné hrozby – výzva pre Európsku úniu. In *Medzinárodné vzťahy 2016 : aktuálne otázky svetovej ekonomiky a politiky*. Bratislava : Vydavateľstvo Ekonóm, 2016, s. 542-550. ISBN 978-80-225-4365-1.

JURČÁK, V. - TURAC, J. 2018. Hybridné vojny – výzva pre NATO. In *Bezpečnostné fórum 2018 : zborník vedeckých prác*. Banská Bystrica : Interpolis, 2018. s. 177-184. ISBN 978-80-972673-5-3.

KAZANSKÝ, R. - MIJOČ, N. 2022. O bezpečnosti v kontexte DDoS útokov. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 8-19. ISBN 978-80-8054-968-8.

MAMUNTS, D. a kol. 2017. Models and Algorithms for Estimation and Minimization of the Risks Associated with Dredging. In *Transport and Telecommunication Journal*, 2017, roč. 18, č. 2, s. 139 - 145. ISSN 1407-6179.

MANKO, O. – MIKHIEIEV, Y. 2018. Defining the Concept of 'Hybrid Warfare' Based on Analysis of Russian Agression against Ukraine. In *Connections*, 2018. [cit. 06.04.2022] Dostupné na: <https://connections-qj.org/system/files/4107_mikhieiev_manko.pdf>.

MESKAUSKAS, T. 2021. AZORult Trojan. In *PCrisk*, 2021. [online] [cit. 05.06.2022] Dostupné na: <https://www.pcrisk.com/removal-guides/13200-azorult-virus>.

MILLER, M. 2015. *Hybrid Warfare: Preparing for Future Conflict*. Montgomery : Air War College, 2015. 34 s.

MÜLLEROVÁ, J – ŠIŠULÁK, S. 2020. Criminality software control tools of environmental crime. In *20th International Multidisciplinary Scientific GeoConference Proceedings SGEM 2020*, Sofia : Stef92, s. 207-212. ISBN 978-619-7603-10-1.

MURRAY, W. – MANSOOR, P. R. 2012. *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge : Cambridge University Press, 2012. 321 s. ISBN 978-1-107-02608-7.

PS. 2022. SQL injection. In *PortSwigger*, 2022. [online] [cit. 03.06.2022] Dostupné na: <https://portswigger.net/web-security/sql-injection>.

SCROXTON, A. 2021. Agent Tesla trojan finds new ways to sneak past defences. In *Computer Weekly.com*, 2021. [online] [cit. 05.06.2022] Dostupné na: <https://www.computerweekly.com/news/252495678/Agent-Tesla-trojan-finds-new-ways-to-sneak-past-defences>.

SIGHOLM, J. 2016. Non-State Actors in Cyberspace Operations. In *Journal of Military Studies*, 2016, roč. 4, č. 1, s. 1-37. ISSN 1799-3350. [online] [cit. 25-02-2022] Dostupné na: <https://ccdcoe.org/research/tallinn-manual/>

SINGER, P. W. – FRIEDMAN, A. 2014. *Cybersecurity and Cyberwar (What Everyone Needs to Know)*. Oxford : Oxford University Press, 2014. 306 s. ISBN 978-0-19991-811-9.

SMEETS, M. 2017. Organizational integration of offensive cyber capabilities: A primer on the benefits and risks. In *9th International Conference on Cyber Conflict (CyCon) – Conference Proceedings*. Tallinn : IEEE, 2017. ISSN 2325-5374.

STONE, M. 2021. Cookie Hijacking: More Dangerous Than it Sounds. In *Security Intelligence*, 2021. [online] [cit. 03.06.2022] Dostupné na: <https://securityintelligence.com/articles/guide-to-cookie-hijacking/>.

TCRA. 2019. Cyber Threats: key insights from the best reports. In *The Cyber Rescue Alliance*, 2019. [online] [cit. 04.06.2022] Dostupné na: <https://www.cyberrescue.co.uk/library/threat>.

TRELLIX. 2022. What Is Stuxnet? In *Trellix*, 2022. [online] [cit. 04.06.2022] Dostupné na: <https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html>.

U.S. DoA. 2017. *FM 3-12 Cyberspace and Electonic Warfare Operations*. Washington : United States Department of the Army, 2017.

U.S. DoD. 2003. *Joint Publication 3-53*. Washington : United States Department of Defense, 2003.

VALOUCH, J. – HROMADA, M. 2016. *Bezpečnostní futurologie*. Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2016. 144. s. ISBN 978-80-7454-621-1.

VALUCH, J. 2019. *Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti*. Bratislava : Wolters Kluwer, 2019. 160 s. ISBN 978-80-571-0154-3.

Van HAASTER, J. 2019. *On cyber: the utility of military cyber operations during armed conflict*. Amsterdam : University of Amsterdam, 2019. 359 s. [online] [cit. 25-02-2022] Dostupné na: <https://pure.uva.nl/ws/files/37093787/Thesis.pdf>

VOERZIO, M. 2021. *Hybrid War: Attack on the West*. Garden City : Babelcube, 2021. 96 s. ISBN 978-1-6674-1523-9.

W3C. 2019. DDoS Attacks. In *The World Wide Web Security FAQ*, 2019. [online] [cit. 03.06.2022] Dostupné na: <https://www.w3.org/Security/Faq/wwwsf6.html>.

YAAKOBI, O. 2022. What Is Agent Tesla Spyware and How Does It Work? In *Datto*, 2022. [online] [cit. 05.06.2022] Dostupné na: <https://www.datto.com/blog/what-is-agent-tesla-spyware-and-how-does-it-work>.

ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 8-19. ISBN 978-80-8054-968-8.

ŽIVÉ. 2019. Spear phishing: Cielený podvod priamo na vás. In *Živé.sk*, 2019. [online] [cit. 04.06.2022] Dostupné na: <https://zive.aktuality.sk/clanok/109427/spear-phishing-cieleny-podvod-priamo-na-vas/>.