POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Kyberterorismus

Bakalářská práce

Cyberterrorism

Bachelor thesis

VEDOUCÍ PRÁCE
RNDr. Václav HNÍK, CSc.

AUTOR PRÁCE
Jana ČEPOVÁ

PRAHA
2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Milovicích, dne 22. 2. 2022

Jana Čepová

Poděkování

Na tomto místě bych ráda poděkovala RNDr. Václavu Hníkovi, CSc. za cenné připomínky a odborné rady, kterými přispěl k vypracování této bakalářské práce.

ANOTACE

Bakalářská práce se zabývá problematikou kyberterorismu. Práce je rozdělena na teoretickou a praktickou část. Teoretická část definuje základní pojmy z oblasti kyberprostoru, jak je možné jej chápat z různých úhlů pohledů. Jádrem práce je kyberterorismus jako současná bezpečnostní hrozba, popisují se zde jeho obecné funkce, metody i cíle. Pozornost je zde věnována i kyberdžihádu, jsou zmíněny taktiky a techniky kyberdžihádistů a v neposlední řadě je popsána legislativa a odpovědné instituce kybernetické bezpečnosti s těmito souvisejícími problémy. Praktická část je zaměřena na případovou studii vybraného kyberdžihádistického útoku.

KLÍČOVÁ SLOVA

kyberterorismus * kybernetická bezpečnost * kyberprostor * kybernetický útok * aktéři * kyberdžihád * propaganda * rekrutace * internet * sociální sítě

ANNOTATION

The bachelor thesis deals with the issue of cyberterrorism. The work is divided into theoretical and practical part. The theoretical part defines the basic concepts of cyberspace, how it can be understood from different perspectives. The core of the work is cyberterrorism as a current security threat, it describes its general functions, methods and objectives. Attention is also paid to cyber jihad, tactics and techniques of cyber jihadists are mentioned, and last but not least, the legislation and responsible institutions of cyber security with these related problems are described. The practical part is focused on a case study of a selected cyber jihadist attack.

KEYWORDS

cyberterrorism * cyber security * cyberspace * cyberattack * actors * cyberjihad * propaganda * recruitment *internet * social networking services

OBSAH

ÚVOD

Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad způsobuje rozsáhlé ekonomické škody ve veřejném i v soukromém sektoru a současně jsou schopny vyvolat negativní politické důsledky, a to jak v národním měřítku, tak v měřítku globálním.

V devadesátých letech zažil internet svůj dramatický rozmach, rozšířil se do celého světa, do všech oblastí našich životů a dal vzniknout miliardovým online odvětvím.

S odchodem komunismu nastala v naší republice tzv. internetová revoluce. 13. února to bylo již 30 let, kdy proběhlo oficiální slavnostní připojení naší republiky k internetu. Internet, jako nová technologie, nám ve velké míře usnadňuje každodenní život, zároveň se s rozšířením pokrytí zvyšuje rychlost a klesá cena připojení, proto je připojení dostupné téměř pro všechny sociální vrstvy. S tím souvisí i situace ve světě. S nárustem používání informačních a komunikačních technologií roste nejen závislost společnosti, ale i riziko zneužívání sítě. Internetové připojení je dnes dostupné pro široké masy obyvatel a tím roste i potencionální hrozba terorismu. Společnost, která využívá moderní ICT[1] v každodenním životě, je a bude stále více ohrožena úmyslným či neúmyslným zneužitím těchto technologií.

Příchodem nového milénia se svět, ve kterém žijeme, zásadně změnil. Změnil se i život lidí, najednou musí počítat s novými nástrahami, které jim život přináší.

Seznam nástrah, které se týkají fungování moderního internetu není zrovna krátký: Hackerské útoky, úniky soukromých dat, tajné kampaně, dezinformace, špionáž, kyberútoky. Útoky v rámci kyberprostoru se stávají součástí života nás všech. V historii to byli jen hackeři, kdo ohrožoval internet. Nyní jsme ale svědky rozvoje kybernetických teroristických organizací. Útočníci používají stále sofistikovanější a komplexnější metody útoků. Důvodů, proč se útočníci rozhodli pro své aktivity používat internet, je nepřeberné množství. Kyberterorismus má široké mediální pokrytí je anonymní a levný.

[1] Information and Communication Technologies

Kyberteroristé si hledají cíle, kde by mohli co nejvíce uškodit větší mase obyvatel nebo získat výhodu nad systémem, popřípadě systém vyřadit úplně z provozu.

Cílem kyberteroristů je tedy poškození nebo vyřazení počítačové infrastruktury, krádež či zničení důležitých dat apod. Útoky mají politický motiv a cílem je narušení systému, vyvolání strachu, propaganda. Největším rizikem mohou být útoky na strategické cíle nebo na kritickou infrastrukturu.

Islámský stát a další teroristické skupiny se ve svém boji neomezují pouze na využívání tradičních zbraní, používají internet jako prostředek k šíření svých myšlenek, náboru a komunikaci. Stále propojenější svět nabízí teroristům nové možnosti. Kyberdžihádisté plní sociální sítě a internetová média svými propracovanými příspěvky a tisíce mladých lidí po celém světě jejich propagandě podléhají.

Stát i komerční sféra si uvědomuje riziko těchto hrozeb a snaží se různými prostředky chránit své informační technologie. Sice se většina odborníků shoduje na tom, že kyberteroristický útok dosud zaznamenán nebyl, to ale neznamená, že bychom měli hrozbu v budoucnu podceňovat. Pokud nepodceníme přípravu a vybudování bezpečné infrastruktury, poté bude mít útočník menší šanci na úspěch. Samozřejmě záleží i na dalších souvislostech, jako např. školení personálu, zabezpečení pracovních stanic, které budou odolné na spuštění škodlivých programů.

Při zpracovávání mé bakalářské práce jsem se snažila čerpat z nejaktuálnější dostupné literatury a ověřených internetových zdrojů.

1. POJMY Z OBLASTI KYBERPROSTORU

1.1 Kyberprostor

Rozvoj informačních a telekomunikačních technologií spolu s připojením na komunikační a informační služby vede k vytváření zvláštního prostoru, který se nazývá kyberprostor.

Termín kyberprostor můžeme interpretovat různými způsoby. Někdy je pojem kyberprostor používán jako synonymum pro virtuální realitu. Virtuální počítačový svět, který je zcela závislý na technologiích reálného světa. Nejčastěji je vnímán jako imaginární svět, metafora internetové sítě, včetně telefonů, TV[2] a dalších komunikačních sítí.

Kyberprostor je rozsáhlý nehmotný počítačový svět, složený z prvků informačních a komunikačních technologií, které tvoří celosvětovou, globální počítačovou síť, která je základem online komunikace. Do této sítě jsou připojeny a integrovány menší, po světě rozeseté jednotlivé počítačové systémy, které užívají TCP/IP[3] protokol.

Základními znaky kyberprostoru jsou jeho decentralizovanost, globálnost, otevřenost, bohatost na informace, interaktivnost a možnost ovlivňování mínění skrze uživatele.

Kyberprostor je otevřený širokému spektru uživatelů, kterým umožňuje výměnu dat a elektronickou komunikaci. Anonymitou umožňuje vlastně jakékoliv jednání bez zodpovědnosti, umožňuje svým uživatelům komunikovat, sdílet a vyměňovat si informace a nápady, hrát hry, účastnit se diskuzí na sociálních fórech, provádět obchodní transakce, atd…[4]

Kyberprostor s sebou nutně nese riziko jeho zneužití pro společensky nebezpečné aktivity nového typu – kybernetickou kriminalitu.

---

[2] televize
[3] Transmission Control Protocol/Internet Protocol
[4] JANSSEN, Cory. *Cyberspace* [online]. [cit. 24.1.2022].
Dostupné z: https://www.techopedia.com/definition/2493/cyberspace

1.1.1 Pojetí kyberprostoru

Termín „cyberspace“ poprvé použil americko-kanadský spisovatel Sci-Fi William Gibson ve své povídce Burning Chrome, publikované roku 1982 v časopise Omni. Později použil pojem kyberprostor roku 1984 ve své knize Neuromancer, kde jej definoval takto: *„A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding“*

„Konsenzuální halucinace prožívaná denně miliardami legitimních operátorů, v každém národě, dětmi, které se učí matematickým pojmům... grafické zobrazení dat abstrahovaných z pamětí každého počítače v lidské společnosti. Nepředstavitelná komplexita. Linie světla rozprostírající se v neprostoru mysli, klastry a konstelace dat. Jako světla velkoměsta, vzdalující se."[5]

Nejčastěji se popisuje kyberprostor takto: „*Kyberprostor je globální a vyvíjející se doména popisovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace. Kyberprostor zahrnuje: a) fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (SCADA zařízení, smartphony/tablety, počítače, servery atd.), b) počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému, c) spojení počítačových sítí, d) uživatelské vstupy a uzly zprostředkovatelů spojení, e) informace – uživatelská data.“*[6]

Zákon o kybernetické bezpečnosti rozumí kybernetickým prostorem *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.”*[7] Kybernetický prostor je

[5] viz GIBSON, William, *Neuromancer*, překlad Josef Rauvolf, Laser-books, 2010, ISBN 978-80-7193-318-2
[6] viz *Academia.edu: How_would you define Cyberspace* [online]. [cit. 24.1.2022]. Dostupné z: https://www.academia.edu/7096442/How_would_you_define_Cyberspace
[7] viz § 2 písm. a), Zákon č. 181/2014 Sb., o kybernetické bezpečnosti [online]. [cit. 9.2.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

zde jasně definován technickým výčtem potřebné infrastruktury a výčtem, co infrastruktura umožňuje.[8]

Oxford dictionary definuje kyberprostor jako *„fiktivní prostředí, ve kterém dochází ke komunikaci skrze počítačové sítě.“*[9]

1.2 Kybernetické hrozby

V souvislosti s vývojem a pronikáním informačních technologií do všech oblastí života, dochází bohužel i k nárůstu rizik, která z těchto technologií plynou. Útočníci si stále více uvědomují výhody kyberprostoru, jeho rychlost, praktičnost a především anonymitu. Jejich útoky jsou komplexnější a sofistikovanější. Používají pokročilé metody, jsou kvalitně a podrobně plánované, přesně cílené a hlavně trvalé. Rozsah těchto cílených útoků proti informačním a komunikačním technologiím přesahuje národní a přesouvá se do globálního měřítka.

1.3 Kybernetický útok

Výkladový slovník kybernetické bezpečnosti definuje kybernetický útok, jako: *„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“*[10]

1.4 Kybernetická kriminalita

Pojem kybernetická kriminalita je odvozen od pojmu kybernetický prostor. Kybernetická kriminalita je jev poměrně nový, útoky můžou vést ke značným škoda a ztrátám, je pro ni typická rychlost výměny dat a též jistá míra anonymity.

„Kybernetická trestná činnost je společensky škodlivé jednání útočící na počítačový systém nebo na jiný objekt za výrazného užití počítačového systému“.[11]

---

[8] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

[9] viz *Oxford Learner's Dictionaries*: *Cyberspace* [online]. [cit. 13.2.2022]. Dostupné z: https://www.oxfordlearnersdictionaries.com/definition/english/cyberspace

[10] viz str. 71, JIRÁSEK Petr; NOVÁK Luděk a POŽÁR Josef. *Výkladový slovník kybernetické bezpečnosti.* [online]. [cit. 13.2.2022]. 3. aktualiz. vyd. Praha: AFCEA, 2015

[11] *Internetem bezpečně: Co je kybernetická kriminalita* [online]. [cit. 8.2.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/kyberneticka-kriminalita/

Počítačová síť se tedy může stát jak objektem, tak i subjektem kybernetické kriminality.

Podle slovníku kybernetické bezpečnosti můžeme definovat kybernetickou kriminalitu takto:

„Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.“[12]

1.5 Kybernetická válka

Kybernetická válka je rozsáhlá často politicky či strategicky motivovaná kybernetická operace, jejímž cílem je oslabení nebo zničení informačních systémů protivníka.

V tomto boji útočníci místo klasických zbraní používají myš a správné povely zadávají do klávesnice.

[12] viz str. 57, JIRÁSEK Petr; NOVÁK Luděk a POŽÁR Josef. *Výkladový slovník kybernetické bezpečnosti*. [online]. [cit. 13.2.2020]. 3. aktualiz. vyd. Praha: AFCEA, 2015

2. KYBERTERORISMUS

Kyberterorismus můžeme vnímat jako jednu z největších hrozeb 21. století z pohledu rozvoje a budoucnosti informační společnosti. Rozvojem informačních a komunikačních sítí roste závislost společnosti na rychlém a okamžitém přístupu k informacím a online spolupráce, a tím se také zvyšuje zranitelnost takto vybudovaných kanálů třetími osobami.

Pojem „kyberterorismus“ pochází z anglického výrazu „cyberterrorism“. Jedná se o kombinaci slov – „cyber“ označujícího něco virtuálního a slova „terrorism“ znamenající „terorismus“.

Předpona „kyber-" odkazuje na kybernetický prostor a vypovídá o povaze útoku, nikoliv o aktérech, jejich způsobu komunikace nebo o jejich cílech a motivacích.

„Jedná se o plánovanou činnost, motivovanou zpravidla politicky či nábožensky, která je realizována spíše malými, ne vojensky organizovanými strukturami. Cílem těchto skupin je především ovlivnění veřejného mínění. Kyberterorismus představuje velké nebezpečí a teroristickými skupinami je využíván ve stále rostoucí míře.“[13]

Kyberterorismus neboli kybernetický terorismus je typem terorismu, který můžeme chápat jako prolnutí klasického terorismu do tzv. kyberprostoru. Jeho principem je především zneužívání ICT jako prostředku a prostředí pro uskutečnění útoku. Zjednodušeně je tedy kyberterorismus spojení mezi prvky informačních a komunikačních technologií s kyberprostorem jako takovým.[14]

Podle některých odborníků kyberterorismus neexistuje. Tvrdí, že se jedná pouze o útoky jednotlivců, skupin a organizací, které pro dosažení svých cílů využívají informačních technologií. Tyto útoky však oproti obvyklým teroristickým činům nezpůsobují smrtící následky.

Ekonomické dopady kyberterorismu dosahují obrovských hodnot. Například vyčíslení škod po viru Code Red, který ohrožoval americké servery, se podle

---

[13] viz str. 129, JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007

[14] viz str. 106, DUNNINGAN, James F. *Bojiště zítřka*. Baronet, 2004. ISBN 80-7214-642-4.

studie nevládní výzkumné organizace „Computer Economics“ v roce 2001 vyšplhalo až k hodnotě 2,6 miliardy dolarů.[15]

2.1 Historie a současnost kyberterorismu

O nebezpečí zneužití internetu pro teroristické účely se začalo uvažovat již na začátku devadesátých let, kdy užívání internetu zaznamenalo obrovský nárůst. National Academy of Science ve Spojených státech to komentovala slovy: *„Jsme v ohrožení. Amerika je stále více a více závislá na počítačích… příští teroristé budou moci napáchat daleko více škody klávesnicí než bombou.“*[16]

Historicky sahá až do slavné teroristické organizace Al-Káida. Al-Káida byla první džihádistickou organizací, která využívala World Wide Web, a Usáma bin Ládin byl prvním teroristou, který přijal internetovou technologii již v roce 1997.

Ayman al Zawahiri, současný vůdce Al-Káidy, v roce 2005 prohlásil, že *„jsme v bitvě a více než polovina této bitvy je v médiích“.*[17] Tento projev Aymana Al Zawahiriho byl jiskrou, počátkem vzniku kybernetického džihádu, který dnes zuří.[18]

Členové Al-Káidy a dalších teroristických skupin používali při plánování svých teroristických činů moderní technologie. Důkazy naznačují, že teroristé používali internet při plánování své operace na 11. září 2001. Muhammad Atta,[19] vůdce útoků, provedl rezervaci letenek online a buňky Al-Káidy údajně používali internetové telefonní služby ke komunikaci s ostatními buňkami v zámoří. Khalid Shaikh Mohammed,[20] strůjce útoků proti World Trade Center,[21] údajně používal internetový chatovací software pro komunikaci s únosci letadel.

---

[15] DUNNINGAN, James F. *Bojiště zítřka*. Baronet, 2004. ISBN 80-7214-642-4.
[16] viz str. 2, WEIMANN, Gabriel. *Cyberterrorism: How Real is the Threat?* [online]. [cit. 24.1.2022]. Místo vydání: United States Institute of Peace. December, 2004. Dostupné z: http://www.usip.org/sites/default/files/sr119.pdf.
[17] viz KLAUSEN, J., *Tweeting the Jihad: Sociální sítě západních zahraničních bojovníků v Sýrii a Iráku* [online]. [cit. 24.1.2022]. Dostupné z: https://www.tandfonline.com/doi/pdf/10.1080/1057610X.2014.974948.
[18] LIANG, Christina Schori. *Kyberdžihád: porozumění propagandě Islámského státu a boj proti ní*. GSCP Policy Paper, 2.4. 2015 [online]. [cit. 24.1.2022]. Dostupné z: https://www.gcsp.ch/Christina-Schori-Liang
[19] Muhammad Atta byl vůdce skupiny únosců letadel během teroristických útoků 11. září 2001, který sám navedl let American Airlines 11 do Severní věže Světového obchodního centra
[20] Chálid Šajch Muhammad je vysoce postavený člen Al-Ká'idy, hlavním organizátorem teroristických útoků z 11. září 2001
[21] Světové obchodní centrum v New Yorku

Většina mezinárodních teroristických skupin, včetně Al-Káidy využívá pokroky v technologii, jako je optoelektronika (vojenská zařízení pro noční vidění), speciální komunikační zařízení, systémy GPS a další elektronické zařízení.

Teroristická organizace ISIS[22] využívá internet a sociální sítě k rekrutaci nových členů, propagandě a skrze internetové technologie řídí činnost svých operativců v zahraničí. Teroristé své činy horlivě tweetují, streamují a instagramují. Terorismus je takto přenášen po celém světě v reálném čase během několika sekund. Internet je primárním nástrojem, který ISIS používá k lákání a tzv. „vymývání mozků" mladých lidí, aby se připojili k džihádu Islámského státu.

Sociální média se svými nevýhodami byla použita s několika destruktivními online strategiemi pro úspěšný nábor mladých lidí po celém světě. Podle zprávy OSN se odhaduje, že asi 15 000 cizinců se připojilo k ISIS a mnoha extrémním islamistickým skupinám, které sídlí v Iráku a Sýrii.[23]

2.2 Definice kyberterorismu

Při konceptualizaci kyberterorismu rozhodně nelze zapomenout na to, že každá definice a každý případ kyberterorismu musí zároveň spadat i pod obecnější definici terorismu samotného. Celá řada bezpečnostních organizací definuje kyberterorismus i s přihlédnutím k těmto důsledkům, které se vážou k hmotnému světu.

Existuje několik definic pojmu kyberterorismus.

2.2.1 Definice kyberterorismu podle NATO publikovaná P. Everardem

NATO formulovalo v roce 2008 definici kyberterorismu jako: *„A cyberattack using or exploiting computer or communication networks to cause sufficient destruction or distruption to generace fear or to intimidate society into ideological goals"*[24] tedy jako kybernetický útok užívající či zneužívající počítač nebo

[22] Islámský stát je radikální islámská teroristická organizace původem z Iráku
[23] The Guardian*: Hoda Muthana 'deeply regrets' joining Isis and wants to return home* [online]. [cit. 9.2.2022]. Dostupné z: https://www.theguardian.com/world/2019/feb/17/us-woman-hoda-muthana-deeply-regrets-joining-isis-and-wants-return-home
[24] viz str. 118–119, EVERARD, P., *NATO and Cyber Terrorism, In Responses to Cyber Terrorism, In Responses to Cyber Terrorism,* [online]. 2008. [cit. 23.1.2022]. ISBN 978-1-58603-836-6.

komunikační sítě za účelem způsobení dostatečné škody s cílem zastrašit společnost a mající ideologický podtext.

2.2.2 Definice kyberterorismu podle Dorothy E. Denningové

Dorothy E. Denningová je jedním z odborníků na problematiku kyberterorismu právě její definice kyberterorismu je dnes zřejmě tou nejcitovanější:

„Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.“[25]

V překladu je to: Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů. D. E. Denningová pokládá za kyberterorismus pouze teroristické útoky v kyberprostoru proti kritické infrastruktuře a naopak útoky, které nenarušují klíčové služby za akty kyberterorismu nepovažuje. Podle její definice tedy mají kyberútoky jen málokdy za cíl fyzické zničení objektu. Ve skutečnosti však většinou dochází k narušení určitých funkcí nebo jejich součástí a útok tedy není cíleně zaměřen proti vládě. Její definice tedy nevystihuje nejčastější formy útoků. Jako nejpoužívanější definici jevu známého jako kyberterorismus si můžeme zvolit tuto *„Kybernetický terorismus představuje společný střet reálných subjektů ve virtuální realitě v tzv. kyberprostoru (cyberspace).“*[26]

---

[25] viz DENNING, Dorothy E.*,“Cyberterrorism – Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives”,* In: New York: Nova Science Publishers. [online]. 2007 [cit. 23.1.2022]. ISBN: 978-1-60021-709-8.
Dostupné z: https://books.google.cz/books?id=wlDs42YMDIC&pg=PA71&lpg=PA71&dq=Testimony

[26] viz DENNING, Dorothy E.*,“Cyberterrorism,* In: Georgetown University [online], 2000
[cit. 23.1.2022]. Dostupné z: https://www.nato.int/structur/library/bibref/cyberterrorism.pdf

2.2.3 Definice kyberterorismu podle A. Colarika a L. Janczewskiho

„Kybernetický terorismus lze definovat jako představitele aktivit vedených nebo koordinovaných státem s cílem získat informační převahu nebo vyřadit technologickou infrastrukturu protivníka.“[27]

Lech Janczewki a Andrew Colarik pak dále vysvětlují kyberterorismus jako: *„…promyšlený, politicky motivovaný útok sub-státních skupin, tajných agentů nebo jednotlivců proti informačním a počítačovým systémům, počítačovým programům a datům, jehož výsledkem je násilí proti civilním osobám (nebojovým cílům)“*[28]

2.2.4 Definice kyberterorismu podle Národního bezpečnostního úřadu

NBÚ[29] definuje kyberterorismus takto: *„Kyberterorismus zahrnuje agresivní a excesivní jednání, které je prováděno se záměrem vyvolat strach ve společnosti, a jehož prostřednictvím je dosahováno politických, náboženských nebo ideologických cílů. Za využití kyberprostoru a informačních a komunikačních technologií ohrožuje chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy.“*[30]

Jako nejpoužívanější definici jevu známého jako kyberterorismus si můžeme zvolit tuto: *„Kyberterorismus spojuje terorismus a kyberprostor. Chápeme ho jako úmyslný útok proti počítačovým sítím a kritické infrastruktuře za účelem zastrašit nebo donutit vládu a obyvatele k plnění požadavků a cílů teroristické skupiny.“*[31]

---

[27] viz str.229, JANCZEWSKI, L, COLARIK, A. *Managerial Guide For Handling Cyber-Terrorism And Information Warfare*, 2005, London: IGP, ISBN 1-59140-583-1.
[28] viz str. 43, JANCZEWSKI, L., COLARIK, A. *Managerial Guide For Handling Cyber-Terrorism And Information Warfare*. 2005, London: IGP, ISBN 1-59140-583-1.
[29] Národní bezpečnostní úřad
[30] Vzhledem k absenci definice kyberterorismu v českém prostředí vytvořil NBÚ pro potřeby Auditu zcela novou definici.
[31] viz str. 130, JIROVSKÝ, Václav, *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007

2.3 Kyberteroristé a jejich motivace

Kyberterorismus vykonávají aktéři, kteří jsou buď součástí větších teroristických skupin, jako je například dobře známá Al-Káida nebo jednotliví útočníci. Motiv útočníků může být různý, nejčastěji se setkáváme s motivem ekonomickým, sociálním, politickým a ideologickým. S ideologickým pojetím se nejčastěji setkáváme u militantních islamistických skupin.

Kyberteroristé si uvědomují závislosti společnosti na internetu a v důsledku toho jej zneužívají. Komunikace přes internet je efektivní a relativně bezpečná, a je snazší vyhnout se odhalení prostřednictvím šifrovacích komunikačních nástrojů nebo šifrovacích softwarů.

2.4 Důvody kyberterorismu

Útočníci mají mnoho důvodů, proč se uchylují ke kyberterorismu:

- pomáhá oslabit operační schopnosti nepřítele,
- ničí pověst organizace, národa,
- ukazuje, že teroristické skupiny jsou schopny svým cílům způsobit značné škody,
- útočníci přesvědčují napadené, aby změnili způsob myšlení.

Hlavním účelem však bývá způsobit vybraným cílům masivní poškození a maximalizovat škodlivé následky.

Cíle náchylné ke kyberterorismu:

- centra řízení letového provozu,
- navigační systémy na palubách letadel a lodí,
- přehrady,
- elektrárny,
- plynovody,
- ropovody.

Mezi další zranitelné cíle patří vodovodní sítě a dopravní infrastruktura, finanční instituce (banky a burzy), zdravotnická zařízení.

Útoky mohou být byly kvalifikované jako kyberterorismus, pokud budou způsobovat značné ztráty nebo vyvolávat pocit strachu.

2.5 Využití kyberprostoru teroristy

Různé faktory využití kyberprostoru:

- možnosti pro šíření propagandy a rekrutace nových členů,
- kyberterorismus jako nízkonákladový prostředek,
- kyberprostor poskytuje anonymitu,
- možnost zahájit kybernetický útok na jakoukoli odlišnou část světa.

Teroristické organizace využívají kyberprostor k šíření své ideologie a také k rekrutaci nových členů. Rozšíření internetu vedlo k tomu, aby si teroristické organizace vytvořili své virtuální výcvikové tábory. Teroristé využívají internet k tomu, aby oslovili široké masy, které chtějí inspirovat k teroristickým činům.

Kyberterorismus je pro teroristy na rozdíl od fyzického terorismu levný a teroristické skupiny mohou způsobit se stejným množstvím finančních prostředků lidem a společnosti větší škody.

Kyberprostor poskytuje navíc útočníkům anonymitu, čímž umožňuje kyberteroristům skrýt svou identitu.

Internet umožňuje kyberteroristům zahájit kybernetický útok, ať se jejich cíl vyskytuje kdekoliv na světě. Globální propojenost kybernetického prostoru má dále za následek šíření potenciálních cílů, na které mohou teroristé zaútočit, což jej činí nebezpečnějším než jiné teroristické útoky. Útoky mohou mít mnohem větší dosah než kdykoli předtím.

Takovéto bezkonkurenční schopnosti kyberterorismu dávají teroristům mimořádný vliv k tomu, aby způsobili společnosti další škody.

Všudypřítomný kybersvět umožňuje teroristům spouštět kybernetické útoky s dalekosáhlými dopady a způsobující ohromující škody, závažnější než fyzické útoky.

2.6 Metody kyberteroristických útoků

Záměrem kyberteroristických skupin je způsobit masový chaos, narušit kritickou infrastrukturu, podporovat politický aktivismus nebo hacktivismus nebo způsobit fyzické poškození, a dokonce ztráty na životech. Aktéři kyberterorismu používají různé metody. Patří mezi ně následující typy útoků:

Útočníci by nemohli být schopni dosáhnout svého cíle, pokud by neměli vhodné nástroje. Jednotlivým typům útoků pak bude věnována následující kapitola.

Základní rozdělení typů útoků:

- krátkodobé typy útoků,
- dlouhodobé typy útoků.

2.6.1 Krátkodobé typy útoků

Mezi tyto typy řadíme:

- malware,
- DOS útoky,[32]
- ransomware,
- phishingové útoky,
- logické bomby.

K čemu se používají:

- virtuální blokády,
- zamezení přístupu na web,
- krádeže identity/osobních údajů,
- nabourání se do bezpečnostních systémů.

[32] Denial-of-Service attack

2.6.2 Dlouhodobé typy útoků

Teroristické organizace používají následující nástroje zejména k rekrutaci nových členů a propagandě. Blogy pak slouží především k propagandě kyberdžihádu, prostřednictvím kterých jejich tvůrci dále nabádají další lidi, k propagaci nebo dokonce i k jiným aktivním účastem při kyberdžihádu.

Mezi tyto typy řadíme:

- webové stránky,
- sociální sítě – Facebook,[33] Youtube,[34] Twitter,[35]
- blogy – Tumblr,[36]
- online video.

K čemu se používají:

- propaganda,
- rekrutace členů,
- dezinformace,
- zastrašování,
- šíření informací o výrobě zbraní,
- plánování „offline“ útoků.

[33] Facebook je největší online sociální síť, slouží hlavně k tvorbě sociálních sítí, komunikaci mezi uživateli nebo sdílení multimediálních dat.
About Facebook [online]. [cit. 21.1.2022 [online]. Dostupné z: https://about.facebook.com
[34] Youtube je největší internetový server pro sdílení videosouborů, založený v únoru 2005 Youtube.
About Youtube. [online]. [cit. 21.1.2022]. Dostupné z: https://about.youtube
[35] Twitter je poskytovatel sociální sítě a mikroblogu Twitter. Místo všeho dění.
About Twitter [cit. 25.1.2022]. Dostupné z: https://about.twitter.com
[36] Tumblr je americká sociální síť pro mikroblogování a
Tumblr [online]. [cit. 25.1.2022]. Dostupné z: https://www.tumblr.com

3. TYPY KYBERNETICKÝCH ÚTOKŮ

3.1 Malware

Malware je typ škodlivého programu, který vytváří útočníkovi tajný přístup do vašeho zařízení. Tento škodlivý program využívá zranitelnost k narušení sítě. Uživatel klikne na nebezpečný odkaz nebo přílohu e-mailu, která slouží k instalaci škodlivého softwaru do systému. Malware zahrnuje různé typy útoků včetně spywaru, virů a červů.

Malware a škodlivé soubory v počítačovém systému mohou:

- odepřít přístup ke kritickým součástem sítě,
- získat informace načtením dat z pevného disku nebo paměti,
- narušit systém nebo jej dokonce vyřadit z provozu,
- kompromitovat osobní údaje.

3.1.1 Viry

Škodlivé programy, které se dokáží šířit bez vědomí uživatele. Virus se replikuje a infikuje další kód v počítačovém systému.[37] Počítačový virus je získává kontrolu nad počítačovým systémem a poté poškozuje PC uživatele. Nejčastěji se šíří viry prostřednictvím e-mailu. Pokud otevřeme nakaženou přílohu e-mailu a klikneme na odkaz vedoucí na infikovanou webovou stránku, tak tím stáhneme a spustíme zavirovaný soubor.

3.1.2 Trojské koně

Tyto škodlivé programy se ukrývají uvnitř počítačových programů. Je to nejčastější typ malwaru. Na první pohled se tváří neškodně se škodlivými účely. Na rozdíl od virů se trojský kůň nereplikuje a běžně se používá k vytvoření zadních vrátek, které mohou útočníci zneužít. Trojský kůň je často šířen infikovanými e-mailovými přílohami, pokud na ně uživatel klikne, spustí se program (trojský kůň).[38]

[37] *Eset: Co je počítačový virus?* [online]. [cit. 14.2.2022]. Dostupné z: https://www.eset.com/cz/virus/
[38] *Avast: Co je to Trojský kůň?* [online]. [cit. 14.2.2022]. Dostupné z: https://www.avast.com/cs-cz/c-trojan

3.1.3 Červi

Škodlivé programy, na rozdíl od virů neútočí na hostitele, jsou to samostatné programy, které se šíří po sítích a počítačích. Počítačoví červi jsou schopni posílat kopií sebe sama na jiné počítače. Červi se často instalují prostřednictvím e-mailových příloh a posílají svou kopii každému kontaktu v seznamu e-mailů infikovaného počítače. Běžně se používají k přetížení e-mailového serveru a dosažení útoku typu denial-of-service.

3.1.4 Ransomware

Je druh škodlivého programu, který blokuje počítačový systém nebo šifruje data v něm zapsaná, a pak požaduje od oběti výkupné za obnovení přístupu. Název je složený z anglických slov „ransom“ - výkupné“ a software.

Nejznámějším ransomware útokem byl WannaCry, který se odehrál v roce 2017 ve Velké Británii a zaměřil se na britskou Národní zdravotní službu (NHS).[39] Hackerům se tehdy podařilo infikovat nejméně 16 zdravotních středisek a 200 000 počítačů a ochromilo více než 1 200 kusů diagnostických zařízení. Tento ransomwarový útok se rozšířil prostřednictvím počítačů s operačním systémem Microsoft Windows. Soubory uživatele byly drženy jako rukojmí a za jejich vrácení bylo požadováno výkupné v bitcoinech.

3.1.5 Spyware

Spyware je typ škodlivého špehovacího malwaru, který je velice těžké odhalit. Tajně sbírá informace o historii prohlížených stránek nebo jiné osobní údaje (například čísla kreditních karet) a získané informace Často posílá bez našeho vědomí třetím stranám. Útočník pak může použít informace pro účely vydírání nebo stáhnout a nainstalovat další škodlivé programy z webu.[40]

3.2 Phishing

Phishing znamená česky rybaření a spočívá v tom, že kyberzločinci rozešlou „návnady“ (e-mailové zprávy), a doufají, že „uloví“ nějaké oběti.

---

[39] National Health Service

[40] *Avast: Co je spyware?* [online]. [cit. 14.2.2022]. Dostupné z: https://www.avast.com/cs-cz/c-spyware

Tento pojem zahrnuje způsob zasílání podvodných zpráv, které vypadají, že pocházejí z důvěryhodného zdroje. Obvykle se provádí prostřednictvím e-mailu. Cílem útočníků je ukrást citlivá data, jako jsou údaje z kreditních karet, přihlašovací údaje nebo nainstalovat malware do počítače oběti.[41]

Kybernetičtí zločinci používají phishingové e-maily, protože tato metoda je levná, snadná a efektivní. Získat e-mailové adresy je pro útočníky snadné a rozesílání e-mailů je prakticky zdarma. S malým úsilím a malými náklady mohou phisheři rychle získat přístup k cenným datům. Útočníci se snaží své útoky stále vylepšovat a optimalizovat.

Phishingové útoky mohou probíhat také prostřednictvím sociálních sítí a dalších online komunit, prostřednictvím přímých zpráv od jiných uživatelů se skrytým záměrem. Útočníci často využívají sociální inženýrství a další veřejné informační zdroje ke shromažďování informací o zájmech a aktivitách oběti, což jim dává výhodu důvěryhodné identity.

Existuje několik různých typů phishingových útoků:

3.2.1 Spear Phishing

Spear Phishing je metoda phishingu, která se zaměřuje na konkrétní skupiny nebo jednotlivce na rozdíl od klasického phishingu, který doručuje hromadné e-maily náhodným příjemcům. Účelem je získat přístup k tajným informacím. Typický spear phishingový e-mail obsahuje nejen odkaz, ale i přílohu.

3.2.2 Whaling[42]

Útočníci se při těchto útocích vydávají za vedoucí pracovníky organizace. Ve phishingových e-mailech žádají podřízené o sdělení citlivých interních informací, které následně zneužijí. Tyto akce mohou zahrnovat zasílání finančních výkazů, podvodných odkazů nebo dokonce platební příkazy peněz na neznámé účty.

---

[41] *Cisco: Co je phishing?* [online]. [cit. 14.2.2022].
Dostupné z: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html
[42] Česky velrybářství, lov velryb

3.2.3 Pharming

Pharming využívá napadení mezipaměti DNS k zachycení přihlašovacích údajů uživatele prostřednictvím falešné přihlašovací vstupní stránky.

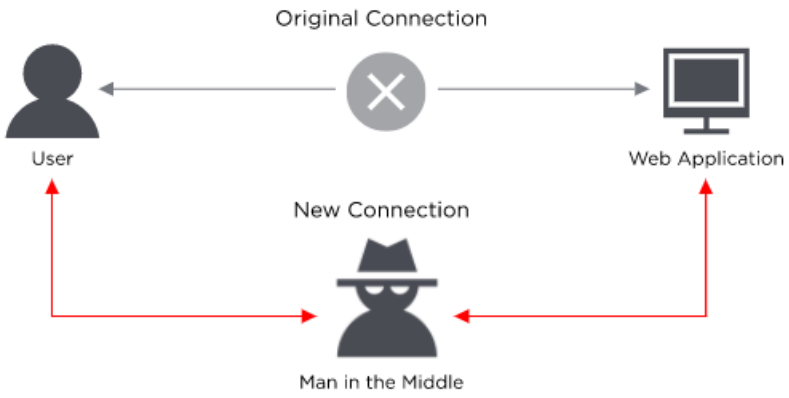
3.2.4 Další typy phishingu

Phishingové útoky mohou probíhat také prostřednictvím hlasové a mobilní komunikace. Útočníci při těchto formách útoků využívají ke krádeži informací:

- hlasové zprávy (voice phishing nebo vishing),
- textové zprávy (SMS phishing nebo smishing).

3.3 Man-in-the-Middle (MitM) útoky

Jsou to typy odposlouchávacích útoků, které útočníkům umožňují zachytit komunikaci mezi dvěma cíli. Útočník vstoupí do komunikace mezi dva subjekty a převezme nad ní kontrolu. Při této formě útoku manipuluje s oběma stranami a získá přístup k datům nebo citlivým informacím. Útoky tohoto typu představují vážný bezpečnostní problém.[43]



Obrázek 1: Man-in-the-Middle útok

Laicky řečeno, útočník (MitM) je ekvivalentem poštovního doručovatele, který otevře náš bankovní výpis, zapíše si citlivé informace, poté obálku znovu zalepí a doručí nám ji do schránky.

[43] *Veracode: What Is a Man-in-the-Middle Attack?* [online]. [cit. 14.2.2022]. Dostupné z: https://www.veracode.com/security/man-middle-attack

Cílem MitM útoku je ukrást osobní údaje, jako jsou přihlašovací údaje, údaje o účtu a čísla kreditních karet.

3.4 Denial-of-Service (DOS) útok

DOS[44] útok se snaží zabránit legitimním uživatelům v přístupu k cílovým počítačovým systémům, zařízením nebo jiné počítačové síti. Kyberútočníci v tomto případě zahltí koncové prvky žádostmi o zpracování a tím je vyřadí z provozu. Terčem se často stávají vládní instituce, úřady nebo informační systémy veřejné správy.

3.5 SQL injection

SQL injection je typem útoku, při kterém útočník vloží škodlivý kód na server pomocí jazyka SQL[45], čímž server přinutí vydat chráněné informace. Tento typ útoku obvykle zahrnuje odeslání škodlivého kódu do nechráněného komentáře na webu nebo vyhledávacího pole. Postupy bezpečného kódování, jako je použití připravených příkazů s parametrizovanými dotazy, jsou účinným způsobem, jak zabránit injekcím SQL. Tento typ útoku může vést k neoprávněnému přístupu k citlivým datům, jako jsou hesla, údaje o kreditních kartách nebo osobní údaje uživatele.

3.6 Zero-day Exploit

Tento pojem označuje kybernetický útok zaměřený na dosud neznámou zranitelnost softwaru. Útočník využije k útoku programátorské chyby tzv. zero-day exploit. K útoku nultého dne dojde, jakmile je tato chyba nebo zranitelnost softwaru zneužita. Útočníci napadnou systém dříve, než má vývojář příležitost vytvořit záplatu k opravě zranitelnosti softwaru. Útoky zero-day jsou závažnou bezpečnostní hrozbou, je obtížné se jim bránit a mají vysokou pravděpodobnost úspěšnosti.[46]

---

[44] Denial-of-Service attack
[45] Server query language
[46] *Impreva: Co je zero-day (0day) exploit?* [online]. [cit. 14.2.2022].
Dostupné z: https://www.imperva.com/learn/application-security/zero-day-exploit/

Typické cíle zero-day exploit jsou:

- webové prohlížeče,
- operační systémy,
- kancelářské aplikace (MS Office),
- hardware, obsahující firmware.

3.7 Password Attack

Password Attack[47] je útokem, kdy se útočníci pokouší ukrást heslo. Je to proces k získání správného hesla k účtům neoprávněným způsobem

Útočníci často používají různé techniky k prolomení nebo uhodnutí hesel.[48]

3.7.1 Brute Force[49]

Tento způsob je nejčastějším typem útoku. Útočník použije software, zaměřený na automatické generování hesel, který zkouší všechny možné varianty a kombinace k prolomení hesla.

3.7.2 Dictionary attack[50]

Útočníci využívají běžných slov nebo krátkých hesel v kombinaci s čísly nebo speciálními znaky, které doplňují před nebo za hesla.

3.7.3 Keylogger Attack

Útočníci používají škodlivý software (spyware), který běží na pozadí operačního systému a zaznamenává stisky kláves provedených uživatelem. Díky nim dokáže zjistit uživatelská jména, hesla a webové stránky nebo aplikace, kde jsou tyto přihlašovací údaje použity.

3.8 Cross-site Scripting

Tento pojem označuje útok, který spočívá ve vkládání kódu do webové stránky nebo webové aplikace. K útoku dojde, když uživatel navštíví webovou stránku nebo webovou aplikaci, která spouští škodlivý kód. Webová stránka nebo webová

---

[47] útok heslem
[48] *BlueVoyant: Different types of password attacks and how they work.* [online]. [cit. 14.2.2022]. Dostupné z: https://www.bluevoyant.com/blog/password-attacks-and-prevention/
[49] útok hrubou silou
[50] slovníkový útok

aplikace se stává prostředkem pro doručení škodlivého skriptu do prohlížeče uživatele. Obvykle se tento škodlivý kód skládá z kódu Javascript spuštěného prohlížečem oběti, ale může zahrnovat Flash, HTML a XSS. Zranitelnými prostředky, které se běžně používají pro útoky Cross-site Scripting, jsou fóra, nástěnky a webové stránky, které umožňují komentáře.[51]

3.9 Rootkity

Rootkity jsou zákeřné počítačové programy určené k provádění široké škály škodlivých činností. Jsou instalovány uvnitř legitimního softwaru, kde mohou získat vzdálenou kontrolu a přístup k systému na úrovni správy. Útočník pak použije rootkit ke krádeži hesel, klíčů, přihlašovacích údajů a získání důležitých dat.[52]

3.10 Logické bomby

Logické bomby jsou škodlivé aplikace, které se za určitých podmínek samy spustí. Skládají se ze dvou základních částí – rozbušky a akce. Na rozdíl od virů a červů, které mohou infikovat systém samy o sobě, jsou logické bomby často vloženy někým, kdo má vnitřní znalosti systému. Kvalitní logické bomby jsou velmi zákeřné a je obtížné je odhalit.

[51] *Acunetix: Cross-site Scripting*. [online]. [cit. 14.2.2022].
Dostupné z: https://www.acunetix.com/websitesecurity/cross-site-scripting/
[52] *Avast: Co je to rootkit?* [online]. [cit. 14.2.2022]. Dostupné z: https://www.avast.com/cs-cz/c-rootkit

4. TAXONOMIE KYBERÚTOČNÍKŮ

Kybernetické útoky představují pro všechny vysoké riziko, je třeba s ním počítat a dostatečně se proti němu bránit.

V souvislosti s kybernetickými útoky se můžeme setkat s pojmy hacker a cracker. Tyto dva pojmy označují ty, kteří se snaží proniknout do počítačového systému. Hackeři a crackeři mají odlišné zájmy a cíle.

Hackeři chrání systém před škodlivými útoky, pronikají do systému, aby ho chránili. Crackeři jsou ti, kteří představují pro systém hrozbu, chtějí systém poškodit a získaná data zneužít ke svému prospěchu.

Zjednodušeně se dají hackeři nazývat dobrými lidmi, protože své znalosti využívají k dobrému účelu a nepoškozují data, crackeři špatnými, protože se nabourávají do systému a své znalosti zneužívají.[53]

Útočníky můžeme rozdělit do několika skupin:

- začátečníci,
- aktivisté,
- kybernetičtí zločinci,
- interní útočníci,
- státní aktéři.

4.1 Začátečníci – script kiddies

Tento termín označuje méně zkušené útočníky bez větších technických znalostí, kteří používají nástroje volně dostupné na internetu. Tito útočníci obvykle nerozumí vnitřnímu fungování softwaru a počítačových sítí. Pro své útoky používá již naprogramované skripty, v nichž je potřeba zadat pouze cílovou adresu serveru nebo počítače, na který bude útok prováděn. Tito útočníci bývají motivováni zvědavostí, snahou o získání zkušeností nebo uznání okolí. Pravděpodobnost jeho odhalení je tedy vzhledem k nízkým zkušenostem vysoká.[54]

---

[53] *Jigsaw Academy: Difference Between Hacker And Cracker – An Easy Overview* [online]. [cit. 9.2.2022.]. Dostupné z: https://www.jigsawacademy.com/blogs/cyber-security/difference-between-hacker-and-cracker/

[54] *Axians.cz: Kybernetická bezpečnost – Jak probíhá kybernetický útok?* [online]. [cit. 9.2.2022.]. Dostupné z: https://www.axians.cz/cs/novinky/jak-probiha-kyberneticky-utok/

4.2 Aktivisté (hacktivists)

Tento termín označuje útočníky, kteří se snaží prosadit své politické názory prostřednictvím útoků na informační infrastrukturu. Hacktivisté mohou být motivováni politickými názory, kulturním/náboženským přesvědčením, národní hrdostí nebo teroristickou ideologií.[55]

Mezi nejznámější hacktivistické skupiny patří „Anonymous“, která provedla stovky kybernetických útoků.

4.3 Kybernetičtí zločinci (cybercriminals)

Tento termín označuje útočníky, kteří páchají počítačové trestné činy. Počítač používají jako nástroj nebo jako cíl útoku. Tito útočníci mají finanční motivaci. Útoky směřují na velký počet uživatelů, často se zaměřují na konkrétní organizace.[56]

4.4 Interní útočníci (insiders)

Tento termín označuje útočníky, kteří útočí na systém zevnitř organizace. Znají interní síť organizace a mají do ní přístup. Často se jedná o nespokojeného nebo bývalého zaměstnance. Motivem takového útočníka bývá pomsta nebo osobní prospěch.[57]

4.5 Státní aktéři (state-sponsored attackers)

Tento termín označuje útočníky, kteří mají většinou výborné technologické znalosti a útočníci používající přesně cílené útoky a pokročilé techniky. Jsou to profesionální hackerské skupiny, u nichž se předpokládá, že jsou řízeny různými státy a věnují se špionáži. Útočníci jsou schopni se delší dobu pohybovat v napadených sítích, aniž by byli odhaleni. Obrana proti těmto útokům je velmi složitá.[58]

---

[55] *ScienceDirect: Hactivists* [online]. [cit. 09.02.2022].
Dostupné z: https://www.sciencedirect.com/topics/computer-science/hacktivists
[56] *Axians.cz: Kybernetická bezpečnost – Jak probíhá kybernetický útok?* [online]. [cit. 9. 2 2022.].
Dostupné z: https://www.axians.cz/cs/novinky/jak-probiha-kyberneticky-utok/
[57] tamtéž
[58] tamtéž

5. KYBERDŽIHÁD

Termín kyberdžihád nemá žádnou ustálenou definici. Nejpřesněji vystihuje tento pojem toto vyjádření: Kyberdžihád je jakákoliv muslimská aktivita, která je zprostředkována online. Může zahrnovat i kyberterorismus, rekrutaci, shromažďování informací, trénink a šíření propagandy a vojenských informací.[59]

První kyberdžihád realizovali pro-palestinští a pro-izraelští hackeři v letech 1999–2000. Kyberdžihádisté využívají své počítačové dovednosti k tomu, aby se nabourali se do serverů společností a dalších organizací, aniž by o tom tyto společnosti věděli.[60]

Aktéry v oblasti kyberdžihádu jsou převážně muslimové. Skrze internet si navzájem posílají zprávy, které mohou obsahovat instrukce, jak vyrobit bombu a na koho má být následně zacílená. Dále skrze internet provádějí propagandu.

Nejčastěji se jedná o členy těch nejznámějších teroristických skupin Al-kaidy a IS.[61] Tyto skupiny využívaly intenzivně internet k přípravě svých teroristických útoků.

5.1 Techniky a taktiky kyberdžihádistů

Kyberdžihádisté využívají internet prostřednictvím různých bezplatných a široce dostupných technologií. Využívají své počítačové dovednosti k tomu, aby se nabourali se do serverů společností a dalších organizací, aniž by o tom tyto společnosti věděly.[62]

Možností, prostřednictvím kterých teroristé realizují kyberdžihád, nabízí internet mnoho. Mezi nejčastější taktiky, které teroristé používají, patří hlavně e-mail, diskuzní fóra a blogy.

IS nadále těží z kořenů již tak vysoce rozvinuté komunikační strategie Al-Kájdy.

IS má propracovanou a efektivní komunikační strategii, která využívá nástroje online médií k šíření své multidimenzionální propagandy. Zaplnila platformy

---

[59] GLAZOV, Jamie. FrontPageMagazine.com. *Symposium: Cyber Jihad.* [online]. 2008 [cit. 21.1.2022]. Dostupné z: http://archive.frontpagemag.com/readArticle.aspx?ARTID=30072

[60] *Jihadi.org: What is Cyber-Jihad?* [online]. [cit. 21.1.2022]. Dostupné z: http://www.jihadi.org/p/what-is-cyber-jihad.html

[61] Islámský stát

[62] KOHLMANN, Evan F. WASH. *Online Discussion: Al Qaeda and the internet?* [online]. [cit. 21.1.2022]. Dostupné z: https://www.jstor.org/stable/20032074

sociálních médií a přilákala globální síť příznivců, kteří formulují, zvětšují a šíří její násilné extremistické zprávy po celém světě.

IS strategicky nabírá mladé muže a ženy po celém světě pomocí internetových stránek, online magazínů, ale především nástrojů sociálních médií, včetně Facebooku, YouTube, Twitteru, Instagramu a Ask.FM.[63]

[63] lotyšská sociální síť

6. KYBERTERORISMUS A KYBERNETICKÁ BEZPEČNOST

6.1 Kybernetická bezpečnost

Termín, který zastřešuje široké spektrum bezpečnostních oblastí, zahrnuje všechny preventivní a reaktivní aktivity státu v oblasti ochrany dat, informací, systémů, služeb a sítí.

S růstem významu informačních a komunikačních technologií v dnešní společnosti, dochází také ke koncipování nových organizací, které se aktivně zabývají kybernetickou bezpečností. Mimo jiné dochází k budování bezpečnostních týmů, tzv. CERT[64]. Jedná se o tým, který je zodpovědný za řešení kybernetických bezpečnostních incidentů, tedy místo, na které se mohou orgány a osoby obrátit se zjištěným kybernetickým bezpečnostním incidentem nebo i jen podezřením.

Zákon o kybernetické bezpečnosti rozumí kybernetickou bezpečností: *„Kybernetickou bezpečností se rozumí souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění nerušeného a bezvadného fungování kybernetického prostoru.“*[65]

6.2 Kybernetická bezpečnost v ČR

Základním dokumentem pro zajišťování kybernetické bezpečnosti v ČR je BS 2015[66], na kterou navazuje Národní strategie kybernetické bezpečnosti na období let 2021 až 2025 (Strategie), jakožto stěžejní dokument upravující strategický rámec zajišťování kybernetické bezpečnosti v ČR. Ze Strategie vychází Akční plán kybernetické bezpečnosti ČR na období let 2021 až 2025 (Akční plán), který definuje konkrétní úkoly, stanovuje u nich zodpovědnost, termíny jejich plnění a kontrolu.

Zahrnuje především preventivní opatření reaktivního charakteru vůči napadeným subjektům v případě kybernetických bezpečnostních incidentů.

---

[64] Computer Emergency Response Team
[65] viz § 2 písm. b), Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
[66] Bezpečnostní strategie 2015

Gestorem kybernetické bezpečnosti v ČR je za „normálního“ stavu, stavu nouze a stavu kybernetického nebezpečí NBÚ.[67]

Za stavu ohrožení státu a ve válečném stavu je gestorem kybernetické bezpečnosti Vojenské zpravodajství.[68]

6.3 Stav kybernetického nebezpečí

„Stavem kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací[69], a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.“[70]

Tento stav je možné vyhlásit, pokud jsou bezpečnost informací v IS[71], bezpečnost služeb nebo sítí elektronických komunikací ohroženy v takovém rozsahu, že tím dojde k ohrožení nebo porušení zájmu ČR. Stav kybernetického nebezpečí vyhlašuje ředitel NBÚ nejdéle na 7 dnů s možností prodloužení v souhrnu na nejvýše 30 dnů.

---

[67] Národní bezpečnostní úřad

[68] Vojenské zpravodajství je jednotnou ozbrojenou zpravodajskou službou ČR integrující rozvědnou a kontrarozvědnou činnost. Základním úkolem Vojenského zpravodajství je získávat, shromažďovat a vyhodnocovat informace důležité pro obranu České republiky. Vojenské zpravodajství je přímou součástí Ministerstva obrany. V jeho čele stojí ředitel, který je z výkonu své funkce odpovědný ministru obrany. *Vojenské zpravodajství: Zabezpečujeme informace v oblasti obrany* [online]. [cit. 21.1.2022]. Dostupné z: https://vzcr.cz

[69] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů [online]. [cit. 21.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-127

[70] Zákon č. 181/2014 S., o kybernetické bezpečnosti [online]. [cit. 21.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[71] Informační systém

7. LEGISLATIVA KYBERNETICKÉ BEZPEČNOSTI V ČR

Moderní doba s sebou přináší řadu výhod, ale také nová rizika a hrozby v oblasti kybernetické bezpečnosti.

„Kybernetickou bezpečnost tedy právo vnímá jako ochranu národního kyberprostoru před bezpečnostními hrozbami. Jednotlivé bezpečnostní incidenty samozřejmě mohou dosáhnout takové intenzity, že se negativně projeví v národním měřítku, tj. dojde například k výpadku páteřní sítě.“[72]

Stěžejním zákonem v oblasti kybernetické bezpečnosti je **zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů** (ZKB) a podzákonných předpisech, které úpravu tohoto zákona dále rozvíjejí.

Cílem ZKB je zvýšit bezpečnost kyberprostoru a snažit se chránit tu část infrastruktury, která je důležitá pro fungování státu a jejíž narušení by mělo za následek poškození nebo ohrožení zájmu ČR.

Zákon zavádí nové pojmy jako např. kybernetický prostor, kritická informační infrastruktura,[73] významný informační systém,[74]významná síť,[75] kybernetická bezpečnostní událost,[76] kybernetický bezpečnostní incident.[77]

Tento zákon v § 3 vymezuje orgány a osoby, kterým ukládá povinnosti v oblasti kybernetické bezpečnosti, upravuje způsob zajištění kybernetické bezpečnosti, definuje kybernetickou bezpečnostní událost, určuje činnost NBÚ a vymezuje dohledová pracoviště vládní CERT a národní CERT (vládní/národní CERT) a v neposlední řadě zavádí stav kybernetického nebezpečí, který vyhlašuje, jak už bylo řečeno ředitel NBÚ.

---

[72] viz *CyberSecurity.CZ: Legislativa v české republice* [online]. [cit. 21.1.2022]. Dostupné z: https://cybersecurity.cz/law.html

[73] prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti (tato oblast je definována novelizací Nařízení vlády č. 432/2010 Sb.)

[74] informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci (§ 2 písm. d), Zákon č. 181/2014 Sb., o kybernetické bezpečnosti)

[75] síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře (§ 3 písm. b Zákon č. 181/2014 Sb., o kybernetické bezpečnosti)

[76] událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací

[77] narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události

V roce 2017 proběhla prostřednictvím zákona č. 205/2017 Sb. novelizace ZKB[78] s účinností od 1. srpna 2017, následně byly provedeny další změny. Poslední novelizace proběhla v roce 2021 zákonem č. 261/2021 Sb. Aktuální znění zákona je účinné od 1. září 2021.

Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).[79]

Vyhláška stanovuje náležitosti hlášení kybernetických bezpečnostních incidentů, kontaktních údajů dále konkretizuje bezpečnostní opatření uvedené v § 5 ZKB, a stanovuje rozsah a strukturu bezpečnostní dokumentace.

Vyhláška č. 360/2020 Sb., vyhláška, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb.[80]

Důvodem novelizace této vyhlášky bylo zjednodušení a zpřesnění procesu identifikace VIS[81] a odstranění pochybností o tom, které informační systémy orgánů veřejné moci spadají do rozsahu regulace zákona o kybernetické bezpečnosti.[82]

Dále v oblasti kybernetické bezpečnosti působí normy práva ústavního, občanského, trestního, správního a autorského.

---

[78] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti [online]. [cit. 21.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[79] Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti [online]. [cit. 21.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-316

[80] Vyhláška č. 360/2020 Sb., vyhláška, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb. [online]. [cit. 21.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317

[81] významné informační systémy

[82] *Národní úřad pro kybernetickou a informační bezpečnost:* Nová pravidla pro určování významných informačních systémů [online]. [cit. 21.1.2022]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1627-nova-pravidla-pro-urcovani-vyznamnych-informacnich-systemu/

8. AKTÉŘI PŮSOBÍCÍ V OBLASTI PROBLEMATIKY KYBERNETICKÉ BEZPEČNOSTI

Pro ochranu kyberprostoru je potřeba zřizovat odpovědné instituce a orgány, které vykonávají určené činnosti, v oblasti kybernetické bezpečnosti.

8.1 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Ústředním orgánem v oblasti je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Tento úřad spadá pod NBÚ, který je gestorem kybernetické bezpečnosti v ČR za „normálního“ stavu, stavu nouze a stavu kybernetického nebezpečí. Úřad vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).“[83]

„Národní úřad pro kybernetickou a informační bezpečnost je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galileo.“[84]

Výkonnou sekcí úřadu je Národní centrum kybernetické bezpečnosti (NCKB). Ředitel NÚKIB se pravidelně účastní jednání Bezpečnostní rady státu (BRS) a je členem Výboru pro kybernetickou bezpečnost, který je stálým pracovním orgánem BRS pro koordinaci plánování opatření k zajišťování kybernetické bezpečnosti České republiky.

8.2 Národní centrum kybernetických operací NCKO

Bylo vybudováno na základě vládního akčního plánu ke kybernetické bezpečnosti z roku 2015. Úkolem centra je vytvoření účinného systému obrany v kybernetickém prostoru tak, aby Česká republika byla schopna zastavit a případně odvrátit kybernetické útoky, a tím zabezpečit ochranu civilního obyvatelstva a infrastruktury.[85]

---

[83] *Národní úřad pro kybernetickou a informační bezpečnost: O NÚKIB* [online]. [cit. 20.1.2022]. Dostupné z: www.govcert.cz

[84] tamtéž

[85] Centrum kybernetické bezpečnosti: Národní centrum kybernetických operací: Centrum kyberobrany představilo svou strategii do roku 2022 – Centrum kybernetické bezpečnosti [online]. [cit. 23.1.2022].

„Národní centrum kybernetických operací (NCKO) vypracovalo Strategii kybernetické obrany České republiky pro období 2018–2022, která stanovuje koncepční podmínky pro zajišťování obrany státu v kybernetickém prostoru. Dokument definuje základní vizi a cíle, které popisují plánovaný vývoj kybernetické obrany v jednotlivých dílčích oblastech.“[86]

8.3 Dohledová bezpečnostní pracoviště

ČR má zřízena dvě dohledová bezpečnostní pracoviště. Jsou jimi vládní CERT[87] a národní CERT. Tato pracoviště mají důležitou roli při ochraně kritické informační infrastruktury a významných informačních systémů. Byla zřízena podle zákona o kybernetické bezpečnosti.

Základní úlohou těchto týmů je řešení a koordinace bezpečnostních incidentů, osvětová a školící činnost a proaktivní služby v oblasti bezpečnosti pro orgány státu, organizace i občany.

- **Vládní CERT**, nazývaný též GovCERT.CZ, provozuje NÚKIB.[88]
- **Národní CERT** provozuje sdružení CZ.NIC dle veřejnoprávní smlouvy a zákona o kybernetické bezpečnosti.[89]

Dostupné z: https://centrumkyberbezpecnosti.cz/centrum-kyberobrany-predstavilo-svou-strategii-do-roku-2022/

[86] viz Vojenské zpravodajství: *Kybernetická obrana: Vojenské zpravodajství zajišťuje kybernetickou obranu* české republiky [online]. [cit. 22.1.2022]. Dostupné z: https://vzcr.cz/kyberneticka-obrana-46

[87] CERT – Computer Emergency Responce Team – Počítačový team nouzové reakce

[88] *Národní úřad pro kybernetickou a informační bezpečnost: Kybernetická bezpečnost – Vládní CERT* [online]. [cit. 23.01.2022]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/

[89] *CZ.NIC: CSIRT.CZ Národní CSIRT České republiky* [online]. [cit. 23.1.2022]. Dostupné z: https://www.csirt.cz/cs/

9. ADVANCED PERSISTENT THREAT (APT)

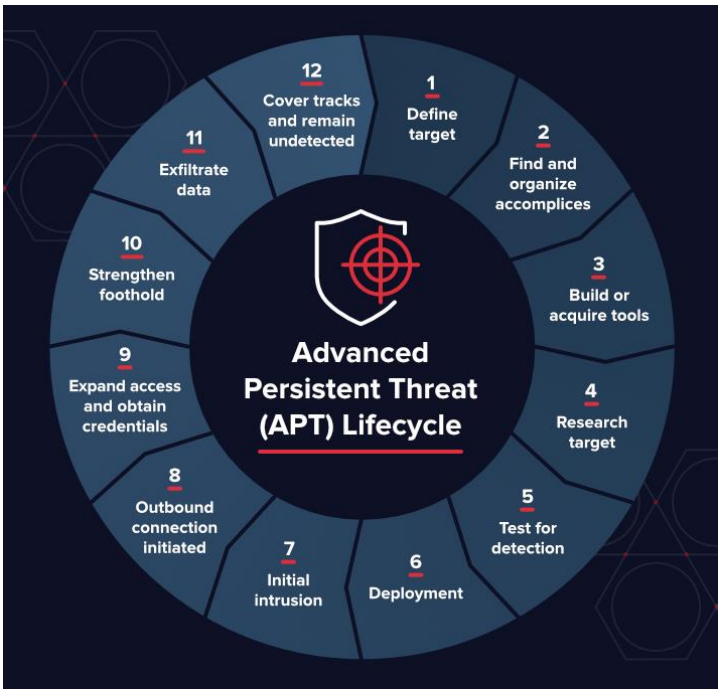
Vzhledem k tomu, že se chci v této části práce věnovat vybraným APT[90] útokům, je třeba si nejprve říci pár slov o tom, co to vlastně APT útoky jsou, kdo a je provádí.

APT útok je označením pro jeden z nejnebezpečnějších typů kybernetických útoků současnosti. Tyto útoky mají specifické rysy, které je odlišují od ostatních typů kybernetických hrozeb.

APT může mít s kyberterorismem a kybernetickou kriminalitou společných poměrně dost znaků.

Tyto útoky jsou typem útočné kampaně, které provádí obvykle skupiny zkušených kyberzločinců – hackerů, kteří jsou sponzorování organizací nebo dokonce vládou za účelem zisku citlivých dat/zásadních informací. Některé útoky APT jsou financované vládou a používané jako kybernetické válečné zbraně.

Na obrázku 2 vidíme životní cyklus pokročilé trvalé hrozby.[91]



Obrázek 2: Pokročilá trvalá hrozba – životní cyklus

[90] APT – Advanced Persistent Threat (pokročilá trvalá hrozba)
[91] *Varonis: What is an Advanced Persistent Threat (APT)* [online]. [cit. 10.2.2022]. Dostupné z: https://www.varonis.com/blog/advanced-persistent-threat

Americký Národní institut standardů a technologie (NIST)[92] APT definuje takto: *„Protivník, který má sofistikované odborné znalosti a zdroje, které mu umožňují vytváření příležitostí k dosažení svých cílů pomocí více útočných vektorů. Tyto cíle obvykle zahrnují zakládání a rozšiřování zázemí v informačně-technologické infrastruktuře vybraně organizace za účelem exfiltrace informací či bránění kritickým aspektům mise, programu či organizace. Advanced persistent threat: (1) opakovaně sleduje své cíle v průběhu dlouhého časového období; (2) přizpůsobuje se obranným kapacitám cíle; (3) je odhodlá udržovat úroveň interakce, která je potřebná pro dosažení jeho cílů.“*[93]

Útočníci využívají široké spektrum technologií a technik pro vniknutí do daného zařízení či sítě. Jen tak se nevzdají, když se dostanou do systému, snaží se v něm zůstat co nejdéle.

Advanced persistent threat se skládá ze 3 pojmů:

- **Advanced**[94]
- **Persistent**[95]
- **Threat**[96]

9.1 Fáze APT útoku[97]

Příprava

V přípravné fázi anglicky nazývané reconnaissance[98] útočníci analyzují veřejně dostupné informace a hledá zranitelnosti subjektu, který je jeho cílem.

---

[92] NIST – National Institute of Standards and Technology NIST je laboratoř měřicích standardů při ministerstvu obchodu USA. Cílem instituce je podpora inovací a průmyslové konkurenceschopnosti USA zlepšováním vědeckých měření, standardů a technologie s ohledem na ekonomickou bezpečnost a zlepšování kvality života.

[93] viz *National Institute of Standards and Technology*: Managing Information Security Risk: Organization, Mission and Information System View [online]. [cit. 9.2.2022]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[94] pokročilý

[95] vytrvalá

[96] hrozba

[97] *Clever&Smart Management: APT: Jak probíhá cílený útok* [online]. [cit. 4.2.2022]. Dostupné z: https://www.cleverandsmart.cz/apt-jak-probiha-cileny-utok/

[98] průzkum

Infiltrace

Ve druhé fázi infiltraci neboli průniku dochází k infiltraci a spuštění škodlivého kódu do zařízení, které jsou organizací používány pro přístup k interním systémům, ze kterých je v další fázi veden útok na další zařízení v síti organizace. Útočníci používají nejčastěji spear phishing obsahující přílohu s exploitem nebo jen prostý e-mail s odkazem na stránky, na kterých se nachází nějaký ten drive-by download malware.

Kompromitace

Ve třetí fázi útoku nazývané též jako data gathering,[99] tedy ve fázi, kdy už útočník ovládl zařízení, dochází k tomu, že útočník z tohoto ovládaného zařízení vyhledává další systémy v síti organizace, snaží se zajistit si vzdálený přístup a tyto systémy kompromitovat.

Dokončení

Dokončení je závěrečná fáze, nazývaná též exfiltration.[100] V této fázi dochází k dokončení APT útoku. Útočníci často napadenou organizaci vydírají a vyhrožují zveřejněním nebo prodejem citlivých informací konkurenci. Není také výjimkou, že útočníci vyhrožují, že data smažou nebo zašifrují a požadují „výkupné“ za poskytnutí dešifrovacího klíče.

Na obrázku 3 jsem graficky znázornila fáze APT útoku.[101]

Obrázek 3: Fáze APT útoku

Důsledky APT útoků jsou rozsáhlé a zahrnují:

- krádeže duševního vlastnictví (např. obchodní tajemství nebo patenty),
- prolomené citlivé informace (např. soukromé údaje zaměstnanců a uživatelů),
- sabotáž kritických organizačních infrastruktur (např. mazání databáze),
- celkové převzetí webových stránek.

[99] sběr dat
[100] exfiltrace
[101] vlastní zpracování

9.2 Aktéři APT

Aktéři stojící za APT útoky jsou typicky skupiny zkušených hackerů pracující koordinovaně. Tyto skupiny často pracují jako vládní či vojenské kyber jednotky.

9.3 Vybrané APT skupiny

APT skupiny jsou špionážní skupiny útočníků, které prokazatelně cílí na konkrétní společnosti a vládní instituce. Jejich útoky spočívají v pronikání do informačních systémů a získávání přístupu k v nich uloženým datům.

V posledních letech byly z masivních útoků obviněny převážně ruské hackerské skupiny. Útočníci postupují systematicky a využívají pestrou škálu útoků známých ze všedního života.[102] Jejich útoky spočívají převážně v tom, že jejich zkušení hackeři proniknou prostřednictvím ransomwaru do počítačové sítě, zašifrují soubory organizace a vyhrožují jejich zveřejněním nebo smazáním, pokud nebude zaplaceno vysoké výkupné.

Odborníci na kybernetickou bezpečnost označují na základě dosavadních aktivit skupiny APT jako jednoho z nejnebezpečnějších aktérů v této oblasti.

9.3.1 APT 28/ FANCY BEAR

Skupina APT 28, známá také jako FANCY BEAR, je ruská kybernetická špionážní skupina, která představuje hrozbu pro širokou škálu organizací po celém světě (viz Obrázek 4).[103]

FANCY BEAR je mimo jiné spojován s útoky na německý Bundestag a francouzskou televizní stanici TV5 Monde v dubnu 2015.[104]

Obrázek 4: APT 28 FANCYBEAR

[102] *Security-Portal.cz: Seznamte se – APT* [online]. [cit. 4.2.2022]. Dostupné z: https://www.security-portal.cz/clanky/seznamte-se-apt
[103] *CrowdStrike: Kdo je FANCY BEAR (APT28)?* [online]. [cit. 4.2.2022]. Dostupné z: https://www.crowdstrike.com/blog/who-is-fancy-bear/
[104] tamtéž

Metody a cíle FANCY BEAR

K útoku na své oběti obvykle využívají phishingové zprávy nebo získávají pověření pomocí falešných webových stránek.

Útoky této skupiny se primárně zaměřují především na vládní subjekty, oblast obrany, energetiky a mediální sektory.

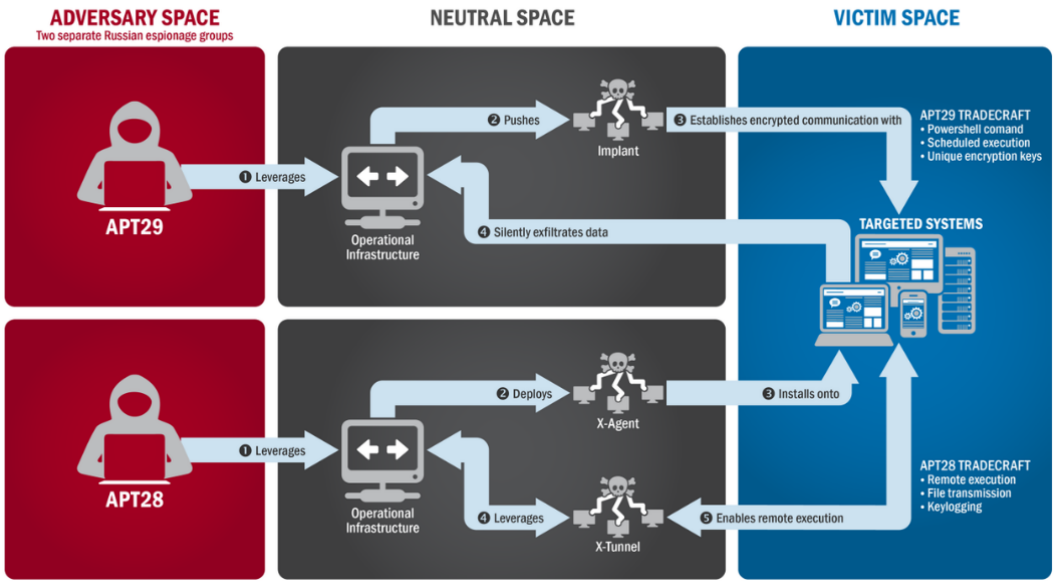
9.3.2 APT 29/ COZY BEAR

Skupina APT 29 známá jako Cozy Bear je hackerská skupina ruského původu, která je spojována s ruskými zpravodajskými agenturami.

Metody a cíle COZY BEAR

Útočníci používají obvykle spear phishing,[105] malware[106] nebo rozesílají falešná flashová videa přímo jako přílohy e-mailu (viz Obrázek 5).[107]

Útoky této skupiny se zaměřují na komerční subjekty a vládní organizace v USA, Německu, Jižní Koreji a Uzbekistánu.[108]



Obrázek 5: Schéma, jak Cozy Bear napadá počítačové systémy

[105] *Avast:* Mějte se na pozoru před spear phishingem [online]. [cit. 8.2.2022]. Dostupné z: https://blog.avast.com/cs/mejte-se-na-pozoru-pred-spear-phishingem

[106] *Avast: Co je malware a jak ho odstranit* [online]. [cit. 8.2.2022]. Dostupné z: https://www.avast.com/cs-cz/c-malware#gref

[107] *Wikiwand: Cozy Bear, Schéma popisující, jak skupina Cozy Bear napadá počítačové systémy.* [online]. [cit. 4.2.2022]. Dostupné z: https://www.wikiwand.com/cs/Cozy_Bear

[108] *SECURELIST: The CozyDuke APT* [online]. [cit. 8.2.2022]. Dostupné z: https://securelist.com/the-cozyduke-apt/69731/

9.3.3 VOODOO BEAR

Ruská hackerská skupina VOODOOBEAR, známá také jako Sandworm Team nebo Unit 74455, je údajně ruská kybervojenská jednotka GRU.[109] Je to organizace, která má na starosti ruskou vojenskou rozvědku.

Metody a cíle VoodooBear

Útoky této skupiny cílí na subjekty na Ukrajině a je velmi pravděpodobné, že stojí za útoky na ukrajinský energetický sektor, které koncem roku 2015 způsobily rozsáhlé výpadky elektřiny a dále za kyberútoky na Ukrajinu z roku 2017 pomocí malwaru Petya.[110]

[109] GRU – Glavnoje razvedyvatělnoje upravlenije, česky: Hlavní správa rozvědky
Ministerstvo oborony Rossijjskojj Federacii: Glavnoe upravlenie Generalnogo shtaba Vooruzhennykh Sil Rossijjskojj Federacii [online]. [cit. 8.2.2022].
Dostupné z: https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=9711@egOrganization
[110] malware, který požaduje výkupné za obnovení přístupu k osobním datům
WIRED: NotPetya, the Most Devastating Cyberattack in History [online]. [cit. 4.2.2022].
Dostupné z: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

10. PŘÍPADOVÁ STUDIE APT ÚTOKU NA FRANCOUZSKOU TELEVIZNÍ SÍŤ TV5 MONDE

Ke kybernetickému útoku na francouzskou televizní síť TV5 Monde[111] došlo 8. dubna 2015. Útočníci dokázali pomocí sedmi různých vstupů díky škodlivému softwaru proniknout do programového vysílání stanice. Během útoku přerušili vysílání všech 12 televizních kanálů a současně napadli její webové stránky a účty na sociálních sítích. Hackeři použili pro vstup do systémů televizní hardware nacházející se na různých lokacích po světě, který byl mezi sebou propojený internetovým spojením. Získali nejen kontrolu nad vysíláním, ale podařilo se jim dostat do účtů TV5 Monde na Facebooku a Twitteru. Útok začal být okamžitě připisován skupině Cyber Caliphate, protože se útočníci prezentovali jako „kybernetičtí džihádisté“. Na webových stránkách šířili heslo „Je suis IS" (česky „Já jsem IS") a dále osobní údaje několika francouzských vojáků s odkazem, že za jejich útokem stojí pomsta ze strany tzv. Islámského státu (viz Obrázek 6).[112]

Obrázek 6: TV5 Monde terčem kybernetického útoku

Teprve později byl incident spojen s ruskými hackery napojenými na ruskou vojenskou zpravodajskou skupinu GRU a zodpovědnou za útoky byla označena ruská hackerská skupina APT 28 známá jako FANCY BEAR.

[111] francouzská televizní síť s celosvětovým pokrytím, která vysílá několik kanálů s programem ve francouzštině

[112] *France 24: France's TV5Monde targeted in 'IS group cyberattack'* [online]. [cit. 10.2.2022]. Dostupné z: https://www.france24.com/en/20150409-france-tv5monde-is-group-hacking

TV5 Monde čelila dobře koordinovanému kybernetickému útoku, který zasáhl všechny počítačové komunikační systémy. Celá operace měla 3 fáze.

V první fázi útočníci provedli průzkum společnosti TV5 Monde, aby pochopili způsob, jakým vysílá své signály. Poté vyrobili škodlivý software na míru, aby poškodili a zničili hardware připojený k internetu, který řídil operace televizní stanice, jako jsou kodérové systémy používané k přenosu programů. Poprvé pronikli útočníci do sítě už 23. ledna 2015. Útok začal e-mailem zaslaným koncem ledna redaktorům TV5 Monde formou takzvaného phishingu, tedy podvodnou technikou používanou na internetu k získávání citlivých údajů v elektronické komunikaci. Tři redaktoři na e-mail odpověděli, čímž pirátům umožnili proniknout do systému televize pomocí takzvaného trojského koně.

Ve druhé fázi, která začala asi tři týdny před útokem, hackeři nakazili virem několik počítačů stanice.

Třetí fází byl potom samotný útok, ten začal ve středu 8. dubna 2015 a trval několik hodin. Útočníci získali kontrolu nad vysíláním, přinutili kanál vysílat několik hodin předem nahrané programy. Vyřadili z provozu všech 12 televizních kanálů, „nabourali se“ do účtů TV5 Monde na Facebooku a Twitteru a prostřednictvím sociálních sítí a webových stránek šířili džihádistickou propagandu.

Na obrázku 7 jsem graficky znázornila chronologii útoků z roku 2015 na Tv5 Monde.[113]

Obrázek 7: Chronologie útoků z roku 2015

[113] vlastní zpracování

I když TV5 Monde dostala systémy pod kontrolu po třech hodinách, k obnovení vysílání došlo až následující den. Bezprostředně po útoku se zaměstnanci museli vrátit k používání faxů, protože nemohli odesílat e-maily – nefungoval internet.

Útok měl na společnost obrovský dopad. Finanční náklady na odstranění škod a mnohaměsíční provoz bez internetu vyšly TV stanici jen v prvním roce po útoku na 5,6 milionu dolarů, což je v přepočtu přibližně 140 milionů korun. Na novou bezpečnější ochranu vynakládá nyní společnost každoročně více než 3,4 miliony dolarů, což je asi 85 milionů korun.

Všichni zaměstnanci museli změnit chování, investovalo se hodně do zabezpečení systémů. Pro kontrolu e-mailů ze zahraničí se zavedly speciální autentizační postupy, USB-flash disky se musely začít před použitím otestovat.

Vyšetřováním útoku, které začalo hned 9. dubna 2015, byla pověřena ANSSI.[114] Do vyšetřování byl zapojen tým devíti až patnácti odborníků, složený z jednoho technického koordinátora, dvou až pěti digitálních forenzních vyšetřovatelů, jednoho experta na reverzní inženýrství na malware, dvou bezpečnostních výzkumníků a tří až šesti auditorů.

Vyšetřovatelé ANSSI nashromáždili asi 13 TB kopií obrázků pevného disku, paměti RAM a vestavěných zařízení, na která se útočníci zaměřili.

Tým vyšetřovatelů se zpočátku obával, že útočníci mohli umístit do sítě TV5 Monde „logickou bombu“, nakonec se však tyto obavy nepotvrdily a vyšetřovatelé dospěli k závěru, že útočníci použili pouze vysoce cílený malware, který vyřadil z provozu všech 12 jejích kanálů.

Kybernetický útok, který zasáhl francouzskou televizní společnost TV5 Monde byl masivní. Měl sloužit jako „probuzení“, které lidi přinutí pochopit, že hrozby pro kritickou infrastrukturu nejsou jen fantazií. Naštěstí při tomto útoku nedošlo k žádným zraněním nebo ztrátám na životech. Šance, že k nim dojde, je ale díky sofistikovanějším kybernetickým útokům stále reálnější.

Pokud chce společnost zmírnit riziko tohoto typu útoku, musí brát cílené útoky vážně a přijmout vhodná opatření, aby jim čelila.

---

[114] ANSSI – francouzská národní agentury pro kybernetickou bezpečnost byla zřízena vyhláškou č. 2009-834 ze dne 7. července 2009

11. OCHRANA A PREVENCE

Ochrana a prevence patří mezi hlavní bezpečnostní opatření, které mohou společnosti přijmout k zabránění phishingových útoků. Uvedu zde výčet opatření, které se mi zdají jako stěžejní.

11.1 Školení zaměstnanců

Jedním z nejběžnějších způsobů, jak počítačoví zločinci získávají přístup k našim datům je právě prostřednictvím zaměstnanců. Jedním z nejúčinnějších způsobů, jak se chránit před kybernetickými útoky a všemi typy narušení dat, je opakované školení svých zaměstnanců v oblasti prevence kybernetických útoků a informovat je o aktuálních kybernetických útocích.[115]

Dále je potřeba:

- zkontrolovat odkazy v těle e-mailu dříve, než na ně klikneme,
- zkontrolovat e-mailové adresy z přijatého e-mailu,
- neotevírat přílohy, které neznáme,
- před odesláním citlivých informací používat zdravý rozum.

11.2 Aktualizace softwaru

Ke kybernetickým útokům často dochází proto, že systémy nebo software nejsou plně aktuální, což zanechává slabá místa. Hackeři využívají těchto slabin, k získání přístupu do vaší sítě. Jakmile jsou uvnitř systému, na preventivní opatření je často příliš pozdě.[116]

Abychom tomu zabránili, je rozumné investovat do systému nebo softwaru, který zabezpečí aktuálnost a odolnost všech programů, nebo operačních systémů v organizaci.

11.3 Ochrana přenosných elektronických zařízení

Ochrana přenosných zařízení značí ochranu mobilních zařízení, tabletů a notebooků, které jsou připojeny k podnikovým sítím a poskytují přístupové cesty k bezpečnostním hrozbám. Tyto cesty je třeba chránit pomocí specifického

---

[115] *Algotech.cz: Ochrana dat ve firmě* [online]. [cit. 16.2.2022]. Dostupné z: https://www.algotech.cz/novinky/2020-05-22-ochrana-dat-ve-firme-8-kroku-ke-kyberneticke-bezpecnosti

[116] *Lupa.cz: Jak se bránit phishingu* [online]. [cit. 16.2.2022]. Dostupné z: https://www.lupa.cz/clanky/jak-se-branit-phishingu/

softwaru pro ochranu koncových bodů. Tím mohou být antiviry, osobní firewally nebo jejich kombinace.[117]

11.4 Podniková brána firewall

Umístění sítě za firewall[118] je jedním z nejúčinnějších způsobů, jak se bránit před jakýmkoli kybernetickým útokem. Systém brány firewall zablokuje jakékoli útoky hrubou silou na vaši síť anebo systémy dříve, než může způsobit škodu.[119]

11.5 Zálohování dat

V případě kybernetického útoku musíme mít svá data zálohovaná, abychom předešli jejich ztrátě a vážným finančním ztrátám. Je dobré mít vytvořený zálohovací plán, kdy se která služba a uživatelská data zálohují. Standardem bývá, že přes týden zálohovací systém vytváří pouze přírůstkové zálohy a přes víkend, kdy nejsou síť a systémy vytíženy, následně plné zálohy, které si vyžádají delší čas.[120]

11.6 Fyzická kontrola přístupu

Jeden z útoků, které můžete infikovat na vaše systémy, může být fyzický. Je potřeba mít kontrolu nad tím, kdo má přístup k vaší síti. Ideální použít systém objektové bezpečnosti, abychom zamezili možnosti, že kdokoliv by mohl vejít do naší kanceláře nebo podniku a zasunout USB klíč. Ten by mohl obsahovat infikované soubory a přenést je do jednoho z našich počítačů, což mu umožní přístup k celé vaší síti, kterou dále infikuje.[121]

---

[117] *Algotech.cz: Ochrana dat ve firmě* [online]. [cit. 16.2.2022]. Dostupné z: https://www.algotech.cz/novinky/2020-05-22-ochrana-dat-ve-firme-8-kroku-ke-kyberneticke-bezpecnosti

[118] Brány firewall jsou softwarové programy nebo hardwarová zařízení, která filtrují a zkoumají informace přicházející prostřednictvím připojení k internetu.

[119] *Lupa.cz: Jak se bránit phishingu* [online]. [cit. 16.2.2022]. Dostupné z: https://www.lupa.cz/clanky/jak-se-branit-phishingu/

[120] *Acronis: 10 zásadních kroků pro ochranu vaší společnosti před kybernetickými útoky* [online]. [cit. 16.2.2022]. Dostupné z: https://www.acronis.com/en-gb/articles/company-cyber-attack-protection/

[121] *Algotech.cz: Ochrana dat ve firmě* [online]. [cit. 16.2.2022]. Dostupné z: https://www.algotech.cz/novinky/2020-05-22-ochrana-dat-ve-firme-8-kroku-ke-kyberneticke-bezpecnosti

11.7 Osobní účty zaměstnanců

Každý zaměstnanec musí obdržet své vlastní přihlášení pro každou aplikaci a program. Několik uživatelů připojených pod stejnými přihlašovacími údaji je opět riziko, které musíme eliminovat.

11.8 Správa přístupu

Dalším z velkých z rizik je povolení zaměstnancům instalaci softwaru na firemní zařízení. Tento SW[122] by mohl ohrozit nebo infikovat naše systémy.

Operační systémy lze zabezpečit tak, aby uživatelé neměli možnost nainstalovat jakýkoliv SW bez vědomí správců informačních technologií, kteří za chod systémů zodpovídají.

11.9 Hesla

Nastavení správného hesla je alfou a omegou bezpečnosti. Jeví se jako jednoduchá záležitost a spousta uživatelů si volí co nejlehčí hesla pro dobré zapamatování. To je chyba, na kterou mohou narazit nejen ve firmě, kde pracují, ale i např. ve svém soukromém životě. Je potřeba volit hesla silné, alespoň 12 znaků, které obsahují velká písmena a speciální znaky. Pro české uživatele není vhodné použití písmen „Y“ a „Z“ z důvodu záměny a následné zablokování účtů.[123]

Nejen síla hesla, ale také doba používaní může být potencionální hrozbou útoku. Hesla je potřeba měnit v určitých časových intervalech, aby bylo zabráněno odhadu, odchytu, či jiné kompromitaci.

Jakmile hacker zjistí naše heslo, má přístup ke všemu v našem systému a jakékoli aplikaci, kterou používáme.

---

[122] software

[123] *BlueGhost: 10 pravidel pro silné heslo: Opravdu máte dobře zabezpečené účty?* [online]. [cit. 16.2.2022]. Dostupné z: https://www.blueghost.cz/clanek/10-pravidel-bezpecnost-hesel/

ZÁVĚR

V dnešní moderní době nahlížíme na moderní technologie a internet jako na něco, co nám usnadňuje život a baví nás. A právě internet je jedním z mála vynálezů, který má obrovský dopad na společnost. Přímo i nepřímo ovlivňuje každodenní život každého z nás. Pomáhá nám čerpat informace, spojit se s lidmi na druhém konci světa atd.

Moderní informační a komunikační technologie jsou pro společnost velkým přínosem, na druhou stranu však mohou představovat i do budoucna vysoké bezpečnostní riziko, pokud nebudou dostatečně zabezpečené. V takovém případě dokáží tyto technologie nadělat nevídané problémy. Moderní technologie mohou tedy být nejen cílem, ale i nástrojem kybernetických útoků. Bezpečnost těchto technologií je přitom v dnešním online prostředí ohrožována mnoha způsoby. Moderní technologie mohou sehrát důležitou roli při šíření kyberterorismu.

Tempo pokroku informační a komunikační technologie je nezastavitelné a vynalézavost kyberzločinců nezná hranic. Kyberzločinci mají k dispozici pokročilou technologii, která jim umožňuje rychlejší komunikaci a pružnější reakce. Útočníci používají důmyslné taktiky, ale často se i spoléhají na technologickou negramotnost společnosti.

Z pohledu kybernetické bezpečnosti můžeme za největší hrozbu v této oblasti považovat Advanced Persistent Treat, kde útočníci vynakládají značné úsilí a finanční prostředky k provedení útoku. Aktéři stojící za APT útoky jsou typicky skupiny zkušených hackerů pracující koordinovaně. Tyto skupiny často pracují jako vládní či vojenské kyberjednotky.

Kyberprostor čelí každodenně desítkám bezpečnostních incidentů, které je poměrně obtížné sledovat, a ještě obtížnější předvídat. Tyto incidenty mívají plíživou formu, takže si jich nikdo nemusí všimnout poměrně dlouhou dobu, dokud nedojde k úniku obchodního tajemství nebo jiné finanční ztrátě.

Boj s kyberteroristy je složitý. I přes veškerou snahu budou kyberteroristé vždy o krok napřed. Operují po celém světě a vysledování jejich aktivních buněk nebývá jednoduché.

V minulosti evidujeme případy (i v ČR), kdy se kyberútočníci snažili vyřadit z provozu informační systémy veřejné správy či zdravotnických zařízení. Útoky

neproběhly v takovém rozsahu, aby vyřadily systémy na dlouhou dobu, ale i jednodenní odstávky služeb mohly způsobit nemalé potíže personálu, ale i obyvatelstvu.

Žádný z veřejně známých incidentů doposud nemůžeme kvalifikovat jako kyberterorismus, protože nastalé útoky nenaplnily atributy kyberteroristického útoku. Je však realitou, že využívání kyberprostoru slouží pro propagaci, nábor a výcvik teroristů.

Kyberterorismus představuje pro budoucnost skutečnou hrozbou, kterou není vhodné ani bezpečné ignorovat. Je potřeba vynakládat více finančních prostředků do oblasti kybernetické bezpečnosti, zaměřit se především na prevenci a přijmout dostatečná bezpečnostní opatření pro eliminaci případných potenciálních útoků a infiltrací útočníků do systémů.

Běžný uživatel internetu a jiných moderních technologií si neuvědomuje rozsah nebezpečí, které kyberterorismus a kybernetické útoky představují. Nejslabším článkem kyberprostoru, a tedy i největší kyberhrozbou je člověk sám. Záleží tedy na chování každého jednotlivce, jak se dokáže přizpůsobit aktuálním trendům a jak dokáže zareagovat na potenciální hrozbu.

SEZNAM POUŽITÝCH ZKRATEK

ANSSI – Agences nationale de la sécurité des systèmes d'information (Francouzská národní agentura pro kybernetickou bezpečnost)
APT – Advanced Persistent Threat (pokročilá trvalá hrozba)
BSI – Bundesamt für Sicherheit in der Informationstechnik (Spolkový úřad pro bezpečnost informační techniky)
CERT – Computer emergency response team (Skupina pro reakce na počítačové bezpečnostní incidenty)
DDoS – Distributed Denial of Service (Distribuované odepření služby)
DOS – Denial of Service (Odepření služby)
GRU – Glavnoje razvedyvatělnoje upravlenije (Hlavní správa rozvědky)
ICT– Information and Communication Technologies (Informační a komunikační technologie)
IS – Informační systém
NCKB – Národní centrum kybernetické bezpečnosti, součást Národního bezpečnostního úřadu se sídlem v Brně.
NCKO – Národní centrum kybernetických operací
NHS – National Health Service (Národní zdravotní služba)
NIST – National Institute of Standards and Technology (Národní institut standardů a technologie)
NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost
SQL – Structured Query Language (Strukturovaný dotazovací jazyk)
SW – Software
TCP/IP – Transmission Control Protocol Transmission Control Protocol/Internet Protocol (Přenosový protokol/internetový protokol)
TV – televize
VIS – významné informační systémy
VKB – vyhláška o kybernetické bezpečnosti
ZKB – Zákon o kybernetické bezpečnosti

SEZNAM POUŽITÉ LITERATURY

MONOGRAFIE

[1] EVERARD, P., NATO and Cyber Terrorism, *In Responses to Cyber Terrorism,* [online]. 2008. [cit. 23.1.2022]. ISBN 978-1-58603-836-6.

[2] DUNNINGAN, James F. *Bojiště zítřka*, překlad Kateřina Došlíková, Baronet, 2004, ISBN 80-7214-642-4.

[3] GIBSON, William, Neuromancer, překlad Josef Rauvolf, Laser-books, 2010, ISBN 978-80-7193-318-2

[4] JANCZEWSKI, Lech J. & COLARIK, Andrew M. *Kybernetická válka a kybernetický terorismu*s. In: New york : Information Science Reference, 2008.

[5] JANCZEWSKI, L, COLARIK, A., *Managerial Guide For Handling Cyber-Terrorism And Information Warfare,* In: Hershey PA: Idea Group Publishing, 2005, ISBN 978-1591405832.

[6] JIROVSKÝ, Václav, *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[7] KOLOUCH, Jan, *Cyber Crime.* Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. [online]. [cit. 9.2.2022]. ISBN 978-80-88168-15-7.

[8] KOLOUCH, Jan, Pavel Bašta a kol., *CyberSecurity.* Praha: 2019. CZ.NIC, z.s.p.o., [online]. [cit. 9.2.2022]. ISBN 978-80-88168-34-8

[9] WEIMANN, Gabriel. 2006. *Terror on the internet.* In: Washington, D.C. : US Institute of Peace Press, 2006.

[10] LAVORGNA, Anita. 2020. *Cybercrimes.* In: Trento : Red Globe Press, 2020.

ZÁKONNÁ ÚPRAVA A IAŘ (INTERNÍ AKTY ŘÍZENÍ)

[11] § 2 odst. 1 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) [online]. [cit. 19.2.2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#p2-1–a

[12] Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti [online]. [cit. 21.1.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-316

[13] Vyhláška č. 360/2020 Sb., vyhláška, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb. [online]. [cit. 21.1.2022].
Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317

[14] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). [online]. [cit. 9.2.2022].
Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[15] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů [online]. [cit. 9.2.2022].
Dostupné z: https://www.zakonyprolidi.cz/cs/2005-127

[16] Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktur. [online]. [cit. 9.2.2020].
Dostupné z: https://www.zakonyprolidi.cz/cs/2010-432

WEBOVÉ STRÁNKY A ELEKTRONICKÉ ZDROJE

[17] *About Facebook* [online]. [cit. 21.1.2022].
Dostupné z: https://about.facebook.com

[18] *About Twitter* [online]. [cit. 25.1.2022]. Dostupné z: https://about.twitter.com

[19] *About Youtube* [online]. [cit. 21.1.2022]. Dostupné z: https://about.youtube

[20] *Academia.edu: How_would you define Cyberspace* [online]. [24.1.2022].
Dostupné z: https://www.academia.edu/7096442/How_would_you_define_Cyberspace

[21] *Acronis: 10 zásadních kroků pro ochranu vaší společnosti před kybernetickými útoky* [online]. [cit. 16.2.2022].
Dostupné z: https://www.acronis.com/en-gb/articles/company-cyber-attack-protection/

[22] *Acunetix: Cross-site Scripting.* [online]. [cit. 14.2.2022].
Dostupné z: https://www.acunetix.com/websitesecurity/cross-site-scripting/

[23] *Agence nationale de la sécurité des systèmes d'information* [online]. [cit. 8.2.2022]. Dostupné z: https://www.ssi.gouv.fr/

[24] *Agence nationale de la sécurité des systèmes d'information: Protéger son site Internet des cyberattaques* [online]. [cit. 10.2.2022].
Dostupné z: https://www.ssi.gouv.fr/actualite/proteger-son-site-internet-des-cyberattaques/

[25] *Algotech.cz: Ochrana dat ve firmě* [online]. [cit. 16.2.2022].
Dostupné z: https://www.algotech.cz/novinky/2020-05-22-ochrana-dat-ve-firme-8-kroku-ke-kyberneticke-bezpecnosti

[26] *Avast: Co je malware a jak ho odstranit* [online]. [cit. 8.2.2022]. Dostupné z: https://www.avast.com/cs-cz/c-malware#gref

[27] *Avast: Co je to rootkit?* [online]. [cit. 14.2.2022]. Dostupné z: https://www.avast.com/cs-cz/c-rootkit

[28] *Avast: Co je to Trojský kůň?* [online]. [cit. 14.2.2022]. Dostupné z: https://www.avast.com/cs-cz/c-trojan

[29] *Avast: Mějte se na pozoru před spear phishingem* [online]. [cit. 8.2.2022]. Dostupné z: https://blog.avast.com/cs/mejte-se-na-pozoru-pred-spear-phishingem

[30] *Axians.cz: Kybernetická bezpečnost – Jak probíhá kybernetický útok?* [online]. [cit. 9.2.2022]. Dostupné z: https://www.axians.cz/cs/novinky/jak-probiha-kyberneticky-utok/

[31] BEJTLICH, R., What Is APT and What Does It Want? *TaoSecurity Blog* [online]. 2010 [cit. 24.1.2022]. Dostupné z: https://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html

[32] Bezpečnostní strategie – 2015 | Vláda ČR [online]. [cit. 9.2.2022]. Dostupné z: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

[33] *BlueGhost: 10 pravidel pro silné heslo: Opravdu máte dobře zabezpečené účty?* [online]. [cit. 16.2.2022]. Dostupné z: https://www.blueghost.cz/clanek/10-pravidel-bezpecnost-hesel/

[34] *BlueVoyant: Different types of password attacks and how they work.* [online]. [cit. 14.2.2022]. Dostupné z: https://www.bluevoyant.com/blog/password-attacks-and-prevention/

[35] *CBS News: ISIS-allied hackers claim worrying new attack* [online]. [cit. 9.2.2022]. Dostupné z: https://www.cbsnews.com/news/french-tv-network-tv5-monde-hacked-by-cybercaliphate-in-name-of-isis/

[36] *Centrum kybernetické bezpečnosti: Národní centrum kybernetických operací: Centrum kyberobrany představilo svou strategii do roku 2022 – Centrum kybernetické bezpečnosti* [online]. [cit. 23.1.2022]. Dostupné z: https://centrumkyberbezpecnosti.cz/centrum-kyberobrany-predstavilo-svou-strategii-do-roku-2022/

[37] *Cisco: Co je phishing?* [online]. [cit. 14.2.2022]. Dostupné z: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

[38] *Clever&Smart Management: APT: Jak probíhá cílený útok* [online]. [cit. 4.2.2022]. Dostupné z: https://www.cleverandsmart.cz/apt-jak-probiha-cileny-utok/

[39] *CrowdStrike: Kdo je FANCY BEAR (APT28)?* [online]. [cit. 4.2.2022]. Dostupné z: https://www.crowdstrike.com/blog/who-is-fancy-bear/

[40] *CyberSecurity.CZ: Legislativa v české republice* [online]. [cit. 21.1.2022]. Dostupné z: https://cybersecurity.cz/law.html

[41] CZ.NIC: *CSIRT.CZ Národní CSIRT České republiky* [online]. [cit. 23.1.2022]. Dostupné z: https://www.csirt.cz/cs/

[42] *Daily Storm: MID predupredil, chto chelovechestvu ugrozhaet kibervojna* [online]. [cit. 8.2.2022]. Dostupné z: https://www.dailystorm.ru/news/mid-predupredil-chto-chelovechestvu-ugrozhaet-kibervoyna

[43] DENNING, Dorothy E., *Cyberterrorism,* In: Georgetown University [online]. 2000 [cit. 23.1.2022]. Dostupné z: https://www.nato.int/structur/library/bibref/cyberterrorism.pdf

[44] DENNING, Dorothy E., "*Cyberterrorism – Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives"*, In: New York: Nova Science Publishers. [online]. 2007 [cit. 23.1.2022]. ISBN: 978-1-60021-709-8 Dostupné z: https://books.google.cz/books?id=wlDs42YMDIC&pg=PA71&lpg=PA71&dq=Testimony

[45] *Eset: Co je počítačový virus?* [online]. [cit. 14.2.2022]. Dostupné z: https://www.eset.com/cz/virus/

[46] *France 24: France's TV5Monde targeted in 'IS group cyberattack'* [online]. [cit. 10.2.2022]. Dostupné z: https://www.france24.com/en/20150409-france-tv5monde-is-group-hacking

[47] GLAZOV, Jamie. FrontPageMagazine.com. *Symposium: Cyber Jihad.* [online]. 2008 [cit. 21.1.2022]. Dostupné z: http://archive.frontpagemag.com/readArticle.aspx?ARTID=30072

[48] *Impreva: Co je zero-day (0day) exploit?* [online]. [cit. 14.2.2022]. Dostupné z: https://www.imperva.com/learn/application-security/zero-day-exploit/

[49] *International Business Times: Why Kremlin-backed Russian hackers blamed Isis for cyberattack on Tv 5 Monde?* [online]. [cit. 8.2.2022]. Dostupné z: http://www.ibtimes.co.uk/why-kremlin-backed-russian-hackers-blamed- isis-cyberattack-tv5-monde-1505629

[50] *Internetem bezpečně: Co je kybernetická kriminalita* [online]. [cit. 8.2.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/kyberneticka-kriminalita/

[51] *IT SLOVNÍK.CZ: Co je to logic bomb?* [online]. [cit. 9.2.2022]. Dostupné z: https://www.it-slovnik.cz/pojem/logic-bomb

[52] JANOUŠEK, Michal. Kyberterorismus: Terorismus informační společnosti. *Obrana a Strategie* [online]. [cit. 8.2.2022] Dostupné z: http://www.defenceandstrategy.eu/cs/archiv/rocnik-2006/22006/kyberterorismus-terorismus-informacni-spolecnosti.html.

[53] *Jigsaw Academy: Difference Between Hacker And Cracker – An Easy Overview* [online]. [cit. 9.2.2022]. Dostupné z: https://www.jigsawacademy.com/blogs/cyber-security/difference-between-hacker-and-cracker/

[54] *Jihadi.org: What is Cyber-Jihad?* [online]. [cit. 21.1.2022]. Dostupné z: http://www.jihadi.org/p/what-is-cyber-jihad.html

[55] JIRÁSEK Petr; NOVÁK Luděk a POŽÁR Josef, *Výkladový slovník kybernetické bezpečnosti.* CyberSecurity.CZ. Kybernetická bezpečnost a obrana. [online]. [cit. 21.1.2022] Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf.

[56] *Kaspersky.com: What Is an Advanced Persistent Threat (APT)?* [online]. [cit. 8.2.2022]. Dostupné z: https://www.kaspersky.com/resource-center/

[57] KLAUSEN, J., *Tweeting the Jihad: Sociální sítě západních zahraničních bojovníků v Sýrii a Iráku* [online]. [cit. 24.1.2020]. Dostupné z: https://www.tandfonline.com/doi/pdf/10.1080/1057610X.2014.974948

[58] KOHLMANN, Evan F. WASH. *Online Discussion: Al Qaeda and the Internet?* [online]. [cit. 21.1.2022]. Dostupné z: https://www.jstor.org/stable/20032074

[59] LIANG, Christina Schori. *Kyberdžihád: porozumění propagandě Islámského státu a boj proti ní*. GSCP Policy Paper, [online]. [cit. 24.1.2020]. Dostupné z: https://www.gcsp.ch/Christina-Schori-Liang

[60] *Lupa.cz: Jak se bránit phishingu* [online]. [cit. 16.2.2022]. Dostupné z: https://www.lupa.cz/clanky/jak-se-branit-phishingu/

[61] *MalwareFox: What is Ransomware?* [online]. [cit. 8.2.2022]. Dostupné z: https://www.malwarefox.com/ransomware/

[62] *Ministerstvo oborony Rossijjskojj Federacii: Glavnoe upravlenie Generalnogo shtaba Vooruzhennykh Sil Rossijjskojj Federacii* [online]. [cit. 2021-04-18].
Dostupné z: https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=9711@egOrganizatio

[63] *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 9.2.2022]. Dostupné z: www.govcert.cz

[64] *Národní úřad pro kybernetickou a informační bezpečnost: O NÚKIB* [online]. [cit. 20.1.2022]. Dostupné z: www.govcert.cz

[65] *Národní úřad pro kybernetickou a informační bezpečnost: Kybernetická bezpečnost – Vládní CERT* [online]. [cit. 23.1.2022].
Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/

[66] *Národní úřad pro kybernetickou a informační bezpečnost: Nová pravidla pro určování významných informačních systémů* [online]. [cit. 21.1.2022].
Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1627-nova-pravidla-pro-urcovani-vyznamnych-informacnich-systemu/

[67] *National Institute of Standards and Technology: Managing Information Security Risk: Organization, Mission and Information System View* [online]. [cit. 9.2.2022].
Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[68] *Onelogin: Man-in-the-middle attack* [online]. [cit. 14.2.2022].
Dostupné z https://www.onelogin.com/learn/6-types-password-attacks

[69] *Oxford Learner's Dictionaries: Cyberspace* [online]. [cit. 13.2.2020].
Dostupné z: https://www.oxfordlearnersdictionaries.com/definition/english/cyberspace

[70] *ScienceDirect: Hactivists* [online]. [cit. 9.2.2022].
Dostupné z: https://www.sciencedirect.com/topics/computer-science/hacktivists

[71] *SECURELIST: The CozyDuke APT* [online]. [cit. 8.2.2022].
Dostupné z: https://securelist.com/the-cozyduke-apt/69731/

[72] *Security-Portal.cz: Seznamte se – APT* [online]. [cit. 4.2.2022].
Dostupné z: https://www.security-portal.cz/clanky/seznamte-se-apt

[73] *The Guardian: Hoda Muthana 'deeply regrets' joining Isis and wants to return home* [online]. [cit. 09.02.2022].
Dostupné z: https://www.theguardian.com/world/2019/feb/17/us-woman-hoda-muthana-deeply-regrets-joining-isis-and-wants-return-home

[74] *Tumblr* [online]. [cit. 25.1.2022]. Dostupné z: https://www.tumblr.com

[75] *TV5MONDE: Piratage de TV5MONDE: ce qu'en disent les experts* [online]. [cit. 9.2.2022]. Dostupné z: https://information.tv5monde.com/info/piratage-de-tv5monde-ce-qu-en-disent-les-experts-27578

[76] *Varonis: What is an Advanced Persistent Threat (APT)* [online]. [cit. 10.2.2022]. Dostupné z: https://www.varonis.com/blog/advanced-persistent-threat

[77] *Veracode: What Is a Man-in-the-Middle Attack?* [online]. [cit. 14.2.2022]. Dostupné z: https://www.veracode.com/security/man-middle-attack

[78] *Vojenské zpravodajství. Vojenské zpravodajství* [online]. [cit. 22.1.2022]. Dostupné z: https://vzcr.cz

[79] *Vojenské zpravodajství: Kybernetická obrana: Vojenské zpravodajství zajišťuje kybernetickou obranu české republiky* [online]. [cit. 22.1.2022]. Dostupné z: https://vzcr.cz/kyberneticka-obrana-46

[80] *Vojenské zpravodajství: Zabezpečujeme informace v oblasti obrany* [online]. [cit. 21.1.2022]. Dostupné z: https://vzcr.cz

[81] WEIMANN, Gabriel, *Cyberterrorism: How Real is the Threat? United States Institute of Peace* [online]. 2004 [cit. 9.2.2022]. Dostupné z: https://www.usip.org/sites/default/files/sr119.pdf

[82] WEIMANN, Gabriel. *How Modern Terrorism. United States Institute of Peace* [online]. 2004 [cit. 9.2.2022]. Dostupné z: https://www.usip.org/sites/default/files/resources/sr116.pdf.

[83] *Wikiwand: Cozy Bear, Schéma popisující jak skupina Cozy Bear napadá počítačové systémy.* [online]. [cit. 4.2.2022]. Dostupné z: https://www.wikiwand.com/cs/Cozy_Bear

[84] *WIRED: NotPetya, the Most Devastating Cyberattack in History* [online]. [cit. 4.2.2022]. Dostupné z: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/