Ing. Miroslav Čermák
Policejní akademie České republiky v Praze
student doktorského studia

Identifikace klíčových aktérů ovlivňujících subjektivní percepci událostí v kyberprostoru

Tento příspěvek byl sepsán na základě dlouhodobého monitorování situace v kyberprostoru, analýze bezpečnostních hlášení ohledně probíhajících kybernetických útoků jakožto i bezpečnostních reportů poskytovaných leadery v oblasti kybernetické bezpečnosti a zpracovávaných v rámci služby cyber threat intelligence, a v neposlední řadě pak i na základě šetření skutečných kybernetických incidentů a rozhovorů s manažery informační a kybernetické bezpečnosti, jejichž jména nemohou být s ohledem na ochranu jejich zájmů zveřejněna.

Pokud jde o porozumění tomu, co se skutečně odehrává v kyberprostoru a jakým hrozbám a kybernetickým útokům čelíme, jsme zcela odkázáni na své omezené osobní zkušenosti, zkušenosti našich známých a známých těchto známých a v neposlední řadě pak i na široce prezentovaný a notně pokřivený mediální obraz, neboť žádná databáze obsahující informace o všech proběhnuvších kybernetických útocích na organizace v ČR v zásadě neexistuje. (Zde je třeba si uvědomit, že drtivá většina populace, včetně odborné veřejnosti, přístup k databázím, které vedou soukromé subjekty, nebo orgány činné v trestním řízení, nemá a nikdy mít nebude.)

Jediný, kdo by nám dokázal onen značně deformovaný obraz o situaci v kyberprostoru vyladit do křišťálového jasu, by byly samotné firmy a domácnosti, které se oběťmi těchto útoků stávají. Ovšem to by musely jednotlivé bezpečnostní útoky hlásit, což se nejspíš nikdy nestane. A to nemluvíme o tom, že by nejprve musela existovat i nějaká jednotná terminologie kybernetických hrozeb. Jedině tak bychom se mohli dozvědět, k jakým kybernetickým útokům skutečně dochází a jak často.

Kromě toho je zde několik subjektů, které v kyberprostoru hrají ne nepodstatnou roli, neb minimálně ovlivňují, pokud už ne přímo vytvářejí onen mediální obraz. Netřeba snad dodávat, že tyto subjekty v souladu s tržními principy sledují výhradně své vlastní ekonomické zájmy, kterými je primárně dosažení zisku, což jim nelze mít vůbec za zlé.

V prvé řadě se jedná o firmy, které s větším či menším úspěchem nabízí své produkty, bojují o svůj tržní podíl, vyhledávají tržní niky a snaží se na ně proniknout, a zároveň jsou cílem kybernetických útoků. A také domácnosti, které jsou zákazníky těchto firem, a na které jsou rovněž vedeny útoky. Ty však nemají důvod se útoky, které na ně byly vedeny, chlubit, a proto se o většině těchto útoků nemusíme vůbec dozvědět a také se o nich nedozvídáme.

Dále jsou to útočníci, a je celkem jedno, zda se jedná o script kiddies, osamocené hackery, zločinecké organizace anebo státem sponzorované APT skupiny, které budou charakterizovány dále, a které vedou plošné a cílené útoky v kyberprostoru s cílem dosáhnout co nejvyšších výnosů anebo způsobit protivníkovi v rámci vedení

hybridní války[1] co největší škodu, a proto aktivně vyhledávají známé i neznámé zranitelnosti a snaží se jich zneužít k průniku do informačních systémů a provozních technologií a jejich ovládnutí.

Proti útočníkům pak stojí firmy nabízející bezpečnostní řešení, a které rovněž bojují o přežití, snaží se urvat si svůj podíl na trhu a volí různou strategii, ať už diferenciace nebo koncentrace, případně neváhají uzavírat strategické aliance tam, kde se rudé oceány barví krví a společně jako hlásná trouba pak šířit do světa informace o probíhajících útocích v rámci svého komunikačního mixu, který zahrnuje jak propagaci, tak i PR a v některých případech i vedení dezinformační kampaně, jak tomu bylo např. v případě aplikace SpyHunter.[2]

Tak trochu mimo toto dění stojí a o určitou objektivitu se snaží média, která však získávají informace právě od firem prodávajících bezpečnostní řešení ať už v podobě technologií anebo služeb, a dále pak novináři píšící o bezpečnosti, a konečně i nezávislí blogeři. Ti však v zásadě tyto informace jen přebírají a v podstatě, pokud neprovádí i vlastní výzkum, tak si je ani nemohou ověřit z jiného nezávislého a důvěryhodného zdroje, neboť do skript a monografií se tyto informace nedostávají vůbec anebo se značným zpožděním a pak prostě vydají to, co dostanou.

Z těch nejznámějších jmenujme třeba hrozby zneužívající kritické zranitelnosti Spectre a Meltdown, o kterých svého času informovala snad všechna média, ale jak v rámci experimentu později dokázal třeba Malý, tak snadné jejich zneužití zase nebylo[3] a také k tomu ani v praxi nedocházelo, ale přesto tato kauza dokázala podstatně ovlivnit nákupní chování firem.

Do těchto PSYOPS operací a hrátek informačních služeb se nechala zatáhnout i BIS a potažmo i NÚKIB, když o rok později vydal varování ohledně rizika spojeného s používáním síťových prvků společnosti Huawei,[4] což odborná veřejnost odsoudila, ale na situaci to již nic nezměnilo a zkreslený obraz, který se podařilo vyvolat, opět přispěl nejen k ovlivnění IT strategie v nejedné firmě, ale měl značný dopad i na informační strategii několika suverénních států.

Nepochybně zde dochází ke značnému konfirmačnímu zkreslení, což v konečném důsledku vede k tomu, že bezpečnostní strategie je formulována na základě několika medializovaných útoků a prohlášení bezpečnostních expertů.

---

[1] ČERMÁK, Miroslav. Hybridní hrozby. *CleverAndSmart Management Consulting* [online]. 18. duben 2020 [vid. 10. červen 2020]. Získáno z: https://www.cleverandsmart.cz/hybridni-hrozby/

[2] ČERMÁK, Miroslav. Jak odstranit jakýkoliv malware pomocí aplikace SpyHunter a jí podobných. *CleverAndSmart Management Consulting* [online]. 8. únor 2016 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/jak-odstranit-jakykoliv-malware-pomoci-aplikace-spyhunter-a-ji-podobnych/

[3] MALÝ, Robert. Tak kdepak jsou ty exploity na zranitelnosti Meltdown a Spectre? *CleverAndSmart Management Consulting* [online]. 16. únor 2018 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/tak-kdepak-jsou-ty-exploity-na-zranitelnosti-meltdown-a-spectre/

[4] ČERMÁK, Miroslav. NÚKIB vydal metodiku ke svému varování, zranitelnost se stále hledá. *CleverAndSmart Management Consulting* [online]. 9. leden 2019 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/nukib-vydal-metodiku-ke-svemu-varovani-zranitelnost-se-stale-hleda/

V neposlední řadě je třeba si také uvědomit, že jsou zde organizace, které jsou ze zákona povinny každý útok hlásit, a které z principu nemohou nefunkčnost svého systému zatajit, takže následná medializace těchto útoků pak rovněž vyvolává dojem, že je daný sektor hospodářství zasažen nejvíce, ale nemusí tomu tak vůbec být.

Kybernetické útoky a hrozby

Kybernetický útok (cyber attack) je dle NIST[1] definován jak útok v kyberprostoru s cílem narušit, zničit, odpojit nebo ovládnout daný systém či pozměnit nebo získat citlivá data. Výkladový slovník kybernetické bezpečnosti, zkr. VSKB, který používá Národní centrum kybernetické bezpečnosti, naproti tomu definuje kybernetický útok jako útok na IT infrastrukturu za účelem jejího poškození nebo získání citlivých či strategicky důležitých informací.[2]

Zcela tak ignoruje útok za účelem ovládnutí systému a jeho zneužití k dalšímu útoku, převodu finančních prostředků, pozměnění informací anebo způsobení nedostupnosti, a rovněž se vyhýbá uvedení zdroje útoku, **což vede ke zkreslení informací o tom, kolik útoků a na koho je vedeno.**[3]

S pojmem kybernetický útok pak velice úzce souvisí pojem kybernetická hrozba (cyber threat), který VSKB sice neobsahuje, ale která je dle NIST[4] definována jako událost, která má potenciál způsobit škodu na aktivech a vést k dalším následným ztrátám, vyplývajícím z narušení bezpečnosti informací a systémů.

Ve svém úzkém pojetí by pak za kybernetické hrozby bylo možno považovat jen hrozby přicházející z kyberprostoru, ovšem v širším pojetí tak, jak např. kybernetické hrozby v ČR vnímá aktuální Zákon o kybernetické bezpečnosti, zkr. ZoKB[5] resp. Vyhláška o kybernetické bezpečnosti VoKB,[6] musí být zohledněny i hrozby vyšší moci a fyzické povahy, které by rovněž mohly způsobit škody na informačních aktivech, kritické informační infrastruktuře, významných informačních systémech a systémech základních služeb.

Nejde však jen o to, že není exaktně definováno, co je to kybernetická hrozba, ale není definována ani taxonomie hrozeb, takže jejich subsumace je rovněž problematická, což ve výsledku vede k tomu, že přes snahu je nějakým způsobem evidovat, není zřejmé, ke kolika a jakým útokům v kyberprostoru vlastně dochází. (Předpokládáme, že útok je jen materializace samotné hrozby.) Byť zde určité snahy

---

[1] NIST. *Cyber Attack - Glossary | CSRC* [online]. B.m.: NIST, nedatováno. Získáno z: https://csrc.nist.gov/glossary/term/Cyber-Attack

[2] JIRÁSEK, Petr; NOVÁK, Luděk a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2015, s. 242.

[3] ČERMÁK, Miroslav. Co je a není kybernetický útok. *CleverAndSmart Management Consulting* [online]. 4. únor 2020 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/co-je-a-neni-kyberneticky-utok/

[4] NIST. *Cyber Threat - Glossary | CSRC* [online]. B.m.: NIST, nedatováno [vid. 4. březen 2019]. Získáno z: https://csrc.nist.gov/glossary/term/Cyber-threat

[5] *Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů*.

[6] *Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat*.

o definici kybernetických hrozeb samozřejmě byly[1] a jsou,[2] tak v praxi není tato taxonomie přesto dodržována,[3] což v konečném důsledku vede ke značnému zkreslení, protože dotčené subjekty neví, kam daný útok zařadit, nehledě na to, že ani neví, jak jej započítat v případě v čase opakovaného anebo místně mnohačetného výskytu.

Kybernetický útok pak na rozdíl od hrozeb může být veden jen z kyberprostoru a jeho cílem jsou informační aktiva a operační technologie. Za informační aktiva pak lze dle ISO 27005:2018[4] považovat data, informace a služby poskytované informačním systémem, které jejich vlastníkovi generují zisk. Zatímco informace a služby jsou tzv. primárními aktivy, tak informační systém, který se skládá z mnoha dalších komponent, pak představuje tzv. sekundární aktiva.

Zde je nutné si uvědomit, že byť jsou cílem útočníka zpravidla primární aktiva, tedy informace a služby poskytované daným informačním systémem, tak kybernetický útok je veden na sekundární aktiva, tedy samotný systém, síťovou infrastrukturu, servery, koncová zařízení a jejich uživatele, případně pak i na operační technologie.[5]

Vlastník je tedy nucen za účelem ochrany svých informačních aktiv a technologií zavést vhodná bezpečnostní opatření organizační a technické povahy, a to taková, která sama o sobě nebudou z pohledu celkových nákladů dražší než možná škoda, která by mohla vzniknout v přímé souvislosti s kybernetickým útokem.

Útočník pak v systému hledá jakoukoliv zranitelnost, které by mohl zneužít. Přičemž zranitelnost lze považovat buď za vlastnost aktiva, ale může se nacházet i v samotném bezpečnostním opatření, které může být nedostatečné, anebo zcela chybět, a pak může být s větším či menším úsilím překonáno.

Porozumění tomu, kdo a na koho útočí a s jakým cílem, pak umožňuje se i lépe a efektivněji bránit,[6] ovšem v reálné praxi dochází k tomu, že se např. v médiích stále častěji uvádí, že se ta či ona organizace v ČR stala obětí cíleného kybernetického útoku, např. nemocnice, což ale není pravda, jak později vyplynulo z vyšetřování a nikdo to již nedementoval, a naopak ještě uvedl, odkud byl útok veden.[7] Bezpečnostní komunita samozřejmě tuto analýzu široce diskutovala a odmítla ji,

[1] ENISA Threat Taxonomy - Portál veřejně přístupných dat EU [online]. [vid. 10. červen 2020]. Získáno z: https://data.europa.eu/euodp/en/data/dataset/enisa-threat-taxonomy-1

[2] SANS Institute: Reading Room - Threat Intelligence [online]. [vid. 9. červen 2020]. Získáno z: https://www.sans.org/reading-room/whitepapers/threatintelligence/paper/38360

[3] ČERMÁK, Miroslav. Cyber threat management: taxonomie hrozeb. *CleverAndSmart Management Consulting* [online]. 15. duben 2019 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/cyber-threat-management-taxonomie-hrozeb/

[4] ISO. *Norma ISO/IEC 27005:2018 Information technology. Security techniques. Information security risk management*. Červenec 2018.

[5] ČERMÁK, Miroslav. Provozní technologie: kybernetické útoky. *CleverAndSmart Management Consulting* [online]. 3. duben 2020 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/provozni-technologie-kyberneticke-utoky/

[6] SUNZI a Radim PEKÁREK. *Umění války = The art of war*. Brno: B4U, 2014. ISBN 978-80-87222-35-5.

[7] Místo kyberútoků na české nemocnice odhaleno. Stopy vedou na sever Moskvy - Seznam Zprávy [online]. [vid. 9. červen 2020]. Získáno z: https://www.seznamzpravy.cz/clanek/misto-kyberutoku-na-ceske-nemocnice-odhaleno-stopy-vedou-na-sever-moskvy-106710

ovšem v mainstreamových médiích, která primárně sledují nositelé rozhodnutí, se již tato informace neobjevila.

Jaksi je obecně ignorována skutečnost, že kromě cílených útoků zde již po mnoho let probíhají i útoky plošné, kdy si útočník svou oběť cíleně nevybírá, neboť je mu v zásadě jedno, koho napadne. Dále zde dochází k mylnému zobecňování dílčího jevu na celek, když je např. jen na základě identifikace škodlivého kódu anebo skenování portů v několika málo organizacích spadajících do určitého sektoru národního hospodářství vysloven bezpečnostními experty určité organizace závěr, že aktuálně probíhá cílený útok právě na daný sektor.[1]

S tím pak souvisí i mylné určení zdroje tohoto útoku, který bývá často zaměňován s jazykem použitým ve zdrojovém kódu malware po jeho dekompilaci. Zapomíná se na to, že s exploity se obchoduje stejně jako s jakoukoliv jinou komoditou a, že zvolený jazyk, ve kterém jsou zapsány proměnné, názvy funkcí a komentáře, může být rovněž záměr, jak svést případné vyšetřování jiným směrem anebo v rámci vedení hybridní války poukázat na jinou velmoc a na tu svést útok,[2] což vede ke značnému zkreslení toho, co se odehrává v kyberprostoru.

Skutečnost je taková, že na různé typy organizací jsou vedeny různé útoky, za kterými stojí různí agenti hrozeb nebo také cyber threat actors, kteří sledují i různé cíle. Běžně můžeme v literatuře anebo v bezpečnostních reportech narazit na tyto cyber threat actors:

- haktivisté (hacktivist) – reagují na určité společenské události, kroky vlády nebo korporací, mohou i nemusí být koordinováni, ale zpravidla jsou, aby jejich akce měla požadovaný efekt, tj. aby se o ní mluvilo, výsledkem je defacement webu, koordinovaný DDoS, využívají známých zranitelností a dostupných nástrojů, spíš než způsobit škodu se na sebe a na své téma snaží upozornit;
- kyberteroristi (cyber terrorist) usilují o narušení kritické informační infrastruktury a na rozdíl od hacktivistů je jejich cílem způsobení i co největší škody;
- kyberkriminálníci (cyber criminals) – organizované kriminální skupiny, jejichž motivem je získání finančních prostředků nebo ovládnutí infrastruktury k zastírání svých nelegálních aktivit, dochází zde ke krádeži osobních údajů, přihlašovacích údajů, převodu peněz z účtů, využívání již hotových nástrojů, zneužívání zranitelností nultého dne, nakupují již hotové exploit kity;
- hackeři (hackers) – napadají špatně zabezpečené systémy, zabývají se odhalováním zranitelností, vývojem a prodejem exploitů, záleží na nich, zda budou white hackeři anebo black hackeři a zda budou jednat v souladu se zákonem anebo se z nich stanou kriminálníci;

[1] Národní úřad pro kybernetickou a informační bezpečnost - Hrozba kybernetických útoků na nemocnice a jiné významné cíle ČR [online]. [vid. 9. červen 2020]. Získáno z: https://www.nukib.cz/cs/informacni-servis/aktuality/1425-hrozba-kybernetickych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/

[2] ČERMÁK, Miroslav. Kdo na nás útočí, nevíme, jen se to domníváme a pak z toho vyvozujeme dalekosáhlé závěry. *CleverAndSmart Management Consulting* [online]. 27. květen 2020 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/kdo-na-nas-utoci-nevime-jen-se-to-domnivame-a-pak-z-toho-vyvozujeme-dalekosahle-zavery/

- script kiddies – zpravidla neumí napsat vlastní kód, a proto stahují již hotové exploity z internetu a ty spouští proti nejrůznějším zdrojům, aby se mohli pochlubit mezi svými vrstevníky anebo tak činí prostě jen pro svoje potěšení a škody způsobují spíš svoji nerozvážností a neznalostí;
- státem sponzorované skupiny (nation-state sponsored, foreign nations) vedoucí útoky s cílem ochromit kritickou infrastrukturu protivníka, získat informace, zneužívají zranitelností nultého dne, které nakupují, případně je sami vyhledávají a vyvíjí vlastní exploity, napadají dodavatelsko-odběratelské mezičlánky, infikují HW, na rozdíl od kyberteroristů se snaží pracovat skrytě, aby nebyly odhaleny;
- konkurence (competitors, espionage) – konkurence dost často stojí za krádeží intelektuálního vlastnictví a průmyslovou špionáží, kterou může realizovat i v kyberprostoru;
- insideři (insiders, disgruntled employees) – nespokojení zaměstnanci, manažeři, dodavatelé zneužívají svého legitimního přístupu a znalosti business procesů a interních kontrol ke krádeži firemního know-how, chráněných receptur, klientského portfolia, převodu finančních prostředků, případně mohou spolupracovat s někým zvenku.

Pro úplnost je třeba dodat, že není úplně jasná hranice mezi jednotlivými agenty hrozeb a že vzhledem k tomu, že agentem hrozby je člověk, který se vyvíjí, a sleduje různé cíle, tak může v kyberprostoru rovněž zaujímat i různé role. Ze script kiddies se může stát hackerem, kyberkriminálníkem anebo dokonce i kyberteroristou. Trend je však jednoznačný, útoky se realizují primárně za účelem dosažení zisku a stále více se na těchto útocích podílí soukromý sektor.

Bohužel neschopnost určit zdroj hrozby pak často vede k mylnému závěru ohledně skutečného cíle probíhajícího útoku a rovněž pokud tyto informace vstupují do nejrůznějších bezpečnostních reportů, tak pak dochází i k vyvozování mylných závěrů ohledně skutečné situace v kyberprostoru.

Hrozby můžeme rozdělit mnoha různými způsoby. Nejjednodušší je dělení podle toho, jaký atribut bezpečnosti může být hrozbou narušen. Pokud důvěrnost, lze hovořit o **hrozbách pasivních**, protože nedochází ke změně stavu systému ani informací, pokud může dojít k narušení integrity a dostupnosti, lze hovořit o **aktivních hrozbách**, neboť jejich působením ke změně stavu dochází.[1]

Podle původce hrozby (threat agent) můžeme hrozby rozdělit na **hrozby způsobené lidmi** a **vyšší mocí** (vis maior). V prvním případě je to osoba, která realizuje danou hrozbu, ať už vědomě nebo nevědomě a nese za své jednání plnou odpovědnost, tak ve druhém případě za ní nikdo neodpovídá.[2]

Podle zdroje, tedy odkud hrozby přichází, je možné je ještě rozdělit na vnější a vnitřní, přičemž **vnější hrozby** pochází z vně organizace a jsou zcela mimo její kontrolu a **vnitřní hrozby** pak přichází z prostředí organizace, které má organizace

[1] JIRÁSEK, Petr; NOVÁK, Luděk a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2015, s. 242.
[2] KINCL, Jaromír; URFUS, Valentin a Michal SKŘEJPEK. *Římské právo*. Praha: C. H. Beck, 1995, s. 223. ISBN 978-80-7179-031-0. KINCL, Jaromír; URFUS, Valentin a Michal SKŘEJPEK. *Římské právo*. Praha: C. H. Beck, 1995, s. 223. ISBN 978-80-7179-031-0.

zpravidla možnost ovlivnit, neboť toto prostředí přímo utváří. Když tyto dva pohledy zkombinujeme, získáme v zásadě 4 zdroje hrozeb, které NIST 800-30[1] definuje takto:

- **úmyslné** (adversarial) realizované ze strany jednotlivců, organizovaných skupin, konkurence, státu. Úmyslné hrozby můžeme dále rozdělit podle toho, zda útočník vede útok na konkrétní subjekt anebo je mu jedno, který subjekt se stane jeho příští obětí. Subjektem se v tomto případě myslí buď infrastruktura (koncové zařízení, server, síťový prvek), anebo lidský operátor zastávající v daném systému jakoukoliv roli (uživatel, správce, vývojář). Kdy výsledkem těchto útoků je zpravidla získání informací, kompromitace systému nebo narušení jeho dostupnosti,
- **náhodné** (accidental), kdy se jedná o chybu zaměstnance, ať už uživatele nebo správce systému při vykonávání běžných denních činností. Náhodné nebo také neúmyslné hrozby jsou hrozby, kdy k narušení bezpečnosti došlo z důvodu nedbalosti nebo selhání zaměstnance, kterým svým konáním nebo naopak nekonáním narušení bezpečnosti způsobil. Přičemž je třeba rozlišovat mezi nedbalostí vědomou a nevědomou, protože zatímco v prvním případě zaměstnanec věděl, že by narušení bezpečnosti mohl způsobit, a v nepřiměřené míře spoléhal, že se tak nestane, tak ve druhém případě toto vůbec nepředpokládal,
- **strukturální** (structural), kdy došlo k selhání HW nebo SW ať už v důsledku stáří nebo překročení provozních parametrů. Některé tyto hrozby lze předvídat a předcházet jim v okamžiku, kdy se vytváří vanová křivka a sleduje životnost každé použité komponenty, provádí monitoring výkonnostních parametrů, realizuje kapacitní plánování a jsou připraveny příslušné scénáře,
- **environmentální** (environmental), kdy došlo k nějaké přírodní pohromě/katastrofě a k selhání infrastruktury, která je zcela mimo kontrolu organizace. Patří sem hrozby jako povodeň, požár, zemětřesení, tornádo a výpadek infrastruktury jako je voda, elektřina, telekomunikace, na kterých může být organizace rovněž závislá,

přičemž všechny výše uvedené typy hrozeb mohou mít v případě jejich realizace negativní dopad na informační systémy.

Úmyslné kybernetické hrozby mající povahu kybernetických útoků pak lze rozdělit z pohledu velikosti zásahu na útoky:

- **plošné**, kdy útočníkovi je v zásadě jedno, kdo se stane jeho obětí, a napadne **jakýkoliv subjekt**, která trpí **určitou zranitelností** (Při těchto útocích do určité míry záleží na úrovni zabezpečení ostatních subjektů na trhu, protože útočník realizuje úspory z rozsahu a cílí na tzv. low hanging fruit, tedy ty hůře zabezpečené subjekty;
- **cílené**, kdy útočník vede útok na **konkrétní subjekt** a hledá **jakoukoliv zranitelnost**, které by mohl zneužít. (U těchto typů útoků nehraje úroveň zabezpečení ostatních subjektů na trhu v podstatě žádnou roli, neboť útočník je připraven vyvinout nezměrné úsilí, prostředky a čas k dosažení svého cíle.)

Z pohledu předmětu cílení, byť to ne vždy musí být na první pohled zřejmé, je možné kybernetické útoky rozdělit na útoky vedené primárně na:

[1] NIST. *NIST Special Publication 800-30 Guide for Conducting Risk Assessments* [online]. B.m.: NIST. Září 2012. Získáno z: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

- **lidi**, kdy útočník **zneužívá technik sociálního inženýrství a nedostatečného bezpečnostního povědomí** a snaží se oběť přimět k tomu, aby mu poskytla informaci nebo provedla činnost, kterou on potřebuje,[1]
- **infrastrukturu**, kdy útočník **zneužívá zranitelností, které se nacházejí v návrhu, v kódu anebo implementaci** aplikace, systému nebo sítě, kdy žádná interakce ze strany uživatele není vyžadována.

Otázka je, proč jsou na některé firmy vedeny soustavné kybernetické útoky, zatímco na jiné prakticky vůbec? Na některé organizace jsou vedeny útoky jen proto, že jsou přítomny na internetu, zatímco na jiné proto, proč tam jsou. Obětmi kybernetických útoků a to jak plošných, tak i cílených se stále častěji stávají i malé a střední firmy.

Plošné útoky

Útočníkovi je v zásadě jedno, koho napadne, neboť skenuje určitý IP adresní rozsah, a hledá systémy trpící konkrétní zranitelností, rozesílá phishing e-maily, umísťuje exploit kity na napadené stránky a šíří trojanizované aplikace. Jednoduše používá jen základní vektory útoku a cílí na firmy, které otázku bezpečnosti moc neřeší, resp. ji neřeší vůbec. Neprovádí bezpečnostní osvětu svých zaměstnanců, a ti se pak stávají obětí triviálních phishingových kampaní a provozují neaktualizovaný systém obsahující známé zranitelnosti a chyby v konfiguraci. Kyberkriminálníci se jednoznačně snaží minimalizovat své náklady a v okamžiku, kdy se na internetu nachází velké množství firem, které bezpečnost absolutně neřeší, tak neztrácejí čas pokusem o průnik do firmy, která je na tom, co se týká bezpečnosti, podstatně lépe než ostatní. Z výše uvedeného vyplývá, že pokud na tom bude organizace lépe, než ostatní, a toho lze dosáhnout i s minimálními náklady, tak se významně snižuje riziko, že na ni bude veden kybernetický útok a stanete se další obětí. Ovšem pozor, toto tvrzení platí pouze u plošně vedených útoků, nikoliv cílených, kdy útočník neváhá k dosažení svého cíle vynaložit značné prostředky.

Cílené útoky

Cílené útoky jsou vedeny na organizace, které disponují citlivými informacemi, chráněnými recepturami, významným know-how v oblasti technologie výroby, pracují na vývoji syntetických materiálů, elektroniky, nanotechnologie, léčiv anebo zaujímají podstatné místo na trhu, případně jsou významným dodavatelem některé z výše uvedených organizací. Jinými slovy, kde nic není, ani hacker nebere. Pokud však výše uvedeným daná organizace nedisponuje, tak na ní APT útok s největší pravděpodobností nikdy veden nebude. To ovšem neznamená, že na ní nemůže být veden cílený útok ze strany konkurence, obzvlášť když se danému odvětví nedaří a přichází krize.

Náklady na zajištění odpovídající úrovně bezpečnosti před cílenými kybernetickými útoky jsou značné a útočník je ve výhodě. Je tomu tak proto, že útočníkovi stačí najít jen jednu jedinou zranitelnost, zatímco organizace musí najít pokud možno všechny a ty následně nechat odstranit. A vzhledem k množství

[1] MANN, Ian. *Hacking the human: social engineering techniques and security countermeasures*. Aldershot, England ; Burlington, VT: Gower, 2008. ISBN 978-0-566-08773-8.

zranitelností, kterými může každý informační systém trpět, to může být časově i finančně poměrně náročné.

Když tyto dva přístupy zkombinujeme, získáme matici v podobě *Tabulka 1 – typy útoků*, která zachycuje základní 4 typy kybernetických útoků a co je pro ně charakteristické.

Tabulka 1 – typy útoků

	Plošný (PS)	**Cílený (CS)**
stroje	▪ skenování určitého IP adresního rozsahu, v krajním případě celého internetu ▪ hledání **konkrétních** zranitelností ▪ zneužití konkrétní zranitelnosti ▪ začlenění do botnetu ▪ zneužití k dalšímu útoku např.: C&C, proxy, DDoS, phishing, SPAM, drop box, malvertising ▪ server side ransomware ▪ těžba kryptoměn (cryptojacking)	▪ sběr informací ▪ skenování pouze vybraného serveru nebo omezeného množství serverů ▪ hledání **jakékoliv** zranitelnosti ▪ zneužití jakékoliv zranitelnosti ▪ DoS, DDoS (aplikační, volumetrický) ▪ Změna obsahu webových stránek (defacement) ▪ Kompromitace (kompletní ovládnutí cílového systému) ▪ zneužití k dalšímu útoku, zpravidla APT
lidé	▪ **Sociální inženýrství + nízké bezpečnostní povědomí** ▪ Zranitelnosti (nultého dne výjimečně) ▪ drive-by download (malvertising) ▪ generické trojanizované aplikace ▪ phishing, ▪ SMShing, ▪ ransomware, premium SMS, cryptominery, bankware	▪ **Sociální inženýrství + zranitelnosti nultého dne** ▪ SEO poisoning ▪ DNS poisioning ▪ watering holes ▪ drive-by download ▪ zero-day exploit (ne nutně) ▪ specifické trojanizované aplikace ▪ spear phishing ▪ vishing ▪ SMShing ▪ CEO fraud, exfiltrace dat, přerušení provozu/výroby/služeb
	Plošný (PL)	**Cílený (CL)**

Zdroj: vlastní zpracování

Plošné útoky na lidi (PL)

Plošné útoky vedené na lidi spočívají nejčastěji ve zneužití technik sociálního inženýrství a nízkého bezpečnostního povědomí, a kdy je vyžadována větší či menší

interakce ze strany oběti. Nejčastějším vektorem útoku je phishingový, trojanizovaná aplikace nebo web zobrazující výzvu k instalaci aplikace.

Zde je třeba podotknout, že v podstatě každý se může stát obětí takovéhoto útoku, a dosažená úroveň formálního vzdělání a inteligence nehraje prakticky vůbec žádnou roli. Jde jen o to zvolit ten správný způsob.

V případě aktivního přístupu, který má zpravidla podobu phishingu, útočník rozesílá e-mail na velké množství adres, které buď koupil, stáhl z internetu anebo si je sám podle nějakého klíče vygeneroval. Samotný e-mail je pak zpravidla napsán tak, aby v příjemci zprávy vzbudil důvěru, emoce a zároveň ho dostal do časové tísně. Pokud e-mail přichází od nějaké autority či důvěryhodné instituce jako je banka, police, exekutorský úřad, pošta, je napsán správně česky a používá i stejný design, tak příjemce nevěnuje příliš pozornost tomu, kdo je uveden jako odesílatel a má tendenci obsahu zprávy důvěřovat.

Stejně tak, pokud e-mail přichází od osoby, se kterou příjemce běžně komunikuje, a tudíž takový e-mail očekává, ho nenapadne, že by mohl být počítač odesílatele napaden malwarem a e-mail odešel ze schránky odesílatele bez jeho vědomí. Žádoucí emoce, ať už negativní nebo pozitivní jsou pak v příjemci e-mailu vzbuzeny např. tím, že je mu vyhrožováno, že by vůči němu mohlo být vzneseno obvinění, bude muset uhradit pokutu anebo naopak něco může získat, přičemž musí reagovat do určité doby.

V okamžiku, kdy obsah e-mailu koresponduje a je zasazen do kontextu aktuálního dění a pohotově reaguje na aktuální politickou, kulturní či jinou společenskou událost, tak příjemce e-mailu vzhledem k množství podobných e-mailů přestává věnovat pozornost tomu, od koho e-mail přichází.

Kombinace těchto faktorů vede ke změně stavu mysli a snížené obezřetnosti. Když pak takový e-mail obsahuje přílohu nebo odkaz, tak je pak větší pravděpodobnost, že na ni příjemce e-mailu klikne a dojde ke spuštění škodlivého kódu nebo přesměrování na podvodnou stránku, kde je vyžadováno zadání citlivých údajů.

V případě spíše pasivního přístupu útočník začleňuje škodlivý kód do nějaké široce používané aplikace, dostupné mimo oficiální repository, ale ne nutně, a která vyžaduje vyšší než nezbytně nutná oprávnění, která musí uživatel povolit, dochází ke kompromitaci tímto způsobem.

Dalším možným vektorem útoku je zobrazení výzvy uživateli při jeho běžném surfování po internetu, kdy se na kompromitovaném webu zobrazí uživateli výzva napodobující systémové hlášení k instalaci falešného antiviru nebo jiného bezpečnostního produktu.

Nejčastějším výsledkem těchto útoků jsou zašifrovaná data na disku, uzamčené zařízení a nemožnost pracovat (ransomware), neautorizovaný převod finančních prostředků (bankware), požadavek na zaplacení jinak dojde ke zveřejnění citlivých dat (scareware) anebo je cílem útočníka těžba kryptoměny (cryptominery) či začlenění zařízení oběti do botnetu.

Tyto útoky se vyznačují velice nízkými náklady, a krátkou dobou přípravy i trvání, neboť útočník předem počítá s tím, že jeho útok bude poměrně brzy odhalen, protože

je pravděpodobné, že takovéhoto rozsáhlého útoku si někdo všimne a zareaguje na něj. Nicméně útočník realizuje úspory z rozsahu a v součtu může být výnos z jedné takové kampaně ve výši několika miliónů korun. Přičemž útočníkovi nic nebrání v tom, útok mírně modifikovat a realizovat jej opakovaně.

Plošné útoky na stroje (PS)

Útočník v tomto případě využívá skutečnosti, že každé zařízení může obsahovat nějakou zranitelnost, která mohla vzniknout v jakékoliv fázi SDLC, ať už na jeho samotném počátku, v rámci návrhu, nebo kdykoliv později během kódování anebo při jeho nasazení, kdy došlo k nevhodnému nastavení. Zařízení jednoduše nemusí být secure by design, secure by default a secure by deployment.

Přičemž útočník může danou zranitelnost odhalit sám, koupit ji na černém trhu anebo i oficiálně, neboť se zranitelnostmi se běžně obchoduje jako s jakýmikoliv jinými komoditami,[1] anebo se jedná o zranitelnost veřejně známou, pro kterou zatím nebyl vydán patch anebo byl a daný subjekt ji z nějakého důvodu nenasadil.

Plošné útoky na stroje resp. koncová zařízení a servery pak mohou být aktivní, kdy útočník skenuje určitý IP adresní rozsah, v krajním případě celý internet a hledá zařízení, které trpí jednou konkrétní zranitelností a té zneužívá, a to buď ručně, anebo automatizovaně za použití nějakého online nástroje typu Shodan, který s jistou nadsázkou tvrdí, že je schopen internet analyzovat v řádu sekund,[2] případně si útočník napíše za tímto účelem nástroj vlastní.

V případě spíše pasivního přístupu útočník škodlivý kód začlení do webových stránek, které má pod kontrolou (může se např. jednat o vložený iframe o nulové velikosti, skript, php kód) anebo jej vkládá na web jako běžný uživatel do diskusního fóra, případně škodlivý kód začleňuje do reklamního banneru, který se na webových stránkách zobrazuje v rámci výměnného reklamního systému a využívá skutečnosti, že ten kdo na danou webovou stránku zavítá, tak se nakazí. Jedná se o tzv. drive-by download malware.

V neposlední řadě může útočník začlenit škodlivý kód do široce používané aplikace, která zneužívá nějaké zranitelnosti v systému nebo jiné běžící aplikace a bez jakékoliv interakce s uživatelem dochází k exploitaci dané zranitelnosti a zajištění persistence.

Ve všech případech se pak kompromitované zařízení stává součástí celosvětového botnetu, který slouží útočníkovi anebo je prodáván za úplatu a může být snadno zneužit k dalším útokům. Anebo je dané zranitelnosti neprodleně zneužito k pokusu o okamžitou monetizaci, kdy útočník zašifruje veškerá data, a požaduje platbu za jejich dešifrování anebo stroj zneužije k těžbě nějaké kryptoměny.

Náklady na realizaci těchto útoků jsou poměrně nízké, tyto útoky mohou probíhat zcela automatizovaně a mohou zůstat i dlouhou dobu bez povšimnutí, neboť výsledkem útoku zpravidla bývá začlenění stroje do botnetu a jeho prodej nebo pronájem k dalšímu využití. A až v okamžiku, kdy dojde ke zneužití botnetu k dalším útokům, bývá odhalen.

[1] ZERODIUM - The Leading Exploit Acquisition Platform [online]. [vid. 17. únor 2019]. Získáno z: http://zerodium.com/

[2] Shodan [online]. [vid. 17. únor 2019]. Získáno z: https://www.shodan.io/

Cílené útoky na lidi (CL)

Při cílených útocích na konkrétní osoby v organizaci je rovněž zneužíváno technik sociálního inženýrství. Tyto útoky probíhají přes internet, e-mail a za použití dalších prostředků komunikace a v krajním případě dochází i k fyzickému průniku do prostředí organizace a kontaktování oběti ať už přímo nebo nepřímo. Tento případ ale není tak častý, protože pro útočníka představuje zvýšené riziko, že bude přistižen při činu.

Jedná se o tzv. piggybacking nebo také tailgating,[1] kdy se útočník pokusí dostat do budovy spolu s ostatními zaměstnanci, kdy s někým naváže rozhovor, nese objemnější předmět a nechá si podržet dveře, případně se vydává za někoho jiného. V krajním případě se nechá zaměstnat buď přímo v dané organizaci anebo v organizaci, od které organizace o kterou má primární zájem odebírá určité služby. V okamžiku, kdy útočník pronikne do prostředí dané organizace, tak může instalovat HW keylogger, falešné přístupové body (access point), vlastní síťové prvky a zaznamenávat přihlašovací údaje.

Útočník se snaží o své oběti získat maximum informací a to z veřejných zdrojů jako jsou např. sociální sítě, kde o sobě uživatelé sami informace uvádějí, webové stránky firmy, kde informace o svých zaměstnancích uvádí samotná firma anebo v médiích, kde informace uvádí nezávislí novináři a rovněž i z neveřejných interních zdrojů.

V těchto případech, dochází k falšování identity,[2] kdy se útočník vydává za jinou důvěryhodnou nebo blízkou osobu a volá do dané organizace a snaží se získat další informace nebo je zcizit (vishing), nebo zasílá na míru připravený e-mail (spear phishing), který na první pohled vypadá jako důvěryhodný a obsahuje přílohu, která zpravidla, ale ne nutně, zneužívá nějaké zranitelnosti nultého dne (zero day vulnerability) a v okamžiku, kdy na ni příjemce zprávy klikne, tak se spustí a provede perzistenci.

Nejčastějším vektorem útoku zůstává e-mail, jedná se o tzv. spear phishing nebo také whaling, kdy jsou vedeny na konkrétní osoby v organizaci a předchází mu pečlivá příprava, která může trvat i po dobu několika týdnů.

Další často používanou technikou je tzv. watering hole attack, kdy útočník umísťuje svůj škodlivý kód na důvěryhodné webové stránky, které oběť navštěvuje, a ty se zobrazí jen dané oběti např. za použití geoIP funkcionality, otisku počítače či pokročilejších technik jako je rozpoznávání obličeje, takže ke spuštění škodlivého kódu dojde jen v okamžiku, kdy z daného zařízení přistupuje konkrétní osoba.[3]

---

[1] ČERMÁK, Miroslav. Co je to piggybacking. *CleverAndSmart Management Consulting* [online]. 26. únor 2020 [vid. 10. červen 2020]. Získáno z: https://www.cleverandsmart.cz/co-je-to-piggybacking/

[2] ČERMÁK, Miroslav. Jak přes LinkedIn probíhají cílené kybernetické útoky na zaměstnance firem. *CleverAndSmart Management Consulting* [online]. 21. listopad 2016 [vid. 10. červen 2020]. Získáno z: https://www.cleverandsmart.cz/jak-pres-linkedin-probihaji-cilene-kyberneticke-utoky-na-zamestnance-firem/

[3] ČERMÁK, Miroslav. Na obzoru se objevují nové hrozby, třeste se! – 7. díl. *CleverAndSmart Management Consulting* [online]. 28. leden 2020 [vid. 20. březen 2020]. Získáno z: https://www.cleverandsmart.cz/na-obzoru-se-objevuji-nove-hrozby-treste-se-7-dil/

Poslední, ale neméně používanou technikou je pak pohození paměťového média (např. USB flash disku nebo SD karty) v prostorách organizace anebo v její těsné blízkosti, kdy útočník spoléhá na přirozenou lidskou zvědavost, tzv. baiting.

Cílené útoky na osoby jsou zpravidla součástí tzv. APT útoků. Náklady na realizaci těchto útoku jsou vyšší než v předchozích případech a vyžadují i podstatně delší přípravu a neumožňují realizovat úspory z rozsahu. Nicméně, příslušné techniky je možné opakovaně použít k útokům na další subjekty, obzvláště v případě použití tzv. zero day zranitelností a exploitů, neboť zpravidla nedochází k jejich medializaci. Délka trvání takovéhoto útoku se pohybuje v řádu měsíců a náklady na realizaci pak ve výši několik stovek tisíc až jednotek miliónů. Ale těmto vysokým nákladům pak na druhou stranu odpovídají i výnosy z těchto útoku, které se pohybují v řádech desítek až stovek miliónů korun. V ojedinělých případech pak i jednotek miliard, jako tomu bylo v případě útoků na SWIFT.[1]

Cílené útoky na stroje (CS)

Útočník v tomto případě hledá jakoukoliv zranitelnost, kterou by daný stroj mohl obsahovat. Používá za tímto účelem nějaký automatizovaný skener, kdy zjišťuje, jaké služby na daném serveru běží, a jaká zde běží verze OS a aplikací. Pokud automatizovaný skener zranitelností selže, tak pak útočník hledá zranitelnosti ručně. Následně se snaží jakékoliv zranitelnosti zneužít k průniku do systému nebo k narušení důvěrnosti, integrity nebo dostupnosti, to podle toho, co je jeho cílem.

V případě, že je cílem útočníka odepření služby, tak může realizovat aplikační nebo volumetrický DoS/DDoS útok, kdy daný systém, pokud před tímto typem útoku není chráněn, se tímto stává nedostupným.

Náklady na realizaci těchto útoků jsou minimální a škody pak mohou být značné. Vzhledem k tomu, že útočník nemá z tohoto útoku zpravidla přímý zisk, jsou tyto útoky vedeny s cílem získat výpalné, kdy je tímto útokem jen vyhrožováno, a útočník rozesílá tzv. extortion letter a případně demonstruje svou schopnost v podobě kratšího útoku o menší intenzitě.

V případě, že k útoku skutečně dojde a má delší dobu trvání a to v řádu hodin až dnů, tak je realizován státem sponzorovanou skupinou a lze jej označit za kyber-terorismus a je zpravidla veden na KII, VIS nebo ZS.

V některých případech může také dojít k tomu, že útok byl cílený, ale může se navenek jevit jako plošný, např. v okamžiku, kdy útočník cílí na firmu využívající služeb třetí strany provozující např. datové centrum a v důsledku útoku jsou pak nedostupné systémy všech zákazníka daného poskytovatele.

Náklady na realizaci těchto útoků, vyjma DDoS, které lze pořídit za pouhých několik USD, se pohybují v řádech stovek tisíc, výnosy pak minimálně v řádech jednotek miliónů korun.

[1] ČERMÁK, Miroslav. Roste počet útoků na SWIFT. *CleverAndSmart Management Consulting* [online]. 31. květen 2016 [vid. 10. červen 2020]. Získáno z: https://www.cleverandsmart.cz/roste-pocet-utoku-na-swift/

Zřetězené útoky

Na tomto místě je nutné uvést, že v praxi pak dochází k řetězení těchto útoků, takže jestliže došlo v rámci PL ke kompromitaci blíže neurčitých koncových zařízení a ty byly začleněny do botnetu, tak pak z těchto zařízení mohou být následně vedeny CS, např. DDoS.

A rovněž z nich mohou být vedeny CL, např. spear phishing, což sice nebývá tak časté, ale nelze tuto možnost zcela vyloučit. Servery, které byly kompromitovány v rámci PS, mohou být zneužity PL, kdy např. na nich může být umístěn phishing web anebo se na nich může nacházet malware a rovněž i k CL, kdy vybraný server může sloužit jako watering hole.

Vyloučit samozřejmě nelze ani situaci, kdy dochází k CL nebo CS a jen za tím účelem, aby pak následně bylo možné vést další CL nebo CS, k čemuž dochází v rámci APT útoků, které představují specifický typ útoků, jsou přesně cílené a jsou často vedeny jak na konkrétní osoby, tak i stroje. A mohou využívat plošných útoků jako kouřové clony k realizaci vlastního cíleného útoku na konkrétní subjekt.

V okamžiku, kdy dojde ke kompromitaci stroje, ať už v důsledku PL, PS, CL nebo CS, tak z něj může být opět veden PL, PS, CL nebo CS. Teoreticky může nastat 16 různých útoků, nicméně v reálném světě ne všechny kombinace nastávají, a proto je možné uvažovat spíše jen o osmi různých útocích. Je tomu tak proto, že např. k cílenému útoku na konkrétní osobu je efektivnější odeslat e-mail ze schránky osoby, které daná osoba důvěřuje nebo exploit umístit na web, který daná osoba navštěvuje.

Při plošném útoku, kdy je útočníkovi jedno čí stroj kompromituje, tak může umístit exploit na jakýkoliv web, který má určitou návštěvnost anebo rozeslat e-mail na všechny adresy, které najde v adresáři, neboť jeho cílem je co největší zásah.

Podobně při cíleném útoku na konkrétní server je útočníkovi v zásadě jedno z jakého zařízení DDoS útok nebo hacking provede, a využije za tímto účelem jakékoliv zařízení, které bude pod jeho kontrolou, aby zahladil stopy a znesnadnil tak své odhalení.

APT

Na některé společnosti jsou vedeny útoky jen proto, že jsou přítomny na internetu, na jiné však proto, co dělají, to je případ tzv. APT útoků.

Dle SANS[1] byl pojem APT poprvé použit v roce 2006 analytiky United States Air Force, a měl vyjadřovat pokročilou a přetrvávající hrozbu (Advanced Persistent Threat, zkr. APT).

Ve výkladovém slovníku NIST[2] je pak APT hrozba definována jako hrozba, kdy útočník disponuje sofistikovanými znalostmi a významnými zdroji, které mu umožňují vytvářet si příležitosti k dosažení svých cílů, které obvykle vedou k průniku a uhnízdění se v infrastruktuře organizace, která je předmětem zájmu útočníka za účelem získání

[1] BINDE, Beth E.; McREE, Russ a Terrence J. O'CONNOR. Assessing Outbound Traffic to Uncover Advanced Persistent Threat. nedatováno, s. 35.

[2] NIST. *advanced persistent threat (APT) - Glossary | CSRC* [online]. B.m.: NIST, nedatováno [vid. 6. březen 2019]. Získáno z: https://csrc.nist.gov/glossary/term/advanced-persistent-threat

informací, narušení provozu, nebo způsobení škody a to hned anebo kdykoliv v budoucnu, opakovaně, během delšího časového období, kdy se útočník brání odhalení, maskuje se, zahlazuje stopy a zároveň si zajišťuje potřebnou úroveň interakce za účelem splnění svých cílů.

Musa[1] pak dodává, že APT útok je kontinuální proces, kdy dochází k pečlivě připravenému, postupnému a nenápadnému hackování vyhlédnuté entity.

Naproti tomu dle Bruce Schneiera nejsou pokročilé a přetrvávající hrozby (Advanced Persistent Threat, zkr. APT) nic jiného než cílené útoky[2] a jedná se tak trochu o buzzword, a jak tvrdí Čermák, mohlo by se stejně tak hovořit i o léty prověřených technikách, Aged Proven Techniques nebo ještě poetičtěji Ancient Proven Techniques,[3] protože se vždy jedná o kombinaci technik sociálního inženýrství a zranitelností nultého dne. To potvrzují i nejrůznější analýzy, např. společnost Imperva tvrdí, že mnohdy je spíše než nějakých pokročilých technik využito technik naprosto běžných.[4]

Dle FireEye se doba po kterou zůstává APT útok nedetekován, postupně zkracuje, v roce 2011 to bylo 416 dní, tedy více než rok, zatímco v roce 2018 už jen 78 dní, tedy něco přes dva měsíce.[5] To však v mnoha případech může být stále doba dostatečně dlouhá k dosažení cíle, protože dle společnosti Verizon je cíle dosaženo zpravidla za mnohem kratší dobu.[6]

Předmětem APT útoků jsou zpravidla organizace, které jsou součástí kritické infrastruktury státu, provozující kritickou informační infrastrukturu, zkr. KII, významné informační systémy, zkr. VIS a systémy základních služeb, zkr. SZS, disponují cenným know-how, které je předmětem průmyslové špionáže anebo realizují velké obraty peněz.

Tyto útoky jsou realizovány ze strany vysoce organizovaných a dost často i státem sponzorovaných skupin a probíhají i po dobu několika měsíců až let. A byť jsou náklady na tyto útoky značné a pohybují se v řádu stovek tisíc až miliónů, tak výnosy se pohybují v řádu vyšších stovek miliónů až jednotek miliard. V ČR nebylo evidováno příliš mnoho útoků tohoto typu. V posledním roce byl v zásadě zdokumentován jen jeden případ úspěšného útoku, kdy došlo ke kompromitaci,

---

[1] MUSA, Sam. Advanced Persistent Threat - APT | Dr. Sam Musa - Academia.edu [online]. [vid. 6. březen 2019]. Získáno z: https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT

[2] SCHNEIER, Bruce. Advanced Persistent Threat (APT) - Schneier on Security. *Schneier on Security* [online]. 9. listopad 2011 [vid. 4. březen 2019]. Získáno z: https://www.schneier.com/blog/archives/2011/11/advanced_persis.html

[3] ČERMÁK, Miroslav. APT je jen další buzzword. *CleverAndSmart* [online]. 27. únor 2012 [vid. 4. březen 2019]. Získáno z: https://www.cleverandsmart.cz/apt-je-jen-dalsi-buzzword/

[4] *HII_The_Non-Advanced_Persistent_Threat.pdf* [online]. [vid. 8. březen 2019]. Získáno z: https://www.imperva.com/docs/HII_The_Non-Advanced_Persistent_Threat.pdf

[5] FIREEYE. *M-Trends 2019* [online]. B.m.: FireEye. 2019 [vid. 8. březen 2019]. Získáno z: https://content.fireeye.com/m-trends

[6] *DBIR_2018_Report.pdf* [online]. [vid. 8. březen 2019]. Získáno z: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

a to v nejmenované finanční instituci.[1] Ovšem skutečný počet obětí těchto útoků neznáme, což opět vede k určitému zkreslení, neboť naše představa je utvářena jen na základě dostupných informací.

Samotný APT útok lze rozdělit do několika na sebe navzájem navazujících fází, přičemž jejich počet a pojmenování se autor od autora výrazně liší. Některé zdroje uvádí 12 fází,[2] jiné 10 fází,[3] 7 fází[4] a některé jen 5 fází.[5] Onen rozdíl je však způsoben jen detailním rozepisováním čtyřech základních fází, kterými jsou: příprava, průnik, kompromitace a dokončení.

- **Příprava** – v této fázi se útočník snaží o předmětu svého cíle zjistit co nejvíce informací. Informace čerpá z veřejných zdrojů, jako jsou sdělovací prostředky, výroční zprávy, webové stránky dané organizace a sociální sítě. Vytváří si tak představu o tom, jak veliká daná organizace je, jaká je její organizační struktura, kdo jsou její zaměstnanci, na jakých pozicích se nachází, a s jakými dalšími organizacemi v odběratelsko-dodavatelském řetězci organizace spolupracuje, protože mnohdy je snazší vést útok na organizaci, která např. dodává HW a SW vybavení a začlenit do něj backdoor, nechat se u dané organizace zaměstnat a tím následně získat fyzický přístup do organizace, která je primárním cílem útočníka. V této fázi dále dochází k zjišťování informací o provozovaných systémech, probíhá skenování služeb vystavených do internetu, a jejich odpovědí na dotazy. Následně pak probíhá hledání zranitelností v provozovaných technologiích a vývoj nebo nákup exploitů potřebných k jejich zneužití, případně k začlenění backdooru do HW nebo SW používaného danou organizací. Tato přípravná fáze, kdy dochází rovněž k vytvoření nezbytné infrastruktury, C&C serverů, phishingových, e-mailů, falešných identit, apod. může probíhat i po dobu několika týdnů až měsíců a útočník při ní může využívat technik sociálního inženýrství, navazovat i intimní vztahy se zaměstnanci dané organizace za účelem získání informací nebo přístupu, neboť mnohdy je spolupráce s někým zevnitř nezbytná. Tuto přípravnou fázi tak lze rozdělit v zásadě na dvě části sběr informací (external reconnaissance) a vývoj nástrojů a přípravu infrastruktury k realizaci útoku (weaponization).
- **Průnik** - v této fázi dochází k fyzickému nebo vzdálenému průniku do prostředí dané organizace, ať už v přestrojení nebo jako skutečný zaměstnanec třetí strany a zapojením vlastního zařízení, např. falešného access pointu, HW keylogeru

[1] *martin-hlavac-skutecnost-muze-byt-horsi-nez-ocekavani-dsm-2020.pdf* [online]. [vid. 9. červen 2020]. Získáno z: https://www.aec.cz/cz/ztisku/martin-hlavac-skutecnost-muze-byt-horsi-nez-ocekavani-dsm-2020.pdf

[2] Advanced Persistent Threats - Learn the ABCs of APT: Part A [online]. [vid. 6. březen 2019]. Získáno z: https://www.secureworks.com/blog/advanced-persistent-threats-apt-a

[3] RADZIKOWSKI, Przemek Shem. CyberSecurity: Expanded Look at the APT Life Cycle and Mitigation. *Dr.Shem* [online]. 11. únor 2016 [vid. 8. březen 2019]. Získáno z: http://DrShem.com/2016/02/11/cybersecurity-expanded-look-apt-life-cycle-mitigation/

[4] LACEY, David a INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. *Advanced persistent threats: how to manage the risk to your business* [online]. Rolling Meadows, IL: ISACA, 2013 [vid. 8. březen 2019]. ISBN 978-1-60420-347-9. Získáno z: http://www.books24x7.com/marc.asp?bookid=62388

[5] MILLS, Elinor. Attack on RSA used zero-day Flash exploit in Excel. *CNET* [online]. [vid. 8. březen 2019]. Získáno z: https://www.cnet.com/news/attack-on-rsa-used-zero-day-flash-exploit-in-excel/

do vnitřní sítě organizace anebo dodáním HW nebo SW opatřeného backdoorem. Případně může dojít k podvržení falešné aktualizace podepsané klíčem, ke kterému je vydán certifikát od důvěryhodné certifikační autority, která byla za tímto účelem již dříve kompromitována.[1] Daleko častěji se však můžeme setkat s napadením jiného webu, který organizace navštěvuje a umístění exploitu tam (watering hole attack), a v okamžiku, kdy jej zaměstnanec dané organizace navštíví, tak dojde k exploitaci a stažení škodlivého kódu do jeho počítače (drive-by download). Anebo, což je vůbec nejčastější případ, může dojít k distribuci škodlivého kódu e-mailem (spear phishing) nebo na médiu (baiting), které útočník pohodí např. na parkovišti nebo na střeše budovy. I v této fázi se využívá technik sociálního inženýrství v kombinaci se zranitelnostmi nultého dne. Táto fáze má nejkratší trvání, a zpravidla probíhá vzdáleně přes internet, neboť se zde útočník vystavuje největšímu riziku, že si probíhajícího útoku někdo všimne, a proto se vše odehraje během několika málo minut nebo hodin. Tato fáze se dá opět rozdělit do několika částí, doručení exploitu (deliver), spuštění exploitu (exploit) obsahující nálož (payload), kdy se útočník pokouší o zvýšení svých oprávnění v napadeném systému (escalate privileges) zajištění perzistence (establish persistence) a instalace komponenty za účelem vzdáleného přístupu (remote access trojan, zkr. RAT) do napadeného systému.

- **Kompromitace** - v této fázi se již útočník nachází v prostředí organizace, kde kompromitoval jedno či více koncových zařízení nebo serverů, zajistil si v nich perzistenci a nyní se seznamuje se síťovou infrastrukturou (internal reconnaissance), a vyhledává systémy, které by mohl dále napadnout (colaterall movement). Za tímto účelem zachycuje přihlašovací údaje, pořizuje snímky obrazovky, zaznamenává činnosti zaměstnanců ve formě videa, a tyto informace pak zasílá na C&C server útočníka k analýze a stanovení dalšího postupu a to tak dlouho, dokud není dosaženo cíle. Komunikace s C&C serverem pak probíhá šifrovaně, je schována do DNS komunikace anebo je využito pokročilé lingvistické steganografie, kdy informace jsou umně schovány v prostém textu nacházejícím se na webech, které uživatel běžně navštěvuje, jako jsou sociální sítě, O365 nebo Google. Vlastní malware na koncových zařízeních a serverech organizace má pak často podobu tzv. fileless malwaru, tedy bezsouborového malwaru, který se ukrývá do registrů, a běžných procesů a maximálně využívá součástí systému, jako je powershell, apod a je proto velice obtížné jej odhalit. Tato fáze, podobně jako fáze přípravy může trvat poměrně dlouho a to po dobu několika měsíců až let, než se útočníkovi podaří zcela ovládnout daný systém nebo získat přístup k citlivým informacím, které jsou předmětem jeho zájmu.
- **Dokončení** - v okamžiku, kdy dojde ke kompromitaci cílového systému, kompletního ovládnutí infrastruktury, výroby, služby, vyřazení daného systému z provozu anebo získání citlivých informací, které jsou shromážděny (data gathering) a připraveny ke zkopírování na server útočníka (data exfiltration), tak se přesouváme do poslední fáze. Tato fáze trvá rovněž poměrně krátce, ovšem délka jejího trvání do značné míry závisí na tom, co je cílem útočníka, protože pokud je

[1] ČERMÁK, Miroslav. DigiNotar: Operation Black Tulip - CleverAndSmart [online]. 9. září 2011 [vid. 17. únor 2019]. Získáno z: https://www.cleverandsmart.cz/diginotar-operation-black-tulip/

cílem útočníka exfiltrace informace, tak nemusí být vůbec odhalen a přístup k informacím si může udržovat po poměrně dlouhou dobu. Zde jen záleží na tom, jaké je ono množství informací, které potřebuje exfiltrovat, tedy zkopírovat do tzv. drop zóny a zda si někdo všimne zvýšeného provozu, či jiné anomálie, ke které ale také nemusí dojít, pokud bude jako drop zóna zvolen např. cloud Microsoftu, Googlu anebo Amazonu, který organizace běžně využívá. V případě nedostupnosti anebo pozměnění informací či dat pak zpravidla dojde k nějaké škodě a v tu chvíli se i rozjíždí vyšetřování, a je zahájen audit a forenzní analýza. Zde pak záleží na tom, zda se útočníkovi podařilo malware, a případné účty a logy odstranit a jak zkušený je analytik provádějící forenzní analýzu, a zda najde stopy po přítomnosti malwaru v systému anebo dokonce samotný malware.

Pravděpodobnost realizace hrozby může ovlivňovat spousta faktorů, obzvlášť pokud se jedná o úmyslné hrozby. Už samotné aktivum a vidina potenciálního zisku může útočníka přitahovat a činit pro něj dané aktivum atraktivní.

To je i důvod, proč na některé organizace jsou útoky vedeny častěji než na jiné, a na některé vůbec. Nejčastěji se však uvádí tři faktory, které tuto pravděpodobnost ovlivňují, jsou jimi motiv, příležitost a schopnost.

- **Motiv** - může být různý, může se jednat o přímý finanční zisk, což je nejčastější případ, či nepřímý, spočívající v získání nějaké výhody, třeba i tím, že druhé straně vznikne škoda, ale může se jednat i o pomstu, touhu po respektu a uznání. Motiv sám o sobě není dostačující, neboť pokud daná osoba nemá příležitost hrozbu realizovat anebo nedisponuje odpovídajícími znalostmi, nemůže danou hrozbu s úspěchem realizovat.
- **Příležitost** - zde je rozhodující, zda je možné vést útok přes internet anebo je nutné se nacházet na stejné síti anebo se dostat do fyzického kontaktu s předmětným aktivem. V okamžiku, kdy je možné vést útok přes internet, tak se pravděpodobnost hrozby podstatně zvyšuje. Ovšem i když má osoba příležitost hrozbu realizovat, tak to neznamená, že ji realizuje, neboť ještě musí mít dostatečně silný motiv a disponovat i odpovídajícími znalostmi.
- **Schopnost** - čím nižší jsou nároky na její realizaci, tedy znalosti a dovednosti, a jestli jsou tyto nároky nízké a v krajním případě ji může realizovat v podstatě každý uživatel internetu, tak se tím podstatně zvyšuje pravděpodobnost, že dojde k její realizaci. Ale i zde platí, že i když bude daná osoba disponovat danou schopností a dokázala by útok realizovat, tak musí mít i motiv a příležitost.

Z výše uvedeného vyplývá, že tyto faktory nelze vyhodnocovat odděleně, ale je třeba je vnímat komplexně, neboť, vždy musí být přítomny všechny tři, aby došlo k realizaci samotné hrozby. Na druhou stranu je třeba připustit, že v okamžiku, kdy bude existovat dostatečně silný motiv a útočník bude disponovat i odpovídajícími finančními prostředky, tak si může najmout někoho, kdo má dané schopnosti a dokáže si vytvořit i odpovídající příležitosti k tomu, aby hrozbu realizoval.

Jednoduše tak nelze od počtu potenciálních útočníků odvozovat pravděpodobnost realizace hrozby, a tvrdit, že v okamžiku, kdy danou schopností a příležitostí disponuje jen pár osob na světě, tak je pravděpodobnost takové hrozby nízká. Tuto hypotézu potvrzují i nejrůznější státem sponzorované útoky nebo útoky

realizované vysoce organizovanými skupinami, kdy došlo ke kompromitaci i velice dobře zabezpečených informačních systémů a k obrovským finančním ztrátám.

Na základě výše uvedených skutečností a rešerše bezpečnostních reportů byly v rámci expertní skupiny formulovány jednotlivé hrozby. Vzhledem k množství kybernetických hrozeb byly vzaty v úvahu jen ty, které mají nějaký potenciál způsobit větší škodu anebo již nějakou škodu způsobily a to na základě veřejně zdokumentovaných případů konkrétních útoků[1] a rovněž i těch, které byly řešeny v rámci uzavřené bezpečnostní komunity, a nemohou být z důvodu zachování mlčenlivosti zveřejněny. Těmito hrozbami jsou jak plošné, tak i cílené útoky, jejichž cílem je:

- **odepření služby** (Denial of Service, zkr. DoS) a tím způsobení nedostupnosti daného systému pro jeho konzumenty, přičemž předmětem hodnocení jsou skutečné DoS útoky, nikoliv jen výhružné e-maily adresované čelním představitelům organizace, tzv. extortion letters, ve kterých útočník vyhrožuje, že když organizace do určité doby nezaplatí, tak že útok provede a přitom ani nedisponuje takovou silou, aby byl schopen útok realizovat po dostatečně dlouhou dobu. Za sledované období došlo k několika masivním DDoS útokům na vybrané cíle v ČR a to v roce 2011 a 2013, což neznamená, že v dalších letech již k DDoS útokům nedocházelo, docházelo, a dochází k nim každý rok, ale již nebyly schopny způsobit viditelný výpadek, neboť na ně bylo včas reagováno;
- **ovládnutí systému** (System Possession, zkr. SP) a způsobení škody a to změnou konfigurace ICS/SCADA zařízení sloužících k řízení výroby,[2] smazáním anebo zašifrováním dat s úmyslem zastavit produkci, snížit výkon, generovat zmetky, způsobit v dané zemi chaos, ohrozit životy, poškodit zdraví, životní prostředí, ochromit její infrastrukturu nebo napomoci chybným rozhodnutím, apod. což může v některých případech vést i k ukončení činnosti dané organizace na trhu, např. z důvodu ztráty důvěry ze strany zákazníků. Vzhledem k tomu, že v tomto případě je motiv útočníka způsobit především škodu, přičemž nelze odmítnout hypotézu, že díky tomu může získat i nemalý finanční prospěch, tak zpravidla je tento útok realizován tzv. APT skupinami a je veden na subjekty, které zaujímají dominantní postavení na trhu, a jsou součástí kritické infrastruktury státu a jsou pravděpodobnější v zemích, kde je nižší index bezpečí;
- **získání citlivých informací** jako je know-how (Know how, zkr. KH) jako je unikátní výrobní postup, chráněné receptury anebo i obchodního tajemství a jeho následný prodej konkurenci nebo využití ve vlastním podnikání, což v konečném důsledku může vést k podstatnému propadu v příjmech a v delším horizontu pak i k ukončení činnosti organizace na trhu neboť již nebude konkurenceschopná. Tyto útoky jsou realizovány jak jednotlivci, např. nespokojenými zaměstnanci, ze strany

[1] ČERMÁK, Miroslav. Seznam organizací v ČR, na které byl veden kybernetický útok. *CleverAndSmart Management Consulting* [online]. 15. leden 2020 [vid. 26. duben 2020]. Získáno z: https://www.cleverandsmart.cz/seznam-organizaci-v-cr-na-ktere-byl-veden-kyberneticky-utok/

[2] MINAŘÍK, Pavel. Bezpečnost průmyslových sítí a systémů SCADA/ICS. *Bezpečnost průmyslových sítí a systémů SCADA/ICS* [online]. 2. říjen 2018 [vid. 12. březen 2019]. Získáno z: https://m.systemonline.cz/rizeni-vyroby/bezpecnost-prumyslovych-siti-a-systemu-scada-ics.htm

konkurence anebo vysoce organizovanými APT skupinami, kterým jde o získání citlivých informací. Na území ČR pak lze zaznamenat především krádež informací ze strany stávajících zaměstnanců, kteří jsou nespokojeni a jsou připraveni si informace o klientech odnést sebou a mnohdy je i cíleně a soustavně po delší dobu shromažďují;

- **získání osobních údajů** klientů nebo zaměstnanců (Personal Data, zkr. PD) za účelem jejich přetažení, prodání anebo zveřejnění a poškození v důsledku uplatnění sankcí dle GDRP, která nesmí být likvidační. Ne všechny organizace však zpracovávají všechny typy osobních údajů. Ty nemají stejnou hodnotu, vždy je proto nutné uvažovat o tom, kolik osobních údajů unikne a jak moc jsou citlivé a zneužitelné. Zpravidla pak dochází ke zcizení osobních údajů klientů ze strany zaměstnance dané společnosti anebo je únik informací výsledkem činnosti hackera, kterému se podařilo získat přístup do DB přes webovou aplikaci dostupnou z internetu, Výsledná škoda pak odpovídá výši pokuty, ztráty obchodní příležitosti a odlivu části klientů. Odliv klientů v důsledku úniku informací však bývá často značně přeceňován a reálné případy spíše ukazují, že k nějakému masivnímu odlivu klientů z důvodu úniku osobních údajů nedochází, což je dáno především tím, že se útoky týkaly organizací s dominantním postavením na trhu aneb naopak menších organizací, kterým klienti i přesto zachovali věrnost;
- **odčerpání peněz** (Money Transfer, zkr. MT) z firemního účtu organizace, což může být výsledkem generického i specifického malware, které útočníkovi umožnilo získat kontrolu nad počítačem, ze kterého je možné tyto transakce realizovat. V případě domácností je pravděpodobnost nákazy výrazně vyšší než v organizacích, protože v organizacích zpravidla provádí finanční transakce jen pověřená osoba a dost často jen na dedikovaném zařízení, které je vybaveno čtečkou čipových karet apod. Škoda je v takovém případě odvislá od objemu prostředků na bankovním účtu a především pak výši limitů finančních transakcí a průměrně převáděné částce. V případě domácností se pohybuje v řádu desítek tisíc, v případě organizací pak ve stovkách tisíc a u bank, kde se již ale jedná výhradně o cílené útoky, pak v miliónech korun, přičemž útočník se snaží převést jen takovou částku, aby si toho nikdo nevšiml, anebo aby si toho všiml pozdě a on mezitím stihl tuto částku vyvést z bankovního oběhu;[1]
- **zašifrování dat** (Ransomware, zkr. RW) a požadování výpalného za jejich opětovné dešifrování, přičemž ransomwarem je zde míněn výhradně plošně šířený ransomware, který cílí na koncová zařízení, připojené síťové disky a servery, nikoliv wiper, jehož cílem je smazat data v konkrétní organizaci, a který je uvažován již v rámci hrozby SP. Většinu ransomware útoků pak tvoří útoky na koncová zařízení, to v konečném důsledku vede k nemožnosti přistupovat k datům uloženým lokálně a na síťových discích a dále pak do jednotlivých systémů, zpracovávat poštu, komunikovat přes internet, či provádět správu zařízení a obsluhovat klienty. Menší procento útoků se pak týká přes internet dostupných serverů s SQL databází, kdy útočník šifruje nikoliv soubory, ale obsah databáze a i v tomto případě požaduje platbu za zpřístupnění klíče a dešifrování. Výnosnost z těchto útoků je však

[1] *Pravo_a_bezpecnost_3-2018.pdf* [online]. [vid. 12. březen 2019]. Získáno z: https://www.vske.cz/data/ke_stazeni/pravo_a_bezpecnost/Pravo_a_bezpecnost_3-2018.pdf

podstatně nižší, neboť DB bývají zpravidla pravidelně zálohovány a jsou promptně obnoveny na rozdíl od koncových zařízení a síťových disků, které dost často zálohovány nejsou. Výsledná škoda se pak odvíjí od toho, zda má oběť aktuální a čitelnou zálohu dat, ze které je schopna data obnovit. Odstranění ransomware nebývá zpravidla problém, pohybuje v řádu jednotek tisíc na jeden počítač, škoda však spočívá především ve ztrátě pro organizaci důležitých dat, která pokud nejsou zálohována, se v mnoha případech již nepodaří obnovit nikdy anebo až za několik měsíců, kdy se bezpečnostním expertům podaří získat šifrovací klíč nebo odhalit chybu v kódu samotného ransomware. Tak dlouho nemůže většina organizací čekat, a tak pokud nejsou schopny data obnovit, tak zaplatí požadovanou částku, jež se pohybuje od několika desítek do stovek tisíc.

Závěr

Byli identifikováni jednotliví aktéři v kyberprostoru, kteří zcela zásadním způsobem formují a utvářejí povědomí odborné i laické veřejnosti a na zcela konkrétních příkladech z posledních let bylo demonstrováno, jak dochází k záměrnému zkreslování situace v kyberprostoru.

Dále byly popsány jednotlivé typy kybernetických hrozeb, vztahy mezi plošnými a cílenými útoky a bylo rovněž poukázáno na skutečnost, jak dlouhodobě neřešené a přitom na první pohled naprosto fundamentální otázky týkající se kybernetické bezpečnosti, jako jsou definice základních pojmů a jejich rozdílné vnímání, mohou vést k diametrálně odlišné interpretaci toho, co se odehrává v kyberprostoru.

Jinými slovy, z analýzy dostupných zdrojů vyplynulo, že situace v kyberprostoru je záměrně zkreslována a neexistence jednotné taxonomie hrozeb a exaktní definice základních pojmů vede k tomu, že autoři bezpečnostních reportů používají různé názvosloví a kategorie hrozeb. Stejně tak i manažeři kybernetické a informační bezpečnosti a CSIRT týmy, které na probíhající kybernetické útoky reagují, a reportují jednotlivé kybernetické útoky nadřízeným orgánům, což situaci ještě zhoršuje.

Vzhledem k omezenému rozsahu tohoto článku nejsou uvedeny následky zmíněných útoku ani dopad na ekonomiku, který z výše uvedených skutečností vyplývá, ale pozorný čtenář si jistě tyto následky sám domyslí.

Literatura

Advanced Persistent Threats - Learn the ABCs of APT: Part A [online]. [vid. 6. březen 2019]. Získáno z: https://www.secureworks.com/blog/advanced-persistent-threats-apt-a

BINDE, Beth E, Russ MCREE a Terrence J O'CONNOR. Assessing Outbound Traffic to Uncover Advanced Persistent Threat. nedatováno, s. 35.

ČERMÁK, Miroslav. DigiNotar: Operation Black Tulip - CleverAndSmart [online]. 9. září 2011 [vid. 17. únor 2019]. Získáno z: https://www.cleverandsmart.cz/diginotar-operation-black-tulip/

ČERMÁK, Miroslav. APT je jen další buzzword. *CleverAndSmart* [online]. 27. únor 2012 [vid. 4. březen 2019]. Získáno z: https://www.cleverandsmart.cz/apt-je-jen-dalsi-buzzword/

ČERMÁK, Miroslav. Jak odstranit jakýkoliv malware pomocí aplikace SpyHunter a jí podobných. *CleverAndSmart Management Consulting* [online]. 8. únor 2016 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/jak-odstranit-jakykoliv-malware-pomoci-aplikace-spyhunter-a-ji-podobnych/

ČERMÁK, Miroslav. Jak přes LinkedIn probíhají cílené kybernetické útoky na zaměstnance firem. *CleverAndSmart Management Consulting* [online]. 21. listopad 2016 [vid. 10. červen 2020]. Získáno z: https://www.cleverandsmart.cz/jak-pres-linkedin-probihaji-cilene-kyberneticke-utoky-na-zamestnance-firem/

ČERMÁK, Miroslav. Roste počet útoků na SWIFT. *CleverAndSmart Management Consulting* [online]. 31. květen 2016 [vid. 10. červen 2020]. Získáno z: https://www.cleverandsmart.cz/roste-pocet-utoku-na-swift/

ČERMÁK, Miroslav. Cyber threat management: taxonomie hrozeb. *CleverAndSmart Management Consulting* [online]. 15. duben 2019 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/cyber-threat-management-taxonomie-hrozeb/

ČERMÁK, Miroslav. NÚKIB vydal metodiku ke svému varování, zranitelnost se stále hledá. *CleverAndSmart Management Consulting* [online]. 9. leden 2019 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/nukib-vydal-metodiku-ke-svemu-varovani-zranitelnost-se-stale-hleda/

ČERMÁK, Miroslav. Co je a není kybernetický útok. *CleverAndSmart Management Consulting* [online]. 4. únor 2020 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/co-je-a-neni-kyberneticky-utok/

ČERMÁK, Miroslav. Co je to piggybacking. *CleverAndSmart Management Consulting* [online]. 26. únor 2020 [vid. 10. červen 2020]. Získáno z: https://www.cleverandsmart.cz/co-je-to-piggybacking/

ČERMÁK, Miroslav. Hybridní hrozby. *CleverAndSmart Management Consulting* [online]. 18. duben 2020 [vid. 10. červen 2020]. Získáno z: https://www.cleverandsmart.cz/hybridni-hrozby/

ČERMÁK, Miroslav. Kdo na nás útočí, nevíme, jen se to domníváme a pak z toho vyvozujeme dalekosáhlé závěry. *CleverAndSmart Management Consulting* [online]. 27. květen 2020 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/kdo-na-nas-utoci-nevime-jen-se-to-domnivame-a-pak-z-toho-vyvozujeme-dalekosahle-zavery/

ČERMÁK, Miroslav. Na obzoru se objevují nové hrozby, třeste se! – 7. díl. *CleverAndSmart Management Consulting* [online]. 28. leden 2020 [vid. 20. březen 2020]. Získáno z: https://www.cleverandsmart.cz/na-obzoru-se-objevuji-nove-hrozby-treste-se-7-dil/

ČERMÁK, Miroslav. Provozní technologie: kybernetické útoky. *CleverAndSmart Management Consulting* [online]. 3. duben 2020 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/provozni-technologie-kyberneticke-utoky/

ČERMÁK, Miroslav. Seznam organizací v ČR, na které byl veden kybernetický útok. *CleverAndSmart Management Consulting* [online]. 15. leden 2020 [vid. 26. duben 2020]. Získáno z: https://www.cleverandsmart.cz/seznam-organizaci-v-cr-na-ktere-byl-veden-kyberneticky-utok/

DBIR_2018_Report.pdf [online]. [vid. 8. březen 2019]. Získáno z: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

ENISA Threat Taxonomy - Portál veřejně přístupných dat EU [online]. [vid. 10. červen 2020]. Získáno z: https://data.europa.eu/euodp/en/data/dataset/enisa-threat-taxonomy-1

FIREEYE. *M-Trends 2019* [online]. B.m.: FireEye. 2019 [vid. 8. březen 2019]. Získáno z: https://content.fireeye.com/m-trends

HII_The_Non-Advanced_Persistent_Threat.pdf [online]. [vid. 8. březen 2019]. Získáno z: https://www.imperva.com/docs/HII_The_Non-Advanced_Persistent_Threat.pdf

ISO. *Norma ISO/IEC 27005:2018 Information technology. Security techniques. Information security risk management*. červenec 2018

JIRÁSEK, Petr; NOVÁK, Luděk a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2015, s. 242.

KINCL, Jaromír; URFUS, Valentin a Michal SKŘEJPEK. *Římské právo*. Praha: C. H. Beck, 1995. ISBN 978-80-7179-031-0.

LACEY, David a INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. *Advanced persistent threats: how to manage the risk to your business* [online]. Rolling Meadows, IL: ISACA, 2013 [vid. 8. březen 2019]. ISBN 978-1-60420-347-9. Získáno z: http://www.books24x7.com/marc.asp?bookid=62388

MALÝ, Robert. Tak kdepak jsou ty exploity na zranitelnosti Meltdown a Spectre? *CleverAndSmart Management Consulting* [online]. 16. únor 2018 [vid. 9. červen 2020]. Získáno z: https://www.cleverandsmart.cz/tak-kdepak-jsou-ty-exploity-na-zranitelnosti-meltdown-a-spectre/

MANN, Ian. *Hacking the human: social engineering techniques and security countermeasures*. Aldershot, England ; Burlington, VT: Gower, 2008. ISBN 978-0-566-08773-8.

martin-hlavac-skutecnost-muze-byt-horsi-nez-ocekavani-dsm-2020.pdf [online]. [vid. 9. červen 2020]. Získáno z: https://www.aec.cz/cz/ztisku/martin-hlavac-skutecnost-muze-byt-horsi-nez-ocekavani-dsm-2020.pdf

MILLS, Elinor. Attack on RSA used zero-day Flash exploit in Excel. *CNET* [online]. [vid. 8. březen 2019]. Získáno z: https://www.cnet.com/news/attack-on-rsa-used-zero-day-flash-exploit-in-excel/

MINAŘÍK, Pavel. Bezpečnost průmyslových sítí a systémů SCADA/ICS. *Bezpečnost průmyslových sítí a systémů SCADA/ICS* [online]. 2. říjen 2018 [vid. 12. březen 2019]. Získáno z: https://m.systemonline.cz/rizeni-vyroby/bezpecnost-prumyslovych-siti-a-systemu-scada-ics.htm

Místo kyberútoků na české nemocnice odhaleno. Stopy vedou na sever Moskvy - Seznam Zprávy [online]. [vid. 9. červen 2020]. Získáno z: https://www.seznamzpravy.cz/clanek/misto-kyberutoku-na-ceske-nemocnice-odhaleno-stopy-vedou-na-sever-moskvy-106710

MUSA, Sam. Advanced Persistent Threat - APT | Dr. Sam Musa - Academia.edu [online]. [vid. 6. březen 2019]. Získáno z: https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT

Národní úřad pro kybernetickou a informační bezpečnost - Hrozba kybernetických útoků na nemocnice a jiné významné cíle ČR [online]. [vid. 9. červen 2020]. Získáno z: https://www.nukib.cz/cs/informacni-servis/aktuality/1425-hrozba-kybernetickych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/

NIST. *NIST Special Publication 800-30 Guide for Conducting Risk Assessments* [online]. B.m.: NIST. září 2012. Získáno z: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

NIST. *advanced persistent threat (APT) - Glossary | CSRC* [online]. B.m.: NIST, nedatováno [vid. 6. březen 2019]. Získáno z: https://csrc.nist.gov/glossary/term/advanced-persistent-threat

NIST. *Cyber Attack - Glossary | CSRC* [online]. B.m.: NIST, nedatováno. Získáno z: https://csrc.nist.gov/glossary/term/Cyber-Attack

NIST. *Cyber Threat - Glossary | CSRC* [online]. B.m.: NIST, nedatováno [vid. 4. březen 2019]. Získáno z: https://csrc.nist.gov/glossary/term/Cyber-threat

Pravo_a_bezpecnost_3-2018.pdf [online]. [vid. 12. březen 2019]. Získáno z: https://www.vske.cz/data/ke_stazeni/pravo_a_bezpecnost/Pravo_a_bezpecnost_3-2018.pdf

RADZIKOWSKI, Przemek Shem. CyberSecurity: Expanded Look at the APT Life Cycle and Mitigation. *Dr.Shem* [online]. 11. únor 2016 [vid. 8. březen 2019]. Získáno z: http://DrShem.com/2016/02/11/cybersecurity-expanded-look-apt-life-cycle-mitigation/

SANS Institute: Reading Room - Threat Intelligence [online]. [vid. 9. červen 2020]. Získáno z: https://www.sans.org/reading-room/whitepapers/threatintelligence/paper/38360

Shodan [online]. [vid. 17. únor 2019]. Získáno z: https://www.shodan.io/

SCHNEIER, Bruce. Advanced Persistent Threat (APT) - Schneier on Security. *Schneier on Security* [online]. 9. listopad 2011 [vid. 4. březen 2019]. Získáno z: https://www.schneier.com/blog/archives/2011/11/advanced_persis.html

SUNZI a Radim PEKÁREK. *Umění války = The art of war*. Brno: B4U, 2014. ISBN 978-80-87222-35-5.

Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

Zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů.

ZERODIUM - The Leading Exploit Acquisition Platform [online]. [vid. 17. únor 2019]. Získáno z: http://zerodium.com/

R E S U M É

Tento příspěvek se zamýšlí nad tím, jak kriticky nahlížet na aktuální situaci v kyberprostoru, identifikuje jednotlivé aktéry v kyberprostoru, kteří vytvářejí mediální obraz a jejich motivaci, popisuje plošné a cílené útoky a rozdíly mezi nimi a uvádí, co způsobuje ono informační zkreslení a navrhuje možný seznam kybernetických hrozeb.

Klíčová slova: kybernetické hrozby, kybernetické útoky, plošné útoky, cílené útoky, APT útoky.

S U M M A R Y

ČERMÁK, Miroslav: IDENTIFICATION OF KEY FACTORS INFLUENCING SUBJECTIVE PERCEPTION OF EVENTS IN CYBERSPACE

This work deals with how to critically examine the current situation in cyberspace, identifies individual actors in cyberspace who create a media image and their motivation, describes widespread and targeted attacks and the differences between them, and states what causes information bias and proposes a list of threats.

Keywords: cyber threat, cyber attacks, bulk attack, targeted attack, APT attacks.