Medializované útoky na IS firem, institucí a státu

Martin Holoubek

2017

Fakulta informačních technologií

Informační bezpečnost

Obsah

Klíčová slova

IT hrozby, útoky, infrastruktura, medializace, hacking, bezpečnost státu

Abstrakt

V textu této práce se zaměřujeme na medializované útoky cílené na informační systémy firem, institucí a států. V první části práce je čtenář seznámen se základními principy a dělením kybernetických útoků a jejich možných cílů.

V další části práce zaměřujeme na jednotlivé medializované kauzy, které vešly v obecné povědomí. Tyto vybrané útoky podrobněji v práci rozebíráme z různých pohledů a hodnotíme je podle různých kritérií. Text zakončujeme shrnutím současného stavu.

Úvod

V současné době, kdy se počítačová bezpečnost opakovaně dostává na přední stránky novin, je nutné řešit bezpečnost infomačních systémů na několika úrovních. Útoky nově nepřichází pouze z vnějšího prostoru, ale stále častěji mají svůj původ uvnitř organizace, či firmy. Společnosti se tomuto stavu postupně přizpůsobují.

Tempo implementace bezpečnostních opatření, i přes růst zájmu ze strany médií, zůstává žalostné. Neuplyne jediný týden, kdy by do večerních zpráv nepronikla zpráva o úniku citlivých dat, napadení informačních systémů a dalších bezpečnostních problémech.

V textu této práce se nejdříve zaměříme na obecnou charakteristiku počítačových systémů a útoku, které na ně mohou cílit. Později si vybereme několik medializovaných útoku, popíšeme si je z několika pohledů a pokusíme se zhodnotit míru jejich závažnosti.

V závěru práce si zrekapitulujeme možné principy obrany proti útokům mířeným na informační systémy a popíšeme náš pohled na budoucnost.

Medializované útoky na IS firem, institucí a státu

Podle zprávy společnosti Symantec za rok 2015 bylo v témže roce vytvořeno 430 milionů kusů malwaru, uniklo 560 milionů citlivých záznamů a celkem bylo medializováno 1 211 případů úniku citlivých dat s upozorněním, že trend bude pokračovat (Symantec, ISTR 2016, 2016).

Když se na tato ohromující čísla podíváme optikou roku 2017, zjistíme, že společnost růst dokonale odhadla. Počet uniklých záznamů se meziročně zdvojnásobil a také téměř všechna ostatní měřítka vzrostla.

Zásadní zvýšení počtu útoku zaznamenala zejména kategorie ransomware, tedy vyděračského softwaru, který cílí na finanční odměnu získanou od společností. Dalším oblíbeným cílem se staly také cloudové služby. Do budoucna společnost předpokládá prudké zvýšení zájmu ze strany útočníků zejména o platformu IoT a nové monetární systémy založené na blockchainu (Symantec, ISTR 2017, 2017).

V optice současného dění, kdy jsou týden, co týden reportovány nové bezpečnostní útoky a příslušné úniky dat, je pouze otázkou času, kdy se obětí stane libovolná společnost, či instituce.

Rozdělení

Abychom si mohli podrobněji rozdělit případné útoky na informační systému, je nutné tento pojem vysvětlit.

Informační systém lze popsat jako soubor lidí, technických prostředků a programů, zabezpečující sběr, přenos a zpracování dat (MOLNÁR, 2009, str. 13).

Způsoby dělení informačních hrozeb:

- Podle způsobu zveřejnění – V ideálním případě je útok v co nejkratším čase sdílen se zasaženými klienty tak, aby měli čas reagovat a podniknout

případné protiakci k omezení následků. Dalším krokem zasažené společnosti by mělo být zveřejnění detailů útoku a také opatření implementovaných jako budoucí prevence.

- Podle motivace útočníka – Typickou motivací je zisk, v některých případech mu však může jít o poškození dobrého jména firmy, či získání utajovaných informací. Vyskytují se také útoky, jejichž cílem je poškození infrastruktury a technického vybavení cíle. V případě jednotlivců může být motivací také snaha upozornit na sebe, či na bezpečnostní problémy.
- Podle typu cíle – Útočník se může zaměřit konkrétně na jednu danou společnost v případě cíleného útoku, nebo může vytvořit útok obecného charakteru. Ten svým plošným účinkem může postihnout různorodé systémy a cíle.
- Podle typu útočníka – Za největšími útoky stojí organizované skupiny, kterým jde o případný zisk, případě jsou sponzorovaná státem. O jejich původu se však často vedou spekulace. Pouze výjimečně se objevují útoky vedené jednotlivcem – v takových případech se často jedná o vynesení interních informací. Často se také objevují útoky na objednávku, zejména v případě útoků typu DDoS.
- Podle způsobu útoku – V cílených útocích jsou často exploitovány dané bezpečnostní slabiny systému tak, aby se útočník dostal k určitému danému cíli. Opačným přístupem jsou hromadné, či plošné útoky, které používají různorodou směs technik a cílí na co největší zásah (MOLNÁR, 2009).

Nejznámější útoky

Yahoo, 2013, 2014

Společnosti Yahoo v roce 2013 unikla téměř 1 miliarda záznamů. Stejný proces se zopakovat o rok později, kdy uniklo dalších 500 milionů uživatelských záznamů. Až o několik let později (2017) společnost přiznala, že celkem unikly 3 miliardy údajů o uživatelích.

Tyto údaje obsahovaly přihlašovací údaje včetně jmen, emailových adres, telefonních čísel a otisků hesel.

Podstatou útoku bylo několik chyb ve webové části portálu. Ten byl zranitelný vůči přihlášení pomocí modifikované cookie v prohlížeči. Útočníkům tak stačilo vytvořit speciální hodnotu cookie ve webovém prohlížeči k získání plnohodnotného přístupu k uživatelským účtům.

Společnost byla médii kritizována za laxní přístup k celé události a pozdní zveřejnění, čímž byla znemožněna včasná reakce zasažených uživatelů. Například únik dat z podzimu 2013 byl nahlášen až v prosinci 2016, tady více než tři roky po samotném útoku.

Následně bylo detekováno několik pokusů o přeprodej uživatelských dat na černém trhu zejména na síti darknet. Celkovou šíři důsledků není možné, kvůli závažnosti úniku a zároveň nedostatku informací, odhadnout. Očekává se ale, že dopady odezní až za několik let.

Původ

Sama společnost Yahoo označila jako původce útoku útočníky sponzorované státem. Přesto, že nikoho přímo nejmenovala, panuje všeobecné podezření, že útok pocházel z Číny, nebo Ruska. Tyto údaje však mohou sloužit pouze jako zastírací manévr ze strany společnosti Yahoo.

Dopad

Tlak na postiženou společnost, která již v době útoků čelila odlivu zákazníků, byl enormní. Následky byly podpořeny i faktem, že pod značku Yahoo spadá větší množství společností, mezi nimiž uživatelé sdíleli své účty a přihlašovací údaje.

V důsledku tlaku byla značka Yahoo transformována do nové pod jménem Altaba.

Equifax, 2017

Společnosti Equifax, které se zabývá vývojem globálních informačních systému, ohlásila v září 2017 průnik do svých systémů a únik údajů o celkem 143 milionech klientů. I přes na první pohled nižší počet záznamů je únik velmi vážný, protože data obsahovala velmi citlivé konkrétní údaje.

Jednalo se zejména o identifikační údaje osob, čísla pojištění, emailové účty, čísla kreditních karet atd. Jde tak o jeden z nejzávažnějších útoků posledních let. Zejména čísla pojištění jsou ve Spojených státech kritickým údajem, které slouží pro přístup žadatelů do systému hypoték. Únik může být tedy snadno zneužitelný a již nyní se objevují první napadení uživatelé (ALFRED NG, 2017).

Nejpravděpodobnějším vektorem útoku je bezpečnostní chyba webové stránky, pomocí níž získali útočníci přístup k databázi uživatelů.

Původ

V tomto případě se zdá, že hlavní motivace útočníků byla finanční stránka. Citlivé údaje lze typicky prodat na černém trhu za velmi vysoké ceny. Další možností je přímé využití získaných dat skupinou útočníků například v bankovních podvodech, vydírání, či použitím počítačových útoků přímo na uživatele.

Dopad

Protože se jedná o nový útok, není možné posoudit celkový dopad na společnosti a zasažené klienty. Z chování společnosti je ale možné vypozorovat snahu vyhnout se zodpovědnosti (ALFRED NG, 2017).

Kreditu společnosti nepřidává fakt, že tři nejvyšší manažeři prodali své části akcií těsně před oznámením útoku. Navíc stránky vytvořené pro napadané uživatele za účelem ověření, zda se na ně únik vztahuje, trpěly bezpečnostními trhlinami a byly opakovaně napadnuty.

Společnosti je také vytýkáno, že na pozici člověka zodpovědného za bezpečnost systém byla dosazena nekompetentní osoba (Burns, 2017).

Ebay, 2014

V roce 2014 rozeslala společnost Ebay žádost na své zákazníky o změnu přístupových údajů. Došlo totiž k masivnímu úniku osobních dat včetně jmen, uživatelských údajů, otisků hesel, telefonních čísel apod. Celkem bylo zasaženo cca 140 milionů účtů (Cox, 2014).

Společnost dále prohlásila, že zcizená databáze neobsahovala žádná data finančního charakteru, díky čemuž byl celkový dopad problému částečně snížen. Mluvčí také prohlásila, že podrobnosti o obsahu uniklých dat, ani detailní postup útoku nebudou zveřejněny s cílem ochránit zákazníky společnosti.

Původ

Vedení společnosti zveřejnilo informace o způsobu, jakým se útočníci dostali do interního systému. V první řadě se podařilo získat sociálním inženýrstvím přihlašovací údaje jednoho ze zaměstnanců do administračního rozhraní. Další postup útočníků vedl k překonání nízké ochrany uvnitř interní sítě a získání zmíněných dat (Cox, 2014).

Zajímavostí je informace, že útočníci měli přístup do celého systému celkem 229 dní, během nichž je nikdo v systému nedokázal identifikovat (Coty, 2014).

Dopad

Podle vlastních slov přistoupila společnost k problému s extrémní závažností s cílem ochránit zákazníky a potenciální cíle dalších případných útoků.

Přes veškerou snahu se společnost nevyhnula vyšetřování ze strany Amerických úřadů. Celková ztráta na dobrém jménu se nedá jednoduše vyčíslit, ale v obratech tak velké firmy musí jít o značnou částku.

Ashley Madison, 2015

15. července 2015 oznámila skupina The Impact Team úspěšně provedený útok na seznamovací web Ashley Madison. Pod výhružkou zveřejnění uniklých dat požadovala okamžité ukončení služby (Madison, 2016).

Z počátku společnost Madison napadení popírala a vyjadřovala jistotu, že žádné údaje odcizeny nebyly. Během měsíce po ohlášení, však byla útočníky zveřejněna celá uniklá databáze o velikosti téměř 60 GB dat. Experti potvrdili validitu dat, které byly navíc podepsané PGP klíčem (Lamont, 2016).

Původ

Skupina, která na seznamovací službu zaútočila prohlásila, že jejich motivací bylo pouze poukázat na neschopnost společnosti zajistit bezpečnost dat svých klientů a další její nekompetenci.

Dopad

Protože se jednalo o únik dat seznamovací služby, byla většina z nich citlivého charakteru. Po zveřejnění databáze se někteří ze zákazníků se stali terčem návazných útoků a vydírání. Jsou známy případy politiků, kteří čelili silné kritice,

za jejich chování na síti. Na sociálních sítích vznikly skupiny, které vyhledávali veřejně známé osobnosti a na základě uniklých dat je pranýřovaly.

Následkem masivního úniku citlivých údajů a byla tak u mnoha uživatelů ztráta soukromí s dopady v různých rovinách. Existují případy osobních útoků, rozpadů manželství, a dokonce i sebevražd. Poměrně častým důsledkem úniku se stalo vydírání (HOSIE, 2017).

Celkově měla kauza na společnost Ashley Madison destruktivní dopad. Všeobecný laxní přístup společnosti vyústil v prudký nárůst zájmu médií následovaný ztrátou důvěry ze strany klientů (Lamont, 2016).

Sony PlayStation Network, 2011

V dubnu 2011 došlo k vypnutí serveru PlayStation Network, určeném k online hraní počítačových her, ze strany společnosti Sony. Později společnost přiznala, že zastavení služby mělo být preventivní obranou vůči probíhajícím útokům.

Bezpečnostní politika Sony, které nedostatečně vynucovala šifrování ukládaných dat, připustila únik dat v čitelné podobě. To se týkalo například uživatelských údajů, hesel a čísel kreditních karet. Aby mohli uživatelé síť využíval bylo původně nutné zadat číslo kreditní karty spolu s dalšími citlivými údaji (Stuart & Arthur, 2011).

Sony později přiznalo, že bezpečnost nebyla prioritou při návrhu sítě a že tím nepřímo vystavili uživatele zbytečnému riziku.

Později dokonce došlo k únikům komunikace útočníků, kdy se dva hackeři domlouvali na způsobu prolomení bezpečnostního perimetru. Přímo bylo zmíněno, že Sony sbírá neuvěřitelné množství informací o svých uživatelích, což nemusí být legální.

Původ

Celkově se únik dat týkal 55 milionů připojených konzolí PlayStation 3 a 77 milionů připojených uživatelů. Původně obviňovaná skupina Anonymous se od útoku distancovala. Technicky byl útok proveden pomocí SQL injection a převzetím databáze (wired.com, 2011).

Předpokládá se spojitost v prolomením ochrany PlayStation 3, která byla kráce před tím tzv. jailbreakována. Předpokládá se tedy, že interní síť se nedokázala vypořádat s útokem, který vycházel právě z takto upravených konzolí. Tyto herní stroje se totiž nacházely v chráněné zóně interní sítě. Je tak možné předpokládat, že Sony s takovým scénářem nepočítalo.

Dopad

Společnosti Sony bylo vytýkáno, že se plně nevěnovala bezpečnostní problematice své infrastruktury. Dále byla médii často diskutována reakční doba, kdy samotné ohlášení útoků trvalo několik dní, což mohlo útočníkům poskytnout náskok.

Mluvčí prohlásila, že útok na jejich síť byl částečně identifikován v počátečních fázích, protože však sít při své velikosti byla v té době oblíbeným terčem, nebyla mu věnována pozornost. Vše se změnilo až později, když došlo k úniku samotných uživatelských dat.

Aby společnost částečně napravila svou reputaci, informovala uživatele přímo emailem, doporučila změnu údajů a sledování pohybů na účtech. Při aktualizaci SW herní konzole PlayStation 3 byli lidé nuceni změnit heslo ke svému účtu, aby se zmírnil možný dopad. Dále byl vytvořen web FAQ, kde uživatelé mohli najít často kladené otázky týkající se úniku dat (Stuart & Arthur, 2011).

Apple iCloud, 2014

V roce 2014 uniklo na veřejnost množství fotografií a osobních údajů celebrit, zejména žen. Množství těchto fotek, které obsahovaly nahotu, byly nahrány na server imgur a reddit.

Tento útok vzbudit pozornost veřejnosti o bezpečnost cloudových řešení a také o bezpečnost uživatelů jako takovou. Znakem tohoto útoku je fakt, že nedošlo k přímému prolomení bezpečnostního perimetru služby. Napadeny byly jednotlivé účty a to poměrně neoriginálním útokem (Apple, 2014).

Na přímém vyšetřování spolupracoval Apple spolu s FBI. V souvislosti v útokem bylo odsouzeno několik občanů USA, Ryan Collins na 18 měsíců a Edward Majerczyk na 9 měsíců (Yuhas, 2016).

Původ

Navzdory původním předpokladům, že útok cílil na samotnou službu iCloud se později ukázalo, že za únikem stála chyba v API. Pomocí ní bylo možné zkoušet libovolné množství pokusů o přihlášení heslem bez uzamknutí účtu. Nedocházelo tedy v lockoutu. Bylo navíc zjištěno, že tento bruteforce útok byl podpořen phishingovou kampaní cílenou na jednotlivé celebrity.

Vyšetřování ukázalo, že útoky a sběr materiálů probíhal po několik měsíců, kdy společnost Apple nebyla schopná akci detekovat.

Dopad

Mimo přímý dopad na společnost Apple a jeho reputaci, vzbudil únik debatu ve veřejném prostoru. Apple byl kritizován za nedostatečnou informovanost veřejnosti a laxní přístup k bezpečnosti. Začalo se také více debatovat o bezpečnostní cloudových služeb a lze prohlásit, že incident měl nepřímo i preventivní dopad na bezpečnost ostatních služeb (ALEX HEATH, 2014).

V přímém důsledku útoku se společnost Apple rozhodla implementovat vícefaktorovou autentizaci a emaily notifikující uživatele o přístupu do účtu.

Stuxnet, 2010

V roce 2010 objevila běloruská firma VirusBlokAda nový druh počítačového červa. Již v době nálezu se odhadovalo, že již byl v oběhu po několik měsíců.

Zvláštností bylo, že se nacházel v systémech po celém světě, ve kterých však neprojevoval žádnou aktivitu a nepůsobil žádné škody (Economist, 2010).

Pozornost výzkumníků upoutalo několik odlišností od běžně se vyskytujícího malware. Program byl neobvykle veliký (0.5 MB), byl vytvořen kombinací několika programovacích jazyků a zejména útočil hned na několik 0-day zranitelností v softwaru společností Microsoft a Siemens.

Červ otestoval, zda se nachází v systému, kde je používán řídící software od společnosti Siemens. V takovém případě otestoval několik dalších podmínek a spustil útok.

Dopad

Původní cíl nebyl z analýzy zřejmý. Teprve po úniku informací o explozi v Íránském jaderném zařízení došlo k propojení viru se explozí v Íránu. Jedná se tak o první známý červ v historii, který zaútočil na průmyslové systémy SCADA.

Pomocí dat zjištěných z infikované sítě se červ dostal přímo do odstředivek na štěpný materiál a pozměnil hodnoty nastavení. Nepatrně se zvýšila rychlost procesu, čímž docházelo k rezonanci a následnému zničení zařízení (Erben, 2014).

Zajímavostí je, že útok byl tak precizní, že senzory až do poslední chvíli ukazovaly očekávané hodnoty a nechal obsluhu zcela nepřipravenou (Beaumont, 2010).

Původ

Cílený útok na jaderné zařízení není ve schopnostech jednotlivců, ani organizovaných skupin. Od počátku tak byly z útoku viněny státy jako je Rusko a Čína s historií v oboru.

Během kauzy Assange, kdy uniklo množství citlivých informací americké armádě vyšlo najevo, že za útokem stály pravděpodobně Spojené státy a Izrael.

Techniky byl úkol, tedy zničení jaderného zařízení, úspěšně splněn. I když mnoho lidí se domnívá, že útok pouze zvýšil snahu Íránu o vytvoření jaderného materiálů a stavbu hlavice (Beaumont, 2010).

Estonské volby, 2007

V roce 2007 autority v Tallinu rozhodly, že dojde k odstranění památníku 2. světové války, který oslavoval Ruskou účast na osvobozování. Rusko varovalo Estonskou stranu z možných následků (DAVIS, 2007).

Krátce poté mnoho Estonců zjistilo, že nefunguje množství webových služeb včetně online novin, státních webů a online bankovnictví.

Později vyšlo najevo, že se nejedná o výpadek, či interní chybu, ale o distribuovaný útok typy DDoS. Počátek útok byl načasován na půlnoc 9. května, kdy Rusko slaví konec 2. světové války v Evropě.

Dopad na Estonskou infrastrukturu byl kritický. Zejména s přihlédnutím k faktu, že již v roce 2007 bylo země silně závislá na internetu (Hall, 2017).

Původ

Bylo zjištěno, že útokem stál 22letý ruský mladík, který v Rusku zorganizoval skupinu pro-Kremelsky laděných přátel. Ruští vlastenci chtěli útokem na

infrastrukturu upozornit na odstranění památníku. Jejich vinou však Estonské straně vznikla značná škoda (TAMKIN, 2017).

Dopad

Kromě finančního dopadu vedl útok ke zhoršení vzájemných vztahů s Ruskem, které útočníky ideologicky podporovalo. Kromě toho bylo Estonsko první zemí, které přístup k internetu prohlásila za základní právo člověka. Blokování přístupu k němu se tak v právní rovině rovnalo omezení práv člověka. Estonsko pohrozilo Rusku odvetnými opatřeními.

Estonsko jako ochranu proti budoucím útokům implementovalo některé typy ochrany, jako je užší spolupráce s poskytovateli internetu, záložní připojení a další techniky. Od té doby však následovalo hned několik dalších pokusů o diskreditaci jejich systému externím útokem (TAMKIN, 2017).

Bezpečnost systémů

Z vybraných medializovaných útoků na informační systému je zřejmé, že existuje široké spektrum způsobů, jak na takový systémů zaútočit. Jednotlivé incidenty se liší motivací, cílem i použitými technikami.

Od toho se odvíjí i možné techniky obrany, které se musí neustále přizpůsobovat změnám. Bezpečnost je komplexní téma, které v kontextu současné doby není možné podceňovat.

V ideálním případě by jednotlivé společnosti, organizace i státy měly vytvořit a pečlivě implementovat způsoby ochrany a také postupy pro případ úspěšného útoku. Pouze prevencí je možné předcházet útokům tak masivního charaktery, jako jsme byli svědky v minulosti.

Závěr

V práci jsme si představili základní rozdělení útoků na informační systémy. Popsali jsme si nejznámější útoky, které proběhly za použití rozmanitých technik. Dopady uvedených útoku byly různé, od úniků citlivých dat, krádeží finančních prostředků, až po ztrátu důvěry klientů a rozpad společností.

Kromě útoků na soukromé společnosti jsme si popsali některé specifické incidenty zaměřené na technické a technologické vybavené a také na státní útvary.

V současném světě každodenních útoků, probíhajících na menší i větší cíle, je stále důležitější poučit se a implementovat příslušné obranné mechanismy. Popis takových možností je však nad rámec této práce, které má za cíl seznámit čtenáře s útoky, které proběhly.

Citovaná literatura

ALEX HEATH. (21. květen 2014). Načteno z cultofmac.com: https://www.cultofmac.com/280189/icloud-hacker-calls-apples-response-little-late/

ALFRED NG. (7. Září 2017). *Equifax data breach may affect nearly half the US population*. Načteno z cnet.com: https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/

Apple, T. (2. září 2014). *Update to Celebrity Photo Investigation*. Načteno z apple.com: https://www.apple.com/newsroom/2014/09/02Apple-Media-Advisory/

Beaumont, P. (30. září 2010). *Stuxnet worm heralds new era of global cyberwar*. Načteno z theguardian.com: https://www.theguardian.com/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar

Burns, M. (15. Září 2017). *Equifax security and information executives are stepping down*. Načteno z techcrunch.com: https://techcrunch.com/2017/09/15/equifax-security-and-information-executives-are-stepping-down/

Coty, S. (2014). *The eBay breach explained*. Načteno z scmagazine.com: https://www.scmagazine.com/the-ebay-breach-explained/article/537762/

Cox, R. (21. Květen 2014). *TRULY MASSIVE DATA BREACH AT EBAY*. Načteno z Rippleshot: http://info.rippleshot.com/blog/ebay

DAVIS, J. (21. srpen 2007). *HACKERS TAKE DOWN THE MOST WIRED COUNTRY IN EUROPE*. Načteno z wired.com: https://www.wired.com/2007/08/ff-estonia/

Economist, T. (4. říjen 2010). Červ v centrifuze. *Respekt*. Načteno z The Economist: Červ v centrifuze. Respekt 4. října 2010: s. 36.

Erben, L. (29. 4 2014). *Příchod hackerů: příběh Stuxnetu*. Načteno z root.cz: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/

Hall, K. (5. září 2017). *Estonia identifies security risk*. Načteno z theregister.co.uk: https://www.theregister.co.uk/2017/09/05/estonia_identifies_security_risk_in_750000_id_cards/

HOSIE, R. (16. leden 2017). *Ashley Madison hacking*. Načteno z independent.co.uk: http://www.independent.co.uk/life-style/love-sex/ashley-madison-hacking-accounts-married-man-exposes-cheating-website-infidelity-rick-thomas-a7529356.html

Lamont, T. (28. únor 2016). *Life after the Ashley Madison affair*. Načteno z theguardian.com: https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked

Madison, A. (2016). *Ashley Madison After The Hack*. Načteno z Ashley Madison: https://www.ashleymadison.com/hack/

MOLNÁR, Z. (2009). *Podnikové informační systémy.* Praha: ČVUT.

Stuart, K., & Arthur, C. (27. duben 2011). Načteno z theguardian.com: https://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony

Symantec. (Duben 2016). *ISTR 2016.* Načteno z Internet Security Thread Report: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Symantec. (Duben 2017). *ISTR 2017.* Načteno z Internet Security Thread Report: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

TAMKIN, E. (27. duben 2017). *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?* Načteno z foreifnpolicy.com: http://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

wired.com. (2011). *PlayStation network hack: Who did it?* Načteno z edition.cnn.com: http://edition.cnn.com/2011/TECH/gaming.gadgets/04/28/playstation.hack.wired/index.html

Yuhas, A. (28. říjen 2016). *Hacker who stole nude photos of celebrities gets 18 months in prison*. Načteno z theguardian.com: Update to Celebrity Photo Investigation