Kybernetická bezpečnost malých firem

Nikola Krenželák

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Nikola Krenželák**
Osobní číslo:	**A14248**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Kybernetická bezpečnost malých firem**
Téma anglicky:	**Cybersecurity in Small Companies**

Zásady pro vypracování:

1. **Seznamte se s problematikou v oblasti kybernetické bezpečnosti.**
2. **Vysvětlete pojem Free a Open source software.**
3. **Popište a vysvětlete Obecné nařízení o ochraně osobních údajů (GDPR).**
4. **Vysvětlete souvislost mezi GDPR a kybernetickou bezpečností malých firem.**
5. **Popište současný stav bezpečnosti Informačních technologií.**
6. **Proveďte analýzu dostupných Open source nástrojů pro kybernetickou bezpečnost se zaměřením na malé firmy.**
7. **Navrhněte možná zlepšení pro bezpečnost malých firem s využitím získaných poznatků.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Obecné nařízení o ochraně osobních údajů [online]. Praha: Mgr. Eva Škorničková, 2017 [cit. 2017-11-20]. Dostupné z: https://www.gdpr.cz/gdpr.**
2. **JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů [online]. Univerzita Tomáše Bati ve Zlíně, 2013 [cit. 2017-11-19]. ISBN 978-80-7454-312-8. Dostupné z: http://digilib.k.utb.cz/handle/10563/25821.**
3. **ŠÍŘ, Ivo. Možnosti využití technologií Open Source a Free Software v malých a středních podnicích [online]. 2004 [cit. 2017-11-19]. ISSN 1210-9479. Dostupné z: www.cssi.cz/cssi/system/files/all/SI_04_3_sir.pdf.**
4. **MACÁK, Petr. Kritéria výběru software pro malé a středně velké společnosti [online]. 2011, s. 121-133 [cit. 2017-11-19]. ISSN 1804-2716. Dostupné z: www.cssi.cz/cssi/system/files/all/si_2011_01_10_Macak.pdf.**
5. **ŠTEC, Zdeněk. Open source software a jeho využití ve výuce tvorby webových stránek v sekundárním vzdělávání. [online]. Olomouc, 2013 [cit. 2017-11-19]. Dostupné z: https://theses.cz/id/6jbqak/00174154-374415625.pdf.**
6. **SINGER, P. W. Cybersecurity and cyberwar: what everyone needs to know. Oxford ; New York: Oxford University Press, 2014. ISBN 978-0-19-991809-6.**
7. **ŠTĚDROŇ, Bohumír. Open Source software ve veřejné správě a soukromém sektoru. Praha: Grada, 2009. ISBN 978-80-247-3047-9.**

Vedoucí bakalářské práce: **Ing. Lukáš Králík**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **27. července 2018**

Termín odevzdání bakalářské práce: **28. srpna 2018**

Ve Zlíně dne 27. července 2018

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. Ing. Martin Sysel, Ph.D.
garant oboru

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Nikola Krenželák, v. r.

ABSTRAKT

Tato bakalářská práce se zabývá kybernetickou bezpečností, která je velmi důležitá při chodu malých, středních a velkých firem a zabezpečení jejich dat. Účelem této bakalářské práce je popsat problematiku kybernetické bezpečnosti a pojmů s ní souvisejících, jako je nařízení o ochraně osobních údajů General data protection regulation a Free a Open Source software. Po nabytí teoretických poznatků, budou popsány nejnovější útoky a stav bezpečnosti. Poté bude provedena analýza dostupných nástrojů pro kybernetickou bezpečnost a na konci bude stručně popsán postup při hodnocení potenciálně využitého software.

Klíčová slova: free a open source software, kybernetická bezpečnost, licence, obecné nařízení o ochraně osobních údajů, osobní data, podvodné praktiky

ABSTRACT

This bachelor thesis is focused on the topic of cybernetic security, which is very important in the running of small, average and big companies and securing their business data. The goal of this bachelor thesis is to describe the problem of cybernetic security and terms related to this topic, including the General Data Protection Regulation or Free and Open Source software. After obtaining theoretical knowledge of this topic, I'm going to describe recent attacks on cybersecurity and companies' attitude towards cyber threats. Then an analysis of available tools for the cybersecurity is going to be performed and at the end of this thesis, I'm going to create a list (package) of possible software to enhance the cybersecurity of companies.

Keywords: cybersecurity, fraudulent practices, free and open source software, general data protection regulation, licences, personal data

Poděkování

Tímto bych chtěl poděkovat vedoucímu práce Ing. Lukáši Králíkovi za poskytnuté konzultace a rady při zpracovávání bakalářské práce. Chtěl bych také poděkovat své rodině za podporu. Bez nich by zpracování nebylo možné.

OBSAH

ÚVOD

Vlastníme-li nějaký drahý předmět (auto, dům, drahé klenoty), je v našich silách udělat vše pro to, aby se těmto věcem nic nestalo. Jsme-li například v kavárně a potřebujeme si zajít na toaletu, nenecháme náš mobil ležet na stole, ale vezmeme si ho s sebou. Odcházíme li z domu, dům zamkneme klíčem. Drahý obraz nenecháme jen tak ležet na zemi, kde se na něho může šlápnout, ale uložíme ho pečlivě na zeď, nebo do krabice.

V dnešní době ale nejsou cenné věci jen fyzického původu. Se stále urychlujícím se rozvojem informačních technologií bylo potřeba zajistit ochranu věcí nehmotných, jako například bankovní účty, nejrůznější hesla, osobní účty, e-maily, platební karty, záznamy o platbách na internetu, nebo firemní databáze. Špatné zajištění bezpečnosti údajů firmy by mohlo tyto firmy stát nemalé peníze, vést ke krádeži, prozrazení citlivých údajů o zákaznících či firmě, nebo vyzrazení firemního tajemství apod. Tato událost by mohla firmu poškodit natolik, až by nebyla schopna se s problémem vypořádat a mohlo by to znamenat i její konec.

Teoretická část bakalářské práce má za cíl poskytnout informace o problematice kybernetické bezpečnosti. Uvedení současných hrozeb, čeho by se měl běžný uživatel internetu vyvarovat. Jsou uvedeny typy software, které se v informatice používají s důrazem na Free a Open source, jelikož není nákladný a dá se s ním pružně pracovat. Důležité je také zmínit nově zavedený GDPR, nebo-li General Data Protection Regulation, jež má za úkol stanovit práva a povinnosti firem, online služeb a občanů a tím zlepšit ochranu osobních údajů, se kterými nakládá. Poté bude uvedena souvislost mezi GDPR a firmami.

Praktická část bakalářské práce se zaměřuje na aktuální stav v oblasti kybernetické bezpečnosti a vztah firem vůči kybernetickým útokům. V mnoha malých firmách mezi tyto opatření patří právě vhodně zvolený software. Mezi tento software se řadí Open Source, který je pro malé firmy přitažlivý z důvodu jeho ceny. Je provedena analýza několika programů typu open source, rozdělených do konkrétních kategorií podle oblasti použití a také je popsána metodika, díky které byla analýza provedena. Práce je zakončena stručným shrnutím procesu, který mohou firmy uplatnit při výběru software.

TEORETICKÁ ČÁST

1 KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost je v dnešní době nepostradatelnou součástí nejrůznějších právnických a fyzických osob a státu. Počátky se objevily v 80. letech, kdy se s rozmachem výpočetní techniky začaly skladovat informace právě do výpočetních systémů. Jednalo se například o evidence plateb, informace o zákaznících, armádní tajemství. [1]

Existuje několik typů bezpečnosti:

a) **Personální bezpečnost –** Jedná se o všechny osoby, které se systémem pracují. Největší podíl na bezpečnostních nehodách mají právě lidé. Neznalost, nezaškolení, bezohlednost a neprovádění kontroly zaměstnanců může vést k chybám vzniklých v systému, proto je potřeba zvolit kvalifikované pracovníky. [2]
b) **Fyzická bezpečnost –** Jde o ochranu všech fyzických věcí firmy. Může se jednat o vybavení jako jsou servery, počítače, suroviny, hotové výrobky, polotovary, nářadí, dokumenty, ale i lidi. Všechny tyto objekty se mohou stát obětí přírodních katastrof, požárů, nebo útoků lidí. [2]
c) **Logická bezpečnost –** Firmy při své činnosti využívají různé typy software. Ať už jde o operační systémy, tak různé databáze, kancelářský software. Pro bezpečný chod firmy by měly být tyto software přístupné jen určitým zaměstnancům. Například správa sítě bude povolena technikovi, který se o tuto síť stará. Operační systém a kancelářský software bude přístupný například sekretářkám. Proto je potřeba zřídit přístup pro jednotlivé osoby. [2]
d) **Komunikační bezpečnost –** Ochrana při přenášení informací přes síť. Můžeme se stát cílem odposlouchávání nebo přetížení. [2]
e) **Organizační bezpečnost –** Bezpečnost se zřizuje pomocí stanovení odpovědnosti osob a skupin v organizaci, nebo společenství. Zřizují se bezpečnostní standardy, Každý zaměstnanec má tím pádem své povinnosti a nezasahuje do práce ostatních, [2]

V dnešní době je kybernetická bezpečnost chápána jako soubor opatření týkajících se nějakého objektu. Ať už mluvíme o firmách, nebo domácnostech. Firmy se snaží zajistit taková opatření, aby se jejich informace (firemní tajemství, informace o zákaznících, transakce, informace o výrobě) nestaly terčem nejrůznějších útoků a nevznikla škoda.

Proto by se firma měla snažit o propojení kybernetické bezpečnosti s výše uvedenými typy bezpečnostmi, k dosažení největší efektivity. [1]

Opatřeními máme na mysli provádět takové činnosti, aby byl informační systém co nejbezpečnější. Jedná se o vhodně zvolené přístupové podmínky do systému, tedy přihlašování do systému pomocí jména a hesla, případně dalších ověřovacích faktorů, jelikož tímto z větší části eliminujeme možnost nabourání do systému. Dále pak zvolený antivirus, který musí být spolehlivý a nesmí propustit viry, které narušují běh systému, či mění a kradou data. Zálohování dat je také nezbytnou součástí bezpečnosti firmy. Firmy, ale i obyčejné fyzické osoby, které se stanou svědky vyhoření serverů, či počítačů s veškerými daty, budou mít těžkou chvíli dostat se zpět na vlastní nohy, neboť příjdou o veškerá nezálohovaná data. Vyhoření nebo selhání serverů / počítačů mohou dokonce způsobit i viry k tomuto účelu navržené, není pak problém tuto škodu způsobit zvenčí.

Měli bychom si být vědomi, že i přes všechna provedená zabezpečení, vždy existuje riziko narušení. Žádný systém není stoprocentně dokonalý a může se stát terčem crackerů. [1]

1.1 Základní pojmy kybernetické bezpečnosti

Abychom mohli s tématem kybernetické bezpečnosti dále pracovat, musíme si stanovit základní pojmy, které se zde vyskytují.

a) **Primární aktivum** – Jsou to informace a služby, které jsou zpracovávány informačním systémem. Narušením těchto aktiv dojde k zastavení činnosti podniku.
b) **Technické aktivum** – Jedná se o programy, komunikační prostředky a technické vybavení, jež jsou součástí informačního systému.
c) **Podpůrné aktivum** – Jde o technická aktiva, dodavatele a pracovníky, organizace, kteří mají podíl na správě informačního systému a jeho rozvoj.
d) **Garant aktiva** – Je to fyzická osoba, která má za úkol zajistit bezpečnost, rozvoj a používání daných aktiv.
e) **Administrátor** – Osoba, která musí zajišťovat správu technických aktiv. Bývá zvolen garantem.
f) **Uživatel –** Fyzická, právnická osoba nebo orgán veřejné moci, který manipuluje s primárními aktivy.

g) **Riziko –** Možnost způsobení škody systému prostřednictvím jeho zranitelného místa
h) **Zranitelnost –** Slabé místo aktiv systému, které se může stát cílem hrozeb
i) **Hrozba –** Vnější příčina, událost negativního ovlivnění aktiva.
j) **Hodnocení rizik** – Provádí se pro zjišťování charakteru rizik a jejich přijatelného množství.
k) **Bezpečnostní politika** – Pravidla a zásady, které mají za úkol zabezpečit aktiva systému.
l) **Integrita** – zaručení bezpečnosti a neporušitelnosti dat v průběhu jejich používání. [3]

1.2 Bezpečnostní politika

Jde o soubor technických a organizačních opatření pro zajištění bezpečnosti všech částí firmy. Proto je vhodné při jeho vytvoření zahrnout nejrůznější oblasti firmy, jako například ekonomické oddělení, personální oddělení, správu sítě, bezpečnostního technika atd. Jedná se například o zajištění proti IT hrozbám, požáru, krádeži atd. Bezpečnostní politika se musí aktualizovat při plánovaném zásahu do technologií, při očekávání vnějších vlivů nebo po vzniknutí nežádoucích událostí (přírodní katastrofy, internetové hrozby). Jedná se o písemný dokument, který pojednává o plánu ochrany aktiv podniku. Udává bezpečnostní postupy a procesy. Zpracovává ho bezpečnostní oddělení spolu se správcem. [4]

Odpovídá na tyto otázky:

- Co je potřeba ochránit
- Proč je to potřeba ochránit
- Jak ochrany docílit
- Kontrola provedené ochrany
- Plány při narušení bezpečnosti

[4]

Bezpečnostní politika se může zabývat:

Ochrana informací – veřejné i neveřejné (obchodní tajemství, citlivá data)

Záloha dat – záloha na jiné médium v případě ztráty dat z média primárního

Fyzická ochrana – ochrana proti přírodním katastrofám, požáru, mechanickému poškození

Ochrana informačních technologií – software pro zajištění systému před kybernetickými útoky (viry, spyware, keylogger atd.) [4]

1.3 Kryptografie v informatice.

Kryptografie je věda o šifrování či utajení znění zprávy. Toto se provádí převodem otevřeného textu na text šifrovaný za použití šifrovacího klíče. Tento text se nedá bez použití nějakého dešifrovacího klíče rozluštit. Zašifrování dát je velice důležitou součástí kybernetické bezpečnosti, neboť můžeme mít jistotu, že si naše zprávy či data nepřečte nežádoucí osoba, pokud nemá k dispozici dešifrovací klíč. Existuje několik typů šifrování, mezi něž patří například symetrické šifrování a šifrování asymetrické. [5]

1.3.1 Symetrické šifrování

U šifrování se rozlišuje takzvaný otevřený dokument (nezašifrovaný) a šifrovaný dokument. Toto šifrování se vyznačuje tím, že se k šifrování a dešifrování používá jeden stejný klíč. Tohle šifrování se může zdát riskantní, neboť klíč mají k dispozici obě strany, bezpečnost šifrování je tedy velice závislá na používaném algoritmu. Symetrické šifry se liší od asymetrických tím, že mají nižší výpočetní náročnost při zpracování počítačem. Mezi známé používané algoritmy například patří AES (Advanced Encryption Standard), IDEA, Twofish nebo Blowfish. [5]

Obr. 1 Symetrické šifrování [5]

1.3.2 Asymetrické šifrování

Toto šifrování se od symetrického šifrování liší používáním dvou klíčů. Jeden klíč se používá pro šifrování – klíč veřejný. Druhý klíč se používá pak pro dešifrování – klíč soukromý. Tyto dva klíče spolu tvoří pár, přičemž nejprve je vytvořen klíč veřejný a až poté klíč soukromý. Asymetrické šifrování se používá pro digitální podpisy, ověření digitálních podpisů, vznik a ověřování časových razítek a pro šifrování zpráv. Veřejné klíče se používají pro šifrování dat a lze je volně šířit. Ovšem při vytváření digitálního podpisu nebo vytváření a podepisování časového razítka, se využívá klíč soukromý. Ověřování se poté provádí klíčem veřejným, tudíž, může kdokoliv, kdo vlastní tento veřejný klíč, ověřit pravost dat. Nejpoužívanějším algoritmem je RSA (iniciály autorů – Rivest, Shamir, Adleman), ale existují také algoritmy DSA (Digital Signature Algorithm) a ECC (Elliptic Curve Cryptography) [5]

Obr. 2 Asymetrické šifrování [5]

1.3.3 Hashování

Jde o funkci, která má za úkol vytvořit hash, nebo-li otisk (sadu znaků) pomocí aplikování hashovací funkce na řetězec dat. Vlastnost hashe je taková, že není možné z hashe zjistit znění původních dat, je tzv. Irreversibilní (nevratná). Hash by vždy měl být unikátní, to znamená že by se nemělo stát, že se vyskytnou 2 identické hashe u různě znějícího textu. V případě, že by dva různé texty měly stejný hash, nazýváme to pak kolizí. Při změně jediného znaku textu, se stane to, že daný hash (otisk) bude vypadat jinak. Zajistí se tak integrita dokumentu. Stane-li se, že bude soubor změněn, tuto skutečnost lze zjistit tak, že porovná starý a nově vytvořený hash souborů a budou-li jiné, došlo pak k úpravě dokumentu a narušení jeho integrity. Mezi známé typy hashe patří například SHA-256 (používá 256 bitů), SHA-384 (384 bitů), MD5 (128 bitů), z nichž se nedoporučuje používat MD5, jelikož je zastaralý. [5]

Věta **„Toto je vytvořený hash“,** bude po vytvoření hashe pomocí hashovací funkce SHA-256 vypadat takto (bez uvozovek):

„10445486f21bb34a2d88d43c60d309b886d16cf28b3c537ee335bc208b63958f“

K hashování patří také pojem „solení“, což je vlastně přidání nějakého dalšího řetězce ke vstupu daného hashe, který zajistí větší bezpečnost. Přidaná „sůl“ může vypadat jakkoliv. Solení je účinnou metodou proti slovníkovým (z předchystaného seznamu slov) útokům k prolomení hashe. [6]

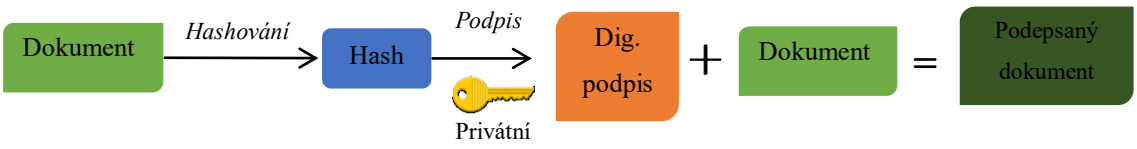
1.3.4 Digitální podpis

Digitální podpis je užitečnou pomůckou při prokazování pravosti a důvěryhodnosti elektronických dokumentů. Po připojení k dokumentu prokazuje, že dokument byl podepsán danou osobou či systémem a také ním odeslán. Jde o dokumenty jako například e-maily nebo přiznání daně z příjmů a dokumenty související s úřady, včetně internetové banky. Pro vytvoření podpisu se používá asymetrické šifrování a hashovací funkce. [7]

Digitální podpis musí pro jeho spolehlivé užívání disponovat několika vlastnostmi.

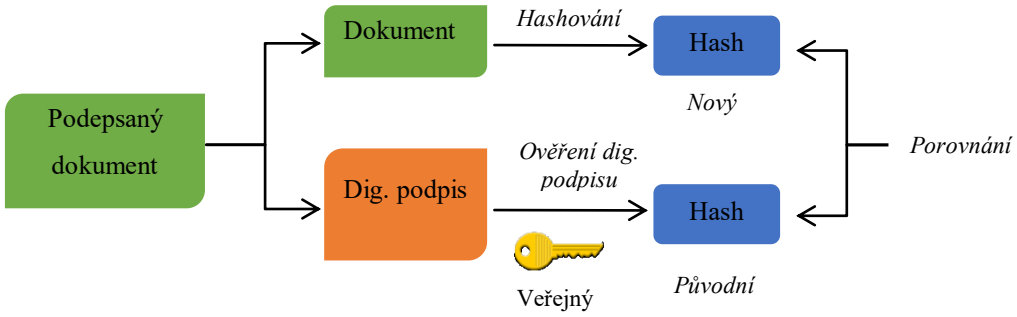
1. Musí být možno **ověřit jeho platnost** u dané certifikační autority
2. Musí být **zajištěna integrita podpisu**
3. Musí být **nepopíratelný** (podepsat lze jen papír s obsahem, ne čistý)
4. Musí být **nezfalšovatelný** (není možno vytvořit podpis bez soukromého klíče podepisované osoby [7]

Při vytvoření digitálního podpisu musíme nejprve vytvořit hash a tento hash poté privátním klíčem dané podepisované osoby zašifrovat. Podpis poté přiložíme k potřebnému dokumentu, který se stane podepsaným. [7]



Obr. 3 Digitální podpis [7]

Při ověření z dokumentu vznikne nově vytvořený hash (stejnou funkcí) a zároveň se digitální podpis dešifruje pomocí veřejného klíče z daného klíčového páru. Nakonec se porovná nově vytvořený hash s původním hashem, dešifrovaného pomocí veřejného klíče. Budou-li stejné, dokument je pak platný. Digitální podpis sám o sobě nezaručuje pravost dokumentu, o tu se starají certifikační autority. [7]



Obr. 4 Ověření digitálního podpisu [7]

1.4 Hrozby a rizika

Pohyb na internetu s sebou nese nespočet rizik. Je potřeba být o těchto hrozbách dobře informován, aby se zabránilo možné škodě. Neznalost zaměstnanců firmy může způsobit krádež či vyzrazení citlivých údajů, ať už se jedná o informace o výrobě, klientech, tak i bankovní údaje, kreditní karty, hesla nebo peníze. Následkem může být pak propuštění, nebo i žaloba / pokuta. Jedná se o podvody, jako jsou například Phishing, Pharming, Malware, Počítačové virusy, Rootkity, Spyware, Keyloggery a další.

Nejčastěji se vyskytují v e-mailech, formou odkazů nebo souborů. Proto je potřeba každý e-mail pečlivě pročíst. Tyto e-maily je vhodné smazat, adresu označit jako spam a varovat ostatní.

1.4.1 Jak se bránit

V prvé řadě je potřeba ke všemu přístupovat rozumně a nespěchat. Není doporučeno ukládat uložená hesla, kódy, pin, názvy účtů v počítači. Před opuštěním počítače je žádoucí se odhlásit z jakýchkoliv aplikací a stránek. Instalací kvalitního antiviru se dá zamezit možným útokům zvenku, neboť je schopný zadržet příchozí viry a jiný škodlivý program. Při interakci s jinými lidmi je potřeba jednat ostražitě a využívat pouze důvěryhodné stránky. Neměly by se navštěvovat pochybné stránky, které mohou být nakaženy virem - tyto stránky se většinou dají poznat z uvedeného odkazu. Před návštěvou stránky je možno odkaz zadat například do google a zjistit o této stránce více informací. [8]

1.4.2 Typy hrozeb

Existuje jich několik a každá hrozba má jiný cíl. Chce-li například útočník zjistit heslo účtu, použije keylogger nebo phishing. Jde-li mu o sledování aktivity na internetu, použije spyware. Každá tato hrozba se specializuje na určitou oblast.

1.4.2.1 Počítačový virus

Jde o program, který má za cíl způsobit škodu systému počítače. Virus obsažený v souborech či programech při spuštění nebo samovolně po nějaké době začne páchat škodu. Může například extrémně zpomalit počítač, nebo v horším případě smazat data na disku či způsobit vyhoření hardware. Virem mohou být infikovány e-maily, webové stránky, aplikace či soubory, které když se stáhnou, s sebou přinesou právě tento virus. Z toho vyplývá, že se by se neměly navštěvovat podezřelé stránky, spouštět podezřelé aplikace a otevírat soubory, u kterých není znám původ. Každý počítač by měl být vybaven minimálně jedním antivirem.

1.4.2.2 Adware

Jde o bezplatné programy, které se snaží vydělat peníze zobrazováním reklam. Tyto reklamy jsou z velké části otravné a neškodné, ale počítač mohou i zpomalovat. Existuje i adware, který může být nebezpečný, neboť může sledovat historii prohlížení nebo osobní informace. Jestli je napaden náš systém adwarem poznáme tak, že se nám samovolně spouští nová okna a bannery, případně se mění domovská stránka prohlížeče. Před adwarem se dá bránit tak, že aktualizovaný veškerý software (operační systém, prohlížeče, antivirové programy atd.). Existuje však i specializovaný anti-adware software. [9]

Obr. 5 Adware [10]

1.4.2.3 Spyware

Cílem spyware je potají sledovat aktivitu uživatele počítače, shromažďovat tyto informace a případně je přeposílat třetím stranám. Jedná se o osobní údaje nebo historii prohlížení. Počítač jím může být nakažen po nainstalování aplikací nebo po otevření přílohy e-mailu, hudby, filmů atd. Projevuje se přesměrováním vyhledávacích dotazů, nebo vznikem neznámých ikon v hlavním panelu. Odstranění se provádí antivirovým programem, nebo programem zaměřeným na odstraňování spyware. Možností je také odinstalovat podezřelé programy. Prohlížeč a antivirus je potřeba udržovat aktuální. Nesmí se spouštět podezřelé aplikace, otevírat e-mailové přílohy a klikat na vyskakovací okna. [11]

1.4.2.4 Rootkit

Snaží se o získání administrátorských práv k systému. Rootkity mohou přijít se staženými bezpečnostními, programy, které na první pohled vypadají neškodně. Mohou se ale také objevit formou dodatečného rozšíření programů. Rootkit se dá zjistit antivirem, který musí při provádění systémové kontroly navíc sledovat funkce DLL knihoven. Rootkit se po nalezení musí odstranit ručně. [12]

1.4.2.5 Ransomware

Jde o program, který po nakažení systému znemožňuje přístup k některým souborům nebo i celému systému. Pro odblokování dat je potřeba zaplatit určitou peněžní částku. S největší pravděpodobností se ale stane, že se data neodblokují a navíc dojde ke ztrátě peněz. Ransomware se může vyskytovat v e-mailových přílohách a na webových stránkách. Dobrou prevencí je mít kvalitní antivirus, který tyto hrozby dokáže zachytit. Je-li systém nakažen, nabízí se dvě možnosti a to – operační systém přeinstalovat, ale přijdeme o naše data, nebo si stáhnout program na dešifrování zablokovaných dat, záleží ale na použitém typu ransomware. [13]

1.4.2.6 Keylogger

Je to program, který má za úkol sledovat používání stisku kláves. Útočník může díky keyloggeru zjistit uživatelská hesla, názvy účtu, čísla bankovních účtů, jaké stránky jsou navštěvovány nebo jakýkoliv text, který byl napsán v e-mailech nebo v jiném textové formě. Keylogger se v počítači může vyskytnou, otevřeme-li e-mailovou přílohu, klikneme na phishingový odkaz nebo jím může být nakažený nějaký software. Nakažený počítač se může chovat zpomaleně, myš se zasekává a klávesy fungují opožděně. Použití správného antiviru by mělo problém vyřešit. Dobré je používání dvoufázového přihlašování. [14]

1.4.2.7 Backdoor

Je to metoda, která umožňuje přístup k programu díky obcházení autentizace, která je při běžné kontrole nezjistitelná. Backdoor bývá zanechán úmyslně programátorem nebo může být jako nástroj ladění programu, který byl omylem zanechán ve finální verzi. [15]

1.4.2.8 Phishing a Pharming

Phishing je praktika, kdy dochází za použití speciálně navržených programů či podvodných webových stránek (které se jeví jako pravé), k ukradení osobních údajů (hesla, přihlašovací jména, čísla účtů atd.). Jsou-li přihlašovací údaje zadány do přihlašovacího okna podvodné stránky (často bývá nerozeznatelná od té právé), objeví se hlášení o chybě a údaje jsou odeslány útočníkovi. Phishing se může používat například u účtů bank, e-mailů, apod. K zamezení možnosti stát se obětí phishingu, je potřeba mít kvalitní antivirus, firewall, prohlížeč a provádět jejich aktualizaci, mít zdravý rozum a pečlivě si před kliknutím na odkaz přečíst plné znění odkazu, není-li v něm chyba, jako znak navíc či znak chybějící.

Pharming je podobný phishingu. Útočník se naboural na DNS (domain name server) dané stránky a kohokoliv kdo tuto stránku navštíví, automaticky přesměruje na stránku podvodnou.

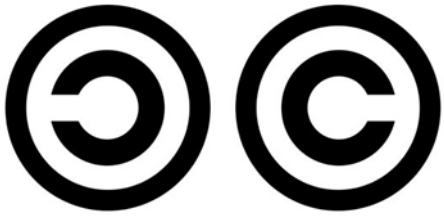
2 FREE A OPEN SOURCE SOFTWARE

Software, nebo-li program, je součást každého počítače. Program je chráněn autorským právem, který udává právo vlastnit a upravovat daný software. Software se může vyskytovat jako placený (komerční), nebo zdarma (Freeware, Shareware, Open Source, Public domain atd.)

2.1 Copyright a Copyleft

Copyright je termín, který udává autorská práva k nějakému výsledku práce. Například hudba, filmy, programy, hry, ale i knihy, divadelní hry nebo digitální či fyzické obrazy. Vlastníkem práva je autor, který dílo vytvořil. Může ovšem toto právo přenést (půjčit) za pomocí licence jiným osobám za podmínky, že užívání, distribuci a úpravu tohoto díla má povoleno jen tehdy, dovolí-li jim to původní autor či vlastník díla. Copyright se vztahuje jen na fyzicky nebo elektronicky vytvořená díla, ne na myšlenky. [16]

Copyleft je opakem Copyrightu. Jedná se o svobodný software a z díla, které je copyleftové, lze vytvořit jiné dílo, které se však musí také považovat za dílo se stejnou licencí. Toto dílo lze upravovat, ale veškerá odpovědnost za škody připadá na osobu, která úpravy provedla. Copyleft se nejčastěji užívá u Open Source software.



Obr. 6: Logo Copyleft (vlevo) a Copyright [17]

2.2 Typy software

Existuje několik typů software. Každý software se od sebe liší způsobem pořízení, podmínkami užívání a šíření. Může se jednat o placené programy, plné verze programů, které jsou zdarma, nebo o programy se zablokovanými funkcemi, jež se odemknou po zaplacení.

2.2.1 Shareware

Je typ software, který je k dispozici zdarma, ovšem s omezenými funkcemi. Jedná se o demoverzi nebo neregistrovaný produkt. Shareware slouží k vyzkoušení dostupných funkcí programu a k odemknutí dalších funkcí je potřeba zaplatit peníze. Program je dovoleno šířit. Může mít také časovou lhůtu. Po uplynutí této doby se funkce programu zablokují a je potřeba si je odblokovat platbou. Autorská práva (copyright) vlastní autor programu.[18]

2.2.2 Freeware

Freeware je program zcela zdarma. Lze ho volně šířit a používat po neomezenou dobu. Programy tohoto typu nelze zpoplaťnovat za účelem vlastního výdělku. Program se nesmí nijak upravovat, neboť autorská práva, náleží tomu, kdo tento program vytvořil. Jako freeware se mohou také považovat odlehčené verze programů zvané Lite, nebo demoverze programů komerčních. [18]

2.2.3 Public domain

Tento typ programu je bez jakýchkoliv autorských práv. Vlastníkem je teoreticky kdokoliv. Zdrojový kód tohoto software je volně dostupný a šířitelný a lze ho upravovat. Zdrojový kód by se neměl celý vzít a vydávat ho za vlastní, ale měl by být pozměněn a vložen k jinému kódu. [18]

2.2.4 Trialware

Je to program, který je k dispozici zdarma, ale jen jeho časově omezená verze, která po vypršení přestane fungovat a je potřeba si plnou verzi zaplatit. Trialware je zakázáno šířit bez svolení autora, z důvodu udržení aktuální oficiální verze, nebo kvůli získávání marketingových údajů. [18]

2.2.5 Komerční programy

Tyto programy mohou být distribuovány pomocí fyzického disku v obchodech. Součástí může být i registrační klíč, kterým se dá produkt aktivovat. Spolu s diskem bývá zahrnut manuál a v případě nefunkčního disku je možná vrácení. Další možností je koupení na stránkách výrobce, kdy po zaplacení obdržíme registrační klíč, kterým je produkt

aktivován. Komerční program je zakázáno šířit nebo upravovat. Jedná se například o koupenou licenci Microsoft Windows. Při instalaci na druhý počítač je potřeba si program koupit znovu.[19]

2.2.6 Software s licencí OEM

Jde o programy, které jsou součástí počítače při jeho pořízení. Stane-li se, že se počítač pokazí, příjdeme o licenci. Jedná se například o operační systém Microsoft Windows jako součást koupě nového počítače. Programy s touto licencí se nesmí přenášet na ostatní počítače.

2.2.7 Free a Open Source software

Jde o software, který je svobodný a otevřený. Open Source je software s volně dostupným zdrojovým kódem. Znamená to tedy, že si kdokoliv může tento program stáhnout zdarma. Má právo zdrojový kód studovat a provádět potřebné změny. Musí být vydáván pod stejnou licencí, s jakou byl obdržen. Není zakázáno ho prodávat, ale i přes tento úkon musí být poskytnuto právo software upravovat a šířit dále. Vzhledem k tomu, že je zdrojový kód dostupný všem, může se kdokoliv podílet na hledání a opravování chyb, tedy rychlost opravy a vývoje je velice velká. [20]

Open Source ale není bezchybný, obsahuje také několik nevýhod. Vývoj programu záleží na programátorech. Opustí-li komunitu schopní programátoři, může se stát, že vývoj úplně skončí, nebo se zpomalí. Vzhledem k tomu, že ke zdrojovému kódu má přístup každý, najdou se lidé, kteří tohoto zneužijí a vytvoří viry, které pak sdílejí dále. Open Source operuje pod několika různými licencemi, jako GNU GPL. Mezi programy typu Open Source patří například operační systém Linux, kancelářský software Open Office, internetový prohlížeč Mozilla Firefox nebo grafický program Gimp či Inkscape. [20]

2.3 Open Source licence

Licence dovolují zdrojovému kódu open source softwaru používání, upravování a šíření. Licencí pro open source software existuje několik, každá se něčím liší, ale většinou mají stejný princip.

2.3.1 GNU General Public Licence

GNU General Public License. Asi nejznámější licence, používaná pro Open Source software. Licence dovoluje zdrojové kódy stahovat, upravovat a šířit dále, ovšem se stejnou licencí, odkud byly převzaty. GNU GPL je copyleftovou licencí, neumožňuje s touto licencí manipulovat a nemůže se stát, že by se nově vytvořené programy vydávaly s jinou licencí. [21]

GPL zaručuje svobodu manipulace programu. Nelze tedy software pod GPL licencí zahrnout v proprietárním systému, který je nesvobodný, jelikož by se omezila svoboda manipulace. Je však možné připojit zdrojový kód, který je pod jinou licencí k zdrojovému kódu, operujícího pod GPL. Licence však musí dovolovat kombinování více licencí a výsledek bude uveden pod GNU GPL. Jednou z podmínek při distribuci open source software je povinnost ke každé vydané kopii zároveň přiložit kopii licence pro seznámení všech, jež software obdrží. Vyvíjí-li se software na žádost klienta, lze uplatnit Non Disclosure Agreement. Znamená to, že verzi vyvíjeného programu je zakázáno zveřejňovat, aniž by to klient schválil. [22]

2.3.2 Lesser General Public Licence

Jedná se o modifikaci GPL licence, která používá méně přísná pravidla, než GPL. Je povoleno použití zdrojového kódu v jiných dílech, které tuto licenci nemají. Jedná se převážně o knihovny, které mohou být součástí komerčních programů. Používá se ale také v některých programech jako jsou prohlížeče Mozilla, nebo kancelářský software Libre Office. Lesser General Public Licence (LGPL) umožňuje komerční využití výsledků softwaru svobodného. [23]

3 GENERAL DATA PROTECTION REGULATION

GDPR je zkratka pro General Data Protection Regulation. Je právní rámec pro ochranu osobních údajů a jejich neoprávněnému užívání, včetně ochrany práv občanů.

GDPR platí pro fyzické, právnické osoby a služby, které pracují s osobními údaji zaměstnanců, dodavatelů, odběratelů a klientů nacházejících se v Evropské unii a nebo podílejících se na evropském trhu. Porušení tohoto nařízení má za následek udělení pokut. Mezi GDPR patří i analýza chování osob v online prostředí. Jde o ochranu digitálních práv osob. [24]

GDPR bylo schváleno 27. dubna 2016.

3.1 Co se považuje za osobní údaje

Jsou to veškeré informace, které dokáží jednoznačně identifikovat konkrétní osobu. Rozdělují se na obecné a citlivé, včetně genetických a biometrických údajů. [25]

3.1.1 Obecné osobní údaje

Mezi obecné osobní údaje patří například: Jméno, bydliště, doručovací adresa, věk, pohlaví, místo a datum narození, osobní stav, rodné číslo, telefonní číslo, IP adresa, e-mail, mzda, čísla různých průkazů vydaných státem – občanský, řidičský průkaz, cestovní pas atd. [25]

3.1.2 Citlivé osobní údaje

Existuje i typ citlivých údajů. Patří mezi ně náboženství, sexuální orientace, politické názory, zdravotní stav (tělesný a duševní), trestní činnosti, rasový původ. Patří zde ale také genetické a biometrické údaje. [25]

3.1.2.1 Genetické osobní údaje

Jde o osobní údaje, které se týkají získaných genetických znaků fyzické osoby z fyzického vzorku. Může se jednat například o krevní skupinu nebo vzorek DNA. [25]

3.1.2.2 Biometrické údaje

Jsou to údaje, které vzinknou technickým zpracováním fyziologických znaků osob, jenž jsou unikátní. Jde například o otisk prstu, podpis, snímek obličeje, či skenování oka. [25]

3.2 Pověřenec pro ochranu osobních údajů

Data Protection Officer (DPO), je osoba, která zodpovídá za monitorování správného zacházení s osobními údaji firmy. Informuje a poskytuje rady správcům a zpracovatelům Pověřenci mohou mít i jiné funkce ve firmě, ovšem nesmí vykonávat funkce, které by způsobily konflikt zájmů (IT, obchodní ředitel atd.) [26]

Pověřence je povinno jmenovat, zpracovávají-li údaje orgány veřejné moci nebo veřejné subjekty nebo jsou-li hlavní činností zpracovatelů a správců operace zpracování, vyžadující rozsáhlé, pravidelné a systematické monitorování občanů, nebo také v případě zpracování zvláštních kategorií údajů nebo údajů týkající rozsudků v trestních věcech. Pověřenci mají znalosti o GDPR, právu, podnikání, vnitřní organizaci správce a také o ochraně údajů. Jeden pověřenec může být jmenován pro více firem či státních orgánů, mají-li tyto firmy podobnou organizační strukturu. Úlohou správce je pak postarat se o to, aby pověřenec své úkoly plnil efektivně. Je vázán tajemstvím a musí být dostupný po fyzické či telefonické stránce občanovi. Dodržování GDPR firmou není odpovědností pověřence, o to se stará správce či zpracovatel. Důležité je, aby pověřenec splňoval všechny podmínky GDPR. Zároveň musí být chráněn ustanoveními GDPR, například nesmí být nespravedlivě propuštěn z důvodu jeho činnosti. [26]

3.3 Důvody zavedení

Jedním z důvodů zavedení GDPR je úprava práv osob, neboť před jeho zavedením se řídilo právy o ochraně osobních údajů z roku 1995, z doby kdy se nepoužívaly cloudy, různá úložiště dat, sociální sítě atd. GDPR poskytuje občanům ochranu a informovanost o svých osobních údajích, se kterými firmy pracují. Ochrana osobních údajů byla a někdy stále je občany podceňována, což má za následek poskytování informací těm, kteří na cizích osobních údajích vydělávají. Osobní data jsou v dnešní době poskytována velmi často, například při platbě na internetu, používání internetových obchodů či registraci na různé stránky. [27]

3.4 Přínos

GDPR přinese jednotné zacházení s osobními údaji, včetně rovnocenných pokut. Poskytne také občanům lepší kontrolu nad svými vlastními údaji. Osoby nakládající s osobními údaji budou muset dokládat, jak s údaji nakládají. Povinnosti udává všem osobám, které data zpracovávají. Rozšiřuje se také definice osobních údajů například o IP a e-mailové adresy, cookies. [28]

Poskytuje také informovanost o právech občanů a umožňuje jim zamezit další zpracování jejich údajů cizími osobami, nebude-li k tomu mít závažný důvod. Občanům musí být umožněn přístup k údajům o jejich osobě. Osoba má také právo zažádat o vymazání údajů, nestanoví-li to právní podmínky jinak. Zpracovatel musí také nahlásit ohrožení zabezpečení nebo únik osobních dat. Tuto událost musí zpracovatel nahlásit Úřadu pro ochranu osobních údajů do 72 hodin od doby, kdy se dozvěděl o problému a v konkrétních případech také musí informovat osoby, jejichž údaje mohly uniknout. [28]

3.5 Práva občanů

Občané mají právo přístupu ke všem údajům vedených o nich, včetně údajů uložených na externích discích, v e-mailech apod. Mají také právo na výsledky diagnóz, vyšetření a našeho celkového zdravotního stavu. Znát účel zpracování údajů, dobu zpracování, příjemce a důsledky zpracování také patří mezi právo. Nesmí se však ohrozit obchodní tajemství a duševní vlastnictví či autorská práva. [29]

Lze požádat o vymazání údajů, neslouží-li údaje nadále svému účelu, byl-li odvolán souhlas pro zpracování, vznesena námitka, není uveden souhlas rodičů, či se s údaji zachází nelegálně. Není-li možné požádat o vymazání údajů, lze vznést námitku a donutit firmy o omezení zacházení s údaji, například přesun do jiného systému, znemožnění přístupu části údajů jiným osobám nebo odstranění údajů z internetu. [29]

3.6 Povinnosti firem

Povinnost firem je zavádět technická, procesní a organizační opatření, tak, aby vyhovovaly podmínkám GDPR. Firmy jsou povinny:

- Zavést ochranu dat

- Vytvořit posudek vlivu ochrany osobních údajů (DPIA - Data Protection Impact Assessment)
- Jmenovat pověřence - Data Protection Officer (DPO)
- Vést pseudonymizaci údajů
- Vést záznamy o zpracování
- Konzultovat s dozorovým orgánem před zpracováním údajů.

DPIA se týká firem, které automatizovaně prováději rozsáhlé vyhodnocení osobních údajů, například u bank a jejich nabízení služeb, firem s cílenou reklamou, nebo nemocnic a pojišťoven. Zpracovávané údaje by měly být co nejmenší, vždy přístupné občanům, měly by být transparentní a pseudonimizace by měla být rychlá. Pseudonimizace znamená, že se některé údaje osob nahradí kódem, například jméno. V případě anonymizace se při zpracovávání jména, příjmení, věku a například náboženského vyznání, nezjišťuje jméno a příjmení, pracuje se jen s věkem a vyznáním. Správce a zpracovatelé údajů musí dokumentovat jejich zpracování a zpřístupňovat na požádání tyto záznamy dozorovému úřadu. Zaznamy obsahuji: jméno a kontakt správce a zpracovatele, účel zpracování, popis kategorií údajových subjektů, kategorie příjemců údajů, lhůty pro vymazání údajů, informace o předávání osobních údajů mezinárodně a popis organizačních a technických opatření. Záznamy se netýkají firem s méně než 250 pracovníky, není-li v jejich náplni práce vést osobní a citlivé údaje a nehrozí-li žádné riziko pro svobodu osob. [30]

3.7 Pokuty za porušení

Poruší-li firma toto ustanovení, pak jim hrozí pokuta až 20 milionů euro nebo až 4 % (podle toho, která je vyšší) z celkového celosvětového obratu firmy za minulý finanční rok. Vše se odvíjí podle typu, délky, škody, snahy předejít porušení. Nastane-li škoda fyzických osob, mohou být firmy obžalovány a nuceny vyplatit náhradu. Firmy tak ztratí svůj respekt. [31]

4 SOUVISLOST MEZI GENERAL DATA PROTECTION REGULATION A KYBERNETICKOU BEZPEČNOSTÍ MALÝCH FIREM

General Data Protection Regulation udává směr a říká firmám, jak by s údaji mělo být zacházeno, udává práva a povinnosti, zlepšuje ochranu osobních údajů. Nepopisuje konkrétně jak situace řešit, neslouží tedy jako prevence proti úniku údajů, tu si musí firma pohlídat sama. Například při nezvolení uchazeče, musí být jeho životopis ihned skartován (nesouhlasí-li se zachováním). Kybernetická bezpečnost bývá menšími firmami z důvodu jejich velikosti často podceňována a to z nich dělá snadné cíle pro krádež dat útočníky.

4.1 Vliv na firmy

GDPR se dotkne každé firmy. Ta bude mít za úkol postarat se o to, aby fungovala v souladu s GDPR. Proto se musí daná firma vypořádat s několika předem danými kategoriemi. Mezi tyto kategorie patří: Osobní údaje, Role firmy, Účely, Zpracování osobních údajů, Poskytování osobních údajů třetím stranám, Ochrana osobních údajů, Práva fyzických osob / nové povinnosti firem. [49]

4.1.1 Osobní údaje

V prvé řadě si firma musí stanovit, jaké osobní údaje zpracovává a vytvořit jejich seznam. Jedná se o jméno, příjmení, číslo účtu, adresa atd. Dále také musí stanovit, zda-li zpracovává údaje o dětech nebo údaje ze zvláštní kategorie (zdravotní stav, politické názory, náboženství, rasa atd.) [49]

4.1.2 Role firmy

Firma rozhodne, zda-li plní roli správce, zpracovatele nebo příjemce. Správce údává způsob a účel zpracovávání údajů. Udává co se bude zpracovávat a jak se bude zpracovávat. Například v případě vykonávání služby autoškoly, bude navíc potřeba od osob znát jejich zdravotní stav. Vykonává-li firma roli zpracovatele, provádí pak činnost, která mu byla zadána správcem. Tedy zpracovává údaje ve jménu správce. Může také ale být příjemcem, kdy přijímá údaje poskytnuté správcem či zpracovatelem, například daňový úřad. [49]

4.1.3 Účel

Je potřeba sepsat, pro jaký účel jsou údaje shromažďovány a také konkrétně jaké údaje jsou sbírány pro daný účel. Může se jednat například o marketing. Dále je potřeba definovat, jestli ke zpracování údajů byl udělen souhlas, jestli zpracování probíhá na základě smlouvy (např. nutná doprava - údaje k doručení), zda-li zpracování vyplývá z právních povinností (údaje nutné pro jejich konání) a v neposlední řadě jedná-li se o oprávněný zájem správce (předání údajů vrámci podniku pro administrativní účel). [49]

4.1.4 Zpracování osobních údajů

V prvé řadě se zjišťuje, na jakých médiích se údaje zpracovávají – zda-li se jedná o fyzický dokument či informační systém a jejich následné vytvoření seznamů. Jaká oddělení údaje zpracovávají, zda-li se užívají pro profilování a dále jejich získávání – kde a jak; jejich aktualizace - kdo a kdy provádí aktualizaci a na jakém místě je výsledek aktualizace zaznamenán; likvidaci – kdo provádí likvidaci a kdy ji provádí. [49]

4.1.5 Poskytnutí údajů třetím stranám

Firma zjistí, zda-li údaje poskytuje vrámci Evropské unie, či mimo ni, zároveň zjišťuje konkrétní třetí strany (například firmy), jemž jsou údaje poskytnuty. [49]

4.1.6 Ochrana osobních údajů

Způsob zajištění ochrany osobních údajů se rozděluje na dvě části – ochranu fyzických dokumentů a systémových dat. V případě fyzických dokumentů to je jejich bezpečné umístění a uzamčení. Systémová data mohou být chráněna přístupovými právy či různě šifrovaná. [49]

4.1.7 Práva fyzických osob, povinnosti

Aby firma vyhovovala GDPR, musí být schopna zajistit výmaz údajů na žádost fyzické osoby při odvolání souhlasu a nebo, nejsou-li potřeba ke konání činnosti firmy. Dále zajistit přístup k údajům vedených o osobě a jejich případnou opravu na základě žádosti. Být schopen jako správce dát zpracovateli příkaz k vymazání osobních údajů, omezit používání osobních údajů na určitou dobu a to jak fyzických dokumentů tak i v systémech a zajištění možného přenosu údajů třetím osobám. Důležité je také být seznámen

s postupem řešení případně vzniklého problému narušení údajů – jak se bude řešit, kdo problém vyřeší a případné informování subjektu údajů. [49]

4.2 Prevence úniku dat

Firmy jsou povinny učinit vše pro to, aby nenastala situace, kdy se údaje o osobách či firemním tajemství dostanou do nesprávných rukou. Mohlo by to poškodit reputaci firmy, vznikly by zbytečné náklady a hlavně ohrozilo bezpečnost osob. Pro zvýšenou bezpečnost by měly být sítě počítačů zaměstnanců odděleny od serverové sítě, chráněny firewallem a antivirovým programem. Také je vhodné omezení práv manipulace s daty a zavedení autentizace.

4.2.1 Data Loss Prevention

GDPR udává přísná pravidla ohledně ochrany dat. Způsobů jak předejít ztrátě dat je několik. Jde především o Data Loss Prevention, což jsou systémy, které mají za úkol hlídat, omezovat a ohlašovat nakládání s daty. Zvolí se data, která se označí jako citlivá, poté se pro tato citlivá data určí pravidla, která se budou odvíjet od pozice či role zaměstnance. Jedna skupina pracovníků bude moci data pouze číst a upravovat, kdežto jiný typ pracovníků (například nadřízení) mají povoleno data také přeposílat. Brání také neautorizovanému spouštění aplikací a tisku. Data lze sledovat, jak je s nimi zacházeno, tudíž se předchází krádeži dat zaměstnanci, především v místech, kde data opouštějí infrastrukturu firmy jako jsou e-maily, proxy servery, instant messaging nebo i USB disky. Data Loss Prevention je schopen bránit před škodlivým software, jako je malware, trojský kůň atd. [32]

4.3 Právo na výmaz

Právo na výmaz je právo, kdy může osoba (subjekt), o níž se vedou údaje, požádat o jejich smazání ze systému. Správce údaje bezodkladně smazat (dovolí-li mu to zákon) a musí informovat ostatní správce a subjekt, že údaje o subjektu byly vymazány. Tento úkon provádí správce a nelze jej odvolat. Lze provést pouze za následujících podmínek: Neslouží-li údaje nadále svému účelu (nutno mazat i bez požádání), osoba odvolá souhlas, poskytnutý ke zpracování údajů a neexistuje-li další právní důvod zpracování. Dále v případě vznesení námitky subjektu údajů proti zpracování, převažuje-li zájem

subjektu nad zájmem správce, nejsou-li údaje zpracovávány podle GDPR. Údaje se musí smazat, přikazuje-li to právní předpis Evropské unie. [33]

V několika případech však správce údaje mazat nesmí: Jde-li o zpracování vrámci svobody projevu (žurnalistika, veřejný rejstřík), na správce působí povinnost Evropské unie (banky, účetnictví). Při zpracování údajů vrámci právních úkonů. V případě zpracovávání za účelem výkonu veřejné moci či veřejném zájmu, v případě archivace, historického a vědeckého výzkumu, statistik. [33]

4.4 Souhlas o zpracování údajů

Souhlasem se dává svolení k užívání osobních údajů subjektu. V praxi se může jednat například o povolení internetového obchodu zasílat nejnovější nabídky na e-mail, nebo souhlas o uvedení fotografie zaměstnance na web. Souhlas musí být doložitelný a odvolatelný. Souhlas musí být svobodný, jednoznačný, informovaný a konkrétní. [34]

4.4.1 Svobodný a jednoznačný

Subjekt musí mít možnost rozhodnout se, zda-li souhlas poskytne. Souhlas zpracování osobních údajů nesmí být podmíknou k uzavření smlouvy a také nesmí být nezbytným krokem v pokračování vyplnění formuláře. Jedná-li se například o mobilní hudební aplikaci, nesmí být vyžadován přístup k poloze, jelikož s funkčností aplikace nesouvisí.

Souhlas musí být jednoznačně udělen subjektem. Nesmí být předem vyplněno políčko souhlasu nebo udělen mlčením (neaktivitou). Musí být srozumitelný a viditelně zobrazen, aby si ho subjekt všiml (převážně v jiných prohlášeních). [34]

4.4.2 Informovaný a konkrétní

Při poskytování souhlasu musí být subjekt dostatečně seznámen s informaceni jako jsou: účel zpracování, totožnost správce, jaké údaje se budou zpracovávat, jestli budou údaje automatizované, zda-li budou poskytnuty do zahraničí, informace o odvolání souhlasu, výmazu, omezení a přístupu, informace o dalším zpracování údajů, zda poskytnutí údajů je smluvním požadavkem. Vše musí být srozumitelně vysvětleno. [34]

4.5 Zveřejňování fotografií a videí na internetu

Ať už se jedná o fotky či videa z veřejných akcí, nebo chce-li zaměstnavatel použít fotku vrámci plnění jeho povinností (například na vizitku, ve firemní síti, monitoring), nebo chce své zaměstnance představit na facebooku, budou se vztahovat různá pravidla.

Jedná-li se o použití fotografie na zaměstnaneckých vizitkách (vrámci činnosti firmy), souhlas není vyžadován. Stejně tak není vyžadován při použití ve firemních systémech nebo při monitorování (vrámci ochrany majetku a zdraví při práci, ne v šatnách). Avšak při vystavení fotky či videa na internetové stránce je potřeba získat od osob, jež jsou na fotce či videu zobrazeny, souhlas. [35]

Souhlas může být písemný, ale také vyplývající z kontextu. Například pokud se pořizují fotky na sociální sítě a oslovené osoby dobrovolně zapózují, žádný problém nenastane. Stejně tak v případě natáčení reportáže z nějaké firemní akce, osoby by však měly znát důvod pořízení a tento důvod nesmí být změněn (například z reportáže na reklamu). [36]

PRAKTICKÁ ČÁST

5 SOUČASNÝ STAV BEZPEČNOSTI INFORMAČNÍCH TECHNOLOGIÍ

V dnešní době jsou firmy v neustálém nebezpečí jak z venku, tak zevnitř. Hackeři se neustále snaží o získání cenných informací (účty, soubory) a majetku využíváním nejrůznějších praktik. Problém může ale nastat i uvnitř firmy, chtějí-li firmě uškodit nespokojení zaměstnanci nebo problém způsobí omylem nezkušení pracovníci. Oblasti působení bezpečnostních technologií jsou například: zdravotní a sociální služby, dodávky pohonné hmoty, plynu, vody, ale také veřejná správa či jiné činnosti firem.

5.1 Připravenost na kybernetický útok

Podle IBM Security se firmy nedostatečně připravují na možný kybernetický útok. Bezpečnost je firmami podceňována. Přibližně 77 % dotazovaných firem (z celkových 2800) sdělilo, že v případě naskytnutého problému nemají zaveden CSIRP, nebo-li Computer Security Incident Response Plan, což je plán, který má za úkol pomoct vypořádat se, zmírnit škody a náklady vyvolané případným kybernetickým útokem. Kolem 1400 dotazovaných firem by problém řešila až při jeho naskytnutí. Důvodem může být absence IT specialistů (77 %) nebo špatně vynaložený rozpočet (jemuž vyhovuje jen 31 % dotázaných). Důležitost se však klade na zkušenosti pracovníků a současně jejich propojení s technickou částí firmy. Většina firem si však myslí, že jejich kybernetická bezpečnost je oproti minulému roku na lepší úrovni především z důvodu zkušených zaměstnanců, avšak stejně důležité je mít zavedeny co nejnovější a nejspolehlivější technické nástroje. Až 60 % považuje současné vynaložení financí do umělé inteligence za nedostatečné. Navíc se také podle 57 % respondentů zvětšil čas potřebný k vypořádání s problémem oproti minulému roku a 65% si myslí, že jsou útoky agresivnější. [46]

5.2 Využití biometrie

Nejpopulárnějším způsobem pro přihlašování k účtů je používaní klasických psaných hesel. Nevýhodou těchto hesel je však to, že většina lidí používá příliš jednoduchá hesla. Ať už jsou tato hesla krátká, bez kombinace čísel, písmen a znaků, tak k jejich oslabení přispívá i využívání stejných hesel na více účtech najednou. Většinou to je z důvodu snažšího zapamatování. Důsledkem je pak mnohem rychlejší odcizení účtů. V roce 2017

bylo ze všech případů krádeže účtů více než 80 % způsobeno vinou vlastníka účtu. Z tohoto důvodu přichází na scénu biometrické přihlašování. [37]

Biometrií se odbourává nutnost pamatovat si několik složitých hesel. V případě biometrie stačí pouze použít otisk prstu, skenování oční duhovky nebo i hlasovou detekci. Této praktiky budou nejvíce využívat finanční společnosti. Společnost IBM provedla studii, kdy se dotazovala čtyř tisíců lidí ohledně digitální autentizace. Vyšlo najevo, že při používání finančních služeb se 70 % dotazovaných lidí zaměřuje spíše na bezpečnost, včetně využívání e-shopů a e-mailů. Jedná-li se o sociální stránky, lidé spíše upřednostňují pohodlí přihlašování (36 %), pak bezpečnost (34 %) a nakonec soukromí (30 %). Největším problémem je, že se biometrické údaje mohou použít pro kompromizaci soukromí nebo bezpečnosti, například použití falešných údajů. Dále z dotazníku vyplývá, že skoro polovina (44 %) dotázaných považuje biometrické přihlášení (konkrétně otisk prstu) za nejvíce bezpečný způsob přihlašování oproti klasických hesel. Až 93 % zákazníků bank preferuje přihlašování biometrickými údaji. [45]

5.3 Studie nákladů při úniku dat

V roce 2017 institut Ponemon a firma IBM zkoumaly finanční škody způsobené únikem dat firem po celém světě. Zkoumáno bylo 11 států: Spojené Státy Americké, Spojené Království, Francie, Japonsko, Itálie, Brazílie, Austrálie, Německo, Indie, Kanada a Jižní Afrika. K těmto státům byly také přiřazeny 2 regiony: Střední východ a Sdružení národů jihovýchodní Asie. Studie probíhala celkem ve 419 společností a zjistilo se, že průměrná celková cena napáchaných škod z důvodu úniku dat za rok 2017 se vyčíslila na průměr 3.62 milionů dolarů, což je o 0.38 milionů dolarů méně než v roce 2016. Dále ze studie vyplývá, že škoda vzniklá z jednoho záznamu činila průměrně 141 dolarů (Nejvíce měly zdravotní služby – 380 dolarů, poté finanční služby 245 dolarů). Chyby vzniklé lidským omylem nebo chybou v systému stály 128 dolarů za záznam a 156 dolarů při útoku zaviněném malwarem. Počet narušených údajů při útoku se podle konkrétní firmy pohyboval mezi 2,6 tisíc až 100 tisíc. Došlo se také na to, že pravděpodobnost dalšího útoku během na tyto firmy činí 27,7 %. Peněžní následky útoku jde z části regulovat pojištěním proti úniku dat. Nedokáží-li firmy předejít nebo rychle jednat při útoku, hrozí jim ztráta klientů a poškození reputace. [38]

5.4 Zavedení WPA3 jako důsledek útoku KRACK

V druhé polovině roku 2017 se vyskytla hrozba zvaná KRACK. Celým názvem Key Reinstallation Attack, který způsobuje zranitelnost protokolu WPA2. Dokáže dešifrovat zabezpečená data a obejít zadávání hesla do wifi. Může dojít například k odcizení údajů kreditních karet a hesel. [47]

Důvodem zavedení WPA3 je právě KRACK. WPA2 je staré 14 let a není již natolik bezpečné. K zabezpečení připojení se budou používat 192 bitové klíče z algoritmu CNSA (Commercial National Security Algorithm). Tento nový protokol podporuje ochranu proti brute force útokům, tedy proti neustálému hádání hesla, kdy se wi-fi přístup zablokuje. Nová podpora také spočívá v lepší bezpečnosti například televizí a jiné elektroniky, včetně těch, u kterých se nevyskytuje displej. K užívání je ale potřeba mít certifikovaný router a zařízení připojená k němu, tudíž to bude chvíli trvat. WPA3 by měl být uveden do provozu v roce 2018. [48]

5.5 Významné hrozby

Význam a důležitost kybernetické bezpečnosti stále roste. Je to hlavně z důvodu neustále se zdokonalujícími technologiemi a to i těmi škodlivými, jako jsou nejrůznější viry, ransomware, spyware atd. Většina důležitých webových stránek či databází je v dnešní době šifrovaná, přesto jsou ale zkušení útočníci schopni tuto ochranu obejít a způsobit celosvětovou škodu.

5.5.1 Botnety

Populárním způsobem pro šíření škodlivého software je využívání e-mailů. Útočníci posílají soubory (spam), které obsahují viry a jiný škodlivý software. A právě zde přicházejí botnety. Jde o síť zařízení, které mají za úkol automaticky rozesílat škodlivý software na různé e-mailové adresy současně. Jsou většinou ovládány z centrálního zařízení. Nakaženým zařízením se také říká zombie. Mezi známé botnety patří například Necurs a Satori. [39]

5.5.1.1 Necurs

Jedná se o největší botnet, který je určen pro šíření malware přes e-mailové přílohy. Během jeho existence bylo zaznamenáno nespočet incidentů tohoto botnetu. Nejnovější

incident však nastal koncem března roku 2018. Během jediného dne rozeslal kolem sto tisíc
e-mailů, které se chovaly jako objednávky s přílohou. Uživatelé tak otevřeli tuto přílohu a byli nakaženi trojským koněm zvaným Quant Loader, který je schopen do počítače vložit ransomware a vymáhat peníze, nebo ukrást citlivá hesla. [40]

5.5.1.2 Satori

Nejnovější verze tohoto botnetu se od ostatních botnetů liší tím, že jeho hlavním cílem jsou zařízení, na kterých se těží kryptoměna zvaná Ethereum. Satori napadne tato zařízení a přepíše cílovou adresu, na kterou je vytěžená částka poslána. Útočí na zařízení, na kterém je nainstalován program pro těžbu, zvaný Claymore. [41]

5.5.2 WannaCry

V květnu 2017 se mnoho počítačů stalo terčem útoků ransomwarem zvaným WannaCryptor 2.0. Jde o zablokování dat, jejichž odblokování stojí peníze. K tomuto útoku došlo začátkem května 2017 a byly napadeny počítače po celém světě (až 99 zemí), V té době bylo hlavní obětí Rusko, kdy bylo napadeno až 57 % z více než 100 000 celkových útoků, včetně ruské telekomunikační firmy Megafon. Toto číslo se nakonec vyšplhalo nad 230 000. Byla také napadena zdravotní služba National Health Service ve Velké Británii, nebo telekomunikační středisko ve Španělsku zvané Telefonica. Za obnovu dat tento ransomware po firmách požadoval bitcoiny v hodnotě 300 dolarů. Ransomware změní příponu zablokovaných souborů na .WNCRY a odblokování lze uskutečnit po zaplacení částky, jinak budou soubory smazány. [42]

5.5.3 NotPetya

Tento malware se začal objevovat v červnu v ukrajinském účetním a daňovém software M.E.Doc (My electronic document). Po uskutečnění útoku a využití zranitelnosti protokolu SMB (Server Message Block), získali útočníci přístup ke zdrojovému kódu. Úpravou zdrojového kódu se malware začal šířit vydáváním za softwarovou aktualizaci, kterou si uživatelé stáhli. Postiženy byly počítače hlavně na Ukrajině, v Dánsku, Rusku, Francii a Španělsku, neboť malware byl cílen na Ukrajinu a s ní obchodující firmy. NotPetya se vydával jako ransomware, ovšem jeho primární cíl bylo zničit data firmy a zjistit informace o transakcích. [44]

6 ANALÝZA DOSTUPNÝCH OPEN SOURCE NÁSTROJŮ

Začínající nebo stávající firmy s menším počtem zaměstnanců mohou na používání open-source software ušetřit. Ať už se jedná o operační systém, tak i kancelářský software, databáze, e-mailové klienty, cloudová úložiště, účetní software atd.

6.1 Zkoumané kategorie

Pro potřebu bakalářské práce a zachování přiměřené délky bylo vybráno 5 typů software určené pro bezpečnost. Těmito typy jsou: Antivirové programy, Šifrování dat, Nástroje pro správu hesel, Firewall, Nástroje pro řízení oprávnění.

Každá firma má jiné požadavky na open source software, neboť se firmy náplní práce od sebe liší. Stejně tak se od sebe liší samotný software, který může pokrývat širokou oblast. Proto se v této části budou zkoumat specifická kritéria určitého software vždy v dané kategorii. Každé kritérium lze ohodnotit jednou z pěti hodnot, kdy hodnota 5 – nejvíce bodů a hodnota 1 – nejméně bodů.

6.1.1 Sdílená kritéria

Následující kritéria jsou z velké části pro všechny kategorie společná. Jde o kritéria popisující obecné předpoklady vybraných open source software.

Tabulka 1: Operační systém

5	Windows 7, 8, 10 + OS X + Linux
4	Windows 7, 8, 10 + OS X nebo Linux
3	OS X + Linux
2	Windows 7, 8, 10
1	OS X nebo Linux

Tabulka 2: Jazyk dokumentace

5	Dostupná v angličtině a češtině
4	Dostupná v češtině
3	Dostupná v angličtině
2	Dostupná pouze mimo angličtinu a češtinu

Tabulka 3: Podpora k programu

5	Forum, mailing list, komerční podpora
4	Forum a mailing list nebo komerční podpora
3	Mailing list a komerční podpora
2	Forum nebo komerční podpora nebo mailing list
1	Neexistuje

Tabulka 4: Ovladatelnost

5	Používá se jednoduché grafické rozhrání
4	Používá se složitější grafické rozhrání
3	Grafické rozhrání + dodatek příkazového řádku
2	Příkazový řádek + dodatek grafického rozhrání
1	Používá se pouze příkazový řádek

Tabulka 5: Aktualizace programu

5	Pětkrát ročně nebo více
4	Čtyřikrát ročně
3	Třikrát ročně
2	Dvakrát ročně
1	Jednou ročně

6.1.2 Antivirové programy

Je zcela známo, že unixové systémy jsou proti virům velmi odolné. Přestože viry nemusí mít na systém vliv, existuje možnost, že se nakažené soubory přepošlou dále (například klientům) a tím se virus rozšíří na ostatní počítače (i ty s windowsem). Mezi nejznámější open source antivirus patří například ClamAV.

6.1.2.1 Specifická kritéria

V následujících tabulkách jsou zobrazená jednotlivá kritéria, včetně popisu jejich bodových hodnot, náležící konkrétně antivirům.

Tabulka 6: Antivirus – Automatická aktualizace virové databáze

5	Více než jednou denně
4	Jednou denně
3	Více než jednou týdně
2	Jednou týdně
1	Není automaticky aktualizována

Tabulka 7: Antivirus – Vestavěná podpora souborů

5	E-mail, dokumenty, archivační formáty
4	E-mail a dokumenty nebo archivační formáty
3	E-mail
1	Bez vestavěné podpory

Tabulka 8: Antivirus – Příkazový řádek jako skener virů

5	Ano
1	Ne

6.1.3 Šifrování dat

Tyto programy dokáží zašifrovat soubory, celý disk, nebo jen jeho část. Dojde k přeměně na nečitelný kód a k zabránění neoprávněnému čtení dat. Nejznámějším softwarem tohoto typu byl TrueCrypt, jehož vývoj byl ovšem zastaven a místo něho se objevil VeraCrypt.

6.1.3.1 Specifická kritéria

V následujících tabulkách jsou zobrazená jednotlivá kritéria, včetně popisu jejich bodových hodnot, náležící konkrétně šifrování dat.

Tabulka 9: Šifrování dat - Počet šifrovacích algoritmů

5	Pět a více
4	Čtyři
3	Tři
2	Dva
1	Jeden

Tabulka 10: Šifrování dat - Počet hashovacích algoritmů

5	Pět a více
4	Čtyři
3	Tři
2	Dva
1	Jeden

Tabulka 11: Šifrování dat - Backdoor

5	Ano
1	Ne

6.1.4 Nástroje pro správu hesel

Používá-li firma hodně služeb, kde jsou potřeba přihlašovací údaje (e-mail, internetový obchod, přihlášení do sítě, k firemním účtům atd.), je potřeba volit dostatečně složitá hesla. Hesla by se neměla opakovat, pro každý účet by mělo být použité heslo jiné. To má za následek rozsáhlý seznam nejrůznějších přihlašovacích údajů, jež může být problém si zapamatovat a vést ho nechráněně není vhodné. Nástroje pro správu hesel jsou výbornou pomůckou pro skladování hesel do databáze za použití šifrování, jedná se například o KeePass.

6.1.4.1 Specifická kritéria

V následujících tabulkách jsou zobrazená jednotlivá kritéria, včetně popisu jejich bodových hodnot, náležící konkrétně nástrojům pro správu hesel.

Tabulka 12: Správce hesel – Kvalita generátoru náhodného hesla

5	Písmena (velká a malá), čísla, speciální znaky, mezery, vlastní řetězec
4	Písmena (velká a malá), čísla, speciální znaky
2	Písmena (velká a malá), čísla
1	Písmena (velká a malá)

Tabulka 13: Správce hesel – Integrace do webových prohlížečů

5	Mozilla Firefox, Chrome, Microsoft Edge, Opera
4	Tři z (Mozilla Firefox, Chrome, Microsoft Edge, Opera)
3	Dva z (Mozilla Firefox, Chrome, Microsoft Edge, Opera)
2	Jeden z (Mozilla Firefox, Chrome, Microsoft Edge, Opera)
1	Bez integrace

Tabulka 14: Správce hesel – Automatické mazání schránky

5	Ano
1	Ne

6.1.5 Firewall

Firewall je určen pro monitorování sítě, detekování nežádoucích událostí v síti a jejich případnému řešení. Může například blokovat, restartovat síť nebo zablokovat komunikaci se serverem nacházejícím se v jiné síti. Mezi tyto firewally patří OPNsense.

6.1.5.1 Hodnocená kritéria

V následujících tabulkách jsou zobrazená jednotlivá kritéria, včetně popisu jejich bodových hodnot, náležící konkrétně firewallů. Při hodnocení není hodnocen.

Tabulka 15: Firewall – Minimální frekvence CPU

5	1 GHz a méně
3	2 GHz
1	4 GHz

Tabulka 16: Firewall – Minimální velikost RAM

5	1 GB RAM a méně
3	2 GB RAM
1	4 GB RAM

Tabulka 17: Firewall – Traffic shaping (řízení provozu)

5	Ano
1	Ne

Tabulka 18: Firewall – Intrusion Prevention System

5	Ano
1	Ne

Tabulka 19: Firewall – Virtual Private Network

5	Ano
1	Ne

Tabulka 20: Firewall – Podpora pluginů

5	Ano
1	Ne

6.1.6 Nástroje pro řízení oprávnění

Vede-li firma zaměstnance, potýká se s rizikem zneužití dat a neoprávněného přístupu. Proto je vhodné mít zavedeny nástroje pro správu identity. Při zavedení tohoto nástroje, se pověří osoba, která se bude o správu starat. Jednoduše pak může zařazovat či vyřazovat osoby ze systému a tím jim odebírat práva. Je potřeba hlavně u firem zabývajících se financemi nebo velkého počtu lidí, z důvodu přísného sledování, kdo má kde přístup. K tomuto účelu lze použít Apache Syncope. [43]

6.1.6.1 Hodnocená kritéria

V následujících tabulkách jsou zobrazená jednotlivá kritéria, včetně popisu jejich bodových hodnot, náležící konkrétně nástrojům pro řízení oprávnění.

Tabulka 21: Řízení oprávnění – Minimální frekvence CPU

5	1 GHz
3	2 GHz
1	3 GHz

Tabulka 22: Řízení oprávnění – Minimální velikost RAM

5	1 GB nebo méně
4	2 GB
3	4 GB
2	8GB
1	Více než 8 GB

Tabulka 23: Řízení oprávnění – Password policy (podmínky hesla)

5	Ano
1	Ne

6.2 Stanovení vah kritérií

Zde budou stanoveny váhy jednotlivých kritérií daných kategorií programů. Ke stanovení vah je použita metoda párového porovnávání, zvaná také jako Fullerova metoda. Po uskutečnění porovnání všech kritérií se všemi ostatními kritérii dané kategorie, stanovení preferencí pro kritérium (součet 1 v řádku + 0 ve sloupci) a následném stanovení pořadí, jsou vypočteny nenormované váhy podle vzorce: $k_i = n + 1 - p_i$, kde n je počet

kritérií a p_i je pořadí i-tého kritéria v jeho preferenčním pořadí, číslo 1 se přičítá proto, aby kritérium nemělo nulovou preferenci. Poté se váhy normují pomocí vzorce:

$v_i = \frac{k_i}{\sum_{i=1}^{n} k_i}$, kde k_i je nenormovaná váha a n je počet kritérií. Jde o podíl nenormované váhy se součtem všech nenormovaných vah. Váhy jsou zaokrouhleny na 2 desetinná místa.

Tabulka 24: Stanovení vah - Antiviry

Kritéria	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	Preferencí	Pořadí	k_i	v_i
K_1	x	1	0	1	0	0	1	1	4	3	6	0.17
K_2		x	0	0	0	0	1	1	2	6	3	0.08
K_3			x	1	1	0	1	1	6	2	7	0.19
K_4				x	1	0	1	1	4	4	5	0.14
K_5					x	0	1	1	4	5	4	0.11
K_6						x	1	1	7	1	8	0.22
K_7							x	1	1	7	2	0.06
K_8								x	0	8	1	0.03

Tabulka 25: Stanovení vah – Šifrování dat

Kritéria	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	Preferencí	Pořadí	k_i	v_i
K_1	x	1	1	1	0	0	0	0	3	6	3	0.08
K_2		x	0	0	0	0	0	0	0	8	1	0.03
K_3			x	1	0	1	1	0	4	3	6	0.17
K_4				x	0	0	0	0	1	7	2	0.06
K_5					x	1	1	1	9	1	8	0.22
K_6						x	0.5	0	3.5	4	5	0.14
K_7							x	0	3.5	5	4	0.11
K_8								x	6	2	7	0.19

Tabulka 26: Stanovení vah – Nástroje pro správu hesel

Kritéria	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	Preferencí	Pořadí	k_i	v_i
K_1	x	1	1	1	0	1	1	0	5	2	7	0.19
K_2		x	0	0	0	1	1	0	2	6	3	0.08
K_3			x	1	0	1	1	1	5	3	6	0.17
K_4				x	0	1	1	1	4	4	5	0.14
K_5					x	1	1	1	7	1	8	0.22
K_6						x	0	0	0	8	1	0.03
K_7							x	0	1	7	2	0.06
K_8								x	4	5	4	0.11

Tabulka 27: Stanovení vah - Firewall

Kritéria	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	Preferencí	Pořadí	k_i	v_i
K_1	x	0	0	0	0	0	0	0	0	0	0	10	1	0.02
K_2		x	1	0	1	1	1	0	0	1	6	4	7	0.13
K_3			x	0	1	1	1	0	0	1	5	5	6	0.11
K_4				x	1	1	1	0.5	0.5	1	8	2	9	0.16
K_5					x	0.5	0	0	0	1	2.5	7	4	0.07
K_6						x	0	0	0	1	2.5	8	3	0.05
K_7							x	0	0	1	4	6	5	0.10
K_8								x	1	1	8.5	1	10	0.18
K_9									x	1	7.5	3	8	0.15
K_{10}										x	1	9	2	0.04

Tabulka 28: Stanovení vah – Nástroje pro řízení oprávnění

Kritéria	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	Preferencí	Pořadí	k_i	v_i
K_1	x	1	0	1	0	0	0	1	3	5	4	0.11
K_2		x	0	0	0	0	0	0	0	8	1	0.03
K_3			x	1	0	1	1	1	6	2	7	0.19
K_4				x	0	0	0	1	2	6	3	0.08
K_5					x	1	1	1	7	1	8	0.22
K_6						x	0.5	1	4.5	3	6	0.17
K_7							x	1	4.5	4	5	0.14
K_8								x	1	7	2	0.06

6.3 Hodnocení software

Zde proběhne popis funkčních prvků jednotlivých programů a také přidělení bodů jednotlivým kritériím různých programů. Kategorie programů byly vybrány tak, aby pokrývaly několik různých oblastí bezpečnosti, jako například správa hesel, ochrana před viry nebo šifrování samotných dat. Udělení bodů bylo docíleno na základě shromáždění potřebných informací o daných programech skrze oficiální stránky programů či uživatelských fór. Každé kritérium je bodově ohodnoceno dle tabulek uvedených v bodech 6.1. Získané body jsou dále využity při výpočtu celkového průměru hodnocení daného programu. Také jsou využity váhy jednotlivých kritérií – bod 6.2, které se použijí u výpočtu finálního průměru. Každé kritérium má uvedeno také své normované bodové ohodnocení. Ke konečnému ohodnocení programů byla použita metoda váženého průměru daného podle vzorce: $\bar{\mathbf{x}} = \frac{\Sigma_{i=1}^{n} v_i * x_i}{\Sigma_{i=1}^{n} v_i}$, kde v_i je normovaná váha a x_i jsou body udělené

jednotlivým kritériím. Výsledný průměr může dosáhnout maxima 5 bodů a je zaokrouhlen na dvě desetinná místa.

6.3.1 Antivirové programy – ClamAV

ClamAV je open source nástroj vyvíjený od roku 2004, určený pro zachytávání škodlivých virů, trojanů a malware. Je licencován pod GNU General Public License verze 2. Lze ho využít pro nespočet operací a to například pro skenování e-mailových příloh, skenování počítače a také skenování webových stránek. Nabízí také širokou podporu archivačních a kancelářských formátů. ClamAV funguje pouze přes příkazový řádek a pro méně znalé uživatele se může jevit problémový, přestože práce přes řádek je rychlejší. Z toho důvodu je k dispozici mnoho modifikací, včetně ClamTk, což je grafické uživatelské rozhraní pro tento antivirus. ClamAV je nejznámější open source antivirus, je zcela zdarma a má dlouhou historii vývoje.

6.3.1.1 Funkční předpoklady

- Pokročilá aktualizace databáze s podporou skriptovaných aktualizací a podpisů
- Aktualizace databáze několikrát denně
- Rychlé skenování pomocí příkazového řádku
- Vestavěná podpora e-mailů
- Filtrování e-mailů
- Podpora archivačních formátů
- Podpora kancelářských formátů MS Office a MacOffice, HTML, Flash, RTF a PDF
- Množství pluginů včetně grafického rozhraní ClamTk

6.3.1.2 Bodové hodnocení

Tabulka 29: Hodnocení - ClamAV

	Body x_i	Normované váhy v_i	Konečné hodnocení
Operační systém	5	0.17	0.85
Jazyk dokumentace	3	0.08	0.24
Podpora k programu	2	0.19	0.38
Ovladatelnost	2	0.14	0.28
Aktualizace programu	5	0.11	0.55
Aktualizace virové databáze	5	0.22	1.10
Podpora souborů	5	0.06	0.30
Příkazový řádek – skener	5	0.03	0.15
Vážený průměr			**3.85**

6.3.2 Šifrování dat – VeraCrypt

Šifrovací programy (anglicky Encryption software) je vynikajícím nástrojem pro bezpečnost. Lze jim totiž zašifrovat data v počítači a to hned několika různými algoritmy. Veracrypt obsahuje těchto algoritmů hned 5 včetně jejich kombinací. Veracrypt (první verze vydána roku2013) vychází z TrueCryptu (2004), jež je jeho přímý předchůdce a podporuje tedy dekrypci dat zašifrovaných TrueCryptem. Je licencován Apache License 2.0 a TrueCrypt License 3.0. Je to populárníprogram pro šifrování dat a to zejména díky jeho osvědčenosti, velkému počtu funkcí a počtu šifrovacích a hashovacích algoritmů.

6.3.2.1 Funkční předpoklady

- Tvorba zašifrovaného virtuálního disku
- Šifrování diskového oddílu nebo celých fyzických disků
- Šifrování diskového oddílu s nainstalovaným Windowsem.
- Automatické šifrování

- Paralelizace – proces šifrování probíhá vícekrát současně (dle dostupných jader procesoru)
- Pipelining – dešifrování probíhá již při načítání dat
- Hardwarově urychlené šifrování
- Šifrovací algoritmy: AES, Camellia, Kuznyechik, Serpent, Twofish a jejich kombinace
- Hashovací algoritmy: RIPEMD-160, SHA-256, SHA-512, Whirlpool a Streebog
- Příkazový řádek

6.3.2.2 Bodové hodnocení

Tabulka 30: Hodnocení - Veracrypt

	Body x_i	Normované váhy v_i	Normované hodnocení
Operační systém	5	0.08	0.40
Jazyk dokumentace	3	0.03	0.09
Podpora k programu	2	0.17	0.34
Ovladatelnost	5	0.06	0.30
Aktualizace programu	3	0.22	0.66
Počet šifrovacích algoritmů	5	0.14	0.70
Počet hashovacích algoritmů	5	0.11	0.55
Backdoor	5	0.19	0.95
Vážený průměr			**3.99**

6.3.3 Nástroje pro správu hesel – KeePass

KeePass je jeden ze softwarů pro správu uživatelských jmen a přihlašovacích hesel. Hesla jsou uložena v jedné offline databázi a poté stačí jedním kliknutím zkopírovat heslo do schránky, která se po určité době či po ukončení programu sama vymaže. Program také obsahuje kvalitní generátor náhodných hesel. Databáze je šifrována algoritmy AES nebo Twofish a k přístupu do databáze je potřeba znát tzv. Master key, tedy něco jako hlavní

klíč. Zapomene-li tento master key, k databázi se již nedostaneme, jelikož program neobsahuje backdoor (zadní vrátka). První verze programu vyšla v roce 2003 a je lincencován GNU GPL. Obsahuje také mnoho pluginů a portů na jiné systémy, včetně iPhone a Android. Je také přeložen do 50 jazyků.

6.3.3.1 Funkční předpoklady

- Silná bezpečnost – šifrování databáze, master key a polí s hesly
- Možnost využití klíčového souboru, či souboru s master key
- Portable verze
- Exportace seznamu hesel
- Snadný převod databáze mezi zařízeními
- Možnost zaheslovat soubory
- Automatické vyplňování formulářů a snadné kopírování polí
- Kopírování do schránky systému a její automatické mazání
- Kvalitní generátor hesla
- Vyhledávání v databázi
- Velké množství pluginů
- Velká podpora jazyků

6.3.3.2 Bodové hodnocení

Tabulka 31: Hodnocení - KeePass

	Body x_i	Normované váhy v_i	Normované hodnocení
Operační systém	5	0.11	0.55
Jazyk dokumentace	3	0.03	0.09
Podpora k programu	2	0.19	0.38
Ovladatelnost	5	0.08	0.40
Aktualizace programu	5	0.22	1.10
Kvalita generátoru náhodného hesla	5	0.17	0.85
Integrace do webových prohlížečů	3	0.14	0.42

Automatické mazání schránky	5	0.06	0.30
Vážený Průměr			**4.21**

6.3.4 Firewall - OPNSense

OPNSense jako open source firewall nabízí většinu funkcí drahých komerčních firewallů a některé funkce i přidává. První verze OPNSense byla vydána v roce 2015 a vychází z pfSense, z něhož se stal odnožím (tzn. fork). Program se velice rychle začal rozvíjet, ale zároveň se snažil zachovat některé aspekty pfSense a m0n0wall. OPNSense klade důraz na bezpečnost a kvalitu kódu. Nabízí pravidelné týdenní menší aktualizace zaměřené na reakci na nové hrozby, včetně dvou větších aktualizací každý rok. Program je vyvíjen pod FreeBSD license. Nabízí také funkce jako traffic shaping, intrusion prevention system nebo virtual private network.

6.3.4.1 Funkční předpoklady

- Směrování provozu
- Dvoufázové ověřování
- Virtual Private Network
- Intrusion Prevention System
- Nastavení dynamické DNS
- DNS server a směrovač
- Podpora pluginů
- Záloha šifrovaného nastavení na Google Drive
- Sledování síťového provozu
- Podpora 802.1Q VLAN
- Vysoká dostupnost a ochrana při selhání hardware
- Stavový firewall
- Captive portal
- Moderní uživatelské rozhrání
- Caching proxy a blacklist (filtrování stránek)
- Možnost zálohování nastavení

6.3.4.2 Bodové hodnocení

Tabulka 32: Hodnocení - OPNSense

	Body x_i	Normované váhy v_i	Normované hodnocení
Jazyk dokumentace	3	0.02	0.06
Podpora k programu	5	0.13	0.65
Ovladatelnost	3	0.11	0.33
Aktualizace programu	5	0.16	0.80
Minimální frekvence CPU	5	0.07	0.35
Minimální velikost RAM	5	0.05	0.25
Traffic shaping (řízení provozu)	5	0.10	0.50
Intrusion Prevention System	5	0.18	0.90
Virtual Private Network	5	0.15	0.75
Podpora pluginů	5	0.04	0.20
Vážený průměr			**4.79**

6.3.5 Nástroje pro řízení oprávnění – Apache Syncope

Apache Syncope je open source software pro správu digitálních identit v podnikovém prostředí. Správa digitálních identit je správa uživatelských dat v systémech a v aplikacích pomocí podnikových procesů. Bere se ohled na uživatelské atributy, role, zdroje a nároky na přístup. Snaží se odpovědět na otázku: kdo má k čemu přístup, kdy, jak a také proč má přístup. Tyto systémy pro správu identit jsou hojně využívány u přidělování pravomocí zacházení s daty. Například povýšení v zaměstnání či při propuštění. První verze tohoto programu vyšla v roce 2012 s licencí Apache License verze 1. Program nyní funguje pod licencí Apache License verze 2.

6.3.5.1 Funkční předpoklady

- Moderní uživatelské prostředí
- Password policy
- Podpora pluginů
- Detailně popsaná dokumentace
- Se zvyšujícím se počtem identit roste potřebný výkon hardware
- Spolupráce s projektem Apache Maven
- Správa z jednoho administrátorského účtu
- Kvalitní komunitní podpora
- Správa služeb, tiskáren, složek, senzorů, pracovních stanic
- Možnost samostatné úpravy údajů uživateli

6.3.5.2 Bodové hodnocení

Tabulka 33: Hodnocení - Apache Syncope

	Body x_i	Normované váhy v_i	Normované hodnocení
Operační systém	5	0.11	0.55
Jazyk dokumentace	3	0.03	0.15
Podpora k programu	3	0.19	0.57
Ovladatelnost	4	0.08	0.32
Aktualizace programu	5	0.22	1.10
Minimální frekvence CPU	3	0.17	0.51
Minimální velikost RAM	4	0.14	0.56
Nastavení pravidel přihlášení	5	0.06	0.30
Vážený průměr			**4.06**

7 NÁVRH ZLEPŠENÍ BEZPEČNOSTI

Návrh zlepšení je proveden jako ukázka postupu a metod, které mohou firmy použít při výběru nového software

Mají-li firmy zájem zvýšit bezpečnost svých nejrůznějších systémů, stanic či databází, měly by sáhnout po kvalitních bezpečnostních programech. Mnohé firmy však k tomuto úkonu postrádají dostatečné finance a proto volí různé programy zdarma. Mohou si zvolit programy zdarma, které mají uzavřený kód, stačí-li jim to. Nebo si místo toho zvolí raději programy zdarma, které však mají otevřený kód. Nabízí se jim pak mnohem větší možnosti co se týče vlastního přizpůsobení a kontroly bezpečnosti programu. Mají-li tedy zájem o bezpečnost a kvalitní volbu programu, mohou tak učinit na doporučení jiných firem či věrohodných osob. Malé firmy a především ty začínající se však ve firemním prostředí nemusí natolik orientovat a proto správně provedená analýza bezpečného programu je velice důležitá. Proto se provádí u potenciálních programů hodnocení jejich funkcí a kvalit. Jak si firmy zhodnotí tyto programy je pouze na nich, je však doporučená vícekriteriální analýza, která je pro volbu software nejvhodnější, jelikož hodnotí jednotlivá kritéria s určitou důležitostí (váhami).

7.1 Metoda vícekriteriální analýzy

Před výběrem programu si firma musí stanovit, jaká kritéria jsou pro daný program a jeho danou kategorii, jež se snaží implementovat, důležitá či pro firmu zajimavá. Může se jednat o obecnější kritéria typu operační systém, hardwarové nároky, jak časté jsou aktualizace, složitost programu, grafické prostředí, nebo se také hodnotí specifická kritéria jako například aktualizace virové databáze, počet šifrovacích algoritmů, zda-li program automaticky generuje náhodná hesla či v případě firewallu, jestli podporuje traffic shaping nebo VPN.

Poté, co si firma stanoví kritéria, je potřeba těmto kritériím určit jejich váhy, tedy jejich důležitost v celkovém hodnocení. Metod ke stanovení vah je několik a každá může být více vhodná pro něco jiného. Mezi tyto metody patří:

- Metoda klasifikace kriterií do tříd
- Metoda pořadí
- Bodovací metoda – Metfesselova alokace
- Metoda hodnotící stupnice

- Metoda porovnání významu kriterií pomocí preferenčního pořadí
- Metoda párového srovnávání (Fullerova metoda) - použita v této práci
- Saatyho metoda
- Analyticko hierarchická metoda

Po vypočtení vah kritérií (nenormovaných či normovaných – záleží na dané metodě), si firma ohodnotí každé kritérium pomocí své předem stanovené stupnice. Přiřadí jim body a následně vypočte vážený průměr všech těchto bodů kritérií. Existují i jiné typy váženého průměru, jako například:

- Vážený geometrický průměr
- Vážený harmonický průměr

Tento průměr může být dále převeden na procentuální hodnotu, či může zůstat v jeho desetinné / setinné podobě. Firmy tak mohou tyto metody využít pro hodnocení velkého množství libovolných programů a vybrat jen ten nejvýhodnější. Záleží vždy na preferencích konkrétní firmy - co se pro jednu firmu může zdát kritické, pro druhou nemusí znamenat vůbec nic. Avšak bezpečnost a bezchybovost by vždy měla být prioritou. Použitá metoda se může podle daného typu software lišit. Hodnocení software si firmy mohou rozšířit například o výpis funkcí programu, výpis historie programu nebo jeho potenciální využití uvnitř firmy. Případně hodnocení může proběhnout pouze z důvodu poskytnutí informací o daném programu bez nějakého blízkého využití.

ZÁVĚR

Teoretická část práce se zabývala nejčastějšími typy škodlivého softwaru, se kterým se firmy i domácnosti mohou setkat. Jde například o phishing, ransomware, spyware, adware atd. Mimo jiné uvádí i typy šifrování, které se v praxi používají – asymetrické, symetrické včetně možnosti digitálního podpisu a certifikátu. Teorie pojednává také o typech dostupného software. Mezi ně se řadí klasický komerční software, včetně OEM softwaru, jenž bývá pořízen s koupeným zařízením, ale také i volně šiřitelný software, jako je Freeware, Shareware a především Open Source. Pojednává také o open source licencích užívaných u open source programů, zejména GNU GPL. Teorie také zahrnuje nově zavedené General Data Protection Regulation, které má za cíl poskytnout občanům ochranu a více práv při interakci s firmami, například požádat o vymazání údajů o nich vedených nebo přístup k nim (osobně a elektronicky) a zároveň udávat povinnosti a prověřovat firmy, zda-li svou práci vykonávají řádně a podle pravidel. Také bylo popsáno, jaký vliv má nově zavedené GDPR na firmy – co musí udělat aby byly v souladu s GDPR.

Úlohou praktické části bylo popsat aktuální stav bezpečnosti a oblasti použití open source nástrojů za cílem zvýšení bezpečnosti firem. Zmíněny byly nedávné kybernetické útoky NotPetya a WannaCry, ale také botnety Satori a Necurs, jež způsobily finanční škody po celém světě. Zastoupení různých open source nástrojů pro bezpečnost firem je velké a proto při analýze byl vybrán jeden program u každé z 5 kategorií. Jednalo se o antiviry, šifrování dat, správce hesel, firewally a identity managery. Tyto programy mají nulovou vstupní cenu, ale mnohé nabízejí také placenou podporu. Záleží také na tom, jaký operační systém firma využívá, jaký má k dispozici hardware a jak moc je zkušená v oblasti programování, jelikož si mohou tento open source software podle vlastní potřeby upravovat a ušetřit tak peníze za komerční podporu. Komerční podpora však dokáže firmám ušetřit čas a práci. Praktická část poskytuje firmám ukázku a návod k tomu, jaký postup mohou použít při vlastním výběru programů s různou důležitostí jednotlivých kritérií (vah). Vzhledem k analýze programů, záleží pouze na dané firmě, zda-li jsou schopny nevýhody tolerovat a tyto programy používat. Záleží také na jejich riziku ohrožení a jaký dopad by narušení mělo na firmu a především na schopnosti tyto programy správně zařadit do své infrastruktury.

SEZNAM POUŽITÉ LITERATURY

[1] JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů* [online]. Univerzita Tomáše Bati ve Zlíně: Vydáno elektronicky, 2013 [cit. 2018-03-07]. ISBN 978-80-7454-312-8. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/25821/Bezpecnost%20Informacnich%20systemu.pdf?sequence=1&isAllowed=n

[2] *Informační bezpečnost* [online]. [cit. 2018-03-07]. Dostupné z: http://www.cleverandsmart.cz/informacni-bezpecnost/

[3] *Kybernetická bezpečnost II.: Management kybernetické bezpečnosti* [online]. Praha, 2015 [cit.2018-03-07]. Dostupné z: https://www.institutpraha.cz/obj/obsah_fck/eGON2/WEB%20-%20materi%C3%A1ly/Pracovn%C3%AD%20se%C5%A1it%20-%202_%C4%8D%C3%A1st.pdf

[4] *Bezpečnostní politika* [online]. [cit. 2018-03-07]. Dostupné z: https://dk.upce.cz/bitstream/handle/10195/25862/text.pdf?sequence=1&isAllowed=y

[5] *Úvod do kryptografie: Asymetrické, symetrické šifry a hashování* [online]. [cit. 2018-03-07]. Dostupné z: http://www.earchivace.cz/technologie/uvod-do-kryptografie/

[6] *Solení hesel* [online]. [cit. 018-03-07]. Dostupné z: http://www.phpguru.cz/clanky/soleni-hesel

[7] *Digitální podpis* [online]. [cit. 2018-03-07]. Dostupné z: http://www.earchivace.cz/technologie/digitalni-podpis/

[8] *Internetový podvod* [online]. [cit. 2018-03-07]. Dostupné z: https://www.avast.com/cs-cz/c-scam

[9] *Adware* [online]. [cit. 2018-03-07]. Dostupné z: https://www.avast.com/cs-cz/c-adware

[10] *Adware ukázka* [online].[cit. 2018-03-08]. Dostupné z: https://www.howtoremoveit.info/adware-what-is-adware-virus-remover-and-adware-removal-tool/

[11] *Spyware* [online]. [cit. 2018-03-07]. Dostupné z: https://www.avast.com/cs-cz/cspyware

[12] *Rootkit* [online]. [cit. 2018-03-07]. Dostupné z: https://www.avast.com/cs-cz/c-rootkit

[13] *Ransomware* [online]. [cit. 2018-03-07]. Dostupné z: https://www.avast.com/cs-cz/c-ransomware

[14] *Keylogger* [online]. [cit. 2018-03-07]. Dostupné z: https://www.avast.com/cs-cz/c-keylogger

[15] ŠTĚDROŇ, Bohumír. Open Source software ve veřejné správě a soukromém sektoru. Praha: Grada, 2009. ISBN 978-80-247-3047-9. Str. 22

[16] *Copyright* [online]. [cit. 2018-03-07]. Dostupné z: https://www.patentsoffice.ie/en/Copyright/

[17] *Copyleft a Copyright* [online]. [cit. 2018-03-08]. Dostupné z: http://www.mamboreta.com/wp-content/uploads/2016/03/Copyright-Copyleft.jpg?x75391

[18] *Shareware, freeware, trialware – konečně jasno* [online]. [cit. 2018-03-07]. Dostupné z: https://www.interval.cz/clanky/shareware-freeware-trialware-konecne-jasno/

[19] *Commercial Software* [online]. [cit. 2018-03-07]. Dostupné z: https://techterms.com/definition/commercialsoftware

[20] ŠTĚDROŇ, Bohumír. Open Source software ve veřejné správě a soukromém sektoru. Praha: Grada, 2009. ISBN 978-80-247-3047-9. Str. 16

[21] ŠTĚDROŇ, Bohumír. Open Source software ve veřejné správě a soukromémsektoru. Praha: Grada, 2009. ISBN 978-80-247-3047-9. Str. 18-19

[22] *GNU-GPL* [online]. [cit. 2018-04-19]. Dostupné z: https://www.gnu.org/licenses/gpl-faq.html#GPLOtherThanSoftware

[23] *Pojem Lesser General Public License* [online]. [cit. 2018-03-07]. Dostupné z: http://www.tovarna.cz/cz/slovnik-pojmu/44-lgpl/

[24] *Co je to General Data Protection Regulation* [online]. [cit. 2018-03-07]. Dostupné z: https://www.gdpr.cz/gdpr/co-je-gdpr/

[25] *Osobní údaje* [online]. [cit. 2018-03-07]. Dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

[26] *Pověřenec pro ochranu osobních údajů* [online]. [cit. 2018-03-07]. Dostupné z: https://www.gdpr.cz/gdpr/dpo/

[27] *Důvody General Data Protection Regulation* [online]. [cit. 2018-03-07]. Dostupné z: https://www.gdpr.cz/gdpr/proc/

[28] *Jaké změny přinese General Data Protection Regulation* [online]. [cit. 2018-03-07]. Dostupné z: https://www.gdpr.cz/gdpr/zmeny/

[29] *Jaká práva General Data Protection Regulation dává občanům* [online]. [cit. 2018-03-07]. Dostupné z: https://www.gdpr.cz/gdpr/prava/

[30] *Jaké povinnosti údává General Data Protection Regulation firmám* [online]. [cit. 2018-03-07]. Dostupné z: https://www.gdpr.cz/gdpr/povinnosti/

[31] *Sankce za ignorování General Data Protection Regulation* [online]. [cit. 2018-03-07]. Dostupné z: https://www.gdpr.cz/gdpr/sankce/

[32] *Data Loss Prevention* [online]. [cit. 2018-03-07]. Dostupné z: https://www.ami.cz/reseni-a-sluzby/bezpecnost-dat/data-loss-prevention-1

[33] *Práva subjektu* [online]. [cit. 2018-03-07]. Dostupné z: https://www.novinkygdpr.cz/prava-subjektu-udaju-1-cast-vymaz-omezeni-zpracovani-vzneseni-namitky/

[34] *Souhlas* [online]. [cit. 2018-04-19]. Dostupné z: https://www.dpo4u.cz/l/souhlas/

[35] *GDPR a souhlas* [online]. [cit. 2018-04-19]. Dostupné z: http://www.gdpr-ochrana-osobnich-udaju.cz/zamestnavatel-a-gdpr-jak-se-pripravit/

[36] *Ochrana osobních údajů na síti* [online]. [cit. 2018-04-19]. Dostupné z: http://lovec-hlav.cz/blog/gdpr/

[37] *Přihlašování biometrickými údaji* [online]. [cit. 2018-22-04]. Dostupné z: http://finparada.cz/4820-Prihlasovani-biometrickymi-udaji-jake-ma-vyhody-oproti-klasickym-heslum.aspx

[38] *Cost of data breach study* [online]. [cit. 2018-03-05]. Dostupné z: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

[39] *Nové techniky hackerů* [online]. [cit. 2018-04-22]. Dostupné z: https://www.systemonline.cz/it-security/zneuzivani-sifrovane-komunikace-a-nove-techniky-hackeru.htm

[40] *Botnet Necurs* [online]. [cit. 2018-04-22]. Dostupné z: https://www.informationsecuritybuzz.com/study-research/necurs-botnet-rises-again-for-easter-check-point-research-shows/

[41] *Satori botnet* [online]. [cit. 2018-04-22]. Dostupné z: https://www.zive.cz/clanky/podivejte-se-jak-botnet-prave-ted-krade-lidem-kryptomeny/sc-3-a-191422/default.aspx

[42] *WannaCry* [online]. [cit. 2018-03-19]. Dostupné z: http://eurodenik.cz/zpravy/agresivni-virus-napadl-tisice-pocitacu-po-celem-svete-po-uzivatelich-pozaduje-penize

[43] *Identity Management* [online]. [cit. 2018-04-26]. Dostupné z: https://www.systemonline.cz/it-security/midpoint-open-source-reseni-pro-identity-management.htm

[44] *Not Petya* [online]. [cit. 2018-03-19]. Dostupné z: https://www.root.cz/clanky/postrehy-z-bezpecnosti-pouceni-z-malwaru-notpetya/

[45] *Používání autentizace* [online]. [cit. 2018-05-03]. Dostupné z: https://www.systemonline.cz/zpravy/studie-ibm-naznacuje-mozny-obrat-v-digitalni-laxnosti-z.htm

[46] *IBM news* [online]. [cit. 2018-05-04]. Dostupné z: https://www-03.ibm.com/press/us/en/pressrelease/53800.wss

[47] *Útok KRACK* [online]. [cit. 2018-05-04]. Dostupné z: https://www.s3c.cz/blog/posts/krack-wi-fi-jiz-neni-bezpecne

[48] *What is WPA3* [online]. [cit. 2018-05-04]. Dostupné z: https://www.guidingtech.com/wpa3-vs-wpa2/

[49] *Soulad firem s GDPR* [online]. [cit. 2018-07-19]. Dostupné z: http://www.create-it.cz/Blog/Stranky/GDPR.aspx

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

GDPR General Data Public Regulation

OEM Original Equipment Manufacture

DPIA Data Protection Impact Assesment

DPO Data Protection Officer

GPL General Public Licence

LGPL Lesser General Public Licence

DNS Domain Name Server

AES Advanced Encryption Standard

IDEA International Data Encryption Algorithm

RSA Rivest Shamir Adleman

DSA Digital Signature Algorithm

ECC Elliptic Curve Cryptography

MD Message-Digest

SHA Secure Hash Algorithm

CSIRP Computer Security Incident Response Plan

WPA Wi-Fi Protected Access

CNSA Commercial National Security Algorithm

KRACKKey Reinstallation Attack

SMB Server Message Block

RAM Random Access Memory

CPU Central Processing Unit

PDF Portable Document Format

RTF Rich Text Format

HTML HyperText Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK