

# Kybernetická bezpečnost malých firem

Nikola Krenželák

---

Bakalářská práce  
2018



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

# 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. Provedte 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 Škorníčková, 2017 [cit. 2017-11-20]. Dostupné z: <https://www.gdpr.cz/gdpr>.
2. **JASEK, 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](http://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](http://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. **ŠTĚDRŮ, 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:

**1. prosince 2017**

Termín odevzdání bakalářské práce:

**25. května 2018**

Ve Zlíně dne 14. prosince 2017



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.

Ve Zlíně, dne 20.5.2018

.....  
podpis diplomanta

## **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 vytvořen seznam (balík) vhodných programů pro posílení kybernetické bezpečnosti firem.

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

## **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: free and open source software, cybersecurity, general data protection regulation, fraudulent practices, 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

<b>ÚVOD.....</b>	<b>10</b>
<b>I TEORETICKÁ ČÁST .....</b>	<b>11</b>
<b>1 KYBERNETICKÁ BEZPEČNOST .....</b>	<b>12</b>
1.1 ZÁKLADNÍ POJMY KYBERNETICKÉ BEZPEČNOSTI .....	13
1.2 BEZPEČNOSTNÍ POLITIKA.....	14
1.3 KRYPTOGRAFIE V INFORMATICE.....	15
1.3.1 SYMETRICKÉ ŠIFROVÁNÍ.....	15
1.3.2 ASYMETRICKÉ ŠIFROVÁNÍ .....	16
1.3.3 HASHOVÁNÍ.....	17
1.3.4 DIGITÁLNÍ PODPIS.....	17
1.4 HROZBY A RIZIKA.....	18
1.4.1 JAK SE BRÁNIT .....	19
1.4.2 TYPY HROZEB.....	19
<b>2 FREE A OPEN SOURCE SOFTWARE.....</b>	<b>23</b>
2.1 COPYRIGHT A COPYLEFT.....	23
2.2 TYPY SOFTWARE.....	23
2.2.1 SHAREWARE .....	24
2.2.2 FREeware.....	24
2.2.3 PUBLIC DOMAIN.....	24
2.2.4 TRIALWARE .....	24
2.2.5 KOMERČNÍ PROGRAMY .....	24
2.2.6 SOFTWARE S LICENCÍ OEM.....	25
2.2.7 FREE A OPEN SOURCE SOFTWARE.....	25
2.3 OPEN SOURCE LICENCE .....	25
2.3.1 GNU GENERAL PUBLIC LICENCE .....	26
2.3.2 LESSER GENERAL PUBLIC LICENCE.....	26
<b>3 GENERAL DATA PROTECTION REGULATION.....</b>	<b>27</b>
3.1 CO SE POVAŽUJE ZA OSOBNÍ ÚDAJE .....	27
3.1.1 OBECNÉ OSOBNÍ ÚDAJE.....	27
3.1.2 CITLIVÉ OSOBNÍ ÚDAJE.....	27
3.2 POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ.....	28

3.3	DŮVODY ZAVEDENÍ .....	28
3.4	PŘÍNOS .....	29
3.5	PRÁVA OBČANŮ .....	29
3.6	POVINNOSTI FIREM .....	29
3.7	POKUTY ZA PORUŠENÍ .....	30
<b>4</b>	<b>SOUVISLOST MEZI GENERAL DATA PROTECTION REGULATION A KYBERNETICKOU BEZPEČNOSTÍ MALÝCH FIREM.....</b>	<b>31</b>
4.1	PREVENCE ÚNIKU DAT .....	31
4.1.1	DATA LOSS PREVENTION.....	31
4.2	PRÁVO NA VÝMAZ.....	31
4.3	SOUHLAS O ZPRACOVÁNÍ ÚDAJŮ .....	32
4.3.1	SVOBODNÝ A JEDNOZNAČNÝ .....	32
4.3.2	INFORMOVANÝ A KONKRÉTNÍ.....	32
4.4	ZVEŘEJŇOVÁNÍ FOTOGRAFIÍ A VIDEÍ NA INTERNETU.....	33
<b>II</b>	<b>PRAKTICKÁ ČÁST .....</b>	<b>34</b>
<b>5</b>	<b>SOUČASNÝ STAV BEZPEČNOSTI INFORMAČNÍCH TECHNOLOGIÍ .....</b>	<b>35</b>
5.1	PŘIPRAVENOST NA KYBERNETICKÝ ÚTOK.....	35
5.2	VYUŽITÍ BIOMETRIE.....	35
5.3	STUDIE NÁKLADŮ PŘI ÚNIKU DAT .....	36
5.4	ZAVEDENÍ WPA3 JAKO DŮSLEDEK ÚTOKU KRACK .....	37
5.5	VÝZNAMNÉ HROZBY .....	37
5.5.1	BOTNETY .....	37
5.5.2	WANNACRY .....	38
5.5.3	NOTPETYA .....	38
<b>6</b>	<b>ANALÝZA DOSTUPNÝCH OPEN SOURCE NÁSTROJŮ .....</b>	<b>39</b>
6.1	ZKOUMANÉ KATEGORIE .....	39
6.2	PŘEDSTAVENÍ KATEGORIÍ SOFTWARE.....	39
6.2.1	ANTIVIROVÉ PROGRAMY .....	39
6.2.2	ŠIFROVÁNÍ DAT.....	40
6.2.3	FIREWALL .....	40
6.2.4	NÁSTROJE PRO SPRÁVU HESEL .....	41
6.2.5	NÁSTROJE PRO ŘÍZENÍ OPRAVNĚNÍ.....	42
6.3	HODNOCENÍ SOFTWARE .....	42



6.3.1	ANTIVIROVÉ PROGRAMY .....	43
6.3.2	ŠIFROVÁNÍ DAT.....	43
6.3.3	FIREWALL.....	44
6.3.4	NÁSTROJE PRO SPRÁVU HESEL.....	45
6.3.5	NÁSTROJE PRO ŘÍZENÍ OPRÁVNĚNÍ.....	46
6.4	SWOT ANALÝZA.....	47
6.4.1	ANTIVIROVÉ PROGRAMY .....	47
6.4.2	ŠIFROVÁNÍ DAT.....	48
6.4.3	FIREWALL.....	48
6.4.4	NÁSTROJE PRO SPRÁVU HESEL.....	49
6.4.5	NÁSTROJE PRO ŘÍZENÍ OPRÁVNĚNÍ.....	50
<b>7</b>	<b>NÁVRH ZLEPŠENÍ BEZPEČNOSTI .....</b>	<b>51</b>
7.1	CLAMAV .....	51
7.2	VERACRYPT.....	52
7.3	OPNSENSE .....	52
7.4	KEEPASS .....	53
7.5	MIDPOINT .....	54
	<b>ZÁVĚR .....</b>	<b>55</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>56</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK .....</b>	<b>60</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>61</b>
	<b>SEZNAM TABULEK.....</b>	<b>62</b>

## ÚVOD

Každý člověk má nějaké potřeby. Ať už jde o potřeby biologické (spánek, potrava, vylučování), tak i potřeby psychické (osobní rozvoj, pocit lásky, vědění). Existuje ale i další nezbytná potřeba, a tou je pocit bezpečí. Co nám dává pocit bezpečí? Dává nám především klid na duši. Máme-li střechu nad hlavou, nemusíme se obávat, že nám bude zima, nebo nám někdo ublíží, zatímco spíme. Máme-li peníze, můžeme si obstarat potravu, platit nájem, dopravu do zaměstnání a spoustu dalších potřeb, nezbytných pro naše spokojené bytí. Jde tedy o bezpečnost. Ta se také vztahuje k majetku. Vlastníme-li 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. S 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, nebo vyzrazení firemního tajemství apod.

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. Práce je zakončena sestavením balíku, jež obsahuje open source programy pro kybernetickou bezpečnost.

## TEORETICKÁ ČÁST

## 1 KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost je v dnešní době nepostradatelnou součástí nejrůznějších právnických a fyzických osob a států. 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 přijdou o veškerá nezalohovaná 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]

### **O jaké systémy se může jednat, aplikujeme-li bezpečnost do systému?**

- a) **Promiskuitní** – Jde o systémy, které nemají žádné zákazy. V praxi se tenhle typ systému nedoporučuje.
- b) **Paranoidní** – V systému je vše zakázáno. Používá se jen tam, kde nám nezbyvá nic jiného, u věcí, které se těžce udržují.
- c) **Přísný** – Povolení se udává na základě whitelistů (bílý list), kde jsou uvedeny výjimky, ke kterým můžeme přistupovat.
- d) **Povolný** – Povolení se udává na základě blacklistů (černý list), kde jsou uvedeny výjimky, ke kterým přistupovat nemůžeme.

[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 vzniku 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.**

Slovo Kryptografie se skládá z 2 řeckých slov – kryptós (skrytý) a gráphein (text). Kryptografie je věda o šifrování či utajení významu zpráv. Toto se provádí převodem nějakého otevřeného textu na text zašifrovaný s použitím šifrovacího klíče. Tento text se nedá bez použití nějakého dešifrovacího klíče rozluštit. Zašifrování dat 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. Výhodou tohoto šifrování je právě ten fakt, že celý proces probíhá velice rychle z důvodu právě sdíleného klíče. [5]

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 soukromý a až poté klíč veřejný, ovšem lze vytvořit dodatkový veřejný klíč. 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. Oproti symetrickému šifrování je však tento způsob bezpečnější, jelikož je nutné vlastnit privátní klíč z klíčového páru, za cenu pomalejšího šifrování. Nejpoužívanějším algoritmem 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 nějaký 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. Hashování se může používat u zpráv (e-mail), souborů, ale také u rychlého vyhledávání dat z databází. 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 priznání daně z příjmů a dokumenty související s úřady, včetně internetové banky. Pro vytvoření podpisu se používá asymetrické šifrování a hashovací funkce. [7]

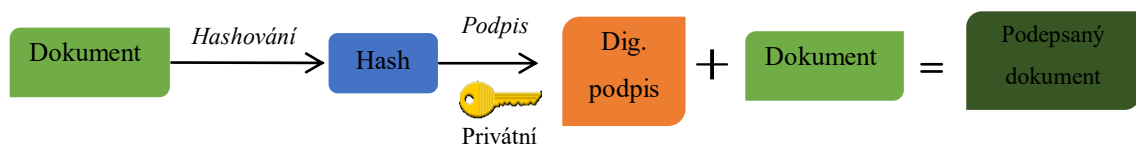
Digitální podpis musí pro jeho spolehlivé užívání disponovat několika vlastnostmi.

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 podepsané osoby

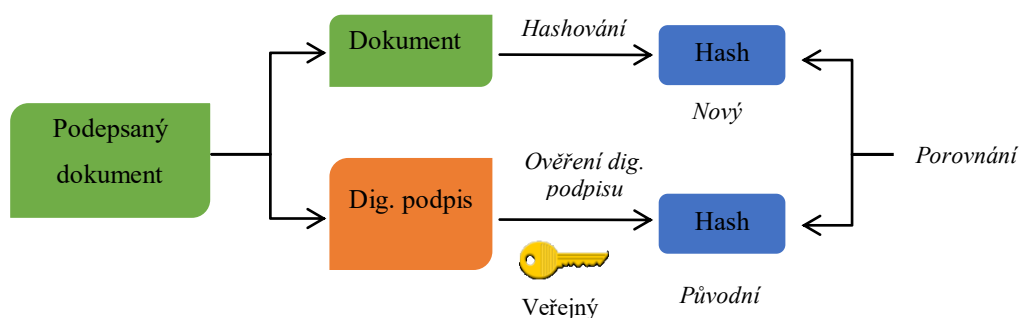
[7]

Při vytvoření digitálního podpisu musíme nejprve vytvořit hash a tento hash poté privátním klíčem 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 viry, Rootkity, Spyware, Keyloggers a další.

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

#### **1.4.1 Jak se bránit**

V první řadě je potřeba ke všemu přistupovat 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 neodoblokují 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 jiné textové formě. Keylogger se v počítači může vyskytnout, 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 pravé), objeví se

hlášení o chybě a údaje jsou odeslány útočnickovi. 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 nabourá na DNS (domain name server) dané stránky a kohokoliv kdo tuto stránku navštíví, automaticky přesměruje na stránku podvodnou.

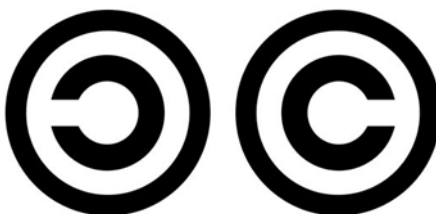
## 2 FREE A OPEN SOURCE SOFTWARE

Software, nebo-li program, je součástí 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 pomoci 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 zpoplatňovat za účelem vlastního výdělků. 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, přijdeme o licenci. Jedná se například o operační systém Microsoft Windows jako součást koupě nového počítače. Programy s touto licencí nesmíme přenášet na jiné 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 kdokoli může tento program stáhnout zdarma. Má právo zdrojový kód studovat a provádět potřebné změny. Musí být vydáván pod stejnou licenci, s jakou byl obdržán. 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 kdokoli 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 programem. 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, operujícímu 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 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, u kterých díky kombinace s jinými informacemi lze identifikovat osobu či osoby. 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 vzniknou 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]

Pověřenec je zvolen, je-li hlavní činnost orgánů veřejné moci a firem, rozsáhlé sledování občanů, zpracování citlivých údajů a údajů u rozsudků trestních činností. Pověřenci mají znalosti o GDPR, právu, podnikání, vnitřní organizaci správce a také o ochraně údajů. Jeden pověřenec může pracovat pro více firem s podobnou organizační strukturou najednou, ale musí plnit svou činnost co nejlépe. Je vázán tajemstvím a musí být dostupný po fyzické či telefonické stránce občanovi. Pověřenci zpracovávají informace například o pacientech nemocnic, telefonických a internetových datech, datech bank a pojišťoven, lokalitách zákazníků a osobních údajích získaných vyhledáváním z důvodu reklam. Dodržování GDPR firmou není odpovědností pověřence. 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. Dalším důvodem je zamezení shromažďování informací o osobách nejrůznějšími institucemi, jako například tajné služby států mimo evropský prostor. 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, například že používají pouze data nezbytně nutná pro práci. 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. Stane-li se, že se ve firmě vyskytne problém s bezpečností, je potřeba nyní tuto událost nahlásit, neboť existuje nebezpečí úniku osobních údajů. Tuto událost musí firma nahlásit Úřadu pro ochranu osobních údajů do 72 hodin od nalezení problému a někdy 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. Znat 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 firmu 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 provádějí 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. Záznamy obsahují: 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 maximálně 20 milionů eur nebo 4 % z celkového ročního obrátu firmy. 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. 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).

### 4.1 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.

#### 4.1.1 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]

### 4.2 Právo na výmaz

Právo na výmaz je právo, kdy může osoba (subjekt), o níž se vedou údaje, požádat o jejich smazání ze systému a ze záloh. 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 námítky subjektu údajů proti zpracování, převažuje-li zájem subjektu nad zájmem správce, nejsou-li údaje zpracovávány podle GDPR. Údaje se musí smazat, prikazuje-li to právní předpis Evropské unie. [33]

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

### **4.3 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]

#### **4.3.1 Svobodný a jednoznačný**

Subjekt musí mít možnost rozhodnout se, zda-li souhlas poskytne. Souhlas zpracování osobních údajů nesmí být podmínkou 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]

#### **4.3.2 Informovaný a konkrétní**

Při poskytování souhlasu musí být subjekt dostatečně seznámen s informacemi 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]

#### **4.4 Zveřejňování fotografií a videí na internetu**

Ať už se jedná o fotky či videa z veřejných akcí, nebo chce-li zaměstnavatel použít fotku v rámci 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 (v rámci činnosti firmy), souhlas není vyžadován. Stejně tak není vyžadován při použití ve firemních systémech nebo při monitorování (v rámci 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 síti 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 Přípravenost 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 pomoci 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 účtům je používání 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 klasickým 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 společnostech a zjistilo se, že průměrná celková cena napáchaných škod z důvodu úniku dat za rok 2017 se vyčíslnila 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 bude k dispozici ve třetím nebo čtvrtém čtvrtletí roku 2018. [48]

## 5.5 Významné hrozby

Za poslední rok otřáslí hackeři kybernetickou bezpečností po celém světě. Jednalo se o viry, ransomware, ale také šíření spamů pomocí botnetů. Většina webových stránek je v dnešní době šifrovaná, přesto jsou ale útočníci schopni tuto ochranu obejít. Dosahují tím právě využitím SSL certifikátů, které jde velice snadno získat. K tomu jsou navíc schopni zaútočit na veřejně dostupné a známé online služby jakou jsou dokumenty Google.

### 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 změnil 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

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. Nakonec bude provedena SWOT analýza dané kategorie software.

### 6.2 Představení kategorií software

Pro potřebu bakalářské práce a zachování přiměřené délky bylo vybráno 5 typů software určené pro bezpečnost. Těmito typy jsou: Antivirové programy, Šifrování dat, Firewall, Programy pro správu hesel, Nástroje pro řízení oprávnění. Software je hodnocen na základě kritérií dané kategorie software. Hodnocení probíhá přidělením bodů na stupnici 1 (výborná), 2 (chvalitebná), 3 (střední), 4 (horší), 5 (nedostatečná). Po přidělení těchto hodnot danému programu, je vytvořen průměr a nakonec jsou programy dané kategorie porovnány mezi sebou. Veškeré hodnocení probíhá na základě vlastního pozorování a výzkumu.

#### 6.2.1 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, včetně ty se systémem Windows. Dostupnost Free a Open source antiviru je velice limitovaná, byl tedy vybrán ClamAV a ClamWin.

##### 6.2.1.1 Hodnocená kritéria

Kritéria hodnocená u antivirových programů jsou následující:

- 1) Podpora operačních systémů – udává, jak moc rozšířený je program mezi operačními systémy

- 2) Zdraví projektu – aktivní vývoj, aktualizace a bug fixy
- 3) Stav dokumentace – je-li program dostatečně popsán a poskytnuty návody k práci s programem.
- 4) Instalace – složitost uvedení programu do provozu
- 5) Složitost ovládání – práce s uživatelským prostředím programu a konfigurace programu
- 6) Podpora projektu – dostupnost komunitní podpory (fóra, mailing list) a podpory komerční
- 7) Kvalita integrace – značí, na jaké úrovni je integrace programu s jiným programem či formáty souborů

## 6.2.2 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. Mezi software tohoto typu patřil TrueCrypt, jehož vývoj byl ovšem zastaven a místo něho se objevil VeraCrypt a AxCrypt.

### 6.2.2.1 Hodnocená kritéria

Kritéria hodnocená u programů pro šifrování dat jsou následující:

- 1) Podpora operačních systémů – udává, jak moc rozšířený je program mezi operačními systémy
- 2) Zdraví projektu – aktivní vývoj, aktualizace a bug fixy
- 3) Stav dokumentace – je-li program dostatečně popsán a poskytnuty návody k práci s programem.
- 4) Instalace – složitost uvedení programu do provozu
- 5) Složitost ovládání – práce s uživatelským prostředím programu a konfigurace programu
- 6) Podpora projektu – dostupnost komunitní podpory (fóra, mailing list) a podpory komerční

## 6.2.3 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 open source firewally patří například OPNsense nebo pfSense.

#### **6.2.3.1 Hodnocená kritéria**

Kritéria hodnocená u firewallů jsou následující:

- 1) Zdraví projektu – aktivní vývoj, aktualizace a bug fixy
- 2) Stav dokumentace – je-li program dostatečně popsán a poskytnuty návody k práci s programem.
- 3) Instalace – složitost uvedení programu do provozu
- 4) Složitost ovládání – práce s uživatelským prostředím programu a konfigurace programu
- 5) Podpora projektu – dostupnost komunitní podpory (fóra, mailing list) a podpory komerční

#### **6.2.4 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. Mezi ně patří KeePass a PasswordSafe.

#### **6.2.4.1 Hodnocená kritéria**

Kritéria hodnocená u nástrojů pro správu hesel jsou následující:

- 1) Podpora operačních systémů – udává, jak moc rozšířený je program mezi operačními systémy
- 2) Zdraví projektu – aktivní vývoj, aktualizace a bug fixy
- 3) Stav dokumentace – je-li program dostatečně popsán a poskytnuty návody k práci s programem.
- 4) Instalace – složitost uvedení programu do provozu

- 5) Složitost ovládání – práce s uživatelským prostředím programu a konfigurace programu
- 6) Podpora projektu – dostupnost komunitní podpory (fóra, mailing list) a podpory komerční
- 7) Kvalita integrace – značí, na jaké úrovni je integrace programu s jiným programem či formáty souborů

### 6.2.5 Nástroje pro řízení oprávnění

Vede-li firma zaměstnance, potýká se neustále 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. Jedná se o programy jako: Apache Syncope, midPoint. [43]

#### 6.2.5.1 Hodnocená kritéria

Kritéria hodnocená u nástrojů pro řízení oprávnění jsou následující:

- 1) Zdraví projektu – aktivní vývoj, aktualizace a bug fixy
- 2) Stav dokumentace – je-li program dostatečně popsán a poskytnuty návody k pracování s programem.
- 3) Instalace – složitost uvedení programu do provozu
- 4) Složitost ovládání – práce s uživatelským prostředím programu a konfigurace programu
- 5) Podpora projektu – dostupnost komunitní podpory (fóra, mailing list) a podpory komerční

### 6.3 Hodnocení software

Zde proběhne srovnání jednotlivých programů v dané kategorii. Každé kritérium je bodově ohodnoceno, body jsou poté sečteny a vyděleny počtem daných kritérií pro danou kapitolu, aby se vytvořil aritmetický průměr bodů daného programu. Zároveň jsou také slovně popsány výsledky hodnocení daných kategorií.

K bodovému ohodnocení byla použita metoda geometrického průměru daného podle vzorce:  $G(x_1, x_2, \dots, x_n) = \sqrt[n]{x_1 * x_2 \dots x_n}$ , kdy  $n$  je nejvyšší počet kritérií a hodnoty  $x$  jsou body konkrétních kritérií. Výsledky jsou zaokrouhleny na dvě desetinná místa.

### 6.3.1 Antivirové programy

Program ClamAV zvítězil nad ClamWin. Je totiž určen pro systémy Linux, OS X, Windows, Solaris atd. Dokumentace je pouze v angličtině, avšak je rozsáhlá. To přispívá snazší instalaci a práci s programem (práce s příkazovým řádkem). Avšak díky jeho rozšíření a možné integraci s jiným software existuje velká komunita včetně mailing listu, což přispívá k vývoji a celkovému zdraví projektu. ClamWin je naopak jednodušší k instalaci a užívání, neboť byl navržen speciálně pro Windows, tím pádem i jeho komunita online je limitovaná pouze na uživatele Windows, avšak také využívá mailing listu a integrace například s Microsoft Outlook.

*Tabulka 1: Antivirové programy*

	ClamAV	ClamWin
Podpora operačních systémů	1	4
Zdraví projektu	2	3
Stav dokumentace	1	4
Instalace	3	1
Složitost ovládání	3	1
Podpora projektu	2	3
Kvalita integrace	1	3
Průměr	1.67	2.38

### 6.3.2 Šifrování dat

VeraCrypt zvítězil nad AxCryptem převážně z důvodu obsáhlosti dokumentace a pravidelnými aktualizacemi. AxCrypt sice má dokumentaci na oficiálním webu, ale není tak rozsáhlá jako u VeraCryptu. Ten umožňuje používání na operačních systémech

Windows, dále na Windows serverech, OS X, Linux a FreeBSD. Oproti tomu AxCrypt v současné době umožňuje použití pouze na Windows a OS X, ale rozdílem je využití na mobilních zařízeních (Android a iOS). Instalace a užívání obou programů probíhá přes jednoduché uživatelské rozhraní. Oba programy mají přibližně stejnou aktivitu komunit, ovšem fórum je ve prospěch VeraCryptu, komerční podpora pak AxCryptu.

Tabulka 2: Šifrování dat

	Veracrypt	AxCrypt
Podpora operačních systémů	1	2
Zdraví projektu	1	2
Stav dokumentace	1	3
Instalace	1	1
Složitost ovládní	1	1
Podpora projektu	2	2
Průměr	1.12	1.70

### 6.3.3 Firewall

Oba dva firewally jsou velmi populární, v tom se odráží jejich častá aktualizace a využívání. Dokumentace poskytuje dostatek informací k obsluze programu, avšak pro instalaci je potřeba menší práce s příkazovým řádkem a nastavování poté probíhá v přehledném uživatelském rozhraní, ovšem odborná znalost sítí je vyžadována. Pokyny pro instalaci a práci s programem se dají vyčíst z právě přiložené dokumentace. Oba programy mají skvělou podporu. Jelikož tyto firewally dosáhly stejného bodového ohodnocení, záleží jen na preferenci konkrétních firem.

Tabulka 3: Firewall

	OPNsense	pfSense
Zdraví projektu	1	1
Stav dokumentace	1	1
Instalace	3	3
Složitost ovládání	3	3
Podpora projektu	1	1
Průměr	1.55	1.55

#### 6.3.4 Nástroje pro správu hesel

Oba dva programy podporují velké množství operačních systémů. Patří mezi ně Windows, OS X a Linux, existují ale i porty na mobilní zařízení. Nové verze obou programů vycházejí přibližně co 3 měsíce, vzhledem k jejich nekomplexnosti však velmi časté aktualizace nejsou vyžadovány. Vítězem je však KeePass. Dokumentace je u KeePassu v mnohem lepším stavu než u Password Safe. Instalace programů je jednoduchá a intuitivní, s tím rozdílem, že pro každý systém je postup instalace trochu jiný. Oba dva programy jsou jednoduché na obsluhu a dá se využít poskytnutá dokumentace. KeePass má vysokou aktivitu komunitního fóra, ale neposkytuje komerční podporu ani mailing list, naopak tomu tak je u Password Safe, ovšem ten zase zaostává v aktivitě na fóru.

Tabulka 4: Nástroje pro správu hesel

	KeePass	PasswordSafe
Podpora operačních systémů	1	1
Zdraví projektu	2	2
Stav dokumentace	1	4
Instalace	1	1
Složitost ovládání	1	1
Podpora projektu	2	2
Kvalita integrace	1	4
Průměr	1.22	1.81

### 6.3.5 Nástroje pro řízení oprávnění

Apache Syncope a midPoint jsou známé a spolehlivé programy pro spravování identit a řízení práv. Nové verze vycházejí přibližně co 3 měsíce. Dokumentace přiložená k software je dostupná z webové stránky projektů a je obsahově velice rozsáhlá s nejrůznějšími návody k práci. Oba dva programy nabízejí komerční podporu a mailing list, ovšem dostupnost fóra je horší. U Apache Syncope se dá využít Internet Relay Chat.

Tabulka 5: Nástroje pro řízení oprávnění

	Apache Syncope	midPoint
Zdraví projektu	1	1
Stav dokumentace	1	1
Instalace	2	2
Složitost ovládání	2	2
Podpora projektu	2	2
Průměr	1.52	1.52

## 6.4 SWOT analýza

Provedená SWOT analýza popisuje silné, slabé stránky a příležitosti, hrozby jednotlivých kategorií software co se týče jejich open source variant.

### 6.4.1 Antivirové programy

Tabulka 6: SWOT analýza – Antiviry

Silné stránky	Slabé stránky
Velké množství podpory operačních systémů Využití zdrojového kódu ke zlepšení Cena	Zranitelnost kódu Složitost
Příležitosti	Hrozby
Vznik nových open source antivirů Zlepšení bezpečnosti	Zneužití kódu Zastínění ne-open source antiviry

Největší výhoda open source antivirových programů je ta, že jsou uživatelé schopni upravovat program podle své potřeby. Dokáží se podílet na bezpečnostních úpravách vytváření portů na jiné systémy či zařízení. Ovšem s otevřeností kódu přichází i riziko jeho zneužití. Získají-li open source antiviry větší popularitu a zajistí-li bezpečnost, lze očekávat více zástupců v tomto odvětví. Mnoho lidí však dává přednost kvalitním a ověřeným komerčním antivirům z důvodu jejich bezpečnosti.

### 6.4.2 Šifrování dat

Tabulka 7: SWOT analýza – Šifrování dat

Sílné stránky	Slabé stránky
Různé typy šifrování Cena	Zranitelnost kódu
Příležitosti	Hrozby
Zvýšení popularity nejen u firem Využití nových typů šifrování	Prolomení šifrování Zavedení backdoor

Šifrování dat by mělo být nezbytnou součástí nejen firem, ale i lidí, kteří spravují větší objem citlivých dat. Grafické uživatelské rozhraní, cena a různé typy šifrování hrají roli v atraktivnosti těchto programů. Jako u každého open source software je však zranitelnost kódu tou největším problémem. S neustálým vývojem technologií se vyvíjí i nové způsoby šifrování, kterým se tyto programy mohou adaptovat. Důležitost šifrování však nesouvisí jen s daty firem, ale i fyzických osob. Je potřeba dát si pozor na výskyt backdooru, který může na jednu stranu pomoci s obnovením zašifrovaných dat v případě ztráty klíče, ale také umožňuje neoprávněným osobám dostat se k datům.

### 6.4.3 Firewall

Tabulka 8: SWOT analýza – Firewall

Sílné stránky	Slabé stránky
Přitažlivost z důvodu ceny Podpora pluginů	Přístupnost zdrojového kódu Složitost konfigurace
Příležitosti	Hrozby
Zdokonalování funkcí a ochrany Tvorba nových pluginů	Vznik nových typů útoků



Nevýhodou komerčních firewallů je jejich velká cena. Proto je open-source firewall mnohem jednodušší pořídit. Avšak komerční firewall má mnohem lepší komerční podporu. Open-source firewall se však může díky lidem zdokonalovat a snižovat hranici mezi komerčním a open-source firewallem.

#### 6.4.4 Nástroje pro správu hesel

Tabulka 9: SWOT analýza – Nástroje pro správu hesel

Sílné stránky	Slabé stránky
Hesla uložená offline Kvalitní generování hesla	Jediný bod prolomení
Příležitosti	Hrozby
Zlepšení zabezpečení Nové způsoby generování hesla Nové způsoby šifrování	Zneužití zdrojového kódu Brute force útoky

Programy pro správu hesel jsou dobré v tom, že dokáží skladovat veškerá hesla na jednom místě. To však znamená, pokud dojde k prolomení ochrany (např. vlivem zneužití dostupnosti kódu nebo pomocí brute force útoku), tak útočník získá přístup ke všem heslům obsažených vně programu. Přesto jsou však tyto programy schopné, neboť veškerá hesla jsou ukládána offline a je možné programy dále rozvíjet.

#### 6.4.5 Nástroje pro řízení oprávnění

Tabulka 10: SWOT analýza - Nástroje pro řízení oprávnění

<b>Sílné stránky</b>	<b>Slabé stránky</b>
Cena za provoz	Administrátorský účet
<b>Příležitosti</b>	<b>Hrozby</b>
Zlepšení funkcí	Odcizení účtu administrátora
Zlepšení uživatelského prostředí	Rozvíjející se útoky
Zlepšení bezpečnosti	

Open source software určený pro řízení oprávnění a spravování identit je pro malé a střední firmy výborným nástrojem, neboť je zdarma a také umožňuje si program upravovat podle sebe. Se zdokonalováním virů a jiných kybernetických hrozeb však nastává problém, když je narušen účet administrátora. Stane-li se tak, jsou pak v ohroženy veškeré subjekty a role, který systém spravuje.

## 7 NÁVRH ZLEPŠENÍ BEZPEČNOSTI

V této části bude sestaven bezpečnostní balík z programů uvedených v otázce 6. Bude zvolen jeden (vítězný) program z každé kategorie. Programy budou popsány a budou uvedeny jejich výhody a nevýhody a proč by měla firma zvolit právě daný program pro zlepšení bezpečnosti. Kapitola slouží k poskytnutí informací o vítězných programech, které může firma zavést za účelem zvýšení bezpečnosti.

### 7.1 ClamAV

Z kategorie antivirů je zvolen ClamAV. Jedná se asi o nejznámější open-source antivirus. Je určen pro operační systémy Windows, OS X, Linux, Solaris a FreeBSD. Dá se využít pro kontrolu webových stránek, e-mailů a ochranu počítače před škodlivým softwarem v reálném čase. ClamAV si automaticky aktualizovává virovou databázi pomocí nástroje „freshclam“ a k práci se používá příkazový řádek. Grafické uživatelské prostředí se však dá použít, nainstaluje-li se ClamTK, což je rozšíření, které umožní práci s antivirem i osobám, které nejsou zblhlé s příkazovým řádkem. ClamAV poskytuje jak výše zmínovanou automatickou aktualizaci databáze, tak také podporu e-mailových souborů a archivačních formátů jako je RAR, Tar, Zip, Bzip2, dále také PDF, RTF, HTML a kancelářské soubory Microsoft Office a MacOffice. Existuje mnoho programů třetích stran, které fungují s ClamAV, například linuxový e-mailový klient Kmail. ClamAV je přitažlivý pro firmy hlavně z důvodu ceny, ale také velkým množstvím vlastního přizpůsobení.

*Tabulka 11: Výhody / nevýhody ClamAV*

Výhody	Nevýhody
Zdarma	Nutná konfigurace
Velké množství přizpůsobení	Neexistuje komerční podpora
Aktivní a velice populární open-source antivir	Dokumentace pouze v angličtině
Podpora nejrůznějších souborů a formátů	

## 7.2 Veracrypt

Nástroj pro šifrování, který vychází z TrueCryptu, jehož vývoj se zastavil v roce 2014. Je určen pro operační systémy Windows, OS X, FreeBSD a Linux. Slouží pro šifrování disku a k tomuto účelu využívá šifrovací algoritmy AES, Twofish, Serpent, Kuznyechik a Camellia. Jako hashovací algoritmus se využívá Sha-256 a 512, Whirlpool a RIPEMD-160. K práci není potřeba příkazový řádek, je tedy vhodný i pro méně znalé uživatele. Existuje možnost překladů programu třetích stran do různých jazyků, ale pouze pro systémy Windows. Šifrování probíhá rychleji díky využití více jader procesoru - paralelní. Firmy může zajímat jednak z důvodu ceny, tak také z důvodu popření šifrování, budou-li chtít autority vymáhat data. Nebo využívají-li TrueCrypt, mohou se zašifrovanými daty pracovat i u Veracryptu, musí si však dávat pozor na ztrátu hesla, neboť neobsahuje možnost backdooru.

*Tabulka 12: Výhody / nevýhody VeraCrypt*

Výhody	Nevýhody
Zdarma	Neexistuje komerční podpora
Velké množství algoritmů	Dokumentace pouze v angličtině
Komunikace s daty TrueCryptu	Nelze obnovit ztracené heslo
Hardwarová akcelerace a paralelnost	

## 7.3 OPNsense

Důvod zvolení OPNsense oproti pfSense je ten, že je novější a přímo z něho vychází. Podporuje 32 a 64 bitové procesory a k zavedení je vyžadováno mít k dispozici alespoň 1 Gigabyte místa na disku, 512 Megabajtů RAM a 500 Megahertzový procesor. Co se týče RAM a procesoru, je však doporučeno dvakrát tolik. Program také vychází z operačního systému FreeBSD. Pro instalaci a konfiguraci jsou vyžadovány znalosti o sítích. OPNsense je lákavý hlavně díky jeho grafickému uživatelskému rozhraní přístupného přes internetový prohlížeč, možnosti vlastního rozšíření pomocí pluginů a také ceně oproti komerčním firewallům. Kromě činností firewallu nabízí řízení provozu (traffic shaping) a Virtual Private Network. Firmy si mohou vybrat mezi 3 typy placené komerční podpory nebo využít bezplatného mailing listu a komunitního fóra.

Tabulka 13: Výhody / nevýhody OPNsense

Výhody	Nevýhody
Zdarma	Dokumentace pouze v angličtině
Množství pluginů	Nutná dobrá znalost sítí pro konfiguraci
Dobrá komerční/komunitní podpora	
Funguje nejen jako firewall	

## 7.4 KeePass

KeePass je velice přehledný program pro správu hesel, který je přeložen do 49 jazyků. Je podporován systémy Windows, Linux, OS X, Android, iOS a BlackBerry. Neposkytuje komerční podporu, avšak komunita je aktivní a samotný program není složitý k užívání díky jeho přehledné dokumentaci a vzhledu. KeePass disponuje velkým počtem pluginů a integrace s webovými prohlížeči Chrome, Firefox a Safari. Využívá se šifrovacího algoritmu AES a ChaCha20 s možností přidání dalších pomocí pluginů a hashovací funkce SHA-256. Firmy mohou po tomto programu sáhnout, hledají-li přehledný a nezáťažový program pro šifrování dat a zároveň kvalitní generátor hesel. Nabízí totiž vytvoření náhodného libovolně dlouhého hesla s obsaženými: Velkými, malými písmeny, mezery, speciální znaky, závorky, čísla, podtržítka, mínus a případně sérii vlastních znaků. Skvělou funkcí je také automatické mazání schránky při kopírování hesel.

Tabulka 14: Výhody / nevýhody KeePass

Výhody	Nevýhody
Zdarma	Neexistuje komerční podpora
Integrace s webovými prohlížeči	Žádná obnova ztraceného hlavního hesla
Jednoduché ovládání	
Nutnost pamatování jediného hesla	
Přeložen do 49 jazyků	

## 7.5 midPoint

Český 7 let starý identity manager, který shromažďuje a spravuje databáze s uloženými údaji o osobách, organizačních jednotkách, spravuje role, skupiny a přiděluje jim určitá práva. Umí ale také spravovat zařízení a služby. Díky tomu že je open-source dovoluje lidem provádět rozsáhlé úpravy a pomáhat tak s vývojem, včetně úpravy grafického uživatelského rozhraní. Práce s programem se provádí přes uživatelské rozhraní s modulárním vzhledem programu prostřednictvím internetového prohlížeče. MidPoint nabízí 4 stupně komerční podpory, vhodné při vývoji nebo s řešením problémů vzniklých při práci s programem. Nabízí také možnosti tréninkových kurzů a certifikátů pro identity management a práci s midPointem. Dokumentace se nachází na wiki midPointu, kde popisuje funkce a nejrůznější návody midPointu včetně názorných ukázek. K dispozici je také kniha (zdarma dostupná na oficiální stránce), kde je popsáno, jak nejlépe využít midPoint pro vytvoření vhodného řešení správy identity. Bývá také překládán do jiných jazyků, je zcela přeložen do češtiny, angličtiny a polštiny.

*Tabulka 15: Výhody / nevýhody midPoint*

Výhody	Nevýhody
Zdarma	Absence komunitního fóra
Práce v prohlížeči, přehledný design	Dokumentace pouze v angličtině
Bohatá dokumentace	
Několik typů komerční podpory včetně tréninkových kurzů	

## 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 férově a podle pravidel. Firmy nesmí začít zpracovávat údaje bez poskytnutého souhlasu osoby, o níž údaje vypovídají. Také je v hodně případech potřeba získat souhlas k uveřejnění fotky nebo videa dané osoby.

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 velká a proto při analýze byly vybrány 2 programy pro každou z 5 kategorií. Jednalo se o antiviry, šifrování dat, firewally, správce hesel a identity managery. Tyto programy mají nulovou vstupní cenu, ale mnohé nabízejí placenou podporu. Záleží také na tom, jaký operační systém firma využívá 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. Pro každou kategorii byla provedena SWOT analýza pro vyzdvihnutí jejich silných, slabých stránek, příležitosti a hrozeb. Na základě vypsání výhod a nevýhod vítězných 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-%20\\_%C4%8D%C3%A1st.pdf](https://www.institutpraha.cz/obj/obsah_fck/eGON2/WEB%20-%20materi%C3%A1ly/Pracovn%C3%AD%20se%C5%A1it%20-%20_%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. 2018-03-07]. 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] ŠTĚDRŮŇ, 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] ŠTĚDRŮŇ, Bohumír. *Open Source software ve veřejné správě a soukromém sektoru*. Praha: Grada, 2009. ISBN 978-80-247-3047-9. Str. 16
- [21] ŠTĚDRŮŇ, Bohumír. *Open Source software ve veřejné správě a soukromém sektoru*. 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/slovník-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 údajů dá 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.novinygdpr.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-vede-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/>

**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
IT	Information Technology
CSIRP	Computer Security Incident Response Plan
WPA	Wi-Fi Protected Access
CNSA	Commercial National Security Algorithm
KRACK	Key Reinstallation Attack
SSL	Secure Sockets Layer
SMB	Server Message Block
RAM	Random Access Memory
PDF	Portable Document Format
RTF	Rich Text Format
HTML	HyperText Markup Language

**SEZNAM OBRÁZKŮ**

<i>OBR. 1 SYMETRICKÉ ŠIFROVÁNÍ [5]</i> .....	16
<i>OBR. 2 ASYMETRICKÉ ŠIFROVÁNÍ [5]</i> .....	16
<i>OBR. 3 DIGITÁLNÍ PODPIS [7]</i> .....	18
<i>OBR. 4 OVĚŘENÍ DIGITÁLNÍHO PODPISU [7]</i> .....	18
<i>OBR. 5 ADWARE [10]</i> .....	20
<i>OBR. 6: LOGO COPYLEFT (VLEVO) A COPYRIGHT [17]</i> .....	23

**SEZNAM TABULEK**

<i>TABULKA 1: ANTIUIROVÉ PROGRAMY</i> .....	43
<i>TABULKA 2: ŠIFROVÁNÍ DAT</i> .....	44
<i>TABULKA 3: FIREWALL</i> .....	45
<i>TABULKA 4: NÁSTROJE PRO SPRÁVU HESEL</i> .....	46
<i>TABULKA 5: NÁSTROJE PRO ŘÍZENÍ OPRÁVNĚNÍ</i> .....	46
<i>TABULKA 6: SWOT ANALÝZA – ANTIUIRY</i> .....	47
<i>TABULKA 7: SWOT ANALÝZA – ŠIFROVÁNÍ DAT</i> .....	48
<i>TABULKA 8: SWOT ANALÝZA – FIREWALL</i> .....	48
<i>TABULKA 9: SWOT ANALÝZA – NÁSTROJE PRO SPRÁVU HESEL</i> .....	49
<i>TABULKA 10: SWOT ANALÝZA - NÁSTROJE PRO ŘÍZENÍ OPRÁVNĚNÍ</i> .....	50
<i>TABULKA 11: VÝHODY / NEVÝHODY CLAMAV</i> .....	51
<i>TABULKA 12: VÝHODY / NEVÝHODY VERACRYPT</i> .....	52
<i>TABULKA 13: VÝHODY / NEVÝHODY OPNSENSE</i> .....	53
<i>TABULKA 14: VÝHODY / NEVÝHODY KEEPASS</i> .....	53
<i>TABULKA 15: VÝHODY / NEVÝHODY MIDPOINT</i> .....	54