Bezpečnost informačních technologií s využitím free a open source nástrojů

Raul Cekota

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Raul Cekota**
Osobní číslo:	**A15004**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnost informačních technologií s využitím free a open source nástrojů**
Téma anglicky:	**Information Technologies Security with the Use of Free and Open Source Tools**

Zásady pro vypracování:

1. **Seznamte se s problematikou bezpečnosti informačních technologií.**
2. **Vysvětlete pojmy Free a Open Source software.**
3. **Proveďte analýzu současného stavu v oblasti bezpečnosti informačních technologií.**
4. **Analyzujte Free a Open Source nástroje v oblasti bezpečnosti a jejich možné uplatnění v podmínkách malých a středních podniků.**
5. **Na základě těchto analýz vytvořte modelový příklad a sestavte základní balíčky Free a Open Source nástrojů pro malé a střední podniky.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 978-80-7454-312-8.**
2. **KAFKA, Milan. Význam ochrany a bezpečnosti IS-IT pro konkurenceschopnost podniku. Zlín: Univerzita Tomáše Bati ve Zlíně, 2011, 36 s. Teze disertační práce. ISBN 978-80-7454-036-3.**
3. **ŠTĚDROŇ, Bohumír. Open Source software ve veřejné správě a soukromém sektoru. Praha: Grada, 2009, 124 s. Průvodce. ISBN 978-80-247-3047-9.**
4. **ŠÍR, Ivo. Možnosti využití technologií Open Source a Free Software v malých a středních podnicích. (online). Vysoká škola ekonomická v Praze, 2004 Dostupné z: www.cssi.cz/cssi/system/files/all/SI_04_3_sir.pdf.**
5. **ŠTEC, Zdeněk. Open source software a jeho využití ve výuce tvorby webových stránek v sekundárním vzdělávání. (online). Olomouc, 2013. Dostupné z: https://theses.cz/id/6jbqak/00174154-374415625.pdf.**
6. **MACÁK, Petr. Kritéria výběru software pro malé a středně velké společnosti. Systémová integrace, 2011, ročník 18, číslo 1, str. 121-133, ISSN 1210-9479.**

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

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 7. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

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 diplomové/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 20.5.2019

Raul Cekota, RAUL CEKOTA
podpis diplomanta

ABSTRAKT

Bakalářská práce je zaměřena na bezpečnost informačních technologií s využitím free a open source nástrojů. Konkrétně téma směřuje do oblasti bezpečnosti informačních technologií v malých a středních podnicích, které mají často tuto sféru nedostatečně chráněnou. V práci jsou vysvětleny základní pojmy spojené s touto problematikou a způsob, jakým by podniky měly tuto bezpečnost zajistit. Uvedeny jsou také nejčastější hrozby, kterým musí podniky čelit a opatření proti nim. Na základě těchto znalostí jsou vybrány a následně analyzovány free a open source bezpečnostní nástroje. Z těchto nástrojů jsou vytvořeny bezpečnostní balíčky, které slouží ke zvýšení bezpečnosti informačních technologií v jednotlivých podnicích.

Klíčová slova: bezpečnost informačních technologií, free a open source nástroje, bezpečnostní nástroje, bezpečnost informačních systémů, informační bezpečnost, hrozby

ABSTRACT

The bachelor thesis is focused on information technology security using free and open source tools. Specifically, the topic is focused on the area of information technology security in small and medium-sized enterprises, which often lack this protection. The thesis explains the basic terms related to this subject and the way in which enterprices should ensure this security. Mentioned are the most common threats that enterprices facing and defense against them. Based on that, free and open source security tools are selected and analyzed. From these tools, are created security packages to improve the security of information technology in individual enterprices.

Keywords: information technology security, free and open source tools, security tools, information system security, information security, threats

Tímto bych chtěl poděkovat vedoucímu bakalářské práce Ing. Lukáši Králíkovi za odbornou konzultaci a čas strávený nad touto prací. Dále chci poděkovat své přítelkyni a celé své rodině za psychickou podporu, kterou mi dali, a bez které bych se při psaní práce neobešel.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 BEZPEČNOST V OBLASTI INFORMAČNÍCH TECHNOLOGIÍ **11**
1.1 Základní pojmy související s bezpečností informačních technologií 11
1.2 Informační bezpečnost, zranitelné místo, hrozba, útok a útočník 13
2 INFORMAČNÍ BEZPEČNOST V PODNIKU **14**
2.1 Bezpečnostní politika 14
2.2 Standardy IT bezpečnosti 15
2.3 Bezpečnostní funkce informačních technologií v organizacích 16
3 BEZPEČNOSTNÍ MECHANISMY **17**
3.1 Základní bezpečnostní mechanismy 17
3.1.1 Hesla a osobní identifikační čísla 17
3.1.2 Magnetické karty 17
3.1.3 Čipové karty 18
3.2 Kryptografické bezpečnostní mechanismy 18
3.2.1 Elektronický podpis 19
3.2.2 Hash Algoritmy 20
3.2.3 Certifikáty 20
4 HROZBY **21**
4.1 Viry 21
4.2 Trojské koně 21
4.3 Červi 21
4.4 Spyware 22
4.5 Adware 22
4.6 Hoax 22
4.7 Phishing a Pharming 22
4.8 Exploit a zero-day attack 23
4.9 APT Hrozby 23
5 OPATŘENÍ PROTI HROZBÁM **24**
5.1 Antivirové programy 24
5.2 Firewall 25
5.3 Zálohovací programy 25
5.4 Systémy IDS a IPS 26
5.5 Technologie SIEM 26
6 FREE A OPEN SOURCE SOFTWARE **27**
6.1 Free software 27
6.2 Open Source software 28
6.3 Rozdíl mezi free a open Source software 28
II PRAKTICKÁ ČÁST **30**
7 SOUČASNÝ STAV V OBLASTI BEZPEČNOSTI INFORMAČNÍCH

TECHNOLOGIÍ **31**
7.1 UMĚLÁ INTELIGENCE 31
7.2 KONTROLA ŠIFROVANÝCH DAT 32
7.3 OCHRANA MOBILNÍCH ZAŘÍZENÍ 32
7.4 POTŘEBA ZVÝŠENÍ BEZPEČNOSTI CLOUDU 32
7.5 REGULACE 33
8 ANALÝZA FREE A OPEN SOURCE NÁSTROJŮ V OBLASTI BEZPEČNOSTI INFORMAČNÍCH TECHNOLOGIÍ **34**
8.1 ANTIVIROVÉ PROGRAMY 38
8.1.1 Windows Defender 38
8.1.2 ClamAV - open source 39
8.1.3 MoonSecure Antivirus – open source 40
8.2 FIREWALL 41
8.2.1 Windows firewall 41
8.2.2 Tinywall Firewall – free software 42
8.2.3 Private Winten – open source 43
8.3 ZÁLOHOVACÍ PROGRAMY 44
8.3.1 Duplicati 2.0 – free software 44
8.3.2 Areca Backup – open source 45
8.3.3 Zálohování v systému Windows 46
8.4 ŠIFROVACÍ PROGRAMY 47
8.4.1 BitLocker 47
8.4.2 VeraCrypt – open source 48
8.4.3 Gpg4win – open source 49
8.5 SPRÁVCE HESEL 50
8.5.1 KeePass – open source 50
8.5.2 Padlock – open source 51
8.6 AKTUALIZAČNÍ SPRÁVCI SOFTWARU 52
8.6.1 SUMo – free software 52
8.7 ANALYZÉR BEZPEČNOSTI OPERAČNÍCH SYSTÉMŮ MICROSOFT WINDOWS 53
9 ZÁKLADNÍ BALÍČKY FREE A OPEN SOURCE NÁSTROJŮ PRO MALÉ A STŘEDNÍ PODNIKY **54**
9.1 ZÁKLADNÍ BALÍČKY FREE A OPEN SOURCE NÁSTROJŮ PRO OPERAČNÍ SYSTÉM WINDOWS 54
ZÁVĚR **58**
SEZNAM POUŽITÉ LITERATURY **59**
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK **62**
SEZNAM OBRÁZKŮ **63**
SEZNAM TABULEK **64**
SEZNAM PŘÍLOH **65**

ÚVOD

Již od vzniku prvních podniků se lidé snažili o co největší zefektivnění a urychlení procesů, které uvnitř i vně každého podniku probíhají. Největší přínos však v posledních letech přineslo postupné zdigitalizováni, které umožnilo využít potenciál výpočetní techniky a informačních technologií. Podniky začaly využívat výhod digitalizace jako faktor pro větší konkurenceschopnost a ekonomickou úspěšnost. Není tedy divu, že v současné době je infrastruktura podniků z větší části tvořena právě informačními technologiemi.

Zatímco přijetí digitalizace představuje velké množství výhod, skrývá i hrozbu v podobě zneužití a narušení bezpečnosti informačních technologií. S tímto problémem se nejčastěji potýkají podniky malé a střední velikosti, které mají nízkou úroveň zabezpečení svých informačních technologií. Často k tomu dochází z důvodu redukce nákladů či malých finančních zdrojů. Na základě toho se bakalářská práce zaměří na možnost řešit zabezpečení informačních technologií pomocí volně dostupných nástrojů.

Teoretická část bakalářské práce má za cíl objasnit, co vlastně pojem bezpečnost v rámci informačních technologií představuje. Ze začátku budou vysvětleny základní pojmy, které se budou v práci vyskytovat, seznámíme se se způsobem, jakým podniky přistupují k bezpečnosti informačních technologií včetně souvislosti s právními předpisy a technickými normami. Dále bude následovat kapitola, která se zaměří na popis nejčastějších hrozeb, jimž musí podniky čelit. Na závěr první poloviny bakalářské práce si rozebereme opatření proti těmto hrozbám a prozkoumáme typy nástrojů, které budeme v praktické části používat.

Praktická část bakalářské práce bude rozdělena na dvě základní kapitoly. První kapitola bude obsahovat popis bezpečnostních nástrojů. Každý tento nástroj bude na základě vlastního pozorování zhodnocen pomocí kriteriální analýzy a porovnán s ostatními nástroji stejného určení. Srovnání a analýzy nástrojů nám poskytnou potřebné informace k tomu, abychom mohli vytvořit základní balíčky volně dostupných bezpečnostních nástrojů pro malé a střední podniky a naplnit tak hlavní cíl této práce.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST V OBLASTI INFORMAČNÍCH TECHNOLOGIÍ

Pojem bezpečnost se dá vyložit několika různými způsoby, avšak téměř vždy platí pravidlo, že s narůstající úrovní bezpečnosti klesá pocit ohrožení. S pojmem bezpečnost se můžeme setkat v mnoha odvětvích a oborech po celém světě. Cílený objekt zabezpečení můžeme rozdělit do třech základních skupin:

- fyzické zdraví a život samotný,
- majetek, a to jak hmotný, tak i nehmotný,
- znalosti, data a informace.

Data a znalosti získané na základě informací tvoří specifickou skupinu, která je náročnější na zpracování, a často nebývá běžné dostupná většímu počtu subjektů např. veřejnosti. Tyto informace jsou pro svého majitele důležité a mají významnou hodnotu, proto bývají často zabezpečené a jejich únik by mohl jejich majiteli způsobit konkurenční nebo jakoukoliv jinou újmu. [1, s. 10]

Podnik, který zpracovává svá data pomocí informačních technologií je každodenně ohrožen jejich zneužitím jak z finančních, tak i z osobních důvodů. A proto je na bezpečnost informačních technologií kladen stejný důraz jako na jejich cenu, spolehlivost a funkčnost. Bezpečnost je součástí mnoha odvětví, ani informační technologie nejsou výjimkou. [1, s. 10]

1.1 Základní pojmy související s bezpečností informačních technologií

V oblasti bezpečnosti informačních technologií se používají některé specifické pojmy, které je pro pochopitelnost problematiky nutné objasnit.

- **Důvěrnost** – důvěrné informace jsou určené pouze autorizovaným osobám. Za tímto účelem jsou vytvořeny speciální řídící mechanismy, které řídí přístupy k nim.
- **Integrita** – pokud jsou důvěrné informace modifikovány (upravovány), je u nich vyžadováno, aby i po těchto modifikacích byly úplné, a práce s nimi nebyla nijak narušena.
- **Dostupnost** – je, kromě integrity, další vlastností, která se u informací vyžaduje. Dostupnost umožňuje přistupovat k informacím v momentě jejich potřeby.

Z výše uvedených vlastností lze vyvodit základní aspekty bezpečnosti informačních technologií, které spočívají v možnosti přistupovat k neporušeným informacím, a to pouze osobám tomu určeným v daný časový okamžik. [7, s. 8-10]

- **Riziko** – představuje pravděpodobnost ztráty nebo škody spojené s informačními technologiemi.
- **Zranitelnost** – slabá místa v bezpečnostním systému.
- **Napadení** – je jednání, které může zapříčinit ztrátu nebo škodu.
- **Kontrola** – reprezentuje opatření, která pomáhají předejít napadení.

Potenciální ztráty nebo škody na bezpečnostním systému mohou být způsobeny následovně:

- **Přerušením** – nejčastěji je přerušení důvodem nedostupnosti či nepoužitelnosti některé ze systémových částí, známe jako Denial of Service (DoS) útoky.
- **Sledováním** – zjištění přístupu autorizované osoby k systémové části za pomocí sledování.
- **Modifikací** – v systému dojde k manipulaci s daty, které jsou následně nepoužitelné. Modifikace ve většině případu není možné odhalit.
- **Falzifikací** – účelná manipulace s daty nebo zavedení falešných dat, které slouží pro odhalení neautorizované osoby.

Bezpečnost informačních technologiích obsahuje tři důležité aspekty, a to:

- **Utajení** – spočívá v zabezpečení přístupu a manipulací s daty za pomocí ověření identity, nejčastěji pomocí zašifrovaného klíče nebo přístupového hesla.
- **Integrita** – modifikace systémových částí může být prováděna pouze ověřenými subjekty. Totožnost subjektu bývá ověřována pomocí digitálního podpisu.
- **Použitelnost** – použití jakékoliv systémové části je podmíněno autorizací subjektu.

Důležitým parametrem v oblasti oprávněných (autorizovaných) přístupů je autentizace.

- **Autentizace** – neboli ověření identity uživatele se provádí pomocí dříve získaných údajů o konkrétním uživateli.

Bezpečnost informačních technologií je rozsáhlé zabezpečení programových, technických prostředků a dat v informačních technologiích, přičemž každá z těchto částí by měla být zabezpečena stejnou prioritou. [7, s. 8-10]

1.2 Informační bezpečnost, zranitelné místo, hrozba, útok a útočník

Bezpečnost v prostředí, kde se vyskytují výpočetní a komunikační systémy zpracovávající informace, se označuje jako informační bezpečnost. [9, s. 10]

Informační bezpečnost je soubor komplexních úkolů, které zajišťují ochranu informací v každém bodě jejich výskytu, tj. ochrana organizačních, programových a technologických části informačního systému, ve kterém jsou informace přenášeny, zpracovávány a ukládány. [9, s. 10]

Přenášení informace mezi dvěma výpočetními systémy nebo technologiemi se pak nazývá komunikační bezpečnost. Ta kromě samotného digitálního přenosu informace řeší i otázku fyzické bezpečnosti, která se týká hrozeb ze strany lidského faktoru, personalistiky a také přírodních jevů. [9, s. 10]

Zranitelné místo je slabina v informačním systému, která může být díky útoku využita ke způsobení škod nebo ztrát. Zranitelná místa jsou důsledkem nedbalosti v návrhu nebo implementaci bezpečnostního systému, a chyb v bezpečnostní analýze. [10, s. 13-17]

Hrozba představuje pro systém příležitost využití zranitelného místa k útoku na něj. [10, s. 13-17]

Útok, rovněž nazýván jako bezpečnostní incident, znamená úmyslné využití zranitelného místa ke způsobení ztrát nebo škod na prostředcích, které mají pro organizaci určitou hodnotu (aktiva). Mezi nejdůležitější formu ochrany vůči pasivním útokům patří prevence. Úplná ochrana však ve většině případech možná není. Ochrana hlavně před aktivními formami útoků závisí na včasné detekci útoků a následné obnově činnosti. Další možnou ochranou je rovněž prevence. Pokud k útoku dojde je důležité, aby si organizace vzala ponaučení ze zjištěných skutečností, a poznatky použije při zlepšování ochran proti útočníkům. [10, s. 13-17]

Útočníkem může být v organizaci útočník vnější nebo vnitřní. Mezi typické příklady útoku patří např. prohlížení systému souborů, prohlížení pamětí, zrušení přístupu ke službám autorizovaným uživatelům, zahlcení počítače emailovými dopisy, vydávání se za jiného autorizovaného uživatele. [10, s. 13-17]

2 INFORMAČNÍ BEZPEČNOST V PODNIKU

Přístup a pohled na bezpečnost informací v podnicích je ovlivněn především charakterem daného podniku, ale převážně je největší důraz kladen na ochranu podnikových business procesů. Takový bezpečnostní informační systém pak musí být navržen s ohledem na plynulost činností v podniku, a nesmí podnik ovlivnit v negativním slova smyslu tak, aby byl narušen správný chod aplikací a s tím spojená i kvalita poskytovaných služeb. S tím je spojeno i zajištění požadavků na bezpečnostní systém podniku ve vztahu k aktuálnosti, dostupnosti a důvěryhodnosti procesů a funkcí. [9, s. 10]

2.1 Bezpečnostní politika

Každý z dílčích komponentů patřící do skupiny informačních technologií organizace se liší jak svým typem, tak i stupněm citlivosti vůči neoprávněnému přístupu. Vzhledem k odlišnosti jednotlivých komponent, a z ekonomických důvodů není možné vytvořit zabezpečení, které by chránilo všechny informační technologie stejným způsobem. Míru zabezpečení a bezpečnostní strukturu pro každý komponent řeší tzv. bezpečnostní politika. Při vytváření bezpečnostního systémů je třeba vzít v potaz hodnotu zabezpečovaných dat, míru zranitelnosti, ceny případných poruch a oprav, a stanovit hrozby a rizika. Dále je pak nutné počítat s dostupnými protiopatřeními, jejich efektivitou a cenou, a cenou za jejich instalaci. [7, s. 11-12]

Bezpečnostní politika je jejich nedílnou součástí informačních systémů. Je popsána jako soubor norem, pravidel a způsobů, která definuje formát informací, jejich způsob ochrany, přenos citlivých informací a dalších systémových částí. Skládá se z fyzického, technického, administrativního, etického, personálního, ekologického, právního a kybernetického přístupu k datům a jejich použití v informačním systému. Bezpečnostní politika je zaváděna z důvodu snížení počtu výskytů možných zneužití informačního systému. V případě organizace mluvíme o tzv. kompromitaci organizace. Bezpečnostní politika organizace pak stanovuje pravidla, zavádí opatření a zahrnuje normy, které je potřeba dodržovat, aby byla zajištěna dostupnost dat a jejich důvěrnost. [7, s. 11-12]

Bezpečnostní politika informačního systému bývá ve formátu dokumentu, který je přijat organizací, jehož cílem je zabezpečení informačního systému. V organizaci je pak veden jako vnitřně-organizační norma. Tento dokument je volně přístupný a je vhodné, aby byl stručný, srozumitelný a pokryl všechny možné otázky v rámci bezpečnosti informačního systému

organizace. Bezpečnostní politika organizace často bývá řešena v souladu se světoznámými standardy (ITSEC, ITEM, TC SEC, ISO/TEC TR 13335, atd.). [7, s. 11-12]

2.2 Standardy IT bezpečnosti

Jako reakce na hrozby, které hrozí informačním systémům, byly vytvořeny postupy, které měly možným útokům zabránit. V historii byla bezpečnost prováděna pouze za pomocí dílčích řešení konkrétních situací, ale postupem času, kdy útoků přibývalo, začaly vznikat normy a metodiky sloužící k ochraně informačních systémů skládající se s certifikovaných ISO norem, které řeší bezpečnost informačních systémů již v navrhované fázi. [10, s. 89-93]

Bezpečnostní normy obsahují obecné bezpečnostní a aplikační protokoly, různé bezpečnostní techniky, které jsou zahrnuty v mezinárodních normách vyvíjené v ISO, IEC, ITU, IEEE. [10, s. 89-93]

Takových norem a právních předpisů existuje celá řada, ale při realizaci a provozu informačních systémů je nutné zavést a dodržovat alespoň některé z nich. Například autoři studijního textu Bezpečnost ICT a ochrana dat, Kodl a Smejkal (2018, s. 12-13) uvádí:

Právní předpisy

- *Nařízení Evropského parlamentu a Rady (EU) 910/2014 o elektronické identifikaci a službách, která zajišťuje důvěryhodnost elektronicky provedených transakcí.*
- *Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů (General Data Protection Regulation.*
- *Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.*
- *Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.*
- *Zákon č. 480/2004 Sb., o některých službách informační společnosti.*
- *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti.*
- *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.*

Technické normy

- *ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.*

- *ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací.*
- *ČSN ISO/IEC 27005:2009 – Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*.

2.3 Bezpečnostní funkce informačních technologií v organizacích

Prvním krokem k zabezpečení informačních technologií v organizaci je vytyčení bezpečnostních cílů a způsob jejich dosažení. Tyto bezpečnostní cíle vytvářejí minoritní přínosy k bezpečnosti, kterou informační technologie mají z hlediska jejich důvěrnosti, integrity a dostupnosti. Pro dosažení cílů se v organizacích používají bezpečnostní funkce rovněž nazývané jako bezpečnostní opatření. Ke stanovení bezpečnostních cílů je třeba znát zranitelná místa organizace a vědět, jak se dají tato zranitelná místa využít. Dále pak i možné formy útoků, potenciální útočníky, ale i uživatele, které svým jednáním mohou způsobit neúmyslnou škodu, pravděpodobnost útoku a výše jeho případné škody a způsob, jak se proti takovým útokům bránit.

Bezpečnostní funkce mohou mít fyzický, logický nebo administrativní charakter, tzn. mohou představovat mechanismy jako jsou hardwarová zařízení, programy, administrativní akce.

Bezpečnostní funkce mohou být rozděleny dle okamžiku uplatnění na:

- **Preventivní** – činnosti, které odstraňují zranitelná místa nebo zvyšují bezpečnostní uvědomění.
- **Heuristické** – činnosti, které snižují riziko vytvářené nějakou hrozbou.
- **Detekční a opravné** – činnosti, které minimalizují účinek útoku ve třech fázích – nalezení, oprava, zotavení. [10, s. 19-20]

3 BEZPEČNOSTNÍ MECHANISMY

Bezpečnostní mechanismy tvoří nástroje, které slouží k implementaci bezpečnostních funkcí. Na základě jejich určení mohou být fyzického, logického, administrativního i technického typu. Při zavádění bezpečnostních funkcí se mnohdy kombinují tak, aby byla dosažena co možná nejpřesnější, nejúčinnější a z ekonomického hlediska nejvýhodnější varianta. [10, s. 57]

3.1 Základní bezpečnostní mechanismy

Mnoho bezpečnostních mechanismů může být použito s užitím několika bezpečnostních funkcí současně. Běžně se v organizacích používá kryptografický algoritmus pro zabezpečení bezpečnostní funkce identifikace a autentizace (vstup do budovy), jako i bezpečnostní funkci integrity (šifrování přenosu informací) a zároveň bezpečnostní funkci důvěrnosti (šifrování přístupu k datům). Podobně jde využít např. magnetickou kartu, díky které je uživatel za pomocí přístupových identifikačních údajů ověřen, a je mu umožněn přístup do bankomatu, ale i do zabezpečených prostor organizace. Takových variací je mnoho, avšak základní bezpečnostní mechanismy zůstávají stejné. [10, s. 57-59]

3.1.1 Hesla a osobní identifikační čísla

Hesla a identifikační čísla bývají v organizacích přidělována subjektům (např. zaměstnancům). Tato hesla a identifikační čísla mají svá opatření, které např. zakazují uchovávání hesel jinde než v paměti subjektu, stavba a délka hesla musí splňovat bezpečnostní náležitosti. Pro ověření správnosti zadaného hesla a následnou autentizaci subjektu, musí být v počítači dostupný vzor hesla pro jeho kontrolu. Takové řešení ale představuje bezpečnostní problém, proto se hesla neuchovávají jako seznamy, nýbrž jako výsledky jejich zpracování. [10, s. 57-59]

3.1.2 Magnetické karty

Magnetické karty patří hned za hesly k jedněm z nejpoužívanějších bezpečnostních mechanismů (použití např. v bankomatech). Paměť, kterou karty poskytují, bývá většinou v řádech stovek bitů, a obsaženy jsou nejčastěji informace o držiteli, číslo bankovního účtu nebo identifikační údaje. K ověření identity uživatele karty je použit nějaký typ aplikačního osobního identifikačního čísla, v případě online systémů je totožnost ověřena centrálně. [10, s. 57-59]

3.1.3 Čipové karty

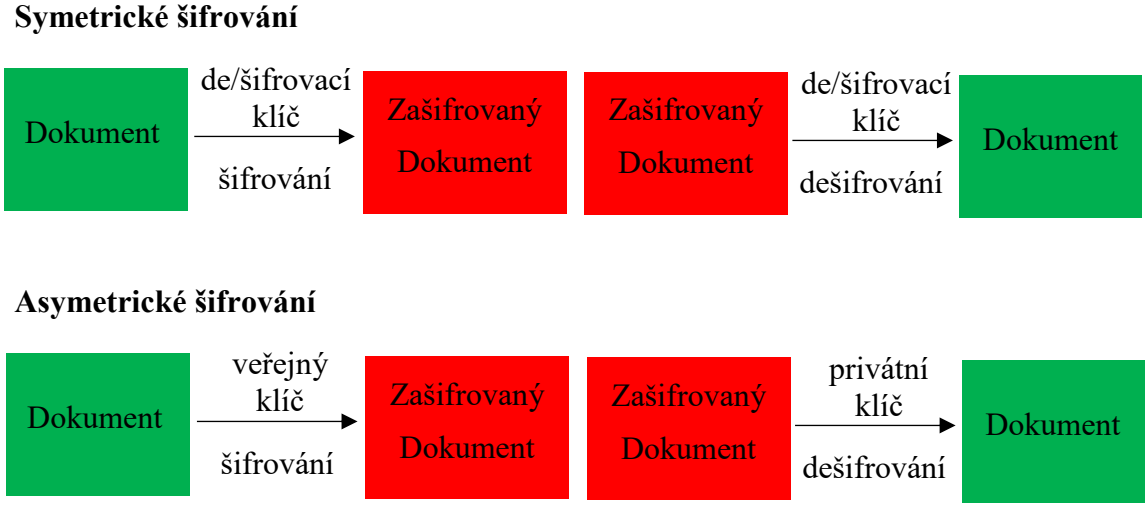
S potřebou vyššího paměťového místa a výpočetního výkonu bylo zapotřebí identifikační karty přizpůsobit, proto vznikly tzv. čipové karty (smart cards). Čipové karty je, narozdíl od magnetických karet, velmi těžké zfalšovat, protože jejich vnitřní uspořádání je výrobci přísně utajeno. [10, s. 57-59]

3.2 Kryptografické bezpečnostní mechanismy

Kryptografie neboli šifrování je v organizacích proces, který slouží k zabezpečení zpráv. Šifrování je proces, ve kterém dochází k převodu zprávy z původního otevřeného textu do podoby, kdy je tato zpráva čitelná pouze díky určitě specifické znalosti a nedochází tak ke stavu, kdy může neoprávněná osoba zprávu jednoduše přečíst. Šifrování se v organizacích rovněž používá jako ochrana proti neoprávněnému přístupu administrátorů systému, kteří k určitým datům nemají přístup povolen. [1, s. 20,21]

Převádění zašifrovaných dat zpět do původní podoby je proces, který se nazývá dešifrování. Oba procesy ke své činnosti potřebují tajnou informaci, která je zašifrovaná určitou metodou, která používá tzv. klíč. Klíč si lze představit jako např. heslo k počítači či klíč od auta. Klíč tedy umožňuje přístup k datům pouze oprávněným osobám. [1, s. 20,21]

Šifrovat lze data jakéhokoliv typu: textové soubory, multimediální soubory, databázové soubory, programy atd. Zašifrovaná data je pak možné ukládat na libovolné médium, nebo mohou být nahrány na internet nebo síťový server v organizaci. Rozmach používání výpočetních technologiích v organizacích, a s tím spojené neustálé narůstání objemu zpracovávaných a ukládaných dat, vede i k vyšší potřebě tyto data zabezpečit. K tomuto účelu mohou být využity technické a programové prostředky, které jsou dostupné v mnoha různých variantách, provedeních a samozřejmě i cenách. Náklady na dokonalou bezpečnostní ochranu jsou obrovské. Stejného efektu ochrany za cenu podstatně menší lze dosáhnout i s využitím šifrovacích nástrojů, s jejichž pomocí lze přenášet i hodně citlivá data po velmi rizikových sítí jako je např. internet. Kryptografii lze provádět dvěma základními směry – asymetrickými a symetrickými šifrovacími algoritmy. [1, s. 20,21]



Obr. 1. Rozdíl mezi symetrickým a asymetrickým šifrováním [22]

3.2.1 Elektronický podpis

Při zabezpečování dat, konkrétně při procesu přenášení, ukládání a zpracování informací, je hlavním požadavkem zachování jejich integrity, tj. zabránění tomu, aby nedošlo k neoprávněné modifikaci dat. U elektronických dokumentů je to řešeno za pomocí připojení určité dodatečné informace k datům, která slouží jako důkaz o pravosti totožnosti odesílatele. [10, s. 66]

Elektronický podpis se nejčastěji používá k podepsání elektronického dokumentu. Tento dokument může nabývat libovolné délky a obsahu, dle kterých se pak dále odvíjí samotná délka řetězce elektronického podpisu, která je k dokumentu připojena. Shrnutí funkcí elektronického popisu:

- elektronický podpis jasně udává, kdo je autorem dokumentu,
- elektronický podpis ujišťuje příjemce dokumentu o skutečnosti, že informace nebyly během přenosu nijak pozměněny nebo smazány,
- elektronický popis jednoznačně určuje autora dokumentu.

Nejčastější kryptografické algoritmy, které se u elektronického podpisu používají, jsou asymetrické algoritmy Rivest, Shamir, Adleman (RSA) a Digital Signature Algorithm (DSA). Samotný proces pak začíná vytvořením tzv. hashe (zkrácený popis zprávy). U algoritmu RSA je to např. funkce Message-Digest algorithm (MD5) u algoritmu Digital Signature Standard (DSS) je to např. funkce Secure Hash Standard (SHS). Z tohoto hashe se za použití soukromého klíče vypočítá elektronický podpis zprávy, který se ke zprávě připojí. Díky tomu si vlastník veřejného klíče ověří platnost elektronického podpisu. [10, s. 66]

3.2.2 Hash Algoritmy

Kromě symetrického a asymetrického šifrování se používá ještě jeden způsob šifrování, u kterého je účelem pouhé zašifrování informace. Typický příklad představuje uložení hesla v systému UNIX nebo Microsoft Windows. Uživatelem vytvořené heslo se zašifruje, a takto zašifrované heslo se uloží do systému. Výsledek šifrování daného hesla je pokaždé stejný, když se uživatel např. přihlašuje, systém mu zadá heslo, jehož zašifrovaný výsledek se porovná již s předchozím uloženým výsledkem. Systém tedy nemusí znát heslo uživatele, ale pouze jeho zašifrovaný výsledek. Zpětné dešifrování zde není potřeba provádět. V systémech se běžně používá délka 64 bitů, obecně se pak doporučuje délka alespoň 160 bitů. [1, s. 30,31]

Kromě jiného se hash algoritmy používají na testování integrity textu za účelem ověření, zdali nebyl text pozměněn. Za pomocí hashovaní se vytvoří tzv. otisk dokumentu, což představuje mnohem menší objem dat, než má samotný dokument, zároveň z něho lze vyčíst jednoznačný obsah dokumentu. [1, s. 30,31]

3.2.3 Certifikáty

Certifikáty v digitální podobě spadají pod asymetrickou kryptografii, a jsou tvořeny jako digitálně podepsaný veřejný šifrovací klíč, jenž vydává šifrovací autorita. Certifikáty jsou uloženy ve formátu X 509, který obsahuje např. sériové číslo certifikátu, údaje o vlastníkovi a o certifikační autoritě, která certifikát vydala, algoritmus použitý k vytvoření digitálního podpisu, digitální podpis veřejného klíče certifikační autority, datum začátku platnosti a konce certifikátu apod. Certifikáty jsou primárně vytvářeny pro bezpečnou identifikaci druhé strany při vytváření spojení typu Hypertext Transfer Protocol Secure (HTTPS), které používá protokol Secure Sockets Layer (SSL), které bylo nahrazeno novějším Transport Layer Security (TLS). Díky tomu je umožněno důvěřovat i neznámým certifikátům, které jsou podepsány ověřenou certifikační autoritou. [9, s. 29]

4 HROZBY

Hrozby, jako jsou např. počítačové viry, představují pro počítače a počítačové sítě v organizacích jedno z nejznámějších rizik. Zabránění jejich vniku do systému nebo jejich případné šíření či působení je jednou ze základních součástí bezpečnosti informačního systému. Aby byl bezpečnostní systém organizace schopen se vůči takovým útokům bránit, je vhodné znát problematiku škodlivých kódů a hrozeb. [13, s. 9-17]

4.1 Viry

Shodnost názvů biologických virů a počítačových virů není náhodná. Vychází ze stejné základní vlastnosti – samo-replikace, při níž dochází k množení viru v hostiteli (počítači). Typickým příkladem jsou executable (spustitelné) soubory za použití určitých aplikací např. dokument vytvořený v Microsoft Word. Pokud tedy uživatel infikovaný dokument spustí, rovněž dojde ke spuštění kódu viru. Virus se pak dál snaží replikovat a nakazit tak další vhodné hostitele. [13, s. 9-17]

4.2 Trojské koně

Stejně jako viry jsou trojské koně nejvíce obsaženy ve spustitelných souborech, a to převážně v souborech s koncovkou EXE. Narozdíl od virů tento soubor neobsahuje nic jiného než pouhé "tělo" trojského koně. Trojské koně nejsou schopny provádět samo-replikaci a infekci souborů, z čehož plyne, že jedinou možností, jak tyto trojské koně odstranit, je smazat nakažený soubor. Trojské koně se na první pohled jeví jako užitečné programy, avšak ve skutečnosti jsou škodlivé. Dnes nejznámější typy trojských koní lze vyčlenit jako: password-stealing trojské koně, destruktivní trojské koně a backdoory. [13, s. 9-17]

4.3 Červi

Červi operují na nižší síťové úrovni, kde se nešíří za pomocí infikovaných souborů, ale díky síťovým paketům. Pokud se podaří těmto paketům infikovat nějaký systém, budou se za pomocí sítě internet šířit k dalšímu systému. V případě zasažení systému se specifickou bezpečnostní dírou bude systém infikován, a červ se bude snažit o vytvoření jiných možností, jak systém infikovat. Červ se tedy šíří skrze bezpečnostní díry v operačním systému. Z toho vyplývá, že červa nelze za pomocí antivirového softwaru detekovat. V organizacích to může znamenat úplnou infekci podnikové Local Area Network (LAN). Příkladem červů jsou např. Code Red, Lovsan / Blaster, SQL Slammer. [13, s. 9-17]

4.4 Spyware

Jedná se o program, který za pomocí internetu neoprávněně odesílá data z počítače uživatele. Převážně se jedná o statistická data jako je např. souhrn navštívených stránek nebo nainstalovaných programů. Hlavním posláním spywarů je z těchto získaných dat vytvořit cílenou reklamu. Spyware programy jsou ve své podstatě legální, avšak je velmi pravděpodobné, že mohou být zneužity pro nekalé úmysly. [13, s. 9-17]

4.5 Adware

Adware představuje v počítači nevyžádanou reklamu. V běžné praxi jde např. o vyskakující pop-up okna s reklamním obsahem, které se objevují při prohlížení internetu. Tato reklama se objevuje, i když si jí uživatel nevyžádal, avšak je součástí licenčního ujednání tzv. "EULA" - End User License Agreement. Toto ujednání bývá zakořeněno ve většině instalací, a pro úspěšné nainstalování daného programu musí s tímto ujednáním uživatel souhlasit. Typickým příkladem je produkt DivX. Odebrání takové reklamy je pak zpoplatněno. [13, s. 9-17]

4.6 Hoax

Hoax nepředstavuje program, který pracuje na základě infiltrování, ale rovněž ho můžeme do škodlivých kódů zařadit. Hoax je prezentován jako falešná zpráva, která varuje uživatele před neexistujícím virem. Pokud uživatel této zprávě uvěří, pošle jí např. prostřednictvím e-mailu dál a tím vznikne proces šíření. Hoax však nemusí být zprávy pouze o virech, ale například i zprávy napodobující důležité oznámení z banky klienta, která vyžaduje číslo účtu a PIN klienta. [13, s. 9-17]

4.7 Phishing a Pharming

Podobně jako v případě hoaxu se phishing šíří pomocí podvodných e-mailů, kdy jsou na velké množství adres hromadně odeslány nepravdivé dopisy. Trik spočívá v odkazu umístěném v e-mailu, který odkazuje například na podvodné stránky s formulářem ve stejném designu jako by nesly stránky originální. Uživatel nemusí poznat, že se jedná o podvod, a tak do připraveného formuláře doplní citlivé údaje a zašle autorům, kteří tak mohou data jednoduše zneužít. Taková manipulace, jejíž účelem je provedení určité akce, se označuje jako sociální inženýrství [13, s. 9-17]

Pharming je podobný Phishingu, taktéž jde o nástroj, který slouží k získání citlivých údajů často spojených s bankovním účtem. Hrozby tohoto druhu používají speciální programy, které napadnou doménový server (DNS), přepíšou IP adresu a tím dojde k přesměrování na podvodné stránky, jenž vzhledově vypadají jako stránky společnosti provozující internetové bankovnictví. [23]

4.8 Exploit a zero-day attack

Exploity jsou tvořeny určitou posloupností příkazů nebo dat, které mohou zneužít programátorskou chybu v softwaru, a tím vyvolat neočekávané chování aplikace nebo hardwarového zařízení, což může být zneužito pro přímý útok nebo pro šíření malwaru. Nejčastěji exploity pronikají do počítačů prostřednictvím webového prohlížeče, a to formou Javascriptů nebo elektronické pošty. Tyto chyby existují v převážné většině softwarů. Pravidelné aktualizace a bezpečnostní záplaty jsou předpokladem k redukci výskytu těchto chyb. Pokud dojde k útoku, který využil programátorskou chybu v softwaru před tím, než pro ni byla vydána bezpečnostní záplata, bude se takový útok označovat jako útok nultého dne (zero-day attack). [16]

4.9 APT Hrozby

Pokročilé přetrvávající hrozby neboli Advanced Persistent Threat (ATP), představují útoky cílené na konkrétní osobu nebo organizaci. Tyto hrozby se dají charakterizovat pokročilým způsobem provedení, při čemž se útočník snaží co nejpodrobněji analyzovat danou organizaci nebo jedince. Na základě těchto analýz přesně odhalí slabé místo a skrze něj pak infiltruje cílený subjekt. Hrozby tohoto typu obvykle nemají destruktivní účel, slouží spíše k trvalému, neoprávněnému přístupu k citlivým datům. [20]

5 OPATŘENÍ PROTI HROZBÁM

Hrozby představují pro organizaci bezpečnostní riziko, které může organizaci znepříjemňovat práci např. vyskakujícími okny s reklamami (adware), jindy může způsobit pouze neškodný povyk ve formě žertovného dopisu (hoax), a v horších případech mohou vést k finanční ztrátě, nebo díky úniku informací do nesprávných rukou zapříčinit její úplný pád. Bezpečnostní opatření proti hrozbám lze realizovat pomocí následujících způsobů.

5.1 Antivirové programy

Fungují na principu vyhledávání virů dle jejich struktury, která je uložená ve virové databázi. Jelikož jsou neustále vyvíjeny nové viry, je potřeba držet tuto databázi neustále aktuální. Databáze obsahuje přesný popis viru, včetně informací o tom, jaký přesně soubor infikoval, a jak ho můžeme bezpečně odstranit. [7, s. 79,82]

Obecné antivirové techniky – cílem jejich funkce je nalezení neznámého viru, který není uložen v databázi. Pro svou funkci používají:

- **Srovnávací testy** – během prvního spuštění dojde k zaznamenání informací o daném souboru (např. čas vzniku, velikost, atributy a specifické součty). Při dalších spuštěních jsou tato data zpětně porovnávána s jejich původním stavem, a pokud došlo k významných změnách v datech je velmi pravděpodobné, že se jedná o virus.
- **Heuristickou analýzou** – spočívá v detailní analýze obsahu souborů uložených na pevném disku počítače, kde se snaží vyhledat podezřelé konstrukce např. převzetí kontroly nad počítačem. Primárně tak funguje bez nutnosti obsahu virové databáze, ale většina programů provádí současně i test na obsah známých virů z virové databáze. Rozšíření této metody se nazývá plná heuristická analýza, která se snaží emulovat činnost počítače při spuštění programu.
- **Testy prostředí na souborové viry** – antivirový program zde kopíruje existující soubory typu .exe a .com, a provádí s nimi různé operace, při nichž kontroluje jejich obsah.

Jádro antivirových balíků je tvořeno pravidelně aktualizovanou virovou databází. Ta obsahuje popis a další informace o nejrozšířenějších virech, které byly vytvořeny před datem poslední aktualizace virové databáze, proto je jejich aktualizace velmi důležitá. [7, s. 79,82]

5.2 Firewall

Firewall je zařízení, které se chová jako brána, jež odděluje provoz mezi dvěma sítěmi (např. firemní sítí a internetem) a propouští pouze data, která odpovídají předem definovaným pravidlům. Tímto způsobem zamezuje neoprávněným průnikům vniknout do sítě, a také zabraňuje odesílání dat ze sítě bez vědomí uživatele. [17]

Firewally můžeme rozdělit do tří základních skupin:

- **Paketové filtry** – nejčastěji se vyskytují v routerech, kde kontrolují pouze přenos paketů mezi zdrojovou a cílovou adresou. Tyto firewally vynikají velkou rychlostí, ale menším stupněm zabezpečení.
- **Aplikační brány** – slouží jako prostředník mezi uživatelem a serverem, ke kterému se připojuje. Uživatel se první připojí k aplikační bráně (proxy), která se následně připojí k serveru. Aplikační brána zkontroluje veškeré pakety (bloky dat přenášené v počítačových sítích) pro danou službu, a zašle je zpět uživateli. Oproti paketovým filtrům poskytují větší ochranu, ale pracují pomaleji. [17]
- **Stavové firewally** – tyto firewally ověřují souvislosti mezi příchozími pakety a předchozími odchozími pakety tak, aby byla zajištěna jejich oprávněnost. Firewall kontroluje pouze stavovou tabulku namísto toho, aby u každého paketu kontroloval nadefinovaná pravidla. [9, s. 37]

5.3 Zálohovací programy

Zálohování je proces, při kterém se vytváří kopie dat. Tato kopie se ukládá na záložní datové nosiče (nejčastěji pevné disky, Network Attached Storage (NAS), optické disky, USB disky, cloudové úložiště). Kopie dat jsou využívány v případě poškození, ztráty nebo jiné potřeby práce s daty uloženými v minulosti.

Strategie zálohování:

- **Úplné zálohování** – zálohují se všechna data obsažená v počítači. Z časového i kapacitního hlediska je tato metoda nejnáročnější.
- **Přírůstkové zálohování** – zálohují se pouze data, které byly přidány nebo pozměněny od provedení poslední úplné nebo přírůstkové zálohy. Tato metoda je velmi rychlá, avšak obnova dat komplikovaná.

- **Diferenční zálohování** – podobně jako u přírůstkového zálohování se zálohují pouze data, které byly přidány nebo změněny od provedení poslední úplné nebo přírůstkové zálohy včetně těch, které již jsou obsaženy v předešlé částečné záloze. Zálohování touto metodou je náročnější na úložný prostor a čas. Obnova dat je pak jednodušší než v případě přírůstkového zálohování. [11, s. 33-37]

5.4 Systémy IDS a IPS

Systémy detekce narušení neboli Intrusion Detection Systém (IDS), sledují události, které probíhají v počítačové síti organizace, kde se snaží objevit aktivity, které by mohly být příčinou vzniku bezpečnostních hrozeb. Tyto nástroje sledují jak provoz na síti, tak i provoz na serverech, kde však z hlediska vyšší výpočetní náročnosti těchto systémů dochází k většímu zatížení. Z hlediska rozpoznání narušení využívají systémy IDS a IPS dvě základní metody založené na popisu a detekci hrozeb.

Systémy prevence narušení neboli Intrusion Prevention Systems (IPS), podobně jako systémy IDS, sledují provoz na síti i na serverech a pracovních stanicích. Jedná se o softwarové produkty, které chrání operační systém před hrozbami a případnými útoky. Kromě samotné detekce jsou tyto systémy schopny útokům zabránit nebo je přerušit.

Systémy IDS a IPS jsou velmi účinné, avšak skrývají nebezpečí v podobě tzv. planých poplachů, které mohou omylem zablokovat síťový provoz na určitém síťovém zařízení. [9, s. 38-40]

5.5 Technologie SIEM

Tyto technologie umožňují sbírat data ze zařízení připojených v IT infrastruktuře a díky nim provádět monitoring a analýzu. Na základě těchto analýz je pak možné identifikovat bezpečnostní hrozby, které by mohly v organizaci způsobit bezpečnostní incident.

Monitoring a analýzy jsou vyobrazeny v grafickém rozhraní, které zároveň přehledně zobrazují data z více zkoumaných zdrojů najednou. Mezi nejčastější zdroje patří databázové, operační, aplikační i síťové systémy a zařízení. [18]

6 FREE A OPEN SOURCE SOFTWARE

Malé a střední podniky jsou převážně charakterizovány počtem zaměstnanců, kterých je v případě malých podniků do 50 lidí a do 250 lidí v případě středních podniků. Jejich hlavním polem působnosti je v převážné většině sektor služeb, ve kterém se zaměřují na uspokojování potřeb zákazníka. Tyto menší a střední podniky jsou schopny se rychle přizpůsobit trhu, a rychle reagovat na jeho požadavky v porovnání s většími podniky. Podniky tohoto typu zaměstnávají více než polovinu všech pracovních sil. [4, s. 53]

Hlavním problémem je kromě omezených finančních zdrojů a konkurence i snaha o co možná nejmenší náklady. S tím je i spojená většinou nízká úroveň zabezpečení informačních technologií. Na základě toho je vhodné využít možnosti free a open source softwaru pro bezpečnost informačních technologií. [4, s. 53]

Samotný software lze rozdělit do mnoha kategorií dle parametrů a způsobu užití. Základním parametrem je druh licence, jakou daný software vlastní. Cílem praktické části práce je vyhledat a analyzovat software s licencí typu free a open source, který by sloužil k zabezpečení informačních technologií v malých a středních organizacích. Na základě toho je vhodné objasnit pojmy s tím související. [4, s. 52]

6.1 Free software

Jedná se o software, který je možné získat zdarma prostřednictvím internetu nebo pomocí různých datových nosičů např. CD, DVD, flash disk. Takový software je možné zdarma používat, kopírovat, šířit, studovat a měnit. Je možno jej charakterizovat ve čtyřech základních bodech:

- svoboda používat software za jakýmkoliv účelem,
- svoboda přístupu ke zdrojovému kódu, a na základě toho provádět studium softwaru a přizpůsobení jeho funkcí svým potřebám,
- svoboda distribuce jeho kopií,
- svoboda v úpravách programu vedoucí k jeho zlepšení a následné zveřejnění těchto změn k prospěchu ostatních uživatelů.

Tyto body podléhají pravidlu zvaném copyleft, které zakazuje omezit některé z uvedených svobod. Nejrozšířenější licence spadající pod toto pravidlo se nazývá General Public License (GPL). [4, s. 52]

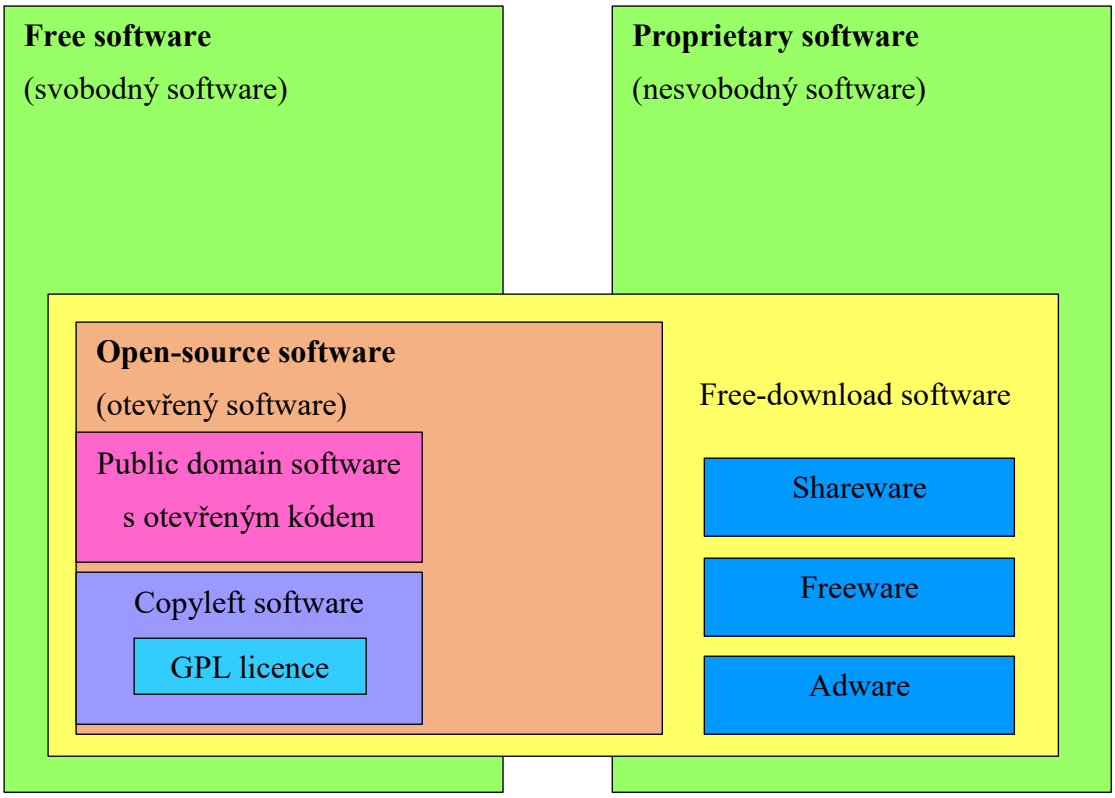
6.2 Open Source software

Narozdíl od free softwaru není ve většině případech open source software produktem firem, ale na jeho vývoji se bez jakéhokoliv nároku na finanční odměnu podílí skupina programátorů z celého světa. Zdrojový kód takového softwaru je možné upravovat a volně šířit, avšak je nutné dodržovat určité licenční omezení, které specifikuje 54 různých licencí vytvořených iniciativou Open Source Initiative (OSI). Open source je možno charakterizovat ve čtyřech základních bodech:

- Otevřená distribuce – při distribuci softwaru nesmí dojít k jakémukoliv omezení či zpoplatnění např. formou honoráře či poplatků.
- Otevřený přístup ke zdrojovému kódu – licence open source softwaru zakazuje jakýmkoliv způsobem skrývat nebo omezovat přístup ke zdrojovému kódu.
- Otevřená možnost úprav. [4, s. 52]

6.3 Rozdíl mezi free a open Source software

Vzhledem k velké podobnosti obou těchto způsobů licencování je velmi složité určit, kde až sahá open source software a kde začíná free software. I přes snahu nadace free software (FSF) a iniciativy OSI se nepodařilo tyto pojmy rozlišit, a to především z toho důvodu, že oba typy softwaru sdílí společný princip přístupu ke zdrojovému kódu. Nadace FSF se zaměřuje především na svobodu manipulace a užívání zdrojového kódu, jakožto i jeho distribuci a zachování správné etiky. Iniciativa OSI cílí na zajištění optimálního přístupu k softwaru, a to zejména z hlediska využití v komerční sféře, kde jsou plně využity praktické výhody open source softwaru. [3, s. 17-19]



Obr. 2. Schématické rozdělení licencování [5, st. 11]

Velmi často dochází k nesprávné záměně free software a freeware. Freeware je dostupný zdarma, rovněž ho lze zdarma používat po neomezenou dobu, avšak na rozdíl od free softwaru není dovoleno jej šířit. Autorská práva k freeware softwaru patří autorovi a bez jeho souhlasu není dovoleno software jakýmkoliv způsobem měnit či upravovat pro komerční účely. [3, s. 20]

II. PRAKTICKÁ ČÁST

7 SOUČASNÝ STAV V OBLASTI BEZPEČNOSTI INFORMAČNÍCH TECHNOLOGIÍ

Donedávna bylo zapotřebí řešit převážně bezpečnost koncových stanic (pracovních počítačů), ale s rozšířením mobilních zařízení jako smartphonů, tabletů a obecně technologií typu Internet of Things (IoT) dochází i k útokům, které využívají zranitelnosti těchto zařízení. Jde především o škodlivé programy (malware), které podobně jako škodlivý program typu červ, dokáží z jednoho zařízení infikovat celou síť. Jelikož se jednotlivá zařízení připojují právě přes firemní síť, musí se bezpečnostní prvky stát její vnitřní součásti a nebudovat se jen kolem ní. [19]

Dnešní útoky využívají především otevřené porty na firewallu, díky čemuž se infikuje celá síť a pomocí odposlechů nebo dalších zranitelností lze získat administrátorské přístupy. Jedním z nejznámějších škodlivých softwarů současnosti se stal vyděračský software (ransomware) WannaCry, který je považován za nejničivější a nejagresivnější útok tohoto druhu (nakaženo bylo více než 250 000 počítačů po celém světě). Jeho funkce spočívá v zašifrování dat uložených na pevném disku počítači, a následně podmínkou zaplatit finanční obnos k tomu, aby byla data rozšifrována. [19]

Problém spočívá v rychlosti šíření a samotném vývoji škodlivých kódů. Rychlost je totiž tak velká, že mnohé organizace nestíhají v rámci bezpečnosti držet krok, a nemají o hrozbách dostatečné množství informací. Strategie ochrany dat se zaměřuje na tři základní části podnikové infrastruktury, a to na uživatele, procesy a technologie. Ochrana dat z uživatelského pohledu je založena na dostatečné informovanosti a seznámení zaměstnanců s nejnovějšími hrozbami. Z hlediska procesů je nezbytné provádět včasné a pravidelné aktualizace, které napomáhají minimalizovat nebo odvrátit kybernetické útoky. Poslední díl strategie ochrany dat se týká samotných hardwarových prvků informačních technologií. Bezpečnost těchto prvků se aktuálně řeší pomocí tradičních metod ochrany koncových bodů jako je např. využití firewallů a antivirových programů. Ve výsledku však není ani tato strategie dostačující, proto mnoho organizací využívá pojištění proti kybernetickým rizikům. Míra využívání tohoto druhu pojištění roste spolu s mírou výskytu malware a ransomware. [19]

7.1 Umělá inteligence

V posledních letech bylo na vývoj a zlepšení umělé inteligence vynaloženo velké množství jak finančních, tak i výzkumných jednotek, a to napříč mnoha odvětvími včetně

bezpečnostních technologií. Úspěšnost umělé inteligence je založena na objemu telemetrických dat, ze kterého algoritmy při svých výpočtech vycházejí. Větší množství dat pak vede k přesnějším výsledkům. Jako typický příklad lze uvést malware, který vznikl na opačné straně světa než se organizace, jejíž informační bezpečnost chceme zajistit, nachází. Včasné objevení tohoto malwaru a vytvoření rychlého protiopatření však není v lidských silách, proto je vhodné využít strojové učení umělé inteligence, které může za pomocí algoritmů tento malware včas identifikovat a následně varovat bezpečnostní systém. [19]

7.2 Kontrola šifrovaných dat

Vzhledem k velké oblibě šifrování souborů se zvedl i jejich celkový počet. Odhalení hrozeb v šifrovaných souborech spjaté s bezpečnostní analýzou takových souborů ztěžuje práci bezpečnostním systémům. Východiskem jsou algoritmy strojového učení, které pasivně monitorují datové prvky na základě analýzy metadat a vzorců chování. [19]

7.3 Ochrana mobilních zařízení

Bezpečnost koncových zařízení, které zaměstnanci využívají při mobilním způsobu práce nebo obecně při každodenním životě, zvyšuje flexibilitu, produktivitu a informovanost, ale pro organizace to představuje bezpečnostní hrozbu, kterou kolikrát nejsou schopny zredukovat nebo úplně odstranit. Je to zejména z toho důvodu, že mobilní platformy jsou využívány k přístupu k citlivým informacím jako jsou firemní emaily. Enterprise Resource Planning (ERP) a Customer relationship management (CRM) systémy rovněž bývají používány k zpracovávání dat včetně obchodních informací. Aktuálně nejvhodnějším řešením je připojování prostřednictvím uzavřené virtuální privátní sítě (VPN). Faktem ale je, že mnoho zaměstnanců toto doporučení nedodržuje a připojují se mimo podnikovou síť, kdy organizace není schopna takové připojení monitorovat a zabezpečit. Nově vznikají tzv. bezpečné internetové brány v cloudech které by mohly problém související s blokováním obsahu mířící na koncová zařízení zaměstnanců, odstranit. Typické útoky na mobilní zařízení jsou prováděny prostřednictvím podvodných Wi-fi sítí, aplikací nebo phishingových SMS útoků. [19]

7.4 Potřeba zvýšení bezpečnosti cloudu

Využívání cloudových služeb se v posledních letech velmi rozmohlo, a to zejména díky možnostem ukládání, sdílení a upravování souborů, což je možné provádět nejen mezi jednotlivými odděleními organizace, ale i mezi různými platformami. S rozmachem převážně

mobilních platforem toho využívá stále větší množství subjektů, z čehož vyplývá nutnost zabezpečení data center a databází včetně mobilních zařízení. [19]

7.5 Regulace

Dalším aktuálním tématem je i regulace v oblasti bezpečnosti informačních technologií, která doposud nebyla důsledně řešena, avšak postupně dochází v této oblasti ke zlepšení, a to v celosvětovém měřítku. Typickým příkladem je nařízení General Data Protection Regulation (GDPR), které nedávno vstoupilo v účinnost a s tím spojená i regulace ePrivacy, na které se momentálně pracuje. Často se s tématem bezpečnosti informačních technologií setkáváme i při spolupráci větších firem, které např. po svých dodavatelích požadují certifikát, který dokazuje jistou míru zabezpečení, nejčastěji pak některé ze série norem ISO 27000. [19]

8 ANALÝZA FREE A OPEN SOURCE NÁSTROJŮ V OBLASTI BEZPEČNOSTI INFORMAČNÍCH TECHNOLOGIÍ

Momentálně je v České republice zhruba 1,5 milionů malých a středních podniků. Většina z nich nepřikládá zabezpečení informačních technologií velkou prioritu. Pouze pro cca 15 % malých organizací je tvorba IT strategie podstatná, v porovnání s většími organizacemi, kde 67 % z nich považuje IT strategii za důležitou. [21]

Malé a střední organizace nepovažují z důvodu jejich malé velikosti bezpečnost informačních technologií za důležitou, a žijí v představě, že nejsou pro kyberzločince vhodným terčem. Stejně tak jako velké organizace rovněž zpracovávají údaje z elektronických plateb, vedou záznamy o zákaznících a uchovávají informace související s konkurenceschopností organizace. Jelikož menší organizace mají nedostatečné zabezpečení informačních technologií, je u nich vyšší pravděpodobnost vzniku kybernetického útoku. Plyne to převážně z nedostatku finančních prostředků či absence bezpečnostního experta. Z tohoto důvodu je využití free a open source softwaru velmi účelné. Po úspěšně provedeném kybernetickém útoku totiž mohou malé a střední organizace utrpět jak finanční škody vynaložené na najmutí IT specialisty, nebo nákupu nového vybavení, ale rovněž i ztracené obchodní příležitosti či psychickou újmu související s poškozením dobré pověsti organizace. Kybernetické útoky nejčastěji míří na finance organizace (phishing) nebo na zašifrování dat (ransomware), kdy za odšifrování dat požadují útočníci výkupné. [21]

Jako základ ochrany před takovými útoky a před škodlivým softwarem by měl být implementován vhodný firewall a antivirový software, který by měl být přítomen na všech koncových zařízeních. Dále by měl být přítomen vhodný zálohovací program, který slouží k obnově dat v případě úspěchu některého z ničivých škodlivých programů a šifrovací software pro zabránění odposlouchávání vnitro organizační komunikace. V neposlední řadě také nástroj pro úschovu a generování složitých hesel a aktualizační správce.

Firmy mají na bezpečnostní nástroje odlišné požadavky, ať už například z hlediska nároků na hardware, jednoduchosti grafického prostředí nebo množství obsažených funkcí. Z tohoto důvodu bude pod každou kategorií bezpečnostních nástrojů přítomna tabulka obsahující zkoumaná kritéria daného softwaru a rovněž výčet silných a slabých stránek.

Jednotlivá kritéria budou hodnocena za pomocí stupnice a to následovně: 1 (výborná), 2 (chvalitebná), 3 (dobrá), 4 (dostatečná), 5 (nedostatečná). Na základě toho bude u jednotlivých nástrojů vypočítán medián. Veškeré hodnocení probíhá na základě vlastního výzkumu a zkušeností.

Stupnice hodnocení pro kritérium přehlednosti a jednoduchosti grafického prostředí

Tab. 1. Stupnice kritéria přehlednosti a jednoduchosti grafického prostředí

1 (výborná)	Použito je jednoduché a přehledné grafické prostředí s popiskami a vysvětlivkami.
2 (chvalitebná)	Použito je jednoduché a přehledné grafické prostředí bez popisků a vysvětlivek.
3 (dobrá)	Použito je grafické rozhraní se složitější nebo skrytou funkcí prvků.
4 (dostatečná)	Použito je grafické rozhraní s nepřehledným rozmístěním prvků.
5 (nedostatečná)	Použit je pouze shell nebo příkazový řádek.

Stupnice hodnocení pro kritérium jazyka nástroje

Tab. 2. Stupnice kritéria jazyků nástrojů

1 (výborná)	Český jazyk
2 (chvalitebná)	Slovenský jazyk
3 (dobrá)	Jednoduchý anglický jazyk se známými výrazy
4 (dostatečná)	Technický anglický jazyk se složitými výrazy
5 (nedostatečná)	Jiný jazyk

Stupnice hodnocení pro dokumentaci k nástroji

Tab. 3. Stupnice kritéria dokumentace k nástrojům

1 (výborná)	Existuje v českém jazyce
2 (chvalitebná)	Existuje ve slovenském jazyce
3 (dobrá)	Existuje v jednoduchém anglickém jazyce se známými výrazy
4 (dostatečná)	Existuje v technickém anglickém jazyce se složitými výrazy
5 (nedostatečná)	Dokumentace neexistuje

Stupnice hodnocení hardwarových nároků nástrojů

Tab. 4. Stupnice kritéria hardwarových nároků na systém

1 (výborná)	Minimální nároky na systém, jmenovitě: Operační systém: Windows 10, 8.1, 8, 7, Vista, XP, ME, 2000, 98, Windows Server 2012, 2008, 2003 Procesor: 2 jádrový (minimálně Intel Pentium 2) RAM: 64 MB Volné místo na pevném disku: 320 MB
2 (chvalitebná)	Střední nároky na systém, jmenovitě: Operační systém: Windows 10, 8.1, 8, 7, Vista Procesor: 2 jádrový RAM: 1 GB Volné místo na pevném disku: 1 GB
3 (dobrá)	Vyšší nároky na systém, jmenovitě: Operační systém: Windows 10 Procesor: 2 jádrový RAM: 1 GB Volné místo na pevném disku: 16 GB

Stupnice hodnocení pro množství obsažených funkcí nástrojů

Tab. 5. Stupnice kritéria pro množství obsažených funkcí v nástroji

1 (výborná)	Velké množství obsažených funkcí (počet funkcí je podobný jako u komerčních nástrojů)
2 (chvalitebná)	Nadstandartní množství funkcí
3 (dobrá)	Průměrné množství funkcí
4 (dostatečná)	Podprůměrné množství funkcí
5 (nedostatečná)	Pouze základní funkce

Stupnice hodnocení pro počet podporovaných platforem

Tab. 6. Stupnice kritéria pro počet podporovaných platforem

1 (výborná)	Windows 7, 8, 10, Vista + Linux + OS X + Android/iOS
2 (chvalitebná)	Windows 7, 8, 10, Vista + Linux + OS X
3 (dobrá)	Windows 7, 8, 10, Vista + pouze Linux/OS X
4 (dostatečná)	Windows 7, 8, 10, Vista
5 (nedostatečná)	Windows 10

Stupnice hodnocení pro bezpečnost z hlediska poslední vydané aktualizace (verze) nástroje

Tab. 7. Stupnice kritéria pro bezpečnost z hlediska poslední vydané aktualizace

1 (výborná)	Aktualizace na denní bázi
2 (chvalitebná)	Aktualizace na týdenní bázi
3 (dobrá)	Aktualizace na měsíční bázi
4 (dostatečná)	Aktualizace na roční bází
5 (nedostatečná)	Aktualizace jsou více než rok staré

8.1 Antivirové programy

Antivirový program (hovorově antivirus) je software, který v sobě sdružuje několik nástrojů, jenž převážně slouží k nalezení a odstranění škodlivých programů. Současné antivirové programy obsahují ochranu před ransomware, adware, spyware, trojskými koni, viry a dalšími malwary. Dále obsahují firewally, ochrany webových prohlížečů a e-mailů (spamů), Wi-Fi sítí a další nástroje související s bezpečností, jako možnost vytvoření virtual private network (VPN) sítě, sdružení a ochrana uložených hesel, zabezpečení webových kamer, aktualizační manažer, ochrana internetového bankovnictví apod. Dostupnost jednotlivých funkcí záleží na typu licence.

8.1.1 Windows Defender

Windows Defender je anti-malware nástroj vyvíjený speciálně pro operační systém Windows společnosti Microsoft. Poprvé byl uveden pro Windows XP jako free anti spyware software. Později byl implementován s operačními systémy Windows Vista a později i Windows 7. Postupem času byl vyvíjen a vylepšován až nahradil základní bezpečnostní nástroje společnosti zvané Microsoft Security Essentials a od vydání Windows 8 se stal plnohodnotnou součástí systému.

Windows Defender je komplexní bezpečnostní program šitý přímo na míru operačnímu systému Windows. Jeho úplná integrace do systému zajišťuje absolutní kompatibilnost a velmi rozsáhlé možnosti nastavení a přizpůsobení.

Základní funkcí je ochrana před viry a hrozbami. Tato funkce standardně nabízí ochranu v reálném čase s návazností na cloudovou ochranu, která zajišťuje přístup k aktuální virové databázi, a neustále tak chrání počítač před novými typy škodlivých programů. V návaznosti na cloudovou ochranu sbírá Windows Defender tzv. infikované vzorky ze zařízení, které odesílá k analýze, na základě níž je vytvořeno protiopatření, které je následně poskytnuté dalším uživatelům. Program nabízí i možnost tzv. řízeného přístupu k citlivým souborům nebo složkám, což po aktivování zamezí přístup aplikací k provádění neoprávněných změn ve vybraných datech. Podobně je možné i specifikovat soubor nebo složku, která nebude při bezpečnostní analýze kontrolována.

Samozřejmostí je provedení rychlé kontroly, důkladné kontroly či specifické kontroly zařízení, při které je možné přesně určit, co bude předmětem kontroly. Aktualizace definic pro

tyto kontroly probíhá automaticky bez zásahů uživatele. Frekvence těchto kontrol je v průměru denní.

Užitečným nástrojem v programu Windows Defender je i tzv. ochrana účtu, která umožňuje spravovat účty v systému a hesla k přístupu do něj. Velmi chytrý způsob přístupu do systému představuje dynamický zámek, který nahrazuje klasická hesla zařízením používající technologii Bluetooth, jenž se po spárování se zařízením používající Windows Defender stane pomyslným klíčem. Zařízení se v případě ztráty signálu Bluetooth automaticky uzamkne. Windows Defender nabízí kromě klasického hesla nebo PIN kódu i možnost odemknutí pomocí biometrických údajů např. otiskem prstu nebo skenem obličeje.

Velmi rozsáhlé možnosti nabízí Firewall, který je možné zvlášť přizpůsobit doménové (firemní), privátní (domácí) nebo veřejné síti. Firewall je možné upravovat dle požadavků uživatele, je tak možné např. stanovit příchozí a odchozí pravidla, díky nimž může povolit nebo blokovat připojení k určitým programům nebo portům. V praxi se tak může jednat např. o autorizovaného uživatele, skupiny nebo počítače.

Windows Defender obsahuje i pokročilejší nástroje ochrany jako např. integritu paměti. Po aktivaci této funkce dojde k zabránění vkládání škodlivého kódu do procesů s vysokým zabezpečením. Umožňuje také sledovat a kontrolovat výkon zařízení a provádět aktualizace nainstalovaného softwaru.

Tab. 8. Silné a slabé stránky Windows Defender

Silné stránky	Slabé stránky
- není nutná instalace - plná kompatibilita se systémem - přehledné prostředí - vysvětlivky funkcí v českém jazyce - není nutné jej nastavovat - komplexní nástroj - podpora velkého množství jazyků - časté aktualizace	- nízká ochrana v porovnání s konkurenčními produkty - podpora pouze platformy Windows

8.1.2 ClamAV - open source

ClamAV je jednoduchý antivirový software s open source (GPL) licencí, který za pomocí automaticky aktualizované databáze provádí operace jako je základní skenování celých disků či jednotlivých složek, skenování emailů a webové skenování. ClamAV podporuje skenování i archivních souborů jako např. Zip, RAR, Dmg, Tar, Gzip, dále souborů, které

umožnují kompresi spustitelných souborů UPX, FSG a běžných kancelářských souborů Mac Office, MS Office, HTML, Flash, RTF and PDF.

Všechny operace jsou řízeny z příkazového řádku u systému Windows z textového shellu se skriptovacím jazykem.

Tab. 9. Silné a slabé stránky ClamAV

Silné stránky	Slabé stránky
- dostupnost pro mnoho platforem - podrobná dokumentace - minimální hardwarové nároky - aktivní vývoj ze strany vývojářů - velmi časté aktualizace virových definic	- nemá grafické rozhraní - dokumentace pouze v anglickém jazyce - pomalý průběh skenování - neexistuje podpora uživatelů - obtížná instalace - možnost poškození neodborným zásahem uživatele do zdrojového kódu

8.1.3 MoonSecure Antivirus – open source

MoonSecure Antivirus využívá stejný open source antivirový engine jako předchozí ClamAV s tím rozdílem, že práce s ním probíhá přes jednoduché grafické rozhraní. Antivirus umožňuje skenovat celý počítač metodou velmi důkladného skenu, kdy jsou prohlíženy všechny pevné disky včetně archívů a pomocí hlubokého skenu, kdy skenování probíhá pouze v pevných discích bez archivů a rychlý sken, který skenuje paměť, systémové složky a kritické oblasti, které bývají často napadány. Všechny tyto skeny však nedosahují tak velké rychlosti jako konkurenční antiviry. MoonSecure antivirus rovněž obsahuje modul pro skenování v reálném čase.

Tab. 10. Silné a slabé stránky MoonSecure Antivirus

Silné stránky	Slabé stránky
- přístupnost zdrojového kódu - minimální hardwarové nároky - velmi časté aktualizace virových definic - obsahuje přehledné grafické rozhraní - komplexní nástroj	- obsahuje pouze anglický jazyk - neexistující dokumentace - pomalý průběh skenování - neexistuje podpora uživatelů - podpora pouze systémů Windows - možnost poškození neodborným zásahem uživatele do zdrojového kódu

Tab. 11. Kriteriální porovnání antivirových nástrojů

Kritéria	Antivirové programy		
	Windows Defender	ClamAV	MoonSecure Antivirus
Přehlednost a jednoduchost grafického prostředí	1	5	2
Jazyk nástroje	1	4	3
Dokumentace k nástroji	1	4	5
Hardwarové nároky	2	1	1
Množství funkcí	1	5	4
Podpora dalších platforem	4	2	4
Stáří poslední vydané aktualizace (verze)	1	1	1
Medián	**1**	**4**	**3**

8.2 Firewall

Firewall představuje zeď umístěnou mezi koncové zařízení (počítač) a internet, která se snaží zabránit neoprávněnému přístupu do privátní sítě organizace. Tato zeď na jedné straně kontroluje informace z internetu, a na straně druhé kontroluje informace, které odesílá počítač.

Tyto informace odpovídají definovaným pravidlům, na základě kterých firewall vyhodnocuje, zdali může informace přijmout či odeslat. Firewally bývají součástí operačních systémů, a také většiny placených antivirů. Firewall by měl být jedním ze základních bezpečnostních opatření každého počítače, který je připojen k internetu.

8.2.1 Windows firewall

Microsoft začal importovat firewall, tehdy ještě pod názvem Internet Connection Firewall, již do svých operačních systémů Windows XP a Windows Server 2003. Od vydání Windows 10 se přejmenoval na Windows Defender Firewall, který je součástí bezpečnostních nástrojů Windows Defender.

Tento Firewall zastává jen základní funkce jako je monitoring a zabezpečení síťového spojení. Umožňuje spravovat doménovou, privátní i veřejnou síť řadou pravidel. V těchto

pravidlech je možné vyhledat subjekt, který ve firewallu operuje, a jeho atributy např. místní adresu, vzdálenou adresu, protokol, místní port, vzdálený port, oprávnění uživatele, autorizované počítače apod.

Tab. 12. Silné a slabé stránky Windows Firewall

Silné stránky	Slabé stránky
- není nutná instalace - plná kompatibilita se systémem - vysvětlivky funkcí v českém jazyce - není nutné jej nastavovat - podpora velkého množství jazyků	- podpora pouze platformy Windows - absence pokročilých funkcí - zabezpečení pouze příchozích spojení

8.2.2 Tinywall Firewall – free software

Tinywall je firewall, který nabízí jednoduše uspořádané grafické prostředí s dobrou orientací. Tento software obsahuje nadstandartní funkce, které konkurenčním firewallům často schází. Mezi ně patří možnost volby módu firewallu: normální ochrana, blokovat vše, povolit firewall, vypnout firewall a auto trénink, kdy firewall povolí veškerou komunikaci a zapamatuje si aplikace, které se připojily k internetu. Umožnuje vytvářet tzv. white listy aplikací, procesů a oken, jejíž internetová komunikace pak není firewallem blokována. Tyto výjimky však mohou být i blokovány pouze na určitou dobu (např. 5 minut). Jednou z nadstandartních funkcí je zaheslování přístupu do nastavení firewallu. Samozřejmostí je pak zobrazení všech připojení včetně jejich zdrojových portů, zdrojových adres a cílových portů. Firewall je v českém jazyce. Instalace a samotná aplikace je z hlediska velikosti velmi malá (jednotky megabytů). Běh firewallu je plynulý a neobtěžuje uživatele například vyskakujícími okny. Nevýhodou je to, že od samotného začátku jsou blokovány všechny aplikace, které mají přístup na internet a je tak nutné je ručně povolit.

Tab. 13. Silné a slabé stránky TinyWall Firewall

Silné stránky	Slabé stránky
- vysvětlivky funkcí v českém jazyce - nezatěžuje systém - jednoduché grafické prostředí - podpora velkého množství jazyků - nadstandartní možnosti nastavení	- podpora pouze platformy Windows - zpočátku je nutné jej nastavit - jazyk oficiálních webových stránek pouze v anglickém jazyku - neexistující dokumentace

8.2.3 Private Winten – open source

Private Writen je bezpečnostní open source nástroj, který obsahuje firewall, a sdružuje i nastavení soukromí v systému Windows 10. To je rozdělené do několika kategorií – Microsoft účet, vyhledávání, Cortana a telemetrie.

Firewall obsažený v Private Winten blokuje přístup programům k sítí, a umožní spravovat již existující pravidla v systému Windows, které většina jiných firewallů neumožňuje. Tyto programy jsou popsány svým názvem, cestou, odchozí IP adresou, portem a protokolem.

Private Winten je nástroj pomocí něhož, lze zabránit systému Windows sbírání osobních dat uživatele. Ve své podstatě neobsahuje žádné speciální funkce, ale dává uživateli možnost spravovat systémové nastavení, které je v normálním případě skryté nebo obtížně dohledatelné. Z tohoto důvodu je tento nástroj určen hlavně pro pokročilé uživatele.

Tab. 14. Silné a slabé stránky Private Winten

Silné stránky	Slabé stránky
- obsáhlé možnosti nastavení - přehledné grafické rozhraní	- pouze pro zkušené uživatele - pouze anglický jazyk - neexistuje dokumentace - existuje pouze krátkou dobu - možnost poškození neodborným zásahem uživatele do zdrojového kódu

Tab. 15. Kriteriální porovnání firewallů

Kritéria	Firewall		
	Windows Firewall	TinyWall Firewall	Private Winten
Přehlednost a jednoduchost grafického prostředí	1	1	3
Jazyk nástroje	1	1	3
Dokumentace k nástroji	1	5	5
Hardwarové nároky	1	2	3
Množství funkcí	3	2	3
Podpora dalších platforem	4	4	5
Stáří poslední vydané aktualizace (verze)	3	5	4
Medián	**1**	**2**	**3**

8.3 Zálohovací programy

Data, která jsou mnohdy cílem útoků škodlivých programů ať už z důvodu jejich kompromitace, zničení nebo využití jako subjekt pro výkupné, patří k nejcennějšímu majetku každé organizace. Není proto žádným překvapením, že bezpečnost informačních technologií velmi úzce souvisí se zálohováním dat. Je to hlavně z toho důvodu, že pokud škodlivý program úspěšně infikuje, znepřístupní nebo smaže data, stane se záloha těchto souborů jedinou možností jejich obnovy. Mezi další příčiny ztráty dat patří i selhání hardwarové (selhání harddisku, paměti, proudové přepětí) nebo softwarové (chybný zápis dat do databáze). Zálohy se využívají i v případě lidského selhání (přepis nebo smazání důležitých dat).

Výsledkem zálohování je tedy navrácení dat do stavu, v jakém byla, než došlo k jejich nechtěné změně. Zálohy by měly být umístěné odděleně od zdrojových dat, aby například v případě požáru nedošlo ke zničení zdrojových a zároveň záložních dat.

8.3.1 Duplicati 2.0 – free software

Duplicati je nástroj, který slouží k vytváření záloh s možností komprese nebo šifrování. Díky tomuto nástroji je možné vytvářet jak úplné, tak i přírůstkové zálohy. Zálohy mohou být šifrované pomocí pokročilého šifrovacího standardu AES-256 s vlastním nastavením hesla.

Oproti ostatním zálohovacím softwarům nabízí Duplicati, kromě uložení na vlastní datové uložiště zařízení, velmi rozsáhlé možnosti uložení záloh např. Microsoft OneDrive, Microsoft SharePoint, Dropbox, Google Drive, Amazon Cloud Drive apod. Samotný přenos záloh je možné realizovat i pomocí různých přenosových protokolů např. FTP, SFTP, WebDav, apod. s možností použití SSL. Do záloh je pak možné umístit jednotlivé soubory, složky, archívy nebo celé diskové oddíly. Při zálohování lze použít nejrůznější filtry, které umožní vynechat specifické složky, soubory a to na základě různě nastavitelných pravidel (velikost, název, přípona atd.). V předposledním kroku Duplicati umožní nastavit automatické spouštění záloh, a to v přesný den a hodinu.

Tab. 16. Silné a slabé stránky Duplicati 2.0

Silné stránky	**Slabé stránky**
- jednoduché grafické prostředí - podpora mnoha platforem - český jazyk prostředí - minimální hardwarové nároky - vhodné i pro méně zkušené uživatele	- dokumentace pouze v anglickém jazyce - pomalejší průběh zálohování - žádná podpora uživatelů - závislost na internetovém připojení

8.3.2 Areca Backup – open source

Areca Backup je graficky velmi jednoduchý open source nástroj určený pro zálohování obsahující i pokročilé nastavení, které nabízí pouze placený software. Areca Backup nabízí možnost vytvořit úplnou, rozdílovou nebo přírůstkovou zálohu, která může být uložena na lokálním umístění v počítači nebo prostřednictvím protokolů FTP a SFTP na vzdáleném serveru. Zálohy je možné zkomprimovat, a to díky kompresi ve formátu Zip nebo Zip 64 včetně nastavení úrovně komprese, způsobu kódování a rozdělení na části dle požadované velikosti. Šifrování záloh se provádí metodou AES 128 a to pomocí vlastního hesla nebo vygenerovaného 16 bitového klíče.

Samozřejmostí je provedení zálohy na základě pravidel zahrnující příponu souboru, výraz, umístění, velikost a datový typ. Velmi pokročilou funkcí je možnost nastavení akce před nebo po provedení zálohy. Software tak umožňuje před zálohováním například spustit skript, odstranit poslední archív nebo zaslat e-mail, a to v případě úspěchu, varování nebo chyby zálohování. Po zálohování je možné sloučit starší archivy, uložit výsledek na disk. Areca Backup zobrazuje u provedených záloh tzv. logické zobrazení, což je seznam souborů, které jsou v záloze obsaženy, včetně souborů jinak skrytých. Obsaženy jsou i statistické informace nebo jednoduchý Log. Zálohování je před spuštěním možné simulovat.

Tab. 17. Silné a slabé stránky Areca Backup

Silné stránky	Slabé stránky
- obsahuje rozšířené funkce - velmi podrobné manuály - český jazyk prostředí - podpora uživatelů - plynulost prostředí	- zastaralé grafické prostředí - již nevychází nové verze - možnost poškození neodborným zásahem uživatele do zdrojového kódu

8.3.3 Zálohování v systému Windows

Systém Windows 10 umožňuje zálohovat data dvěma základními způsoby. Prvním způsobem je zálohování pomocí tzv. historie souborů. Historie souborů umožňuje přidat jednotku např. systémovou jednotku C. Celá tato jednotka pak bude zálohována na externí disk nebo síťový disk. Nastavení související s tímto způsobem zálohování se ani zdaleka nemůže rovnat zálohovacím softwarům uvedeným výše. Nastavit lze pouze jak často má docházet k zálohování, a za jak dlouho mají být předchozí verze záloh smazány.

Druhým způsobem, jak zálohovat data, je vytvoření tzv. bitové kopie. Ta obsahuje veškerá uložená data (operační systém, aplikace, programy, datové soubory atd.) v jednom velkém komprimovaném souboru. Bitovou kopii je rovněž možné uložit na externí disk nebo disk v síti. Zálohování touto metodou trvá velmi dlouho. Na konci procesu je možné vytvořit záchranné médium. Vzhledem k tomu, že tato funkce je již součástí operačních systémů Windows, je zálohování těmito metodami nejpohodlnější, a v případě nutnosti obnovy také nejefektivnější. Postrádá však mnoho funkcí specializovaných zálohovacích nástrojů.

Tab. 18. Silné a slabé stránky Zálohování ve Windows

Silné stránky	Slabé stránky
- není nutná instalace - plná kompatibilita se systémem - přehledné prostředí - vysvětlivky funkcí v českém jazyce - není nutné jej nastavovat	- podpora pouze platformy Windows - absence pokročilých funkcí

Tab. 19. Kriteriální porovnání zálohovacích nástrojů

Kritéria	Zálohovací programy		
	Duplicati 2.0	Areca Backup	Zálohování v systému Windows
Přehlednost a jednoduchost grafického prostředí	1	3	1
Jazyk nástroje	1	1	1
Dokumentace k nástroji	3	4	1
Hardwarové nároky	1	2	2
Množství funkcí	2	1	3
Podpora dalších platforem	1	3	4
Stáří poslední vydané aktualizace (verze)	3	5	3
Medián	**1**	**3**	**2**

8.4 Šifrovací programy

Autentizace uživatelů k operačním systémům probíhá nejčastěji za použití uživatelského jména a hesla, druhořadně pak pomocí biometrie a čipových karet. Tyto metody využívají jistou funkci založenou na ověření např. hash hesla, vektorového markantu otisku prstů apod., při čemž tyto údaje jsou téměř vždy uloženy na pevném disku. Pokud není tento disk šifrovaný, nic nebrání neautorizovanému uživateli tyto autentizační data získat, a obejít tak proces autentizace. Tento problém se může vyskytnout i u jednotlivých souborů, složek, zpráv, přístupu do jednotlivých aplikací. Šifrovací nástroje se z tohoto důvodu stávají velmi užitečné a jejich použití opodstatněné.

8.4.1 BitLocker

BitLocker je šifrovací nástroj, který je součástí systému Windows již od Windows Vista a Windows Server 2008. Je určen k šifrování celých diskových oddílů nebo výměnných datových médií. K šifrování se používal algoritmus AES s využitím 128 nebo 256bitového klíče, a od vydání Windows 10 verze 1511 bezpečnější algoritmus XTS-AES. V průběhu procesu nastavení šifrování nabízí BitLocker tři různé možnosti dešifrování obsahu,

jmenovitě pak pomocí PIN kódu, USB flash disku nebo automaticky za pomocí dešifrovacího nástroje BitLockeru. V dalším kroku se vybírá způsob uložení obnovovacího klíče, který slouží jako náhrada v případě ztráty dešifrovacího klíče. Tento obnovovací klíč může mít podobu USB flash disku nebo ho lze uložit do souboru, případně vytisknout klíč na papír. BitLocker také dává na výběr, zdali má být zašifrovaný celý disk včetně prázdného místa, což zajistí, že i v budoucnu smazaná data budou zašifrovaná nebo bude zašifrována jen používaná část disku.

Tab. 20. Silné a slabé stránky BitLocker

Silné stránky	Slabé stránky
- není nutná instalace - plná kompatibilita se systémem - vysvětlivky funkcí v českém jazyce - podpora velkého množství jazyků	- nízká ochrana v porovnání s konkurenčními produkty - podpora pouze platformy Windows - absence pokročilých funkcí - složitější nastavení - méně obsažených funkcí

8.4.2 VeraCrypt – open source

VeraCrypt je open source šifrovací nástroj, který vychází z kódu populárního šifrovacího nástroje TrueCrypt, jehož provoz byl ukončen. Tento šifrovací nástroj umožňuje pokročilé šifrování souborů, složek, diskových oddílů nebo celých disků interních i externích prostřednictvím několika šifrovacích algoritmů (AES, Serpent, Twofish, Camellia a Kuzněčik) a hashovacích funkcí (SHA-512, SHA-256, Whirlpool, RIPEMD-160, STREEBOG).

Samotné šifrování souborů začíná vytvořením tzv. souborového svazku, který se připojuje stejně jako disk. Tento souborový svazek je zašifrován a slouží pro ukládání dat, v případě potřeby může být i skrytý. Následuje možnost výběru šifrovacího algoritmu a hashovací funkce a s tím spojená volba hesla, které bude sloužit pro odemknutí tohoto svazku. Určit lze i velikost a formát souborového svazku.

VeraCrypt je díky svému nastavení a způsobu šifrování velmi pokročilý nástroj, ale díky českému jazyku prostředí a obsaženým detailním popisem u každého kroku šifrování může tento nástroj využívat i méně zkušený uživatel. VeraCrypt je dostupný na všech používaných desktopových platformách (Microsoft Windows, macOS a Linux) a šifrování pomocí tohoto nástroje je považováno za velmi bezpečné.

Tab. 21. Silné a slabé stránky VeraCrypt

Silné stránky	Slabé stránky
- podpora mnoha platforem - český jazyk prostředí - stálá uživatelská podpora - považován za velmi bezpečný	- dokumentace pouze v anglickém jazyku - vhodnější pro zkušenější uživatelé - možnost poškození neodborným zásahem uživatele do zdrojového kódu

8.4.3 Gpg4win – open source

Open source software Gpg4win tvoří sada nástrojů určená pro šifrování. Kromě možnosti běžného šifrování souborů a složek je tu navíc obsažen správce certifikátů pro tzv. OpenPGP – nástroj Kleopatra, což je nejrozšířenější standard pro šifrování emailů. Šifrování emailů v nejpoužívanějším emailovém klientu MS Outlook (verze 2010 a novější) se provádí nástrojem GpgpOL, jenž je možný používat skrze doplněk (plugin). Samozřejmostí je i nástroj pro šifrování v samotném Průzkumníku Windows (File Explorer). Veškeré šifrování běží na šifrovacím jádru GnuPG, což je velmi výkonný otevřený šifrovací standard. GnuPG používá šifrovací systém založený na veřejném klíči.

Při prvotním spuštění je nutné vytvořit certifikát, který slouží k podepisování souborů, složek nebo emailů. K vytvoření certifikátu je zapotřebí zadat jméno, email a bezpečné heslo, které se zadává vždy, když potřebujeme něco podepsat nebo zašifrovat.

Gpg4win není určen pouze pro operační systém Windows, jak se může z názvu zdát, ale lze jej nainstalovat i na operační systémy MacOS X nebo Linux. Prostředí tohoto šifrovacího nástroje je v českém jazyce a je velmi přehledné. Chybí však dodatečné popisky u některých funkcí a na základě toho není vhodné pro začínající uživatele. Certifikát generovaný tímto programem, lze považovat za bezpečnou alternativu jinak placených certifikátu jako je například Post Signum.

Tab. 22. Silné a slabé stránky Gpg4win

Silné stránky	Slabé stránky
- jednoduché grafické prostředí - podpora mnoha platforem - český jazyk prostředí - obsahuje i pokročilé funkce	- dokumentace pouze v anglickém jazyku - chybí popisky funkcí - spíše pro zkušené uživatele - možnost poškození neodborným zásahem uživatele do zdrojového kódu

Tab. 23. Kriteriální porovnání šifrovacích nástrojů

Kritéria	Šifrovací programy		
	Bitlocker	VeraCrypt	Gpg4win
Přehlednost a jednoduchost grafického prostředí	1	3	4
Jazyk nástroje	1	1	1
Dokumentace k nástroji	1	3	3
Hardwarové nároky	2	1	2
Množství funkcí	4	2	1
Podpora dalších platforem	4	2	4
Stáří poslední vydané aktualizace (verze)	3	3	2
Medián	**2**	**2**	**2**

8.5 Správce hesel

Hesla jsou používána v každé organizaci, nicméně mnoho uživatelů používá jednoduchá, snadno předvídatelná hesla, jejichž prolomení není nikterak náročné. Uživatelé neberou složitost hesel velmi vážně, a často používají pro více služeb stejné heslo, které nedodržuje základní pravidla týkající se jeho délky, použití kombinací velkých písmen, číslic a symbolů.

Správce hesel obsahuje databázi, ve které je pro každou službu uloženo uživatelské jméno, heslo a další údaje. Přístup do této databáze je umožněn až po zadání tzv. primárního hesla, které slouží jako šifrovací klíč.

8.5.1 KeePass – open source

KeePass je jednoduchý nástroj pro systém Windows, který ukládá hesla do databáze chráněné primárním heslem. Celá tato databáze je šifrována pokročilou šifrovací funkcí AES nebo Twofish. Hesla je možné řadit dle vybraných složek např. internet, Windows, bankovnictví apod.

Tab. 24. Silné a slabé stránky KeePass

Silné stránky	Slabé stránky
- podpora mnoha platforem - český jazyk prostředí - mnoho dostupných pluginů	- dokumentace pouze v anglickém jazyce - zastaralý vzhled prostředí - nepřehledné prostředí - možnost poškození neodborným zásahem uživatele do zdrojového kódu

8.5.2 Padlock – open source

Padlock je správce hesel, který se od ostatních liší zejména jednoduchým a moderním vzhledem, jenž usnadňuje a zpříjemňuje uživateli práci s ním. Kromě základního třídění hesel a účtů dle kategorií, importu nebo exportu hesel, umožňuje Padlock automatické vypínání aplikace po určité době v případě nečinnosti. Další velmi užitečnou funkcí je tzv. generátor hesel, který dokáže generovat velmi silná hesla dlouhá až 50 znaků. Tato hesla jde jednoduše zkopírovat a vložit do požadované služby.

Tab. 25. Silné a slabé stránky Padlock

Silné stránky	Slabé stránky
- podpora více platforem - jednoduché a přehledné prostředí - menší hardwarová zátěž	- dokumentace pouze v anglickém jazyce - placené některé funkce - neobsahuje český jazyk - možnost poškození neodborným zásahem uživatele do zdrojového kódu.

Tab. 26. Kriteriální porovnání nástrojů pro správu hesel

Kritéria	Správce hesel	
	KeePass	Padlock
Přehlednost a jednoduchost grafického prostředí	3	2
Jazyk nástroje	1	3
Dokumentace k nástroji	4	3
Hardwarové nároky	2	2
Množství funkcí	2	4
Podpora dalších platforem	1	1
Stáří poslední vydané aktualizace (verze)	2	3
Medián	**2**	**3**

8.6 Aktualizační správci softwaru

Aktualizace softwaru je činnost, při které dochází k instalaci nejnovější verze používaného softwaru. Aktualizace se provádí z důvodu implementace nových funkcí nebo vylepšení softwaru, a hlavně z důvodu opravy programátorských chyb, které software obsahuje. Aktualizace jsou u některých druhů softwaru prováděny automaticky, jiné je třeba aktualizovat ručně. K tomuto účelu lze využít aktualizační správce softwaru.

8.6.1 SUMo – free software

SUMo (Software Update Monitor) je aktualizační správce, který na základě skenu nainstalovaného softwaru rozpozná zastaralou verzi, a nabídne aktualizaci odkazem na stažení přímo ze stránek výrobce softwaru. Nainstalovaný software je vyobrazen v přehledné tabulce, kde s ním lze provádět funkce jako: ověřit aktualizace, ignorovat aktualizace nebo ho úplně vymazat. Aktualizační správce je v českém jazyce. Vzhled prostředí je zastaralý, ale přehledný. Kontrola aktualizací probíhá vždy při spuštění aktualizačního správce. SUMo je jediný free (open source) software ve své kategorii.

Tab. 27. Silné a slabé stránky SUMo

Silné stránky	Slabé stránky
- jediný free (open source) software ve své kategorii - jednoduchá orientace v nástroji - malé hardwarové nároky - český jazyk prostředí	- zastaralé prostředí - neexistující dokumentace - žádná uživatelská podpora

8.7 Analyzér bezpečnosti operačních systémů Microsoft Windows

Microsoft Baseline Security Analyzer je speciální, volně stažitelný nástroj pro operační systémy Windows. Tento nástroj umožňuje otestovat počítač, síť nebo doménu na výskyt různých bezpečnostních nedostatků. Prováděny jsou především kontroly týkající se zranitelnosti systému, síly použitých hesel, zabezpečení webového serveru, zabezpečení databázového serveru SQL a aktualizací systému. Po provedení kontroly jsou veškeré bezpečnostní nedostatky vypsány v přehledné tabulce, která u většiny hrozeb nabízí i možnost najít vhodné opatření. Samotné prostředí nástroje je zastaralé a svými funkcemi je vhodné především pro zkušenější uživatelé. V nástroji není obsažen český jazyk. Nástroj byl vyvinut firmou Microsoft, a dokáže cíleně vyhledat bezpečnostní slabiny ve svém vlastním operačním systému. Z tohoto důvodu ho lze považovat za jedinečný.

Tab. 28. Silné a slabé stránky Microsoft Baseline Security Analyzer

Silné stránky	Slabé stránky
- jediný free software ve své kategorii - jednoduchá orientace v nástroji - malá konkurence v kategorii - plně kompatibilní se systémy Windows	- zastaralé prostředí - neexistující dokumentace - žádná uživatelská podpora - pouze pro platformy Windows

9 ZÁKLADNÍ BALÍČKY FREE A OPEN SOURCE NÁSTROJŮ PRO MALÉ A STŘEDNÍ PODNIKY

Pro kompletní zabezpečení bezpečnosti informačních technologií je na základě mnoha hrozeb, kterým podnik čelí, nutno vytvořit bezpečnostní balíky, které dokážou pokrýt většinu z nich. Jak lze vyčíst z případové studie společnosti Cisco Systems, [14] největšímu počtu hrozeb a útokům čelí koncové stanice (počítače), proto je nutné tyto zařízení zabezpečit primárně. Zajištění bezpečnosti všech informačních technologií v organizacích (servery, aktivní a pasivní síťové prvky, periferie apod.) pomocí free a open source nástrojů by značně přesáhlo rozsah určený pro bakalářskou práci. Z tohoto důvodu budou základní balíčky směřovány na ochranu počítačů. Samotný výběr balíčků je založen na statistice, dostupné na [15], z které lze vyčíst procentuální zastoupení jednotlivých operačních systémů v České republice. K 1.únoru 2019 má největší zastoupení v kategorii desktopové platformy operační systém Windows (60,36 %), konkrétně ve verzích Win10 (61,58 %), Win7 (27,46 %), Win8.1 (6,06 %), WinXP (2,19 %) a další.

9.1 Základní balíčky free a open source nástrojů pro operační systém Windows

Jedním ze základních rozlišovacích vlastností u operačních systémů Windows, ale rovněž u bezpečnostních nástrojů, jsou nároky na hardwarové zařízení.

Modelový příklad č. 1

Malá organizace (15 zaměstnanců) s místem obchodu v tuzemsku se zabývá výrobou hubek na nádobí. Pro tuto organizaci představují primární náklady nákup materiálu a podpůrných věcí určených pro výrobu hubek. Jelikož pro organizaci není prioritní ani účelné vlastnit nejnovější informační technologie, počítače jsou staršího data. Ve firmě jsou celkem tři počítače určené pro správu objednávek, vedení účetnictví a řešení obecné administrativy. Počítače pro takovou činnost vyžadují pouze minimální hardwarové nároky. Z tohoto důvodu v organizaci nevznikla potřeba zakoupit počítače nové. Hardwarové specifikace těchto počítačů obsahují pro koupi v té době typickou sestavu složenou z: operačního systému Windows 7, 2 jádrového procesoru, 2 GB paměti RAM, 250 GB HDD a periferií. Omezující specifikace podobné sestavy jsou založeny na malém výkonu hardwarových komponentů a zastaralém operačním systému Windows 7. K tomu bylo přihlédnuto i při výběru balíčku (kompletní hardwarové nároky všech vybraných nástrojů jsou obsaženy v příloze č. I).

Tab. 29. Balíček bezpečnostních nástrojů určený pro Modelový příklad č. 1

Antivirový nástroj	CalmAV / MoonSecure Antivirus
Firewall	TinyWall
Zálohovací nástroj	Areca Backup
Šifrovací nástroj	VeraCrypt
Správce hesel	Padlock
Aktualizační správce softwaru	SUMo
Analyzér bezpečnosti operačního systému	Microsoft Baseline Security Analyzer

Balíček se skládá z open source antivirového nástroje ClamAV, popřípadě lze využít i MoonSecure Antivirus, který má stejné virové jádro jako ClamAV, ale narozdíl od ClamAV nabízí jednoduché grafické rozhraní. Důvodem využití open source antivirů je v tomto případě zrušení podpory free antivirových nástrojů ze strany tvůrců, kteří tak následovali společnost Microsoft, která rovněž plánuje přestat operační systém Windows 7 z důvodu velkého stáří podporovat. Open source nástroje jsou podporovány nehledě na stáří systému, a vzhledem k jejich jednoduchému grafickému rozhraní nezatěžují tolik systém, což je důležité, jelikož počítače ve firmě obsahují málo výkonné komponenty. Ve směru malého zatížení počítačů byly vybrány i další bezpečnostní nástroje, které vyžadují pouze minimální hardwarové nároky.

Modelový příklad č. 2

Malá organizace (25 zaměstnanců) s místem obchodu v tuzemsku a Evropě, se zabývá strojní výrobou lisovacích nástrojů. Tato organizace na základě zvýšení produktivity a efektivity práce vynaloží převážnou většinu svých financí do modernizace a automatizace tvářecích strojů. V organizaci se nachází celkem pět počítačů. Dva z nich jsou určeny pro zahraniční a tuzemské vyřizování zakázek, jeden pro správu účetnictví, jeden pro obecnou administrativu, a jeden slouží konstruktérovi na vytváření 2D výkresové dokumentace. Jelikož Computer Aided Design (CAD) software pro vytváření 2D výkresů již vyžaduje větší nároky na výkon samotného počítače, jsou počítače v organizaci každých 5 let nahrazeny za novější. V současnosti jsou zde počítače, které svými parametry spadají do průměru. Operačním systémem je zde Windows 10, procesor má 2 jádra a je doprovázen 4 GB paměti RAM spolu

s 1 TB HDD a periferiemi. Taková počítačová sestava je dostatečně výkonná pro optimální běh bezpečnostních nástrojů.

Tab. 30. Balíček bezpečnostních nástrojů určený pro Modelový příklad č. 2

Antivirový nástroj pro Windows	CalmAV / MoonSecure Antivirus
Firewall	Windows Firewall
Zálohovací nástroj	Duplicati 2.0
Šifrovací nástroj	BitLocker
Správce hesel	KeePass
Aktualizační správce softwaru	SUMo
Analyzér bezpečnosti operačního systému	Microsoft Baseline Security Analyzer

Jelikož je výběr free a open source antivirových programů velmi omezen, byl znova vybrán ClamAV nebo MoonSecure Antivirus. Jako zálohovací nástroj byl vybrán Duplicati, jenž nabízí v porovnání s dalšími free a open source nástroji rozsáhlé možnosti nastavení a funkcí. Pro zálohování, vzhledem k menší velikosti organizace, bude šifrovací nástroj BitLocker implementovaný v systému Windows plně dostačující.

Modelový příklad č. 3

Středně velká organizace (60 zaměstnanců) s místem obchodu v tuzemsku, Evropě a Americe se zabývá výrobou zahradních traktorů. Kromě běžných nákladů spojených s nákupem materiálu, polotovarů a dílů rovněž musí své výrobky prezentovat formou reklamních obrázků, kampaní a krátkých reklamních spotů. V organizaci se nachází celkem třináct počítačů. Tři z nich jsou určeny pro vyřizování tuzemských, evropských a amerických zakázek, jeden pro vedení účetnictví a jeden pro administrativní záležitosti. Pět počítačů je určeno pro vytváření, úpravy a střih natočených videí a reklamních spotů, editací a vytváření obrázků a jejich použití v katalozích a reklamních letáků organizace. Zbylé tři slouží konstruktérům pro tvorbu 2D a 3D dílenských objektů, a pro provádění simulací výrobních procesů. Na výkon komponentů těchto počítačů se kladou vysoké požadavky, proto je nutné udržovat počítače z hlediska komponentů stále aktuální. Z tohoto důvodu jsou počítače vždy po maximálně třech letech vyměněny za nové. V současnosti tyto počítače obsahují Windows 10, procesor se 4 jádry, 8 GB paměti RAM, SSD a HDD disky s periferiemi. Podobná počítačová sestava nemá žádný limit, co se výkonnosti a stáří operačního systému týče.

Tab. 31. Balíček bezpečnostních nástrojů určený pro Modelový příklad č. 3

Antivirový nástroj	Windows Defender
Firewall	Private Winten
Zálohovací nástroj	Zálohování systému Windows
Šifrovací nástroj	Gpg4win
Správce hesel	Keepass
Aktualizační správce softwaru	SUMo
Analyzér bezpečnosti operačního systému	Microsoft Baseline Security Analyzer

Problém velkého množství počítačů spočívá ve vyšší pravděpodobnosti vzniku hrozby, proto byl jako antivirus použit Windows Defender, který se se svými funkcemi a ochranou může rovnat placené konkurenci. Tento antivirus rovněž nabízí aktualizace na denní bázi. Jako firewall je použit implementovaný systémový firewall obohacen o funkce, které nabízí Private Winten, který je účinný a díky podpoře Microsoftu spolehlivý. Organizace má velké množství odběratelů po celém světě, to znamená, že denně rozešle několik emailů, které mohou obsahovat například důležité kupní smlouvy či vnitropodnikové informace. Z tohoto důvodu je v balíčku obsažen pokročilý šifrovací nástroj Gpg4win, který kromě šifrování emailů a jednotlivých souborů, zašifruje i celé disky.

ZÁVĚR

Hlavním cílem této práce bylo vytvořit analýzu free a open source nástrojů zaměřených na bezpečnost informačních technologií. Na základě těchto analýz pak vytvořit modelové příklady, a sestavit bezpečnostní balíčky nástrojů určených pro malé a střední podniky.

Bakalářská práce je rozdělena na dvě základní části. Teoretická část se věnovala hlavně popisu problematiky tématu. Na začátku bylo nutné objasnit význam bezpečnosti v oblasti informačních technologií a základní pojmy, které se v práci dále vyskytovaly, a které byly pro další pochopení klíčové. Druhá kapitola nazvaná jako bezpečnostní politika popisuje způsob, dle kterého se podniky v rámci bezpečnosti informací řídí. V kapitole jsme si popsali nejdůležitější právní předpisy a technické normy, které jsou pro tuto oblast stanoveny. Dále bylo vysvětleno základní dělení bezpečnostních funkcí v informačních technologií podniku, což nám pomohlo lépe pochopit následující část bakalářské práce zabývající se bezpečnostními mechanismy. Rovněž jsme objasnili i základní funkci a účel kryptografických bezpečnostních mechanismů používaných u některých dále popisovaných nástrojů. Na závěr teoretické části jsme se věnovali popisu hrozeb a také opatřením, které proti těmto hrozbám existují a jsou použity v praktické části.

Praktická část bakalářské práce je zaměřena hlavně na free a open source nástroje. Jejich výběr spočíval v postupném nainstalování a odzkoušení několika nástrojů z každé kategorie. Na základě toho byly jednotlivě popsány, analyzovány a srovnány, dle předem stanovených kritérii. Z těchto nástrojů pak byly vytvořeny základní bezpečnostní balíčky free a open source nástrojů pro malé a střední podniky, čímž byl naplněn hlavní cíl práce.

Tato práce by mohla pomoci zlepšit bezpečnost informačních technologií v podnicích, které nemají dostatečné finance na zakoupení komerčních bezpečnostních nástrojů. Myslím si, že mnohé volně dostupné nástroje nabízí podobnou ochranu jako nástroje komerční. Avšak existují i určitá negativa spojená s bezplatným řešením. Pokud se podnik rozhodne k pořízení placeného bezpečnostního balíku, obvykle je jeho součástí i uživatelská podpora. Naproti tomu při používání free a open source nástrojů není tato služba ve většině případech dostupná a uživatelé si tak musí poradit sami. Další nevýhoda používání free a open source nástrojů spočívá ve skutečnosti, že některé tyto nástroje obsahují různé nevyžádané rozšíření, které se instaluje spolu se samotným nástrojem, a uživatele při práci obtěžuje například vytvářením reklam, které pomáhají tvůrcům nástrojů vydělat peníze. V případě pořízení free a open source nástrojů je vhodné znát i tato negativa.

SEZNAM POUŽITÉ LITERATURY

[1] JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 978-80-7454-312-8. Dostupné také z: http://hdl.handle.net/10563/25821.

[2] KAFKA, Milan. Význam ochrany a bezpečnosti IS-IT pro konkurenceschopnost podniku Zlín: Univerzita Tomáše Bati ve Zlíně, 2011, 36 s. Teze disertační práce. ISBN 978-80-7454-036-3.

[3] ŠTĚDROŇ, Bohumír. Open Source software ve veřejné správě a soukromém sektoru. Praha: Grada, 2009, 124 s. Průvodce. ISBN 978-80-247-3047-9.

[4] ŠÍR, Ivo. Možnosti využití technologií Open Source a Free Software v malých a středních podnicích. (online). Vysoká škola ekonomická v Praze, 2004 Dostupné z: .www.cssi.cz/cssi/system/files/all/SI_04_3_sir.pdf

[5] ŠTEC, Zdeněk. Open source software a jeho využití ve výuce tvorby webových stránek v sekundárním vzdělávání. (online). Olomouc, 2013. Dostupné z: https://theses.cz/id/6jbqak/00174154-374415625.pdf

[6] MACÁK, Petr. Kritéria výběru software pro malé a středně velké společnosti. Systémová integrace, 2011, ročník 18, číslo 1, str. 121-133, ISSN 1210-9479

[7] ČANDÍK, Marek. Základy informační bezpečnosti. Zlín: Univerzita Tomáše Bati, 2004, 107 s. Učební texty vysokých škol. ISBN 8073182181.

[8] ŠULC, Vladimír. Vybrané aspekty bezpečnosti informačních systémů. Právo-Bezpečnost-Informace[online]. 2018, 2018(2017), 11-14 [cit. 2019-01-10]. Dostupné z: http://www.teorieib.cz/pbi/files/344-SuCa.pdf

[9] KODL, Jindřich a Vladimír SMEJKAL. BEZPEČNOST ICT A OCHRANA DAT [online]. Olomouc, 2018 [cit. 2019-02-01]. Dostupné z: https://mvso.cz/wp-content/uploads/2018/02/Bezpe%C4%8Dnost-ICT-a-ochrana-dat-studijn%C3%AD-text.pdf. Studijní opora pro kombinované studium. Moravská vysoká škola Olomouc, o. p. s.

[10] HANÁČEK, Petr a Jan STAUDEK. Bezpečnost informačních systémů [online]. Praha, 2000 [cit. 2019-01-20]. Dostupné z: http://media0.vesele.info/files/media0:50f8645ae2040.pdf.upl/uvis_bezpecnost_20000701.pdf. Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií.

[11] SOMSEDIK, Jan. Zabezpečení informačního systému v podniku [online]. Praha, 2014 [cit. 2019-02-14]. Dostupné z: https://is.am-bis.cz/th/y7tmx/JAN_SOMSEDIK_.pdf. Diplomová práce. Bankovní institut vysoká škola Praha.

[12] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. Expert. ISBN 978-80-247-4644-9.

[13] HÁK, Igor. Moderní počítačové viry [online]. Třetí vydání. 2005 [cit. 2019-04-14]. Dostupné z: https://viry.cz/download/kniha.pdf

[14] Cisco [online]. [cit. 2019-02-13]. Dostupné z: https://www.cisco.com/c/en/us/products/security/security-reports.html?CCID=cc000160&DTID=esootr000515&OID=wprsc011272#~2019%20Threat%20Report

[15] Operating System Market Share Worldwide. Statcounter Global Stats [online]. [cit. 2019-02-20]. Dostupné z: http://gs.statcounter.com/os-market-share

[16] Jak se bránit zneužívání zranitelných míst IT. SystemOnLine [online]. [cit. 2019-03-01]. Dostupné z: https://www.systemonline.cz/it-security/jak-se-branit-zneuzivani-zranitelnych-mist-it.htm

[17] Firewally. Antivirové Centrum [online]. [cit. 2019-03-01]. Dostupné z: https://www.antivirovecentrum.cz/firewally.aspx

[18] K čemu je SIEM?. SystemOnLine [online]. [cit. 2019-03-14]. Dostupné z: https://www.systemonline.cz/it-security/k-cemu-je-siem.htm

[19] Trendy kybernetické bezpečnosti v roce 2018. SystemOnLine [online]. [cit. 2019-03-16]. Dostupné z: https://www.systemonline.cz/it-security/trendy-kybernetickebezpecnosti-v-roce-2018.htm

[20] APT je jen další buzzword. Clever And Smart [online]. [cit. 2019-03-20]. Dostupné z: https://www.cleverandsmart.cz/apt-je-jen-dalsi-buzzword/

[21] Bezpečnost malých a středních podniků. SystemOnLine [online]. [cit. 2019-04-01]. Dostupné z: https://www.systemonline.cz/it-security/bezpecnost-malych-a-strednich-podniku.htm

[22] Úvod do kryptografie. Earchivace.cz [online]. [cit. 2019-04-08]. Dostupné z: http://www.earchivace.cz/technologie/uvod-do-kryptografie/

[23] Pharming. IT Slovník.cz [online]. [cit. 2019-04-22]. Dostupné z: https://it-slovnik.cz/pojem/pharming

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
RSA	Rivest, Shamir, Adleman
DSA	Digital Signature Algorithm
MD5	Message-Digest algorithm
DSS	Digital Signature Standard
SHS	Secure Hash Standard
HTTPS	Hypertext Transfer Protocol Secure
SSL	Secure Sockets Layer
TLS	Transport Layer Security
EXE	Executable
LAN	Local Area Network
NAS	Network Attached Storage
IoT	Internet of Things
ERP	Enterprise Resource Planning
CRM	Customer relationship management
GDPR	General Data Protection Regulation
SQL	Structured Query Language
CAD	Computer Aided Design
RAM	Random-Access-Memory
SSD	Solid State Drive
HDD	Hard Disk Drive

SEZNAM OBRÁZKŮ

Obr. 1. Rozdíl mezi symetrickým a asymetrickým šifrováním [22] 19
Obr. 2. Schématické rozdělení licencování [5, st. 11] 29

SEZNAM TABULEK

Tab. 1. Stupnice kritéria přehlednosti a jednoduchosti grafického prostředí 35
Tab. 2. Stupnice kritéria jazyků nástrojů 35
Tab. 3. Stupnice kritéria dokumentace k nástrojům 36
Tab. 4. Stupnice kritéria hardwarových nároků na systém 36
Tab. 5. Stupnice kritéria pro množství obsažených funkcí v nástroji 37
Tab. 6. Stupnice kritéria pro počet podporovaných platforem 37
Tab. 7. Stupnice kritéria pro bezpečnost z hlediska poslední vydané aktualizace 37
Tab. 8. Silné a slabé stránky Windows Defender 39
Tab. 9. Silné a slabé stránky ClamAV 40
Tab. 10. Silné a slabé stránky MoonSecure Antivirus 40
Tab. 11. Kriteriální porovnání antivirových nástrojů 41
Tab. 12. Silné a slabé stránky Windows Firewall 42
Tab. 13. Silné a slabé stránky TinyWall Firewall 43
Tab. 14. Silné a slabé stránky Private Winten 43
Tab. 15. Kriteriální porovnání firewallů 44
Tab. 16. Silné a slabé stránky Duplicati 2.0 45
Tab. 17. Silné a slabé stránky Areca Backup 46
Tab. 18. Silné a slabé stránky Zálohování ve Windows 46
Tab. 19. Kriteriální porovnání zálohovacích nástrojů 47
Tab. 20. Silné a slabé stránky BitLocker 48
Tab. 21. Silné a slabé stránky VeraCrypt 49
Tab. 22. Silné a slabé stránky Gpg4win 49
Tab. 23. Kriteriální porovnání šifrovacích nástrojů 50
Tab. 24. Silné a slabé stránky KeePass 51
Tab. 25. Silné a slabé stránky Padlock 51
Tab. 26. Kriteriální porovnání nástrojů pro správu hesel 52
Tab. 27. Silné a slabé stránky SUMo 53
Tab. 28. Silné a slabé stránky Microsoft Baseline Security Analyzer 53
Tab. 29. Balíček bezpečnostních nástrojů určený pro Modelový příklad č. 1 55
Tab. 30. Balíček bezpečnostních nástrojů určený pro Modelový příklad č. 2 56
Tab. 31. Balíček bezpečnostních nástrojů určený pro Modelový příklad č. 3 57

SEZNAM PŘÍLOH

Příloha PI Minimální hardwarové nároky jednotlivých nástrojů

Příloha PII Ukázky grafického prostředí jednotlivých bezpečnostních nástrojů

PŘÍLOHA P I: MINIMÁLNÍ HARDWAROVÉ NÁROKY JEDNOTLIVÝCH NÁSTROJŮ

Windows Defender

Operační systém: Windows 10, 8.1, 8, 7 nebo Vista

Procesor: 2 jádrový

RAM: 1 GB

Volné místo na pevném disku: implementováno v systému Windows

ClamAV

Operační systém: Windows 10, 8.1, 8, 7, Vista, XP, ME, 2000, 98, Windows Server 2012, 2008, 2003

Procesor: 2 jádrový (minimálně Intel Pentium 2)

RAM: 64 MB

Volné místo na pevném disku: 320 MB

MoonSecure Antivirus

Operační systém: Windows 10, 8.1, 8, 7, Vista, XP

Procesor: 2 jádrový (minimálně Intel Pentium 2)

RAM: 64 MB

Volné místo na pevném disku: 320 MB

Windows Firewall

Operační systém: Windows 10, 8.1, 8, 7, Vista, XP

Procesor: 2 jádrový (minimálně Intel Pentium 2)

RAM: 64 MB

Volné místo na pevném disku: implementováno v systému Windows

TinyWall Firewall

Operační systém: Windows 10, 8.1, 8, 7 nebo Vista

Procesor: 2 jádrový

RAM: 1 GB

Volné místo na pevném disku: 500 MB

Private Winten

Operační systém: Windows 10

Procesor: 2 jádrový

RAM: 1 GB

Volné místo na pevném disku: 16 GB

Duplicati

Operační systém: Windows 10, 8.1, 8, 7, Vista, XP

Procesor: 2 jádrový (minimálně Intel Pentium 2)

RAM: 64 MB

Volné místo na pevném disku: 320 MB

Areca Backup

Operační systém: Windows 10, 8.1, 8, 7, Vista, XP

Procesor: 2 jádrový

RAM: 1 GB

Volné místo na pevném disku: 1 GB

BitLocker

Operační systém: Windows 10, 8.1, 8, 7, Vista

Procesor: 2 jádrový

RAM: 512 MB

Volné místo na pevném disku: implementováno v systému Windows

VeraCrypt

Operační systém: Windows 10, 8.1, 8, 7, Vista, XP, Windows Server 2012, 2008, 2003

Procesor: 2 jádrový

RAM: 64 MB

Volné místo na pevném disku: 1 GB

Gpg4win

Operační systém: Windows 10, 8.1, 8, 7

Procesor: 2 jádrový

RAM: 1 GB

Volné místo na pevném disku: 1 GB

KeePass

Operační systém: Windows 10, 8.1, 8, 7, Vista

Procesor: 2 jádrový

RAM: 1 GB

Volné místo na pevném disku: 1 GB

Padlock

Operační systém: Windows 10, 8.1, 8, 7, Vista

Procesor: 2 jádrový

RAM: 1 GB

Volné místo na pevném disku: 1 GB

SUMo

Operační systém: Windows 10, 8.1, 8, 7, Vista, XP

Procesor: 2 jádrový

RAM: 1 GB

Volné místo na pevném disku: 1 GB

Microsoft Baseline Security Analyzer

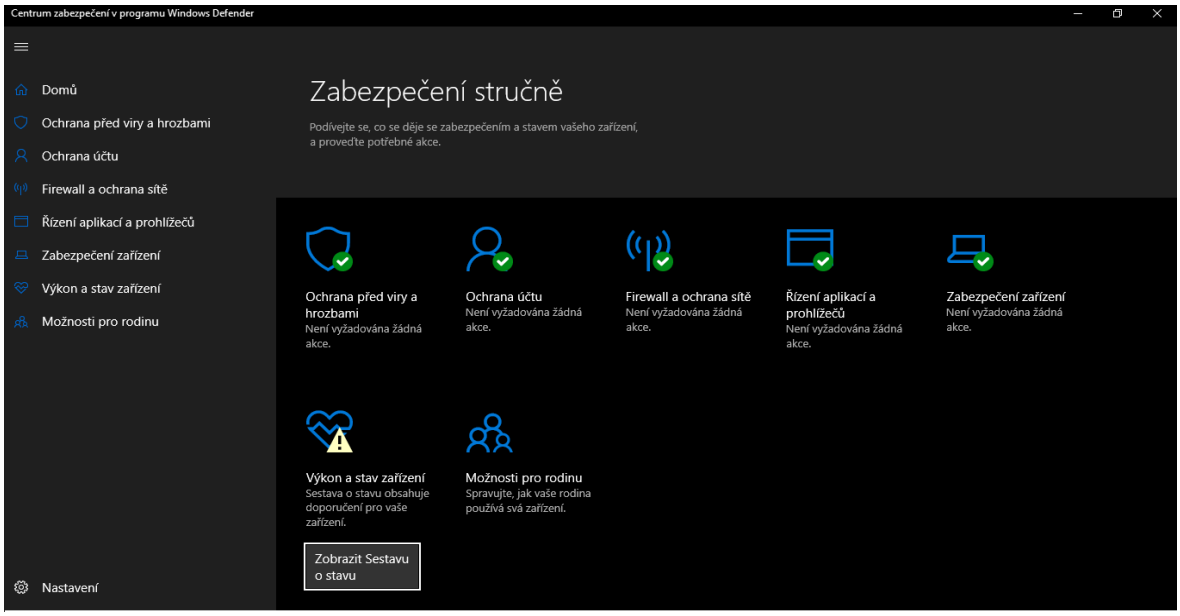
Operační systém: Windows 10, 8.1, 8, 7, Vista, XP

Procesor: 2 jádrový

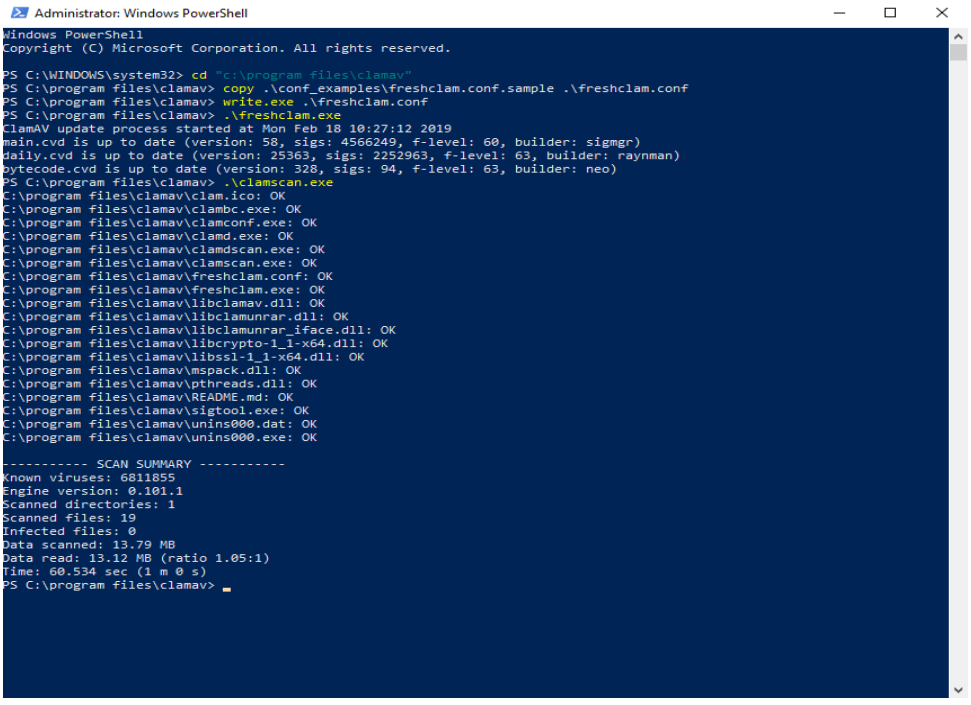
RAM: 1 GB

Volné místo na pevném disku: 1 GB

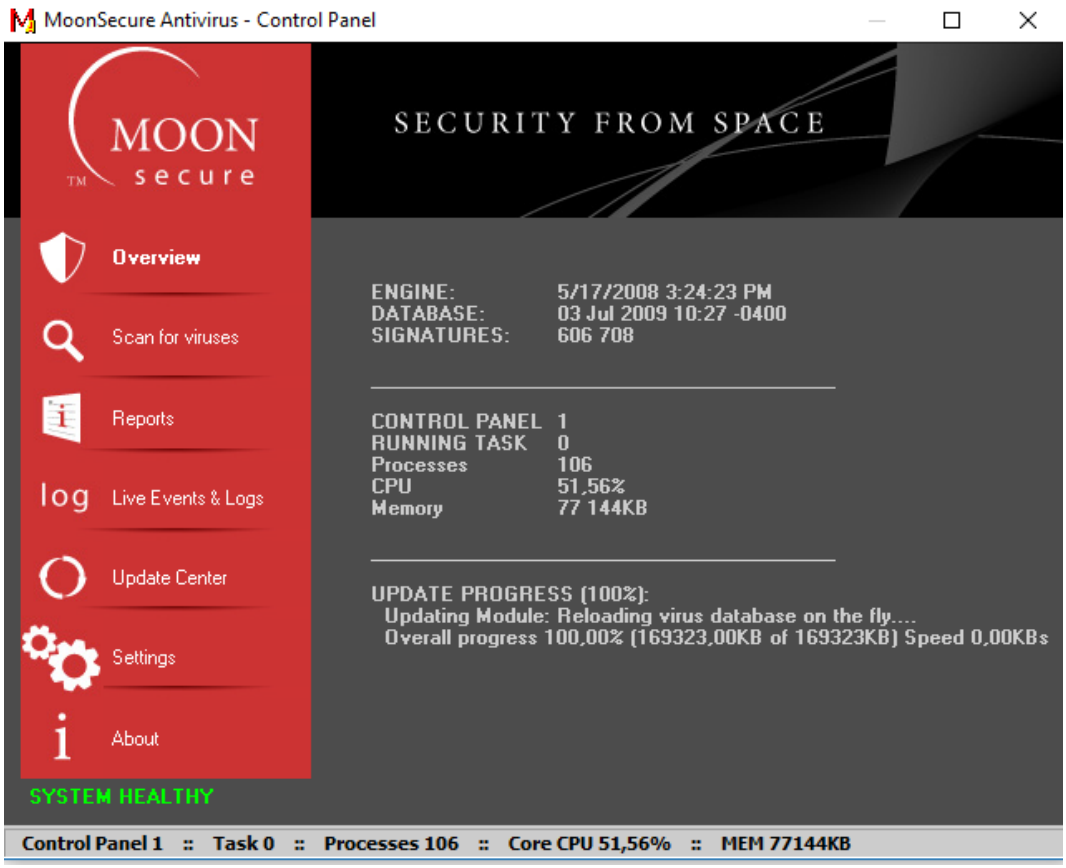
PŘÍLOHA P II: UKÁZKY GRAFICKÉHO PROSTŘEDÍ JEDNOTLIVÝCH BEZPEČNOSTNÍCH NÁSTROJŮ



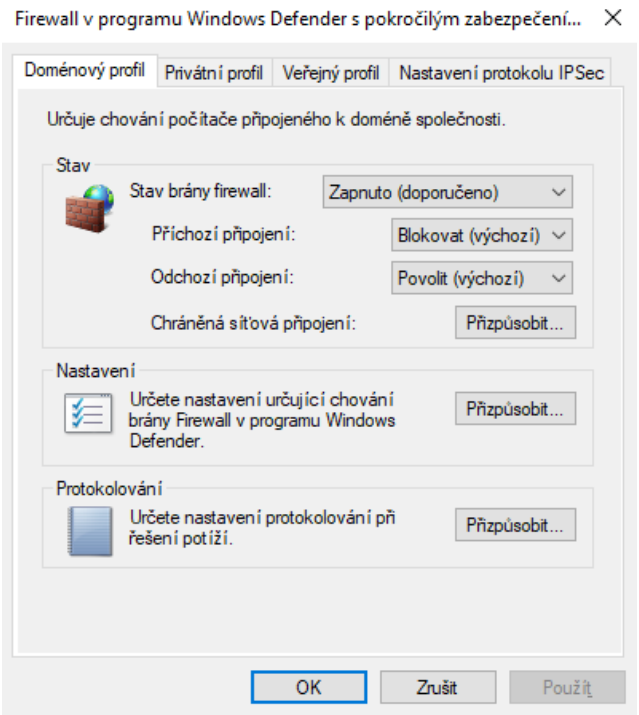
Prostředí Windows Defender



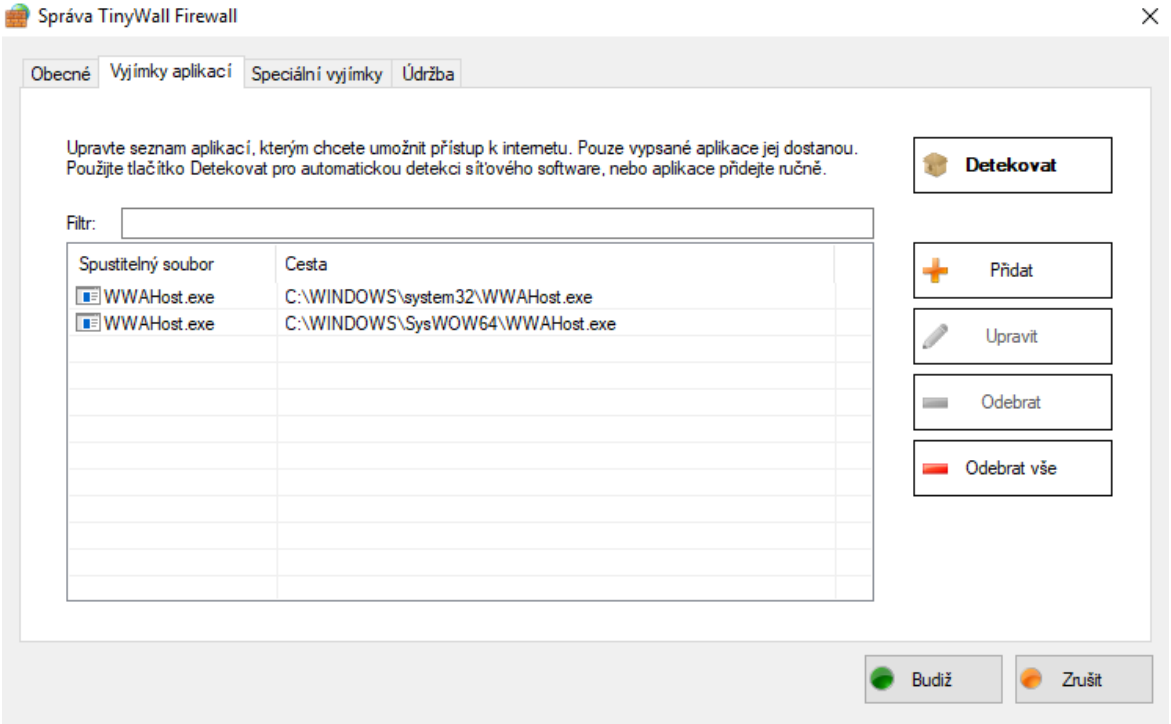
Prostředí ClamAV



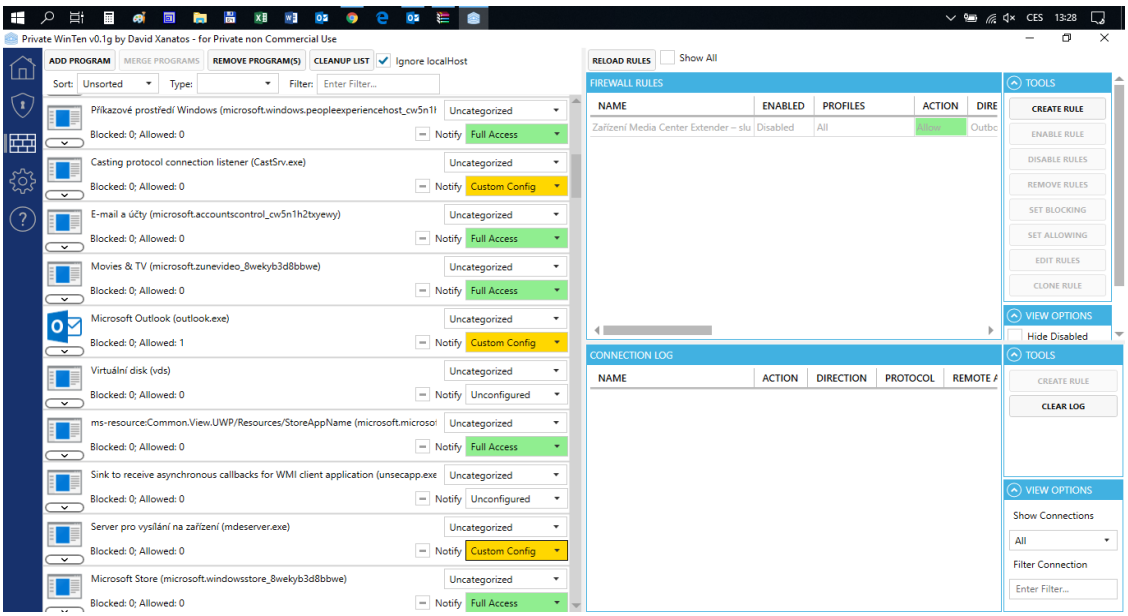
Prostředí MoonSecure Antivirus



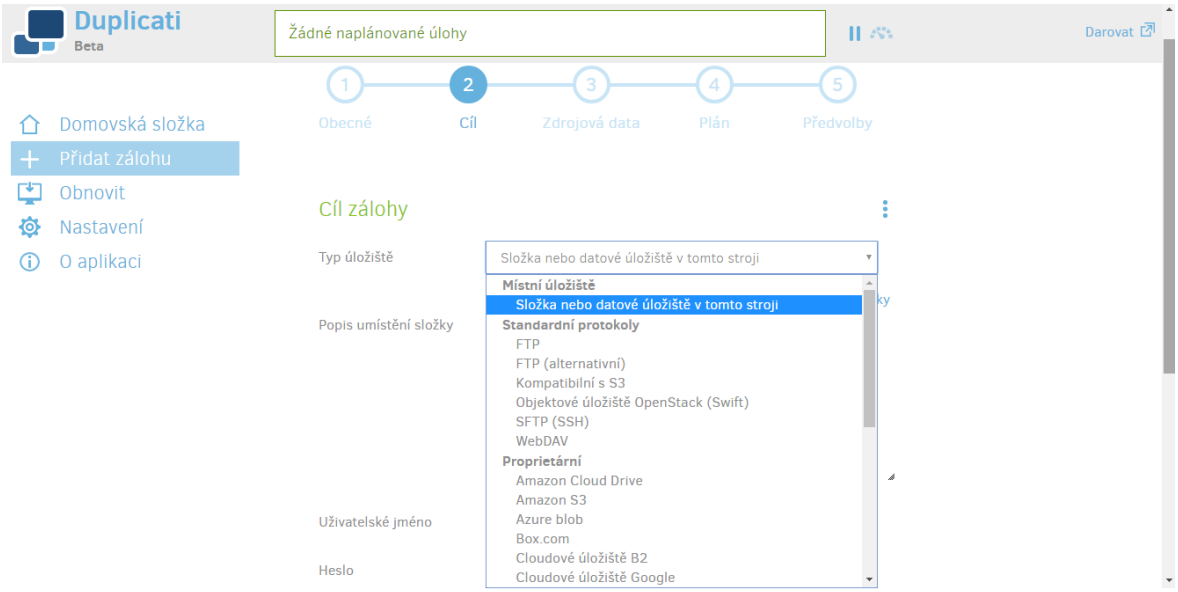
Prostředí Windows Firewall



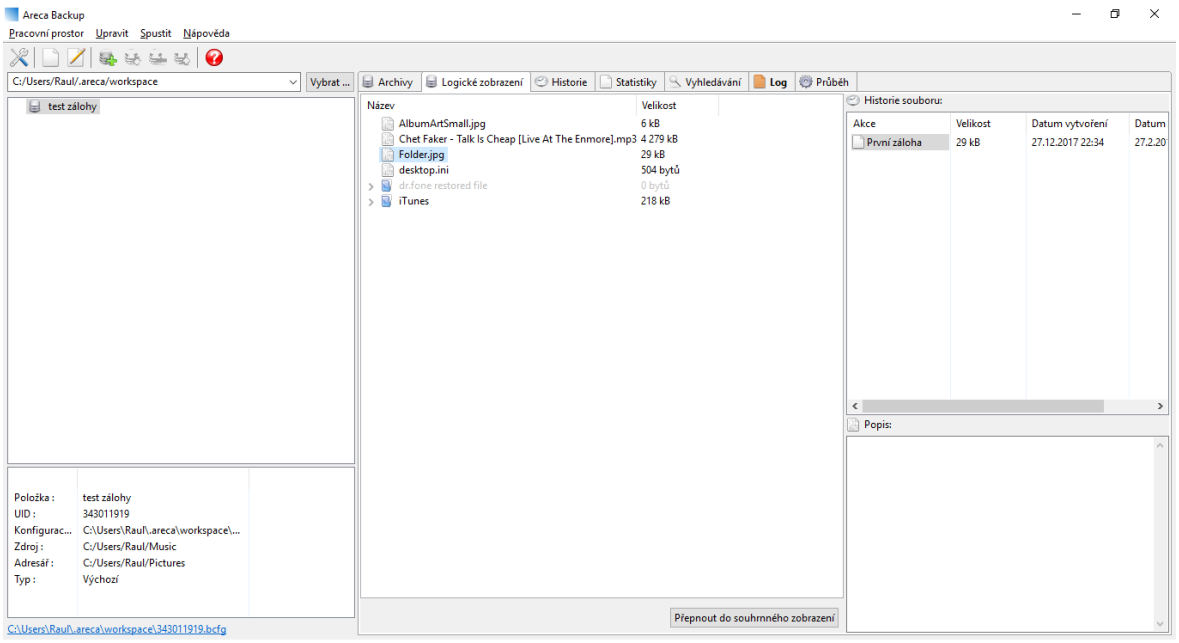
Prostředí TinyWall Firewall



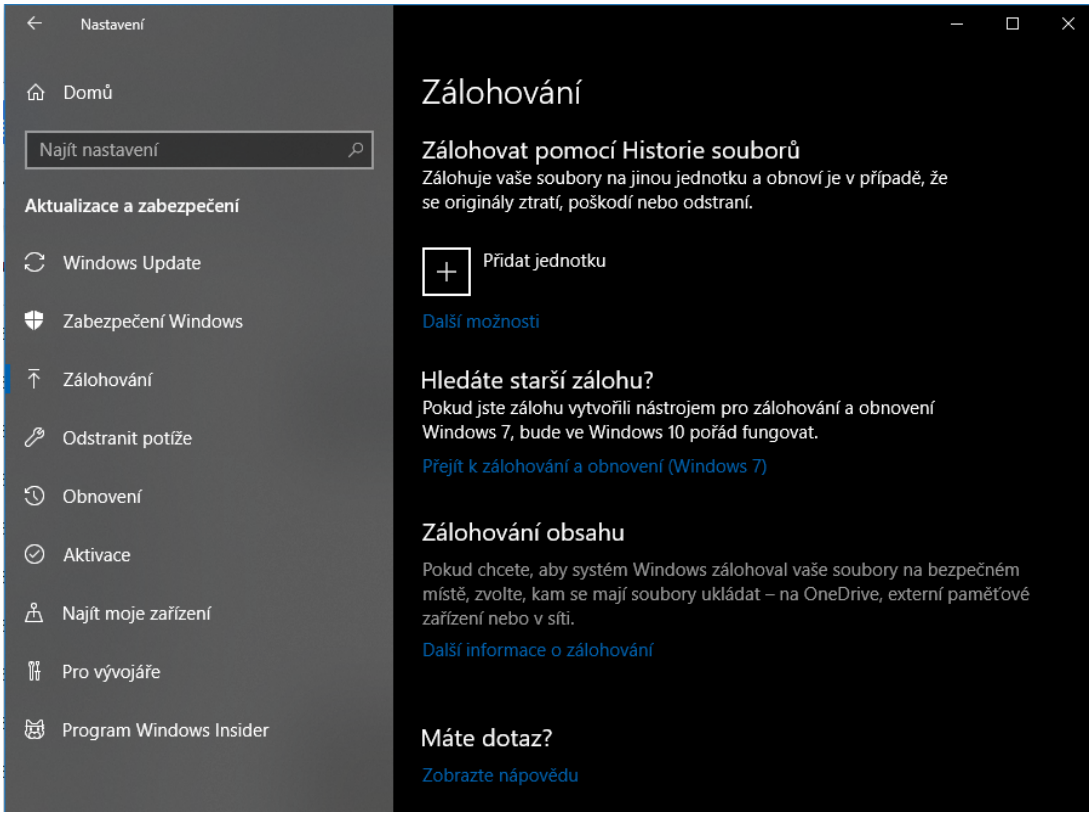
Prostředí Private Winten



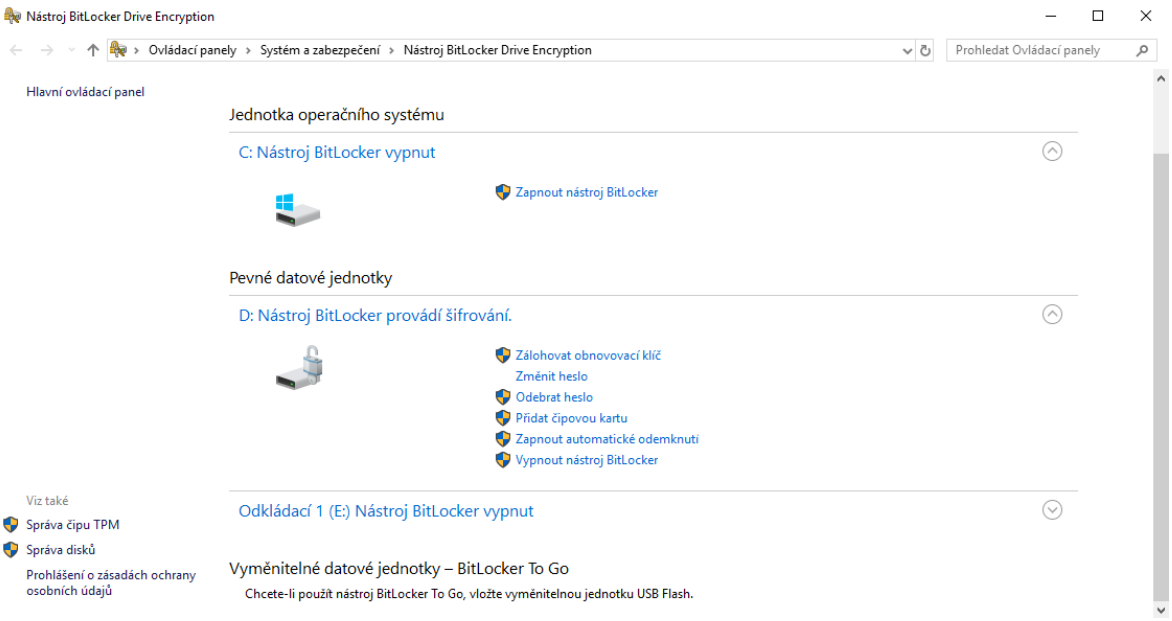
Prostředí Duplicati 2.0



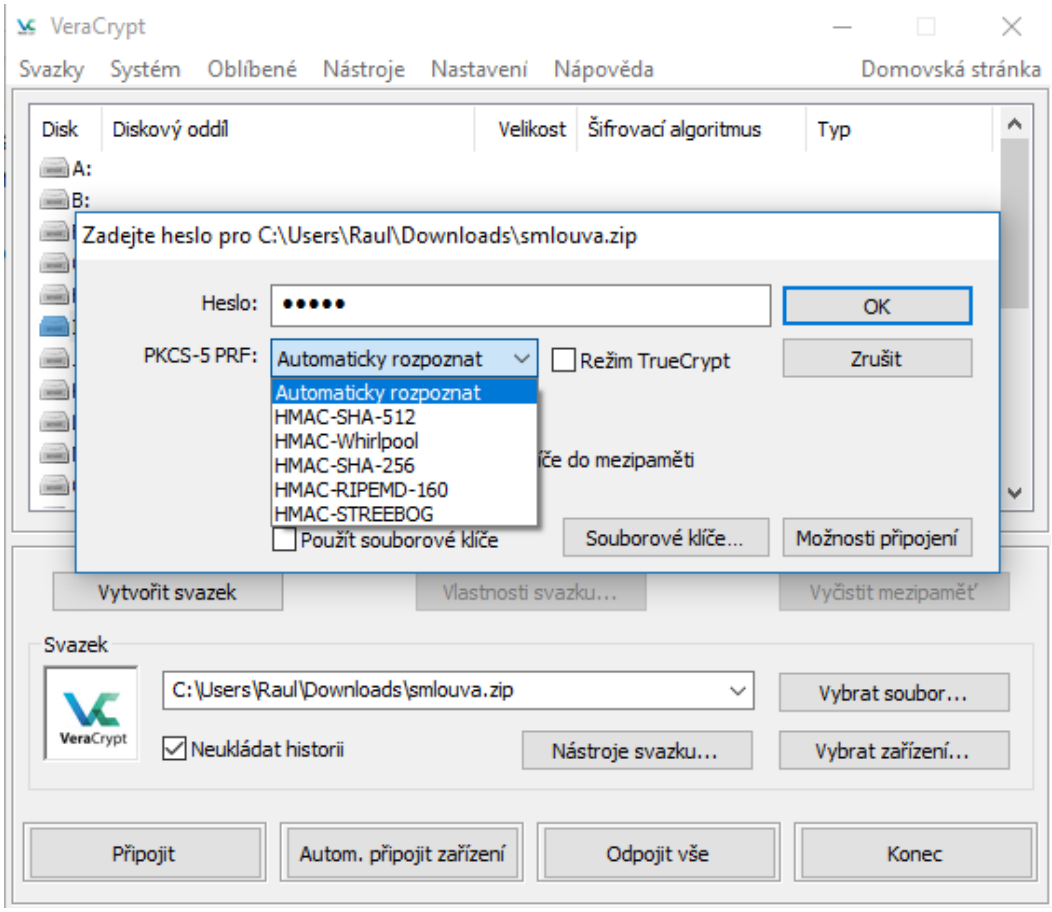
Prostředí Areca Backup



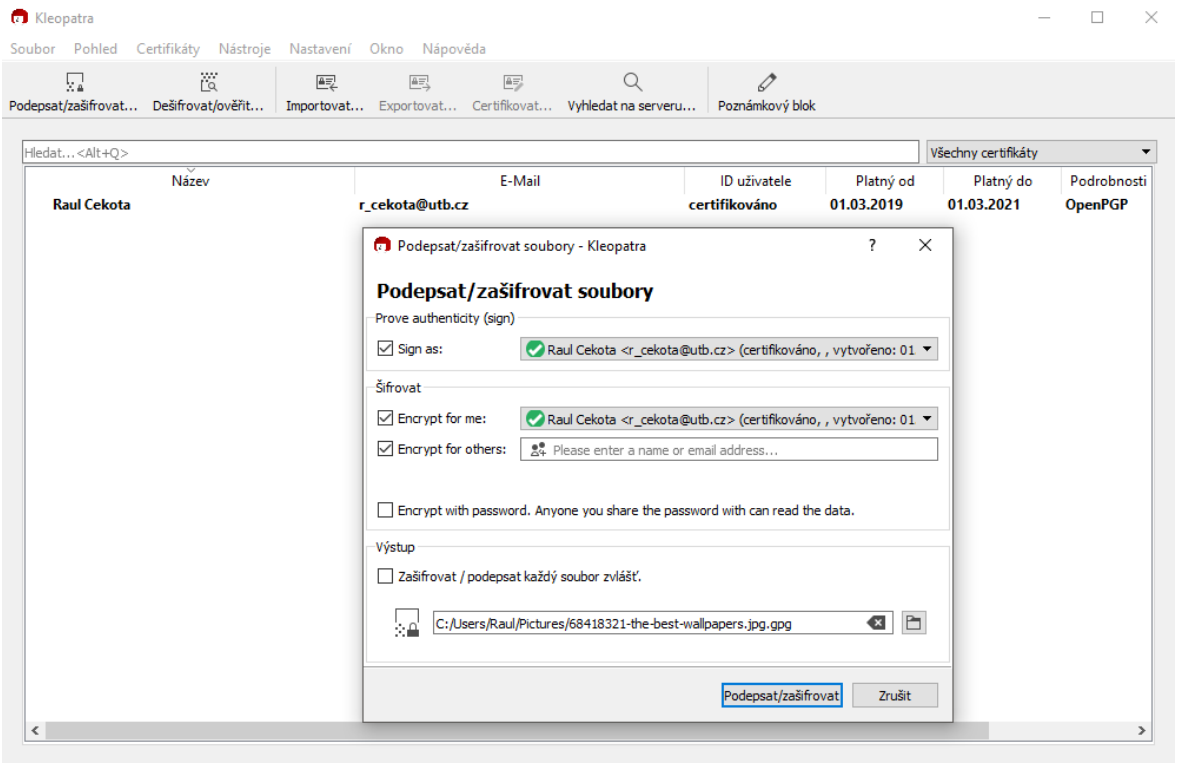
Prostředí zálohování ve Windows



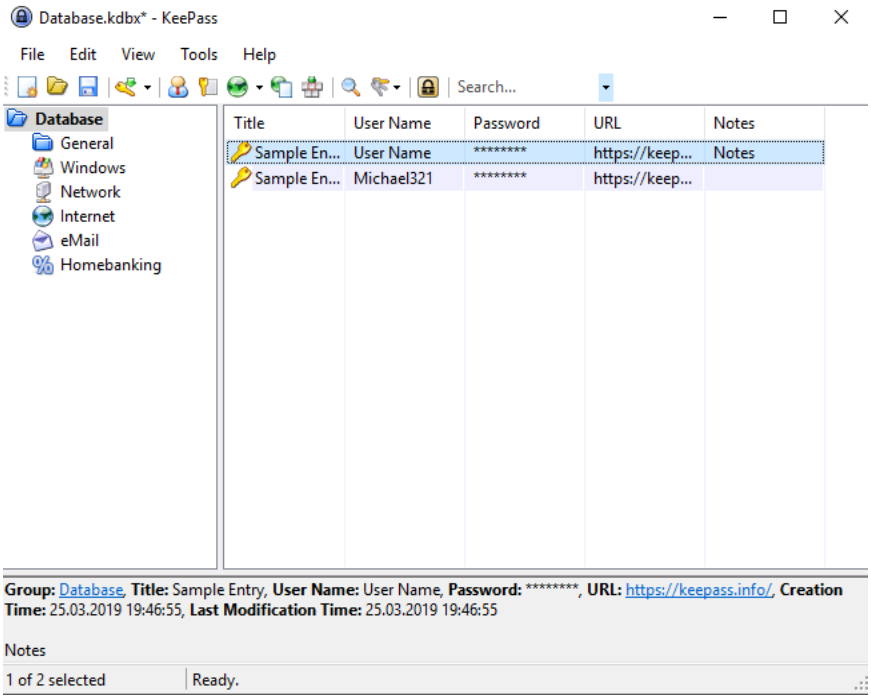
Prostředí BitLocker



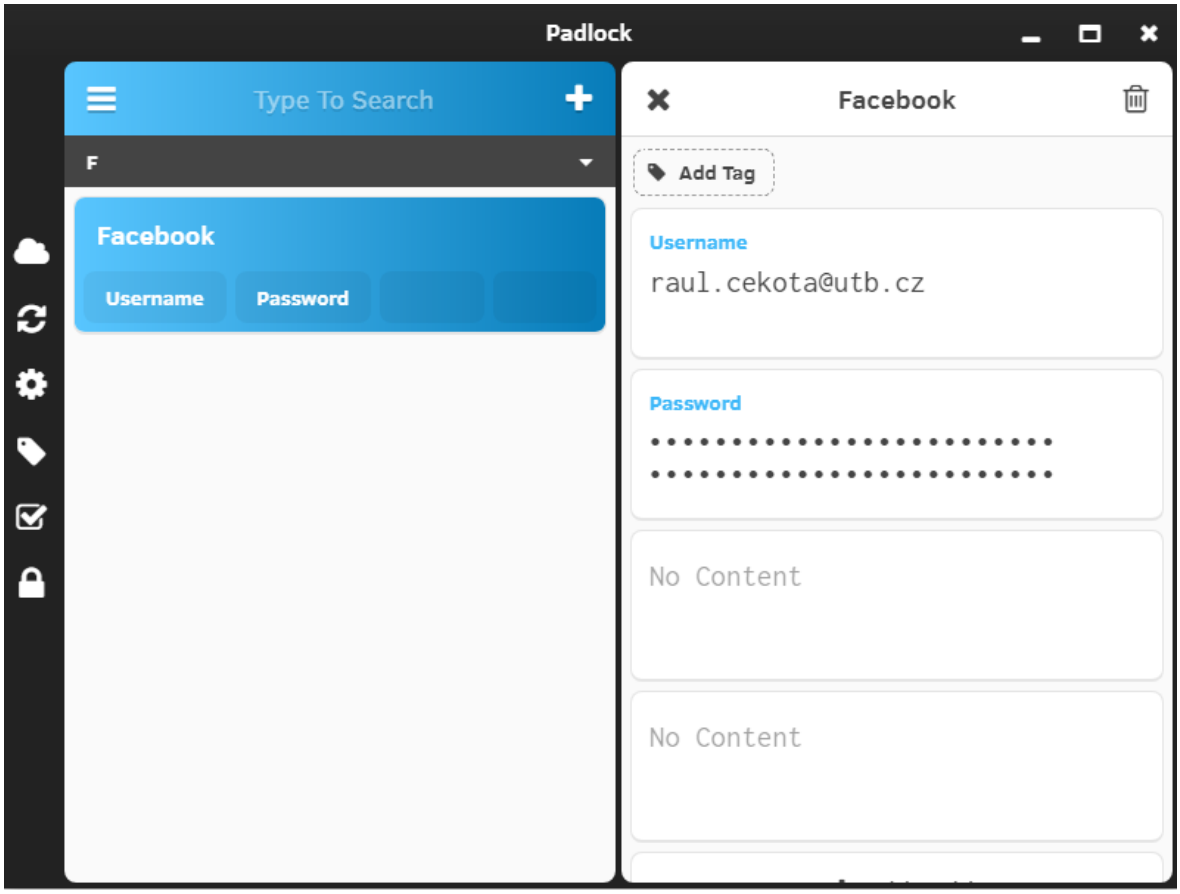
Prostředí VeraCrypt



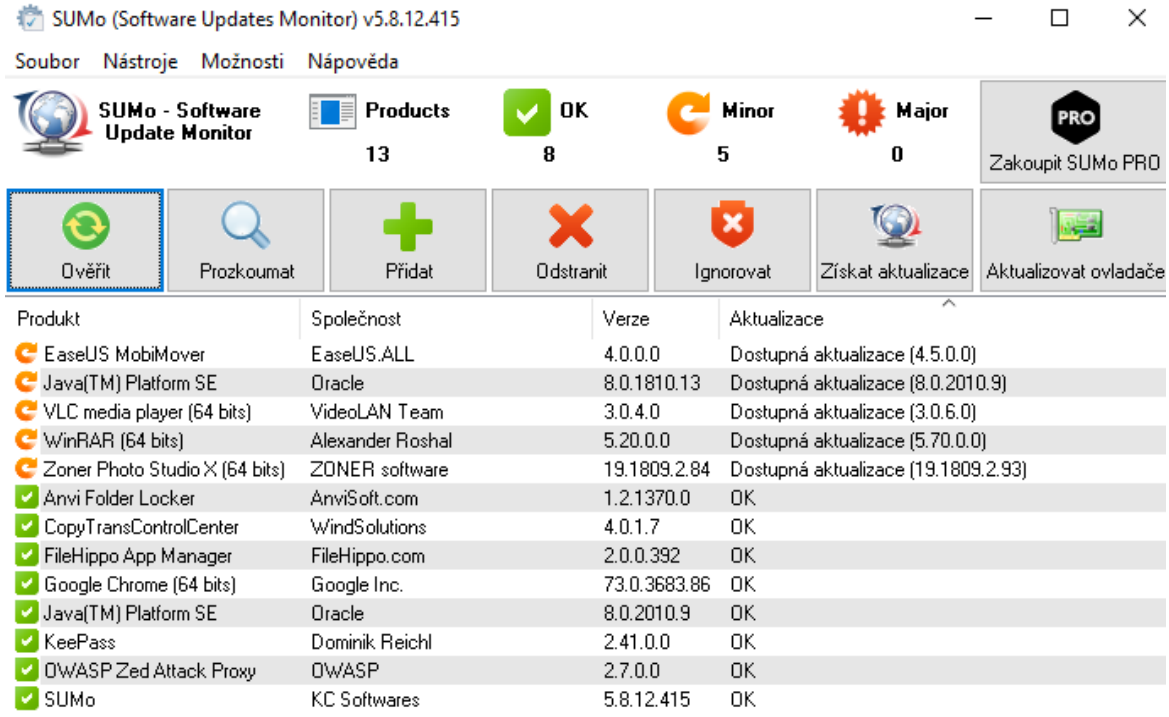
Prostředí Gpg4win



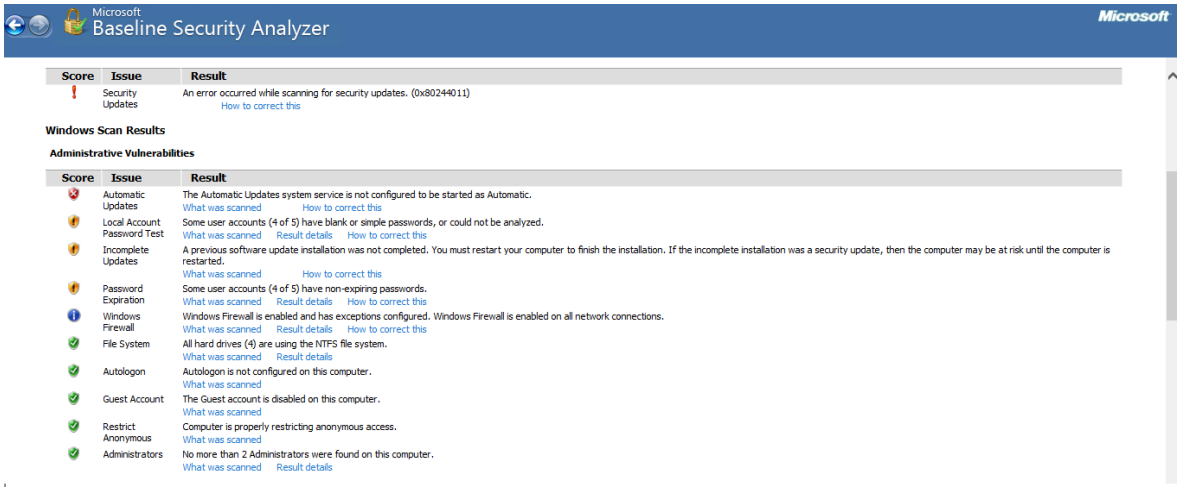
Prostředí Keepass



Prostředí Padlock



Prostředí SUMo



Prostředí Microsoft Baseline Security Analyzer