VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

SYSTÉMOVÉ ŘEŠENÍ BEZPEČNOSTI INFORMACÍ V ORGANIZACI

SYSTEMATIC SOLUTION FOR INFORMATION SECURITY IN ORGANISATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Jan Palička**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Jan Palička**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Systémové řešení bezpečnosti informací v organizaci

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Pro vybranou organizaci na základě analýzy vypracujte metodický postup pro zavedení ISMS.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17.

V Brně, dne 28. 2. 2017

doc. RNDr. Bedřich Půža, CSc.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

Abstrakt

Tato diplomová práce zpracovává problematiku zavedení ISMS ve společnosti Netcope Technologies, a. s., která se věnuje výrobě síťových karet pro vysokorychlostní akceleraci. Práce je rozdělena na dvě logické části. V první části je uveden teoretický základ práce, včetně vybraných metod pro zavedení bezpečnosti informací. Ve druhé části potom analýza společnosti a navrhovaná opatření.

Abstract

This diploma thesis deals with ISMS implementation in Netcope Technologies, a. s., which is involved in the production of network cards for high speed acceleration. This thesis is divided into two logical parts. In the first part the theoretical basis information is presented, including selected methods for implementing information security. In the second part, the analysis of the company and the proposed measures are presented.

Klíčová slova

ISMS, informační bezpečnost, analýza rizik, hrozby, opatření, ČSN ISO/IEC 27000, ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, ČSN ISO/IEC 27005.

Keywords

ISMS, Information Security, risk analysis, threads, measures, ČSN ISO/IEC 27000, ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, ČSN ISO/IEC 27005.

Bibliografická citace práce

PALIČKA, Jan. *Systémové řešení bezpečnosti informací v organizaci*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 119 s. Vedoucí práce Ing. Petr Sedlák.

Prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 22. května 2017

.....

Jan Palička

Poděkování

V této části bych rád poděkoval vedoucímu této diplomové práce Ing. Petru Sedlákovi za odborné rady, ochotu a pomoc. Dále pak panu Ing. Petru Kaštovskému a všem zaměstnancům společnosti Netcope Technologies a. s. za poskytnuté informace. V neposlední řadě také všem ostatním, kteří mi byli oporou při vypracovávání této práce.

Obsah

Úvod

Informační bezpečnost je v dnešní době stále více zmiňovaným pojmem, avšak přístup řady firem je v této oblasti tristní. V takových firmách je buďto úroveň informační bezpečnosti velmi nízká, informační bezpečnost je neúplná nebo chybí úplně.

Cílem této diplomové práce je vytvoření systémového přístupu k řešení bezpečnosti informací ve společnosti. Mnou vybraná společnost Netcope Technologies, a. s. je příkladem malé IT firmy, která se zabývá návrhem hardwarových síťových karet pro vysokorychlostní síťovou akceleraci. Součástí firmy je rovněž oddělení, jež vytváří řešení pro vysokofrekvenční obchodování.

Tato diplomová práce je rozdělena do 5 kapitol. Kapitola 1 specifikuje cíle této diplomové práce a stanovuje rozsah informační bezpečnosti zpracovávané v rámci této diplomové práce.

Kapitola 2 obsahuje teoretické pozadí této práce. V této kapitole jsou popsány základní elementy informační bezpečnosti, jako je vymezení organizační bezpečnosti (viz podkapitola 2.2 na straně 15), vymezení bezpečnosti v informatice v podkapitole 2.2.1 na straně 16 apod. Stěžejní částí této kapitoly jsou zejména informace o modelu PDCA v podkapitole 2.3 následované informacemi o managementu bezpečnosti informací (ISMS) v podkapitole 2.4. Zbylá části 2. kapitoly informuje, mimo jiné o metodách analýzy aktiv, posuzování hrozeb spojených s aktivy, realizaci zabezpečení informací apod.

V kapitole 3 jsou pospána vybraná technická řešení pro zavedení bezpečnosti informací. Jsou mezi nimi zmíněny například technologie RADIUS serveru určeného pro ověřování uživatelů nebo technologie virtuálních lokálních sítí (VLAN), pomocí níž je možné vytvořit více virtuálních sítí na jednom fyzickém médiu. V této kapitole jsou navíc zmíněny systémy pro správu verzí, které jsou velmi vhodné pro společnosti zabývající se činností v IT, jelikož jim tyto programy napomáhají spravovat zdrojové kódy svých produktů.

Stěžejními částmi v této práci jsou kapitoly 4 a 5. V kapitole 4 je pospán současný stav informační bezpečnosti ve společnosti Netcope Technologies, a. s., jsou identifikována aktiva společnosti, je provedeno ohodnocení těchto aktiv a jsou analyzována rizika spojená s těmito aktivy. Na základě zjištěných rizik jsou posléze identifikovány hrozby, které jsou již řešeny některým firemním nařízením a také jsou stanoveny hrozby, pro něž budou dále hledána bezpečnostní opatření.

Kapitola 5 přináší samotný návrh řešení dle normy ČSN ISO/IEC 27002:2014. Součástí této kapitoly je i finanční zhodnocení navrhovaných opatření. Veškerá použitá literatura je uvedena v závěru práce.

Kapitola 1

Cíle diplomové práce

Hlavním cílem této diplomové práce je vytvoření systémového řešení bezpečnosti informací na základě analýzy současného stavu ve společnosti Netcope Technologies, a. s. Při vypracovávání této práce bude postupováno dle norem řady ČSN ISO/IEC 27000. Výstupem práce bude návrh na systémové řešení bezpečnosti informací v podobě sady navržených bezpečnostních opatření. Dílčí cíle práce jsou potom následující:

- Vymezení teoretických východisek práce.
- Analýza současného stavu ve zvolené společnosti.
- Identifikace aktiv ve zvolené společnosti.
- Analýza rizik, hrozeb a scénářů ve zvolené společnosti dle rodiny norem ČSN ISO/IEC 27000.
- Návrh opatření pro zvolenou společnost dle rodiny norem ČSN ISO/IEC 27000.

Kapitola 2

Teoretické pozadí práce

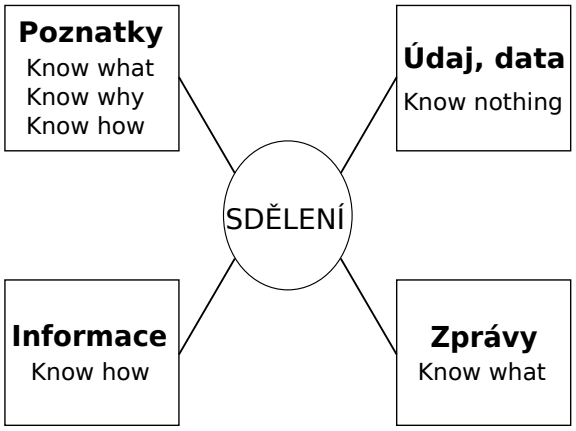
V této kapitole bude popsáno teoretické pozadí diplomové práce. K tomuto teoretickému základu bude dále odkazováno z ostatních kapitol.

2.1 Informace a její bezpečnost

V nejširším slova smyslu je možné informaci chápat jako údaj o prostředí, jeho stavu a procesech, které v tomto prostředí probíhají. Pokud bychom chtěli být více specifičtí, je informace prostředek pro:

- srozumitelné přenesení úkolů vykonavatelům,
- úspěšné organizováni i operativní řízení bezpečnostních akcí,
- efektivnost kontroly.

Architektura informačních pojmů je zobrazena na obrázku 2.1.



Obr. 2.1: Architektura informačních pojmů [1, str. 37]

Ve firemním prostředí jsou užívány především následující typy informací (viz [2, str. 4]):

- interní informace o společnosti, její strategické záměry a plány,
- interní znalostní informace, které nejsou obecně dostupné konkurencí („know-how“), interní předpisová základna,
- informace o zaměstnancích společnosti,
- databáze o klientech, spolupracujících společnostech a subjektech,
- informace získané z volně dostupných zdrojů (například odborné publikace, internet, tisk).

Takovéto informace je nutné zabezpečit, a to hned z několika důvodů ([2, str. 5]):

- Z důvodů plynoucích z platné legislativy: zejména jde o zákon 101/200 Sb.[1], o ochraně osobních údajů a dále také dle legislativních norem vydaných Evropskou unií.
- vlastní obchodní zájmy firmy – především se jedná o utajení interních důvěrných informací, zamezení jejich zneužití, dostupnost potřebných informací a jejich celistvost.
- závazky společnosti vůči spolupracujícím externím společnostem i klientům vyplývající z podmínek uzavřených smluv a dohod.

2.1.1 Zabezpečení informací

Ve firemním prostředí můžeme informace chápat jako souhrn několika entit. Mezi tyto entity patří strojově a lidsky čitelné texty (soubory kancelářských aplikací, textové soubory, interní směrnice, interní postupy, zdrojové kódy apod.), emaily, číselné údaje. V případě společností zabývajících se vývojem v oblasti IT (vývoj SW, vývoj HW apod.) je nutné zařadit do tohoto výčtu informace v binární podobě (prototypy programů s ladícími informacemi, překladové skripty apod.).

V mnoha případech se pracovníci zodpovědní za zabezpečení informací soustředí zejména na zabezpečení přístupu do organizační počítačové sítě pro neoprávněné osoby. Tento postup ale není dostatečný, neboť zabezpečení informací je míněno splnění takzvané „informační triády“, tedy zajištění důvěrnosti, integrity a dostupnosti. V literatuře jsou tyto pojmy definovány následovně ([2, str. 5]):

- *důvěrnost* – prevence neoprávněného užití informace. Přístup k aktivům mají pouze autorizované subjekty, tj. osoba, proces nebo zařízení disponující oprávněními k provádění činností v IS/ICT,
- *integrita* – prevence neautorizované modifikace informace. Možnost změny informace mají pouze autorizované subjekty,

[1] Dostupné online z: https://www.uoou.cz/files/101_cz.pdf

- *dostupnost* – autorizované subjekty mohou na své vyžádání vykonat činnosti a není jim odepřen k činnosti přístup.

Vedoucí pracovníky často zajímá pouze zajištění dostupnosti informací, aby byla umožněna realizace plánovaných aktivit společnosti. Nezbytnost zajištění důvěrnosti a integrity si často uvědomí až při vzniku a řešení bezpečnostního incidentu.

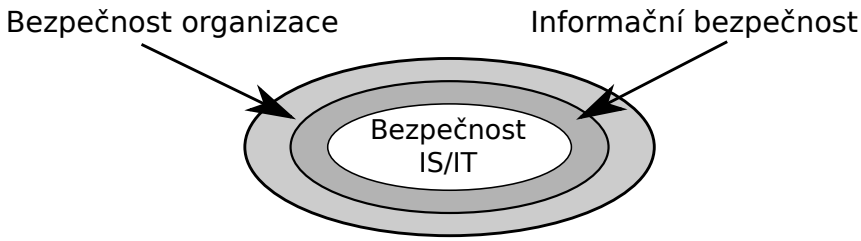
2.2 Organizace a její bezpečnost

Smyslem zabezpečení organizace je snížení rizika a hrozeb a předcházení bezpečnostním incidentům, jako možným zdrojům bezpečnostních hrozeb. Pro zajištění bezpečnosti organizace existují normy z rodiny ISO 27000, které nabízí celistvý pohled na problematiku bezpečnosti.

Společně s pojmem bezpečnost organizace a jejího IS a použitých ICT je nutné zmínit dva další pojmy:

- Bezpečnost informací.
- Organizační bezpečnost.

Jejich vzájemné vztahy (nadřízenost a podřízenost) je zobrazena na obrázku 2.2:



Obr. 2.2: Bezpečnost v organizaci a její vztahy [1, str. 254]

Nejvyšší vrstvou zabezpečení a zároveň vrstvou s nejširším záběrem je bezpečnost organizace. Do této vrstvy patří zabezpečení objektu, majetku jako takového a je do ní možné zařadit i ostrahu objektů, tedy i zabezpečení přístupu pouze oprávněným osobám. Zajištěním přístupu pouze oprávněným osobám též dochází ke splnění bezpečnostních aspektů vrstvy bezpečnosti IS/ICT.

Jak je možné vidět z obrázku 2.2 bezpečnost organizace v sobě zahrnuje i samotnou informační bezpečnost. Cílem informační bezpečnosti je zahrnout v sobě bezpečnost přístupu a práce se všemi druhy informací, které se v organizaci nacházejí. Nejde tedy jen o zajištění bezpečnosti digitálních informací, informační bezpečnost též popisuje zásady nakládání s nedigitálními daty. Oproti bezpečnosti IS/ICT způsob zpracování, uložení a správy nedigitálních dat, dále popisuje zásady a způsoby skartace materiálů, popisuje zásady a bezpečnostní pravidla pro jejich transport apod. V neposlední řadě též informační bezpečnost popisuje způsob prezentace informací třetím stranám. Popisuje tak například pravidla pro jednání s tiskem, popřípadě pravidla pro veřejné vystupování pracovníků organizace.

Nejnižší vrstvou bezpečnosti v organizaci je bezpečnost IS/ICT, která v sobě v podstatě zahrnuje pouze bezpečnost těch aktiv, která jsou součástí informačního systému dané organizace společně s podporovanými informačními a komunikačními technologiemi [1, str. 254].

2.2.1 Bezpečnost v informatice

Problematika bezpečnosti v informatice je v současné době stále častěji diskutovaným tématem, neboť množství informací, které jsou uchovávány, či vyměňovány pomocí prostředků ICT, prudce roste. Naštěstí již existují ucelené směrnice a „Best Practices“, které napomáhají zajištění bezpečnosti.

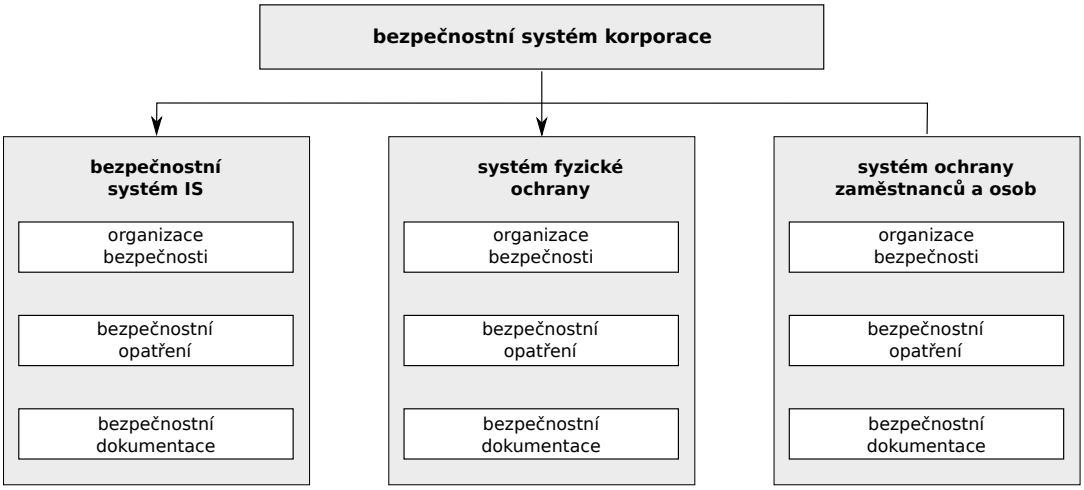
Zajištění bezpečnosti v informatice nelze, jako tomu bylo dříve, omezit pouze na zajištění ochrany proti neoprávněnému přístupu k datům. Bezpečnost v informatice je problémem mnohem širším. Náhled na oblasti bezpečnosti přináší obrázek 2.3.

Obr. 2.3: Oblasti řešení bezpečnosti [3, str. 377]

Jak je možné vidět na obrázku 2.3, proniká zajištění bezpečnosti IS/ICT do více oblastí bezpečnosti, konkrétně jde o tyto oblasti (viz [3, str. 377]):

- **objektová bezpečnost** – zajištění ochrany budov a prostor, do které patří i ochrana proti požáru či jiné škodě způsobené vnějšími vlivy,
- **bezpečnost a ochrana zdraví při práci** – na základě charakteru činnosti organizace dochází ke stanovení podmínek bezpečnosti práce (BOZP),
- **bezpečnost IS/ICT** – řeší bezpečnost informačního systému, jako každého jiného aktiva.

Pro zajištění optimální a silné bezpečnostní politiky organizace musí platit, že jak celková bezpečnostní politika, tak veškeré aktivity společnosti probíhající v oblasti informační bezpečnosti, musí být v souladu se strategickými cíli dané organizace. Pohled bezpečnostní systém společnosti podává obrázek 2.4:



Obr. 2.4: Schéma bezpečnostního systému korporace [2, str. 12]

Procesy spojené se zajištěním informační bezpečnosti jsou v organizaci zaváděny pomocí modelu PDCA (více o modelu PDCA je uvedeno v kapitole 2.3). Jak již bylo zmíněno dříve, nejde informační bezpečnost v organizaci omezit pouze na IS nebo ICT v dané organizaci, ale je nutné, aby zahrnovalo i organizační procedury a chování jednotlivých zaměstnanců a všech, kdo přijdou do kontaktu s podnikovou ICT architekturou.

2.3 Model PDCA

Model PDCA je iterativní metodou postupného zlepšování, jejíž použití je téměř neomezené. Neustálé opakování dále uvedených kroků vede k neustálému zlepšování a rozvoji. Tyto iterace jsou následující [4, str. 24]:

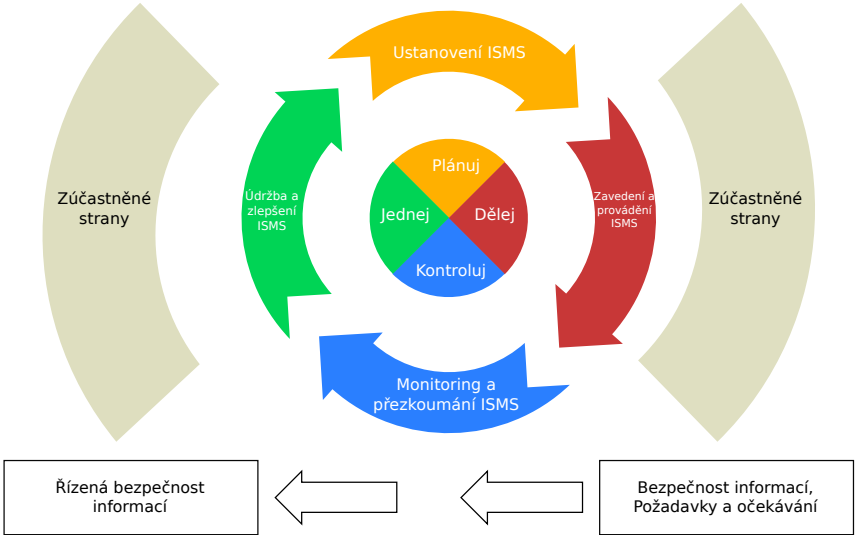
- Plan (*plánuj*) – naplánování zamýšleného zlepšení (záměr).
- Do (*dělej*) – realizace plánu.
- Check (*kontroluj*) – ověření výsledku realizace oproti původnímu záměru.
- Act (*jednej*) – úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe.

Součástí modelu PDCA je též dokumentace každé jednotlivé etapy z výčtu uvedeného výše. Tato dokumentace je klíčovou součástí daného modelu. Pro práci s procesy v modelu PDCA je nutné:

- Identifikovat jednotlivé procesy.
- Popsat a zdokumentovat jednotlivé procesy.

- Řízení procesů na základě dokumentace z modelu PDCA.
- Následná optimalizace průběhu procesu (viz [4, str. 25]).

Grafické znázornění modelu PDCA v prostředí ISMS je na vidět na obrázku 2.5.



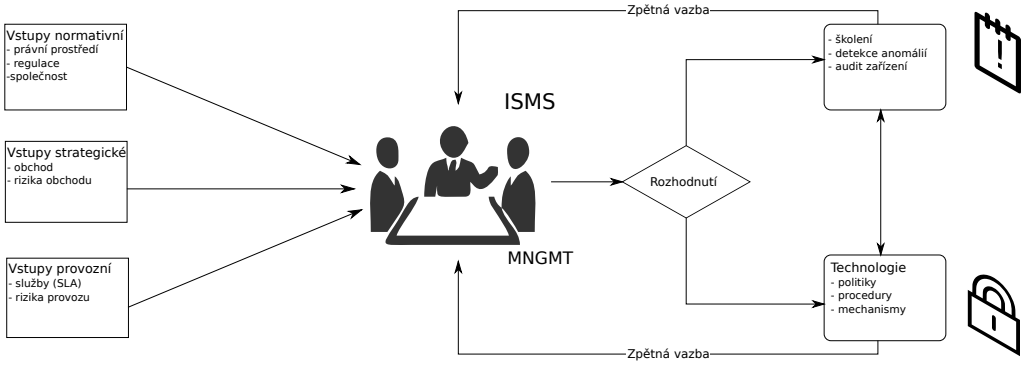
Obr. 2.5: Model PDCA v prostředí ISMS [4, str. 25]

2.4 Definice ISMS

Pro definování pojmu ISMS stačí, když pochopíme, co znamenají jednotlivá písmena. ISMS je zkratkou pro *Information Security Management System* neboli *Systém řízení bezpečnosti informací*. Slovo systém není jen tak samoúčelné, jelikož ISMS má několik navzájem spojených etap, které na sebe musejí navazovat. Je také nutné, aby bylo pamatováno na to, že ISMS je součástí systému řízení organizace ([4, str. 25]). ISMS jako takové je potom založeno na metodologii PDCA (viz kapitola 2.3) a má čtyři etapy ([4, str. 14]):

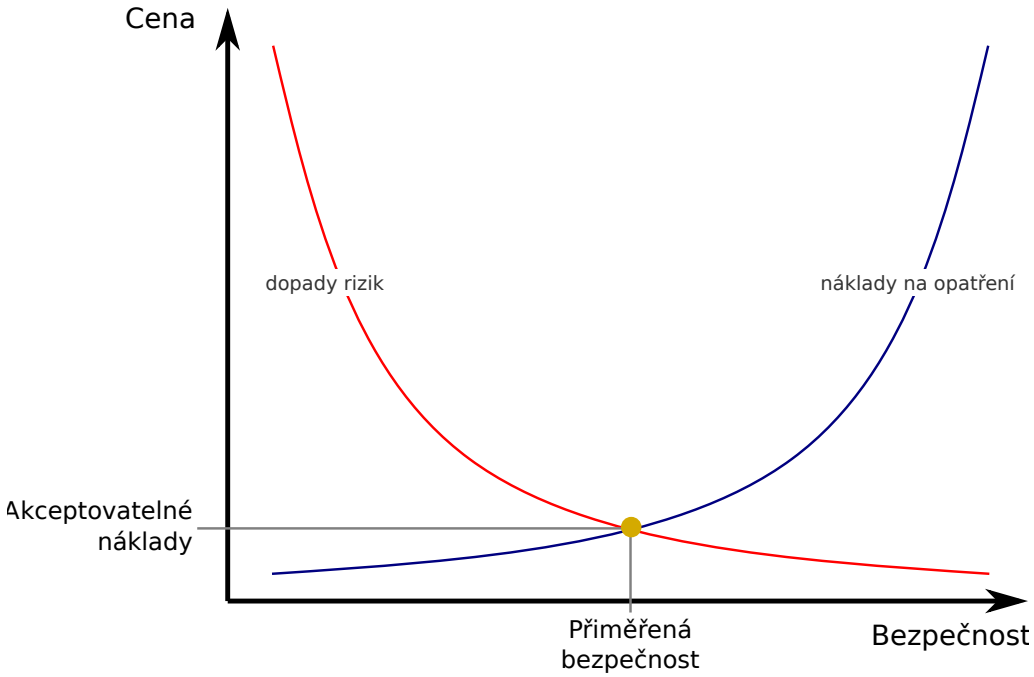
- Ustanovení ISMS v organizaci (určení rozsahu opatření a odpovědností za opatření).
- Zavedení a provoz ISMS (prosazování navržených bezpečnostních opatření).
- Monitorování a přezkoumání ISMS (získání zpětné vazby a hodnocení rizik).
- Zlepšování ISMS (na základě zpětné vazby dochází k vylepšení a změnám v ISMS),

Struktura ISMS je zobrazena na následujícím obrázku:



Obr. 2.6: Struktura ISMS [4, str. 15]

S pojmem ISMS souvisí také takzvaná přiměřená bezpečnost. Přiměřená bezpečnost je definována, jako optimum mezi vynaloženými finančními prostředky a získanou (dosaženou) bezpečností. Úkolem managementu v případě zavádění ISMS je stanovit, jak velkou úroveň zabezpečení potřebujeme a jakou úroveň si můžeme dovolit. Větší váhu při rozhodování má, zpravidla, finanční rámec, jelikož společnost má většinou omezené prostředky.



Obr. 2.7: Graf přiměřené bezpečnosti [4, str. 36]

Jak je možné vidět na obrázku 2.7, malé náklady na zajištění bezpečnosti mohou vést k její nedostatečnosti. Naopak v případě, kdy náklady na zajištění bezpečnosti zvýšíme nad určitou mez, nedostáváme adekvátní zvýšení bezpečnosti. Jak již bylo zmíněno, je nutné, aby management organizace při zavádění ISMS našel takový kompromis, který maximalizuje bezpečnost a náklady udrží v rozumné výši.

2.5 Certifikace a normy

Abychom byli schopni v lidské společnosti zavést určitý proces a tento proces byli schopni opakovat bez změn, vznikají certifikace a normy. S normami se setkáme takřka v každé lidské činnosti a oblasti. Normy a standardy používají informační systémy pro bezproblémové dorozumění, normy používáme, když řídíme automobil a stejně tak se normy využívají i v oblasti informační bezpečnosti.

Tvorbou norem se zabývá množství organizací, ať už na mezinárodní úrovní nebo na úrovni čistě národní. Řada těchto institucí, věnujících se profesionálnímu vytváření norem, platí ve svém oboru za skutečné autority. Některé z těchto norem jsou přebírány i českými úřady a můžeme se s nimi setkat i v rámci české legislativy. Jaké typy norem tedy můžeme v českém právním prostředí potkat [5, str. 142]:

- **ISO normy** – jsou vydávány institucí s názvem International Organisation for Standardisation.
- **IEC normy** – jsou vydávány institucí s názvem International Electrotechnical Commision.
- **ITU normy** – tyto normy vydává Mezinárodní telekomunikační unie.

V IT branži je možné se setkat (například v rámci manuálů nebo v dokumentacích) s normami, které vycházejí z norem vydaných některou autoritou z předchozího seznamu, ale byly přeloženy národními normotvornými úřady. Mezi nejznámější zástupce patří tyto normy:

- **DIN** – normy vydané německým Deutsches Institut für Normung e. V. (*Německý ústav pro průmyslovou normalizaci*).
- **ANSI** – normy vydané americkým American National Standars Institute (*Americký národní standardizační institut.*

Mimo tyto organizace existuje i řada oborových organizací, které vydávané normy zaštiťují svou odbornou praxí a autoritou. Mezi neznámější normy patří normy takových velikánů, jako je organizace IEEE (*Institute of Eletrical and Electronics Engineers*) nebo normy amerického NIST (*National Institute for Standards and Technology*) [5, str. 142].

2.5.1 Normy v České republice

V České republice se vydáváním norem zabývá Úřad pro technickou normalizaci, metrologii a státní zkušebnictví a jeho normy nesou označení ČSN. V případě, kdy vydávána norma převzatá od některé nadnárodní organizace, zůstává v názvu normy i název této mezinárodní organizace a je zachováno i původní číslování (např. ČSN ISO 27001).

ČSN ISO/IEC 27000:2014

`Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Přehled a slovník`

Jak již značení normy napovídá, jedná se o mezinárodní normu, která byla přejata Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví a jejímž hlavním smyslem je poskytování přehledu systémů řízení bezpečnosti informací. Její součástí jsou termíny a definice, které se používají v rámci norem z rodiny ISMS. Rodina těchto norem má napomoci libovolné organizaci se zavedením a řízením ISMS [4, str. 48].

ČSN ISO/IEC 27001:2014

`Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky`

Tato norma poskytuje metodologii, jak aplikovat vybraná opatření z normy ISO/IEC 27002 v rámci procesu zavádění, provozu, údržby a zlepšování ISMS v organizaci. Je prosazováno přijetí principu PDCA (viz kapitola 2.3) ve všech procesech ISMS, tak jak je definuje tato norma, napříč celou organizací.

Samotná norma je dále harmonizována s normami řízení procesů ISO/IEC 9001:2000 a normou pro řízení kvality ISO/IEC 14001:2004, kde je zejména kladen důraz na konzistentní zavedení a provoz všech uvedených norem [4, str. 49].

Hlavní částí normy je specifikace požadavků na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a případnou certifikaci zdokumentovaného systému ISMS. Dále norma specifikuje požadavky na výběr a zavedení opatření, která chrání in formační aktiva. V příloze této normy jsou uvedeny cíle opatření jednotlivých opatření, která přímo korelují s cíli a opatřeními v normě ISO/IEC 27002:2014 [4, str. 49].

ČSN ISO/IEC 27002:2014

`Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů`

Jak již z názvu vypovídá, jedná se o stěžejní normu pro zavedení ISMS. Tato norma obsahuje více než 100 strukturovaných oblastí doporučení rozdělených do 18 kapitol. V rámci těchto kapitol stanovuje množství přímých nebo odvozených bezpečnostních opatření, která lze implementovat v rámci ISMS. Výhodou těchto opatření je to, že lze ke každému opatření přiřadit osobu odpovědnou za jeho prosazování, a tak lze v relativně krátké době vytvořit fungující bezpečnost informací v libovolné organizaci [4, str. 49].

Velkou výhodou je také možnost vytvoření východisek pro dodatečné zlepšení. To spočívá především v tom, rozhodnout, které oblasti bezpečnosti informací nejsou dle normy dostatečně zajištěny a soustředit se tak na zajištění takto zjištěných oblastí.

ČSN ISO/IEC 27005:2013

`Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Řízení rizik bezpečnosti informací`

Jelikož k řízení bezpečnosti informací je vhodné přistupovat formou řízení rizik, byla vytvořena tato norma, která řízení rizik nad bezpečností informací podporuje. Na druhou stranu tato norma nepřináší přesnou metodologii, jak přistupovat k řízení rizik nad bezpečností informací. Záleží tedy na konkrétní organizaci, jak informace obsažené v této normě implementuje (dle oboru, rozsahu ISMS apod.). Tato norma navíc umožňuje, aby byla rizika nad bezpečností informací řízena některou z řady obecných metodik pro řízení rizik [4, str. 51].

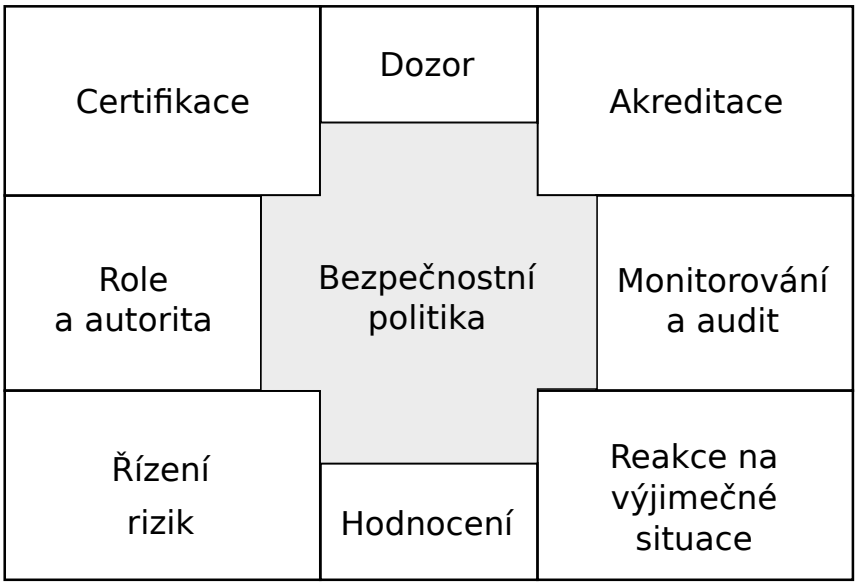
2.6 Bezpečnost organizace

Bezpečnostní politika je základním dokumentem informační bezpečnosti organizace. Je doporučené, aby tento dokument byl součástí norem a nařízení společnosti. Je vhodné zvolit psanou formu dokumentu, neboť forma předávaná ústně má sklon k modifikacím (ať už záměrným nebo nechtěným). Bezpečnostní politika organizace by měla obsahovat zejména tyto body [5, str. 168]:

- Stanovení toho, co chceme bezpečnostní politikou chránit.
- Stanovení toho, proč danou věc chceme chránit.
- Stanovení metod, jak danou věc budeme chránit.
- Stanovení metod ověření, že je ochrana důsledná.
- Stanovení opatření, která přijmeme v případě, že se ochrana nezdaří nebo bude kompromitována.

Jak vyplývá ze seznamu výše, je nutné identifikovat prostředky, které budeme v rámci politiky ISMS chránit. Pro tyto prostředky si dále zaveďme pojem aktiva. Platí však pravidlo, že ne všechna aktiva je nutné chránit, a ne všechna aktiva je nutné chránit na stejné úrovni. Míra ochrany konkrétního aktiva by měla odpovídat tomu, jak moc je dané aktivum pro společnost důležité [5, str. 168].

Ruku v ruce s procesem zavedení bezpečnostních opatření jde i jejich kontrola. Zejména je nutné zkontrolovat, že zavedená opatření jsou zvolena správně a jejich fungování je správné. Při této kontrole musíme vyloučit lidské chyby, ať už úmyslné nebo neúmyslné. Kontroly by měly probíhat periodicky tak, aby bylo zajištěno, že přijatá opatření neztratila svůj efekt, nebyla záměrně či neúmyslně odstraněna nebo neztratila účinnost v kombinaci s jiným prostředkem [5, str. 169].



Obr. 2.8: Obsah řešení bezpečnosti IS/ICT [3, str. 380]

Obsah řešení bezpečnosti IS/ICT je zobrazen na následujícím obrázku:

Jak je z obrázku 2.8 vidět, vedle budování bezpečnostní politiky je nutná stálá analýza bezpečnostních rizik, hledání protiopatření na tato rizika, a to včetně implementace plánů pro řešení výjimečných situací (*disaster recovery plan*). Tyto činnosti můžeme zařadit do skupiny činností označených jako řízení rizik. Další činnosti zobrazené v obrázku 2.8 se zaměřují na zajištění kontroly a auditu bezpečnostní politiky a její monitorování, akreditaci, certifikaci a hodnocení [3, str. 380].

Prostředí, do něhož je bezpečnostní politika organizace zasazena se časem stále vyvíjí, proto by tyto změny měla reflektovat i samotná bezpečnostní politika. V průběhu času se mění složení a typ hrozeb, které je nutné z bezpečnostního pohledu sledovat [5, str. 169].

Pro bezproblémové užívání bezpečnostní politiky je nutné, aby s ní byli seznámeni všichni zaměstnanci a sami zaměstnanci se musejí s pokyny obsaženými v bezpečnostní politice plně ztotožnit. Samotná výkonná moc bezpečnostní politiky potom spadá na bedra vedoucích jednotlivých oddělení [5, str. 169].

2.6.1 Definice pojmů použitých v bezpečnostní politice

V následující podkapitole budou definovány pojmy, které se objevují v bezpečnostní politice organizace.

Informační systém (Information system)

Pojem informační systém označuje skupinu počítačů, serverů, disků a ostatních záznamových zařízení, společně s propojovacími médii (ať už jde o propojovací kabely nebo síťové kabely) [5, str. 169].

Informační bezpečnost (Information security)

Pojem informační bezpečnost je oborem zabývajícím se bezpečností informačních a komunikačních technologií. Obecně lze informační bezpečnost definovat jako systém ochrany dat a informací během celého jejich životního cyklu (od vytvoření dat, přes jejich uložení, až po proces jejich likvidace), obsahující organizační, programové a technické opatření. Cílem těchto opatření je zamezení ztráty důvěrnosti, integrity a dostupnosti chráněných dat [1, str. 252].

Aktivum (Asset)

Pan Jaroslav Mlýnek definuje ve své knize *Zabezpečení obchodních informací* aktivum jako hmotný nebo nehmotný statek, který má v informačním systému organizace určitou hodnotu [2, str. 17]. Obecně lze tedy říct, že aktiva jsou takové statky, které mají pro danou organizaci určitou hodnotu. Nejvyšší hodnotu mívají většinou peníze, jelikož poskytují nejvyšší likviditu.

V současné době se mezi stále cennější aktiva řadí i informace, ať už jde o informace obchodní, know how nebo zkušenosti zaměstnanců. Neméně důležitým aktivem pro společnosti jsou prostředky pro zpracování těchto informací. Stejnou důležitost, jako zařízení pro zpracování informací mají pro organizaci i zaměstnanci, kteří daná zařízení spravují nebo s nimi operují [3, str. 377].

Bezpečnost (Security)

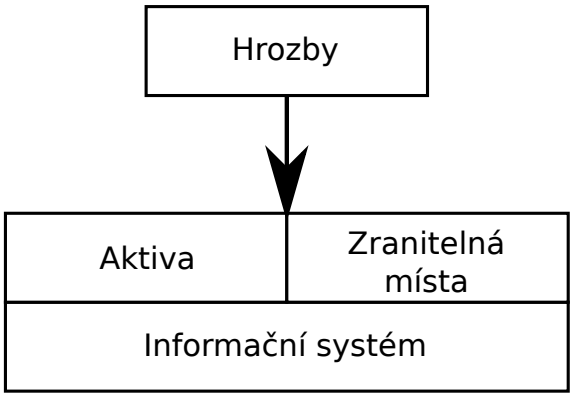
Pojem bezpečnost definuje stupeň ochrany určitého prvku, která určuje míru ochrany daného prvku proti možným hrozbám, škodám nebo jiným nepříznivým vlivům [1, str. 252].

Citlivá data (Sensitive data)

Citlivá data jsou takové informace v informačním systému organizace, které vyžadují vždy ochranu, neboť vždy existuje pravděpodobnost jejich zneužití a působení hrozeb na tato data je velice nebezpečné. Mezi citlivá data je možné zařadit personální data zaměstnanců (jejichž ochranu vyžaduje zákon), dále pak o obchodní data firmy a v neposlední řadě o know how dané organizace [1, str. 252].

Hrozba (Threat)

Hrozba je událost nebo akce, která může využít zranitelnost a způsobit tak stav, kdy budou informace nebo prostředky pro jejich zpracování záměrně nebo náhodně ztracena, modifikována nebo kompromitována, nebo se stanou nedostupnými. Takový stav může vést k finanční újmě společnosti [2, str. 17]. Hrozbou může být negativně ovlivněna bezpečnost organizace [1, str. 252]. Vtah hrozeb a aktiv ukazuje následující obrázek:



Obr. 2.9: Vztah hrozeb a aktiv [5, str. 168]

Hrozba, jako taková, zůstává hrozbou, dokud není naplněna. Potom se již z hrozby stává útok a ten vede v bezpečnostní incident [5, str. 170].

Ohodnocení rizik (Risk Assessment)

Ohodnocení rizik je proces vyhodnocení míry hrozeb, které působí. V našem případě budeme hodnotit hrozby. které působí na informační systém dané organizace. Metody ohodnocení rizik jsou kvantitativní a kvalitativní, kdy kvalitativní metody jsou přesnější [6, str. 67]. Cílem tohoto procesu je zjištění, kde jsou bezpečnostní opatření dostatečná, a kde je nutné je změnit, aby došlo ke snížení dopadu hrozby na přijatelnou úroveň [1, str. 252].

Ohodnocení rizik (Risk Assessment)

Ohodnocení rizik je proces vyhodnocení míry hrozeb, které působí. V našem případě budeme hodnotit hrozby. které působí na informační systém dané organizace. Metody ohodnocení rizik jsou kvantitativní a kvalitativní, kdy kvalitativní metody jsou přesnější [6, str. 67]. Cílem tohoto procesu je zjištění, kde jsou bezpečnostní opatření dostatečná, a kde je nutné je změnit, aby došlo ke snížení dopadu hrozby na přijatelnou úroveň [1, str. 252].

Riziko (Risk)

Riziko je pravděpodobnost, v širším slova smyslu, „vystavení nepříznivým okolnostem“ [6, str. 47]. Konkrétněji je možné riziko chápat, jako pravděpodobnost toho, že nastane zničení, poškození nebo zneužití aktiv, a to působením hrozeb a ke vzniku škody [2, str. 17].

Zranitelnost (Vulnerability)

Zranitelnost je slabé místo hodnoceného aktiva. Toto slabé místo může vzniknout například jako důsledek chybného návrhu, chybné implementace nebo jako důsledek chybného provozu [2, str. 18]. Úroveň zranitelnosti aktiva je hodnocena dle náchylnosti aktiva k poškození a podle důležitosti aktiva v rámci informačního systému.

Bezpečnostní incident (Security Incident)

Bezpečnostní incident, někdy též označován jako útok, je vědomé nebo nevědomé využití zranitelného místa ke způsobení škodlivého na aktivech. Škodou rozumíme poškození nebo zničení aktiva. Při stanovování obrany proti bezpečnostními incidentu je nutné zvážit, jakým způsobem může incident vzniknout, jak se do tohoto incidentu může zapojit kybernetická kriminalita apod. Nejběžnější formou útoku je kompromitace dat, kdy je jsou data pozměněna, odposlechnuta či modifikována přidáním hodnoty [1, str. 253].

Zranitelné místo

Zranitelné místo je místo v informačním systému, které může být útočníkem zneužito k vytvoření škody nebo ztrát z informačního systému. Zranitelné místo je úzce spjato se zranitelností a vniká stejně, jako zranitelnost sama, tedy chybou v době návrhu, implementace nebo údržby. Dále můžeme zranitelné místo považovat za důsledek složitého systému, vysokou hustotou uložených dat nebo existencí takového prostředku pro přenos informací, který není dokumentován [1, str. 253].

Existuje několik typů zranitelných míst [3, str. 378]:

- **Fyzické**, kdy je prvek IS/ICT fyzicky umístěn v prostředí, ve kterém může snadno dojít k jeho poškození, zničení či ztrátě.
- **Přírodní**, kdy prvek IS/ICT nemá schopnost se vyrovnat s některými objektivními faktory, jako je záplava, požár, blesk apod.
- **Technologické**, kdy prvek IS/ICT svými konstrukčními charakteristikami neumožňuje zajistit např. požadovaný trvalý plynulý provoz.
- **Fyzikální**, kdy prvek IS/ICT pracuje na takových fyzikálních principech, které umožňují jejich zneužití. Příkladem může být elektromagnetické vyzařování některých komponent, jako jsou monitory, kabeláž komunikační sítě apod.
- **Lidské**, kdy prvek IS/ICT je ohrožen působením lidí, jejich omylů a neznalosti [3, str. 378].

Útokem na zranitelné místo vniká bezpečnostní incident, který byl zmíněn v kapitole 2.6.1.

Útočník

Útočníkem může být osoba uvnitř organizace, nebo může jít o osobu mimo organizaci. Útok může mít jasný úmysl, nebo se jedná o neúmyslný útok. V případě osob, které realizují úmyslné útoky, se požívá pro jejich označení několik termínů, zejména [3, str. 379]:

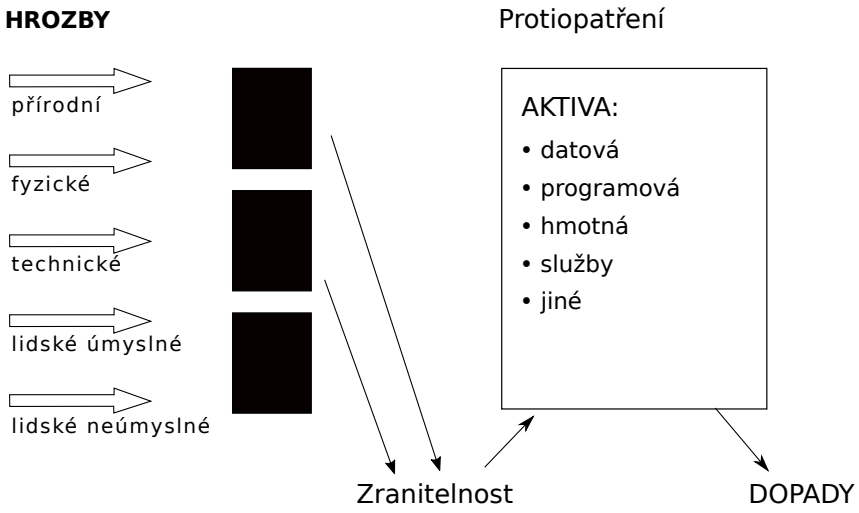
- **Hacker** – bere útok jako výzvu a prostředek získání prestiže.
- **Vyzvědač (*„spy“*)** – provádí útoky za účelem zisku informací, které jsou využívány pro různé politické účely.

- **Terorista (*„terrorist“*)** – provádí útoky za účelem vyvolání obavy a strachu.
- **Kriminálník (*„criminal“*)** – útočí na systémy pro svůj osobní finanční zisk.
- **Vandal (*„vandal“*)** – útočí na systémy s cílem systém zničit či poškodit.
- ***Cracker*** (zpravidla programátor) –snaží se proniknout do systémů jiných vlastníků za účelem jejich krádeže. Typicky se orientuje na krádež duševního vlastnictví, tj. těch částí systémů, které jsou chráněny autorským zákonem.
- **Phracker** – jeho cílem je získání bezplatného přístupu k telefonním službám.
- **Phreaker** – jeho cílem jsou telekomunikační informace, které mu umožňují získávat přístup k dalším počítačům [3, str. 379].

2.7 Bezpečnostní hrozby

Hrozba má schopnost způsobit nežádoucí incident, který může mít za následek poškození informačního systému, organizace nebo aktiv. Schopnost způsobit incident je u hrozby však pouze potenciální [4, str. 86].

Základní schéma zajištění bezpečnosti IS/ICT představuje vztahy mezi aktivy dané organizace, hrozbami potenciálně působícími na aktiva, možnou zranitelností, kterou hrozby způsobují, dopady reálných hrozeb na aktiva společnosti a protiopatřeními zajišťujícími ochranu aktiv organizace pomocí bezpečnostních opatření. Schéma těchto vztahů je vidět na následujícím obrázku:



Obr. 2.10: Schéma zajištění bezpečnosti IS/ICT [1, str. 257]

Je nutné, aby nebylo na hrozby nahlíženo, jako na izolované události, jelikož se skoro vždy jedná o kombinaci více hrozeb, které působí v jeden okamžik, a které představují riziko pro dané aktivum. Při provádění analýzy je pak nutné zaměřit se na všechny tyto hrozby a zejména určit míru jejich dopadu a pravděpodobnost toho, že daná hrozba nastane [2, str. 18].

Z obrázku 2.11 je možné také vidět rozdělení hrozeb [3, str. 381]:

- **přírodní a fyzické** – živelné pohromy a poruchy, jako je například požár nebo povodeň,
- **technické** – poruchy datových nosičů, síťových prvků, počítačů a serverů,
- **technologické** – poruchy způsobené programovým vybavením a podvodnými programy,
- **lidské** – ty dělíme na dvě podskupiny:
  - **neúmyslné** – vyplývající z neznalostí, omylů a zanedbání povinností,
  - **úmyslné** – ty můžeme rozdělit způsobu působení na:
    - **vně systému** – útok hackerů, teroristů nebo špionů,
    - **uvnitř systému** – útoky zlomyslných, chamtivých zaměstnanců nebo zvědavých hostů organizace.

Více než 50 % všech hrozeb patří do kategorie těch neúmyslných [3, str. 381].

2.8 Posouzení dopadu hrozeb

Posouzení dopadu hrozeb provádíme dle následujících kritérií [4, str. 86]:

- **ztráta důvěrnosti** – může vést například ke ztrátě důvěry vůči zákazníkům, právní odpovědnosti, ohrožení osobní bezpečnosti nebo finanční ztrátě,
- **ztráta integrity** – může vést například k přijetí nesprávných rozhodnutí nebo narušení funkčnosti organizace,
- **ztráta dostupnosti** – může vést například k neschopnosti vykonávat kritické činnosti organizace,
- **ztráta individuální odpovědnosti** – může vést například k podvodu, špionáži nebo krádeži,
- **ztráta autentičnosti** – může vést například k použití neplatných dat, která vedou k neplatným výsledkům,
- **ztráta spolehlivosti** – může vést například k nespolehlivým dodavatelům nebo demotivaci zaměstnanců.

Při posuzování dopadu hrozby je nutné brát v potaz také takzvaný následný efekt hrozby. Uvedeme si ho na příkladu výpadku elektrické energie, kdy tento výpadek neznamená pouze nedostupnost dat, ale může při dlouhodobém výpadku vést k narušení činnosti organizace nebo k ohrožení fyzického zdraví člověka. Při posuzování dopadů hrozeb je tedy vždy nutné promyslet možné dopady až do nejmenších podrobností [4, str. 86].

2.9 Bezpečnostní incident

Naplněná bezpečnostní hrozba se již nazývá bezpečnostní incident. Bezpečnostní incident je vždy provázen informačními ztrátami. Po zjištění nového bezpečnostního incidentu, ať už probíhajícího nebo ukončeného, je třeba vyšetřit jeho příčinu, podrobně analyzovat situaci systému s cílem zjistit zdroje narušení systému, a nakonec uvést systém zpět do důvěryhodného stavu.

Ruku v ruce s odstraněním dopadů bezpečnostního incidentu jde i přijetí takových opatření, které v budoucnosti znemožní opakování bezpečnostního incidentu. Obecný postup aplikovatelný na šetření bezpečnostního incidentu by měl být následující [1, str. 259]:

1. Zjistit zdroj napadení, podezření na napadení systému ihned hlásit.
2. Zajistit dostatek důkazů podrobným šetřením. Všechny kompromitované účty musí ihned změnit přístupové údaje.
3. Zjistit možnost fyzického přístupu ke zdroji a osobní odpovědnost pracovníků za daný zdroj.
4. Zpracovat protokol o incidentu a uvést pracovníky, kteří by mohli nebo měli být účastníky incidentu.
5. Na základě důkladného šetření vyvodit kázeňská nebo disciplinární opatření s viníky. Dále je vhodné se zamyslet nad oceněním pracovníků, kteří zabránili většímu rozšíření hrozby (pokud takový existují).
6. Přijmout preventivní opatření v informačním systému a na příslušných pracovištích, která budou inspirována výsledky šetření incidentu.

Bezpečnostní incidenty způsobené uživatelem nebo vnějším vlivem můžeme rozdělit do několika skupin, a to [1, str. 260]:

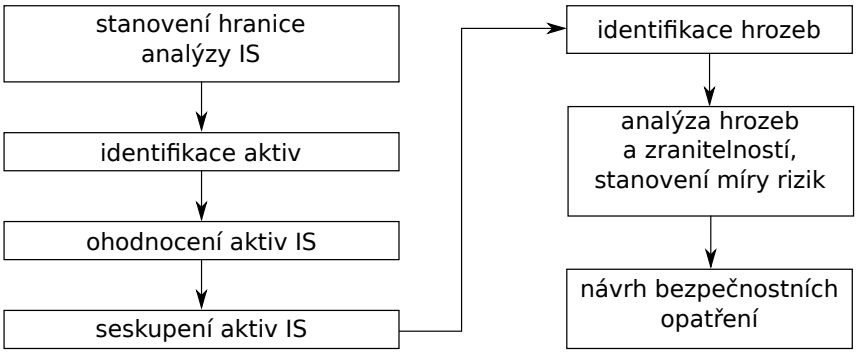
- **Incident způsobený uživatelem**, ten můžeme dále dělit na:
  - **Úmyslný**.
  - **Neúmyslný**.
- **Incident způsobený jiným vlivem**, ten můžeme dále dělit na:
  - **Havárie**.
  - **Chyba systému**.

2.10 Analýza rizik

Při vytváření bezpečnostní politiky informačního systému musí být nejprve provedeno zkoumání toho, co chceme chránit (jaká aktiva) a proti čemu (jakým hrozbám). Analýza rizik potom slouží k odhadu ztrát, které mohou vzniknout působením hrozeb na prvky

informačního systému. Analýza rizik navíc udává přehled o síle jednotlivých hrozeb, konkrétních zranitelnostech informačního systému a o rizicích, jímž je analyzovaný systém vystaven [2, str. 18].

Jednotlivé kroky analýzy rizik nad informačním systémem jsou znázorněny na následujícím obrázku:



Obr. 2.11: Postup analýzy rizik informačních systémů [2, str. 19]

Při analýze rizik je nutné určit priority jednotlivých rizik z pohledu dopadu a pravděpodobnosti, že dané riziko nastane. Na základě těchto výpočtů jsou pak stanoveny klíčové rizikové oblasti, na které se bezpečnostní politika informačního systému vztahuje [2, str. 18].

`P` – značí pravděpodobnost vzniku a existence rizika. Rozlišujeme následující stupně rizik [4, str. 90]:

1. Nahodilá.
2. Nepravděpodobná.
3. Pravděpodobná.
4. Velmi pravděpodobná.
5. Trvalá.

`R` – značí míru rizika potom může mít následující stupně [4, str. 90]:

- 0–10: Bezvýznamné riziko.
- 11–20: Akceptovatelné riziko.
- 21–30: Mírné riziko.
- 31–60: Nežádoucí riziko.
- 61–120: Nepřijatelné riziko.

2.10.1 Stanovení hranic analýzy

Stanovení hranice analýzy je akt, který předchází samotné analýze rizik a pomáhá určit, kterých prvků se analýza bude týkat (např. aktiva IT), a které prvky už budou z analýzy vyřazeny. Tím je zajištěno, že v rámci analýzy nebude prováděna zbytečná práce, a že nebudou analyzovány prvky, u nichž není analýza potřebná nebo, na něž se nevztahuje bezpečnostní záměr organizace [4, str. 93].

2.10.2 Identifikace aktiv

Cílem tohoto kroku je vytvoření seznamu aktiv, která leží uvnitř stanovených hranic analýzy rizik. V případě IT firmy se bude jednat převážně o následující aktiva [2, str. 19]:

(a) informace (databáze, sestavy dat, dokumenty),

(b) hardware – servery, pracovní stanice, směrovače, tiskárny, kabely,

(c) software – operační systémy, aplikační programy,

(d) budovy a místnosti, v nichž se aktiva typu a) až c) fyzicky nacházejí.

Pro samotnou identifikaci aktiv je nutné, aby byla aktiva seskupena podle skupiny, do které patří a dále, aby byla ke každému aktiva nalezena odpovědná osoba. Odpovědná osoba je přímo vlastník aktiva, který v pozdější fázi pomáhá určit přesnou hodnotu daného aktiva (viz kapitola 2.10.3) [4, str. 82].

2.10.3 Ohodnocení aktiv

Nyní, když už máme stanoveny hranice analýzy a identifikovali jsme všechna aktiva spadající do této hranice, můžeme přejít k samotnému ohodnocení jednotlivých aktiv. Vstupním údajem tohoto kroku bude informace získaná od vlastníka aktiva. Tuto informaci je možné získat dotazníkovým šetřením nebo pomocí interview s vlastníkem aktiva [4, str. 93].

Stanovení hodnoty aktiva můžeme provést například tak, že hodnotu odvodíme od ceny nového nebo adekvátního aktiva (tento postup je možné použít například v případě stanovení hodnoty pájecí stanice) [2, str. 20]. Nesmíme však zapomínat na to, že hodnota aktiva je odvozena také z důležitosti aktiva pro celé IS/ICT nebo od ceny informací zpracovávaných na tomto aktivu. Hlediskem, pomocí kterého je možné stanovit cenu aktiva, je i nákladnost překlenutí škody v případě napadení nebo vyřazení aktiva. Hledisek stanovení hodnoty aktiva existuje ale velké množství a je závislé případ od případu [3, str. 378].

Příklad stupnice pro kvantitativní stanovení hodnoty aktiv v případě havárie je následující [4, str. 82]:

1	žádný dopad na organizaci	bezvýznamné riziko
2	zanedbatelný dopad na organizaci	akceptovatelné riziko
3	potíže či finanční ztráty	nízké riziko
4	vážné potíže či podstatné finanční ztráty	nežádoucí riziko
5	existenční potíže	nepřijatelné riziko

Obr. 2.12: Příklad stupnice hodnocení aktiv

Barevné odlišení je vhodné použít například ve velkých tabulkách, kde pomáhá zlepšené orientaci.

2.10.4 Výpočet hodnoty aktiva

Nejpoužívanějším postupem pro hodnocení aktiva je takzvaný součtový algoritmus, ten má následující tvar [4, str. 83]:

$$Hodnota = \frac{\text{dostupnost} + \text{důvěrnost} + \text{integrita}}{3}$$

2.10.5 Identifikace hrozeb

Identifikovat všechny hrozby spojené s bezpečností konkrétního aktiva v informační systémy není snadné a vzhledem k dynamice informačního systému vždy dojde ke stavu, kdy se na některou hrozbu zapomene. Existují tři způsoby identifikace hrozeb.

Prvním způsobem je důkladný rozbor odpovědí na jednoduchou otázku *„Co se stane, pokud útočník provede tuto akci a tuto akci?“* Z takto získaných odpovědí vytvoříme seznam hrozeb. Je téměř stoprocentně jisté, že v něm bude některá hrozba chybět. To se většinou dozvíme v ten nejnevhodnější okamžik [5, str. 171].

Druhým způsobem identifikace hrozeb je využití již existujícího seznamu, který byl vytvořen pro podobné prostředí. Vzhledem k tomu, že nedochází k vytváření celého seznamu hrozeb od začátku, je pravděpodobnost opomenutí některé hrozby nižší, než v prvním případě [5, str. 171].

Třetím způsobem je využití dotazníkového šetření, kdy pro různé části prostředí. Identifikace rizik je pak postavena na expertním vyhodnocení dotazníku pro všechna prostředí. Tak se zjistí, jak si daný systém vede v určitém prostředí. Výhodou těchto dotazníků je prakticky stoprocentní pokrytí všech hrozeb, které konkrétnímu systému v konkrétních prostředích hrozí. Nevýhodou je nutnost opravdu kvalitního dotazníku a také to, že dotazníky nejsou nijak standardizovány, a proto není možné použít předpřipravené dotazníky a je nutné si je v každé organizaci vytvořit vlastními silami [5, str. 172].

2.10.6 Hodnocení hrozeb

Hrozby byly již dříve popsány v kapitole 2.7. Základní katalog hrozeb je uveden v normě ČSN ISO/IEC TR 13335-3 v příloze C. Jelikož hrozby jsou přímo spřaženy s aktivy organizace, bude dáno i jejich hodnocení do souvislosti s identifikovanými aktivy organizace [4, str. 93].

2.10.7 Odhad zranitelnosti

Tento krok slouží ke zjištění (odhadnutí) slabých míst, ať už jde o slabá místa ve fyzickém prostředí, slabá místa v organizaci, postupech personálu nebo se jedná o slabá místa spojená s prostředky pro zpracování informací, jako jsou slabá místa přístupu do administrace SW a HW. Do zranitelnosti může být zařazeno i komunikační zařízení, jehož ovládnutí útočníkem může způsobit škody na aktivech [4, str. 93].

2.10.8 Vlastní analýza rizik

Nyní již máme k dispozici všechny potřebné informace a můžeme proto přikročit k vlastní analýze rizik. Vycházíme ze seznamu aktiv, která se v daném systému vyskytují (máme k dispozici i jejich finanční ohodnocení), a také ze seznamu hrozeb, které aktivům v daném prostředí hrozí [5, str. 172].

Nyní procházím pro každé aktivum seznam hrozeb a stanovujeme hodnotu každé jedné hrozby. Výsledkem našeho snažení je seznam aktiv s přiřazenými hrozbami, které mohou nastat v daném prostředí. Každé této dvojici aktivum-hrozba je možné navíc přiřadit pravděpodobnost, s níž k dané hrozbě může dojít. Získáváme tak kvantifikovaný odhad hrozeb pro jednotlivá aktiva a můžeme se rozhodnout, pro které pravděpodobnosti hrozeb budeme informační systém organizace chránit [5, str. 172].

Identifikace plánovaných a existujících bezpečnostních opatření

Součástí analýzy rizik je i identifikace všech opatření, která ve spojitosti s riziky budou realizována nebo již realizována jsou. Výsledkem je tedy seznam všech prováděných nebo plánovaných bezpečnostních opatření [4, str. 93].

Výběr bezpečnostních opatření

Nyní již známe hodnotu aktiv a pravděpodobnost hrozeb ovlivňujících daná aktiva, byla stanovena hranice pravděpodobnosti hrozeb, pro niž budeme opatření hledat. Teď už zbývá jen výběr vhodných bezpečnostních opatření.

Princip těchto patření spočívá v minimalizaci případných rizik. Pro usnadnění popisu bezpečnostních opatření jsou v rámci normy zavedeny jejich kategorie. Tyto kategorie jsou následující [4, str. 134]:

- řízení a politiky bezpečnosti IT,
- kontrola bezpečnostní shody,

- řešení incidentů,
- personální opatření,
- provozní problémy,
- plánování kontinuity činnosti organizace,
- fyzická bezpečnost.

Nyní již zbývá bezpečnostní opatření navrhnout, ideálně tak, aby byla navržena opatření pro všechny dvojice aktivum-hrozba. Avšak v mnohých případech dochází k tomu, že aplikací jednoho opatření dojde k pokrytí více hrozeb. Ideálním způsobem je proto postup shora dolů a navržení bezpečnostního opatření pro každou dvojici a vyčíslení nákladů na jeho zavedení a udržování [5, str. 172].

Opětovný odhad rizik

Cílem tohoto odhadu je zjištění rizik, kterým jsou aktiva vystavena i po přijetí bezpečnostních opatření.

Zbytková rizika

I po aplikování bezpečnostních opatření dojde ke stavu, kdy na analyzovaný systém mohou působit takzvaná zbytková rizika. Zbytková rizika můžeme dále rozdělit na akceptovaná a neakceptovaná rizika, kdy v případě druhé skupiny musíme opět provést výběr bezpečnostního opatření. V těchto případech je ale velmi vysoká pravděpodobnost, že vybrané opatření bude buďto příliš nákladné nebo z hlediska bezpečnostních opatření zcela zbytečné [4, str. 94].

Politika bezpečnosti systému informačních technologií

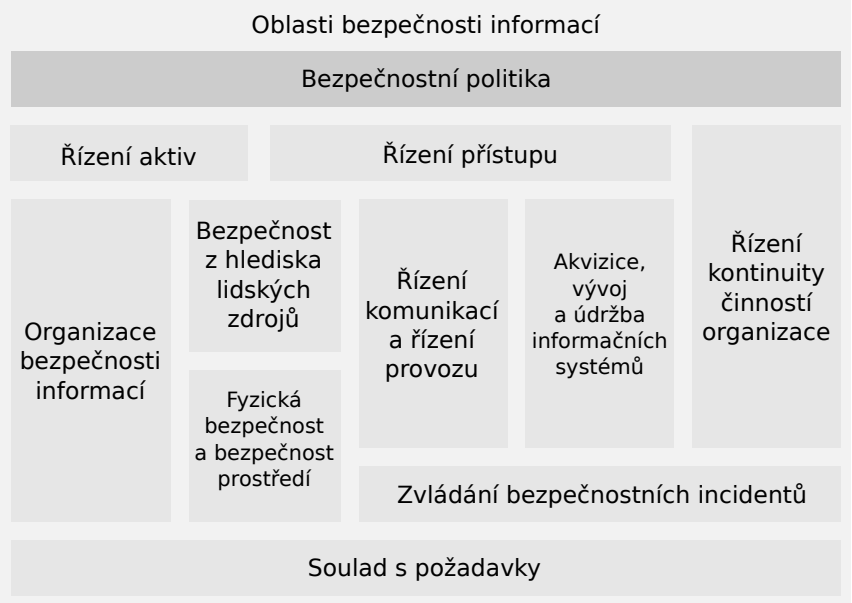
Politika bezpečnosti systémů informačních technologií by měla obsahovat seznam navrhovaných bezpečnostních opatření a u každého opatření dále popis tohoto opatření a informaci o tom, proč je přijetí tohoto opatření nezbytné [4, str. 94].

Plán bezpečnosti informačních technologií

Jedná se o dokument, jež stručně popisuje veškerá akce nutné pro implementaci plánovaných bezpečnostních opatření [4, str. 94].

2.10.9 Realizace bezpečnosti informací

Pro realizaci bezpečnosti informací budeme postupovat podle nejlepších zkušeností obsažených v normě ČSN ISO/IEC 27002:2014. Ta definuje jednotlivé oblasti bezpečnosti informací, viz obrázek 2.13 [7, str. 125]:



Obr. 2.13: Rozdělení oblasti bezpečnosti informací

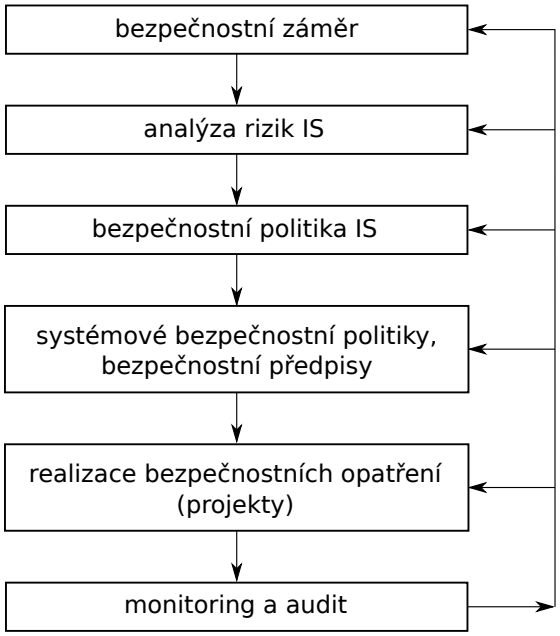
Jednotlivé oblasti znázorněné na obrázku 2.13 jsou definovány následovně [7, str. 126]:

- **Soulad s požadavky** – dokládá naplnění právních, smluvních a jiných závazků.
- **Zvládání bezpečnostních incidentů** – definuje pravidla a postupy pro zvládání bezpečnostních incidentů včetně pokynů pro shromažďování důkazních materiálů.
- **Fyzická bezpečnost a bezpečnost prostředí** – definuje pravidla pro přístup osob ke klíčovým aktivům organizace a do klíčových prostor. Dále definuje pravidla ochrany klíčových zařízení, zejména zařízení prostředí ICT.
- **Organizace bezpečnosti informací** – definuje strukturu pro řízení bezpečnosti informací, jak uvnitř organizace samotné, tak ve vztahu k externím subjektům – zákazníkům, dodavatelům apod.
- **Bezpečnost z hlediska lidských zdrojů** – definuje povinnost ochrany informací u všech pracovníků a budování bezpečnostního povědomí.
- **Řízení komunikací a řízení provozu** – definuje pravidla pro zajištění spolehlivého a bezpečného fungování produkčních a komunikačních informačních systémů dané organizace.
- **Akvizice, vývoj a údržba informačních systémů** – definuje prosazení principů bezpečnosti informací do projektů vývoje a rozvoje ICT.
- **Řízení kontinuity činnosti organizace** – definuje pravidla pro prevenci nebo minimalizaci škod v organizaci, které jsou důsledkem případné havárie či jiné mimořádné události.

- **Řízení aktiv** – definuje pravidla pro udržování přehledu o aktivech organizace včetně pravidel o stanovení odpovědnosti za udržování přiměřené míry ochrany jednotlivých aktiv organizace.
- **Řízení přístupu** – definuje pravidla přidělování přístupu ke všem prvkům ICT systémů, včetně definice pravidel pro sledování způsobu využití volných prvků ICT.
- **Bezpečnostní politika** – definuje základní pravidla bezpečnosti informací v organizaci. Dále deklaruje podporu vedení organizace k zavedení bezpečnostní politiky.

2.11 Zabezpečení elektrických informací a jeho realizace

Systémové zabezpečení informačního systému se skládá z několika, navzájem propojených, kroků. Tyto kroky ukazuje následující obrázek [2, str. 14]:



Obr. 2.14: Proces zabezpečení IS [2, str. 14]

V následujících kapitolách bude probrána každá část tohoto procesu.

2.11.1 Bezpečnostní záměr

Samotné myšlenka na zlepšení zabezpečení je sice chvályhodná věc, ale k jeho realizace je nutné, aby tímto záměrem vedení podniku pověřilo některou pracovní skupinu nebo oddělení. Samotná podpora ze strany vedení je taktéž velmi důležitým krokem při realizaci zabezpečení elektronických informací [2, str. 14].

Pověřený útvar nebo oddělení ve firmě zpracuje dokument nazvaný *Bezpečnostní záměr* a předloží ho ke schválení nejvyššímu vedení společnosti. Rozsah dokumentu není stěžejní, může jít i o krátký dokument v rozsahu jedné strany formátu A4. Důležitý je obsah tohoto dokumentu. Ten by měl deklarovat následující informace [2, str. 14]:

- Jakým způsobem bude bezpečnost řešena.
- Jakým je cílový stav.
- Jakým způsobem bude cílového stavu dosaženo.

Základním cílem bezpečnosti informací by pro každou organizaci mělo být zajištění a pokrytí takzvané **Bezpečnostní triády**, ta zahrnuje tyto akce[2] [2, str. 14]:

1. Zabezpečení důvěrnosti.
2. Zabezpečení integrity.
3. Zabezpečení dostupnosti.

Zajištěním Bezpečnostní triády dochází ke snížení negativních dopadů hrozeb.

Dokument deklarující bezpečnostní záměr organizace může, například z důvodů omezených financí, obsahovat bezpečnostní záměr pouze pro určitou část aktiv nebo pro určitou geografickou lokalitu [2, str. 14].

2.11.2 Analýza rizik

Na základě bezpečnostního záměru a cílů pro zajištění bezpečnosti informačního systému v něm obsažených je nutné, aby společnosti zmapovala skutečný stav bezpečnosti. Pro zmapování skutečného stavu zabezpečení je proto nutné, aby společnost provedla analýzu rizik spojených s bezpečností informačního systému. Do týmu zpracovávajícího analýzu rizik je vhodné zapojit, mimo vlastních zaměstnanců, i pracovníky externí firmy, kteří mají s analýzou rizik nějaké zkušenosti. vlastní zaměstnanci, jež budou zařazeni do analytického týmu by měli být vybíráni s ohledem na to, že budou analýzu rizik provádět samostatně v následujících obdobích [2, str. 14].

Výstupem provedené analýzy rizik je dokument, který obsahuje popis daného stavu bezpečnosti informačního systému v organizaci společně s riziky, která v současné době existují. Na tato rizika také, zpravidla, aplikuje opatření pro snížení jejich dopadu na přijatelnou úroveň [2, str. 15].

2.11.3 Bezpečnostní politika IS

Bezpečnostní politika informačního systému vychází ze závěrů analýzy rizik a definuje akce pro každé další akce společnosti spojené s bezpečností informačního systému.

Závěry obsažení v bezpečnostní politice informačního systému jsou posléze schváleny vedením společnosti a stávají se tak závaznými pro všechny zaměstnance dané společnosti a pro všechny pracovníky externích společností, kteří pracují s informačním systémem dané společnosti [2, str. 15].

[2]Tyto akce platí pro neprůmyslové odvětví. U průmyslových odvětví je primární zajištění dostupnost, potom zajištění integrity a až nakonec zajištění důvěrnosti

2.11.4 Systémové bezpečnostní politiky IS

Na základě principů obsažených v bezpečnostní politice informačního systému je nutné rozpracovat tyto základní principy důkladněji v systémových bezpečnostních politikách informačního systému a v ostatních bezpečnostních nařízeních a předpisech [2, str. 15].

2.11.5 Realizace bezpečnostních opatření

Bezpečnostní opatření vycházející z bezpečnostní politiky informačního systému je možné rozdělit, dle náročnosti realizace, na dvě skupiny:

- Snadno realizovatelná.
- Náročnější na realizace.

Snadno realizovatelná bezpečnostní opatření nejsou většinou náročná ani dle času, ani dle požadavku na množství personálu. Naopak druhá skupina opatření je na realizaci náročnější, a proto se většinou řeší formou dlouhodobých projektů, do kterých mohou být zapojeny i externí firmy [2, str. 16].

2.11.6 Monitoring a audit

Po samotném zavedení bezpeční politiky informačního systému je nutné stále sledovat stav zabezpečení a provádět jeho kontrolu. Na základě této kontroly je potom nutné odstraňovat zjištěné nedostatky v bezpečnostní politice informačního systému [2, str. 16].

2.11.7 Zlepšování bezpečnostních politik informačního systému

Jelikož je informační systém společnosti stále živoucí organismus zasazený ve stále se vyvíjejícím prostředí, je nutné, aby tyto změny a nové požadavky reflektovala i bezpečnostní politika informačního systému. Tyto změny by měly probíhat periodicky a dle předem stanovené metodiky [2, str. 16].

Kapitola 3

Technická řešení pro zavedení bezpečnosti informací

V následující části budou popsána vybraná technická řešení, která mohou být použita při zavádění bezpečnosti informací v organizaci.

3.1 RADIUS server

RADIUS (`Remote Authentication Dial In User Service`) je AAA služba pro vzdálenou autentizaci, autorizaci a účtování, která se používá pro přístup k síti. RADIUS je popsán v RFC 2865 (viz [8]).

Autentizace probíhá two-way hand-shakingem, který probíhá v několika krocích. V první kroku vydá uživatel pokyn klientovi k zahájení autentizace. Klient následně vytvoří Požadavek na přístup (`Access-Request`). Tento požadavek obsahuje uživatelské jméno, šifrované heslo a ID portu, přes který komunikace probíhá. Požadavek je odeslán RADIUS serveru a je nastaven timeout, po který se čeká na odpověď od RADIUS serveru. Pokud není odpověď obdržena po dobu timeoutu, je celý požadavek odeslán znovu a opět se čeká na odpověď. Počet odeslání požadavku je omezen. Jako doporučené množství pokusů je v normě uvedeno 3-5 pokusů.

Server příjme požadavek na autentizaci od klienta a ověří uživatelské údaje, které jsou v požadavku zaslané. Pokud některý údaj nesouhlasí (např. nepodaří se najít uživatelské jméno, nesouhlasí hash uživatelského hesla,...), odešle paket typu Odmítnutí přístupu (`Access-Reject`). Tento paket může v datové části, dle normy, obsahovat pouze textovou zprávu, která se zobrazí uživateli. Žádné další části nesmí, dle normy, datová část paketu obsahovat.

Jestliže se podaří uživatel ověřit v databázi RADIUS serveru (např. v databázi LDAP), je klientovi zpět odeslán paket typu Povolení přístupu (`Access-Accept`). V datové části paketu jsou potom umístěny všechny informace týkající se uživatele a přístupu k síti. Mezi tyto informace patří například konfigurační síťové informace (IP adresa brány, maska podsítě) a další informace nutné pro konkrétní službu.

Obecný formát RADIUS paketu je následující [8]:

Code	Identifier	Length
Authenticator		
Atribute		

Tab. 3.1: Formát RADIUS paketu

RADIUS paket je zabalen do datové části UDP paketu. Hodnota portu je nastavena na 1812. Formát paketu je následující:

- *Code (8 bitů)* – identifikuje typ RADIUS paketu (Access-Accept, Access-Reject atd.)
- *Identifier (8 bitů)* – obsahuje unikátní číslo paketu. Pomocí tohoto čísla je možné identifikovat duplicitní požadavky.
- *Length (16 bitů)* – specifikuje délku RADIUS paketu, konkrétně délku polí Code, Identifier, Length, Authenticator a Attribute. Hodnota tohoto pole je minimálně 20 bitů a maximálně 4096 bitů. Oktety mimo tento rozsah musí být považovány za zarovnání a musí být ignorovány. Pokud je délka paketu menší než velikost uvedená v této části, musí být v tichosti zahozen.
- *Authenticator (128 bitů)* – je náhodně vygenerované číslo, které je použito na ověřování správné autentizace. Ověření správnosti je provedeno pomocí jednocestného hashovaní sdíleného tajemství a hodnoty z pole Authenticator.

3.2 Systémy správy verzí

Systémy správy verzí pomáhají v organizaci vést agendu verzování produktu. Systémy pro správu verzí nabízejí několik funkcí, které organizace zaměřená na vývoj software nebo hardware ocení. Mezi tyto funkce patří:

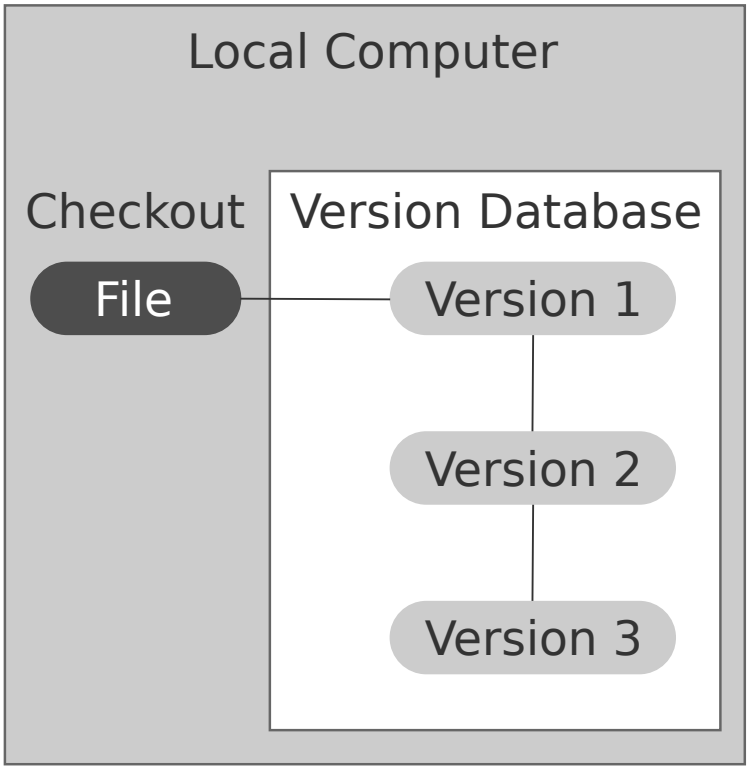
- Záznam změn souboru v čase.
- Vrácení změn v souboru do stavu dle určitého data.
- Návrat k původní verzi projektu.
- Zobrazení změn, které byly provedeny jinými uživateli.

Dále rozdělujeme dva základní typy systémů pro správu verzí [9]:

- Lokální.
- Centralizovaný.
- Decentralizovaný.

3.2.1 Lokální systém správy verzí

Tento systém pracuje na principu ukládání verzí na lokálním počítači. Je velmi podobný stavu, kteří používají někteří méně zkušení uživatelé, kteří své soubory ukládají do podsložek pojmenovaných dle data, kdy na projektu pracovali.



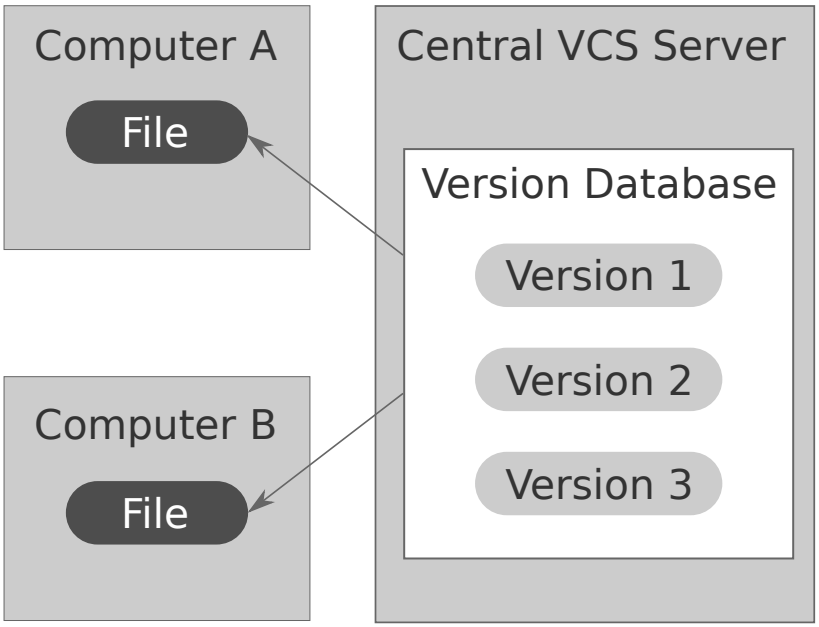
Obr. 3.1: Schéma lokálních systémů správy verzí [9]

Podobných způsobem fungují i lokální systémy pro správu verzí. Tyto systémy si na speciální místo v systému ukládají informace o změnách v pracovních souborech. Zástupcem tohoto přístupu je například oblíbený systém RCS. Ten funguje tak, že si z každého pracovního souboru ukládá seznam rozdílů (RCS používá pojem záplaty). Aplikací těchto záplat je možné poskládat libovolný předchozí kteréhokoliv souboru v libovolném čase.

3.2.2 Centralizovaný systém správy verzí

Centralizovaný systém správy verzí nabízí řešení největšího neduhu lokálních systémů správy verzí, a to problém spolupráce více uživatelů na jednom projektu. Pro tuto potřebu byl vytvořen Centralizovaný Server pro Správu Verzí. Funkcí tohoto serveru je centralizované uchování seznamu rozdílů. Přístup k těmto seznamům mají potom všichni uživatelé. Uživatelé však nestahují celou historii změn, ale pouze nejnovější verzi (takzvaný Snapshot). Zástupcem tohoto přístupu je například CVS nebo Subversion.

Samotné seznamy jsou ale uloženy pouze na jednom místě, na serveru samotném. To znamená, že v případě poruchy serveru (výpadek napájení, systémová chyba) není možné

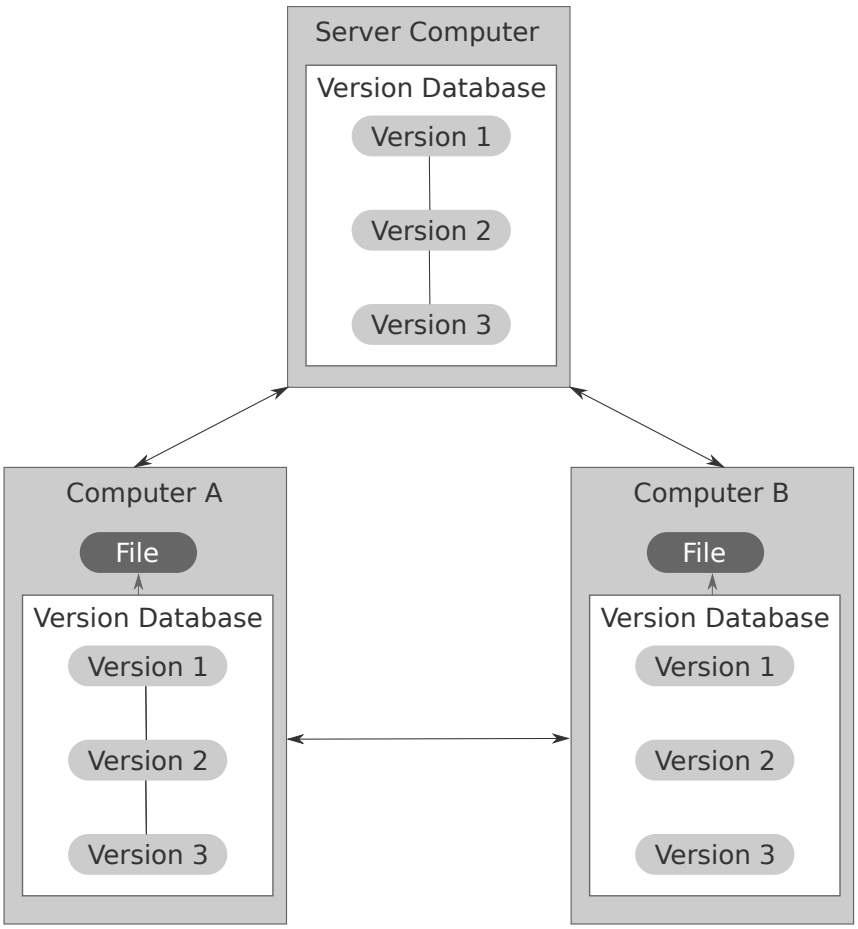


Obr. 3.2: Schéma centralizovaných systémů správy verzí [9]

stahovat změny, popřípadě nahrávat změny nové. Dojde-li k poruše pevného disku, není možné a v případě, že nebyly dobře prováděny zálohy, tak dochází ke ztrátě veškeré historie změn souborů. Jednoduše řečeno, ve všech případech, kdy je historie souborů uložena na jednom místě, riskujete, že v případě problémů přijdete o vše.

3.2.3 Distribuovaný systém správy verzí

Distribuované systémy správy verzí přináší prozatím nejdokonalejší způsob sdílení změn mezi uživateli. U distribuovaných systémů správy verzí uživatel nestahuje pouze Snapshoot, ale zrcadlí stav celého repositáře na svém lokálním pracovišti. Samotná práce potom probíhá tak, že uživatel pracuje se svou lokální kopií, kterou může po skončení práce nahrát na server, odkud si ji můžou stáhnout všichni ostatní spolupracovníci. Zástupcem toho přístupu je verzovací systém Git nebo systém Mercurial.

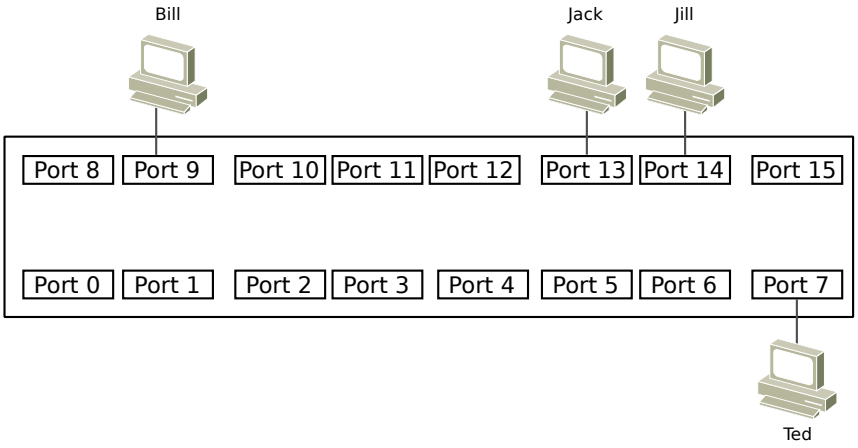


Obr. 3.3: Schéma distribuovaných systémů správy verzí [9]

3.3 Technologie VLAN

Virtuální VLAN (*Virtual Local Area Network*) slouží k logickému rozdělení počítačové sítě, které je nezávislé na fyzickém uspořádání. Pomocí technologie VLAN je tedy možné původní počítačovou síť rozdělit na menší sítě uvnitř fyzické struktury [10].

Klasický systém zapojení počítačů do jednoho přepínače demonstruje obrázek 3.4:



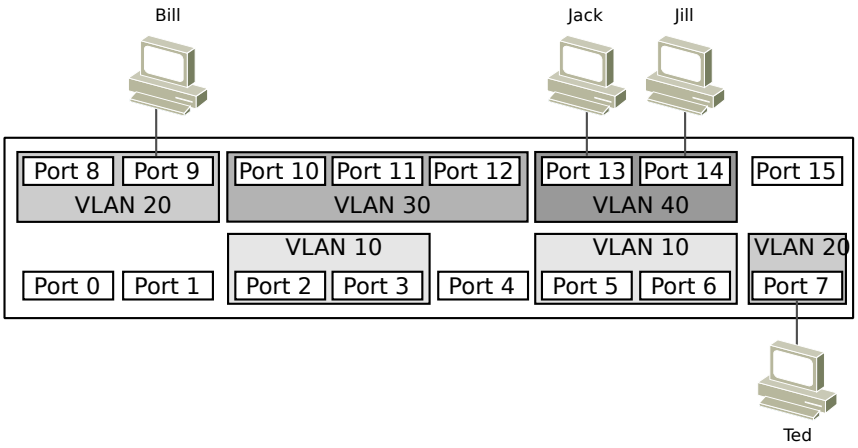
Obr. 3.4: Klasické schéma sítě zapojené do jednoho přepínače bez VLAN [11, str. 24] (upraveno)

U takto strukturované sítě jsou všichni klienti připojeni do jedné fyzické sítě a mají tak přístup prakticky ke všem zdrojům. Pakliže by přepínač disponoval ještě bezdrátovým rozhraním (šlo by tedy fakticky o kombinaci přepínače a přístupového bodu), potom by měli přístup ke stejným zdrojům i uživatelé s mobilními zařízeními.

Problém nastává v případě, kdy chceme oddělit od sebe jednotlivé typy uživatelů. Jako příklad můžeme použít společnost zabývající se implementací informačních systémů. Taková firma má oddělení vývojářů a obchodníků a skupinu vedoucích pracovníků (management). V případě, kdy by se například vedení společnosti rozhodlo znemožnit přístup zaměstnanců marketingu na zdroje využívané vývojem, muselo by řešit oddělení těchto skupin uživatelů. Existovaly by dvě možnosti.

- Vytvoření nové fyzické sítě.
- Použití virtuálních sítí.

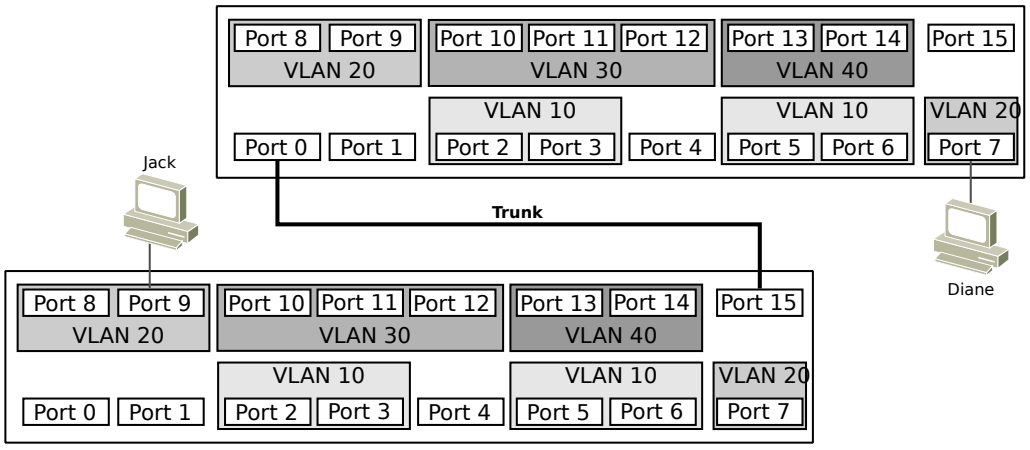
Použití virtuálních sítí by v tomto případě znamenalo pouze změnu nastavení přepínače o vytvoření adekvátních virtuálních sítí.



Obr. 3.5: Schéma několika VLAN sítí na jednom přepínači [11, str. 24]

Jak je vidět na obrázku 3.6, byly vytvořeny čtyři virtuální sítě, každá pro určité pracovníky. Také platí, že se uživatelé ze sítě VLAN 40 defaultně nedostanou například do sítě VLAN 20. Došlo tak k logické segmentaci počítačové sítě na několik podsítí, aniž by bylo nutné měnit fyzickou topologii sítě.

V případě, že bychom chtěli propojit v rámci jedné virtuální sítě uživatele oddělené například na dvou patrech budovy, museli bychom propojit i přepínače samotné. K tomuto účelu slouží takzvaný **trunk**. Trunk je přenosový spoj propojující dva přepínací systémy (přepínače nebo směrovače). Použití „trunku“ je zobrazeno na následujícím obrázku:



Obr. 3.6: Použití Trunku mezi dvěma přepínači [11, str. 26]

3.3.1 Komunikace v rámci VLAN

V praxi existují dvě situace, při nichž se řeší příslušnost k virtuální síti, a to v případě komunikace v rámci jednoho přepínače a při komunikaci v rámci dvou a více přepínačů.

Při komunikaci v rámci jednoho přepínače je situace jednodušší, stačí, aby si přepínač ve své operační paměti udržoval tabulku portu a příslušné virtuální sítě. V případě komunikace potom jen, na základě směrovacích pravidel, směruje či zahodí danou komunikaci.

V případě komunikace mezi více přepínači přichází na řadu standard IEEE 802.1Q [12], který upravuje standardní Ethernetový rámec a přidává do něj VLAN tag.

Preambule	**Oddělovač začátku rámce**	**Cílová MAC adresa**	**Zdrojová MAC adresa**	**802.1Q tag (volitelný)**	**Délka**	**Data**	**FCS**	**Mezera mezi pakety**
7 B	1 B	6 B	6 B	4 B	2 B	42 – 1500 B	4 B	12 B

Tab. 3.2: Ethernetový rámec s VLAN Tag polem

Formát 802.1Q tagu je potom následující:

16 bitů	**3 bity**	**1 bit**	**12 bitů**
TPID	TCI		
	PCP	DEI	VID

Tab. 3.3: Formát 802.1Q tagu [12, str. 160]

Kde jednotlivé položky mají následující význam:

- **TPID** – *Tag protocol identifier* (VLAN protokol ID) je generická hodnota, která identifikuje, že se jedná o protokol s VLAN tagem. Hodnota tohoto pole je vždy 0x8100.
- **TCI** – *Tag control information* obsahuje tyto další informace:
  - **PCP** – *Priority code point* obsahuje tříbitovou hodnotu uživatelské priority rámce a určuje, do které fronty má být na přepínači zařazen.
  - **DEI** – *Drop eligible indicator* identifikuje, zda může být rámec zahozen v případě, kdy nastane přetížení.
  - **VID** – *VLAN identifier* určuje číslo virtuální sítě. Z délky plyne, že je možné mít v jedné síti maximálně 4096 virtuálních LAN. Jelikož jsou však dva identifikátory rezervovány 0xFFF a 0x0, může být virtuálních LAN v jedné fyzické síti maximálně 4094.

Kapitola 4

Analýza současného stavu

V analytické části práce bude kladen důraz na analýzu současného stavu zabezpečení přístupu k datům ve zvolené společnosti. Analýza si dále klade za cíl odhalení nedostatků současného řešení. Z takto zjištěných nedostatků bude, později, vyplývat návrh sady bezpečnostních opatření.

4.1 Popis společnosti

Tato práce je zaměřena na společnost Netcope Technologies, a. s. se sídlem v brněnské městské části Komín. V současné době, kdy je zpracovávána tato analýza, firma sídlí v prostorách VTP Unis na ulici Sochorově, kam se přestěhovala z prostor Jihomoravského inovačního centra.

Společnost samotná vznikla v roce 2015, kdy se od mateřské společnosti Invea-Tech, a. s. oddělilo oddělení vývoje FPGA. Po vzniku společnosti existovala v rámci společnosti dvě oddělení, a to oddělení vývoje FPGA a oddělení pro vysokofrekvenční obchodování (oddělení HFT[1]). Dále ve společnosti existovalo obchodní oddělení a pozice technického ředitele. V současné době má společnost stále stejnou strukturu, avšak narostl počet pracovníků ve všech odděleních. Oddělení vývoje (FPGA i HFT) zaměstnává 11 lidí, zaměstnanců obchodního oddělení a marketingu je celkem 7. Technický ředitel byl jmenován generálním ředitelem, pozice technického ředitele není momentálně obsazena, a dále byla obsazena pozice ředitele pro operativu. Celkem tedy ve společnosti, ke dni zpracovávání této analýzy, pracuje 20 osob.

Obr. 4.1: Logo společnosti Netcope Technologies, a. s.

Hlavní činností společnosti je vývoj síťových karet pro vysokorychlostní akceleraci síťového provozu, vedlejší činností je vývoj hardware pro vysokofrekvenční obchodování. Běžný

[1] High Frequency Trading

zaměstnanec vývoje tak přijde do kontaktu, jednak se síťovou kartou ve formě surového hardware (osazené PCB), tak s programovými kódy firmwaru a obslužného software. Od roku 2016 je společnost Netcope Technologies, a. s. držitelem certifikátu ISO 9001.

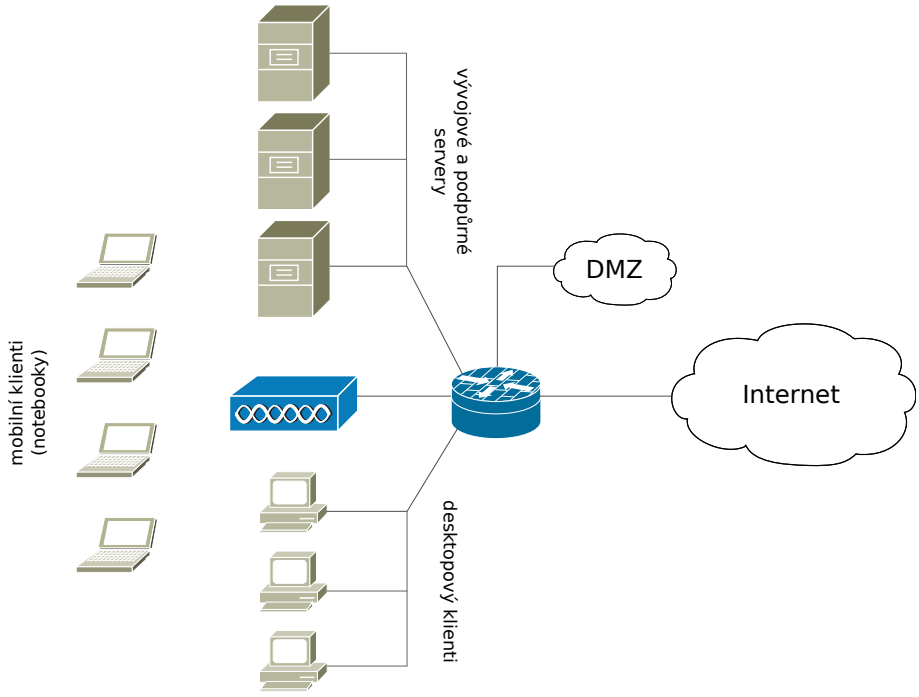
4.2 Popis současné infrastruktury

Infrastruktura společnosti je umístěna jen v rámci sídla firmy. Princip *Bring your own device* není společností tolerován. Většina pracovníků pracuje se stolními počítači, jen zaměstnanci obchodního oddělení, marketingu a vedoucí vývoje (FPGA i HFT) mají firmou přidělené notebooky.

Infrastruktura v sídle společnosti je rozdělena na dva bezpečnostní úseky:

- Vnitřní síť.
- Demilitarizovaná zóna.
- VoIP ústředna.

Schéma sítě je znázorněno na obrázku 4.2.



Obr. 4.2: Schéma vnitřní sítě

Popis jednotlivých částí sítě bude popsán v následujících podkapitolách.

4.2.1 Vnitřní síť

Vnitřní síť společnosti obsahuje větší množství různých produkčních a pomocných serverů:

- vývojové servery – několik strojů Dell různých typů a dále pak několik vývojových strojů postavených nad základními deskami od společnosti SuperMicro,
- sdílené datové uložiště QNAP TS-879U-RP[2] ,
- CentOS Linux server v roli interního DNS serveru,
- Zaměstnanecké počítače a notebooky.

Většina zaměstnanců vývojového týmu pracuje na strojích Fujitsu nebo Dell s nainstalovanými operačními systémy z rodiny Linuxových distribucí (OpenSUSE, Fedora, Manjaro Linux), jen jeden zaměstnanec využívá operační systém Microsoft Windows 10.

V případě obchodního oddělení a ředitelů jsou na pracovních noteboocích nainstalovány operační systémy Microsoft Windows 10, ale opět se zde najde výjimka, jeden notebook s operačním systémem Ubuntu Linux.

V rámci vnitřní síťové infrastruktury je zapojen Wi-Fi router ZyXEL NBG6616[3] a dále pak síťová tiskárna s kopírkou a skenerem od společnosti Y-SOFT (konkrétně se jedná o model Konica Minolta C364). Tato tiskárna má v sobě vestavěný tiskový a kopírovací/skenovací server. Přístup k tiskárně je možný pouze se zaměstnaneckou kartičkou.

4.2.2 Demilitarizovaná zóna

Samotný perimetr síťového prostoru je zabezpečen hraničním firewallem, který je poskytnut v rámci sítě v objektu VTP Unis.

Demilitarizovaná zóna je ve společnosti zřízena zejména z důvodu, kdy zaměstnanci obchodního oddělení potřebují prezentovat firemní produkty zákazníkovi. Jelikož by byl transport veškeré výpočetní techniky, nutné pro prezentaci produktu, velmi náročný, bývá prezentační server zapojen do DMZ a je mu přiřazena veřejná IP adresa. Takový server je pak dostupný, jak z vnější, tak i z vnitřní sítě. Pro server samotný je ale vnitřní síť nedostupná.

4.2.3 VoIP ústředna

Vedení společnosti plánuje v dohledné době pořízení vlastní VoIP ústředny. Tato ústředna by měla sloužit pro zaměstnance obchodního oddělení, kteří by přes ni měli realizovat hovory v době, kdy budou pracovně mimo území České republiky. Motivací pro pořízení vlastní VoIP ústředny je snížení nákladů za hlasové služby v době služebních cest.

4.3 Interní služby a zdroje

V rámci interní počítačové sítě existuje několik služeb a zdrojů, jejich dostupnost je kritická pro korektní fungování firemního prostředí a pro korektní pracovní činnost. Mezi tyto služby patří:

[2] Více informací na: https://www.qnap.com/en/product/model.php?II=16
[3] Více informací na: http://www.zyxel.com/products_services/nbg6616.shtml?t=p&tabOrder=5

- Vývojové servery.
- GIT Lab server.
- SVN server.
- DNS server.
- Samba server.

4.3.1 Vývojové servery

Nejdůležitějším zdrojem v interní síti jsou vývojové servery. Pro potřeby vývoje jsou, v rámci vnitřní sítě, zapojeny vývojové servery. Jelikož veškerý vývoj, jak hardware, tak software probíhá vzdáleně na vývojových serverech, je jejich stoprocentní dostupnost klíčová pro plynulý chod firmy.

Jako vývojové servery jsou použity, jak už bylo zmíněno dříve, vesměs 1U – 2U zařízení od společnosti Dell a potom volně stojící základní desky značky SuperMicro a Advantech. Tato zařízení mají rozdílnou konfiguraci, společnou vlastností je osazený procesor z rodiny Intel 26x serverové provenience a vždy alespoň 32 GB RAM paměti.

4.3.2 GIT Lab Server

Druhou nejdůležitější službou je GIT Lab server, kde jsou uloženy repositáře systému GIT, který zastupuje rodinu distribuovaných systémů správy verzí (viz 3.2.3).

Opět platí, že dostupnost této služby je pro plynulý chod vývoje velmi důležitá. V případě, kdy by došlo ke krátkodobé nedostupnosti této služby, je tento fakt řešitelný již z podstaty distribuovaných systémů správy verzí, jelikož každý uživatel má u sebe dostupnou celou historii revizí a na GIT Lab server slouží pouze jako centrální uložiště těchto informací.

4.3.3 SVN server

GIT Lab server nahradil v minulosti SVN server, který sloužil pro správu zdrojových kódů dříve. SVN server je příkladem centralizovaného systému správy verzí (viz 3.2.2).

V současné době jsou v rámci tohoto serveru dostupné některé finální designy pro koncové uživatel. Jeho stoprocentní dostupnost pro plynulý chod firmy není zcela kritická, avšak jeho dlouhodobý výpadek by mohl znamenat problém s dostupností produktů pro zákazníky.

4.3.4 DNS server

V interní síti je též připojen stroj, jehož funkcí je poskytování DNS záznamů. Jedná se o starý vývojový server Dell s pouze 2 GB RAM paměti, jehož funkcí je právě převod interních IP adres na lidsky srozumitelné pojmenování vývojových serverů a klientských počítačů.

Nutnost DNS záznamů pro klientské počítače není na první pohled tak důležitá, ale jelikož platí, že na všechny servery se přihlašuje pod jedním vývojovým uživatelským účtem, je vhodné vědět, kdo jiný na vývojovém stroji pracuje. Právě proto bylo rozhodnuto o zřizování klientských DNS záznamů i pro jednotlivé klientské (vývojové) stanice. DNS server je nakonfigurován tak, že adresy z rozsahu `1-99` přiřazuje staticky, tedy klientům s DNS záznamem, adresy `100-254` jsou určeny pro dynamické přiřazení. Formát lidsky čitelné adresy je následující: `address.int.netcope.com`.

Pro snadnou správu a přehled DNS záznamů je veden seznam s uvedenou statickou IP adresou a DNS záznamem. Proto v případě, kdy by DNS server nebyl dostupný, tak je možné použít tento seznam a přístup na vnitřní vývojové servery nebude nijak omezen, jen může být méně rychlý a komfortní.

4.3.5 Samba server

Posledním zdrojem v rámci vnitřní sítě je SAMBA server, na kterém jsou uložena starší vývojová data a používá se už spíše sporadicky pro uložení méně důležitých nebo nepracovních dat. Objevují se na něm tak většinou fotografie s týmových akcí. Jeho dostupnost by neměla nijak výrazně ovlivnit chod firmy.

4.4 Externí služby

V následující kapitole budou popsány služby, které nejsou provozovány přímo v sídle společnosti, ale jsou poskytovány externími dodavateli.

4.4.1 Google Apps

V roce 2016 došlo na úrovni managementu firmy k rozhodnutí o migraci e-mailů, interních kalendářů a interních dokumentů do cloudového uložiště. Jako dodavatel tohoto řešení byla zvolena společnost Google se svým programem G Suite (dříve Google Apps for Work)[4].

Ze SLA uzavřených mezi společností Netcope Technologies, a. s. a společností Google plyne například závazek, kdy poskytovatel zaručuje, že data budou uložena v datových centrech, která splňují všechny mezinárodní bezpečnostní normy. Dále je poskytovatelem zabezpečeno, že data budou uložena v jeden okamžik minimálně ve třech datových centrech na různých tektonických deskách, aby byla zajištěna maximální dostupnost dat i v případě živelné havárie. V neposlední řadě obsahuje SLA ustanovení, podle kterého je společnost Netcope Technologies, a. s. majitelem dat a společnost Google pro tato data poskytuje pouze úložný prostor.

4.4.2 Webový server

Web server s firemní webovou prezentací je umístěn v datovém centru mimo sídlo firmy. Prostředky v datovém centru jsou zabezpečeny maximální ochranou obsahující ochranu

[4] Viz https://gsuite.google.cz/

přístupu do budovy a samotná serverovna je zabezpečena přístupovým systémem s přístupem na čipovou kartu. V rámci bezpečnostních politik jsou definovány přesné skupiny zaměstnanců, které mají oprávnění pro přístup do serverové části datového centra.

Dalším stupněm zabezpečení je instalovaný kamerový systém se záznamem a v neposlední řadě je serverovna připojena ke dvěma redundantním zdrojům elektrické energie s externími motorgenerátory pro případ výpadku elektrické energie.

Požární ochrana dat je řešena pomocí plynového hasícího systému, kdy v případě požáru je do serverovny tlakově nahnán nehořlavý plyn, který vytěsní kyslík, a tak zamezí hoření.

4.4.3 Server správy majetku

Jako nástroj pro správu majetku používá společnost Netcope Technologies, a. s. řešení od společnosti NetSuite. Toto řešení provozuje společnost NetSuite na vlastních webových serverech ve vlastním datacentru. Proto pro veškerý přístup k majetku je nutná plná dostupnost těchto serverů.

Stejně, jako v případě webového serveru, jsou datové servery umístěny v datovém centru s vypracovanými bezpečnostními politikami. Samozřejmostí je i vysoká ochrana dat proti požáru.

4.4.4 Vývojové servery sdružení CESNET

Společnost Netcope Technologies, a. s. úzce spolupracuje se sdružením CESNET, z. s. p. o. Využívá taktéž jeho vývojové servery. Tyto servery jsou umístěny v objektu Fakulty informačních technologií Vysokého učení technického v Brně. Serverovna, která vznikla v rámci projektu IT4I splňuje všechny bezpečnostní požadavky, mezi které patří definovaná bezpečnostní politika, přístup do serverové části na čipovou kartu a v neposlední řadě také moderní hasicí systém.

4.5 Fyzická a personální bezpečnost

V následující části bude popsána bezpečnost z pohledu fyzické a personální bezpečnosti:

4.5.1 Fyzická bezpečnost budovy

Společnost sídlí v prostorách budov VTP Unis na ulici Sochorově v Brně. Komplex VTP Unis leží v nezáplavové oblasti a v rámci celého komplexu je zřízen kamerový systém se záznamem. Pro vstup do prostor společnosti je nutné použití přístupových karet.

Pro fyzický přístup k vývojovým serverům je nutné speciální oprávnění, které mají pouze vedoucí jednotlivých vývojových úseků. V rámci objektů VTP Unis je nainstalována účinná klimatizace pro udržení optimální teploty vývojových serverů. Pro zajištění business continuity jsou instalovány záložní zdroje.

4.5.2 Personální bezpečnost

Personální bezpečnost v organizaci je zabezpečena zejména pomocí smluvních vztahů a nastavených přístupových oprávnění dat v rámci serverů Google. Jednotlivý zaměstnanci tak mají přístup pouze k dokumentům, které jsou pro jejich práci nezbytné. Přístup k citlivým souborům (například smlouvám jednotlivých zaměstnanců nebo jejich osobním údajům) je umožněn pouze pověřeným zaměstnancům s použitím speciálního hardwarového klíče. Služby spojené s účetnictvím společnost využívá služeb externího dodavatele.

4.6 Analýza rizik v současném stavu

V rámci analýzy rizik budou definována aktiva společnosti a případná rizika a hrozby, která mohou nastat ve vztahu k těmto aktivům.

4.6.1 Identifikace a ohodnocení aktiv

Společnost spravuje aktiva v těchto kategoriích:

- `Data`: Důležitou váhu ve společnosti mají interní informace. Jde zejména o know-how společnost, o zdrojové kódy produktů, interní informace o zapojení síťové infrastruktury a podobně. Většina těchto informací je uložena v rámci serverů společnosti Google, zdrojové kódy jsou uloženy v rámci databáze systému GIT na interních serverech společnosti.

  Dalšími důležitými daty jsou informace o vyplývající z obchodních vztahů. Jedná se především o smlouvy mezi společností a klienty, v menší míře o smlouvy mezi společností a dodavateli. Všechny smlouvy jsou hostovány na serverech společnosti NetSuite, která firmě dodává stejnojmenné řešení.

- `Hardware`: Nejdůležitějším aktivem společnosti, z pohledu její podnikatelské činnosti, je hardware. Tím nejpodstatnějším prvkem hardware jsou vývojové servery a příslušná síťová infrastruktura. Síťovou infrastrukturou jsou zamýšleny jak přepínače a routery, ale také generátor síťového provozu Spirent. Jelikož společnost vyvíjí vysokorychlostní síťové aplikace na vlastních FPGA vývojových kartách, je nutné do hardwarových aktiv započítat také tyto vývojové karty.

  Každý zaměstnanec společnosti má svůj vlastní počítač nebo notebook. Součástí vnitřní sítě firmy je i síťová tiskárna.

- `Software`: Do software společnosti patří zejména operační systémy nainstalované na jednotlivých pracovních stanicích (v případě systémů Microsoft Windows k nim patří i licence). Dalším důležitých softwarem je vývojový software Xilinx Vivado.

- `Služby`: Mezi aktiva, která můžeme zařadit do skupiny služeb patří zejména služba správy zdrojových kódů (GIT), služba sdílení dat (Google Drive) a služba správy majetku (NetSuite). Mezi další služby patří připojení k internetu nebo telefonní linka. Neméně důležitou službou je i poskytování elektrické energie.

S aktivy samotnými jsou spojena rizika, která můžeme ohodnotil. Hodnocení rizik dle dopadu na organizaci zobrazuje tabulka 4.1.

Hodnota aktiva	Riziko	Dopad na organizaci
1	bezvýznamné	Nemá dopad na organizaci
2	akceptovatelné	Zanedbatelný dopad na organizaci
3	nízké	Mohou vzniknout potíže či finanční ztráty
4	nežádoucí	Vážné potíže a finanční ztráty
5	nepřijatelné	Hrozí zaniknutí společnosti

Tab. 4.1: Hodnocení rizik dle dopadu na organizaci [4, str. 82]

Shrňme si nyní i seznam identifikovaných aktiv dle skupiny (viz 4.2:

Typ	Aktivum
Data	Data zaměstnanců (smlouvy a osobní data)
	Data zákazníků
	Data dodavatelů
	Interní informace (zdrojové kódy, know-how)
HW	pracovní stanice
	notebooky
	vývojové servery
	generátor síťového provozu Spirent
	vývojové karty
	ostatní servery
	síťová tiskárna
	přepínače
	routery
SW	operační systém a licence
	vývojový software Xilinx Vivado
Služby	služba správy zdrojových kódů (GIT)
	služba sdílení dat (Google Drive)
	služba správy majetku (NetSuite)
	připojení k internetu
	telefonní linka
	zdroj elektrické energie

Tab. 4.2: Seznam a typ identifikovaných aktiv

Když máme vytvořeny seznamy aktiv a také tabulku, která nám pomůže hodnotit aktiva dle dopadu na organizaci, zbývá už jen vzorec pro výpočet hodnoty aktiva:

$$Hodnota = \frac{\text{dostupnost} + \text{důvěrnost} + \text{integrita}}{3}$$

Nyní již můžeme přistoupit k samotnému ohodnocení aktiv:

Typ	Aktivum	Dostupnost	Důvěrnost	Integrita	Hodn. aktiva
Data	Data zaměstnanců	5	5	5	5
	Data zákazníků	3	5	3	4
	Data dodavatelů	3	3	3	3
	Interní informace	5	5	5	5
HW	pracovní stanice	3	5	3	4
	notebooky	3	5	3	4
	vývojové servery	5	5	5	5
	generátor síťového provozu Spirent	2	2	2	2
	vývojové karty	4	2	2	3
	ostatní servery	3	2	1	2
	síťová tiskárna	2	1	3	2
	přepínače	5	4	4	4
	routery	5	4	4	4
SW	operační systém a licence	3	4	4	4
	vývojový software	5	3	4	4
Služby	služba správy zdrojových kódů	3	5	4	4
	služba sdílení dat	5	5	5	5
	služba správy majetku	4	4	4	4
	připojení k internetu	3	1	3	2
	telefonní linka	2	2	2	2
	zdroj elektrické energie	3	1	2	2

Tab. 4.3: Aktiva a jejich ohodnocení

4.6.2 Identifikace a ohodnocení hrozeb dle ČSN ISO/IEC 27005

Identifikace a ohodnocení hrozeb dle ČSN ISO/IEC 27005:2014 [13] zobrazuje následující tabulka:

	Dostupnost	**Důvěrnost**	**Integrita**
Fyzické poškození			
Oheň	3	1	1
Poškození vodou	3	1	1
Znečištění	3	1	3
Zničení vybavení nebo médií	3	1	3
Prach, koroze, zamrznutí	3	1	3
Přírodní události			
Povodně	3	1	1
Ztráta klíčových služeb			
Selhání klimatizace nebo chladícího systému	2	1	2
Ztráta energie	3	1	3
Kompromitování informací			
Špionáž a škodlivý kód	1	5	1
Krádež média nebo dokumentu	2	5	3
Krádež vybavení	4	5	4
Získání dat ze zničených médií	1	5	1
Data z nedůvěryhodných zdrojů	1	4	3
Manipulace s hardware	4	2	5
Manipulace se software	4	5	4
Technická selhání			
Selhání zařízení	4	1	4
Selhání software	4	1	5
Neoprávněné akce			
Neoprávněné použití zařízení	4	5	4
Podvodné zkopírování software	3	5	3
Použití ukradeného nebo zkopírovaného software	4	5	4
Poškození dat	4	2	4
Nelegální zpracování dat	3	4	4
Kompromitování funkcí			
Chybné použití	3	3	2
Zneužití práv	3	5	3
Padělání práv	2	4	2

Tab. 4.4: Identifikace a ohodnocení hrozeb dle ČSN ISO/IEC 27005:2014

4.6.3 Matice rizik a matice zranitelnosti

Na základě identifikovaných aktiv a hrozeb byly stanoveny dvě matice:

- **Matice zranitelnosti** – určuje zranitelnost aktiva vůči konkrétní hrozbě.
- **Matice rizik** – určuje míru možného rizika.

Pro potřeby hodnocení si dále stanovíme dvojici stupnic:

- Stupnici pravděpodobnosti hrozeb.
- Stupnici míry rizika.

Následující tabulka zobrazuje stupnici pravděpodobnosti hrozeb:

Stupeň	**Pravděpodobnost**
1	nahodilá
2	nepravděpodobná
3	pravděpodobná
4	velmi pravděpodobná
5	trvalá

Tab. 4.5: Stupnice pravděpodobnosti rizika [4, str. 90]

Jelikož bylo identifikováno větší množství aktiv, je tabulka s maticí zranitelnosti rozdělena na dvě části:

Zranitelnost (V)	Popis aktiva	data zaměstnanců	data zákazníků	data dodavatelů	interní informace	pracovní stanice	notebooky	vývojové servery	Spirent	vývojové karty	ostatní servery	tiskárna	přepínače	routery
	Hodnota aktiva (A)	5	4	3	5	4	4	5	2	3	2	2	4	4
Popis hrozby	**Pravděpodobnost (T)**													
Fyzické poškození														
Oheň	1	3	2	2	3	2	2	2	1	2	2	1	2	2
Poškození vodou	1	3	2	2	3	2	2	2	1	2	2	1	2	2
Znečištění	3				1	3	3	3	1	3	3			
Zničení vybavení nebo médií	2	3	3	3	3	3	3	2	2	3	2	1	2	2
Prach, koroze, zamrznutí	2	3	3	3	2	3	3	2	2	3	2	1	2	2
Přírodní události														
Povodně	1	3	3	3	3	3	2	3	3	3	2	2	3	3
Ztráta klíčových služeb														
Selhání klimatizace nebo chladícího systému	2				2	2	1	3	3	2	2	1	2	2
Ztráta energie	3				2	3	2	3	3	1	2	1	3	3
Kompromitování informací														
Špionáž a škodlivý kód	4	4	4	4	4	4	4	4	1		3	1	3	3
Krádež média nebo dokumentu	3	4	4	4	4									
Krádež vybavení	2		3			3	3	2	1	2	1	1	2	2
Získání dat ze zničených médií	2	4	4	4	3									
Data z nedůvěryhodných zdrojů	2	3	3	3	3									
Manipulace s hardware	2	2	2	2	2	3	3	3	1	2	1	1	1	1
Manipulace se software	2	3	3	3	3									
Technická selhání														
Selhání zařízení	3	1	1	1	3	3	3	2	1	3	2	1	3	3
Selhání software	2	1	1	1	1			2	1	1	1	1	3	3
Neoprávněné akce														
Neoprávněné použití zařízení	3	4	4	4	3	2	3	3	2	1	2	1	3	3
Podvodné zkopírování software	2	2	2	2	3									
Použití ukradeného nebo zkopírovaného software	2	2	2	2	3									
Poškození dat	3	4	4	4	4									
Nezákonné zpracování dat	2	3	3	3	3									
Kompromitování funkcí														
Chybné použití	3	3	4	3	3									
Zneužití práv	2	3	3	3	3									
Padělání práv	2	3	3	3	3									

Tab. 4.6: Matice zranitelnosti aktiv (1. část)

Zranitelnost (V)	Popis aktiva	operační systém a licence	vývojový software	správa zdroj. kódů	služba sdílení dat	služba správy majetku	připojení k internetu	telefonní linka	zdroj elektrické energie
	Hodnota aktiva (A)	4	4	4	5	4	2	2	2
Popis hrozby	**Pravděpodobnost (T)**								
Fyzické poškození									
Oheň	1	2	2	2	2	2	2	1	1
Poškození vodou	1	2	2	2	2	2	2	1	1
Znečištění	3							2	2
Zničení vybavení nebo médií	2	2							2
Prach, koroze, zamrznutí	2							2	2
Přírodní události									
Povodně	1								3
Ztráta klíčových služeb									
Selhání klimatizace nebo chladícího systému	2			2	1	2			
Ztráta energie	3	3	3	3	3	3	3	2	3
Kompromitování informací									
Špionáž a škodlivý kód	4	4	3	2	3	1			
Krádež média nebo dokumentu	3			2	3	1			
Krádež vybavení	2						2		
Získání dat ze zničených médií	2	2		3	1	1			
Data z nedůvěryhodných zdrojů	2	3		2	1	1			
Manipulace s hardware	2	2	3	3	1	2	3	2	1
Manipulace se software	2	3	2	1					
Technická selhání									
Selhání zařízení	3	2	3	2	2	2	3	1	1
Selhání software	2	3	3	1					
Neoprávněné akce									
Neoprávněné použití zařízení	3	3	3	2	2	1			
Podvodné zkopírování software	2	3	1	2					
Použití ukradeného nebo zkopírovaného software	2	2	1	1					
Poškození dat	3	3	1	3	1	2			
Nezákonné zpracování dat	2								
Kompromitování funkcí									
Chybné použití	3	3	2	2	3	1	2		
Zneužití práv	2	3	2	2	3	1	2		
Padělání práv	2	3	2	2	3	1	2		

Tab. 4.7: Matice zranitelnosti aktiv (2. část)

Na základě hodnot získaných stanovením matice zranitelností, můžeme vypočítat míru rizika. Pro tento výpočet použijeme vzorec:

$$R = T \times A \times V \tag{4.1}$$

kde R značí vypočítanou míru rizika, T značí pravděpodobnost toho, že hrozba, jako taková, nastane, A značí hodnotu aktiva a konečně V označuje míru zranitelnosti.
Následující tabulka zobrazuje stupně rizika a dopad na organizaci:

Stupeň	**Pravděpodobnost**	**Dopad na organizaci**
<0, 10)	bezvýznamné	Bez dopadu na organizaci
<10, 20)	akceptovatelné	Zanedbatelný dopad
<20, 30)	nízké	Může mít malý negativní dopad nebo finanční ztrátu
<30, 60)	nežádoucí	Vážné potíže a finanční ztráty
>60	nepřijatelné	Hrozí zánik firmy

Tab. 4.8: Míra rizika [4, str. 90]

Jelikož bylo identifikováno velké množství aktiv, byla matice rizika rozdělena na dvě tabulky (viz tabulky 4.9 a 4.10[5]):

[5]Obě tabulky jsou vytvořeny vlastnoručně

Zranitelnost (V)	Popis aktiva	data zaměstnanců	data zákazníků	data dodavatelů	interní informace	pracovní stanice	notebooky	vývojové servery	Spirent	vývojové karty	ostatní servery	tiskárna	přepínače	routery
	Hodnota aktiva (A)	5	4	3	5	4	4	5	2	3	2	2	4	4
Popis hrozby	**Pravděpodobnost (T)**													
Fyzické poškození														
Oheň	1	15	8	6	15	8	8	10	2	6	4	2	8	8
Poškození vodou	1	15	8	6	15	8	8	10	2	6	4	2	8	8
Znečištění	3				15	36	36	45	6	27	18			
Zničení vybavení nebo médií	2	30	24	18	30	24	24	20	8	18	8	4	16	16
Prach, koroze, zamrznutí	2	30	24	18	20	24	24	20	8	18	8	4	16	16
Přírodní události														
Povodně	1	15	12	9	15	12	8	15	6	9	4	4	12	12
Ztráta klíčových služeb														
Selhání klimatizace nebo chladícího systému	2				20	16	8	30	12	12	8	4	16	16
Ztráta energie	3				30	36	24	45	18	9	12	6	36	36
Kompromitování informací														
Špionáž a škodlivý kód	4	80	64	48	80	64	64	64	8		24	8	48	48
Krádež média nebo dokumentu	3	60	48	36	60									
Krádež vybavení	2		24			24	24	20	4	12	4	4	16	16
Získání dat ze zničených médií	2	40	32	24	30									
Data z nedůvěryhodných zdrojů	2	30	24	18	30									
Manipulace s hardware	2	20	16	12	20	24	24	30	4	12	4	4	8	8
Manipulace se software	2	30	24	18	30									
Technická selhání														
Selhání zařízení	3	15	12	9	45	36	36	30	6	27	12	6	36	36
Selhání software	2	10	8	6	10			20	4	6	4	4	24	24
Neoprávněné akce														
Neoprávněné použití zařízení	3	60	48	36	45	24	36	45	12	9	12	6	27	27
Podvodné zkopírování software	2	20	16	12	30									
Použití ukradeného nebo zkopírovaného software	2	20	16	12	30									
Poškození dat	3	60	48	36	60									
Nezákonné zpracování dat	2	30	24	18	15									
Kompromitování funkcí														
Chybné použití	3	45	48	27	45									
Zneužití práv	2	30	24	18	30									
Padělání práv	2	30	24	18	30									

Tab. 4.9: Matice rizik (1. část)

Zranitelnost (V)	**Popis aktiva**	operační systém a licence	vývojový software	správa zdroj. kódů	služba sdílení dat	služba správy majetku	připojení k internetu	telefonní linka	zdroj elektrické energie
	Hodnota aktiva (A)	4	4	4	5	4	2	2	2
Popis hrozby	**Pravděpodobnost (T)**								
Fyzické poškození									
Oheň	1	8	8	8	10	8	4	2	2
Poškození vodou	1	8	8	8	10	8	4	2	2
Znečištění	3							12	12
Zničení vybavení nebo médií	2	16							8
Prach, koroze, zamrznutí	2							8	8
Přírodní události									
Povodně	1								6
Ztráta klíčových služeb									
Selhání klimatizace nebo chladícího systému	2			16	10	16			
Ztráta energie	3	36	36	36	45	36	18	12	12
Kompromitování informací									
Špionáž a škodlivý kód	4	64	48	32	60	16			
Krádež média nebo dokumentu	3			24	45	12			
Krádež vybavení	2						8		
Získání dat ze zničených médií	2	16		24	10	18			
Data z nedůvěryhodných zdrojů	2	24		16	10	8			
Manipulace s hardware	2	16	24	24	10	16	12	8	4
Manipulace se software	2	24	16	8					
Technická selhání									
Selhání zařízení	3	24	36	24	30	24	18	6	6
Selhání software	2	24	24	8					
Neoprávněné akce									
Neoprávněné použití zařízení	3	36	36	24	30	12			
Podvodné zkopírování software	2	24	18	16					
Použití ukradeného nebo zkopírovaného software	2	16	18	8					
Poškození dat	3	36	12	36	15	24			
Nezákonné zpracování dat	2								
Kompromitování funkcí									
Chybné použití	3	36	24	24	45	15	12		
Zneužití práv	2	36	24	24	45	15	12		
Padělání práv	2	36	24	24	45	15	12		

Tab. 4.10: Matice rizik (2. část)

4.7 Zhodnocení současného stavu

Z analýzy provedené v předchozí kapitole vyplývá fakt, že největší míra rizika plyne ze skupin *Kompromitování informací*, *Neoprávněné akce* a *Kompromitování funkcí*. Proto bude v návrhu řešení přikročeno k vyhledání řešení zejména pro tyto skupiny hrozeb. V rámci hledání bezpečnostních opatření bude kladen důraz také na vyhledání opatření pro mobilní a přenosná zařízení, jelikož jich v organizaci existuje větší množství.

Vedením společnosti bylo rozhodnuto, po předložení matice rizik, akceptovat všechna bezvýznamná a akceptovatelná rizika. Naopak rizika s nízkým, nežádoucím a nepřijatelným stupněm rizika akceptována nejsou. Následující tabulka shrnuje akceptovaná a neakceptovaná rizika:

Riziko	**Akceptace**
Fyzické poškození	
Oheň	Ano
Poškození vodou	Ano
Znečištění	Ne
Zničení vybavení nebo médií	Ne
Prach, koroze, zamrznutí	Ne
Přírodní události	
Povodně	Ano
Ztráta klíčových služeb	
Selhání klimatizace nebo chladícího systému	Ne
Ztráta energie	Ne
Kompromitování informací	
Špionáž a škodlivý kód	Ne
Krádež média nebo dokumentu	Ne
Krádež vybavení	Ne
Získání dat ze zničených médií	Ne
Data z nedůvěryhodných zdrojů	Ne
Manipulace s hardware	Ne
Manipulace se software	Ne
Technická selhání	
Selhání zařízení	Ne
Selhání software	Ne
Neoprávněné akce	
Neoprávněné použití zařízení	Ne
Podvodné zkopírování software	Ne
Použití ukradeného nebo zkopírovaného software	Ne
Poškození dat	Ne
Nezákonné zpracování dat	Ne
Kompromitování funkcí	
Chybné použití	Ne
Zneužití práv	Ne
Padělání práv	Ne

Tab. 4.11: Souhrn akceptovaných a neakceptovaných rizik

Velká většina hrozeb je již ve společnosti řešena formou interních nařízení a předpisů. Tyto hrozby shrnuje následující tabulka 4.12. Řádky, u nich je ve sloupci *Vyřešeno* uvedena hodnota „Ne“ znázorňují oblasti zabezpečení, kde není bezpečnost řešena dostatečně a bude jim proto věnována zřetel v praktické části této práce.

Hrozba	Přijatá opatření	Vyřešeno
Fyzické poškození		
Oheň	A.11.1.4	Ano
Poškození vodou	A.11.1.4	Ano
Znečištění	—	Ne
Zničení vybavení nebo médií	A.11	Ano
Prach, koroze, zamrznuté	A.11.2.4	Ano
Přírodní události		
Povodně	A.11.1.4, A.11.1.5, A.11.2.1	Ano
Ztráta klíčových služeb		
Selhání klimatizace nebo chladícího systému	A.11.2.2, A.11.2.4	Ano
Ztráta energie	—	Ne
Kompromitování informací		
Špionáž a škodlivý kód	A.9.1.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.4.1, A.11.2.6, A.12.2.1, A.12.6.2, A.14.1.2, A.14.1.3	Ne
Krádež média nebo dokumentu	A.6.2.1, A.8.3.3, A.9.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.4.1, A.11.2.5, A.11.2.6, A.11.2.8, A.12.2.1, A.13.2.1, A.13.2.2, A.14.1.2, A.14.1.3	Ne
Krádež vybavení	A.7.2.3, A.7.3.1, A.11.1.1, A.11.1.2, A.11.1.3, A.11.2.1, A.11.2.5	Ano
Získání dat ze zničených médií	A.11.2.7	Ano
Data z nedůvěryhodných zdrojů	A.12.6.2, A.13.1	Ano
Manipulace s hardware	A.11.1.1, A.11.1.3, A.11.2.1	Ano
Manipulace se software	A.6.2.2, A.9.1.1, A.9.2.2, A.9.2.3, A.11.2.8, A.11.2.9, A.12.2.1, A.12.5.1, A.12.6.2, A.14.2.4	Ano
Technická selhání		
Selhání zařízení	A.11.1.4, A.11.1.5, A.11.2.1, A.11.2.4	Ne
Selhání software	A.12.4.4	Ne
Neoprávněné akce		
Neoprávněné použití zařízení	A.9.1.2, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.2, A.11.1.1, A.11.1.2, A.11.1.3, A.11.2.1, A.11.2.6, A.11.2.8, A.12.2.1, A.12.4.1, A.12.4.3, A.13.1.3	Ne
Podvodně zkopírovaný software	A.7.2.3, A.11.2.8, A.12.5.1	Ano
Použití ukradeného nebo zkopírovaného software	A.7.2.3, A.12.5.1	Ano
Poškození dat	A.9.1.2, A.9.4.1, A.12.2.1 A.11.2.8, A.12.3.1, A.12.6.2, A.14.1.3	Ne
Nezákonné zpracování dat	A.11.2.8, A.11.2.9, A,12.2.1, A.12.4.1, A.12.4.3, A.13.2.1, A.13.2.2, A.13.2.3, A.14.1.2, A.14.1.3	Ano
Kompromitování funkcí		
Chybné použití	—	Ne
Zneužití práv	A.7.2.3, A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.3, A.12.4.1, A.12.4.3	Ne
Padělání práv	A.9.2.1, A.9.4.2	Ano

Tab. 4.12: Souhrn vyřešených a nevyřešených hrozeb

Kapitola 5

Návrh řešení

5.1 Bezpečnostní opatření dle ČSN ISO/IEC 27002:2014

Na základě analýzy rizik z předchozí kapitoly a komunikace s vedením společnosti byla vybrána sada opatření z přílohy A normy ČSN ISO/IEC 27001:2014. Pro samotnou realizaci byla využita norma ČSN ISO/IEC 27002:2014.

Následující tabulka 5.1 shrnuje opatření dle ČSN ISO/IEC 27002:2014, která budou nově zavedena nebo revidována na základě informací získaných z analýzy rizik:

Hrozba	**Opatření**
Fyzické poškození	
Znečištění	A.11.2.4
Ztráta klíčových služeb	
Ztráta energie	A.11.2.2
Kompromitování informací	
Špionáž a škodlivý kód	A.6.2.1, A.9.1.2, A.9.2, A.9.3.1, A.9.4.2, A.9.4.3, A.9.4.5, A.11.1.1, A.11.2.9, A.13.1.1, A.13.1.3
Krádež média nebo dokumentu	A.9.1.2, A.9.2, A.9.3.1, A.9.4.2, A.9.4.3, A.9.4.5, A.11.1.1, A.11.2.9, A.13.1.1, A.13.1.3
Technická selhání	
Selhání zařízení	A.11.2.2, A.11.2.4
Selhání software	A.11.2.4
Neoprávněné akce	
Neoprávněné použití zařízení	A.9.1.2, A.9.2, A.9.3.1, A.9.4.2, A.9.4.3, A.9.4.5, A.11.1.1, A.11.2.9, A.13.1.1, A.13.1.3
Poškození dat	A.12.3
Kompromitování funkcí	
Chybné použití	A.7.2.3
Zneužití práv	A.7.3.1, A.9.4.2, A.11.2.9, A.13.1.3

Tab. 5.1: Souhrn opatření pro potlačení hrozeb

5.1.1 Organizace bezpečnosti informací (A.6)

Cílem této části normy ISO 27001:2014 je vytvoření řídícího rámce, který bude zodpovědný za zahájení a udržování bezpečnosti informací v organizaci. Úkolem tohoto řídícího rámce je taktéž zajištění bezpečnosti dat při jejich využívání na mobilních zařízeních a při práci na dálku (například z domu – *homeoffice*).

Kontakt se zvláštními zájmovými skupinami A.6.1.4

Pro zajištění optimální úrovně bezpečnosti a povědomí o aktuálních hrozbách je doporučeno, aby CISO („*chief information security officer*“) pravidelně sledoval stránky národního centra kybernetické bezpečnosti https://www.govcert.cz/ a stránky národního CSIRT České republiky (viz https://www.csirt.cz/). Dále se doporučuje účast na událostech spojených s bezpečností a jejím vylepšováním. Tyto události jsou uvedeny pod záložkou *Informační servis, Akce/Události* na stránkách národního centra kybernetické bezpečnosti.

Společně s událostmi zaměřenými na bezpečnost nabízí Národní centrum kybernetické bezpečnosti též pravidelná školení zaměřená na legislativu spojenou s kybernetickou a informační bezpečností. CISO se také důrazně doporučuje aplikovat doporučení získaná ze stránek národního centra kybernetické bezpečnosti v co nejkratším termínu, aby byla plně zachována bezpečnost informací v síti.

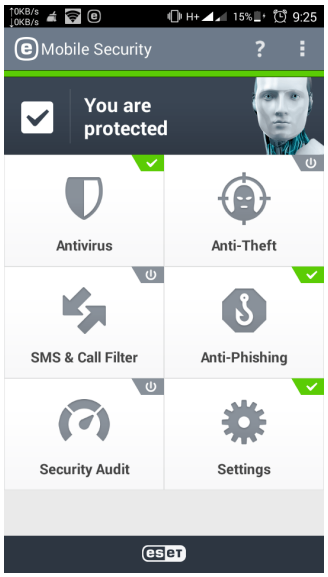
Přínosem tohoto opatření pro organizaci je získání bezpečnostního povědomí a získání přehledu o aktuálních trendech v oblasti bezpečnosti informací. Stejně tak může společnost navázat kontakt nebo i cílenou spolupráci s odborníky na bezpečnost.

Politika mobilních zařízení A.6.2.1

Zajištění bezpečnosti mobilních zařízení pro zajištění bezpečnosti informací je podobně důležité, jako zajištění bezpečnosti informací a pracovních stanicích a noteboocích. Vhledem ke stále rostoucí oblibě mobilních zařízení a jejich stále většího používání je tedy nutné, aby byla tato zařízení taktéž přísně zabezpečena.

Samozřejmostí na všech mobilních zařízeních je nastavení dostatečně silného vstupního hesla (PINU). Délka hesla by měla být minimálně 4 znaky. PIN pro přístup do telefonu by měl být pravidelně měněn. Interval změny PINU pro přístup do mobilního zařízení by neměl přesáhnou 6 měsíců.

Společně s dostatečně silným a často aktualizovaným vstupním heslem je samozřejmostí, aby byl v mobilním zařízení nainstalován vhodný antivirový program. Z vlastní zkušenosti preferuji řešení společnosti ESET, papírově je však v roce 2017 nejlepším antivirovým programem Bitdefender. Ve prospěch řešení společnosti ESET však mluví i fakt, že má v Česku své přímé obchodní zastoupení, zato společnost Bitdefender prodává svá řešení v Česku pouze přes prostředníka. Proto bylo jako nejvhodnější antivirové řešení pro společnost vybráno řešení slovenské společnost ESET software.



Obr. 5.1: Uživatelské prostředí aplikace ESET Mobile Security for Android [14]

Pro kompletní zabezpečení mobilních zařízení v organizaci je přípraven produkt **ESET Endpoint Security pro Android**, ten nabízí tyto vlastnosti [14]:

- Ochrana koncových zařízení:
  - **Ochrana v reálném čase** – Kontroluje všechny aplikace a navázané komunikace na přítomnost škodlivého kódu. Chrání před online i offline hrozbami, detekuje útoky USSD.
  - **Anti-Phishing** – Chrání před podvodnými stránkami, které se snaží získat citlivé informace jako je uživatelské jméno, heslo, podrobnosti o kreditních kartách nebo bankovnictví.
  - **Kontrola při nabíjení** – Umožňuje provést kontrolu v případech, kdy se zařízení nabíjí nebo je zamknutá obrazovka.
  - **Filtr volání a SMS** – Na zařízení se dovolá a pošle zprávu jen určená osoba. Definovat lze také čas, kdy je zařízení dostupné.
- Bezpečnost zařízení:
  - **Mobile Device Management (MDM)** – Administrátor má možnost uplatňovat na zařízení základní bezpečnostní politiky pro mobilní zařízení. Produkt automaticky upozorňuje uživatele a správce v případech, které nejsou v souladu s firemní politikou, a doporučuje provést změny. Mezi tato nastavení patří:
    * Definovat požadavek na silné heslo.
    * Určit maximální počet pokusů pro odemknutí zařízení. Při překročení dojde automaticky k přechodu do továrního nastavení.
    * Určit maximální dobu platnosti hesla.
    * Určit čas pro zamknutí obrazovky při nečinnosti.

    * Vyzvat uživatele k šifrování zařízení.
    * Zablokovat integrovanou kameru.

- **Kontrola aplikací:** umožňuje tato nastavení:
  - Zablokovat definované aplikace.
  - Blokovat dle kategorií – hry, sociální sítě atd.
  - Blokovat dle práv – kam aplikace přistupují.
  - Blokovat dle zdroje.
  - Vytvořit výjimky na základě whitelistů.
  - Přes ESET Remote Administrator definovat seznam povinně instalovaných aplikací.

- Anti-Theft:
  - **Události** – Všechny vzdálené příkazy provádí správce pomocí ESET Remote Administrator nebo přes SMS s dvou-faktorovou autentizací, případně přímo z grafického rozhraní.
  - **Zpráva na obrazovku** – Odešle libovolnou zprávu např. s kontaktními informacemi na ztracené zařízení. Zpráva se zobrazí na obrazovce formou vyskakovacího okna.
  - **Admin kontakty** – Obsahují seznam důvěryhodných telefonních čísel chráněných administrátorským heslem. SMS příkazy je poté možné odesílat jen z těchto čísel. Uvedené kontakty dostávají upozornění z Anti-Theftu.
  - **Informace na zamknuté obrazovce** – Správce může vytvořit a odeslat na zařízení vlastní zprávu (např. s kontaktními informace). Zpráva se zobrazí na obrazovce i v případě, že je zařízení zablokováno.
  - **Základní vzdálené akce** – Správce může vzdálené zamknout/ odemknout zařízení, spustit zvukovou sirénu, lokalizaci, smazat data a podobně.

Pro korektní a systematické chování antiviru na všech zařízením je nutné, aby bylo hned po jeho nainstalování přikročeno k jeho nastavení. Toto nastavení může být provedeno jednak ručně pomocí vestavěného průvodce – to ale není pro větší počet zařízení příliš komfortní – ale také pomocí ESET Remote Administrator. ESET Remote Administrator nabízí tyto moduly a funkcionality:

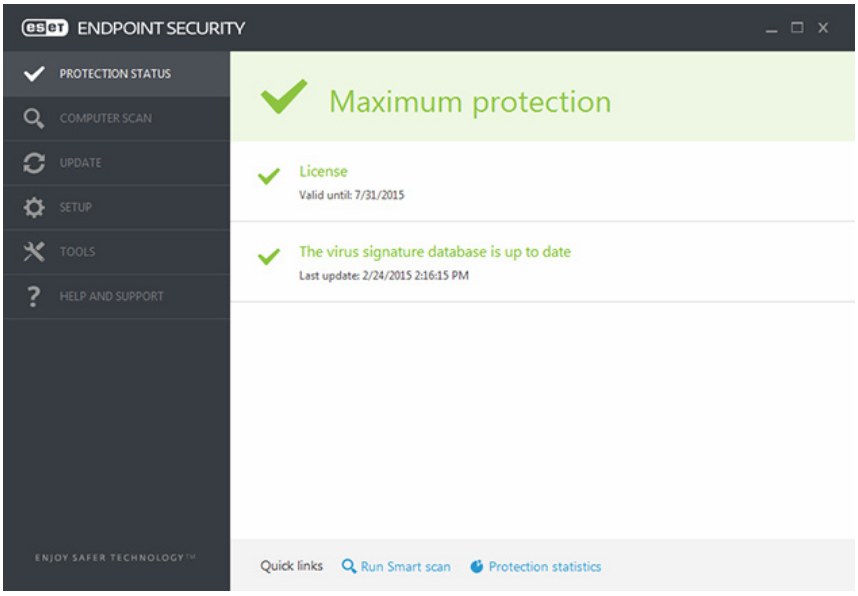
- Správa všech licencí na jednom místě přes prohlížeč i mimo ESET Remote Administrator.
- Vytvoření více administrátorů s různými oprávněními.
- Bezpečná komunikace s klienty založená na šifrování TLS 1.0.
- Administrátorský systém chránění 2FA.

- Nastavení politik.
- Dynamické statistiky skupiny.
- a další

Bezpečnost stolních počítačů a notebooků

Stejně, jako v případě mobilních zařízení, platí i pro pracovní stanice a notebooky povinnost chránit svá data antivirem. Jelikož byl, pro mobilní platformu, zvolen antivirus z rodiny produktů společnosti ESET, je nasnadě vybrat podobný antivirus i pro stolní počítače a notebooky. Tímto vybraným produktem je ESET Endpoint Security for Windows, který nabízí tyto vlastnosti a funkce [15]:

- Ochrana koncových stanic:
  - **Antivirus a Antispyware** – Odstraňuje všechny typy hrozeb, včetně virů, rootkitů, červů a spyware. Volitelné používání cloudové databáze vylepšuje výkon a detekci.
  - **Pokročilá kontrola paměti** – Monitoruje chování škodlivých procesů a kontroluje je ihned po rozbalení v paměti. Takto je schopná detekovat i těžce šifrované hrozby.
  - **Exploit Blocker** – Nová technologie detekce škodlivého kódu chrání před cílenými útoky a dosud neznámými hrozbami tzv. zero day útoky.
  - **Optimalizace pro virtuální prostředí** – ESET Shared Local Cache ukládá metadata kontrolovaných souborů a znovu se nekontrolují (i v rámci virtuálního prostředí), což má pozitivní dopad na rychlost skenování systému.



Obr. 5.2: Uživatelské prostředí aplikace ESET Endpoint Security [15]

- Ochrana přístupu k datům:
  - **Anti-Phishing** – Chrání uživatele před pokusy získat jejich citlivé informace, jako jsou hesla, bankovní data nebo údaje o kreditních kartách.
  - **Firewall** – Brání neautorizovanému přístupu do firemní sítě a chrání firemní data před zneužitím.
  - **Vulnerability Shield** – Rozšiřuje schopnosti firewallu a zlepšuje detekci tzv. CVE (*Common Vulnerabilities and Exposures*), neboli běžných zranitelností v síti na protokolech SMB, RPC, RDP.
  - **Kontrola zařízení** – Umožňuje blokovat nebo povolit konkrétní výměnná média jako jsou CD, DVD, USB apod. Umí vytvořit pravidla pro uživatelské skupiny.
  - **Web kontrola** – Filtruje přístup k internetovým stránkám dle kategorií např. hry, sociální sítě, nakupování a další.
  - **Ochrana proti botnetu** – Chrání před infiltrací botnet malwarem – zabraňuje šíření spamu a síťových útoků z daného zařízení.
- Snadné použití:
  - **Nízké systémové nároky**.
  - **Přívětivá vzdálená správa** – Produkt lze snadno připojit do nástroje vzdálené správy ESET Remote Administrator, který nabízí perfektní přehled nad bezpečností v síti.
  - **Odinstalace jiných řešení** – Při instalačním procesu se proskenuje počítač, a pokud je v systému nalezen nadbytečný bezpečnostní software, dojde k jeho odstranění.
  - **Nastavitelná viditelnost GUI** – Grafické rozhraní programu je možné kompletně zneviditelnit pro koncového uživatele, včetně ikony v dolní liště na hlavní obrazovce.

5.1.2 Bezpečnost lidských zdrojů (A.7)

Disciplinární řízení (A.7.2.3)

Jelikož společnost Netcope Technologies, a. s. nemá dosud implementován disciplinární řád, je doporučeno disciplinární řád implementovat. V následující části je uveden návrh disciplinárního řádu (návrh se inspiruje z disciplinárního řádu VUT [16]).

1. **Úvodní ustanovení**
   Tento disciplinární řád upravuje disciplinární přestupky zaměstnanců společnosti Netcope Technologies, a. s., zejména procesy před zahájením disciplinárního řízení, stanovuje předpisy pro disciplinární komisi a také stanovuje postupy pro udělování sankcí.

2. **Disciplinární přestupek**
   Disciplinárním přestupkem se rozumí takové jednání, které je v rozporu s nařízeními společnosti nebo v rozporu s nařízeními a zákony české republiky. Za disciplinární přestupek je též považováno porušení bezpečnostních pokynů a nařízení.

3. **Sankce**
   Za disciplinární přestupek lze zaměstnanci udělit tyto sankce:

   (a) `Napomenutí` – používá se v případě méně závažného přestupku nebo za přestupek spáchaný z nedbalosti.

   (b) `Udělení pokuty až do výše 4,5násobku platu` – tato sankce se používá v případech, kdy přestupkem vznikla společnosti finanční ztráta. Výše sankce se odvíjí od výše způsobené škody.

   (c) `Ukončení pracovního poměru` – v případě, kdy byl přestupek spáchán vědomě a (nebo) je přestupek páchán opakovaně. K ukončení pracovního poměru může být přistoupeno s okamžitou platností. V případě této sankce může být rozhodnuto i tom, zda bude poskytnuto odstupné.

   (d) `Soudní vyrovnání` – uděluje se v případě zvláště závažného porušení firemních nařízení, které mělo prokazatelně vést k poškození firmy.

   Při ukládání sankcí se přihlíží k formě, jakou k disciplinárnímu přečinu došlo. Stejně tak se přihlíží k okolnostem, které k disciplinárnímu přečinu vedly, ke škodám, které firmě vznikly, k míře zavinění a také k dosavadnímu chování zaměstnance. Při ukládání sankce je též nutné přihlédnout k tomu, k míře snahy zaměstnance o nápravu následků.

   Od uložení sankce může být upuštěno v případě, kdy samotné projednávání přestupku vede k nápravě. Popřípadě je možné od sankce ustoupit v případě, kdy k přestupku došlo z nedbalosti (tedy neúmyslně) anebo je přestupek méně závažný.

4. **Disciplinární komise**
   Disciplinární komise je složena ze CIO, vedoucího zaměstnance, který je podezřelý ze spáchání disciplinárního přestupku a z dalších tří zaměstnanců, kteří dané problematice rozumí. Komise je usnášení schopná pouze v případě, kdy jsou přítomni všichni její členové. Za nepřítomné členy disciplinární komise je nutné vybrat adekvátní náhradu. Hlasy všech členů disciplinární komise jsou si rovny.

5. **Účastník disciplinárního řízení**
   Účastníkem disciplinárního řízení je vždy zaměstnanec, proti kterému je vedeno disciplinární řízení. Tento má rovněž právo během disciplinárního řízení předkládat důkazy a vyjadřovat se ke všem podkladům pro jednání.

6. **Disciplinární řízení**
   Před samotným zahájením disciplinárního řízení je nutné shromáždit informace o disciplinárním přestupku:

(a) ověřit, že šlo skutečně o disciplinární přestupek,

(b) ověřit, zda šlo o událost opakovanou nebo jde o první případ,

(c) ověřit, zda byl incident způsobem záměrně nebo z nedbalosti. Pokud to není možné, je čin klasifikován, jako disciplinární přestupek z nedbalosti,

(d) zjistit, zda byl zaměstnanec správně informován o svých odpovědnostech a povinnostech.

Projednání přestupku je oznámeno osobě, proti které je disciplinární řízení vedeno a to nejméně 30 dní před zahájením disciplinárního řízení. O podání oznámení a jeho převzetí musí existovat písemný doklad.

7. **Jednání komise**
Pro jednání komise během disciplinárního řízení jsou stanovena tato pravidla:

(a) Je svoláno iniciační jednání komise, kde jsou předloženy zjištěné důkazy a je stanoven termín projednávání přestupku se zaměstnancem.

(b) Zaměstnanec je informován o zahájení disciplinárního řízení a o termínu projednávání disciplinárního přestupku s jasným vyjádřením, že se očekává její účast. Součástí oznámení musí být i poučení o možnosti dodat důkazy na svou obhajobu.

(c) Ve stanovený den je opět svolána disciplinární komise s účastí zaměstnance, proti kterému je vedeno disciplinární řízení. Pokud se zaměstnanec opakovaně nezúčastní anebo se z jednání řádně neomluví, má komise právo vydat rozhodnutí i bez účasti osoby, proti které je vedeno disciplinární řízení.

(d) V odůvodněných případech (zejména v případě vážnějšího přestupku) může komise vydání svého rozhodnutí odložit. V takovém případě může osoba, která je předmětem disciplinárního řízení, využít času mezi jednáními k předkládání nových důkazů.

(e) Disciplinární komise rozhodne o sankci.

(f) Rozhodnutí komise je předloženo zaměstnanci a sankce je vykonána.

Během celého procesu disciplinárního řízení může být toto řízení, na popud libovolného člena komise, zastaveno nebo zrušeno. O zastavení nebo zrušení disciplinárního jednání musí rozhodnou jednohlasně disciplinární komise.

Z jednání disciplinární komise musí být v každém případě zpracován a archivován písemný report.

5.1.3 Řízení přístupu (A.9)

Cílem tohoto opatření je zamezení přístupu k informacím a k vybavení pro zpracování informací osobám s nedostatečnými oprávněními. Uživatelé jsou, dle tohoto opatření, plně zodpovědní za ochranu svých autentizačních prostředků (přístupové informace, přístupové karty atd.). Součástí tohoto opatření je též stanovení dostatečné bezpečnosti přístupu.

Přístup k sítím a síťovým službám A.9.1.2

Pro sdílení důležitých interních informací používá společnost Netcope Technologies služeb společnosti Google, konkrétně jde o využívání balíku Google Apps. Pro sdílení informací je používána součást Google Drive, jež umožňuje nastavení přístupových práv pro všechny uživatele. Pro přístup do této služby je nutná autorizace účtem společnosti Google.

Tento účet zaměstnanci rovněž používají pro přistup k emailu, kalendáři a ostatním službám, které jsou v rámci balíku Google Apps nabízeny.

Pro přístupy k vývojovým serverům využívají všichni uživatelé osobní SSH klíče. Bez tohoto SSH klíče není umožněn přístup na žádný vývojový server. V případě poruchy vývojového serveru je možný přímý přistup pouze z výrobní místnosti, do nichž má přístup pouze vedoucí výroby.

Pro přístup k podpůrným serverům, jako je například server se zdrojovými kódy, je vyžadováno ověření na základě kombinace uživatelského jména a hesla. V případě poruchy se přístup řídí stejnými pravidly, jako v případě poruchy vývojových serverů.

Pro ověření přístupu k síti a získání oprávnění pro přístup k síťovým serverům je doporučená instalace serveru pro ověření uživatelských oprávnění. Doporučovaným řešením je instalace RADIUS serveru (technologie RADIUS serveru byla popsána v kapitole 3.1).

Správa a řízení přístupu uživatel A.9.2

Pro zajištění správy přístupových práv musí být stanoven dostatečný rámec pro registraci a deregistraci příchozích a odchozích zaměstnanců – uživatelů.

Při příchodu nového zaměstnance by měl tento zaměstnanec obdržet tyto přístupové informace:

- Přístupový čip pro přístup do prostor společnosti.
- Přístupový údaje (uživatelské jméno a jednorázové heslo) ke službám poskytovaným v rámci Google Apps.
- Přístupové údaje (uživatelské jméno a jednorázové heslo) pro přístup na server se zdrojovými kódy.
- Uživatelské jméno a jednorázové heslo pro přístup k pracovnímu stroji (*v případě, kdy si neinstaluje vlastní operační systém na pracovní stroj*).

Novému zaměstnanci by měla být nastavena taková oprávnění, která se shodují s jeho firemní pozicí, tedy například vývojář by měl obdržet oprávnění pro přístup k informacím nutným pro vývoj, nikoli však k obchodním nebo marketingovým informacím. Přidělování dodatečných oprávnění by mělo být řízeno přírůstkovou metodou, kdy se dodatečná oprávnění přidělují postupně. O všech oprávněních by měly být vedeny přesné a aktuální informace. Řízení přístupových informací je v kompetenci systémového administrátora. Zjednodušená matice uživatelských oprávnění je zobrazena v tabulce 5.2.

Dalším důležitým opatřením v případě řízení uživatelských práv by mělo být jejich časové omezení. Výjimkou z tohoto principu by byla základní uživatelská práva (tedy ta

Uživatelské jméno	Pozice	Oprávnění			
		Vývoj	Marketing	Obchod	HR
Uživatel 1	Vývoj	Ano	Ne	Ne	Ne
Uživatel 2	Produktový manager	Ano	Ano	Ne	Ne
Uživatel 3	CTO	Ano	Ne	Ne	Ne
Uživatel 4	CSO	Ne	Ano	Ano	Ne
Uživatel 5	HR	Ne	Ne	Ne	Ano

Tab. 5.2: Zjednodušená matice uživatelských oprávnění

práva, která se vztahují přímo k vykonávané pozici). Všechna dodatková práva by měla být udělována jen na příslušnou dobu a po uplynutí této doby by měla být odebírána.

Můžeme tedy matici oprávnění rozšířit způsobem zobrazeným v tabulce 5.3 (za povšimnutí stojí pozice *Produktový manager*, který má omezené oprávnění pro přístup k marketingovým a obchodním materiálům):

Uživatelské jméno	Pozice	Oprávnění			
		Vývoj	Marketing	Obchod	HR
Uživatel 1	Vývoj	neomezené	Ne	Ne	Ne
Uživatel 2	Produktový manager	neomezené	31.8.2017	31.5.2017	Ne
Uživatel 3	CTO	neomezené	Ne	Ne	Ne
Uživatel 4	CSO	Ne	neomezené	neomezené	Ne
Uživatel 5	HR	Ne	Ne	Ne	neomezené

Tab. 5.3: Tabulka oprávnění rozšířená o datum konce platnosti oprávnění

Používání tajných autentizačních informací A.9.3.1

Pro udržení vysoké úrovně bezpečnosti informací je nutné, aby byla zajištěna kvalita autentizačních informací. Kvalitní autentizační informace pomáhají zabránit neautorizovanému přístupu. Doporučuje se proto, aby byli všichni zaměstnanci seznámeni s následujícími bezpečnostními opatřeními.

Vlastnosti silného a bezpečného hesla:

- délka hesla minimálně 8 znaků,
- nepoužívat diakritiku,
- používat velká a malá písmena,
- použít alespoň 1 speciální znak,
- nepoužívat slovníková hesla, jména a osobní informace,
- používat číslice,
- střídat znaky a číslice.

Při práci s hesly je nutné se vyvarovat následujícímu:

- kamkoli si zapisovat hesla (to při větším množství hesel může být problém, proto se doporučuje používat správce hesel (*například LastPass*),
- nesdílet hesla s další osobou,
- nepoužívat hesla pro vícero přístupů,
- nepoužívat stejná hesla pro pracovní a osobní účty (např. pro e-mailové schránky),
- neukládat v prohlížečích přihlašovací hesla (pro tento účel je možné použít správce hesel.

Pro zvýšení bezpečnosti autentizace je vhodné použít některou z dále navrhovaných metod:

- použití dvou faktorového ověření všude tam, kde je to možné,
- použití hardwarového klíče pro druhotné ověření identity (společně s heslem) všude tam, kde je to možné.

i nadále je nutné, aby byla zachována pravidelná obměna hesel všech uživatelů. K této obměně by mělo dojít i v případě, kdy dojde k podezření z kompromitace služby. Vzhledem ke stanoveným doporučením je nutné zavést pravidlo, kdy pro každou službu musí existovat jedno unikátní heslo.

Bezpečné postupy přihlášení A.9.4.2

Pro přihlašování k systémům, aplikacím a serverům společnosti se vyžaduje takové zařízení, které má nastavenou dostatečnou bezpečnostní ochranu a také dostatečně silní heslo (podle kapitoly 5.1.3).

Pro systémové přihlašování platí tato pravidla:

- přihlašovací dialog musí zobrazovat minimum informací,
- zobrazovat informaci, že k systému má přístup pouze identifikovaný uživatel,
- nezobrazovat nápovědy pro vyplnění hesla,
- proces přihlašování vykonat až v případě, kdy je dokončeno vkládání všech autentizačních informací,
- nezobrazovat heslo, ani počet jeho znaků,
- v případě nezdařené autentizace nezobrazovat informaci, ve které části autentizačních informací je chyba,
- v případě autentizačního nezdaru vytvořil bezpečnostní událost a v případě, kdy bude překročen určený počet pokusů (obvykle 3 pokusy), tak účet zablokovat, vytvořit bezpečnostní incident a informovat odpovědnou osobu,

- nepřenášet hesla přes síť v nechráněném (čitelném) tvaru,
- zaznamenávat, formou logů, informace o přihlášení.

Po přihlášení do systému zobrazit informaci o posledním úspěšném přihlášení a také informaci o jakémkoliv pokusu o přihlášení od posledního úspěšného přihlášení.

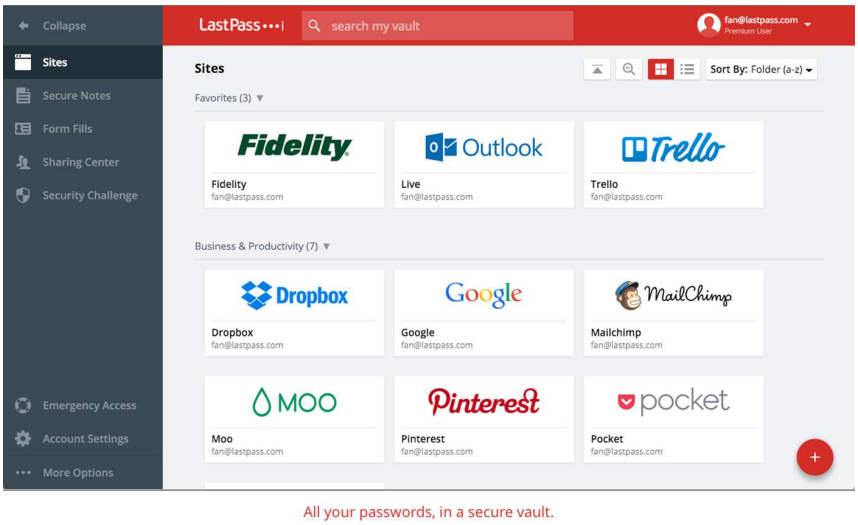
Systémy správy hesel A.9.4.3

Pro přihlášení k webovým službám a aplikacím, které implicitně nepodporují dvou faktorové ověření je doporučeno zavést vhodný systém pro správu hesel a nastavit pro konkrétní webovou službu dostatečně silné heslo. Takovým nástrojem je například program `LastPass` od společnosti LastPass.

LastPass

Aplikace LastPass pro jednotlivce nabízí správu hesel a jejich bezpečné uložení. Princip jejího fungování je následující:

- **Ochrana dat pomocí šifrování** – hesla spravovaná touto aplikací zašifruje pomocí dvojice algoritmů, konkrétně se jedná o algoritmus AES-256 a PBKDF2 SHA-256. Společně s výstupem z tohoto šifrovacího algoritmu je použit také takzvaný `salt`. `Salft` je náhodná hodnota vygenerovaná z uživatelského jména a silného hlavního hesla. Její funkcí je zanesení dodatečné náhodnosti do procesu šifrování hesel.
- **Ochrana dat pomocí více faktorů** – pro přístup ke službám chráněných heslem spravovaným aplikací LastPass je možné nastavit dvou faktorové ověření. Aplikace LastPass nabízí množství možností, pomocí kterých lze provést druhotné ověření. Mezi tyto možnosti patří ověření pomocí e-mailu, SMS zprávy, HW tokenu nebo pomocí schválení přihlášení v mobilní aplikaci LastPass.
- **Důvěryhodná zařízení** – aplikace LastPass umožňuje nastavit zařízení příznak důvěryhodnosti. To v podstatě znamená, že na tomto zařízení bude docházet k autentizaci pouze pomocí hlavního hesla a nebude požadována autentizace pomocí druhého faktoru. V případě ostatních zařízení (sdílený pracovní notebook, pracovní mobilní telefon) bude vyžadována autentizace pomocí dvou faktorů.
- **Široká podpora systémů** – aplikace LastPass podporuje všechny hlavní operační systémy, a to jak desktopové, tak mobilní.
- **Pokročilé možnosti podnikového nasazení** – aplikace LastPass nabízí pokročilé možnosti nastavení pro podnikové prostředí. Mezi tyto možnosti patří například nastavení minimálních požadavků pro heslo, možnost okamžitého resetování všech hesel, pokročilá správa uživatel a v neposlední řadě také možnost oddělení pracovních a osobních účtů.



Obr. 5.3: Uživatelské prostředí aplikace LastPass [17]

Řízení přístupu ke zdrojovému kódu A.9.4.5

Pro přihlášení k vývojovým serverům slouží jeden přihlašovací účet s maximálními oprávněními. Tento přístup je nutný pro testování. Aby ale bylo přihlašování uživatelů ověřeno a bylo zabráněno přihlášení neoprávněných uživatelů, doporučuje se, aby bylo přihlášení vázáno na bezpečnostní uživatelský SSL certifikát s dostatečně silným heslem.

Dále se doporučuje, aby bylo zakázáno vzdálené přihlášení pomocí uživatelského účtu `root` a celá práce probíhala nad protokolem SSH. Přihlášení k serveru pomocí tohoto protokolu je možné ze všech Linuxových operačních systémů pomocí vestavěných systémových knihoven. Pro systémy Windows 8.1 a nižší je nutné použít software třetích stran, jako ku příkladu aplikace PuTTY. V případě uživatel s operačním systémem Windows 10 je možné přímo do systému nainstalovat doplněk *Bash for Windows*, který přidává možnosti Linuxového subsystému do prostředí Windows včetně podpory přihlašování na SSH servery.

5.1.4 Fyzická bezpečnost a bezpečnost prostředí (A.11)

Cílem těchto opatření je zabránit v neoprávněném přístupu, poškození a narušování informací a zařízení pro zpracování informací v organizaci.

Fyzický bezpečnostní perimetr A.11.1.1

Společnost Netcope Technologies má své sídlo umístěno v rámci jednoho z brněnských technologických parků. Součástí služeb poskytovaných firmám je mimo jiné hlídání přístupů do firmy. Technologický park má jeden vstup s vrátnicí a ostrahou. Provozní doba vrátnice je v pracovní dny od 7:00 do 21:00. V nepracovní dny není služba na vrátnici konána a celý technologický park je zastřežen alarmem. Pro tento případ mají zaměstnanci firmy přiděleny své unikátní kódy pro odkódování svého sídla. Přístupy všech zaměstnanců se logují pro pozdější potřeby.

Pro přístup do sídla společnosti, tedy lépe řečeno do části technologického parku, kde se společnost nachází, je nutné prokázání oprávnění. Nosičem informací o zaměstnanci je čipová karta se zaměstnaneckou identifikací. Návštěvy mohou do sídla společnosti vstoupit pouze s pověřeným zaměstnancem.

V rámci společnosti Netcope Technologies je vybavena jedna místnost jakožto výrobní. V této místnosti jsou umístěny prostředky pro fyzickou inspekci FPGA karet. Dále jsou zde umístěny vývojové servery a další podpůrné prostředky pro chod firmy. Součástí výrobní místnosti je i sklad materiálu a FPGA karet. Pro přístup do této místnosti je nutné prokázání dostatečných oprávnění, které se prakticky děje pomocí čipového přístupového systému. Přístup do této místnosti mají vedoucí výroby. Ostatní zaměstnanci mohou do těchto prostor vstoupit pouze se svolením vedoucího výroby a mohou se v místnosti nacházet pouze v jeho přítomnosti.

Síťový bezpečnostní perimetr

Ochrana síťového bezpečnostního perimetru je stejně důležitá, jako ochrana fyzického bezpečnostního perimetru. Proto se doporučuje, aby bylo pro jeho vytvoření vynaloženo stejné úsilí, jako v případě fyzického bezpečnostního perimetru.

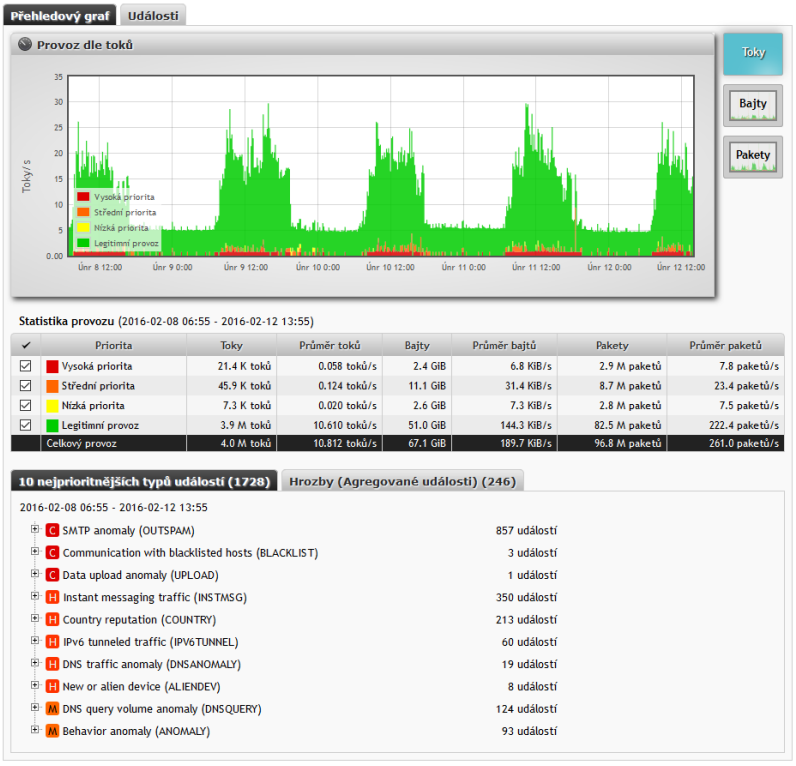
Pro potřeby společnosti Netcope Technologies, a. s. je dobré, aby byla prováděna neustálá detekce anomálií ve vnitřním síťovém provozu. Stejně tak je nutné analyzovat síťový provoz pocházející vně firemní sítě. Jako řešení poskytující tyto vlastnosti se doporučuje nasazení řešení **Flowmon Probe** s doplňkem **Flowmon ADS** od brněnské společnosti Flowmon Networks, a. s. Řešení Flowmon Probe nabízí tyto funkce [18]:

- **Ukládání a pokročilou analýzu flow dat díky vestavěnému kolektoru** – využití statistik o síťovém provozu z vrstev L2-L4 a L7.
- **Nejvýkonnější technologii na trhu** – sondy v reálném čase zaznamenávají každý paket i na 100 Gb/s linkách.
- **Viditelnost do vrstvy L7** – využití informací z HTTP hlaviček, protokolu DNS a VoIP hlaviček a dalších pro lepší správu sítě.
- **Plnou kompatibilitu chránící vložené investice** – sondy jsou plně kompatibilní s kolektory ostatních výrobců podporujících sběr NetFlow/IPFIX dat.
- **Jednoduché nasazení a intuitivní GUI** – sondu lze umístit do libovolného bodu v síti. Její nasazení a konfigurace je naprosto intuitivní a umožňuje mít plně automatické NetFlow monitorovací řešení během několika minut.

Společně s instalací řešení Flowmon Probe je doporučeno použít i rozšíření Flowmon ADS, které nabízí rozšířené analytické nástroje. Tyto nástroje využívají informace právě z řešení Flowmon Probe. Mezi klíčové vlastnosti Flowmon Probe patří:

- **Široká škála detekčních metod** – detekce anomálií v podnikové síti i na jejím perimetru detekující anomálie v DNS, DHCP a dalších typech provozu.

- **Aktivní ochrana před moderními hrozbami** – řada předdefinovaných detekčních metod odhaluje nežádoucí vzory chování. Flowmon ADS aktivně identifikuje pokročilé hrozby typu APT, botnety a infikovaná zařízení v síti, malware, pro který neexistuje signatura, konfigurační problémy, nežádoucí aktivity uživatelů, zneužívání datové sítě atd.
- **Komplementarita šetřící investice** – řešení Flowmon ADS je připraven pro nasazení v libovolné fyzické nebo virtuální síti. Nezáleží na tom, jaká zařízení, od jakých výrobců a jaké standardy datových toků jsou použity.
- **Real-time monitoring a propracovaný systém upozornění** – řešení Flowmon ADS umožňuje permanentní dohled nad vaším fyzickým i virtuálním prostředím. Propracovaný systém notifikace událostí a jejich exportu do systémů třetích stran (syslog, SNMP, CVS) umožňuje mít síť neustále pod kontrolou.



Obr. 5.4: Prostředí řešení Flowmon ADS [18]

Podpůrné služby (A.11.2.2)

Společnost v současné době nevyužívá žádným způsobem UPS, proto v případě výpadku elektrické energie hrozí ztráta rozpracovaných neuložených souborů na všech vývojových serverech. Společnost Netcope Technologies využívá řadu serverů značky Dell (zejména Dell R620, Dell R630 a Dell R520). Tyto servery jsou umístěny ve výrobní místnosti. Dále využívá serveru Dell R230, na kterém běží síťové služby (*Open vSwitch*[1]).

[1] Viz http://openvswitch.org/

Pro případ výpadku energie je vhodné, aby tyto servery byly dostatečně kryty z UPS. Dostatečné krytí v tomto případě znamená alespoň takovou dobu, aby mohla být uložena rozdělaná práce a tyto servery mohly být bezpečně vypnuty. Pro tyto potřeby je nutný záložní zdroj s minimálním výkonem 1000 W. Proto se doporučuje pro výrobní místnost záložní zdroj značky APC, konkrétně jde o výrobek APC Smart-UPS X 1500VA LCD [19]. Jedná se o záložní zdroj velikosti 2U o maximálním výkonu 1200 W, který umožňuje instalaci do RACK skříně. Dimenzování UPS tedy počítá s 20% nárůstem spotřeby ze strany vývojových a podpůrných serverů.

Obr. 5.5: APC Smart-UPS X 1500VA LCD [19]

Nastavení UPS je možné provést na místě pomocí proprietárního kabelu podobnému RS232 (*sériový port*) nebo pomocí kabelu USB. Další možností správy, kterou tato UPS nabízí je vzdálená správa přes webové rozhraní.

Pro komfortní práci vývojářů se doporučuje pořízení malých UPS do kanceláří, jejichž úkolem bude pokrytí odběru stolních počítačů a monitorů po dobu minimálně 5 minut. Pro tyto potřeby se doporučuje pořízení 7 kusů kancelářských záložních zdrojů značky APC, konkrétně jde o záložní zdroje APC Back-UPS ES 700 [20]. Tyto UPS nabízejí jmenovitý maximální výkon 405 W a nabízejí až 15 minut krytí při poloviční zátěži a 5 minut krytí při maximálním zatížení.

Obr. 5.6: APC Back-UPS ES 700 [20]

Údržba zařízení A.11.2.4

Pro zajištění správného fungování všech zařízení spojených s výrobou se zavádí pravidelné kontrolování jejich funkčnosti. Tato kontrola bude probíhat pravidelně 1x za 14 dní a budou

při ní ověřena všechna zařízení, ať už tak, která jsou používána denně, ale i ta, která jsou používána méně často.
V případě vývojových a podpůrných serverů se budou testovat následující vlastnosti:

- Korektní síťová konfigurace.
- Dostupnost serveru v interní síti.
- Chyby čtení a zápisu všech diskových jednotek.
- Kontrola bezchybného fungování BIOS.

V případě ostatních aktiv se budou testovat tyto vlastnosti:

- Správné fungování UPS.
- Správné fungování všech síťových prvků.
- Korektní nastavení a fungování vzdáleného přístupu.

V případě všech testování bude výstupem report o provedeném testování. Tento report bude obsahovat následující informace:

- Datum a čas testování.
- Datum a čas předcházejícího testování.
- Popis jednotlivých testů a jejich výsledky.
- Seznam zjištěných nedostatků.

Zásada prázdného stolu a prázdné obrazovky monitoru (A.11.2.9)

Zajištění bezpečnosti zařízení určeného ke zpracování citlivých informací doporučuje přijetí takzvané *zásady prázdného stolu a obrazovky monitoru*. Na základě této zásady je doporučeno přijetí následujících opatření:

- Citlivé informace, ať už v papírové formě nebo na elektronickém paměťovém médiu, by měly být v případě, kdy nejsou používány, uzamčeny (nejlépe v trezoru, skříni nebo jiném zabezpečeném vybavení). Tato zásada by měla být striktně dodržována v případě, kdy je kancelář opuštěna.
- Je nutné, aby byla u všech reprodukčních zařízení (*kopírky, skenery, digitální fotoaparáty apod.*) zabezpečeny proti neoprávněnému použití.
- Počítače a vývojové terminály by měly být zabezpečeny automatickým uzamykáním obrazovky nebo odhlášením uživatele v případě, kdy nejsou používány.
- Média obsahující citlivé nebo klasifikované informace by měla být ihned odebrána z tiskáren.

Tyto zásady by měly být platné i v případě vzdálené práce (ze služební cesty nebo homeoffice). Seznámení všech zaměstnanců s těmito zásadami by mělo být rovněž provedeno.

5.1.5 Bezpečnost provozu (A.12)

Většina bezpečnostních opatření, které dosud nemá společnost stanoveny, byly popsány již v předchozích kapitolách. Následuje proto poslední nepokrytá oblast bezpečnosti provozu, konkrétně část věnovaná zálohování.

Zálohování (A.12.3)

V současné době společnost zálohuje vlastními silami především veškeré zdrojové kódy a také vydané balíčky, které distribuuje zákazníkům (ty jsou uloženy na serveru odděleném od serveru se zdrojovými kódy). Ostatní provozní soubory jsou umístěny ve službě Google Apps, kde je zálohování zajištěno přímo dodavatelem (společnost Google) v rámci smlouvy SLA. Samotné zálohování probíhá takzvaně *onsite*, tedy v místě umístění datových serverů. Zálohuje se na redundantní diskové pole umístěné ve stejné síti, jako servery se zdrojovými kódy a server s balíčky.

Tento stav není ideální, protože hrozí ztráta dat vlivem chyby diskového pole nebo vlivem zanesení viru do sítě. Samotná data pak nemusí být korektně obnovena v případě, kdy dojde k chybě v síti. Proto se doporučuje, jako další stupeň zálohování provádět takzvané *offsite backup* zálohování. Principem tohoto zálohování je záloha na server umístěný vně organizaci v certifikovaném datovém centru.

Vhodným kandidátem na pokrytí této funkcionality je brněnská společnost Faster. Tato nabízí firmám i jednotlivcům diskový prostor pro zálohování pod názvem *datový sklad*. Jako vhodnou kapacitu pro zálohování je doporučené zvolit 2TB.

Pro zvýšení bezpečnosti nabízí Faster přenos dat pomocí SW agenta striktně odděleného od Internetu (pro zvýšení zabezpečení). Samotný přenos dat probíhá buďto pomocí VPN nebo pomocí vyhrazené linky. Samozřejmostí je šifrování přenášených a ukládaných dat a certifikace ISO 27000 pro celé datové centrum.

5.1.6 Bezpečnost komunikací a přenos dat (A.13)

Opatření v sítích (A.13.1.1)

Jelikož společnost Netcope Technologies, a. s. navrhuje a prodává síťové karty pro vysokorychlostní zpracování paketů, není pro společnost síťová problematika ničím neznámým. I z tohoto důvodu si společnost spravuje svou počítačovou síť sama.

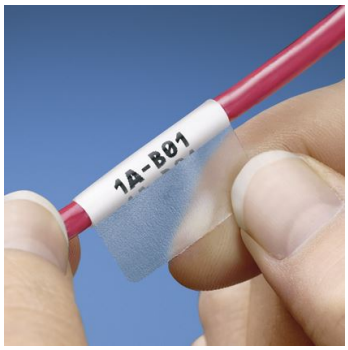
Většina síťových prvků je umístěna ve vývojovém skladu, z toho důvodu leží fyzická správa sítě na bedrech vedoucího výroby. Tento stav ale není ideální. Doporučuje se, aby byla ve společnosti zřízena pozice síťového správce, který by se této problematice mohl věnovat na plný úvazek, tedy v režimu 5x8. Adekvátní ochrana fyzické vrstvy je základem všech dalším bezpečnostních opatření a není možné na ni, při návrhu bezpečnostních opatření, zapomínat.

Dále se doporučuje, aby byla přijata opatření týkající se zabezpečení síťových kabelů a síťových portů. Mezi tato opatření patří blokátory na nevyužité porty, konektorové zámky na již zapojené kabely a pro vizuální zlepšení kontroly je vhodné zavést štítky s popisky.

Vhodným komplexním dodavatelem těchto prvků je společnost Panduit, jehož produkty jsou zobrazeny na následujících obrázcích:

Obr. 5.7: Panduit zámek portu RJ45 [21]

Obr. 5.8: Panduit zámek konektoru RJ45 [22]



Obr. 5.9: Panduit štítek pro popis kabelu [23]

Princip oddělení v sítích (A.13.1.3)

V současné době komunikují všichni uživatelé (ať už návštěvníci nebo zaměstnanci) a systémy na jedné síti. Tento stav není ideální pro zachování bezpečnosti informací.

Proto se společnosti doporučuje, aby bylo v rámci interním počítačové sítě zřízeno několik oddělených virtuálních sítí. Rozdělení do sítí by mělo být následující:

- Virtuální síť pro oddělení vývoje.
- Virtuální síť pro oddělení marketingu a obchodu[2].
- Virtuální síť pro vývojové servery.
- Virtuální síť pro podpůrné servery.
- Virtuální síť pro management.
- Virtuální síť s DHCP klientem pro mobilní zařízení.
- Virtuální síť pro návštěvníky.

Přiřazení práv pro přístup do konkrétní podsítě by mělo být stanoveno na základě autentizace proti RADIUS serveru. Tedy například v případě přihlášení hosta (návštěvy) by byl znemožněn přístup do všech podsítí, s výjimkou návštěvnické sítě. Naopak v případě přihlášení vývojáře by byl umožněn přístup do podsítě pro vývojové a podpůrné servery.

[2]Jedna síť je zvolena z tohot důvodu, že společnost v současné době nemá striktně vymezené oddělení marketingu. Na marketingu se tak do velké míry podílejí zaměstnanci obchodu.

5.2 Ekonomické zhodnocení

Ekonomické zhodnocení všech plánovaných opatření pro zajištění bezpečnosti informací ve společnosti Netcope Technologies, a. s. osahuje následující tabulka:

Položka	**Množství**	**Jednotková cena**	**Pořizovací cena**	**Obnovovací cena**
ESET Secure Office+	10 kusů	1 029 Kč	10 290 Kč	10 290 Kč
APC Smart-UPS X 1500VA LCD	1 kus	22 306 Kč	22 306 Kč	0 Kč
APC Back-UPS ES 700	7 kusů	2 471 Kč	17 297 Kč	0 Kč
LastPass Enterprise	25 licencí	48 USSD	960 USSD	960 USD
Panduit PSL-DCPLX	30 kusů	677 Kč (10 kusů)	2 031 Kč	0 Kč
Panduit PSL-DCJB-VL	100 kusů	4362 Kč (100 kusů)	4 362 Kč	0 Kč
Panduit S100X150VBC	200 kusů	1 591 Kč (200 kusů)	1 591 Kč	0 Kč
Faster datový sklad (2TB)	1 licence	1 500 Kč/měsíc	18 000 Kč	18 000 Kč
Flowmon Probe s ADS	1 licence	8 329 €	8 329 €	1 330 €

Tab. 5.4: Náklady na zavedení opatření[3]

Poznámka: Řešení ESET Secure Office+ obsahuje ESET Endpoint Security i ESET Mobile Security for Android.

Celková pořizovací cena všech opatření je 323 800 Kč, obnovovací cena potom činí 87 240 Kč. Pro ceny v USD byl uvažován přepočtový kurz 24 Kč/USD. Pro ceny v € byl uvažován přepočtový kurz 27 Kč/€.

Největší částka pro zavedení opatření je poplatek za řešení Flowmon Probe s doplňkem ADS, následované poplatky za SW licence a UPS. Částka za obnovení opatření potom obsahuje vesměs pouze poplatky za licence. Z pohledu celkového ročního obratu společnosti potom obnovovací poplatky představují jen asi 0,5 % celkového ročního obratu. Proto doporučuji, aby společnost zavedla všechna navrhovaná opatření.

[3] Všechny náklady jsou bez DPH

Závěr

Cílem této diplomové práce bylo navržení systematického řešení bezpečnosti informací na základě norem z rodiny ISO/IEC řady 27000. Společnost Netcope Technologies, a. s. v současné době neuvažuje o certifikaci ISO 27000, avšak v rámci této práce dostává návod, jak zavést bezpečnost informací dle norem ČSN ISO/IEC 27001:2014 a ČSN ISO/IEC 27002:2014.

Samotná práce je rozdělena do 5 kapitol. Ve druhé kapitole byl uveden teoretický základ celé práce. Byly v ní pospány pojmy jako informace a jejich bezpečnost, bezpečnost organizace, model PDCA. Dále byly v této části popsány vybrané normy z rodiny ISO/IEC 27000, které byly dále použity v praktické části práce a byl zde objasněn pojem bezpečnostní politiky organizace. Nejobsáhlejší část této kapitoly byla věnována analýze rizik spojených s elektronickými informacemi a způsobu realizace jejich zabezpečení.

Ve třetí kapitole byly uvedeny vybrané technologie pro podporu realizace bezpečnosti elektronických informací, jako je technologie RADIUS serveru nebo technologie virtuálních místních sítí.

Čtvrtá kapitola se zaměřuje na analýzu současného stavu ve společnosti. Je v ní popsána síťová infrastruktura, včetně serverů a služeb, které jsou v rámci síťové infrastruktury dostupné. Největší část této kapitoly však zaujímá analýza rizik spojených s elektronickými informacemi. Při analýze rizik byl použit rámec z normy ČSN ISO/IEC 27005:2013. Z výsledků analýzy vyplynul fakt, že neohroženějším aktivem společnosti jsou data zaměstnanců a interní informace, dále pak vývojový HW a služba sdílení dat. Možné zneužití nebo zničení těchto aktiv by mělo na společnost fatální, nejspíše likvidační, následky. Z hlediska bezpečnostních rizik ukázala analýza jako největší rizika špionáže, krádeže dokumentů, poškození dat nebo neoprávněné použití zařízení. Jako významné se ukázalo též riziko selhání zařízení a ztráty elektrické energie.

Pátá kapitola práce se věnovala návrhu bezpečnostních opatření pro systémové řešení bezpečnosti informací. Zde byl vedení společnosti doporučen kontakt se zájmovými skupinami z oblasti bezpečnosti informací, zejména stránky národního centra kybernetické bezpečnost a stránky národního CSRIT týmu České republiky. Dále byla společnosti navržena řada opatření týkajících se zabezpečení mobilních zařízení, stolních počítačů a notebooků. Tato opatření se mimo jiné týkala používání antivirů na všech uživatelských strojích, používání silných hesel a jejich správců. Z oblasti hesel byla přidána i část věnující se stanovení minimálních bezpečnostních požadavků pro uživatelská hesla.

Hledisko ochrany dat před odcizením nebo vynesením byla společnosti doporučena revize interních pravidel a v rámci této práce byla též navržena směrnice pro disciplinární řízení se zaměstnanci, kteří se dopustili nějaké bezpečnostního incidentu.

Z hlediska ochrany dat před poškozením bylo společnosti doporučeno zavést důslednější systém zálohování postavený zejména na tzv. offsite zálohování, kdy jsou data zálohována do datových center třetích stran. V tomto konkrétním případě bylo doporučeno využít nabídky brněnské společnosti Faster, jež nabízí zálohování přes vyhrazenou linku, která je, z důvodu vyšší bezpečnosti, zcela odstíněna od Internetu.

Dále byla společnosti navržena opatření týkající se bezpečnosti perimetru, kde byl kladen důraz zejména na zabezpečení síťového perimetru. Jako opatření bylo společnosti doporučeno zakoupení řešení Flowmon Probe s modulem ADS.

Z hlediska bezpečnosti hardware byla v práci navržena zejména opatření týkající se redundance napájení. Proto bylo společnosti doporučeno zakoupení jednoho kusu 1500 VA UPS, která má zajisti pokrytí spotřeby serverů nutné pro jejich vypnutí v případě výpadku elektrické energie. Dále bylo doporučeno zakoupení 7 kusů menších kancelářských UPS pro pokrytí spotřeby stolních počítačů v případě jejich vypínání v důsledku výpadku elektrické energie. Společně s těmito opatřeními byla společnosti doporučena instalace blokátorů na nevyužité porty, zámků na již používané kabely a štítků pro jejich lepší identifikaci a zvýšení přehlednosti.

Z hlediska bezpečnosti počítačových sítí bylo doporučeno oddělení sítí pro různá oddělení figurující v rámci interních struktur společnosti, jako je oddělení obchodu a marketingu, oddělení vývoje apod. Od všech interních sítí by potom měla být striktně oddělena síť pro návštěvníky.

Všechna bezpečnostní opatření byla navržena tak, aby eliminovala možná rizika, která byla zjištěna při analýze současného stavu ve společnosti. Při analýze rizik byl využit rámec hrozeb stanovený normou ČSN ISO/IEC 27005:2014. Pro samotné zpracování opatření byly využity normy ČSN ISO/IEC 27001:2014 a ČSN ISO/IEC 27002:2014. Celková částka pro zavedení opatření byla stanovena na 323 800 Kč, každoroční částka nutná pro obnovení opatření (zejména SW licencí) potom činí částku 87 240 Kč, což je necelé půl procento ročního obratu společnosti.

V příloze práce je zpracováno prohlášení o aplikovatelnosti, uvádějící celistvý pohled na informační bezpečnost v organizace, které je pracováno dle přílohy A normy ČSN ISO/IEC 27001:2014.

Stanovený cíl práce – systematické řešení bezpečnosti práce v organizaci – na základě norem z rodiny ČSN ISO/IEC 27000, byl naplněn. Vedení společnosti bylo informováno o závěrech analýzy rizik a vedením společnosti bylo přislíbeno zavedení všech opatření navržených v této diplomové práci.

Seznam literatury

[1] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 9788073802769.

[2] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Brno: Computer Press, 2007. ISBN 9788025115114.

[3] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky*. Praha: Grada, 2006. Management v informační společnosti. ISBN 8024712784.

[4] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

[5] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 8025101061.

[6] RAIS, Karel a Radek DOSKOČIL. *Risk management: studijní text pro kombinovanou formu studia*. Brno: Akademické nakladatelství CERM, 2007. ISBN 9788021435100.

[7] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 9788074310508.

[8] RIGNE, Charles, Willens LIVINGSTON a Rubens MERIT. *Remote Authentication Dial In User Service (RADIUS)*. RFC 2865, RFC Editor, červen 2000. Dostupné také z: https://www.rfc-editor.org/rfc/rfc2865.txt

[9] CHACON, Scott. *Pro Git*. Praha: CZ.NIC, 2009. CZ.NIC. ISBN 978-80-904248-1-4.

[10] VLAN – Virtual Local Area Network. *Samuraj.cz* [online]. Praha: Petr Bouška, 2007 [cit. 2017-05-08]. Dostupné z: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

[11] DONAHUE, Gary A. *Network warrior*. Sebastopol, CA: O'Reilly Media, 2007. ISBN 9780596101510.

[12] *IEEE Std 802.1Q: Bridges and Bridged Networks*. 2014. New York: IEEE, 2014.

[13] *ČSN ISO/IEC 27002: Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. 3. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[14] ESET Endpoint Security pro Android.In: *ESET* [online]. Bratislava: ESET, spol. s r.o., 2017 [cit. 2017-04-01]. Dostupné z: http://www.eset.com/cz/firmy/produkty/android-security/

[15] ESET Endpoint Security. In: *ESET* [online]. Bratislava: ESET, spol. s r.o., 2017 [cit. 2017-04-01]. Dostupné z: https://www.eset.com/cz/firmy/ochrana-dat/windows-security/

[16] DISCIPLINÁRNÍ ŘÁD PRO STUDENTY. In: *Vysoké učení technické v Brně* [online]. Brno: VUT Brno, 2017 [cit. 2017-05-08]. Dostupné z: https://www.vutbr.cz/uredni-deska/vnitrni-predpisy-a-dokumenty/vnitrni-predpisy-vut-disciplinarni-rad-pro-studenty-vut-d136007/disciplinarni-vut-5-msmt-final-pdf-p128945

[17] LastPass: Free Password Manager. In: *Microsoft Store Česká republika* [online]. Praha: Microsoft, 2017 [cit. 2017-05-08]. Dostupné z: https://www.microsoft.com/cs-cz/store/p/lastpass-free-password-manager/9nblggh4v7x0#

[18] FLOWMON NETWORKS. *The most powerful NetFlow/IPFIX exporters in the world* [online]. [cit. 2017-04-29]. Dostupné z: https://www.flowmon.com/cs/products/flowmon/probe

[19] APC. *APC Smart-UPS X 1500VA Rack/Tower LCD 230V* [online]. [cit. 2017-04-01]. Dostupné z: http://www.apc.com/shop/uk/en/products/APC-Smart-UPS-X-1500VA-Rack-Tower-LCD-230V/P-SMX1500RMI2U

[20] APC. *APC úsporný zdroj Back-UPS ES, 8 zásuvek 700VA 230V CEE 7/5* [online]. [cit. 2017-04-01]. Dostupné z: http://www.apc.com/shop/cz/cs/products/APC-Power-Saving-Back-UPS-ES-8-Outlet-700VA-230V-CEE-7-5/P-BE700G-CP

[21] PANDUIT: *RJ45 Plug lock-in device* [online]. [cit. 2017-04-17]. Dostupné z http://www.panduit.com/en/products-and-services/products/copper-systems/patch-cords-and-cable-assemblies/accessories/lockin-devices/standard/PSL-DCPLX

[22] PANDUIT: *Jack module block-out device* [online]. [cit. 2017-04-17]. Dostupné z http://www.panduit.com/en/products-and-services/products/safety-and-security/physical-network-security/blockout-devices/PSL-DCJB-VL

[23] PANDUIT: *Self-laminating label cassette* [online]. [cit. 2017-04-17]. Dostupné z http://www.panduit.com/en/product/S100X150VAC

[24] *ČSN ISO/IEC 27000: Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*. 3. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

[25] *ČSN ISO/IEC 27001: Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictvíÍ, 2014.

[26] *ČSN ISO/IEC 27002: Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

Seznam zkratek

AAA	Autentizace, autorizace, audit (*accounting*)
AP	Přístupový bod
ČSN	Označení české technické normy
FCS	Kontrolní součet Ethernetového rámce
FPGA	Programovatelné hradlové pole (polovodičová součástka)
GUI	Grafické uživatelské rozhraní
HW	Hardware
ICT	Informační a komunikační technologie
IEEE	Institut pro elektrotechnické a elektronické inženýrství
IS	Informační systém
ISO	Mezinárodní normalizační organizace
ISMS	Systém řízení bezpečnosti informací
IT	Informační technologie
LAN	Lokální síť
SSH	Secure Shell (bezpečný shell)
SSL	Secure Sockets Layer („bezpečná soketová vrstva“)
SVN	Subversions (systém pro správu verzí)
SW	Software
VPN	Virtuální privátní síť

Seznam obrázků

Seznam tabulek

Seznam příloh

Příloha číslo 1: Prohlášení o aplikovatelnosti

A.5 Politiky bezpečnosti informací

A.5.1 Pokyny managementu organizace k bezpečnosti informací

Cíl: Poskytnout pokyny a podporu ze strany managementu pro bezpečnost informací v souladu s požadavky podnikatelské činnosti organizace a příslušnými zákony a předpisy.

A.5.1.1 Politiky pro bezpečnost informací

Cíl: Sada politik pro bezpečnost informací, která bude schválena managementem, bude zveřejněna a dána na vědomí zaměstnancům a relevantním externím stranám.
Vyloučeno: Ano
Způsob plnění: Politika ISMS

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Cíl: Politiky pro bezpečnost informací by měly být přezkoumány v plánovaných intervalech, nebo pokud dojde k významným změnám. aby byla zajištěna jejich neustálá vhodnost, přiměřenost a efektivnost.
Vyloučeno: Ano
Způsob plnění: Příručka ISMS

A.6 Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: Ustanovit řídící rámec pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace.

A.6.1.1 Role a odpovědnost bezpečnosti informací

Cíl: Všechny odpovědnosti za bezpečnost informací by měly být definovány a přiděleny.
Vyloučeno: Ne
Způsob plnění: Příručka ISMS

A.6.1.2 Princip oddělení povinnosti

Cíl: Konfliktní povinnosti a oblasti působnosti by měly být odděleny, aby se omezily příležitosti pro neoprávněné nebo neúmyslné změny nebo zneužití aktiv organizace.
Vyloučeno: Ano
Způsob plnění: Pro každého zaměstnance je vytvořen dokument, který popisuje uživatelovi povinnosti a odpovědnost. Do schvalovacího procesu je zapojeno i vedení. Dokument je posléze zpřístupněn v Google Drive, kde je možné jej modifikovat. Modifikace může provádět pouze nadřízený pracovník se schválením vedení společnosti. Podle tohoto dokumentu jsou posléze stanovena přístupová oprávnění pro přístup ke složkám souborům v Google Drive.

A.6.1.3 Kontakt s autoritami

Cíl: Měly by být udržovány přiměřené kontakty s příslušnými autoritami.
Vyloučeno: Ano
Způsob plnění: Jelikož je společnost Netcope Technologies malou společností, probíhá kontakt napříč firmou každodenně a není nutné jej nijak řídit.

A.6.1.4 Kontakt se zvláštními zájmovými skupinami

Cíl: Měly by být udržovány přiměřené kontakty se zvláštními zájmovými skupinami nebo dalšími fóry specialistů na bezpečnost a profesními sdruženími.
Vyloučeno: Ne
Způsob plnění: Pravidelné sledování stránek národního centra kybernetické bezpečnosti a CIRT týmu; účastnění se akcí těchto organizací.

A.6.1.5 Bezpečnost informací v řízení projektu

Cíl: Bezpečnost informací by měla být řešena v rámci řízení projektů, bez ohledu na typ projektu.
Vyloučeno: Ano
Způsob plnění: Každý projekt, který společnost realizuje se řídí platnými normami České republiky.

A.6.2 Mobilní zařízení a práce na dálku

Cíl: Zajistit bezpečnost práce na dálku a bezpečnost použití mobilních zařízení.

A.6.2.1 Politika mobilních zařízení

Cíl: K řízení rizik zavedených používáním mobilních zařízení by měla být přijata politika a podpůrná bezpečnostní opatření.
Vyloučeno: Ne (revidovat)
Způsob plnění: Manuál uživatele

A.6.2.2 Práce na dálku

Cíl: Na ochranu informací, k nimž je přistupováno v rámci práce na dálku, zpracovávaných nebo ukládaných v místech práce na dálku by měla být zavedena politika a podpůrná bezpečnostní opatření.
Vyloučeno: Ne (revidovat)
Způsob plnění: Manuál uživatele

A.7 Bezpečnost lidských zdrojů

A.7.1 Před vznikem pracovního poměru

Cíl: Zajistit, aby zaměstnanci a smluvní strany chápali své povinnosti, a zajisti, aby byli vhodní pro úkoly, pro které jsou uvažováni.

A.7.1.1 Prověřování

Cíl: Prověřování minulosti všech uchazečů o zaměstnání by mělo být prováděno v souladu s příslušnými zákony, nadřízeními a v souladu s etikou a mělo by být úměrné požadavkům souvisejícím s činností organizace, klasifikací informací, ke kterým má být umožněn přístup, a vnímaným rizikům.
Vyloučeno: Ano
Způsob plnění: Výběrové řízení na libovolnou pozici je prováděno v několika kolech, během kterých zaměstnanec jedná přímo s vedením společnosti. Během těchto kol navíc zaměstnanec prokazuje své odporné znalosti a zkušenosti.

A.7.1.2 Podmínky pracovního poměru

Cíl: Smlouvy se zaměstnanci a smluvními stranami by měly uvádět odpovědnost zaměstnanců/smluvních stran a organizace za bezpečnost informací.
Vyloučeno: Ano
Způsob plnění: Pracovní smlouva.

A.7.2 Během pracovního poměru

Cíl: Zajistit, aby si zaměstnanci a smluvní strany byli vědomi svých povinností, a zajistit, aby je plnili.

A.7.2.1 Odpovědnost managementu organizace

Cíl: Management by měl od všech zaměstnanců a smluvních stran požadovat, aby aplikovali bezpečnost informací v souladu se zavedenými politikami a postupy organizace.
Vyloučeno: Ne
Způsob plnění: Příručka ISMS.

A.7.2.2 Povědomí, vzdělávání a školení o bezpečnosti informací

Cíl: Všichni zaměstnanci organizace a tak, kde je to vhodné, i smluvní strany by měli získat odpovídající povědomí o bezpečnosti informací formou vzdělávání a školení a pravidelných aktualizací politik a postupů organizace, dle významu pro zastávanou pracovní funkci.
Vyloučeno: Ano
Způsob plnění: Bezpečnostní školení probíhají dle interních nařízení.

A.7.2.3 Disciplinární řízení

Cíl: Měl by existovat formální disciplinární proces oznámený všem, pro podniknutí kroků vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací.
Vyloučeno: Ne
Způsob plnění: Příručka ISMS.

A.7.3 Ukončení a změna pracovního poměru

Cíl: Chránit zájmy organizace jako součást procesu změny nebo ukončení pracovního poměru.

A.7.3.1 Odpovědnosti při ukončení nebo změně pracovního poměru

Cíl: Odpovědnosti a povinnosti v oblasti bezpečnosti informací, které zůstávají v platnosti i po ukončení nebo změně zaměstnání, by měly být definovány, sděleny zaměstnanci nebo smluvní straně a prosazovány.
Vyloučeno: Ne (revidovat)
Způsob plnění: Definované kroky, které dělat při ukončení pracovního poměru jsou součástí této práce a po schválení vedením budou umístěny do Google Drive.

A.8 Řízení aktiv

A.8.1 Před vznikem pracovního poměru

Cíl: Identifikovat aktiva organizace a definovat odpovědnosti za přiměřenou ochranu.

A.8.1.1 Seznam aktiv

Cíl: Aktiva související s informacemi a vybavením pro zpracování informací by měla být identifikována a měl by být sestaven a udržován seznam těchto aktiv.

Vyloučeno: Ano
Způsob plnění: Seznam aktiv je součástí analytické části této práce a je již ve společnosti definováno.

A.8.1.2 Vlastnictví aktiv

Cíl: Aktiva udržovaná v seznamu by měla mít vlastníka.
Vyloučeno: Ano
Způsob plnění: Vlastnictví aktiv je již ve společnosti definováno.

A.8.1.3 Přípustné použití aktiv

Cíl: Měla by být identifikována, dokumentována a implementována pravidla pro přípustné používání informací a aktiv spojených s informacemi a vybavením pro zpracování informací.
Vyloučeno: Ano
Způsob plnění: Již zpracováno v interních normách (např. normě pro výpůjčku demo strojů).

A.8.1.4 Vrácení aktiv

Cíl: Všichni zaměstnanci a uživatelé z externích stran by měli po ukončení svého zaměstnání, smlouvy nebo dohody vrátit všechna aktiva organizace, která měli v držení.
Vyloučeno: Ano
Způsob plnění: Společnost má již zpracovány pokyny, co dělat v případě ukončení pracovního poměru.

A.8.2 Klasifikace informací

Cíl: Zajistit, aby informace získala odpovídající úroveň ochrany v souladu s jejím významem pro organizaci.

A.8.2.1 Klasifikace informací

Cíl: Informace by měly být klasifikovány z hlediska právních požadavků, hodnoty, kritičnosti a citlivosti ve vztahu k neoprávněnému prozrazení nebo modifikaci.
Vyloučeno: Ano
Způsob plnění: Způsob klasifikace informací a nakládání s nimi je již ve společnosti definováno.

A.8.2.2 Označování informací

Cíl: Pro označování informací by měly být vypracovány a implementovány vhodné soubory postupů, v souladu se schématem informací přijatým organizací.
Vyloučeno: Ano

Způsob plnění: Na základě způsobu klasifikace informací a nakládání s nimi je již ve společnosti stanoven postup pro označování informací.

A.8.2.3 Manipulace s aktivy

Cíl: Pro zacházení s aktivy by měly být zavedeny postupy, v souladu se schématem klasifikace informací přijatým organizací.
Vyloučeno: Ano
Způsob plnění: Na základě způsobu klasifikace informací a nakládání s nimi je již ve společnosti stanoven postup pro manipulaci s aktivy.

A.8.3 Manipulace s médii

Cíl: Zabránit neoprávněnému prozrazení, modifikaci, odstranění nebo zničení informací uložených na médiu.

A.8.3.1 Správa výměnných médií

Cíl: Pro správu výměnných médií by měly být zavedeny postupy, v souladu se schématem klasifikace přijatým organizací.
Vyloučeno: Ano
Způsob plnění: Způsob klasifikace informací a nakládání s nimi je již ve společnosti definováno.

A.8.3.2 Likvidace médií

Cíl: Pokud již média nejsou zapotřebí, měla by být bezpečně zlikvidována dle formálních postupů.
Vyloučeno: Ano
Způsob plnění: Likvidace médií se provádí buďto fyzickým zničení média (v případě optického média). V případě paměťového média je provedeno několikanásobné naformátování s přepisem náhodou matricí (data tak nelze zrekonstruovat).

A.8.3.3 Přeprava fyzických médií

Cíl: Média obsahující informace by měla být během přepravy chráněna před neoprávněným přístupem, zneužitím nebo poškozením.
Vyloučeno: Ano
Způsob plnění: Způsob manipulace s médii v případě jejich přepravy je již ve společnosti definován.

A.9 Řízení přístupu

A.9.1 Požadavky organizace na řízení přístupu

Cíl: Omezit přístup k informacím a k vybavení pro zpracování informací.

A.9.1.1 Politika řízení přístupu

Cíl: Na základě požadavků vyplývajících z podnikatelské činnosti a požadavků na bezpečnost informací by měla být stanovena, dokumentována a přezkoumávána politika řízení přístupu.
Vyloučeno: Ano
Způsob plnění: Na základě dokumentu definujícímu role uživatelů ve společnosti bude provedeno nastavení oprávnění k souborům v Google Drive. Soubor s oprávněním bude udržován v aktuálním stavu.

A.9.1.2 Přístup k sítím a síťovým službám

Cíl: Uživatelům by měl být poskytován přístup pouze k těm sítím a síťovým službám, pro jejichž použití byli výhradně autorizováni.
Vyloučeno: Ano
Způsob plnění: Na základě ověření proti RADIUS serveru jsou uživateli zpřístupněny takové síťové služby, k nimž je autorizován.

A.9.2 Správa a řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a zabránit neoprávněnému přístupu k systémům a službám.

A.9.2.1 Registrace a zrušení registrace uživatele

Cíl: Pro přidělování přístupových práv by měl být zaveden proces formální registrace a deregistrace uživatele.
Vyloučeno: Ano
Způsob plnění: Řízení přístupu je definováno v příslušném dokumentu v Google Drive.

A.9.2.2 Zřízení přístupu uživatele

Cíl: Měl by být zaveden formální proces poskytování přístupu uživatel pro přiřazení nebo zrušení přístupových práv pro všechny typy uživatel a ke všem systémům a službám.
Vyloučeno: Ano
Způsob plnění: Zřizování přístupu je definováno v příslušném dokumentu v Google Drive.

A.9.2.3 Řízení privilegovaných přístupových práv

Cíl: Přidělování a použití privilegovaných přístupových práv by mělo být omezeno a řízeno.
Vyloučeno: Ano
Způsob plnění: Řízení přístupu je definováno v příslušném dokumentu v Google Drive.

A.9.2.4 Řízení tajných přístupových práv uživatelů

Cíl: Přidělení tajných autentizačních informací by mělo být řízeno prostřednictvím formálního procesu řízení.
Vyloučeno: Ano
Způsob plnění: Zásady pro bezpečné heslo jsou součástí této práce a budou sepsány v příslušném dokumentu v Google Drive. Součástí tohoto dokumentu budou i doporučené SW prostředky pro nakládání s hesly (ukládání hesel, generování hesel atd.)

A.9.2.5 Přezkoumání přístupových práv uživatelů

Cíl: Vlastníci aktiv by měli v pravidelných intervalech přezkoumávat přístupová práva uživatelů.
Vyloučeno: Ano
Způsob plnění: Vlastníci aktiv přezkoumávají v pravidelných intervalech přístupová práva uživatelů.)

A.9.2.6 Odebrání nebo úprava přístupových práv

Cíl: Přístupová práva všech zaměstnanců a uživatelů z externích stran k informacím a vybavení pro zpracování informací by měla být po ukončení jejich zaměstnání, smlouvy nebo vypršení dohody odstraněna nebo po změně upravena.
Vyloučeno: Ano
Způsob plnění: Společnost má již zpracovány pokyny, co dělat v případě ukončení pracovního poměru.)

A.9.3 Odpovědnosti uživatelů

Cíl: Učinit uživatele odpovědné za ochranu svých autentizačních informací.

A.9.3.1 Použití tajných autentizačních informací

Cíl: Pro uživatele by mělo být vyžadováno, aby při používání tajných autentizačních informací dodržovali postupy organizace.
Vyloučeno: Ne (revidovat)
Způsob plnění: Odpovědnost uživatelů a pokyny, jak se chovat jsou součástí pracovní smlouvy. Pokyny samotné jsou potom součástí příslušného dokumentu v Google Drive.

A.9.4 Řízení přístupu k systémům a aplikacím

Cíl: Zabránit neoprávněnému přístupu k systémům a aplikacím.

A.9.4.1 Omezení přístupu k informacím

Cíl: Přístup k informacím a funkcím aplikačních systémů by měl být omezen v souladu s politikou řízení přístupu.
Vyloučeno: Ne (revidovat)
Způsob plnění: Na základě autentizace pomocí RADIUS serveru jsou uživateli zpřístupněny jen ty systémy a aplikace, které jsou nezbytně nutné pro jeho pracovní činnost.

A.9.4.2 Bezpečné postupy přihlášení

Cíl: Pokud to vyžaduje politika řízení přístupu, přístup k systémům a aplikacím by měl být řízen bezpečným postupem přihlášení.
Vyloučeno: Ne (revidovat)
Způsob plnění: Bezpečné postupy přihlášení jsou součástí příslušného dokumentu v Google Drive.

A.9.4.3 Systém správy hesel

Cíl: Systémy správy hesel by měly být interaktivní a měly by zajistit kvalitní hesla.
Vyloučeno: Ne (revidovat)
Způsob plnění: Doporučené systémy správy hesel jsou součástí konkrétního dokumentu v Google Drive.

A.9.4.4 Použití privilegovaných obslužných programů

Cíl: Použití obslužných programů, které by mohly být schopné potlačit systémová a aplikační opatření by mělo být omezeno a přísně kontrolováno.
Vyloučeno: Ne (revidovat)
Způsob plnění: Vedení společnosti by mělo přísně kontrolovat, zda nejsou používány aplikace, které jsou schopné překonávat systémové nebo aplikační kontroly.

A.9.4.5 Řízení přístupu ke zdrojovým kódům programu

Cíl: Přístup ke zdrojovému kódu programu by měl být omezen.
Vyloučeno: Ne
Způsob plnění: Na základě ověření proti RADIUS serveru jsou uživateli zpřístupněny jen ty zdrojové kódy, k nimž má oprávnění přistupovat.

A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: Zajistit správné a efektivní využití kryptografie na ochranu důvěrnosti, autenticity a/nebo integrity informací.

A.10.1.1 Politika použití kryptografických opatření

Cíl: Měla by být vypracována a realizována politika použití kryptografických opatřené na ochranu informací.
Vyloučeno: Ne (revidovat)
Způsob plnění: Politika používání kryptografických klíčů je součástí konkrétního dokumentu v Google Drive.

A.10.1.2 Správa klíčů

Cíl: Měla by být definována a realizována politika v oblasti použití, ochrany a životního cyklu kryptografických klíčů během celého jejich životního cyklu.
Vyloučeno: Ne (revidovat)
Způsob plnění: Politika používání kryptografických klíčů je součástí konkrétního dokumentu v Google Drive.

A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.1 Fyzický bezpečností perimetr

Cíl: Zabránit neoprávněnému fyzickému přístupu, poškození a narušování informací a vybavení pro zpracování informací organizaci.

A.11.1.1 Fyzický bezpečností perimetr

Cíl: Měly by být definovány bezpečnostní perimetry a ty by měly být použity k ochraně oblastí, které obsahují buď citlivé, nebo kritické informace a vybavení pro zpracování informací.
Vyloučeno: Ano
Způsob plnění: Zásady pro fyzickou bezpečnost jsou součástí konkrétních firemních dokumentů a školení. Vývojové a podpůrné servery jsou umístěny v uzamčené serverovně, přístup do této serverovny je zaznamenáván a je umožněn pouze pověřeným osobám. Data společnosti jsou uloženy na serverech společnosti Google (v rámci služby Google Drive). Na základě SLA jsou tato data chráněna nejvyšším stupněm ochrany a zaměstnanci Google nemají k těmto datům přístup. Pro přístup do sídla společnosti je nutné se prokázat oprávněním na recepci a pro přístup do sídla samotného je nutné se prokázat přístupovým čipem. Celý objekt je navíc střežen kamerovým systémem se záznamem.

A.11.1.2 Fyzické kontroly vstupu

Cíl: Zabezpečené oblasti by měly být na vstupu chráněny vhodnými opatřeními, aby se zajistilo, že přístup mají povolen pouze oprávněné osoby.
Vyloučeno: Ne
Způsob plnění: Pro přístup do budovy je nutné se prokázat na recepci nebo se autentizovat přístupovým čipem. Pro přístup k vývojovým a podpůrným serverům je nutné se prokázat dostatečnými přístupovými oprávněními.

A.11.1.3 Zabezpečení kanceláří, místností a vybavení

Cíl: Měla by být navržena a uplatněna opatření pro fyzickou bezpečnost kanceláří, místností a vybavení.
Vyloučeno: Ano
Způsob plnění: Již vyřešeno v bezpečnostních nařízeních společnosti.

A.11.1.4 Ochrana před vnějšími a přírodními hrozbami

Cíl: Měla by být navržena a uplatněna fyzická ochrana před přírodními katastrofami, zlomyslnými útoky nebo nehodami.
Vyloučeno: Ano
Způsob plnění: Řešení tohoto požadavku je přeneseno na pronajímatele prostor, kde firma sídlí.

A.11.1.5 Práce v zabezpečených oblastech

Cíl: Měly by být navrženy a uplatněny prostupy pro práci v zabezpečených oblastech.
Vyloučeno: Ano
Způsob plnění: Sídlo společnosti se nachází v bezpečné oblasti. Pro přístup do sídla společnosti jsou vyžadovány přístupové kary pro autentizaci. Přístup do sídla společnosti je dále podmíněn fyzickou kontrolou na recepci. Pro přístup k zařízením je vyžadována autentizace proti RADIUS serveru nebo pomocí osobního certifikátu. Další zásady bezpečnosti jsou součástí interních firemních nařízení a pravidelného školení.

A.11.1.6 Oblasti pro nakládku a vykládku

Cíl: Místa přístupu, jako jsou prostory pro vykládku a nakládku, a další místa, kde by mohly neoprávněné osoby vstupovat do objektů, by měly být kontrolovány, a pokud je to možné, izolovány od vybavení pro zpracování informací, aby se zabránilo neoprávněnému přístupu.
Vyloučeno: Ne
Způsob plnění: Neoprávněné osoby se dostanou pouze na recepci (kam musí být vpuštěni recepční). Do prostor společnosti se dostanou po prokázání oprávnění. Navíc je celý prostor střežen kamerovým systémem se záznamem. Samotné prostory společnosti jsou především open-space kanceláře, kde není problém sledovat pohyb cizích osob.

A.11.2 zařízení

Cíl: Zabránit ztrátě, poškození, odcizení nebo kompromitaci aktiv a přerušení provozu organizace.

A.11.2.1 Umístění zařízení a jeho obrana

Cíl: Zařízení by mělo být umístěno a chráněno tak, aby byla snížena rizika vyplývající z hrozeb a nebezpečí ze strany životního prostředí a z možnosti neoprávněného přístupu.
Vyloučeno: Ano
Způsob plnění: Zařízení jsou umístěna v bezpečných místech uvnitř sídla společnosti.

A.11.2.2 Podpůrné služby

Cíl: Zařízení by mělo být chráněno před výpadkem napájení a dalšími poruchami způsobenými selháním podpůrných služeb.
Vyloučeno: Ne (revidovat)
Způsob plnění: Všechna kriticky důležitá zařízení jsou napojena na UPS, jejíž funkčnost je pravidelně ověřována.

A.11.2.3 Bezpečnost kabelových rozvodů

Cíl: Silová a telekomunikační kabeláž určená pro přenos dat nebo podpůrných informačních služeb by měla být ochráněna před odposlouchávánim, rušením nebo poškozením.
Vyloučeno: Ne
Způsob plnění: Přístup k rozvaděčům a kabelovým trasám je možný jen pro oprávněné osoby. Výpadky jsou důsledně monitorovány.

A.11.2.4 Údržba zařízení

Cíl: Zařízení by mělo výt správně udržováno pro zajištění jeho stálé dostupnosti a integrity.
Vyloučeno: Ne (revidovat)
Způsob plnění: V rámci interních nařízení jsou definovány povinnosti související s údržbou konkrétních zařízení.

A.11.2.5 Přemístění aktiv

Cíl: Zařízení, informace nebo software by neměly být přemístěny mimo organizaci bez předchozího povolení.
Vyloučeno: Ano
Způsob plnění: Servery nejsou přemísťovány mimo organizaci. Pro přemisťování mobilních zařízení (pracovní mobilní telefony, notebooky, ...) jsou stanovena pravidla v rámci vnitřních předpisů společnosti.

A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace

Cíl: Bezpečnost by se měla týkat aktiv mimo prostory organizace, s přihlédnutím k různým rizikům činnosti mimo prostory organizace.
Vyloučeno: Ano
Způsob plnění: Ochrana aktiv mimo prostory organizace je chráněna pomocí SLA. Ochrana zařízení mimo organizaci je řešena v rámci interních předpisů pro služební cesty.

A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení

Cíl: Všechny části zařízení obsahujícího paměťová média by měly být prověřeny s cílem zajistit, aby byla před likvidací nebo opakovaném použití odstraněna nebo bezpečně přepsána všechna citlivá data a licencovaný software.
Vyloučeno: Ano
Způsob plnění: Znehodnocení probíhá buďto fyzickým zničením (optická média) nebo několikanásobným přepsáním náhodnou matricí (data tak nelze rekonstruovat).

A.11.2.8 Neobsluhovaná uživatelská zařízení

Cíl: Uživatelé by měli zajistit přiměřenou ochranu neobsluhovaného zařízení.
Vyloučeno: Ano
Způsob plnění: Bezpečnost neobsluhovaných zařízení je obsažena v interních předpisech společnosti.

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Cíl: Pro vybavení pro zpracování informací by měla být přijata zásada prázdného stolu, týkající se papírových dokumentů a vyměnitelných paměťových médií, a zásada prázdné obrazovky.
Vyloučeno: Ne
Způsob plnění: Pro zajištění tohoto požadavku existují interní nařízení a předpisy.

A.12 Bezpečnost provozu

A.12.1 Provozní postupy a odpovědnost

Cíl: Zajistit správné a bezpečné provozování vybavení pro zpracování informací.

A.12.1.1 Dokumentace provozních postupů

Cíl: Provozní postupy by měly být dokumentovány a být k dispozici všem uživatelům, kteří je potřebují.
Vyloučeno: Ano
Způsob plnění: Společnost má dokumentované postupy a procesy v rámci certifikace ISO 9001.

A.12.1.2 Řízení změn

Cíl: Změny v organizaci podnikových procesech, vybavení pro zpracování informací a systémech, které mají vliv na bezpečnost informací, by měly být řízeny a kontrolovány.
Vyloučeno: Ano
Způsob plnění: Všechny změny jsou řízeny vedením, které o nich informuje.

A.12.1.3 Řízení kapacit

Cíl: K zajištění požadovaného výkonu systému z pohledu budoucích požadavků na kapacity by mělo být používání zdrojů monitorováno, optimalizováno a naplánováno.
Vyloučeno: Ano
Způsob plnění: Monitoring výkonu a jeho zajištění provádějí vedoucí jednotlivých oddělení. Případné nedostatky nebo problémy jsou řešeny v rámci denní komunikace.

A.12.1.4 Princip oddělení prostředí vývoje, testování a provozu

Cíl: Vývojová, testovací a provozní prostředí by měla být oddělena, aby se snížila rizika neoprávněného přístupu nebo změny provozního prostředí.
Vyloučeno: Ano
Způsob plnění: Testovací a vývojové prostředí je provozováno na rozdílných serverech.

A.12.2 Ochran před malwarem

Cíl: Zajistit, že informace a vybavení pro zpracování informací jsou před malwarem chráněny.

A.12.2.1 Opatření na ochranu proti malwaru

Cíl: Měla by být implementována opatření pro detekci, prevenci a zotaven na ochranu před malwarem, v kombinaci s vhodným zvyšováním povědomí uživatelů.
Vyloučeno: Ano
Způsob plnění: Využití bezpečnostního software společnosti ESET (antivirus, antimalware, firewall). Pravidelné zálohování důležitých dokumentů mimo prostory organizace. Bezpečnostní chování uživatelů je popsáno v rámci vnitřních předpisů.

A.12.3 Zálohování

Cíl: Ochrana před ztrátou dat.

A.12.3.1 Zálohování informací

Cíl: Pravidelně by měly být pořizovány a testovány záložní kopie informací, softwaru a bitových kopií systému v souladu se schválenou politikou zálohování.
Vyloučeno: Ne

Způsob plnění: Je sestaven plán pro zálohování. Zálohování je prováděno takzvanou metodou offsite.

A.12.4 Zaznamenávání formou logů a monitorování

Cíl: Zaznamenávat události a vytvářet záznamy.

A.12.4.1 Zaznamenávání událostí formou logů

Cíl: Musí být pořizovány, uchovávány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.
Vyloučeno: Ano
Způsob plnění: Logy jsou uchovávány v rámci záloh.

A.12.4.2 Ochrana logů

Cíl: Prostředky pro zaznamenávání formou logů a logy musí být chráněny proti zfalšování a neoprávněnému přístupu.
Vyloučeno: Ano
Způsob plnění: Zálohy jsou umístěny offsite a ze SLA plyne povinnost poskytovatele datového prostoru umisťovat zálohy na více, geolokačně oddělených, míst. Pro přístup k zálohám je nutná VPN nebo prioritní telefonní linka oddělená od klasického Internetu.

A.12.4.3 Logy o činnosti administrátorů a operátorů

Cíl: Aktivity systémového administrátora a systémového operátora musí být logovány a logy chráněny a pravidelně přezkoumávány.
Vyloučeno: Ano
Způsob plnění: Logy jsou uchovávány v rámci záloh.

A.12.4.4 Synchronizace hodin

Cíl: Hodiny všech důležitých systémů pro zpracování informací musí být v rámci organizace nebo bezpečnostních domén synchronizovány s jediným referenčním zdrojem času.
Vyloučeno: Ano
Způsob plnění: Synchronizace času všech kritických systémů probíhá proti společnému časovému serveru.

A.12.5 Správa provozního softwaru

Cíl: Zajistit integritu provozních systémů.

A.12.5.1 Instalace softwaru na provozní systémy

Cíl: Musí být implementovány postupy řízené instalace softwaru na provozních systémech.
Vyloučeno: Ano

Způsob plnění: Na základě ověření proti RADIUS serveru nebo proti osobnímu certifikátu jsou uživateli přidělena taková práva, která jsou nezbytně nutná pro výkon jeho práce. Instalace software na důležité systémy je povolená pouze správci.

A.12.6 Řízení technických zranitelností

Cíl: Zabránit využívání technických zranitelností.

A.12.6.1 Instalace softwaru na provozní systémy

Cíl: Musí být zajištěno včasné získání informací o existenci technických zranitelností provozovaných informačních systémů, vyhodnocena úroveň ohrožení organizace vůči těmto zranitelnostem a přijata příslušná opatření na zvládání souvisejících rizik.
Vyloučeno: Ano
Způsob plnění: Kritické systémy jsou zdvojeny (je na ně tedy aplikována metoda ochrany redundancí).

A.12.6.2 Omezení instalace softwaru

Cíl: Musí být ustanovena a implementována pravidla ohledně instalace softwaru uživateli.
Vyloučeno: Ano
Způsob plnění: Na základě ověření proti RADIUS serveru nebo proti osobnímu certifikátu jsou uživateli přidělena taková práva, která jsou nezbytně nutná pro výkon jeho práce. Instalace software na důležité systémy je povolená pouze správci.

A.12.7 Hlediska auditu informačních systémů

Cíl: Minimalizovat dopady auditních činností na provozní systémy.

A.12.7.1 Opatření k auditu informačních systémů

Cíl: Požadavky auditu a činnosti zahrnující verifikaci provozních systémů musí být pečlivě naplánovány a schváleny, aby se minimalizovalo narušení procesů organizace.
Vyloučeno: Ano
Způsob plnění: Provádění auditu si zajišťuje společnost vlastními silami a jeho plánování je vždy prováděno vedoucími jednotlivých oddělení.

A.13 Bezpečnost komunikací

A.13.1 Správa bezpečnosti sítě

Cíl: Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací.

A.13.1.1 Opatření v sítích

Cíl: K ochraně informací v systémech a aplikacích musí být sítě řízeny, spravovány a kontrolovány.
Vyloučeno: Ne (revidovat)
Způsob plnění: Vzhledem k oboru podnikání si společnost bezpečnost sítě spravuje a řídí sama.

A.13.1.2 Bezpečnost síťových služeb

Cíl: Musí být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní mechanismy, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb, ať už jsou zajišťovány interně nebo cestou outsourcingu.
Vyloučeno: Ano
Způsob plnění: Vzhledem k oboru podnikání si společnost bezpečnost sítě spravuje a řídí sama.

A.13.1.3 Princip oddělení v sítích

Cíl: V sítích musí být odděleny skupiny informačních služeb, uživatelů a informačních systémů.
Vyloučeno: Ano
Způsob plnění: Zřízení několika virtuálních sítí. Přístup do sítí je přidělen na základě oprávnění získaných ověřením proti RADIUS serveru.

A.13.2 Přenos informací

Cíl: Zachovat bezpečnost informací přenášených v rámci organizace a s jakýmkoli externím subjektem.

A.13.2.1 Politiky a postupy při přenosu informací

Cíl: K ochraně přenosu informací prostřednictvím všech druhů komunikačních zařízená by měly být zavedeny formální politiky, postupy a opatření.
Vyloučeno: Ano
Způsob plnění: Zachování bezpečnosti informací při přenosu je již součástí interních předpisů.

A.13.2.2 Dohody o přenosu informací

Cíl: Dohod by měly řešit bezpečný přenos obchodních informací mezi organizací a externími stranami.
Vyloučeno: Ano
Způsob plnění: Bezpečnost přenosu informací je součástí konkrétních dohod se zákazníky.

A.13.2.3 Elektronické předávání zpráv

Cíl: Informace zahrnuté v elektronicky předávaných zprávách by měly být přiměřeně chráněny.
Vyloučeno: Ano
Způsob plnění: Společnost již má ochranu elektronicky předávaných zpráv implementovanou v rámci interních předpisů.

A.13.2.4 Dohody o důvěrnosti nebo mlčenlivosti

Cíl: Měly by být identifikovány, pravidelně přezkoumávány a dokumentovány požadavky týkající se dohod o zachování důvěrnosti nebo mlčenlivosti odrážející potřeby organizace pro ochranu informací.
Vyloučeno: Ano
Způsob plnění: Dohoda o ochraně informací a mlčenlivosti je součástí pracovní smlouvy. Dále vychází ze zákona číslo 101/2000 Sb. (*Zákon o ochraně osobních údajů a o změně některých zákonů*) a dle platných ustanovení občanského zákoníku o ochraně vlastnictví (konkrétně jde o § 1040-1042).

A.14 Akvizice, vývoj a údržba systémů

A.14.1 Bezpečnostní požadavky informačních systémů

Cíl: Zajistit, aby se bezpečnost informací stala nedílnou součástí informačních systémů během celého životního cyklu. To zahrnuje také požadavky na informační systémy poskytující služby přes veřejné sítě.

A.14.1.1 Analýza a specifikace požadavků bezpečnosti informací

Cíl: V požadavcích na nové informační systémy nebo ve vylepšeních stávajících informačních systémů by měly být zahrnuty požadavky související s bezpečností informací.
Vyloučeno: Ano
Způsob plnění: Nesouvisí s předmětem podnikání společnosti.

A.14.1.2 Zabezpečení aplikačních služeb ve veřejných sítích

Cíl: Informace zahrnuté v aplikačních službách probíhajících přes veřejné sítě by měly být chráněny před podvodnou činností, smluvními spory a neoprávněným zpřístupněním a změnou.
Vyloučeno: Ano
Způsob plnění: Všechny aplikační služby provozované mimo interní síť jsou šifrované a provozované nad HTTPS.

A.14.1.3 Ochrana transakcí aplikačních služeb

Cíl: Informace zahrnuté v transakcích aplikačních služeb by měly být chráněny, aby se zabránilo nedokončenému přenosu, chybnému směrování, neoprávněnému pozměnění zprávy, neoprávněnému zveřejnění, neoprávněnému duplikování nebo opakovanému přenosu zprávy.
Vyloučeno: Ano
Způsob plnění: Všechny aplikační služby provozované mimo interní síť jsou šifrované a provozované nad HTTPS.

A.14.2 Bezpečnostní v procesech vývoje a podpory

Cíl: Zajistit, aby byla v rámci životního cyklu vývoje informačních systémů koncipována a implementována bezpečnost informací.

A.14.2.1 Politika bezpečného vývoje

Cíl: V rámci organizace by měla být stanovena a při vývoji uplatněna pravidla pro vývoj softwaru a systémů.
Vyloučeno: Ano
Způsob plnění: Bezpečností pravidla jsou součástí interních pokynů ve společnosti.

A.14.2.2 Postupy řízení změn systémů

Cíl: Změny systémů v rámci životního cyklu vývoje by měly být řízeny a kontrolovány pomocí formálních postupů řízení změn.
Vyloučeno: Ano
Způsob plnění: Nesouvisí s předmětem podnikání společnosti.

A.14.2.3 Technické přezkoumání aplikací po změnách provozní platformy

Cíl: Při změnách provozních platforem by měly být přezkoumány a otestovány aplikace kritické pro činnosti organizace, aby se zajistilo, že změny nemají nepříznivý dopad na provoz nebo bezpečnost organizace.
Vyloučeno: Ano
Způsob plnění: Společnost má implementovány interní postupy pro zabezpečení bezpečnosti a kontinuity aplikací při změně provozní platformy.

A.14.2.4 Omezení změn softwarových balíků

Cíl: Modifikace softwarových balíků by neměly být žádoucí, měly by být omezeny na nezbytné změny a všechny změny by měly být striktně řízeny.
Vyloučeno: Ano
Způsob plnění: Nesouvisí s předmětem podnikání společnosti.

A.14.2.5 Princip inženýrství bezpečnostních systémů

Cíl: Měly by být ustanoveny, zdokumentovány a udržovány principy inženýrství bezpečnostních systémů a aplikovány na všechny programy implementace informačního systému.
Vyloučeno: Ano
Způsob plnění: Nesouvisí s předmětem podnikání společnosti.

A.14.2.6 Bezpečné vývojové prostředí

Cíl: Organizace by měly ustavit a přiměřeně chránit bezpečná vývojová prostředí pro vývoj systémů a integrační program, které porývají celý životní cyklus vývoje systému.
Vyloučeno: Ano
Způsob plnění: Nesouvisí s předmětem podnikání společnosti.

A.14.2.7 Vývoj zajišťovaný externími zdroji

Cíl: Organizace by měla monitorovat a dohlížet na vývoj systému zajišťovaného externími zdroji.
Vyloučeno: Ano
Způsob plnění: Nesouvisí s předmětem podnikání společnosti.

A.14.2.8 Testování bezpečnosti systému

Cíl: Testování funkčnosti bezpečnosti by mělo být uskutečněno během vývoje systému.
Vyloučeno: Ano
Způsob plnění: Nesouvisí s předmětem podnikání společnosti.

A.14.2.9 Testování akceptace systému

Cíl: Pro nové informační systému, aktualizace a nové verze by měly být ustanoveny programy pro akceptační testy a související kritéria.
Vyloučeno: Ano
Způsob plnění: Nesouvisí s předmětem podnikání společnosti.

A.14.3 Data pro testování

Cíl: Zajistit ochranu dat použitých při testování.

A.14.3.1 Ochrana dat pro testování

Cíl: Data pro testování by měla být pečlivě vybrána, chráněna a kontrolována.
Vyloučeno: Ano
Způsob plnění: Testovací data jsou anonymizována dle stávajících nařízení společnosti.

A.15 Vztahy s dodavateli

A.15.1 Bezpečnost informací ve vztazích s dodavateli

Cíl: Zajistit ochranu těch aktiv organizace, která jsou přístupná dodavatelům.

A.15.1.1 Politika bezpečnosti informací pro oblast vztahů s dodavateli

Cíl: Požadavky v oblasti bezpečnosti informací na zmírnění rizik spojených s přístupem dodavatele k aktivům organizace by měly být s dodavatelem dohodnuty a zdokumentovány.
Vyloučeno: Ano
Způsob plnění: Dodavatelé nemají přístup k aktivům společnosti.

A.15.1.2 Řešení bezpečnosti v rámci smluv s dodavateli

Cíl: Měly by být stanoveny všechny podstatné požadavky na bezpečnost informací a odsouhlaseny s každým dodavatelem, který může k informacím organizace přistupovat, zpracovávat je, ukládat, přenášet je nebo pro ně poskytovat komponenty IT infrastruktury.
Vyloučeno: Ano
Způsob plnění: Tato problematika je řešena prostřednictvím smluv s dodavateli.

A.15.1.3 Řetězec dodavatelů informačních a komunikačních technologií

Cíl: Smlouvy s dodavateli by měly zahrnovat požadavky na řešení rizik v oblasti bezpečnosti informací souvisejících se službami informačních a komunikačních technologií a produkty řetězce dodavatelů.
Vyloučeno: Ano
Způsob plnění: Vzhledem k velikosti společnosti a z toho plynoucí vyjednávají síle není společnost schopna relevantně ovlivnit toto kritérium.

A.15.2 Řízení dodávky služeb dodavatelem

Cíl: Udržovat dohodnuté úrovně bezpečnosti informací a dodávky služeb v souladu s dodavatelskými smlouvami

A.15.2.1 Monitorování a přezkoumávání služeb dodavatelů

Cíl: Organizace by měly pravidelně monitorovat, přezkoumávat a provádět audit dodávky služeb dodavateli.
Vyloučeno: Ne
Způsob plnění: V současné době probíhá pravidelné audit služeb dodavatele. V případě nesplnění požadavků je dodavateli vyměřena pokuta dle SLA.

A.15.2.2 Řízení změn služeb dodavatelů

Cíl: Změny v poskytování služeb ze strany dodavatelů, včetně udržování a zlepšování stávajících politik bezpečnosti informací, postupů a opatření, by měly být řízeny, s ohledem na kritičnosti souvisejících informací, systémů a procesů, a opětovné posuzování rizik.
Vyloučeno: Ne
Způsob plnění: Tato problematika je řešena prostřednictvím smluv s dodavateli.

A.16 Řízení incidentů bezpečnosti informací

A.16.1 Řízení incidentů bezpečnosti informací a zlepšování

Cíl: Zajistit důsledný a efektivní přístup k řízení incidentů bezpečnosti informací, včetně komunikace ohledně bezpečnostních událostí a slabých míst.

A.16.1.1 Odpovědnosti a postupy

Cíl: Měly by být ustanoveny odpovědnosti a postupy managementu s cílem zajistit rychlou, efektivní a řádnou odezvu na incidenty bezpečnosti informací.
Vyloučeno: Ano
Způsob plnění: Odpovědnost a povinnosti uživatelů jsou součástí interních předpisů společnosti.

A.16.1.2 Podávání zpráv o událostech bezpečnosti informací

Cíl: Události bezpečnosti informací by měly být, co nejrychleji oznámeny prostřednictvím příslušných řídících kanálů.
Vyloučeno: Ano
Způsob plnění: Události jsou ihned hlášeny příslušným pracovníkům.

A.16.1.3 Podávání zpráv o slabých místech bezpečnosti informací

Cíl: Zaměstnanci a smluvní strany používající informační systém a služby organizace by měli být povinni upozornit a oznámit veškerá zpozorovaná nebo domnělá slabá místa bezpečnosti a měly by proto být hlášeny jako události bezpečnosti informací.
Vyloučeno: Ano
Způsob plnění: Povinnost stanovena v rámci interních předpisů organizace.

A.16.1.4 Posuzování a rozhodování o událostech bezpečnosti informací

Cíl: Události bezpečnosti informací by měly být posouzeny a mělo by být rozhodnuto, zda mají být klasifikovány jako incidenty bezpečnosti informací.
Vyloučeno: Ano
Způsob plnění: Posuzování a rozhodování o událostech bezpečnosti informací provádí k tomu určení pracovníci na základě povinností stanovených v rámci interních nařízení organizace.

A.16.1.5 Odezva na incidenty bezpečnosti informací

Cíl: Na incidenty bezpečnosti informací by mělo být reagováno v souladu s dokumentovanými postupy.
Vyloučeno: Ne (revidovat)
Způsob plnění: Odezva na incidenty bezpečnosti informací je rozdělena do několika stupňů. Nejvyšším stupněm je odezva na napadnutí systému. V takovém případě je nutné jednat rychle – v řádu minut. V ostatních případech je událost zaznamenána na logů a následně je vypracován report o události (*pokud již na tuto událost report neexistuje*) a je doporučen postup pro zvládání incidentu.

A.16.1.6 Poučení z incidentů bezpečnosti informací

Cíl: Znalosti získané z analýzy a řešení incidentů bezpečnosti informací by měly být použity ke snížení pravděpodobnosti nebo dopadu budoucích incidentů.
Vyloučeno: Ne (revidovat)
Způsob plnění: Viz předchozí krok.

A.16.1.7 Shromažďování důkazů

Cíl: Organizace by měla definovat a aplikovat postupy pro identifikaci, shromažďování, získávání a uchování informací, které mohou sloužit jako důkazy.
Vyloučeno: Ano
Způsob plnění: Archivují se logy z řešení Flowmon Probe.

A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

A.17.1 Kontinuita bezpečnosti informací

Cíl: Kontinuita bezpečnosti informací by měla být začleněna do systémů řízení kontinuity činností organizace.

A.17.1.1 Plánování kontinuity bezpečnosti informací

Cíl: Organizace by měla stanovit své požadavky na bezpečnost informací a kontinuitu řízení bezpečnosti informací v nepříznivých situacích, například během krize nebo katastrofy.
Vyloučeno: Ano
Způsob plnění: Společnost má definovány požadavky na bezpečnost informací a kontinuitu řízení jejich bezpečnosti při nepříznivých situacích. Na základě těchto požadavků je vytvořen zálohovací plán a je nastavena různá granularita zálohování pro různě kritické informace.

A.17.1.2 Implementace kontinuity bezpečnosti informací

Cíl: Organizace by měla ustavit, dokumentovat, zavést a udržovat procesy, postupy a opatření k zajištění požadované úrovně bezpečnosti informací během nepříznivé situace.
Vyloučeno: Ano
Způsob plnění: Řešeno v rámci smluv s dodavateli a také v rámci procesů, které jsou certifikovány dle normy ISO 9001.

A.17.1.3 Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací

Cíl: Organizace by měla ověřovat ustavená a zavedená opatření kontinuity bezpečnosti informací v pravidelných intervalech, aby se zajistilo, že jsou během nepříznivých situací platná a efektivní.
Vyloučeno: Ano
Způsob plnění: Zaměstnanci jsou pravidelně školeni z problematiky kontinuity bezpečnosti informací. V rámci tohoto školení probíhají i testování znalostí.

A.17.2 Redundance

Cíl: Zajistit dostupnost vybavení pro zpracování informací.

A.17.2.1 Dostupnost vybavení pro zpracování informací

Cíl: Vybavení pro zpracování informací by mělo být zaváděno s dostatečnou redundancí, aby byly splněny požadavky dostupnosti.
Vyloučeno: Ano
Způsob plnění: Redundance není zavedena pro všechny prvky, ale jen u těch, které jsou kritické pro kritické pro podnikání. Příkladem je redundance síťových tras k vývojovým serverům.

A.18 Soulad s požadavky

A.18.1 Soulad se zákonnými a smluvními požadavky

Cíl: Zamezit porušení právních, zákonných, předpisových nebo smluvních povinností souvisejících s bezpečností informací a jakýchkoli požadavků bezpečnosti.

A.18.1.1 Identifikace příslušné legislativy a smluvních požadavků

Cíl: Všechny zákonné, předpisové, smluvní požadavky příslušné legislativy a přístup organizace ke splnění těchto požadavků musí být explicitně identifikovány, dokumentovány a udržovány v aktuálním stavu pro každý informační systém a organizaci.
Vyloučeno: Ano
Způsob plnění: K tomuto účelu má společnost vytvoření speciální oddělení, které dohlíží

na dodržování legislativy. Pokud nastanou nějaké nejasnosti, jsou tyto nejasnosti konzultovány s firemním právníkem.

A.18.1.2 Práva k duševnímu vlastnictví

Cíl: Pro zajištění souladu s legislativními, předpisovými a smluvními požadavky týkající se práv duševního vlastnictví a používání proprietárních softwarových produktů by měla být implementována vhodná opatření.
Vyloučeno: Ano
Způsob plnění: Ochrana duševního vlastnictví je implementována v rámci interních předpisů společnosti.

A.18.1.3 Ochrana záznamů

Cíl: Záznamy by měly být chráněny před ztrátou, zničením, falšováním, neoprávněným přístupem a neoprávněným vydáním v souladu s legislativními, předpisovými, smluvními požadavky a požadavky týkajícími se činnosti organizace.
Vyloučeno: Ano
Způsob plnění: Všechny záznamy se převádějí do digitální podoby (*pokud již v digitální podobě nejsou pořízeny*) a probíhá nad nimi plánované zálohování.

A.18.1.4 Soukromí a ochrana osobních údajů

Cíl: Soukromí a ochrana osobních údajů by měla být zajištěna v souladu s požadavky příslušné legislativy a nařízení tam, kde lze požadavky uplatnit.
Vyloučeno: Ano
Způsob plnění: Ochrana osobních údajů a soukromí se řídí dle zákona číslo 101/2000 Sb. (*Zákon o ochraně osobních údajů a o změně některých zákonů*) a dle platných ustanovení občanského zákoníku o ochraně vlastnictví (konkrétně jde o § 1040-1042).

A.18.1.5 Regulace kryptografických opatření

Cíl: Kryptografická opatření by měla být používána v souladu se všemi příslušnými dohodami, legislativou a předpisy.
Vyloučeno: Ano
Způsob plnění: Kryptografická opatření a jejich používání jsou součástí interních předpisů.

A.18.2 Přezkoumání bezpečnosti informací

Cíl: Zajistit, že bezpečnost informací je implementována a provozována v souladu s politikami a postupy organizace.

A.18.2.1 Nezávislé přezkoumání bezpečnosti informací

Cíl: Přístupy organizace k řízení bezpečnosti informací a její implementaci (tj. cíle opatření, politiky, procesy a postupy pro bezpečnost informací) by měl být nezávisle přezkou-

mán v naplánovaných intervalech, nebo když dojde k významným změnám.
Vyloučeno: Ano
Způsob plnění: Po plném zavedení bezpečnosti informací bude bezpečnost auditována nezávislou organizací v pravidelných intervalech nebo pokud dojde k významným změnám.

A.18.2.2 Soulad s bezpečnostními politikami a normami

Cíl: Vedoucí pracovníci by měli pravidelně přezkoumávat soulad zpracování informací a postupy v rámci své působnosti s příslušnými bezpečnostními politikami, normami a jakýmikoli dalšími požadavky na bezpečnost.
Vyloučeno: Ano
Způsob plnění: Společnost pravidelně přezkoumává bezpečnost informací z interního pohledu. Tuto agendu provádějí vybraní pracovníci (*většinou vedoucí oddělení*). Pro zpracování důvěrných nebo tajných informací z prvků kritické infrastruktury nemá společnost certifikaci.

A.18.2.3 Přezkoumání technického souladu

Cíl: Informační systémy by měly být pravidelně přezkoumávány z hlediska souladu s politikami a normami bezpečnosti informací organizace.
Vyloučeno: Ano
Způsob plnění: Nesouvisí s předmětem podnikání společnosti.