VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

BEZPEČNOST MOBILNÍCH ZAŘÍZENÍ V MALÉ SPOLEČNOSTI

SMALL COMPANY MOBILE SECURITY

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Radek Válka

AUTHOR

VEDOUCÍ PRÁCE — Ing. Viktor Ondrák, Ph.D.

SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Radek Válka**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2019/20

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 bakalářskou práci s názvem:

Bezpečnost mobilních zařízení v malé společnosti

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout management bezpečnosti mobilních zařízení.

Základní literární prameny:

BLOKDYK, Gerardus. ISO IEC 27001 Lead Auditor A Complete Guide - 2019 Edition. 5STARCooks, 2019. ISBN 978-0655540854.

DOHERTY, Jim. Wireless and mobile device security. Burlington, MA: Jones & Bartlett Learning, 2016. Jones & Bartlett Learning information systems security & assurance series. ISBN 978-1284059274.

HUMPHREYS, Edward. Implementing the iso/iec 27001 isms standard, second edition. 2nd ed. Boston: Artech House, 2016. ISBN 978-1608079308.

TRIM, Peter R. J. a Yang-Im LEE. Cyber security management: a governance, risk and compliance framework. Burlington, VT: Gower, 2014. ISBN 978-1472432094.

WASCHKE, Marvin. Personal cybersecurity: how to avoid and recover from cybercrime. Bellingham, Washington: Apress, 2017. ISBN 978-1484224298.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

V průběhu práce je vytvořena analýza problematiky bezpečnosti s užíváním mobilních zařízení v malé společnosti. Na základě této analýzy jsou zjištěna rizika, která by mohla mít dopad na bezpečnost informací společnosti z důvodu škodlivého kódu v mobilním zařízení nebo neoprávněného přístupu do mobilního zařízení. Pro odstranění nebo snížení těchto rizik jsou navrhnuta bezpečnostní opatření inspirovaná opatřeními v normě ČSN ISO/IEC 27002, na která je bakalářská práce zaměřena.

Klíčová slova

Bezpečnostní opatření, bezpečnost informací, BYOD, informační systém, IT, ISO/IEC 27001, ISO/IEC 27002, MDM, mobilní zařízení, notebook, smartphone, směrnice, zabezpečení dat

Abstract

In the course of the work, an analysis of security issues with the use of mobile devices in a small company is created. Based on this analysis, are identified risks that could have an impact on the security of the company's information due to malicious code on the mobile device or unauthorized access to the mobile device. To eliminate or reduce these risks, are proposed safety measures inspired by the measures in the ČSN ISO/IEC 27002 standard, on which the bachelor's thesis is focused.

Key words

BYOD, data security, directives, information security, information system, IT, ISO/IEC 27001, ISO/IEC 27002, MDM, mobile devices, notebook, security measures, smartphone

Bibliografická citace

VÁLKA, Radek. *Bezpečnost mobilních zařízení v malé společnosti* [online]. Brno, 2020 [cit. 2020-05-05]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/125765. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

Čestné prohlášení

Prohlašuji, že předložená bakalářská 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 31. května 2020 ----------

podpis studenta

Poděkování

Tímto bych rád poděkoval především svému vedoucímu práce Ing. Viktoru Ondrákovi, Ph.D., za jeho rady, vstřícný přístup a čas, který mi věnoval při tvorbě této práce. Zároveň bych chtěl poděkovat zaměstnancům společnosti za jejich spolupráci a poskytnutí potřebných údajů k práci a také přátelům a rodině, kteří mě při tvorbě práce podporovali.

OBSAH

ÚVOD

Mobilní zařízení se rychle stávají nezbytným komunikačním a výpočetním nástrojem pro zaměstnance v různých typech společností. Poskytují jim větší flexibilitu, informační sílu, ale také nová rizika. Stále častěji používané funkce, jako jsou e-mail, surfování po internetu, sociální sítě a rozšířenější přístup k podnikovým sítím a důvěrným informacím, mohou pro podniky představovat významné riziko pro bezpečnost dat. Pokud nejsou použita příslušná technická a organizační opatření, mohou být tato zařízení zdrojem neoprávněného přístupu k datové a IT infrastruktuře společnosti.

Pro zajištění výše zmíněných opatření je v této práci zvolen postup pro zajištění bezpečnosti mobilních zařízení definovaný normou ISO/IEC 27001 Systém managementu bezpečnosti informací. Tato norma se stala velice uznávaným mezinárodním standardem, který specifikuje požadavky pro řízení bezpečnosti důvěry informací, procesů, IT systémů, zařízení a strategií společnosti.

Zabezpečení mobilních zařízení je v této bakalářské práci řešeno pro malou společnost, která se zabývá vývojem softwaru pro veřejnou dopravní infrastrukturu. Řešení problematiky bezpečnosti mobilních zařízení je součástí přípravy společnosti na certifikaci systému managementu bezpečnosti informací dle normy ISO/IEC 27001.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

V první části práce jsou vysvětleny teoretické pojmy, které souvisejí s tématem práce a jsou potřebné pro pochopení dané problematiky. Jedná se zejména o výrazy z normy ISO/IEC 27001 a z vybraných částí normy ISO/IEC 27002. Mezi pojmy je popsán systém řízení bezpečnosti informací, tzv. ISMS, jenž norma ISO/IEC 27001 charakterizuje. Práce obsahuje názvosloví používané ve vztahu s mobilními zařízeními a jejich systémy. Zároveň jsou zde také popsány možné hrozby, které mohou bezpečnost informací na mobilních zařízeních ohrozit. Ke konci teoretické části jsou vysvětleny pojmy používané v interní struktuře společnosti, které se práce taktéž věnuje.

V druhé části práce je popsána společnost, pro kterou je zabezpečení mobilních zařízení navrhováno. Je stanoven rozsah a hranice, ve kterých je řízení bezpečnosti informací aplikováno. Pro tuto práci se jedná o malou společnost pohybující se v oboru informačních technologií, která se připravuje na certifikaci systému řízení bezpečnosti informací podle normy ISO/IEC 27001. Po představení společnosti následuje analýza jejího současného stavu zabezpečení mobilních zařízení. Analýza je provedena v souladu se specifikovanými požadavky normy ISO/IEC 27001. Dále je posouzeno, která zařízení a systémy jsou zaměstnanci používány a jaká jsou současná opatření pro bezpečnost mobilních zařízení před začátkem implementace požadavků z normy ISO/IEC 27001. Pro zjištění potřebných bezpečnostních opatření je vypracována analýza rizik. Její průběh je podrobně v práci popsán a výstupy této analýzy jsou vloženy do příloh.

Posledním krokem práce je navržení technických zlepšení spolu s technickými a organizačními opatřeními. Účel těchto opatření je snížení rizik, které společnost stanovila jako neakceptovatelná a mohou mít dopad na bezpečnost informací ve společnosti z důvodu škodlivého kódu v mobilním zařízení nebo neoprávněného přístupu do mobilního zařízení.

Cílem práce je tedy zajistit společnosti adekvátní technické a organizační opatření pro zamezení vniknutí škodlivého kódu do mobilního zařízení nebo neoprávněného přístupu do mobilního zařízení, jenž by vedlo k narušení bezpečnosti informací. Tato opatření budou součástí celkových opatření pro řízení rizik před certifikací systému managementu bezpečnosti informací společnosti podle normy ISO/IEC 27001.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V této kapitole jsou popsána základní teoretická východiska, týkající se bezpečnosti informací, problematiky bezpečnosti mobilních zařízení a normy ISO/IEC 27001.

1.1 Systém řízení bezpečnosti informací (ISMS)

ISMS (anglicky Information security management system) je detailní zdokumentovaný systém, který nám popisuje, jak řídit a spravovat ve společnosti informační aktiva. Informační aktiva jsou samotné informace, ale i systémy, zařízení či dokumenty, které obsahují informace, vztahující se ke společnosti. Jsou pro společnost důležitá a mohou být osobou mimo společnost zneužita. Řízení a správa těchto informací podle ISMS by měla zamezit jakékoliv možnosti informace poškodit, nechat si je odcizit nebo ztratit (1).

Pro zajištění bezpečnosti těchto informací je podle ISMS nutné brát ohled zejména na tzv. bezpečnostní atributy informace. Bezpečnostními atributy informace jsou její důvěrnost, integrita a dostupnost.

Zabezpečením důvěrnosti informace zamezujeme, aby se k této informaci nedostal někdo, kdo by k ní neměl mít oprávněný přístup (2). Zajištěním integrity informace zajišťujeme, že je informace správná, přesná a úplná. Zabezpečením posledního atributu, atributu dostupnosti, zajišťujeme, aby informace a jakékoliv aktivum s ní spojené bylo dostupné vždy, když jej oprávněné osoby požadují (2).

Z důvodu, že způsobů zajištění bezpečnosti těchto atributů může být mnoho, je nutné určit, jaká společnosti hrozí rizika, která by mohla bezpečnost jejich aktiv ohrozit. Po určení a ohodnocení takovýchto rizik, která společnosti mohou hrozit, je nutné na nejvíce pravděpodobná a nejnebezpečnější rizika stanovit opatření, která tato rizika budou řešit. Aby mohla společnost určit potřebná opatření, je nutné vypracovat analýzu rizik, která výše zmíněná nejpravděpodobnější a nejnebezpečnější rizika identifikuje.

Dále by měla při implementaci ISMS společnost stanovit svoji bezpečnostní politiku. Jedná se o dokument, který popisuje, prohlašuje a vysvětluje, jakým způsobem je ve společnosti zajištěna bezpečnost (3).

ISMS může být zavedeno pro jakoukoliv organizační složku společnosti, informační systém nebo jeho část, nebo do něj lze zahrnout celou společnost.
Celková struktura ISMS by se dala tedy shrnout do těchto bodů:

- vymezení rozsahu a hranic ISMS,
- definování bezpečnostní politiky,
- identifikování a ohodnocení rizik,
- určení vhodného řízení rizik,
- výběr vhodných opatření,
- vytvoření přehledu zavedených a nezavedených bezpečnostních opatření v Prohlášení o aplikovatelnosti (1).

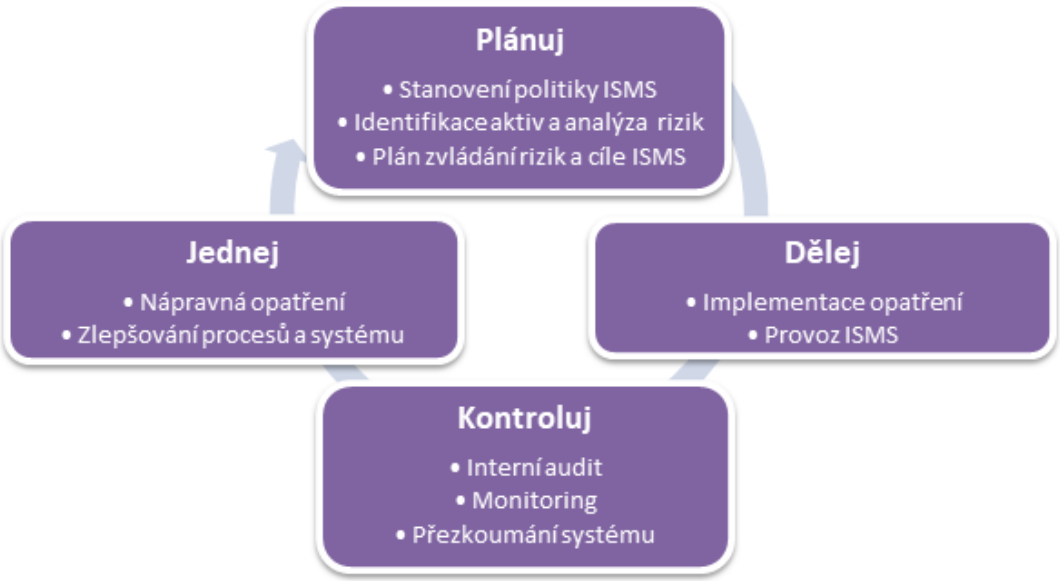
1.1.1 Model systému řízení bezpečnosti informací

Celý systém řízení bezpečnosti informací je založený na Demingově cyklu, tzv. PDCA modelu. Jedná se o metodu, kterou je možné dosáhnout postupného zlepšování bezpečnosti informací neustálým opakováním čtyř základních činností:

- plan (naplánování) – naplánování zamýšleného zlepšení (záměr),
- do (vykonání) – realizace plánu,
- check (zkontrolování) – ověření výsledku realizace oproti původnímu záměru,
- act (jednání) – úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe (4).

Díky držení se tohoto modelu je zavedení ISMS nejenom jednorázovou aktivitou, ale také jeho neustálým opakováním vede k postupnému zlepšování. Použitím tohoto modelu je bezpečnost informací udržována aktuální a jsou brány v potaz jakékoliv změny ve společnosti, nebo jakékoliv nové hrozby, které by mohly narušit bezpečnost informací (5).

Využití modelu PDCA pro neustálé zlepšování ISMS je znázorněno následujícím obrázkem:



Obrázek č. 1: Cyklus PDCA pro zlepšování ISMS (Zdroj: vlastní tvorba)

Jelikož je použití cyklu PDCA velmi univerzální, dá se využít pro postupné zlepšování i v jiném případě než v ISMS, například kvality výrobku, služeb nebo kvality aplikace.

1.1.2 Řada norem ISO/IEC 27000

Systém řízení bezpečnosti informací je určený řadou (rodinou) mezinárodních norem ISO/IEC 27000. Cílem této řady norem je poskytnutí podpory pro ustanovení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací (5). Nejpodstatnější a hlavní normou z této řady norem je ISO/IEC 27001, která definuje mezinárodně stanovené požadavky pro zajištění ISMS. Splněním těchto požadavků a následným provedením úspěšného auditu ISO/IEC 27001 od certifikační společnosti, může společnost získat mezinárodně platný certifikát, udávající, že společnost splňuje požadavky pro ISMS a zajišťuje bezpečnost informací.

Jednotlivé normy z rodiny se poté zaměřují na různé aspekty informační bezpečnosti (6). Nepodstatnějšími z norem jsou, kromě hlavní normy ISO/IEC 27001, norma ISO/IEC 27002, jež obsahuje soubor nejlepších praktik, rozdělených do čtrnácti oblastí pro zvýšení bezpečnosti informací v rámci ISMS (7) a dále norma ISO/IEC 27003, která je návodem pro zavedení ISMS.

1.1.3 Chráněné informace

Pro určení, jaké informace společnosti je nutné chránit z hlediska důvěrnosti, tzn. že se k nim nedostane nikdo, kdo by k nim neměl mít povolen přístup, slouží klasifikace informací. Celkový postup klasifikace informací je v ISMS poněkud komplikovanější, pro práci se ho pokusím zjednodušit rozdělením informací (klasifikací) na:

- veřejné informace: jedná se o široký okruh informací k zajištění činností společnosti, které jsou schváleny ke zveřejnění nebo se staly obecně dostupnými veřejnosti,
- neveřejné informace (chráněné):
    - interní informace: neveřejné informace, jejichž vyzrazení, zneužití nebo poškození může být pro společnost nevýhodné a prozrazení těchto informací může ovlivnit činnost společnosti,
    - citlivé informace: informace, jejichž nutnost ochrany vyplývá z legislativy nebo ze závazků společnosti. Jejich vyzrazení nebo zneužití může vést k výraznému ohrožení zájmů společnosti.

Při řízení systému bezpečnosti informací musí společnosti udržovat zejména důvěrnost chráněných informací. Zajištění důvěrnosti chráněných informací je zakomponováno do návrhu technických a organizačních opatřeních pro mobilní zařízení, kterému se práce věnuje.

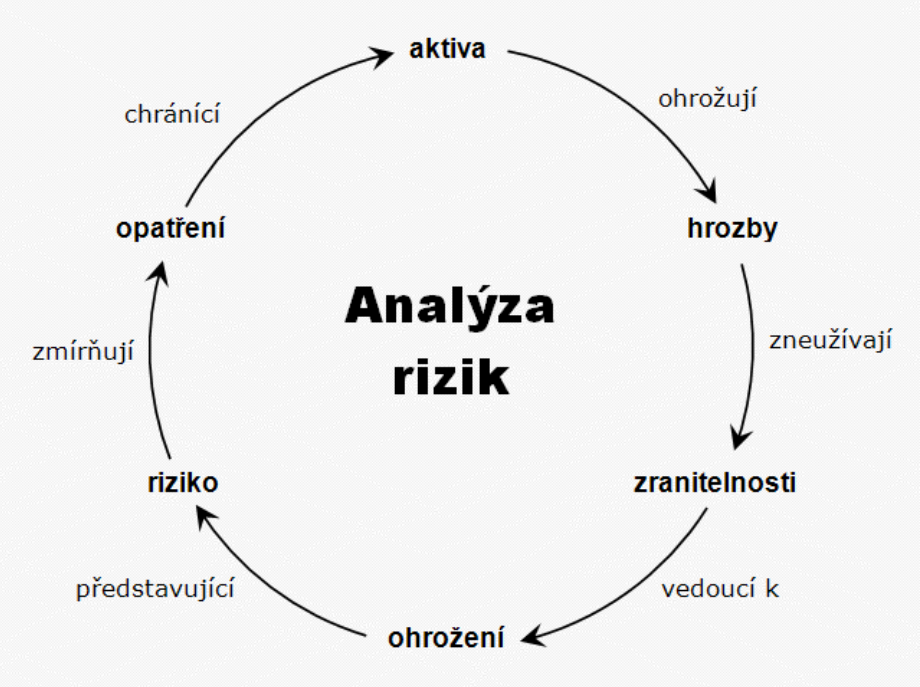
1.1.4 Analýza rizik

Analýza rizik (risk management) v informační bezpečnosti je proces, díky kterému lze rozpoznat rizika, která mohou mít vliv na bezpečnost informací a na základě něho můžeme určit nejvhodnější kroky pro eliminaci těchto rizik. Tento proces je však nejefektivnější, pokud společnost investuje své zdroje (finanční nebo lidské) tak, že dopad na bezpečnost informací u chráněných aktiv je úměrný nákladům za bezpečnostní opatření. Tento aspekt závisí na rozsahu možné hrozby, kterému může být aktivum vystaveno. Pro určení vhodného investování zdrojů do bezpečnostních opatření je tedy nutné zvolit vhodnou metodiku analýzy rizik (54).

Cílem analýzy rizik je identifikovat aktiva a určit jejich význam pro fungování společnosti (ohodnocení aktiv) k nalezení možných zdrojů nebezpečí (hrozeb) těchto

aktiv. Na základě těchto hrozeb je vyhodnocena současná úroveň ochrany, která slouží k nalezení existujících slabých stránek těchto ochranných opatření (zranitelností) a podle nich se určuje konečná míra rizika ohrožující aktivum (54).

Průběh celého procesu znázorňuje následující obrázek:



Obrázek č. 2: Celkový proces analýzy rizik (Zdroj: cleverandsmart.cz) (54)

1.1.5 Bezpečnostní událost

Bezpečnostní událost v informační bezpečnosti je taková událost, která může způsobit narušení bezpečnosti informací. Narušení bezpečnosti informací je považováno za porušení jednoho ze tří bezpečnostních atributů poškozeného aktiva. Bezpečnostní událost se může vyskytnout v informačních systémech, nebo narušením bezpečnostních služeb a komunikačních sítí. Za bezpečnostní událost může být považován i pokus o narušení fyzické bezpečnosti společnosti (34).

1.1.6 Bezpečnostní incident

Bezpečnostní incident je situace, která ústí z bezpečnostní události. Na rozdíl od bezpečnostní události, při vzniku incidentu prokazatelně došlo k narušení bezpečnosti

informací. Bezpečnostní incident nejčastěji vzniká v důsledku selhání či nedodržení bezpečnostních opatření nebo porušení bezpečnostní dokumentace (35).

Příklady bezpečnostního incidentu mohou být:

- užívání nelegálního SW,
- neautorizovaný přístup k datům nebo službám IS,
- zneužití přístupových práv administrátorů,
- porušení autorských práv (nelegální kopírování SW),
- požár, oheň, kouř, výbuch, narušení konstrukce budovy s dopadem na bezpečnost aktiv ve společnosti,
- ztráta nezabezpečeného zařízení (např. telefonu), obsahující osobní údaje o větším počtu zákazníků.

1.2 Definice malé společnosti

Organizace, na kterou je zaměřena tato práce, je společností s ručeným omezeným, která je jedním z druhů obchodních společností. Dále bude v této práci nazývána pouze jako „společnost“.

Podle „zákona č. 563/1991 Sb., zákon o účetnictví“ jsou rozděleny společnosti na čtyři kategorie účetních jednotek, kterými jsou:

- mikro účetní jednotka,
- malá účetní jednotka,
- střední účetní jednotka,
- velká účetní jednotka (36).

Dle stanovených kritérií „Zákonem o účetnictví“, spadá tato společnost do kategorie malé účetní jednotky, jelikož má méně než 50 zaměstnanců a hodnota aktiv společnosti nepřekračuje 100 000 000 Kč (36).

1.3 Organizační role v rámci bezpečnosti informací

Pro řízení systému bezpečnosti informací je nutné ve společnosti stanovit tzv. bezpečnostní role. Tyto role jsou zvoleny z důvodu, že bezpečnost informací prochází při jejím řízení všemi úrovněmi managementu. Z toho důvodu je nutné stanovit

role, které budou bezpečnost informací na jednotlivých úrovních managementu zajišťovat (8).

Jelikož se tato práce věnuje zajištění bezpečnosti informací v malé společnosti, jsou na základě předpokládaného rozsahu společnosti definovány pouze tři základní organizační role.

1.3.1 Manažer informační bezpečnosti

Osoba, která bude zastávat bezpečnostní roli manažera informační bezpečnosti, je odpovědná za celkové řízení systému bezpečnosti informací. Měla by být pro roli odborně způsobilá a vyškolená. Manažer informační bezpečnosti by měl vrcholové vedení společnosti informovat o stavu ISMS a být jakýmsi mezičlánkem mezi vrcholovým vedením a zaměstnanci, které řídí (8). V praxi poskytuje pokyny, řídí a koordinuje činnosti zaměstnanců pod jeho vedením v rámci ISMS.

1.3.2 Garant aktiva

Garant aktiva je osoba, která má za cíl zajištění rozvoje, použití a bezpečnosti aktiva, ke kterému je přiřazena. Nejčastěji bývá touto osobou vedoucí určitého oddělení. Zajištěním bezpečnosti aktiva je v rámci ISMS myšleno zajištění důvěrnosti, integrity a dostupnosti aktiva.

V praxi garant tedy rozhoduje u svěřených aktiv o jejich zabezpečení a na základě svého uvážení rozhoduje o tom, jaká opatření by měla být pro aktivum zavedena. Zodpovídá se a konzultuje svá rozhodnutí s manažerem informační bezpečnosti (8).

1.3.3 Správce ICT

Jelikož garanti aktiv z velké části nejsou IT ani techničtí specialisté a rozhodují o bezpečnosti aktiv zejména z organizačního hlediska, musí existovat osoba, která úkony garanta aktiv vykoná. Takovou osobou je správce ICT. Jeho činností je technické vykonávání rozhodnutí garanta aktiva a manažera informační bezpečnosti. Stará se o správu, provoz, použití a údržbu aktiva. Nejčastěji tuto funkci ve společnosti zastává vedoucí IT oddělení.

1.4 Prostředky zabezpečení dat

Bezpečnostními prostředky jsou technické a programové nástroje, nebo systémové činnosti, které zabezpečují důvěrnost nebo integritu informací společnosti.

1.4.1 Antivirový program

Podle normy ISO/IEC 27002 je implementace aktivní a aktuální ochrany antivirovým programem jedno z nejdůležitějších opatření pro hrozby škodlivých programů, které mohou napadnout výpočetní zařízení a ohrozit tak bezpečnost informací společnosti (23). Antivirový program sleduje nejdůležitější místa, ať už jsou vstupní nebo výstupní, kterými by se mohl škodlivý program dostat do počítačového systému společnosti. Sledováním těchto míst se snaží proniknutí škodlivých programů předcházet (37).

Antivirový program by měl být nainstalován na všech výpočetních zařízeních, která pracují s informacemi společnosti a mají přístup do počítačové sítě společnosti. Tato zařízení spolu s antivirovým programem by měla být pravidelně aktualizována, aby se předcházelo nově vzniklým hrozbám.

1.4.2 Firewall

Firewall je hardwarový nebo softwarový prvek, který v počítačové síti povoluje nebo naopak blokuje příchozí a odchozí komunikaci. Toto povolování a blokování provádí na základě nastavených pravidel. Tato pravidla mohou být přednastavená, nebo zvolená uživatelem (9). Jelikož se jedná z hlediska bezpečnosti o jakousi základní bránu mezi bezpečností počítačové sítě společnosti a vnějšími hrozbami, měla by každá společnost brát velký důraz na jeho správu.

Jak uvádí publikace „CyberSecurity“ docenta Jana Koloucha, ke zvýšení bezpečnosti je nutné nastavit firewall jako aplikační bránu (proxy bránu), nebo jako stavový paketový[1] filtr pro filtrování příchozí a odchozí komunikace ze sítě (39).

Proxy brána slouží jako komunikační prostředník mezi klientem (uživatelem) a cílovým serverem. Proxy brána překládá požadavky klienta vůči serveru a přebírá jeho odpověď,

[1] paket – blok dat uzpůsobený pro přenášení po elektronických komunikacích

kterou doručuje zpět klientovi. Během komunikace blokuje příchozí komunikaci podle jejího obsahu (38).

1.4.3 VPN (Virtual private network)

V případě, že je nutné propojit dvě zařízení a předávané informace mezi zařízeními nesmí být přístupné jakékoliv třetí osobě, je vhodné zvolit VPN. VPN je bezpečné propojení dvou a více zařízení. Mezi zařízeními se vytvoří tzv. tunel, v němž se přenáší všechny informace šifrovaně. Tuto metodu je vhodné využít např. při práci zaměstnanců mimo pracoviště v případě, že se potřebují připojit do sítě společnosti nebo při komunikaci více poboček společnosti.

1.4.4 Správa mobilních zařízení

Ve firmách se často používají zařízení různých výrobců a operačních systémů nebo zaměstnanci používají pro pracovní účely svá vlastní zařízení. Správa těchto zařízení je mnohdy časově náročná a komplikovaná. IT technici musí každé zařízení spravovat zvlášť a u každého zařízení může konfigurace probíhat jinak. Na zařízeních je také často nutná jednotná kontrola přístupu k firemním informacím. V případě, že se odhalí bezpečnostní problém, na jehož základě je nutné změnit nastavení mobilních zařízení, může dojít z důvodu časové prodlevy k daleko většímu negativnímu dopadu. Tato prodleva může být způsobena absencí centrální správy a nutnou postupnou změnou nastavení všech mobilních zařízení (10).

Jako sofistikované řešení lze využít nástroj pro správu mobilních zařízení, anglicky Mobile Device Management (MDM). MDM je technologie, která slouží ke zvýšení bezpečnosti zařízení a firemních dat. Pomocí MDM lze centrálně spravovat firemní mobilní zařízení a spojit zařízení s podnikovým IT prostředím (11).

Nástrojem pro MDM lze technicky vynucovat bezpečnostní pravidla, která stanoví např. bezpečnostní politiky. Důležitým aspektem je také, že požadovaná technická bezpečnostní pravidla lze nastavit pouze jednou v systému a následně budou pravidla aplikována jednotně na všech mobilních zařízeních, která jsou napojena na MDM.

Pomocí MDM lze řešit například jednotné uzamykání zařízení, vyžadování hesla pro jeho odemknutí, samo uzamykání zařízení při nečinnosti, šifrování paměti zařízení nebo

vzdálené smazání obsahu zařízení v případě ztráty nebo odcizení zařízení. Každá společnost může mít své specifické požadavky na MDM podle toho, jakou úroveň správy poskytuje jednotlivým zaměstnancům či jejich skupinám (11).

Druhů nástrojů pro MDM je v dnešní době mnoho. Existují rozdílné nástroje pro např. mobilní telefony nebo přenosné notebooky. Velký počet výrobců často používaných aplikací nebo systémů v organizacích nabízí možnost propojení správy těchto aplikací, které jsou nainstalovány na zařízeních zaměstnanců a umožňují využití tohoto propojení jako MDM. Dobrým příkladem je například nástroj od společnosti ESET Security Management Center.

1.4.5 Autentizace

Podle postupů v normě 27002 by měla být na každém mobilním zařízení nastavena nutná autentizace zaměstnance (23). Nutnou autentizací zaměstnance lze zamezit hrozbám, jako je zneužití identity nebo zneužití a neoprávněné modifikaci údajů, ke kterým má uživatel přístup přes mobilní zařízení.

Autentizace je ověření určité identity nějakého subjektu. Toto ověření má za cíl zjistit, zda je daný subjekt skutečně ten, za kterého se vydává (40).

Autentizace subjektu může proběhnout několika různými způsoby, jelikož bývá založena na tom, že zaměstnanec:

- **něco ví** – nejpoužívanější autentizační metoda. Metoda je založena na znalosti určité věci. Nejčastěji se jedná o znalost uživatelského jména a hesla zaměstnance, méně častěji je používáno, že zaměstnanec odpoví na otázku, na niž zná odpověď pouze on (26),
- **něco má** – tato metoda je založena na vlastnictví určitého předmětu zaměstnancem. Předmětem může být například USB token[2], karta, nebo čip. Zaměstnanec je systémem vyzván k použití předmětu (26),
- **něco je** – metoda je založena na autentizaci zaměstnance pomocí biometrických charakteristik. Takovými charakteristikami může být otisk prstu, nebo snímek duhovky. V případě rozhodnutí o využívání této metody autentizace v organizaci

[2] USB token – fyzický doplněk k autentizaci obsahující skrytou informaci v elektronické podobě

může manažer informační bezpečnosti rozhodnout o nakupování mobilních zařízení s možností biometrické autentizace. Nejčastějšími zařízeními s touto možností jsou mobilní telefony a notebooky se zabudovanou čtečkou pro otisk prstu (26).

Publikace „CyberSecurity“ od docenta Jana Koloucha uvádí, že vhodnou a bezpečnou autentizací je použití alespoň dvou ze tří výše uvedených základních druhů autentizace.

Pro výběr vhodné metody autentizace, o které by měli dle normy 27002 rozhodovat garanti jednotlivých aktiv, by jim k rozhodnutí měly pomoci následující otázky:

- Jak často bude probíhat autentizace zaměstnance?
- Kolik zaměstnanců bude danou autentizační metodu využívat?
- Na jakém místě se budou zaměstnanci nejčastěji autentizovat? Bude to doma, na pracovišti nebo na veřejném místě (27)?

1.4.6 Šifrování

Jedná se o proces, kterým se za pomocí kryptografického algoritmu převádí data nezabezpečená na data šifrovaná, která lze přečíst pouze za pomocí dešifrovacího klíče. Toto zabezpečení je vhodné v případech, kdy by se útočníkovi podařilo přistoupit k datům prolomením ostatních bezpečnostních opatření, aby byla data pro útočníka nečitelná (39). Jak uvádí publikace „Importance of Cryptography in Information Security“ z University of Firat, kryptografické prostředky jsou klíčovým nástrojem k ochraně informací (41).

Zašifrování dat se může docílit použitím specializovaných šifrovacích nástrojů. Tyto nástroje mohou být softwarové, tzn. uživatel si může zavést aplikaci, která šifruje data, jež si uživatel zvolí. Dále je možné zabezpečit data instalováním tzv. TPM čipu. TPM je malý čip, který je obvykle připájený na základovou desku zařízení, aby jeho odstranění bylo na první pohled viditelné. Čip slouží jako hardwarový základ pro šifrování zařízení. Díky šifrování paměti udržuje čip stálou „důvěryhodnou paměť“, do které má přístup pouze on sám (42).

1.4.7 Fyzické zabezpečení zařízení pomocí portů

Docent Jan Kolouch ve své publikaci „CyberSecurity“ uvádí, že je vhodné v prostorách společnosti, kde se pohybují nejen zaměstnanci, ale i třetí osoby a dodavatelé, zabezpečit mobilní zařízení pomocí zámků využívajících např. Kensington Security Slot. Jedná se o malou, kovem zesílenou zdířku, která se používá spolu s příslušným kabelem a zámkem. Zámek je celkem viditelný, a proto jeho účelem zejména odradit osoby od krádeže tohoto zařízení (39).

Dnešní velkou hrozbou je i možnost přidání malého zařízení do USB portu (KeyGrabber) zapisujícího data, která zaměstnanec předává systému prostřednictvím klávesnice a prostřednictvím bezdrátové sítě je bude útočníkovi odesílat. Docent Jan Kolouch doporučuje, aby si zaměstnanci vždy zkontrolovali, zda do jejich zařízení není připojeno jakékoliv zařízení. Dále je možné využívat zařízení zvané USB Port Lock, které mechanicky zabezpečí USB port a odemknout ho lze pouze prostřednictvím klíče (39).

1.4.8 Management logů

Důležitou součástí bezpečného provozu systémů, služeb a aplikací je zaznamenávání informací o jejich činnosti a běhu, tzv. logování. Záznamy (logy) mohou být ukládány ve formě prostého textového souboru, nebo mohou být ukládány do databázového souboru (39).

Logy slouží nejčastěji správci sítě nebo IT pracovníkovi ke zpětné analýze a rozpoznání, zda došlo k chybě, případně slouží také ke zjištění, kdy a proč k chybě došlo.

Obecný koncept managementu logů je, že na centrální nástroj jsou sbírány logy z různých ostatních nástrojů. Tyto logy je možné poté vytřídit, vybrat pouze ty, které uživatele zajímají a ty si buď virtualizovat, nebo si nastavit upozorňování při zjištění nějakého nestandardního chování. Monitorování logů může být tedy užitečné pro včasné zachycení počítačového útoku, kontrolu uživatele a z mnoha dalších důvodů (43).

1.4.9 VLAN

VLAN neboli virtuální lokální síť slouží k logickému uspořádání sítě nezávisle na fyzickém uspořádání. Lze tedy díky této možnosti rozdělit síť na několik menších sítí

uvnitř fyzicky zapojené původní sítě. Tyto sítě jsou nezávislé, nemohou spolu nijak komunikovat a jsou vytvořeny na stejných fyzických prvcích (44).

Díky tomuto rozdělení sítě je značně sníženo riziko, pokud se do jedné z těchto sítí dostane útočník. V takovém případě je pro něj nemožné se dostat do jiných částí sítě, pouze do části sítě v rámci dané VLAN (45).

1.4.10 IEEE 802.1x

Podle publikace „Mobilní IP technologie a aplikace“ od společnosti Cisco je vhodným zabezpečením sítě, před neoprávněným přístupem cizího zařízení, autentizace pomocí standardu IEEE 802.1x (46).

Jedná se o standard pro kontrolu přístupu do sítě založenou na portu. Využívá protokol EAP, v angličtině Extensible Authentication Protocol. Pokud je port, ke kterému se zařízení připojilo v neautorizovaném stavu, tak nepřijímá žádnou jinou komunikaci, než pomocí standardu 802.1x. Je mu pouze povoleno odeslat autentizační údaje na autentizační server, tzv. RADIUS server. Tento server rozhoduje o povolení nebo zamítnutí žádosti o přístup k síti. Pokud RADIUS server zašle zpět potvrzení o úspěšné autentizaci, tak se port přepne do autorizovaného stavu a zařízení může začít komunikovat v síti (47).

1.4.11 Systém prevence průniku

Jedná se o systém, který monitoruje síť a aktivity operačních systémů před škodlivou činností. Jeho hlavní funkcí je identifikace těchto škodlivých činností, zaznamenávání informací o jejich průběhu, následném blokování těchto činností a také jejich nahlašování (48). Systém IPS je zařazen přímo do síťového provozu, a tak může aktivně předcházet detekovanému nežádoucímu a nebezpečnému provozu na síti, popřípadě může dojít k jeho blokování (49).

Podle docenta Jan Koloucha je pro nejefektivnější zabezpečení sítě vhodné zkombinovat IPS systém s bezpečnostním nastavením firewallu. Výstupy získané firewallem a IPS systémem by měly sloužit jako jedny ze vstupů do systému SIEM (viz kapitola 1.4.12) (39).

1.4.12 SIEM

SIEM, anglicky Security Information and Event Management je proces řízení bezpečnostních informací a událostí. Využívaný jako samostatný systém monitoruje, ukládá a spravuje bezpečnostní události reprezentované záznamy, které jsou sesbírány z různých nástrojů nacházejících se v síti. Takovými nástroji, sloužícími jako vstup pro SIEM, může být logování, firewall nebo IPS (50).

Za pomocí analytických funkcí, které si může uživatel nastavovat, dokáže SIEM identifikovat bezpečnostní hrozby, které se mohou stát bezpečnostními incidenty. Moderní SIEM systémy mohou zobrazovat své výstupy v grafických podobách a tyto výstupy mohou být také využity pro účely forenzní analýzy[3] (50).

1.4.13 Řízení technických zranitelností

Řízení technických zranitelností je proces, kterým jsou redukována rizika vyplývající z využívání publikovaných technických zranitelností. Publikace „Systém managementu bezpečnosti informací“ od Martina Drasticha uvádí, jaký je správný postup procesu. Odborně způsobilou osobou ve společnosti musí být získávány aktuální informace o existenci technických zranitelností v provozovaných informačních systémech. Tyto informace mohou být získávány z odborných zdrojů, vydaných zranitelností od výrobce na jeho stránkách nebo z diskuzí na předmětných fórech. Informační systémy, pro které jsou získávány informace o zranitelnostech, by měly vycházet z analýzy aktiv vytvořené ve společnosti. Po získání informací musí být vyhodnoceno, jaký mohou mít dopad zjištěné zranitelnosti na bezpečnost informací ve společnosti a na základě tohoto vyhodnocení přijmout potřebná opatření pro minimalizaci dopadu. Publikace dále uvádí, že pokud jsou bezpečnostním opatřením záplaty, je nutné nejdříve vyhodnotit riziko záplaty, následně otestovat záplatu před instalací a až poté záplatu aplikovat (52).

Součástí řízení technických zranitelností je i penetrační testování. Jedná se o druh využití tzv. etického hackingu[4]. Oprávněná osoba s povolením vedení společnosti se snaží

[3] forenzní analýza – hledání právních důkazů v počítačích zařízeních a systémech

[4] etický hacking – osoba mající znalosti hackera nevyužívající je k ilegální činnosti

proniknout přes zabezpečení určitého systému. Pokusy o proniknutí vedou k nalezení chyb v zabezpečení testovaného systému (53).

1.5 Hrozby pro bezpečnost informací

1.5.1 Kybernetická kriminalita

S nárůstem a rozvojem informačních a komunikačních technologií roste i možnost zneužití těchto technologií ke kriminální činnosti. Vzhledem k rozsáhlejší možnosti využívání technologií v domácnostech a možnosti anonymizace uživatele na internetu, je páchání kybernetické kriminality rok od roku snadnější (12).

V rámci historie byl pro kyberkriminalitu významným momentem vznik počítačových sítí a především utvoření „internetu“. Od této doby se stala možnost trestné činnosti unikátní v tom, že se pachatel mohl nacházet na zcela geograficky jiných místech než jeho oběť (13).

V dnešní době může mít dopad kyberkriminality na společnost velmi významný vliv. Následky kyberkriminality nemusí pro společnost znamenat pouze finanční ztrátu, ale má také velký dopad na služby, spolehlivost a na pověst společnosti v očích veřejnosti, akcionářů, a dokonce i vlastních zaměstnanců (14).

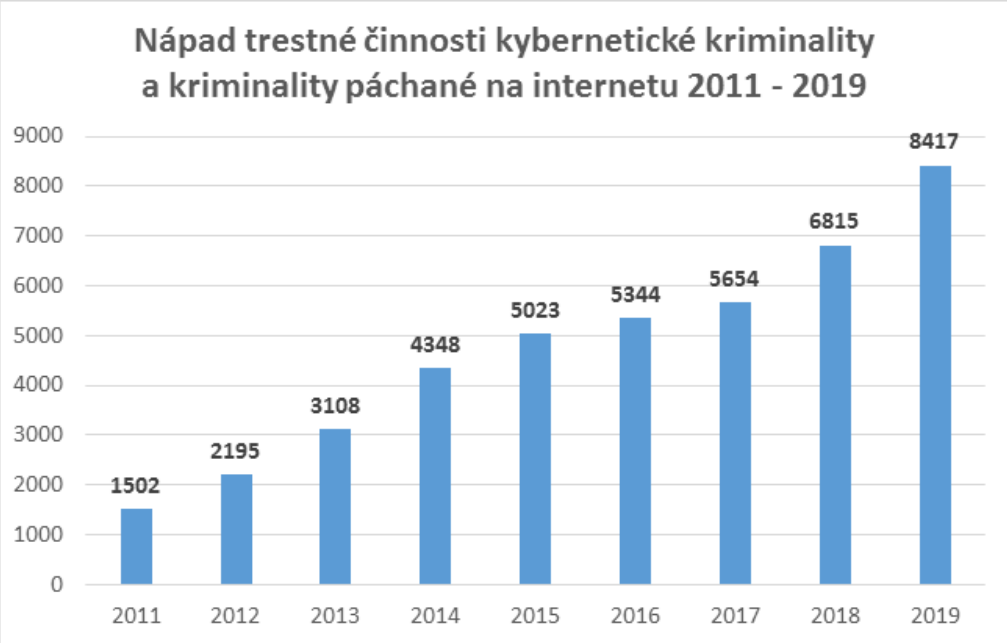
Jak uvádí zpráva z analýzy kyberkriminality společnosti Spiceworks z roku 2018, jejími nejčastějšími cíli jsou pro společnost koncová zařízení, jako jsou např. stolní počítače, notebooky nebo mobilní telefony (15).

Obrázek č. 3: Procentuální možnost ohrožení koncových zařízení podle analýzy společnosti Spiceworks (Zdroj: business.att.com) (15)

Z výše uvedené analýzy můžeme tedy určit, že zajištění bezpečnosti informací pro koncová zařízení a převážně pro mobilní zařízení, by měla být základem řízení bezpečnosti informací společnosti.

1.5.2 Kybernetická kriminalita v České republice

Od roku 2011 se sleduje vývoj a počet trestných činů spáchaných v kyberprostoru i v České republice. O sledování vývoje kriminality se v tomto případě stará Policie ČR. Dle jejích zveřejněných údajů měření bylo zjištěno markantní navýšení trestných činů v rámci kyberkriminality od roku 2011, kdy jich bylo zjištěno 1502 na počet 8417 v roce 2019 (16).



Obrázek č. 4: Počet trestných činů v rámci kyberkriminality od roku 2011 do roku 2019 (Zdroj: policie.cz) (16)

Nejpočetnější hrozbou v ČR jsou podvodná jednání, zejména pojistné podvody a dále neoprávněné přístupy k počítačovým systémům a nosičům informací (hacking) (16).

1.5.3 Vnější hrozby

Vnějšími hrozbami pro bezpečnost informací jsou takové hrozby, které jsou vedeny útočníky mimo počítačovou síť společnosti.

Sociální inženýrství

Jedním z velmi rostoucích a nejčastějších typů vnějších útoků je sociální inženýrství. Tento útok se zaměřuje na selhání lidského faktoru, tedy zaměstnanců. Cílem je klamavým dojmem docílit získání informací nebo se dostat do počítačové sítě společnosti. Útok využívá řady triků, manipulačních technik nebo obcházení zabezpečení, aby uživatele obelstil k dobrovolnému vydání chráněné informace, nebo aby uživatel udělal úkon, který útočník požaduje (17).

Nejčastějším příkladem sociálního inženýrství je tzv. phishing, kdy např. velmi důvěryhodně vypadající e-mailová zpráva upozorňuje uživatele na nějaký problém. K vyřešení tohoto problému nejčastěji stačí zadání osobních údajů o uživateli nebo zadání přístupových údajů (např. do IS společnosti nebo bankovnictví) (18).

1.5.4 Vnitřní hrozby

Vnitřní hrozby pro bezpečnost informací pochází z prostředí společnosti. Nejčastější vnitřní hrozbou je pochybení zaměstnanců. Dalšími vnitřními hrozbami může být např. povolení zařízení, které nemá společnost ve správě a nijak nerozhoduje o jejich zabezpečení, nebo porucha zařízení, která ohrozí bezpečnost informací (19).

Zaměstnanci

Lidský faktor je v současnosti nejzávažnější vnitřní hrozbou ve společnostech. Zapříčiněno je to často nedostatkem odborníků na vykonávanou pracovní činnost, nebo neznalostí bezpečnostních pravidel při jejich pracovní činnosti. Norma ISO/IEC 27005 dále uvádí, že příčinou ohrožení bezpečnosti informací ze strany zaměstnance může být jeho zvědavost, ego, finanční prospěch v případě zneužití chráněných informací nebo úmyslné poškození společnosti bývalým zaměstnancem (20).

Pro předcházení hrozbám ze strany zaměstnanců by měla společnost ustanovit organizační a technická opatření nebo pravidla, která budou po zaměstnancích vyžadována. Dále by měli být zaměstnanci dostatečně a pravidelně školeni v oblasti bezpečnosti informací na základě údajů, ke kterým mohou mít přístup.

BYOD

BYOD (anglicky Bring Your Own Device) je v současnosti narůstající trend, avšak s vysokými a četnými bezpečnostními riziky. Jedná se o povolení vydané zaměstnancům využívat pro pracovní činnost jejich vlastní výpočetní zařízení. Tato výhoda dělá společnost pro zaměstnance velmi atraktivní, umožňuje zaměstnancům vyšší mobilitu a možnost virtualizace celých uživatelských prostředí. Povolením vlastních zařízení se ale také zvyšuje riziko úniku dat ze společnosti nebo vstupu škodlivého kódu ze zařízení do firemní sítě, jelikož zařízení není ve správě společnosti a často nijak nepodléhá firemním bezpečnostním pravidlům (55).

Paměťová média

Na základě bezpečnostních instrukcí vydaných Agenturou pro kybernetickou bezpečnost a infrastrukturu (CISA) jsou velkým bezpečnostním rizikem USB zařízení připojující se do zařízení. USB zařízení může být využito pro infikování mobilního zařízení škodlivým kódem. Zaměstnanec může zařízení infikovat nevědomě, například stáhnutím malwaru[5] na USB při osobním použití a poté následným použitím USB v pracovní činnosti. V některých případech mohou zaměstnanci použít USB zařízení, která nejsou v jejich vlastnictví, pouze byla zaměstnanci nalezena a nejsou si sami vědomi jejího obsahu (51).

Bezpečnostní instrukce vydané agenturou CISA doporučují, aby zaměstnanci měli zakázáno používaní jakýchkoliv cizích USB zařízení, které jim nebyly poskytnuty organizací. Dále CISA uvádí, aby antivirové programy implementované na mobilních zařízeních vždy automaticky skenovaly USB zařízení a nepovolily jeho použití, dokud nebude skenování úspěšné (51).

1.6 Mobilní zařízení

Pro tuto práci jsou jako mobilní zařízení brána všechna výpočetní zařízení, jejichž funkčnost nevyžaduje stálou polohu na jednom místě a lze je používat i za pohybu. Většina mobilních zařízení má podobné charakteristiky, kterými jsou:

- přes zařízení je možné se připojit na internet,
- zařízení obsahuje baterii, která dokáže napájet zařízení po určitý čas,

[5] malware – program určený k poškození nebo vniknutí do počítačového systému

- má klávesy nebo dotykovou obrazovku pro vložení informací,
- jejich velikost a váha umožňuje uživateli držet zařízení pouze v jedné ruce,
- zařízení může provádět bezdrátové operace (21).

Ve společnosti mohou být mobilními zařízeními notebooky, smartphony, chytré hodinky, čtečky knih, tablety nebo PDA.

2 ANALÝZA SOUČASNÉHO STAVU

Informace uvedené v této části byly zjištěny během několika konzultací s jednatelem společnosti a s vedoucími pracovníky jednotlivých oddělení. Dále byly informace k analýze shromážděny seznámením se s běžnou pracovní činností zaměstnanců přímo na pracovišti a prohlídkou jejich pracovních prostorů.

2.1 Charakteristika společnosti

Z důvodů zajištění bezpečnosti informací společnosti bylo rozhodnuto, že společnost, která poskytla informace k vytvoření této práce, nebude jmenována. Důvodem je to, že pro tuto práci společnost zveřejnila zranitelnosti, které lze zneužít a narušit tak bezpečnost informací ve společnosti.

Níže jsou popsány základní informace o společnosti pro pochopení problematiky a posouzení stavu bezpečnosti mobilních zařízení.

2.1.1 Předmět podnikání

Zaměřením společnosti je vývoj informačních systémů v oblasti veřejné dopravy. V rámci služeb společnost nabízí servisní činnost a outsourcing služeb.

2.1.2 Základní údaje o firmě

Společnost působí po celé České republice a v sousedních státech České republiky. Sídlo společnosti a kanceláře zaměstnanců se nachází pouze na jednom pracovišti v Brně.

Společnost má dvacet jedna zaměstnanců a je rozdělena na šest oddělení. Dále v ní figurují dva projektoví manažeři a jednatel společnosti. Každé oddělení má svého vedoucího oddělení, který se organizačně zodpovídá jednateli společnosti. Oddělení ve společnosti jsou rozdělena na:

- vývojové oddělení,
- testovací oddělení,
- service desk (oddělení technické podpory pro zákazníky),
- obchodní oddělení,
- oddělení HR (oddělení pro lidské zdroje),

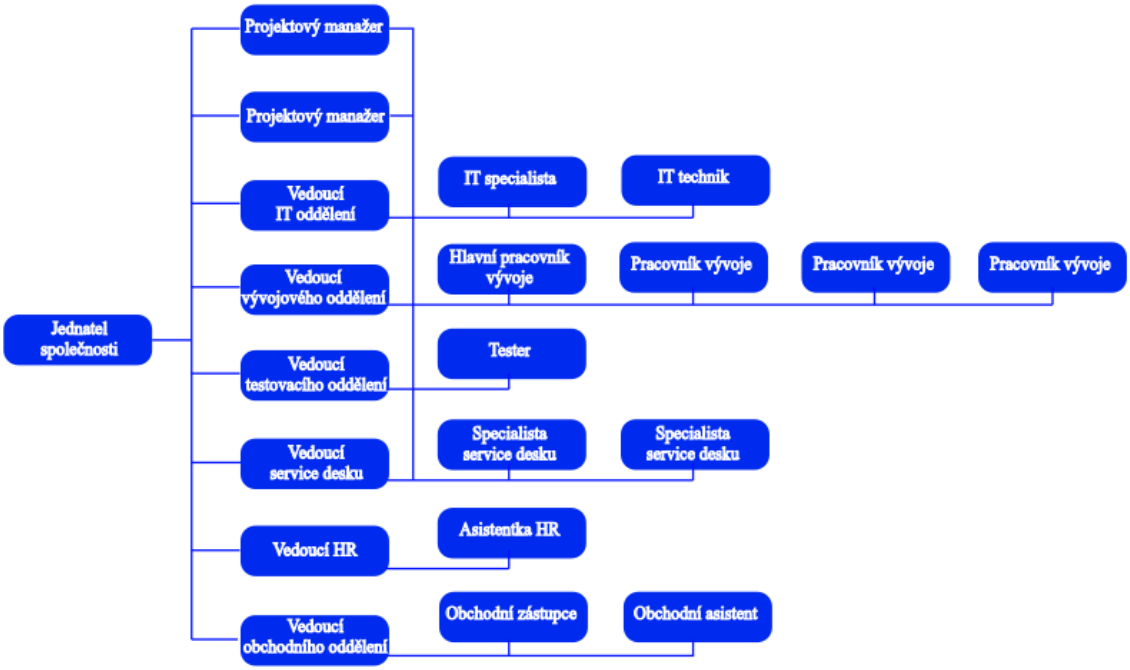
- oddělení IT (oddělení spravující ICT infrastrukturu společnosti).

V případě vytvoření projektu ve společnosti může být do projektu zapojeno více oddělení. V takovém případě vede projekt projektový manažer a zodpovídá se jednateli společnosti. Právní a účetní záležitosti společnosti jsou vedeny přes externí společnost.

Komunikace se zákazníky probíhá převážně pomocí telefonu, e-mailu a tiketovacího systému, kde mohou zákazníci online vyřizovat své zakázky a zároveň psát do společnosti i své požadavky a dotazy.

Jako garanti aktiv jsou zvoleni, při určování organizační struktury pro bezpečnost informací, vždy jednotliví vedoucí oddělení podle oddělení, k němuž se aktivum vztahuje. Funkci manažera informační bezpečnosti v rámci systému řízení bezpečnosti informací díky jeho odborným znalostem zastává jednatel společnosti.

2.1.3 Organizační schéma společnosti



Obrázek č. 5: Organizační schéma společnosti (Zdroj: vlastní tvorba)

2.2 Rozsah systému řízení bezpečnosti informací

Do rozsahu systému řízení bezpečnosti informací budou začleněna všechna aktiva společnosti, která jsou využívána pro předmět podnikání společnosti a z hlediska organizace jsou zahrnuty všechny organizační jednotky, které jsou uvedeny v organizačním schématu výše.

Vzhledem k rozsahu je možné tedy do návrhu bezpečnostních opatření pro mobilní zařízení zahrnout všechna mobilní zařízení, která jsou využívána zaměstnanci společnosti.

2.3 Řízení bezpečnostní dokumentace ve společnosti

V současnosti není ve společnosti vytvořen žádný dokument, který by obsahoval technická, nebo organizační pravidla pro bezpečnost informací. Zaměstnanci se řídí pouze několika pravidly, která však jsou předávána pouze verbálně a nejsou nikde zaznamenána.

Jedinými dokumenty pro bezpečnost informací, kterými se mohou zaměstnanci řídit, jsou manuály a dokumentace vydané dodavateli zařízení a informačních systémů, které společnost využívá.

2.4 Současný stav fyzického zabezpečení

Prostory společnosti se nachází v samostatné budově. Budova disponuje vlastním dvorem, který je po celém obvodu zabezpečený plotem. Na části tohoto dvora se nachází parkoviště. Vstup do dvora společnosti je možný pouze přes vstupní bránu. Otevření vstupní brány je řešeno aplikací v mobilních telefonech zaměstnanců, jež jim umožňuje dálkové otevření brány.

Vstup do budovy je povolen pouze po autentizaci zaměstnance přístupovým čipem. Budova je chráněna EZS[6] a EPS[7].

[6] EZS – elektronický zabezpečovací systém

[7] EPS – elektronický požární systém

Vstup do jednotlivých kanceláří v budově je zabezpečen mechanickými zámky. Klíče od jednotlivých kanceláří mají pouze zaměstnanci, kterým kancelář slouží pro výkon jejich pracovní činnosti. Jeden univerzální klíč je uložen v kanceláři jednatele společnosti.

Celý areál společnosti je snímán kamerovým systémem, jehož záznam se ukládá na server pro kamerový systém v serverovně. Do kamerového systému má jednatel společnosti možnost nahlížet ze svého firemního zařízení.

2.5 Současný stav informačních technologií využívaných ve společnosti

2.5.1 Počítačová síť

Síť společnosti je realizována kombinací místní LAN sítě a WLAN. Do sítě jsou připojeny servery, pracovní stanice umístěné v kancelářích zaměstnanců a mobilní zařízení zaměstnanců přes bezdrátovou síť.

Místní síť LAN

Propojení uzlů v LAN síti společnosti je realizováno hvězdicovou topologií. V prostorách společnosti je zavedena lokální síť typu Ethernet verze Fast Ethernet.

Datové zásuvky pro připojení do lokální sítě jsou vedeny do všech jednotlivých kanceláří. Jejich počet je vyšší, než je počet pracovních stanic, aby bylo umožněno zaměstnancům do lokální sítě připojit mobilní zařízení, nebo síťovou tiskárnu. Ve společných prostorech v budově nejsou umístěny žádné datové zásuvky, aby nebylo možné připojit se do lokální sítě třetí stranou, která by byla návštěvou v budově.

Aktivní prvky a server jsou umístěny v serverovně v přízemí budovy.

Bezdrátová síť WLAN

Připojení do bezdrátové sítě je realizováno Wi-Fi access pointy[8], které pokrývají pro připojení celou budovu. Bezdrátová síť je chráněna zabezpečením WPA2 s šifrovacím algoritmem AES.

Do bezdrátové sítě se mohou připojit všichni zaměstnanci využívající mobilní zařízení po autentizaci heslem. Pro návštěvy a jiné třetí osoby je v prostorách společnosti vytvořena

[8] access point – zařízení ke kterému se uživatel připojuje pro přístup k síti nebo internetu

sekundární Wi-Fi síť, která je oddělená od lokální sítě společnosti a slouží pouze pro přístup na internet.

Vzdálené připojení do sítě

Do firemní sítě společnosti je umožněn vzdálený přístup. Tento přístup je povolen pouze vybraným pracovníkům zejména z obchodního oddělení, jednateli společnosti a zaměstnancům s povolením výkonu práce z domova. Vzdálené připojení do sítě je zabezpečeno pomocí VPN. Pro VPN připojení je implementován virtuální VPN server. Pro využití VPN je nutné nainstalování VPN klienta na mobilní zařízení zaměstnance, který se připojuje na firemní IP adresu po autentizaci zaměstnance uživatelským jménem a heslem.

Připojení do firemní sítě společnosti přes VPN je umožněno také některým dodavatelům v rámci jejich servisní činnosti. Pro připojení jsou povinni si nainstalovat VPN klienta s nutnou autentizací, avšak do firemní sítě se připojují přes své vlastní zařízení, které není ve správě společnosti.

Firewall

Pro zabezpečení sítě je implementován hardwarový firewall s unixovým operačním systémem. Na firewallu jsou nastavena natovací a routovací pravidla a vybrané zakázané porty.

2.5.2 Hardware

Základními hardwarovými zařízení ve společnosti jsou servery, pracovní stanice a mobilní zařízení. Za celkovou správu hardwaru ve společnosti je odpovědné oddělení IT.

Servery

Pro řízení sítě jsou využívány dva fyzické servery. Jeden server využívá operační systém Windows a na druhém serveru běží operační systém Linux. První server zajišťuje provoz poštovního serveru, slouží jako DNS a DHCP server, VPN server, fileserver, aplikační a databázový server. Druhý server je využíván pro vývoj a testování pracovníky vývoje. Fileserver slouží pro uložení sdílených firemních dat, která jsou pravidelně zálohována na server, sloužící pro zálohu, každý den po 22. hodině.

Spolu s výše zmíněným serverem pro zálohu je zaveden ještě server pro kamerový systém.

Pracovní stanice

Jako pracovní stanice slouží běžné stolní počítače od výrobce HP, kterých je zhruba šest. Pro zaměstnance oddělení HR a testování jsou počítače využívány pouze pro kancelářské činnosti a jsou na nich nainstalovány operační systémy Windows 10. Pro ostatní zaměstnance jsou na počítačích nainstalovány linuxové operační systémy.

Mobilní zařízení

Zaměstnanci z oddělení vývoje, obchodu, servis desku, IT a projektoví manažeři, kteří mají povolenou práci mimo pracoviště, využívají pro práci přenosné notebooky. Dále pro práci využívá notebook jednatel společnosti.

Všechny notebooky, které zaměstnanci využívají k pracovní činnosti a přístupu k datům, jsou majetkem společnosti a jsou jim předávány při nástupu do zaměstnání. Zaměstnanci nemají povoleno přistupovat k firemním datům ze svých osobních zařízení. Jedinou výjimkou jsou čtyři notebooky vývojářů, kteří si nosí svá vlastní zařízení s preferovaným softwarem pro vývoj. Použití těchto zařízení mají vývojáři schváleno jednatelem společnosti.

Současným bezpečnostním pravidlem pro mobilní zařízení je vyžadování autentizace zaměstnance, kdy si on sám může zvolit, jaký způsob autentizace bude používat. Zaměstnanci jsou pouze upozorněni na stahování neznámých aplikací z neověřených zdrojů do mobilních zařízení, avšak toto pravidlo není nijak monitorováno a není nijak ošetřeno ve směrnici nebo politice společnosti.

Zařízení nejsou nijak centrálně spravována. Všechny aktualizace operačních systémů, aplikací a antivirového programu si zaměstnanci dělají sami, nebo požádají zaměstnance IT oddělení v případě, kdy se jim objeví upozornění na nutnost aktualizace.

Všichni zaměstnanci pracují na zařízeních (noteboocích i na pracovních stanicích) na lokálním administrátorském účtu.

V případě ztráty, nebo krádeže mobilního zařízení nemají zaměstnanci žádné písemné informace o tom, jak mají postupovat a pouze je jim předložena informace, aby o této skutečnosti informovali zaměstnance IT oddělení.

Pokud zaměstnanec svou činností naruší bezpečnost informací ve společnosti, je s ním vedeno disciplinární řízení. O průběhu a výsledku disciplinárního řízení rozhoduje manažer informační bezpečnosti.

2.5.3 Software

Operační systémy

Pro servery jsou ve společnosti využity operační systémy Windows server 2019 a SUSE Linux Enterprise Server.

Na pracovních stanicích a noteboocích jsou instalovány operační systémy Windows 10 pro kancelářskou práci a operační systémy Debian GNU/Linux pro práci související s vývojem projektů.

Všichni zaměstnanci používají firemní mobilní telefony značky Samsung s operačním systémem Android verze 9.0.

Využívaný aplikační software

Zaměstnanci s operačními systémy Windows využívají pro kancelářskou práci balík Microsoft Office 2013. Ostatní zaměstnanci s linuxovými operačními systémy využívají kancelářský balík LibreOffice. Jako poštovní klient je využívaný Microsoft Office Outlook 2013 a Mozzila Thunderbird. Pro práci s databázemi je využíván Oracle Database server.

Pro vývoj a testování nejsou stanoveny aplikace, které by byly jednotně schváleny společností. Zaměstnancům vývoje a testování je povolena instalace aplikací, které si sami zvolí jako vhodné pro pracovní činnost.

Jako informační systém využívá společnost svůj vlastní software. Tento software využívá oddělení HR pro práci s údaji o zaměstnancích a obchodní oddělení pro řízení obchodu.

Oddělení servis desk využívá jako tiketovací systém aplikaci Redmine. Zároveň je tato aplikace využívána zaměstnanci vývoje a projektovými manažery pro zaznamenávání jednotlivých kroků implementace během práce na projektu.

Antivirová ochrana

Pro antivirovou ochranu je ve společnosti využíván program McAfee, který je nainstalován na pracovních stanicích a noteboocích. Na serverech ani mobilních telefonech nejsou nainstalované antivirové programy.

Pro zabezpečení před spamy je využíváno zabudované řešení v poštovním serveru MS Exchange, který filtruje příchozí zprávy podle databáze známých spamových domén[9].

Zálohování dat

Zaměstnanci jsou poučeni o tom, že data na sdílených discích jsou každodenně zálohována. Jsou tedy odpovědni za ukládání svých dat na sdílené disky ve firemní síti, aby předcházeli jejich ztrátě.

Sdílené disky jsou každý den v pozdních hodinách zálohovány na oddělená úložiště. Záloha na těchto úložištích je k dispozici 7 dní zpětně. Dále jsou zálohovány bitové kopie serverů, data z databází a kamerové záznamy.

2.6 Analýza aktiv

Pro účely řízení systému bezpečnosti informací byla ve společnosti vytvořena analýza aktiv, jejímž výsledkem bylo sepsání aktiv společnosti do evidence a tato aktiva byla následně ohodnocena z hlediska bezpečnosti.

Analýza aktiv byla vytvořena v souladu s postupem navrhovaným normou ISO/IEC 27001. Ve společnosti byla identifikována všechna aktiva, ať už hmotná či nehmotná, která mají pro společnost hodnotu.

[9] doména – jednoznačné označení počítače nebo počítačové sítě v internetové síti

Tato aktiva byla následně rozdělena do čtyř tříd:

- hardware,
- software,
- služby,
- informace/data.

Po identifikaci byla aktiva ohodnocena. Ohodnocení proběhlo podle základních kritérií bezpečnosti informací, kterými jsou důvěrnost, dostupnost a integrita.

Jako klasifikační schéma pro ohodnocení aktiva, vzhledem k bezpečnostním atributům, sloužilo klasifikační schéma navrhované „Vyhláškou o kybernetické bezpečnosti“. Tato klasifikační schémata lze vidět níže. Na základě dopadu porušení bezpečnostního atributu je vybíráno mezi čtyřmi hodnotami „nízká“, „střední“, „vysoká“ a „kritická“. Každá z hodnot zastupuje hodnoty od 1 do 4. Aktiva byla ohodnocena individuálně pro každý bezpečnostní atribut.

Tabulka č. 1: Klasifikační schéma pro hodnocení důvěrnosti (Zdroj: Vyhláška o kybernetické bezpečnosti) (28)

Úroveň		Popis
1	**Nízká**	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy společnosti.
2	**Střední**	Aktiva nejsou veřejně přístupná a tvoří know-how společnosti, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.
3	**Vysoká**	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství, osobní údaje).
4	**Kritická**	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).

Tabulka č. 2: Klasifikační schéma pro hodnocení integrity (Zdroj: Vyhláška o kybernetické bezpečnosti) (28)

Úroveň		Popis
1	**Nízká**	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy společnosti.
2	**Střední**	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů společnosti a může se projevit méně závažnými dopady na aktiva.
3	**Vysoká**	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů společnosti s podstatnými dopady na aktiva.
4	**Kritická**	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů společnosti s přímými a velmi vážnými dopady na aktiva.

Tabulka č. 3: Klasifikační schéma pro hodnocení dostupnosti (Zdroj: Vyhláška o kybernetické bezpečnosti) (28)

Úroveň		Popis
1	**Nízká**	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
2	**Střední**	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů společnosti.
3	**Vysoká**	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů společnosti. Aktiva jsou považována jako velmi důležitá.
4	**Kritická**	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů společnosti. Aktiva jsou považována jako kritická.

Celková evidence aktiv vytvořená ve společnosti spolu s ohodnocením jednotlivých aktiv vzhledem k bezpečnostním atributům je uvedena v příloze č. 1.

2.7 Analýza rizik

Pro identifikování rizik, která by mohla představovat vysoký dopad na bezpečnost informací, byla vytvořena ve společnosti analýza rizik. Tato analýza byla vytvořena v souladu s postupem navrhovaným „Vyhláškou o kybernetické bezpečnosti“.

Jelikož není důvod zahrnovat do analýzy všechna aktiva, ale pouze ta, která jsou z pohledu bezpečnosti pro společnost nejpodstatnější, byla do analýzy rizik vybrána všechna aktiva, u kterých byl bezpečnostní atribut ohodnocen stupněm „vysoký“, nebo „kritický“.

Vybraná aktiva byla následně sloučena do skupin, aby byla analýza rizik pro společnost jednodušší. Do jedné skupiny byla zahrnuta aktiva stejných vlastností nebo aktiva, na která následně vybrané hrozby a zranitelnosti mohou mít podobný dopad.

Po seskupení aktiv byly určeny ve společnosti hrozby, které mohou poškodit aktiva a zranitelnosti, díky nimž mohou vybrané hrozby nastat. Při určování hrozeb a zranitelností v této společnosti bylo vycházeno ze seznamu hrozeb a zranitelností sestavených „Vyhláškou o kybernetické bezpečnosti“. Každá skupina aktiv, vybraná pro analýzu, byla porovnána se všemi hrozbami a byla ohodnocena pravděpodobnost, zda může pro daná aktiva nastat. Jako klasifikační schéma pro ohodnocení pravděpodobnosti hrozby bylo vybráno klasifikační schéma navrhované „Vyhláškou o kybernetické bezpečnosti“ zobrazená níže.

Tabulka č. 4: Klasifikační schéma pro hodnocení pravděpodobnosti hrozby (Zdroj: Vyhláška o kybernetické bezpečnosti) (28)

Úroveň		Popis hrozby
1	**Nízká**	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
2	**Střední**	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
3	**Vysoká**	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
4	**Kritická**	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Jelikož jednu hrozbu může způsobit více zranitelností, byly u každé skupiny aktiv přiřazeny hrozbám odpovídající zranitelnosti z předem vybraného seznamu. Tato skupina zranitelností byla následně ohodnocena podle dosavadních možností společnosti zamezit zranitelnostem.

Z důvodu délky pojmenování zranitelností bylo rozhodnuto o přiřazení zkratek jednotlivým zranitelnostem. Do výsledných analýz rizik byly poté zapsány pouze tyto zkratky. Ty byly zranitelnostem přiřazeny následovně:

- **Z1** – nedostatečná údržba informačního a komunikačního systému,
- **Z2** – zastaralost informačního a komunikačního systému,
- **Z3** – nedostatečná ochrana vnějšího perimetru,
- **Z4** – nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
- **Z5** – nedostatečná údržba informačního a komunikačního systému,
- **Z6** – nevhodné nastavení přístupových oprávnění,
- **Z7 –** nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
- **Z8** – nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
- **Z9** – nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
- **Z10** – nedostatečná ochrana aktiv,
- **Z11** – nevhodná bezpečnostní architektura,
- **Z12** – nedostatečná míra nezávislé kontroly,
- **Z13** – neschopnost včasného odhalení pochybení ze strany zaměstnanců.

Klasifikační schéma pro ohodnocení zranitelností bylo inspirováno klasifikačním schématem navrhovaným „Vyhláškou o kybernetické bezpečnosti“.

Tabulka č. 5: Klasifikační schéma pro hodnocení možnosti výskytu zranitelností (Zdroj: Vyhláška o kybernetické bezpečnosti) (28)

Úroveň		Popis zranitelností
1	**Nízká**	Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
2	**Střední**	Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena.
3	**Vysoká**	Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
4	**Kritická**	Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Pro následné určení výsledného rizika byly použity nejvyšší hodnoty ohodnocení bezpečnostních atributů jednotlivých skupin aktiv spolu s hodnotami pravděpodobnosti výskytu hrozby a hodnotami možnosti využití zranitelností. Na základě postupu uvedeném ve „Vyhlášce o kybernetické bezpečnosti“ bylo vedením společnosti rozhodnuto, že výpočet rizika bude určen následujícím matematickým vzorcem:

$$\mathbf{R = D \times H \times Z}$$

- R úroveň rizika,
- D nejvyšší ohodnocení bezpečnostního atributu aktiv ve skupině,
- H pravděpodobnost hrozby,
- Z snadnost zneužití zranitelností.

Tento postup výpočtu byl aplikován na všechny skupiny aktiv zahrnuté do analýzy rizik a výsledek byl poté zapsán do jednotlivých analýz rizik.

Analýzy rizik, které se vztahují k aktivům relevantním pro rozsah a cíl této práce, jsou vyobrazeny v příloze č. 2.

Z těchto analýz rizik byl vytvořen tzv. přehled rizik. Přehled rizik zobrazuje všech 85 rizik v hodnotách úrovně rizika od 3 do 48. Tento přehled rizik je seřazen podle úrovně rizika, tzn. jaká je pravděpodobnost, že kvůli možným zranitelnostem hrozba nastane.

Pro rizika byla vedením společnosti stanovena hranice akceptovatelnosti, určující, zda identifikované riziko může být akceptováno tak, jak je, nebo jestli je nutné zvolit adekvátní opatření pro snížení rizika. Tato hranice byla vedením společnosti stanovena na hodnotu 24 s tím, že pro všechna rizika vyšší než hodnota 24, musí být navrženo opatření pro snížení těchto rizik.

Přehled rizik s vyznačenou hranicí akceptovatelnosti je uveden v příloze č. 3. V příloze č. 4 je upravený přehled neakceptovatelných rizik, ve kterém jsou odebrána všechna rizika vztahující se k hrozbám, které nesouvisí s tématem a cílem této práce.

Pro rizika, jež jsou stanovena v příloze č. 4, je nutné navrhnout opatření, která by je snížila na vedením akceptovatelnou úroveň. Opatření sníží riziko v případě, kdy sníží pravděpodobnost vzniku hrozby, které toto riziko způsobuje, nebo pravděpodobnosti vzniku hrozby zamezí. Celkový přehled těchto hrozeb je předložen v následující tabulce:

Tabulka č. 6: Celkový přehled hrozeb způsobující rizika nad akceptovatelnou úrovní (Zdroj: vlastní tvorba)

Hrozby rizik nad akceptovatelnou úrovní
Skupina aktiv: BYOD
Cílený útok pomocí sociálního inženýrství, použití špionážních technik
Pochybení ze strany zaměstnanců
Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance
Škodlivý kód (například viry, spyware, trojské koně)
Zneužití identity
Zneužití nebo neoprávněná modifikace údajů
Zneužití vyměnitelných technických nosičů dat
Ztráta, odcizení nebo poškození aktiva
Skupina aktiv: Notebooky
Cílený útok pomocí sociálního inženýrství, použití špionážních technik

Pochybení ze strany zaměstnanců
Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance
Škodlivý kód (například viry, spyware, trojské koně)
Zneužití identity
Zneužití nebo neoprávněná modifikace údajů
Zneužití vyměnitelných technických nosičů dat
Ztráta, odcizení nebo poškození aktiva
Skupina aktiv: Síťová infrastruktura
Napadení elektronické komunikace (odposlech, modifikace)
Pochybení ze strany zaměstnanců
Škodlivý kód (například viry, spyware, trojské koně)
Zneužití identity
Zneužití nebo neoprávněná modifikace údajů
Skupina aktiv: Telefony
Cílený útok pomocí sociálního inženýrství, použití špionážních technik
Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance
Škodlivý kód (například viry, spyware, trojské koně)
Zneužití identity
Ztráta, odcizení nebo poškození aktiva
Skupina aktiv: VPN připojení
Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance
Škodlivý kód (například viry, spyware, trojské koně)
Zneužití identity
Zneužití nebo neoprávněná modifikace údajů
Ztráta, odcizení nebo poškození aktiva

2.8 Požadavky investora

Dle konzultace s jednatelem společnosti je jeho cílem zajištění bezpečnosti informací, které jsou uloženy na mobilních zařízeních a informací, ke kterým mohou mít zaměstnanci ze svých mobilních zařízení přistup.

Jednatel požaduje, aby byla navrhnuta taková bezpečnostní opatření, která by připravila společnost na certifikaci dle normy ISO/IEC 27001 a zároveň, aby zamezila opakovanému vzniku předešlých bezpečnostních incidentů, jakými byly:

- napadení mobilního zařízení a sítě malwarem z důvodu otevření přílohy v neznámém e-mailu,
- odcizení notebooku zaměstnanci na veřejně přístupném místě,
- nepovolený vstup zaměstnance, který ukončoval pracovní vztah se společností k citlivým informacím.

Další nedostatky, které by jednatel rád zlepšil výstupem této práce, je návrh dokumentací, které by zaměstnancům pomohly zvýšit bezpečnostní povědomí o vedených bezpečnostních opatřeních. Dále by dokumentace seznamovala zaměstnance s postupem ovládání využívaných bezpečnostních systémů.

2.9 Zhodnocení analýzy

Z analýzy současného stavu společnosti a z výsledků analýzy rizik lze vidět, že společnost má mobilní zařízení nedostatečně zabezpečená a několikrát u nich z tohoto důvodu nastal bezpečnostní incident. Nejzávažnějším z těchto incidentů bylo, dle vyjádření jednatele společnosti, napadení malwarem nejprve mobilního zařízení a následně celé sítě z důvodu otevření neověřené přílohy u neznámého e-mailu.

Kromě nutné autentizace do zařízení nejsou zaměstnanci nijak omezeni v používání mobilních zařízení. Nejsou na ně kladeny žádné požadavky v chování na mobilním zařízení a zároveň není stanoveno, jak si mají zaměstnanci zařízení chránit. Z těchto důvodů je vysoká pravděpodobnost, že mobilní zařízení může být napadeno nebo ho může neoprávněná osoba zneužít.

Zaměstnanci se, bohužel, snaží svou práci často zjednodušit. Pracují pod administrátorským účtem a neověřují si aplikace, které si instalují na zařízení. Hesla, která využívají pro autentizaci, často volí jednoduchá, nebo používají vlastní jména osob či krátké slovníkové výrazy.

Velkou hrozbou je, že zařízení jsou spravována samotnými zaměstnanci a tato správa není svěřena jiné odborně způsobilé osobě, jako je například pracovník IT oddělení.

Zaměstnanci také nemají vytvořeny žádné dokumenty, které by jim určovaly postup pro bezpečné používání mobilních zařízení, nebo by je informovaly o možných hrozbách.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

Z výsledků počáteční analýzy rizik a teoretických poznatků vyplývá, že pro společnost existují rizika, která jsou pro vedení společnosti neakceptovatelná a mohou mít značný dopad na bezpečnost informací. Účelem této kapitoly je navržení opatření, která by snížila míru těchto rizik. Vzhledem k rozsahu této práce, budou opatření vybrána pro rizika, která mohou znamenat dopad na bezpečnost informací ve společnosti z důvodů vniknutí škodlivého kódu do mobilního zařízení zaměstnance nebo neoprávněného přístupu cizí osoby do mobilního zařízení.

Jelikož společnost nemá v současnosti vytvořenou žádnou dokumentaci pro bezpečnost informací, je do opatření zahrnuto také vytvoření patřičných bezpečnostních směrnic.

U všech navržených opatření je určeno, kdo je za provedení opatření odpovědný, popis opatření a je stanoveno, kdo je odpovědný za kontrolu dodržování daného opatření. V případě, že opatřením je samotné vytvoření směrnice nebo školení, je popsán obsah dané směrnice či školení.

Navržená opatření jsou rozdělena na základě struktury požadavků normy ISO/IEC 27002 relevantních pro téma této práce.

3.1 Mobilní zařízení a práce na dálku

Z výsledků analýzy rizik byly zjištěny nedostatky v zabezpečení mobilních zařízení a ve vzdáleném připojení k síti přes dodavatele. Na zabezpečení mobilních zařízení nejsou kladeny žádné vyšší bezpečnostní požadavky. Vzdálené připojení do sítě společnosti je sice zabezpečeno VPN tunelem se šifrovanou komunikací, ale pokud mají do sítě povoleno přistoupit přes VPN dodavatelé, nemá společnost jakoukoliv kontrolu nad těmito zařízeními. Přes toto nezabezpečené zařízení může pak do sítě např. vniknout ransomware.

Pro zabezpečení mobilních zařízení a vzdáleného připojení navrhuji tato opatření:

1. **Zavedení a správa MDM na mobilních zařízení vlastněných společností**

   Popis opatření: Navrhuji, aby všechna mobilní zařízení, která mají přístup do sítě nebo k datům společnosti, byla spravována centrálně, a to přes MDM. Registrace mobilního zařízení do MDM musí proběhnout ještě předtím, než je předáno zaměstnanci. Uživatelé by měli mít omezenou možnost konfigurace bezpečnostního nastavení zařízení a správu zařízení bude provádět pouze správce ICT centrálně (viz kapitola 1.4.4).

   Navrhuji, aby přes MDM sytém byly řízeny minimálně tyto aspekty:

   - Technické vynucení autentizace do zařízení (viz opatření č. 11)
   - Omezení aplikací, které může zaměstnanec na zařízení používat (viz opatření č. 23)
   - Monitorování porušení bezpečnostních pravidel na mobilním zařízení (viz opatření č. 26)

   Zavede: správce ICT spolu s ostatními pracovníky IT oddělení

   Kontroluje: správce ICT

   Dokument: Směrnice pro správu MDM

   Snížené hrozby:

   Notebooky – porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance; pochybení ze strany zaměstnanců.

   Telefony – porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance.

2. **Zavedení a správa MDM na mobilních zařízení BYOD**

   Popis opatření: Pokud zaměstnanci využívají k pracovní činnosti svá mobilní zařízení, navrhuji, aby podléhala centrální správě přes MDM, stejně jako v opatření č. 1. Než jim však bude možné zavést správu přes MDM na vlastní zařízení, navrhuji, aby bylo splněno nejdříve opatření č. 3.

   Zavede: správce ICT spolu s ostatními pracovníky IT

   Kontroluje: správce ICT

   Dokument: Směrnice pro správu MDM

Snížené hrozby:

BYOD – porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance.

3. **Podepsání dohody o užívání vlastního zařízení**

   Popis opatření: Vzhledem k tomu, že v současné době není mezi společností a zaměstnancem, který využívá při práci vlastní zařízení, sepsán žádný podklad o odpovědnosti zaměstnance za toto zařízení, navrhuji podepsání dohody o užívání vlastního zařízení zaměstnancem. Dohoda bude obsahovat ustanovení, týkající se odpovědnosti zaměstnance a popis toho, jak musí být se zařízením nakládáno, pokud je využíváno k pracovní činnosti.

   Zavede: vedoucí HR

   Kontroluje: manažer informační bezpečnosti

   Dokument: Směrnice o používání vlastního zařízení

   Snížené hrozby:

   BYOD – porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance; pochybení ze strany zaměstnance.

4. **Stanovení minimálních bezpečnostních požadavků pro dodavatelská zařízení a jejich vynucování**

   Popis opatření: Navrhuji, aby byly manažerem bezpečnosti informací stanoveny minimální bezpečnostní požadavky pro mobilní zařízení dodavatele (např. instalovaný antivirový program, aktuální OS, nutná autentizace do zařízení). Tyto bezpečnostní požadavky by měly být kontrolovány vždy před připojením dodavatele do interní sítě společnosti (např. VPN serverem) (viz kapitola 1.4.9).

   Zavede: manažer informační bezpečnosti

   Kontroluje: správce ICT

   Dokument: Směrnice pro řízení vzdáleného připojení dodavatelů

   Snížené hrozby:

   VPN – porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance; škodlivý kód (například viry, spyware, trojské

koně); zneužití nebo neoprávněná modifikace údajů; ztráta, odcizení nebo poškození aktiva.

Pro tuto část dále navrhuji vytvořit následující dokumenty:

A. **Směrnice pro správu MDM**

   Obsah směrnice: Ve směrnici by měl být popsán postup registrace mobilních zařízení do MDM. Dále zde musí být popis vytvořený správcem ICT, co vše je přes MDM systém spravováno a také popis toho, jak probíhá pravidelná kontrola zařízení pomocí této správy.

   Vytvoří: správce ICT spolu s ostatními pracovníky IT oddělení

   Kontroluje: správce ICT

B. **Směrnice pro používání vlastního zařízení**

   Obsah směrnice: V této směrnici budou popsány odpovědnosti zaměstnance při používání zařízení k pracovní činnosti. Směrnice by měla rovněž popisovat postup, jakým způsobem zaměstnanec dostává oprávnění pro použití vlastního zařízení a aktuální seznam zaměstnanců, kteří toto oprávnění mají. Dále směrnice musí obsahovat popis, jakým způsobem je zaměstnanec oprávněn zařízení používat, pokud je využíváno k pracovní činnosti.

   Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

   Kontroluje: manažer informační bezpečnosti

C. **Směrnice pro řízení vzdáleného připojení dodavatelů**

   Obsah směrnice: Směrnice musí uvádět minimální bezpečnostní požadavky na zařízení dodavatelů. Dále musí popisovat, jak budou tato opatření kontrolována a stanovit postup v případě nesplnění požadavků dodavatelem.

   Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

   Kontroluje: správce ICT

3.2 Bezpečnost lidských zdrojů

Z důvodu častého rizika, zapříčiněného lidskou chybou, by měli být zaměstnanci pravidelně informováni o správných postupech ve společnosti pro zajištění bezpečnosti

a o jejich vlastní odpovědnosti. Tyto informace by zaměstnanci měli mít nepřetržitě k dispozici a měli by s nimi být opakovaně seznamováni.

V rámci bezpečnosti mobilních zařízení navrhuji tedy tato opatření:

5. **Vedení evidence předaných mobilních zařízení**

   Popis opatření: Navrhuji každému zaměstnanci, již při nástupu do zaměstnání vytvořit evidenci zařízení předaných zaměstnanci a zároveň navrhuji podepsání dohody o hmotné odpovědnosti. Pokud v průběhu zaměstnání bude zaměstnanci předáno další zařízení, navrhuji, aby se provedl zápis do stejné evidence.

   Zavede: zaměstnanec HR oddělení

   Kontroluje: vedoucí HR oddělení

   Dokument: Směrnice pro předávání a odebírání mobilního zařízení zaměstnanci

   Snížené hrozby:

   Notebooky – ztráta, odcizení nebo poškození aktiva.

   Telefony – ztráta, odcizení nebo poškození aktiva.

6. **Vedení evidence o odebraných mobilních zařízení v případě odchodu, nebo změny pozice zaměstnance**

   Popis opatření: Pokud zaměstnanec ukončí pracovní poměr nebo mění pracovní pozici, a jeho nová pracovní pozice vyžaduje použití jiných mobilních zařízení, musí být povinen společnosti vrátit doposud svěřená zařízení. Navrhuji, aby na základě evidence nebyl se zaměstnancem ukončen pracovněprávní vztah nebo nebyla umožněna změna pracovní pozice do té doby, než dojde k navrácení všech převzatých zařízení společnosti.

   Zavede: zaměstnanec HR oddělení

   Kontroluje: vedoucí HR oddělení

   Dokument: Směrnice pro předávání a odebírání mobilního zařízení zaměstnanci

   Snížené hrozby:

   Notebooky – ztráta, odcizení nebo poškození aktiva.

   Telefony – ztráta, odcizení nebo poškození aktiva.

7. **Hlášení odcizení nebo ztráty mobilního zařízení**

   Popis opatření: Všichni zaměstnanci by měli být povinni hlásit odcizení nebo ztrátu mobilního zařízení. Hlášení by mělo probíhat bezodkladně, nejlépe telefonicky správci ICT. Navrhuji také, aby bylo možné tuto skutečnost nahlásit prostřednictvím Helpdesk systému, aby byl o tomto hlášení proveden záznam. Správce ICT by měl, co nejdříve po ohlášení události, postupovat podle opatření č. 4.

   Zavede: správce ICT

   Kontroluje: správce ICT

   Dokument: Směrnice pro postup v případě ztráty nebo odcizení mobilního zařízení

   Snížené hrozby:

   BYOD – zneužití identity; ztráta, odcizení nebo poškození aktiva; zneužití nebo neoprávněná modifikace údajů.

   Notebooky – zneužití identity; ztráta, odcizení nebo poškození aktiva; zneužití nebo neoprávněná modifikace údajů.

   Telefony – zneužití identity; ztráta, odcizení nebo poškození aktiva.

8. **Vzdálená deaktivace, výmaz nebo zablokování zařízení**

   Popis opatření: Navrhuji, aby správce ICT nastavil možnost vzdálené deaktivace, výmazu nebo zablokování zařízení. Po ohlášení odcizení nebo ztráty mobilního zařízení zaměstnancem, by správce ICT měl vzdáleně zařízení deaktivovat, vymazat nebo zablokovat. O výběru úkonu by měl rozhodovat manažer informační bezpečnosti na základě klasifikace informací, ke kterým přes zařízení lze přistupovat.

   Zavede: správce ICT spolu s ostatními pracovníky IT oddělení

   Kontroluje: správce ICT

   Dokument: Směrnice pro postup v případě ztráty nebo odcizení mobilního zařízení

   Snížené hrozby:

   BYOD – zneužití identity; ztráta, odcizení nebo poškození aktiva; zneužití nebo neoprávněná modifikace údajů.

Notebooky – zneužití identity; ztráta, odcizení nebo poškození aktiva; zneužití nebo neoprávněná modifikace údajů.

Telefony – zneužití identity; ztráta, odcizení nebo poškození aktiva.

9. **Umístění bezpečnostních směrnic a manuálů na sdílené úložiště**

   Popis opatření: Aby se mohli zaměstnanci kdykoliv během pracovní činnosti informovat o správném postupu nebo bezpečnostních požadavcích společnosti, navrhuji, aby všechny bezpečnostní směrnice a manuály byly přístupné zaměstnancům na sdíleném úložišti. Na toto úložiště by měli mít zaměstnanci přístup po celou dobu pracovní doby.

   Zavede: správce ICT spolu s ostatními pracovníky IT oddělení

   Kontroluje: správce ICT

   Dokument: Směrnice bezpečného chování uživatele

   Snížené hrozby:

   BYOD – pochybení ze strany zaměstnanců.

   Notebooky – pochybení ze strany zaměstnanců.

Navrhuji vytvoření následujících směrnic:

D. **Směrnice bezpečného chování uživatelů na internetu**

   Obsah směrnice: V této směrnici bude popsáno, jak by se zaměstnanci měli chovat na sociálních sítích, aby jejich chování nemělo žádný dopad na bezpečnost společnosti. Dále navrhuji, aby bylo ve směrnici popsáno používání firemního e – mailu zaměstnance. Zaměstnancům je doporučeno, jak přistupovat k informacím zasílaným e-mailem, jakým způsobem rozpoznat phishingové útoky a jak tyto útoky nahlásit správci ICT.

   Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

   Kontroluje: správce ICT

E. **Směrnice pro předávání a odebírání mobilního zařízení zaměstnanci**

   Obsah směrnice: V této směrnici navrhuji, aby byl sepsán postup při předávání a odebírání mobilních zařízení zaměstnancům. Dále by v této směrnici mělo být uvedeno, jaké konkrétní údaje je nutné z předání či odebrání zařízení evidovat.

   Vytvoří: manažer informační bezpečnosti spolu s vedoucím HR oddělení

Kontroluje: manažer informační bezpečnosti

F. Směrnice pro postup v případě ztráty nebo odcizení zařízení

Obsah směrnice: Směrnice by měla obsahovat postup hlášení ztráty nebo odcizení mobilního zařízení zaměstnancem správci ICT. Dále navrhuji, aby bylo popsáno, podle jakých kritérií bude manažer informační bezpečnosti určovat, zda má být zařízení deaktivováno, smazáno nebo zablokováno a jakým způsobem bude správce ICT tento úkon následně vykonávat.

Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

Kontroluje: správce ICT

Pro zvýšení bezpečnostního povědomí zaměstnanců navrhuji, aby kromě vytvoření směrnic bylo realizováno pravidelné školení. Rovněž doporučuji, aby toto školení bylo povinné pro všechny zaměstnance společnosti bez výjimky a aby obsahovalo seznámení s dodržováním bezpečnosti informací ve společnosti. Navrhuji toto školení:

I. Školení o bezpečnosti informací

Obsah školení: Navrhuji, aby školení zaměstnanců obsahovalo následující body:

- seznámení zaměstnanců s organizační strukturou společnosti,
- seznámení zaměstnanců s postupem a zaváděnými kroky v rámci řízení bezpečnosti informací ve společnosti,
- seznámení zaměstnanců s přístupnou bezpečnostní dokumentací,
- seznámení zaměstnanců s disciplinárními kroky za porušení bezpečnostních pravidel,
- vysvětlení bezpečnostních incidentů zaměstnancům a jejich hlášení odpovědným osobám,
- ukázka bezpečného postupu přihlašování a vhodné struktury a správy hesla,
- postup, jak mají zaměstnanci bezpečně přistupovat vzdáleně do sítě společnosti,

- seznámení zaměstnanců se správnými postupy fyzického zabezpečení budovy a mobilních zařízení,
- seznámení zaměstnanců s postupem přístupu do IS systémů a sítě,
- seznámení zaměstnanců s bezpečným používáním internetu a e-mailu (phishingové e-maily, nezabezpečené webové stránky atd.).

Rovněž navrhuji, aby zaměstnanci tímto školením prošli vždy bezodkladně po nástupu do zaměstnání a poté, aby bylo školení opakováno pro všechny zaměstnance minimálně jedenkrát ročně.

Vytvoří: správce ICT spolu s ostatními pracovníky IT, pracovníky HR a manažerem informační bezpečnosti

Kontroluje: manažer informační bezpečnosti

Snížené hrozby:

BYOD – cílený útok pomocí sociálního inženýrství, použití špionážních technik; škodlivý kód (například viry, spyware, trojské koně); zneužití identity.

Notebooky – cílený útok pomocí sociálního inženýrství, použití špionážních technik; škodlivý kód (například viry, spyware, trojské koně); zneužití identity.

Telefony – cílený útok pomocí sociálního inženýrství, použití špionážních technik; škodlivý kód (například viry, spyware, trojské koně); zneužití identity.

VPN připojení – škodlivý kód (například viry, spyware, trojské koně); zneužití identity.

Síťová infrastruktura – škodlivý kód (například viry, spyware, trojské koně).

3.3 Řízení přístupu

Společnost nemá nijak definované bezpečnostní požadavky pro přístup k mobilním zařízením. Zaměstnanci si mohou volit sami formu autentizace a strukturu hesla.

Pro řízení přístupu navrhuji tato opatření:

10. **Stanovení politiky hesel**

    Popis opatření: Manažer informační bezpečnosti by měl ve společnosti stanovit povinnou strukturu hesla pro autentizaci do mobilního zařízení a povinné zacházení s hesly zaměstnanci. Navrhuji, aby jako vzor pro politiku hesel byla pravidla navržená „Vyhláškou o kybernetické bezpečnosti, v § 19 “ (viz kapitola 1.4.5).

    Zavede: manažer informační bezpečnosti

    Kontroluje: správce ICT

    Dokument: Směrnice pro identifikaci a autentizaci uživatelů

    Snížené hrozby:

    BYOD – zneužití identity.

    Notebooky – zneužití identity.

    Telefony – zneužití identity.

11. **Technické vynucování autentizace**

    Popis opatření: Navrhuji, aby autentizace do mobilních zařízení byla technicky vynucována a dále, aby byla technicky vynucena struktura hesla podle politiky hesel stanovené manažerem informační bezpečnosti.

    Zavede: správce ICT spolu s ostatními pracovníky IT

    Kontroluje: správce ICT

    Dokument: Směrnice pro identifikaci a autentizaci uživatelů

    Snížené hrozby:

    BYOD – zneužití identity.

    Notebooky – zneužití identity.

    Telefony – zneužití identity.

12. **Zavedení dvoufaktorové autentizace**

    Popis opatření: Pro zaměstnance, kteří přes mobilní zařízení přistupují k citlivým informacím společnosti, by měla být zavedena dvoufaktorová autentizace. Dále navrhuji, aby byla zavedena dvoufaktorová autentizace i pro administrátorské účty. Jako typy autentizací navrhuji zadání hesla a biometrický údaj. Pro možnost zadání biometrického údaje doporučuji, aby se společnost při nákupu telefonu

a notebooků zaměřila na ty, které umožňují autentizaci pomocí skenování otisku prstu (viz kapitola 1.4.5).

Zavede: správce ICT spolu s ostatními pracovníky IT

Kontroluje: správce ICT

Dokument: Směrnice pro identifikaci a autentizaci uživatelů

Snížené hrozby:

BYOD – zneužití identity.

Notebooky – zneužití identity.

Telefony – zneužití identity.

Pro řízení přístupu do mobilních zařízení navrhuji vytvořit následující dokumenty:

G. **Směrnice pro identifikaci a autentizaci uživatelů**

Obsah směrnice: Směrnice by měla stanovit, jakým způsobem jsou zaměstnancům přidělována uživatelská jména a jaká je politika hesel ve společnosti. V politice hesel by měla být stanovena struktura hesel, bezpečná manipulace s hesly, omezení zapisování hesel a také správný postup v případě zablokování účtu nesprávnými pokusy při zadávání hesla. Ve směrnici by dále měl být uveden postup pro dvoufaktorovou autentizaci.

Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

Kontroluje: správce ICT

3.4 Kryptografické prostředky

Z analýzy společnosti vyplývá, že nepoužívá šifrování mobilních zařízení, ani výměnných médií, která jsou vkládána do mobilních zařízení. V případě odcizení zařízení tak mohou být informace ze zařízení snadno získána vyjmutím paměťového média.

Navrhuji proto tato opatření:

13. **Pořizování notebooků s TMP čipem**

Popis opatření: Navrhuji, aby při zakupování nových notebooků pro zaměstnance, byly pořizovány notebooky s již zavedeným TMP čipem pro šifrování dat (viz kapitola 1.4.6).

Zavede: vedoucí obchodního oddělení

Kontroluje: manažer informační bezpečnosti

Dokument: Směrnice pro řízení kryptografických prostředků

Snížené hrozby:

Notebooky – zneužití nebo neoprávněná modifikace údajů.

14. Použití šifrovacího nástroje

Popis opatření: Pokud notebooky nedisponují TMP čipem, měly by být opatřeny systémovým nástrojem pro šifrování vnitřního úložiště (např. TrueCrypt) (viz kapitola 1.4.6).

Zavede: správce ICT

Kontroluje: správce ICT

Dokument: Směrnice pro řízení kryptografických prostředků

Snížené hrozby:

Notebooky – zneužití nebo neoprávněná modifikace údajů.

15. Nastavení hesla pro přístup do BIOS

Popis opatření: Na mobilních zařízeních by měl být správcem ICT zabezpečen přístup do BIOSu heslem. Heslo by mělo být vyžadováno vždy při zapnutí zařízení a teprve pak by měla proběhnout autentizace do OS. Útočník tak nebude moci obejít OS zařízení.

Zavede: pracovníci IT oddělení

Kontroluje: správce ICT

Dokument: Směrnice pro řízení kryptografických prostředků

Snížené hrozby:

Notebooky – zneužití nebo neoprávněná modifikace údajů.

16. Šifrování OS Android

Popis opatření: Všechny telefony zaměstnanců by měly mít správcem ICT nastaveno šifrování vnitřního úložiště.

Zavede: správce ICT

Kontroluje: správce ICT

Dokument: Směrnice pro řízení kryptografických prostředků

Snížené hrozby:

Telefony – zneužití identity.

17. **Šifrování výměnných médií**

    Popis opatření: Měla by být zašifrována všechna výměnná média, na nichž jsou ukládány citlivé údaje.

    Zavede: správce ICT

    Kontroluje: správce ICT

    Dokument: Směrnice pro řízení kryptografických prostředků

    Snížené hrozby:

    Notebooky – zneužití nebo neoprávněná modifikace údajů.

Pro řízení kryptografických prostředků navrhuji následující dokumenty:

H. **Směrnice pro řízení kryptografických prostředků**

    Obsah směrnice: Směrnice musí uvádět, jaké algoritmy jsou ve společnosti využity pro šifrování. Dále musí určit, co vše je ve společnosti šifrováno a stanovit, jaké jsou postupy pro šifrování jednotlivých zařízení či systémů.

    Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

    Kontroluje: správce ICT

3.5 Fyzická bezpečnost

Z analýzy společnosti lze vidět, že budova a jednotlivé kanceláře jsou dostatečně zabezpečeny. Budovou se však pohybují často třetí osoby, zejména dodavatelé, kteří nejsou kontrolováni a představují tedy riziko. Zaměstnanci také nejsou nijak poučeni o tom, jak fyzicky zabezpečovat mobilní zařízení, pokud je vynáší mimo prostory společnosti.

Navrhuji tato opatření:

18. **Zabezpečení zařízení mechanickým zámkem**

    Popis opatření: Zaměstnanci by měli být vybaveni mechanickým zámkem (např. Kensigton Security Slot) pro zabezpečení notebooku proti ztrátě v případě jejich nepřítomnosti (viz kapitola 1.4.7).

    Zavede: správce ICT spolu s vedoucím obchodního oddělení

    Kontroluje: správce ICT

    Dokument: Směrnice pro fyzické zabezpečení mobilních zařízení

Snížené hrozby:

Notebooky – ztráta, odcizení nebo poškození aktiva.

BYOD – ztráta, odcizení nebo poškození aktiva.

Telefony – ztráta, odcizení nebo poškození aktiva.

19. Zavedení USB port locku

Popis opatření: Pokud zaměstnanci nechají zařízení jakoukoliv dobu nechráněné, měli by vždy po příchodu zkontrolovat notebook, zda nedošlo k připojení cizích zařízení. Doporučuji, aby byly pro zaměstnance pořízeny USB port locky, kterými zaměstnanci budou povinni zabezpečovat volné USB porty (viz kapitola 1.4.7).

Zavede: správce ICT spolu se zaměstnanci obchodního oddělení

Kontroluje: správce ICT

Dokument: Směrnice pro fyzické zabezpečení mobilních zařízení

Snížené hrozby:

Notebooky – zneužití nebo neoprávněná modifikace údajů.

BYOD – zneužití nebo neoprávněná modifikace údajů.

Telefony – zneužití nebo neoprávněná modifikace údajů.

20. Zamčení neobsluhovaných zařízení

Popis opatření: Na zařízeních zaměstnanců by mělo být nastaveno automatické zamykání po určité době nečinnosti (navrhuji 5 minut). Po opětovném zapnutí zařízení musí být vynucena autentizace zaměstnance.

Zavede: správce ICT spolu s ostatními pracovníky IT

Kontroluje: správce ICT

Dokument: Směrnice pro fyzické zabezpečení mobilních zařízení

Snížené hrozby:

Notebooky – zneužití nebo neoprávněná modifikace údajů.

BYOD – zneužití nebo neoprávněná modifikace údajů.

Telefony – zneužití nebo neoprávněná modifikace údajů.

21. Zabezpečení aktivních prvků a kabeláže

Popis opatření: Aktivní prvky ve společnosti doporučuji umístit do uzamykatelných prostor nebo do uzamykatelných „racků“. Klíč od těchto prostor

by měli mít pouze pracovníci IT oddělení a manažer informační bezpečnosti. Kabeláž, navrhuji, aby byla zabezpečena v kabelových lištách nebo žlabech.

Zavede: správce ICT spolu s manažerem informační bezpečnosti

Kontroluje: správce ICT

Dokument: Směrnice pro zabezpečení aktivních prvků a kabeláže

Snížené hrozby:

Síťová infrastruktura – napadení elektronické komunikace (odposlech, modifikace); zneužití nebo neoprávněná modifikace údajů.

Pro fyzické zabezpečení navrhuji následující směrnice:

I. **Směrnice pro fyzické zabezpečení mobilních zařízení**

Obsah směrnice: Směrnice by měla obsahovat alespoň následující body:

- poučení zaměstnanců o uzamčení mobilních zařízení, pokud je nechávají v prostorách společnosti,
- poučení o tom, že zaměstnanci nemají nikdy nechávat mobilní zařízení nechráněná na veřejně přístupných místech, restauracích, autech atd.
- poučení o zabezpečení zařízení, pokud od něho zaměstnanci odcházejí (zamčení obrazovky, použití USB port locku a mechanického zámku),
- poučení, aby si každý zaměstnanec hlídal své okolí, aby neoprávněná osoba nemohla nahlížet do obrazovky zařízení, nebo odposlouchávat hovor.

Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

Kontroluje: správce ICT

J. **Směrnice pro zabezpečení aktivních prvků a kabeláže**

Obsah směrnice: Tato směrnice by měla popisovat, jak jsou ve společnosti zabezpečeny aktivní prvky a kabeláž. Dále by měla informovat o tom, kdo má povolení manipulovat s aktivními prvky a kdo k nim má povolen přístup.

Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

Kontroluje: správce ICT

3.6 Ochrana před malwarem

Z výsledků analýzy rizik vyplývá, že společnost má jako často vyskytující se hrozbu napadení škodlivým kódem (malwarem). Jediné současné opatření společnosti je základní antivirový program McAfee nainstalovaný na koncových zařízeních. Nastavení antivirového programu není však nijak pevně dáno. Proti malwaru je však nutná i jiná ochrana než pouze antivirový program.

Navrhuji pro zvýšení ochrany tato opatření:

22. **Zavedení antivirového programu na servery**

    Popis opatření: Navrhuji nainstalovat antivirový program na aplikační servery společnosti a poštovní server (viz kapitola 1.4.1).

    Zavede: správce ICT spolu s ostatními pracovníky IT oddělení

    Kontroluje: správce ICT

    Dokument: Směrnice pro nastavení antivirového programu

    Snížené hrozby:

    Síťová infrastruktura – škodlivý kód (například viry, spyware, trojské koně).

23. **Vytvoření „whitelistu" povolených webových serverů**

    Popis opatření: Manažer informační bezpečnosti by měl stanovit seznam webových serverů, které nepředstavují bezpečnostní riziko. Firewall by měl být nastaven tak, aby zaměstnanci mohli vstoupit pouze na tyto servery. Seznam musí být manažerem informační bezpečnosti pravidelně (navrhuji alespoň jednou za 6 měsíců) přezkoumán a popřípadě doplněn o nově zjištěné webové servery, které mohou představovat bezpečnostní riziko (viz kapitola 1.4.2).

    Zavede: manažer informační bezpečnosti spolu se správcem ICT

    Kontroluje: správce ICT

    Dokument: Směrnice pro ochranu před škodlivým kódem, Směrnice pro nastavení firewallu

    Snížené hrozby:

    Síťová infrastruktura – škodlivý kód (například viry, spyware, trojské koně).

    Notebooky – škodlivý kód (například viry, spyware, trojské koně).

    Telefony – škodlivý kód (například viry, spyware, trojské koně).

BYOD – škodlivý kód (například viry, spyware, trojské koně).

24. **Používání vlastních, nebo cizích výměnných paměťových médií**

    Popis opatření: Všichni zaměstnanci společnosti by měli mít zakázáno používat vlastní nebo cizí výměnná paměťová média. Ve všech zařízeních smí být použita pouze média předaná společností.

    Zavede: správce ICT

    Kontroluje: správce ICT

    Dokument: Směrnice pro ochranu před škodlivým kódem

    Snížené hrozby:

    Notebooky – škodlivý kód (například viry, spyware, trojské koně); zneužití vyměnitelných technických nosičů dat.

    BYOD – škodlivý kód (například viry, spyware, trojské koně); zneužití vyměnitelných technických nosičů dat.

25. **Omezení instalace softwaru**

    Popis opatření: Manažer informační bezpečnosti musí stanovit povolený software, který může být ve společnosti implementován. Zaměstnanci by měli mít technicky zablokovanou možnost instalace jiného softwaru, nebo by mělo být nahlášeno správci ICT, že se zaměstnanec pokouší o instalaci nepovoleného softwaru (např. SIEM systémem).

    Zavede: manažer informační bezpečnosti spolu se správcem ICT

    Kontroluje: správce ICT

    Dokument: Směrnice pro ochranu před škodlivým kódem

    Snížené hrozby:

    Notebooky – škodlivý kód (například viry, spyware, trojské koně).

    BYOD – škodlivý kód (například viry, spyware, trojské koně).

    Telefony – škodlivý kód (například viry, spyware, trojské koně).

Navrhuji vytvořit tyto směrnice:

K. **Směrnice pro nastavení antivirového programu**

    Obsah směrnice: Směrnice by měla popisovat instalaci antivirového programu a konfiguraci bezpečnostních opatření programu. Mělo by být stanoveno, kdo

spravuje program a na kterých zařízeních je implementován. Navrhuji, aby ve směrnici bylo uvedeno, co musí být skenováno antivirovým programem od přítomnosti malwaru a aby se směrnice držela následujících bodů:

- Skenování všech souborů přijatých prostřednictvím sítě a paměťových médií připojených k mobilnímu zařízení na přítomnost malwaru, před tím, než jsou použity,
- Skenování příloh přijaté elektronické pošty a stažených dat před jejich použitím na přítomnost malwaru,
- Rozpoznávání phishingových zpráv,
- Skenování webových stránek, na které je přes zařízení přistupováno na přítomnost malwaru,
- Skenování přítomnosti jakýchkoliv neschválených souborů nebo neoprávněných doplňků.

Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

Kontroluje: správce ICT

L. Směrnice pro ochranu před škodlivým kódem

Obsah směrnice: Směrnice by měla zaměstnancům ozřejmit opatření proti malwaru. Ve směrnici by měly být uvedeny nepovolené webové servery a nepovolený software.

Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

Kontroluje: správce ICT

3.7 Zaznamenávání formou logů a monitorování

Velkým rizikem pro společnost je porušování bezpečnostních pravidel zaměstnanci, nebo provádění jakýchkoliv neoprávněných činností. Společnost v současnosti nemá žádný technický nástroj, který by zaměstnance kontroloval a informoval oprávněnou osobu o neoprávněných činnostech zaměstnanců.

Navrhuji tedy tato opatření:

26. Zavedení nástroje pro monitorování a sběr záznamů

Popis opatření: Pro bezpečnost sítě a koncových zařízení navrhuji zavést technický nástroj, který by monitoroval činnosti zaměstnanců a ukládal o činnostech záznamy (logy) (viz kapitola 1.4.8). Doporučuji zaznamenávat minimálně tyto činnosti:

- Úspěšné i neúspěšné pokusy o přístup do systému, k datům nebo dalším zdrojům.
- Změny konfigurace systémů.
- Použití administrátorských práv.
- Poplachy vyvolané systémem pro řízení přístupu.
- Aktivace a deaktivace ochranných systémů (např. antivirového programu).
- Zasílání dat zaměstnanci v aplikacích.

Musí být zabezpečeno, aby správci systémů neměli oprávnění vymazat nebo deaktivovat záznamy formou logů o svých vlastních aktivitách.

Zavede: správce ICT spolu s manažerem informační bezpečnosti

Kontroluje: správce ICT

Dokument: Směrnice pro sběr logů

Snížené hrozby:

Síťová infrastruktura – pochybení ze strany zaměstnance; zneužití nebo neoprávněná modifikace údajů.

27. Napojení zaznamenávání formou logů na SIEM systém

Popis opatření: Navrhuji, aby výstupy ze zaznamenávání formou logů byly spojeny se SIEM systémem a sloužily jako jeden ze vstupů do systému. Spojení logů a SIEM systému pomůže lepší kontrole sítě vyhodnocováním bezpečnostních událostí (viz kapitola 1.4.8).

Zavede: správce ICT spolu s ostatními pracovníky IT oddělení

Kontroluje: správce ICT

Dokument: Směrnice pro sběr logů

Snížené hrozby:

Síťová infrastruktura – pochybení ze strany zaměstnance; zneužití nebo neoprávněná modifikace údajů.

28. **Synchronizování systémového času**

    Popis opatření: Pro správné vyhodnocení záznamů formou logů musí být synchronizován čas na všech serverech a systémech. Pro synchronizaci času doporučuji použít protokol NTP.

    Zavede: správce ICT spolu s ostatními pracovníky IT oddělení

    Kontroluje: správce ICT

    Dokument: Směrnice pro sběr logů

    Snížené hrozby:

    Síťová infrastruktura – zneužití nebo neoprávněná modifikace údajů.

Pro zaznamenávání formou logů navrhuji vytvoření následující směrnice:

M. **Směrnice pro sběr logů**

    Obsah směrnice: Směrnice by měla popisovat ovládání nástroje pro sběr logů správcem ICT. Dále by směrnice měla popisovat, jaké záznamy jsou ukládány, v jaké formě a na jaké místo. Musí být také popsáno propojení nástroje pro sběr logů a SIEM systému.

    Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

    Kontroluje: správce ICT

3.8 Správa a řízení technických zranitelností

Pro snížení rizika napadení škodlivým kódem, které vyšlo v analýze rizik, navrhuji, aby ve společnosti byly řízeny technické zranitelnosti. Proto navrhuji následující opatření:

29. **Řízení technických zranitelností**

    Popis opatření: Navrhuji, aby správce ICT sestavil pro všechny informační systémy, využívané ve společnosti, seznam zdrojů informací o zranitelnostech těchto systémů (např. bulletiny výrobců, specializovaná fóra, databáze zranitelností atd.). Tyto zdroje by měl správce ICT minimálně jednou za šest

měsíců kontrolovat od možných zranitelností, které mohou ohrožovat informační systémy ve společnosti (viz kapitola 1.4.13).

Zavede: správce ICT spolu s manažerem informační bezpečnosti

Kontroluje: správce ICT

Dokument: Směrnice pro řízení technických zranitelností

Snížené hrozby:

BYOD – škodlivý kód (například viry, spyware, trojské koně).

Notebooky – škodlivý kód (například viry, spyware, trojské koně).

Telefony – škodlivý kód (například viry, spyware, trojské koně).

Síťová infrastruktura – škodlivý kód (například viry, spyware, trojské koně).

30. **Penetrační testování**

Popis opatření: Musí proběhnout penetrační testování klíčových systémů společnosti. Posouzení, zda jsou systémy klíčové, navrhuji, aby se určilo na základě ohodnocení systémů podle bezpečnostních atributů v evidenci aktiv. Zjištěné zranitelnosti z penetračních testů musí řešit co nejdříve správce ICT spolu s manažerem informační bezpečnosti. Penetrační testování musí být provedeno poté bezprostředně vždy, když dojde k instalaci nového klíčového systému (viz kapitola 1.4.13).

Zavede: správce ICT spolu s ostatními pracovníky IT oddělení

Kontroluje: správce ICT

Dokument: Směrnice pro řízení technických zranitelností

Snížené hrozby:

BYOD – škodlivý kód (například viry, spyware, trojské koně).

Notebooky – škodlivý kód (například viry, spyware, trojské koně).

Telefony – škodlivý kód (například viry, spyware, trojské koně).

Síťová infrastruktura – škodlivý kód (například viry, spyware, trojské koně).

Pro řízení technických zranitelností navrhuji vytvoření následující směrnice:

N. **Směrnice pro řízení technických zranitelností**

Obsah směrnice: Směrnice by měla obsahovat popis, jak jsou ve společnosti řízeny technické zranitelnosti. To zahrnuje uvedení seznamu zdrojů informací o zranitelnostech, dále popis, jak správce ICT se zranitelnostmi nakládá a jak

často výskyt zranitelností správce vyhledává. Dále by směrnice měla popisovat průběh penetračního testování, výčet systémů, které jsou testovány a řešení zranitelností zjištěných testováním.

Vytvoří: správce ICT spolu s manažerem informační bezpečnosti

Kontroluje: správce ICT

3.9 Správa bezpečnosti sítě

Jelikož mobilní zařízení nemusí být napadena škodlivým kódem pouze přímo, nebo se útočník nemusí vždy pokoušet neoprávněně vniknout do zařízení a být fyzicky u něj, k napadení zařízení může dojít i přes počítačovou síť. Z tohoto důvodu je nutné zabezpečit interní síť společnosti, ke které se mobilní zařízení zaměstnanců pravidelně připojují a vykonávají pomocí ní svou pracovní činnost.

Z analýzy současného stavu společnosti a z výsledků analýzy rizik lze vidět, že ve společnosti nejsou použita žádná bezpečnostní opatření pro zabezpečení sítě, kromě vzdáleného přístupu přes VPN. Společnost tak nemá žádné prostředky proti hrozbě napadnutí sítě a také nemůže nijak v síti zjistit jakoukoliv neoprávněnou činnost vykonávanou zaměstnancem.

Pro zabezpečení interní sítě proto navrhuji tato opatření:

31. Rozdělení sítě na virtuální LAN

Popis opatření: Interní síť společnosti by měla být rozdělena na několik virtuálních LAN sítí. Navrhuji rozdělit síť podle pracovního zařazení zaměstnanců (oddělení), aby měli umožněn přístup pouze k datům a službám, které souvisí s jejich pracovní činností. Měla by být vytvořena také virtuální LAN pouze pro přístup k internetu pro třetí osoby, které nejsou zaměstnanci společnosti (viz kapitola 1.4.9).

Zavede: správce ICT

Kontroluje: správce ICT

Dokument: Směrnice pro řízení technických zranitelností

Snížené hrozby:

Síťová infrastruktura – škodlivý kód (například viry, spyware, trojské koně); napadení elektronické komunikace (odposlech, modifikace); pochybení ze strany zaměstnanců.

32. Ověřování zařízení přistupujícího do sítě

Popis opatření: Navrhuji, aby autentizace zařízení do sítě byla ověřena protokolem IEEE 802.1x. Pro autentizaci musí být zaveden RADIUS server, který bude autentizaci zařízení prověřovat. V případě, že zařízení nebude RADIUS serverem ověřeno, musí být vpuštěno pouze do oddělené virtuální LAN sítě, ve které nemá zařízení přístup k datům ani službám (viz kapitola 1.4.10).

Zavede: správce ICT spolu s ostatními pracovníky IT oddělení

Kontroluje: správce ICT

Dokument: Směrnice pro řízení technických zranitelností

Snížené hrozby:

Síťová infrastruktura – zneužití identity; napadení elektronické komunikace (odposlech, modifikace).

33. Nastavení firewallu jako proxy brána

Popis opatření: Pro zabezpečení příchozí a odchozí komunikace, navrhuji, aby byl firewall nastaven jako proxy brána (viz kapitola 1.4.2).

Zavede: správce ICT

Kontroluje: správce ICT

Dokument: Směrnice pro řízení technických zranitelností

Snížené hrozby:

Síťová infrastruktura – škodlivý kód (například viry, spyware, trojské koně); napadení elektronické komunikace (odposlech, modifikace).

34. Zavedení IPS sondy

Popis opatření: Pro monitorování sítě proti vzniklým anomáliím nebo škodlivé činnosti uživatele, by měl být zaveden systém prevence průniku (IPS). Výstupy z IPS by měly sloužit jako jeden ze vstupů do systému SIEM (viz kapitola 1.4.11).

Zavede: správce ICT spolu s ostatními pracovníky IT a manažerem informační bezpečnosti

Kontroluje: správce ICT

Dokument: Směrnice pro řízení technických zranitelností

Snížené hrozby:

Síťová infrastruktura – škodlivý kód (například viry, spyware, trojské koně); napadení elektronické komunikace (odposlech, modifikace); pochybení ze strany zaměstnanců.

35. **Zavedení SIEM systému**

    Popis opatření: Pro monitorování bezpečnostních incidentů v síti a možnosti předcházení, nebo snížení dopadu těchto incidentů, navrhuji, zavedení systému SIEM. Do systému by měly vstupovat výstupy minimálně z firewallu, logování, antivirového programu a IPS. Upozornění o zjištění bezpečnostního incidentu nebo o jakémkoliv podezření na bezpečnostní incident by mělo být okamžitě zasláno správci ICT. Nehledě na informování o výstupech ze systému SIEM by měl správce ICT sám pravidelně kontrolovat výstupy systému (navrhuji alespoň jedenkrát týdně) (viz kapitola 1.4.12).

    Zavede: správce ICT spolu s manažerem informační bezpečnosti

    Kontroluje: správce ICT

    Dokument: Směrnice pro řízení technických zranitelností

    Snížené hrozby:

    Síťová infrastruktura – škodlivý kód (například viry, spyware, trojské koně); napadení elektronické komunikace (odposlech, modifikace); pochybení ze strany zaměstnanců.

Pro správu bezpečnosti sítě navrhuji vytvoření následujících směrnic:

O. **Směrnice pro bezpečné řízení provozu a komunikační sítě**

    Obsah směrnice: Směrnice bude popisovat rozdělení sítě, to zahrnuje popis jednotlivých segmentů a popis virtuálních LAN sítí. Dále bude směrnice určovat, jak probíhá autentizace zařízení do sítě a z jakých aktivních prvků se síť skládá. Přílohou směrnice by mělo být znázornění rozložení sítě pomocí schématu.

Vytvoří: správce ICT spolu s ostatními pracovníky IT

Kontroluje: manažer informační bezpečnosti

P. Směrnice pro řízení záznamů formou logů

Obsah směrnice: Ve směrnici bude uvedeno, jaké záznamy formou logů jsou ukládány, co vše záznamy obsahují za informace a kam se záznamy ukládají.

Vytvoří: správce ICT spolu s ostatními pracovníky IT

Kontroluje: manažer informační bezpečnosti

Q. Směrnice pro bezpečnostní nastavení firewallu

Obsah směrnice: Směrnice by měla popisovat nutné nastavení bezpečnostních opatření ve firewallu. Součástí směrnice by měl být manuál pro pracovníky IT, jak krok po kroku opatření nastavit a popis funkčnosti firewallu jako proxy server.

Vytvoří: správce ICT spolu s ostatními pracovníky IT

Kontroluje: manažer informační bezpečnosti

R. Směrnice pro řízení systému pro detekci průniku

Obsah směrnice: Navrhuji, aby směrnice popisovala, co je vše systémem v síti monitorováno. Zároveň by zde mělo být stanoveno jaké kroky činí systém v případě výskytu incidentu. Dále by mělo být určeno, kam jsou zasílány výstupy ze systému a jak lze pracovníkem IT systém nastavit.

Vytvoří: správce ICT spolu s ostatními pracovníky IT

Kontroluje: manažer informační bezpečnosti

S. Směrnice pro řízení systému SIEM

Obsah směrnice: Ve směrnici by mělo být uvedeno, jaké jsou všechny vstupy pro systém SIEM a jak systém se vstupy nakládá (učiněná opatření, reporty atd.). Součástí směrnice by měl být i popis informování správce ICT systémem.

Vytvoří: správce ICT spolu s ostatními pracovníky IT

Kontroluje: manažer informační bezpečnosti

T. **Provozní deník**

Obsah směrnice: Pro zpětný přehled vykonaných činností během správy sítě, navrhuji, aby správce ICT vedl provozní deník. Do provozního deníku by měl zapisovat všechny klíčové činnosti, které souvisí se správou sítě společnosti. Takovými činnostmi mohou být například: změna přístupových údajů zaměstnance, konfigurace firewallu, výměna aktivního prvku atd.

Vytvoří: správce ICT

Kontroluje: manažer informační bezpečnosti

3.10 Vyhodnocení bezpečnostních opatření

Po odsouhlasení bezpečnostních opatření jednatelem společnosti bylo 35 výše uvedených bezpečnostních opatření ve společnosti aplikováno a bylo vytvořeno 20 navržených bezpečnostních dokumentů. Po aplikování bezpečnostních opatření a vytvoření směrnic byla ve spolupráci s vedením společnosti přezkoumána vytvořená analýza rizik a byly určeny nové hodnoty pro ohodnocení hrozeb a zranitelností.

Po určení nových hodnot, byly vypočteny aktualizované hodnoty rizik. Jak lze vidět z níže uvedené tabulky, po přezkoumání všech rizik, která před navrženými bezpečnostními opatřeními byla pro společnost neakceptovatelná, se po jejich zavedení snížila na akceptovatelnou úroveň. Tato hranice akceptovatelnosti pro společnost byla stanovena jednatelem společnosti.

Tabulka č. 7: Přehled rizik relevantních pro téma práce po přezkoumání (Zdroj: vlastní tvorba)

Přehled rizik relevantních pro téma práce po přezkoumání						
Riziko						
ID rizika	Název analýzy	Hrozba	Zranitelnosti	Pravděpodobnost hrozby	Snadnost zneužití zranitelnosti	Riziko
1	Skupina aktiv: Síťová infrastruktura	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	2	2	16
2	Skupina aktiv: Notebooky	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	3	2	18
3	Skupina aktiv: Notebooky	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	4	1	12
4	Skupina aktiv: Telefony	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z9, Z13	2	2	12
5	Skupina aktiv: BYOD	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	2	3	18
6	Skupina aktiv: BYOD	Zneužití identity	Z2, Z4, Z8, Z9, Z13	3	2	18
7	Skupina aktiv: Síťová infrastruktura	Zneužití identity	Z4, Z7, Z8, Z9, Z13	3	3	36
8	Skupina aktiv: Síťová infrastruktura	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12	3	3	36
9	Skupina aktiv: Síťová infrastruktura	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	3	3	36
11	Skupina aktiv: Síťová infrastruktura	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z7, Z10	3	3	36
12	Skupina aktiv: Notebooky	Zneužití identity	Z2, Z4, Z8, Z9, Z13	2	2	12
14	Skupina aktiv: Notebooky	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	3	2	18
15	Skupina aktiv: Notebooky	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	2	1	6
16	Skupina aktiv: Notebooky	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z8, Z9, Z10	2	2	12
17	Skupina aktiv: Notebooky	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	3	2	18
18	Skupina aktiv: Notebooky	Zneužití vyměnitelných technických nosičů dat	Z4, Z8, Z12, Z13	2	1	6
19	Skupina aktiv: Telefony	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	2	2	12
20	Skupina aktiv: Telefony	Zneužití identity	Z4, Z6, Z7, Z8, Z9, Z13	2	2	12
21	Skupina aktiv: Telefony	Škodlivý kód (například viry, spyware, trojské koně)	Z2, Z4, Z7, Z8, Z12, Z13	3	2	18
22	Skupina aktiv: Telefony	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	3	1	9
24	Skupina aktiv: BYOD	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	2	2	12
25	Skupina aktiv: BYOD	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	2	2	12
26	Skupina aktiv: BYOD	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z8, Z9, Z10	3	2	18
28	Skupina aktiv: BYOD	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	2	2	12
30	Skupina aktiv: BYOD	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	3	1	9
31	Skupina aktiv: BYOD	Zneužití vyměnitelných technických nosičů dat	Z4, Z8, Z12, Z13	2	2	12
32	Skupina aktiv: VPN připojení	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z11, Z12, Z13	3	2	18
33	Skupina aktiv: VPN připojení	Zneužití identity	Z2, Z4, Z6, Z7, Z9, Z13	2	2	12
34	Skupina aktiv: VPN připojení	Škodlivý kód (například viry, spyware, trojské koně)	Z1, Z2, Z4, Z7, Z8, Z11, Z12, Z13	3	2	18
35	Skupina aktiv: VPN připojení	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	2	2	12
36	Skupina aktiv: VPN připojení	Ztráta, odcizení nebo poškození aktiva	Z3, Z9, Z10, Z13	2	2	12
39	Skupina aktiv: Notebooky	Narušení fyzické bezpečnosti	Z3, Z9, Z10	2	2	12
40	Skupina aktiv: Notebooky	Zneužití vnitřních prostředků, sabotáž	Z7, Z8, Z12	2	1	6
41	Skupina aktiv: Notebooky	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z7, Z10	2	1	6
43	Skupina aktiv: Telefony	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	2	2	12
44	Skupina aktiv: Telefony	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z4, Z5, Z7, Z10	2	1	6
45	Skupina aktiv: BYOD	Narušení fyzické bezpečnosti	Z3, Z9, Z10	2	2	12
46	Skupina aktiv: BYOD	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z7, Z10	2	2	12
47	Skupina aktiv: VPN připojení	Zneužití vyměnitelných technických nosičů dat	Z4, Z12, Z8, Z13	2	3	18
48	Skupina aktiv: VPN připojení	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z6, Z7, Z10	2	2	12
49	Skupina aktiv: Síťová infrastruktura	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z11, Z12, Z13	2	2	16
51	Skupina aktiv: Síťová infrastruktura	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	2	1	8
55	Skupina aktiv: Telefony	Narušení fyzické bezpečnosti	Z3, Z9, Z10	2	2	12
56	Skupina aktiv: Telefony	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z9, Z12	2	2	12
57	Skupina aktiv: Telefony	Zneužití vnitřních prostředků, sabotáž	Z7, Z8, Z12	2	2	12
62	Skupina aktiv: VPN připojení	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	2	2	12
65	Skupina aktiv: VPN připojení	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	2	2	12
67	Skupina aktiv: Síťová infrastruktura	Narušení fyzické bezpečnosti	Z3, Z9	1	2	8
68	Skupina aktiv: Síťová infrastruktura	Ztráta, odcizení nebo poškození aktiva	Z3, Z8, Z9, Z12, Z13	1	2	8
69	Skupina aktiv: Síťová infrastruktura	Zneužití vnitřních prostředků, sabotáž	Z7, Z8, Z12	1	2	8
75	Skupina aktiv: Telefony	Zneužití vyměnitelných technických nosičů dat	Z4, Z12	1	2	6
78	Skupina aktiv: VPN připojení	Narušení fyzické bezpečnosti	Z3, Z9	1	2	6
82	Skupina aktiv: Síťová infrastruktura	Zneužití vyměnitelných technických nosičů dat	Z4, Z12, Z8, Z13	1	1	4

ZÁVĚR

Práce byla zaměřena na existující společnost XY s.r.o., která požadovala, aby nebyla jmenována z důvodu odhalení rizik společnosti spojených s používáním mobilních zařízení. Jedná se však o českou společnost s 21 zaměstnanci, která se zaměřuje na vývoj informačních systémů ve veřejné dopravě.

Bakalářská práce byla psána v průběhu přípravy společnosti na certifikaci podle normy ISO/IEC 27001. Požadavkem jednatele společnosti bylo zabezpečení informací v interní síti společnosti, ke kterým může zaměstnanec přes mobilní zařízení přistupovat a zabezpečení informací uložených na těchto zařízeních. Pro splnění požadavku jsme se s jednatelem dohodli na vytvoření návrhu bezpečnostních opatření, návrhu bezpečnostních směrnic a vytvoření struktury potřebného školení.

K zajištění podkladů pro navrhnutí opatření mi bylo umožněno být přítomen u pracovní činnosti zaměstnanců, projít si prostory společnosti a konzultovat současný stav bezpečnosti informací přímo se zaměstnanci. Dále byla ve spolupráci s vedením vytvořena analýza rizik, díky které došlo ke zjištění, na jaké hrozby je nutné se zaměřit a nalézt k nim požadovaná bezpečnostní opatření.

K naplnění cílů této práce a navrhnutí potřebných bezpečnostních opatření byly využity odborné publikace, Zákon o kybernetické bezpečnosti, Vyhláška o kybernetické bezpečnosti, normy z rodiny ISO/IEC 27000 a informace shromážděné z analýzy společnosti.

U tvoření návrhu bezpečnostních opatření jsem vycházel z postupu a doporučení normy ISO/IEC 27002, aby byla společnost v rámci zabezpečení mobilních zařízení co nejlépe připravena na certifikaci. Dále jsem vycházel ze svých praktických zkušeností a navrhnul opatření tak, aby byla pro společnost co nejvíce ekonomicky výhodná a zároveň, aby se jim zaměstnanci mohli snadno přizpůsobit.

Všechna navrhnutá bezpečnostní opatření byla projednána s jednatelem společnosti. Jednatel všechna opatření odsouhlasil a poskytl dostačující finanční prostředky odpovědným pracovníkům k zavedení navrhnutých opatření. Po úspěšné implementaci

bezpečnostních opatření byla spolu s jednatelem přezkoumána analýza rizik a byly vypočteny nové hodnoty rizik. Aplikováním opatření se podařilo všechna dříve neakceptovatelná rizika snížit na jednatelem akceptovatelnou úroveň.

Dovoluji si tedy tvrdit, že společnost je připravena na certifikaci podle normy ISO/IEC 27001 v rámci zabezpečení mobilních zařízení. Realizace navrhnutých opatření je počátečním krokem k úspěšnému řízení bezpečnosti informací ve společnosti. Jsem však názoru, že pro dlouhodobější úspěšné řízení bezpečnosti informací je nutné dohlížet na dodržování navrhnutých opatření a na dodržování navrhnutých směrnic. Dále je žádoucí, aby společnost pravidelně přezkoumávala možné hrozby, které mohou představovat riziko pro bezpečnost informací a aby na tyto hrozby byla následně navržena další bezpečnostní opatření.

SEZNAM POUŽITÝCH ZDROJŮ

[1] NOVÁK, Luděk a Josef POŽÁR. Systém řízení informační bezpečnosti. In: *CyberSecurity* [online]. s. 10 [cit. 2020-01-27]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf

[2] GOGELA, Robert. Standardy a definice pojmů bezpečnosti informací. In: *CyberSecurity* [online]. s. 5 [cit. 2020-01-27]. Dostupné z: https://www.cybersecurity.cz/data/Gogela.pdf

[3] Bezpečnostní politika (Security policy). In: *ManagementMania.com* [online]. Wilmington (DE) 2011-2020, 20.06.2018 [cit. 27.01.2020]. Dostupné z: https://managementmania.com/cs/bezpecnostni-politika-security-policy

[4] SEDLÁČEK, Miroslav. Demingův cyklus PDCA: a norma ISO/IEC 20000-1:2011. *IT Systems* [online]. 2011, **2011**(12) [cit. 2020-01-27]. Dostupné z: https://www.systemonline.cz/sprava-it/deminguv-cyklus-pdca.htm

[5] Zavedení systému řízení bezpečnosti – ISMS - 1.díl. *Chrantesidata.cz* [online]. [cit. 2020-01-27]. Dostupné z: http://www.chrantesidata.cz/cs/art/472-isms-serial-o-rizeni-bezpecnosti

[6] ISO 27000. In: *ManagementMania.com* [online]. Wilmington (DE) 2011-2020, 23.03.2017 [cit. 27.01.2020]. Dostupné z: https://managementmania.com/cs/iso-27000

[7] ISO 27002 - nejlepší bezpečnostní praktiky. In: ManagementMania.com [online]. Wilmington (DE) 2011-2020, 24.03.2017 [cit. 27.01.2020]. Dostupné z: https://managementmania.com/cs/iso-27002-nejlepsi-bezpecnostni-praktiky

[8] Bezpečnostní role a jejich začlenění v organizaci. In: *Govcert.cz* [online]. 29.1.2019, s. 11 [cit. 2020-01-27]. Dostupné z: https://www.govcert.cz/download/kii-vis/VKB/bezpe%C4%8Dnostn%C3%AD-role_v1.1.pdf

[9] Firewall. *Eset.com* [online]. [cit. 2020-01-27]. Dostupné z: https://www.eset.com/cz/firewall/

[10] Mobile Device Management či Enterprise Mobility Management? *System4u* [online]. 26.9.2019 [cit. 2020-05-04]. Dostupné z: https://www.system4u.cz/mdm-ci-emm/

[11] VAJNER, Radek. Mobile device management: aneb Jak zvládnout rostoucí počet mobilních zařízení v podniku. *IT Systems* [online]. 2012(2) [cit. 2020-05-04]. Dostupné z: https://www.systemonline.cz/sprava-it/mobile-device-management.htm?mobilelayout=false
[12] Kyberkriminalita. *Prevencekriminality.cz* [online]. [cit. 2020-01-27]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/
[13] SMEJKAL, Vladimír. Kybernetická kriminalita – fenomén dneška. *Pravniprostor.cz* [online]. 20.07.2015 [cit. 2020-01-27]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska
[14] CRANE, Casey. 33 Alarming Cybercrime Statistics You Should Know in 2019. *Thesslstore.com* [online]. 14.11.2019 [cit. 2020-01-27]. Dostupné z: https://www.thesslstore.com/blog/33-alarming-cybercrime-statistics-you-should-know/
[15] SHIELDS down. *Business.att.com* [online]. [cit. 2020-01-27]. Dostupné z: https://www.business.att.com/learn/cybersecurity-report-volume-8-5.html#
[16] Kyberkriminalita. *Policie.cz* [online]. [cit. 2020-01-27]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx
[17] Sociální inženýrství (sociotechniky). In: ManagementMania.com [online]. Wilmington (DE) 2011-2020, 23.10.2017 [cit. 27.01.2020]. Dostupné z: https://managementmania.com/cs/socialni-inzenyrstvi
[18] SOCIÁLNÍ INŽENÝRSTVÍ. *Govert.cz* [online]. [cit. 2020-01-27]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/
[19] BROŽ, Vladimír. Bezpečnost a vnitřní hrozby: Nejen vnější hrozby ohrožují v současné době naše počítače. *Computerworld.cz* [online]. [cit. 2020-01-27]. Dostupné z: https://computerworld.cz/securityworld/bezpecnost-a-vnitrni-hrozby-46307
[20] *ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací.*
[21] VISWANATHAN, Priya. What Is a Mobile Device?: Smartphones, tablets and e-readers are all mobile devices. *Lifewire.com* [online]. 23.10.2019 [cit. 2020-01-27]. Dostupné z: https://www.lifewire.com/what-is-a-mobile-device-2373355
[22] Zákon č. 262/2006 Sb., Zákon zákoník práce ze dne 1.července 2007.

[23] ČSN EN ISO/IEC 27002: Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. 2014.
[24] Jak trvale smazat data. *DISKUS* [online]. [cit. 2020-05-05]. Dostupné z: https://www.diskus.cz/clanek/jak-trvale-smazat-data
[25] ANDRAŠČÍK, Jan. *Bezpečnost při využívání osobních mobilních zařízení* [online]. In:. s. 5 [cit. 2020-05-05]. Dostupné z: https://www.interniaudit.cz/download/diskuze/pdfclanky/diskuse.16-andrascik-jan.pdf
[26] ČERMÁK, Miroslav. Autentizace. *Clever and smart* [online]. 2012 [cit. 2020-05-05]. Dostupné z: https://www.cleverandsmart.cz/autentizace/
[27] ČERMÁK, Miroslav. Autentizace: Jak vybrat vhodnou autentizační metodu? *Clever and smart* [online]. 2010 [cit. 2020-05-05]. Dostupné z: https://www.cleverandsmart.cz/autentizace-jak-vybrat-vhodnou-autentizacni-metodu/
[28] Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) ze dne 28. května 2018.
[29] HUJER, Martin. *Šifrování dat v notebooku je nutnost!* [online]. 2013 [cit. 2020-05-05]. Dostupné z: https://blog.martinhujer.cz/sifrovani-dat-v-notebooku-je-nutnost/
[30] VÁCLAVÍK, Lukáš. Android 6.0 už musí mít povinně šifrované úložiště. Na rychlost by to nemělo mít vliv. *Cnews* [online]. 2015 [cit. 2020-05-05]. Dostupné z: https://www.cnews.cz/android-6-0-uz-musi-mit-povinne-sifrovane-uloziste-na-rychlost-by-to-nemelo-mit-vliv/
[31] HALLER, Martin. *Jsou aktualizace opravdu tak důležité?* [online]. 2019 [cit. 2020-05-05]. Dostupné z: https://martinhaller.cz/know-how/jsou-aktualizace-opravdu-tak-dulezite/
[32] ROUSE, Margaret. Remote wipe. *Search Mobile Computing* [online]. 2019 [cit. 2020-05-05]. Dostupné z: https://searchmobilecomputing.techtarget.com/definition/remote-wipe
[33] O stavu připojení k síti. *Kaspersky* [online]. 2020 [cit. 2020-05-05]. Dostupné z: https://help.kaspersky.com/KESWin/10SP2/cs-CZ/44427.htm
[34] Zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ze dne 1.1.2015

[35] Bezpečnostní Incident (Security Incident). Management Mania [online]. [cit. 2020-05-30]. Dostupné z: https://managementmania.com/cs/bezpecnostni-incident
[36] Zákon č. 563/1991 Sb., zákon o účetnictví ze dne 1.1.1992
[37] Antivirový program. Antivirové centrum [online]. [cit. 2020-05-30]. Dostupné z: https://www.antivirovecentrum.cz/antiviry.aspx
[38] Co je to proxy server. Sprava-site.eu [online]. [cit. 2020-05-30]. Dostupné z: https://www.sprava-site.eu/proxy-server/
[39] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN ISBN978-80-88168-32-4.
[40] Autentizace, ověření, identifikace (Authentication). Management Mania [online]. [cit. 2020-05-31]. Dostupné z: https://managementmania.com/cs/autentizace-identifikace
[41] GENÇOĞLU, M.Tuncay. Importance of Cryptography in Information Security [online]. 2019 [cit. 2020-05-31]. Dostupné z: https://www.researchgate.net/publication/331641251_Importance_of_Cryptography_in_Information_Security
[42] PAVLIS, Jakub. TPM - ochrana dat na všech úrovních [online]. 3. 5. 2006 [cit. 2020-05-31]. Dostupné z: https://notebook.cz/clanky/technologie/2006/TPM
[43] VYMAZAL, Radek. MANAGEMENT LOGŮ A INSTALACE GRAYLOG. Connectica [online]. [cit. 2020-05-31]. Dostupné z: https://radekvymazal.cz/management-logu-a-instalace-graylog/
[44] BOUŠKA, Petr. VLAN - Virtual Local Area Network. Samuraj-cz.com [online]. 02.06.2007 [cit. 2020-05-31]. Dostupné z: https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/
[45] Co je VLAN. Správa Sítě [online]. [cit. 2020-05-31]. Dostupné z: https://www.sprava-site.eu/vlan/
[46] RAAB, Stefan a Madhavi W. CHANDRA. Cisco: mobilní IP technologie a aplikace. Praha: Grada, 2007. ISBN 978-80-247-1611-4.
[47] BOUŠKA, Petr. Cisco IOS 11 - IEEE 802.1x, autentizace k portu, MS IAS. Samuraj-cz.com [online]. 10.10.2007 [cit. 2020-05-31]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-11-ieee-802-1x-autentizace-k-portu-ms-ias/

[48] IDS, IPS, Sandbox, ATP. Comguard [online]. [cit. 2020-05-31]. Dostupné z: https://www.comguard.cz/ids-ips-a-advance-thread-protection?sort=14&itemsPerPage=6
[49] IDS/IPS. Pbwcz.cz [online]. [cit. 2020-05-31]. Dostupné z: http://pbwcz.cz/Bezpecnostni%20kategorie/IDSIPS.html
[50] BUDÍN, Emil. K čemu je SIEM? Systemonline.cz [online]. 10. 11. 2014 [cit. 2020-05-31]. Dostupné z: http://m.systemonline.cz/it-security/k-cemu-je-siem.htm
[51] CISA. Using Caution with USB Drives. Us-cert.gov [online]. 10. 11. 2014 [cit. 2020-05-31]. Dostupné z: https://www.us-cert.gov/ncas/tips/ST08-001
[52] MARTIN, D. Systém managementu bezpečnosti informací. Grada Publishing a.s, 2011. ISBN 9788024776163. Dostupné také z: https://books.google.cz/books?id=ezd4CwAAQBAJ
[53] Penetrační testování. Experia [online]. [cit. 2020-05-31]. Dostupné z: https://www.experia.cz/sluzby/penetracni-testovani/
[54] ČERMÁK, Miroslav. Analýza rizik: Jemný úvod do analýzy rizik. Clever and smart [online]. 20. 05. 2010 [cit. 2020-05-31]. Dostupné z: https://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/
[55] DIBLÍK, Jan. Právní aspekty BYOD (Bring Your Own Device) a jeho praktická využitelnost v českých společnostech. Právní prostor [online]. 20. 05. 2010 [cit. 2020-05-31]. Dostupné z: https://www.pravniprostor.cz/clanky/pracovni-pravo/pravni-aspekty-byod-bring-your-own-device-a-jeho-prakticka-vyuzitelnost-v-ceskych-spolecnostech

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

BYOD	Bring your own device
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Systém
EPS	Elektronický požární systém
EZS	Elektronický zabezpečovací systém
HR	Human resources
ICT	Information and communication technologies
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention Systems
ISMS	Information security management system
ISO	International Organization for Standardization
IT	Infomation technologies
LAN	Local Area Network
MDM	Mobile device management
NTP	Network Time Protocol
PDA	Personal digital assistent
PDCA	Plan-Do-Chack-Act
SIEM	Security Information and Event Management
SW	Software
TPM	Trusted Platform Module
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK

SEZNAM PŘÍLOH

Příloha č. 1: Evidence aktiv[10]

Identifikace aktiva				Klasifikace aktiva		
ID	Třída aktiva	Název aktiva	Popis aktiva	Důvěrnost	Integrita	Dostupnost
1	Hardware	Aktivní prvky LAN sítě	Router, 3x switch	Vysoké	Vysoké	Vysoké
2	Hardware	Kabeláž	Rozvod internetu kabeláží, datové zásuvky	Nízká	N/A	Střední
3	Hardware	Wi-Fi	Wi-Fi síť, Access pointy 4x	Vysoká	Vysoká	Střední
4	Hardware	Firewall	Hardwarový firewall	Vysoká	Kritická	Vysoká
5	Hardware	Server ESXA	Zajištění provozu poštovního serveru, DNS a DHCP server, databázového serveru, aplikačního serveru, fileserveru, VPN serveru	Vysoká	Vysoká	Vysoká
6	Hardware	Server ESXB	Server pro vývoj, testování	Střední	Vysoká	Střední
7	Hardware	Server pro kamerový systém	Server pro provoz kamerový systému včetně záznamu	Vysoká	Vysoká	Střední
8	Hardware	Synology NAS	Zálohovací zařízení Synology NAS	Kritické	Vysoká	Střední
9	Hardware	Koncové stanice - PC	HP stolní počítače	Vysoká	Vysoká	Střední
10	Hardware	Koncové stanice - Notebooky	Firemní notebooky zaměstnanců	Vysoká	Vysoká	Střední
11	Hardware	Telefony	Firemní telefony zaměstnanců	Vysoká	Nízká	Střední
12	Hardware	Nefiremní notebooky	Nefiremní notebooky využívaná zaměstnanci pro pracovní činnost	Vysoká	Střední	Nízká
13	Hardware	Kamerový systém	Jednotlivé kamery a rozvod kabeláže	Vysoká	Nízká	Střední
14	Hardware	Podpurná zařízení	Tiskárny, Scannery	Nízká	N/A	Střední
15	Hardware	EZS	Elektronický zabezpečovací systém vč. čidel pohybu	Vysoká	Střední	Vysoká
16	Hardware	EPS	Elektronický požární systém vč. čidel kouře	Střední	Střední	Střední
17	Hardware	Přístupové karty	Elektornické karty pro vstup do budovy a kanceláří	Vysoká	Střední	Střední
18	Software	Firewall	Systém firewall	Vysoká	Kritická	Vysoká
19	Software	Server ESXA	Windows server 2019, MS Exchange, databázový server pro testování, databázový server pro helpdesk, fileserver, VPN server, ...	Vysoká	Vysoká	Vysoká
20	Software	Server ESXB	SUSE Linux Server, testový server	Vysoká	Vysoká	Vysoká
21	Software	Aplikace	Microsoft Office, LibreOffice, Outlook, Adobe, Oracle, Redmine, ...	Vysoká	Střední	Střední
22	Software	OS pro koncové stanice	OS Windows 10, Debian GNU	Vysoká	Střední	Střední
23	Software	OS pro telefony	Android 9.0	Vysoká	Střední	Nízká
24	Prostory	Zabezpečené prostory - technické	Technické zabezpečené prostory s citlivými informacemi (serverovna)	Kritická	Vysoká	Střední
25	Prostory	Zabezpečené prostory - kancelářské	Kancelářské zabezpečené prostory s citlivými informacemi (kancelář jednatele, kancelář správce ICT)	Vysoká	Střední	Střední
26	Prostory	Veřejně přístupné prostory	Prostory budovy do kterých se může dostat veřejnost (vstupní hala, chodby, sociální zařízení, ...)	Střední	Nízká	Střední
27	Prostory	Venkovní areál	Venkovní prostory společnosti	Nízká	Nízká	Střední
28	Služby	Zálohování dat	Služba zálohování dat z fileserveru na NAS	N/A	Vysoká	Vysoká
29	Služby	VPN připojení	VPN připojení z mobilních zařízení do sítě společnosti	Vysoká	Vysoká	Vysoká
30	Služby	Internet	Konektivita k internetu	Střední	Vysoká	Kritická
31	Služby	Elektřina	Elektrické napájení	N/A	N/A	Vysoká
32	Služby	Help desk	Služby ticketovacího systému Redmine	Střední	Střední	Vysoká
33	Služby	MS Exchange	Služby poštovního serveru MS Exchange	Kritická	Vysoká	Střední
34	Služby	File server	Služby přístupu k firemním souborům	Kritická	Vysoká	Střední
35	Informace/data	Data na file serveru	Informace na sdílených souborech	Kritická	Vysoká	Střední
36	Informace/data	Data v help desku	Data zaměstnanců, zákazníků a dodavatelů v tiketovacím systému	Střední	Vysoká	Vysoká
37	Informace/data	Zdrojové kódy	Zdrojové kódy spolu s historií, build skripty a konfigurací	Vysoká	Vysoká	Střední
38	Informace/data	Projektová dokumentace	Smlouvy, objednávky, analýzy, zápisy z jednání, požadavky zadavatele na vývoj, údržbu a techniku	Vysoká	Vysoká	Střední
39	Informace/data	Testovací data	Data vytvořená při vývoji SW, data poskytnutá zadavatelem	Střední	Střední	Střední
40	Informace/data	Provozní informace	Licenční soubory/klíče k vývojářským nástrojům a knihovnám, instalátory uložené na file serveru	Vysoká	Vysoká	Střední
41	Informace/data	Personalistika, mzdy	Informace o zaměstnancích uložené na file serveru a v kancelářích	Vysoká	Vysoká	Nízká
42	Informace/data	Konfigurace aktivních prvků	Informace o konfiguraci aktivních prvků	Vysoká	Vysoká	Střední
43	Informace/data	Konfigurace firewallu	Informace o konfiguraci firewallu	Vysoká	Vysoká	Střední
44	Informace/data	Zálohovaná data	Zálohovaná data na zařízení Synology NAS	Kritická	Vysoká	Střední

[10] N/A – daný bezpečnostní atribut nelze klasifikovat

Příloha č. 2: Počáteční analýzy rizik pro skupiny aktiv vztahující se k tématu práce

Název analýzy	Skupina aktiv: Notebooky	
Zahrnutá aktiva	Informace/data	
	Hardware	*Koncové stanice - notebooky*
	Software	*Aplikace, OS pro koncové stanice*
	Služby	
	Prostory	
Nejvyšší dopad narušení bezpečnosti	*Vysoká - 3*	

ID	Hrozba	Zranitelnosti	H Pravděpodobnost hrozby	Z Snadnost zneužití zranitelnosti	R Riziko
1	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	3	4	36
2	Poškození nebo selhání technického anebo programového vybavení	Z1, Z2, Z10	2	2	12
3	Zneužití identity	Z2, Z4, Z8, Z9, Z13	3	3	27
4	Užívání programového vybavení v rozporu s licenčními podmínkami	Z4, Z8, Z12	3	3	27
5	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	3	3	27
6	Narušení fyzické bezpečnosti	Z3, Z9, Z10	2	3	18
7	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Z11	2	1	6
8	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	3	3	27
9	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z8, Z9, Z10	3	3	27
10	Nedodržení smluvního závazku ze strany dodavatele	Z8, Z9, Z12	1	2	6
11	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	3	3	27
12	Zneužití vnitřních prostředků, sabotáž	Z7, Z8, Z12	2	3	18
13	Dlouh. přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z10, Z11	2	2	12
14	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Z4, Z11, Z12	1	2	6
15	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	4	3	36
16	Zneužití vyměnitelných technických nosičů dat	Z4, Z8, Z12, Z13	3	3	27
17	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z7, Z10	2	3	18

Název analýzy	Skupina aktiv: Telefony	
Zahrnutá aktiva	Informace/data	
	Hardware	*Telefony*
	Software	*OS pro telefony*
	Služby	
	Prostory	
Nejvyšší dopad narušení bezpečnosti	***Vysoká - 3***	

ID	Hrozba	Zranitelnosti	H Pravděpodobnost hrozby	Z Snadnost zneužití zranitelnosti	R Riziko
1	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	3	3	27
2	Poškození nebo selhání technického anebo programového vybavení	Z1, Z2, Z10	2	2	12
3	Zneužití identity	Z4, Z6, Z7, Z8, Z9, Z13	3	3	27
4	Užívání programového vybavení v rozporu s licenčními podmínkami	Z4, Z8, Z9, Z13	2	3	18
5	Škodlivý kód (například viry, spyware, trojské koně)	Z2, Z4, Z7, Z8, Z12, Z13	3	3	27
6	Narušení fyzické bezpečnosti	Z3, Z9, Z10	2	2	12
7	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Z11	1	2	6
8	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z9, Z12	2	2	12
9	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z9, Z13	4	3	36
10	Nedodržení smluvního závazku ze strany dodavatele	Z8, Z12	1	2	6
11	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	2	3	18
12	Zneužití vnitřních prostředků, sabotáž	Z7, Z8, Z12	2	2	12
13	Dlouh. přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z10, Z11	2	2	12
14	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Z4, Z12	1	1	3
15	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	3	3	27
16	Zneužití vyměnitelných technických nosičů dat	Z4, Z12	1	2	6
17	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z4, Z5, Z7, Z10	2	3	18

Název analýzy	Skupina aktiv: BYOD	
Zahrnutá aktiva	Informace/data	
	Hardware	*Nefiremní notebooky*
	Software	*Aplikace, OS pro koncové stanice*
	Služby	
	Prostory	
Nejvyšší dopad narušení bezpečnosti	***Vysoká - 3***	

ID	Hrozba	Zranitelnosti	H Pravděpodobnost hrozby	Z Snadnost zneužití zranitelností	R Riziko
1	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	3	4	36
2	Poškození nebo selhání technického anebo programového vybavení	Z1, Z2, Z10	2	2	12
3	Zneužití identity	Z2, Z4, Z8, Z9, Z13	3	4	36
4	Užívání programového vybavení v rozporu s licenčními podmínkami	Z4, Z8, Z12	3	3	27
5	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	3	3	27
6	Narušení fyzické bezpečnosti	Z3, Z9, Z10	2	3	18
7	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Z11	1	1	3
8	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	3	3	27
9	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z8, Z9, Z10	3	3	27
10	Nedodržení smluvního závazku ze strany dodavatele	Z8, Z9, Z12	3	3	27
11	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	3	3	27
12	Zneužití vnitřních prostředků, sabotáž	Z7, Z8, Z12	3	3	27
13	Dlouh. přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z10, Z11	1	2	6
14	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Z4, Z11, Z12	1	2	6
15	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	3	3	27
16	Zneužití vyměnitelných technických nosičů dat	Z4, Z8, Z12, Z13	3	3	27
17	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z7, Z10	2	3	18

Název analýzy	Skupina aktiv: VPN připojení	
Zahrnutá aktiva	Informace/data	
	Hardware	*Server ESXA, Koncové stanice - notebooky, Nefiremní notebooky*
	Software	*Server ESXA*
	Služby	*VPN připojení*
	Prostory	
Nejvyšší dopad narušení bezpečnosti	***Vysoká - 3***	

ID	Hrozba	Zranitelnosti	H Pravděpodobnost hrozby	Z Snadnost zneužití zranitelnosti	R Riziko
1	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z11, Z12, Z13	3	3	27
2	Poškození nebo selhání technického anebo programového vybavení	Z1, Z2, Z5, Z10	2	2	12
3	Zneužití identity	Z2, Z4, Z6, Z7, Z9, Z13	3	3	27
4	Užívání programového vybavení v rozporu s licenčními podmínkami	Z4, Z8, Z13	2	2	12
5	Škodlivý kód (například viry, spyware, trojské koně)	Z1, Z2, Z4, Z7, Z8, Z11, Z12, Z13	3	3	27
6	Narušení fyzické bezpečnosti	Z3, Z9	1	2	6
7	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Z11	1	1	3
8	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	3	3	27
9	Ztráta, odcizení nebo poškození aktiva	Z3, Z9, Z10, Z13	3	3	27
10	Nedodržení smluvního závazku ze strany dodavatele	Z8	1	2	6
11	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	2	2	12
12	Zneužití vnitřních prostředků, sabotáž	Z6, Z7, Z8, Z12	3	3	27
13	Dlouh. přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z9, Z10, Z11	2	2	12
14	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Z4, Z11, Z12	2	2	12
15	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	2	2	12
16	Zneužití vyměnitelných technických nosičů dat	Z4, Z12, Z8, Z13	2	3	18
17	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z6, Z7, Z10	2	3	18

Název analýzy	Skupina aktiv: Síťová infrastruktura	
Zahrnutá aktiva	Informace/data	*Konfigurace aktivních prvků, Konfigurace firewallu*
	Hardware	*Aktivní prvky LAN sítě, Kabeláž, Wi-Fi, Firewall*
	Software	*Firewall*
	Služby	
	Prostory	
Nejvyšší dopad narušení bezpečnosti	***Kritická - 4***	

ID	Hrozba	Zranitelnosti	H Pravděpodobnost hrozby	Z Snadnost zneužití zranitelnosti	R Riziko
1	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z11, Z12, Z13	2	2	12
2	Poškození nebo selhání technického anebo programového vybavení	Z1, Z2, Z5, Z10	2	2	12
3	Zneužití identity	Z4, Z7, Z8, Z9, Z13	3	3	27
4	Užívání programového vybavení v rozporu s licenčními podmínkami	Z4, Z8, Z13	1	2	6
5	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	4	3	36
6	Narušení fyzické bezpečnosti	Z3, Z9	1	2	6
7	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Z11	3	2	18
8	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12	3	3	27
9	Ztráta, odcizení nebo poškození aktiva	Z3, Z8, Z9, Z12, Z13	1	2	6
10	Nedodržení smluvního závazku ze strany dodavatele	Z8	1	1	3
11	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	3	3	27
12	Zneužití vnitřních prostředků, sabotáž	Z7, Z8, Z12	1	2	6
13	Dlouh. přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z10, Z11	3	3	27
14	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Z4, Z11, Z12	1	1	3
15	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	2	2	12
16	Zneužití vyměnitelných technických nosičů dat	Z4, Z12, Z8, Z13	1	1	3
17	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z7, Z10	3	3	27

Příloha č. 3: Celkový přehled rizik shromážděný z analýz rizik v příloze č. 2

Přehled rizik

Riziko						
ID rizika	Název analýzy	Hrozba	Zranitelnosti	Pravděpodobnost hrozby	Snadnost zneužití zranitelnosti	Riziko
1	Skupina aktiv: Síťová infrastruktura	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	4	3	48
5	Skupina aktiv: BYOD	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	3	4	36
6	Skupina aktiv: BYOD	Zneužití identity	Z2, Z4, Z8, Z9, Z13	3	4	36
3	Skupina aktiv: Notebooky	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	4	3	36
2	Skupina aktiv: Notebooky	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	3	4	36
10	Skupina aktiv: Síťová infrastruktura	Dlouh. přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z10, Z11	3	3	36
11	Skupina aktiv: Síťová infrastruktura	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z7, Z10	3	3	36
9	Skupina aktiv: Síťová infrastruktura	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	3	3	36
7	Skupina aktiv: Síťová infrastruktura	Zneužití identity	Z4, Z7, Z8, Z9, Z13	3	3	36
8	Skupina aktiv: Síťová infrastruktura	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12	3	3	36
4	Skupina aktiv: Telefony	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z9, Z13	4	3	36
30	Skupina aktiv: BYOD	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	3	3	27
27	Skupina aktiv: BYOD	Nedodržení smluvního závazku ze strany dodavatele	Z8, Z9, Z12	3	3	27
28	Skupina aktiv: BYOD	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	3	3	27
24	Skupina aktiv: BYOD	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	3	3	27
23	Skupina aktiv: BYOD	Užívání programového vybavení v rozporu s licenčními podmínkami	Z4, Z8, Z12	3	3	27
25	Skupina aktiv: BYOD	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	3	3	27
29	Skupina aktiv: BYOD	Zneužití vnitřních prostředků, sabotáž	Z7, Z8, Z12	3	3	27
31	Skupina aktiv: BYOD	Zneužití vyměnitelných technických nosičů dat	Z4, Z8, Z12, Z13	3	3	27
26	Skupina aktiv: BYOD	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z8, Z9, Z10	3	3	27
17	Skupina aktiv: Notebooky	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	3	3	27
14	Skupina aktiv: Notebooky	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	3	3	27
13	Skupina aktiv: Notebooky	Užívání programového vybavení v rozporu s licenčními podmínkami	Z4, Z8, Z12	3	3	27
12	Skupina aktiv: Notebooky	Zneužití identity	Z2, Z4, Z8, Z9, Z13	3	3	27
15	Skupina aktiv: Notebooky	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	3	3	27
18	Skupina aktiv: Notebooky	Zneužití vyměnitelných technických nosičů dat	Z4, Z8, Z12, Z13	3	3	27
16	Skupina aktiv: Notebooky	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z8, Z9, Z10	3	3	27
22	Skupina aktiv: Telefony	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	3	3	27
19	Skupina aktiv: Telefony	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	3	3	27
21	Skupina aktiv: Telefony	Škodlivý kód (například viry, spyware, trojské koně)	Z2, Z4, Z7, Z8, Z12, Z13	3	3	27
20	Skupina aktiv: Telefony	Zneužití identity	Z4, Z6, Z7, Z8, Z9, Z13	3	3	27
32	Skupina aktiv: VPN připojení	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z11, Z12, Z13	3	3	27
34	Skupina aktiv: VPN připojení	Škodlivý kód (například viry, spyware, trojské koně)	Z1, Z2, Z4, Z7, Z8, Z11, Z12, Z13	3	3	27
33	Skupina aktiv: VPN připojení	Zneužití identity	Z2, Z4, Z6, Z7, Z9, Z13	3	3	27
35	Skupina aktiv: VPN připojení	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	3	3	27
37	Skupina aktiv: VPN připojení	Zneužití vnitřních prostředků, sabotáž	Z6, Z7, Z8, Z12	3	3	27
36	Skupina aktiv: VPN připojení	Ztráta, odcizení nebo poškození aktiva	Z3, Z9, Z10, Z13	3	3	27
38	Skupina aktiv: Síťová infrastruktura	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Z11	3	2	24
41	Skupina aktiv: Notebooky	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z7, Z10	2	3	18
39	Skupina aktiv: Notebooky	Narušení fyzické bezpečnosti	Z3, Z9, Z10	2	3	18
40	Skupina aktiv: Notebooky	Zneužití vnitřních prostředků, sabotáž	Z7, Z8, Z12	2	3	18
44	Skupina aktiv: Telefony	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z4, Z5, Z7, Z10	2	3	18

Riziko						
ID rizika	Název analýzy	Hrozba	Zranitelnosti	Pravděpodobnost hrozby	Snadnost zneužití zranitelnosti	Riziko
43	Skupina aktiv: Telefony	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	2	3	18
42	Skupina aktiv: Telefony	Užívání programového vybavení v rozporu s licenčními podmínkami	Z4, Z8, Z9, Z13	2	3	18
48	Skupina aktiv: VPN připojení	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z6, Z7, Z10	2	3	18
47	Skupina aktiv: VPN připojení	Zneužití vyměnitelných technických nosičů dat	Z4, Z12, Z8, Z13	2	3	18
51	Skupina aktiv: Síťová infrastruktura	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	2	2	16
49	Skupina aktiv: Síťová infrastruktura	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z11, Z12, Z13	2	2	16
50	Skupina aktiv: Síťová infrastruktura	Poškození nebo selhání technického anebo programového vybavení	Z1, Z2, Z5, Z10	2	2	16
59	Skupina aktiv: BYOD	Poškození nebo selhání technického anebo programového vybavení	Z1, Z2, Z10	2	2	12
53	Skupina aktiv: Notebooky	Dlouh. přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z10, Z11	2	2	12
52	Skupina aktiv: Notebooky	Poškození nebo selhání technického anebo programového vybavení	Z1, Z2, Z10	2	2	12
58	Skupina aktiv: Telefony	Dlouh. přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z10, Z11	2	2	12
55	Skupina aktiv: Telefony	Narušení fyzické bezpečnosti	Z3, Z9, Z10	2	2	12
54	Skupina aktiv: Telefony	Poškození nebo selhání technického anebo programového vybavení	Z1, Z2, Z10	2	2	12
56	Skupina aktiv: Telefony	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z9, Z12	2	2	12
57	Skupina aktiv: Telefony	Zneužití vnitřních prostředků, sabotáž	Z7, Z8, Z12	2	2	12
65	Skupina aktiv: VPN připojení	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	2	2	12
63	Skupina aktiv: VPN připojení	Dlouh. přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z9, Z10, Z11	2	2	12
64	Skupina aktiv: VPN připojení	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Z4, Z11, Z12	2	2	12
62	Skupina aktiv: VPN připojení	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	2	2	12
60	Skupina aktiv: VPN připojení	Poškození nebo selhání technického anebo programového vybavení	Z1, Z2, Z5, Z10	2	2	12
61	Skupina aktiv: VPN připojení	Užívání programového vybavení v rozporu s licenčními podmínkami	Z4, Z8, Z13	2	2	12
67	Skupina aktiv: Síťová infrastruktura	Narušení fyzické bezpečnosti	Z3, Z9	1	2	8
66	Skupina aktiv: Síťová infrastruktura	Užívání programového vybavení v rozporu s licenčními podmínkami	Z4, Z8, Z13	1	2	8
69	Skupina aktiv: Síťová infrastruktura	Zneužití vnitřních prostředků, sabotáž	Z7, Z8, Z12	1	2	8
68	Skupina aktiv: Síťová infrastruktura	Ztráta, odcizení nebo poškození aktiva	Z3, Z8, Z9, Z12, Z13	1	2	8
76	Skupina aktiv: BYOD	Dlouh. přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z10, Z11	1	2	6
46	Skupina aktiv: BYOD	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z7, Z10	2	3	6
45	Skupina aktiv: BYOD	Narušení fyzické bezpečnosti	Z3, Z9, Z10	2	3	6
77	Skupina aktiv: BYOD	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Z4, Z11, Z12	1	2	6
71	Skupina aktiv: Notebooky	Nedodržení smluvního závazku ze strany dodavatele	Z8, Z9, Z12	1	2	6
72	Skupina aktiv: Notebooky	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Z4, Z11, Z12	1	2	6
70	Skupina aktiv: Notebooky	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Z11	2	1	6
74	Skupina aktiv: Telefony	Nedodržení smluvního závazku ze strany dodavatele	Z8, Z12	1	2	6
73	Skupina aktiv: Telefony	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Z11	1	2	6
75	Skupina aktiv: Telefony	Zneužití vyměnitelných technických nosičů dat	Z4, Z12	1	2	6
78	Skupina aktiv: VPN připojení	Narušení fyzické bezpečnosti	Z3, Z9	1	2	6
79	Skupina aktiv: VPN připojení	Nedodržení smluvního závazku ze strany dodavatele	Z8	1	2	6
80	Skupina aktiv: Síťová infrastruktura	Nedodržení smluvního závazku ze strany dodavatele	Z8	1	1	4
81	Skupina aktiv: Síťová infrastruktura	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Z4, Z11, Z12	1	1	4
82	Skupina aktiv: Síťová infrastruktura	Zneužití vyměnitelných technických nosičů dat	Z4, Z12, Z8, Z13	1	1	4
84	Skupina aktiv: BYOD	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Z11	1	1	3
83	Skupina aktiv: Telefony	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Z4, Z12	1	1	3
85	Skupina aktiv: VPN připojení	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Z11	1	1	3

Příloha č. 4: Přehled neakceptovatelných rizik s hrozbami vztahujícími se pouze k tématu a cíli práce

Riziko						
ID rizika	Název analýzy	Hrozba	Zranitelnosti	Pravděpodobnost hrozby	Snadnost zneužití zranitelnosti	Riziko
1	Skupina aktiv: Síťová infrastruktura	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	4	3	48
2	Skupina aktiv: Notebooky	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	3	4	36
3	Skupina aktiv: Notebooky	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	4	3	36
4	Skupina aktiv: Telefony	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z9, Z13	4	3	36
5	Skupina aktiv: BYOD	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	3	4	36
6	Skupina aktiv: BYOD	Zneužití identity	Z2, Z4, Z8, Z9, Z13	3	4	36
7	Skupina aktiv: Síťová infrastruktura	Zneužití identity	Z4, Z7, Z8, Z9, Z13	3	3	36
8	Skupina aktiv: Síťová infrastruktura	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12	3	3	36
9	Skupina aktiv: Síťová infrastruktura	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	3	3	36
11	Skupina aktiv: Síťová infrastruktura	Napadení elektronické komunikace (odposlech, modifikace)	Z2, Z5, Z7, Z10	3	3	36
12	Skupina aktiv: Notebooky	Zneužití identity	Z2, Z4, Z8, Z9, Z13	3	3	27
14	Skupina aktiv: Notebooky	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	3	3	27
15	Skupina aktiv: Notebooky	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	3	3	27
16	Skupina aktiv: Notebooky	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z8, Z9, Z10	3	3	27
17	Skupina aktiv: Notebooky	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	3	3	27
18	Skupina aktiv: Notebooky	Zneužití vyměnitelných technických nosičů dat	Z4, Z8, Z12, Z13	3	3	27
19	Skupina aktiv: Telefony	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z12, Z13	3	3	27
20	Skupina aktiv: Telefony	Zneužití identity	Z4, Z6, Z7, Z8, Z9, Z13	3	3	27
21	Skupina aktiv: Telefony	Škodlivý kód (například viry, spyware, trojské koně)	Z2, Z4, Z7, Z8, Z12, Z13	3	3	27
22	Skupina aktiv: Telefony	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	3	3	27
24	Skupina aktiv: BYOD	Škodlivý kód (například viry, spyware, trojské koně)	Z7, Z8, Z2, Z4, Z12, Z13	3	3	27
25	Skupina aktiv: BYOD	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	3	3	27
26	Skupina aktiv: BYOD	Ztráta, odcizení nebo poškození aktiva	Z3, Z4, Z8, Z9, Z10	3	3	27
28	Skupina aktiv: BYOD	Pochybení ze strany zaměstnanců	Z4, Z7, Z8, Z12, Z13	3	3	27
30	Skupina aktiv: BYOD	Cílený útok pomocí sociálního inženýrství, použití špionážních technik	Z1, Z2, Z4, Z6, Z7, Z8, Z12, Z13	3	3	27
31	Skupina aktiv: BYOD	Zneužití vyměnitelných technických nosičů dat	Z4, Z8, Z12, Z13	3	3	27
32	Skupina aktiv: VPN připojení	Porušení bezp. politiky, provedení neoprávněných činností, zneužití oprávnění ze strany zaměstnance	Z4, Z6, Z8, Z9, Z11, Z12, Z13	3	3	27
33	Skupina aktiv: VPN připojení	Zneužití identity	Z2, Z4, Z6, Z7, Z9, Z13	3	3	27
34	Skupina aktiv: VPN připojení	Škodlivý kód (například viry, spyware, trojské koně)	Z1, Z2, Z4, Z7, Z8, Z11, Z12, Z13	3	3	27
35	Skupina aktiv: VPN připojení	Zneužití nebo neoprávněná modifikace údajů	Z6, Z7, Z8, Z12, Z13	3	3	27
36	Skupina aktiv: VPN připojení	Ztráta, odcizení nebo poškození aktiva	Z3, Z9, Z10, Z13	3	3	27