VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

ZAVÁDĚNÍ BEZPEČNOSTNÍCH OPATŘENÍ DLE ISMS DO MALÉ SPOLEČNOSTI

SMALL COMPANY SECURITY MEASURES IMPLEMENTATION ACCORDING TO ISMS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Josef Kohoutek

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Petr Sedlák

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Kohoutek Josef, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Zavádění bezpečnostních opatření dle ISMS do malé společnosti

v anglickém jazyce:

Small Company Security Measures Implementation According to ISMS

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrh řešení, přínos práce
Závěr
Seznam použité literatury

Seznam odborné literatury:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.
ČSN ISO/IEC 27002, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.
DOUCEK P., L. NOVÁK, L. NEDOMOVÁ a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Vedoucí diplomové práce: Ing. Petr Sedlák

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 29.2.2016

Abstrakt

Ve své diplomové práci se zaměřuji na návrh systému řízení informační bezpečnosti pro společnost INNC s.r.o., která se specializuje na návrh a realizaci počítačových sítí. Diplomová práce je rozdělena do dvou částí. V první části jsou uvedeny teoretické poznatky z dané problematiky. V druhé části pak analýza společnosti a návrh bezpečnostních opatření.

Abstract

In my master´s thesis I focus on the design of information security management system for the company INNC s.r.o., which specializes in the design and implementation of computer networks. The thesis is divided into two parts. The first part provides theoretical knowledge of the issue. Second part is the analysis and proposal of security measures.

Klíčová slova

Informační bezpečnost, ISMS, analýza rizik, ČSN ISO/IEC 27 001, ČSN ISO/IEC 27 002, opatření

Keywords

Information Security, ISMS, risk analysis, ISO / IEC 27001, ISO / IEC 27002, measures

Bibliografická citace práce

KOHOUTEK, J. *Zavádění bezpečnostních opatření dle ISMS do malé společnosti*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 140 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

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

V Brně dne 31. května 2016

……

Josef Kohoutek

Poděkování

Touto cestou bych chtěl poděkovat všem, kteří mi pomohli při vypracování mé diplomové práce, především pak panu Ing. Petru Sedlákovi za všechny jeho rady, odbornou pomoc a ochotu a také panu Ing. Viktoru Ondrákovi, Ph.D. za jeho konstruktivní připomínky a odborné rady. Dále velmi děkuji firmě INNC s.r.o., která mi umožnila zpracovávat tuto diplomovou práci a poskytla mi potřebné informace.

Obsah

Úvod

Informační bezpečnost nabývá v dnešní době stále většího významu. Jedním z prostředků, který ošetřuje tuto oblast v ČR je „Zákon o kybernetické bezpečnosti“, platný od 1. 1. 2015. Zaměřuje se především na veřejnou správu, jeho vliv je však podstatně širší.

Právě informační bezpečnost je u mnoha firem podceňována a opomíjena. Vzhledem k tomu, že většina běžných firem pořádně neví, co si pod tímto pojmem představit, rozhodl jsem se vypracovat svou diplomovou práci právě na toto téma.

Pro svou práci jsem si vybral menší společnost INNC s.r.o. která se zabývá návrhem a realizací počítačových sítí. Z hlediska řízení informační bezpečnosti jsem se zaměřil především na analýzu rizik a návrh bezpečnostních opatření.

1. Cíle práce

Cílem práce je návrh bezpečnostních opatření pro zvýšení informační bezpečnosti na základě analýzy současného stavu společnosti INNC s.r.o. dle norem řady ISO 27 000 – zmapování současného stavu, odhalení případných nedostatků a návrh řešení. Výstupem práce tedy má být návrh na zvýšení informační bezpečnosti společnosti v podobě navržených opatření.

Dílčí cíle práce:

- Teoretické objasnění problematiky
- Analýza současného stavu
- Identifikace aktiv
- Analýza rizik, hrozeb a scénářů dle norem řady ISO 27 000
- Návrh opatření dle norem řady ISO 27 000

Práce si neklade za cíl přinést komplexní řešení bezpečnosti, ale spíše vybrat vhodná opatření na základě komunikace s firmou a dostupných finančních prostředků.

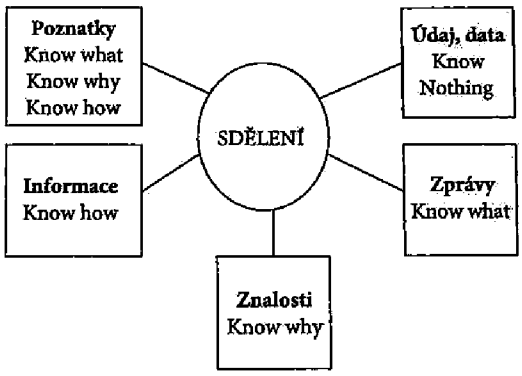
Při realizaci práce jsem čerpal především z ISO norem řady 27 000 a odborné literatury, která je uvedena v závěru.

2. Teoretická východiska práce

První část práce je věnována teoretickému shrnutí problematiky řízení informační bezpečnosti.

2.1. Informace

Na kvalitě informací závisí správnost zhodnocení operativní situace, optimálnost přijímaných rozhodnutí, plánování opatření, srozumitelné přenesení úkolů vykonavatelům, úspěšné organizováni i operativní řízení bezpečnostních akcí, efektivnost kontroly.[1]



Obr. č. 1: Architektura informačních pojmů[2]

Ve společnostech jsou užívány především následující oblasti informací:[3]

- interní informace o společnosti, její strategické záměry a plány,
- interní znalostní informace, které nejsou obecně dostupné konkurencí („know-how"), interní předpisová základna,
- informace o zaměstnancích společnosti,
- databáze o klientech, spolupracujících společnostech a subjektech,
- informace získané z volně dostupných zdrojů (například odborné publikace, internet, tisk).[4]

Jaké důvody vedou firmu k zajištění ochrany informací? Existují tři hlavní důvody:

[1] POŽÁR, Josef. *Manažerská informatika*. s. 36.
[2] tamtéž, s. 37.
[3] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 4.
[4] tamtéž, s. 5.

1) povinnosti vyplývající z platné legislativy v ČR (například zákon 1 101/2000 Sb., o ochraně osobních údajů a o změně některých předpisů) a zásad doporučených v rámci EU,
2) závazky společnosti vůči spolupracujícím externím společnostem i klientům vyplývající z podmínek uzavřených smluv a dohod,
3) vlastní obchodní zájmy firmy - především se jedná o utajení interních důvěrných informací, zamezení jejich zneužití, dostupnost potřebných informací a jejich celistvost.[5]

2.1.1. Zabezpečení informací

Pod pojmem informace je třeba si představit texty, číselné údaje, e-mailové zprávy, počítačové soubory apod. Pracovníci firem často tento pojem ztotožňují se zamezením přístupu k informaci neoprávněným osobám. Jedná se však pouze o dílčí zabezpečení informace. Pod pojmem zabezpečení informace je míněno zajištění důvěrnosti, integrity a dostupnosti informace. Uveďme, jak jsou definovány tyto pojmy:[6]

- *důvěrnost* - prevence proti neoprávněnému užití informace, [7] kdy přístup k aktivům mají pouze autorizované subjekty, tj. osoba, proces nebo zařízení disponující oprávněními k provádění činností v IS/ICT. [8]
- *integrita* - prevence proti neautorizované modifikaci informace, kdy ke změně aktiva nemůže dojít neautorizovaným subjektem, nepovolenou činností či nekompletním provedením změn.[9]
- *dostupnost* - autorizované subjekty mohou na své vyžádání vykonat činnosti a není jim odepřen k činnosti přístup.[10] Vedoucí pracovníky často zajímá pouze zajištění dostupnosti informací, aby byla umožněna realizace plánovaných aktivit společnosti. Nezbytnost zajištění důvěrnosti a integrity si často uvědomí až při vzniku a řešení bezpečnostního incidentu.[11]

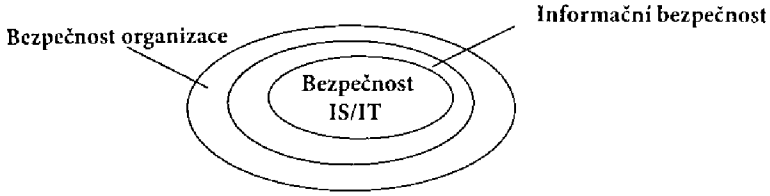
---

[5] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 5.
[6] tamtéž
[7] tamtéž
[8] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika.* s. 380.
[9] tamtéž
[10] tamtéž
[11] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 5.

2.2. Bezpečnost organizace

Smyslem zabezpečení organizace je snížit rizika a hrozby a předcházet bezpečnostním incidentům, které by ji mohly ohrozit. Pro celistvý pohled na bezpečnost existují normy ISO z řady 27 000, dle kterých budu i v této práci postupovat.

V souvislosti s termínem bezpečnost organizace a jejího IS, použitých ICT je nutné se zmínit ještě o dalších dvou pojmech, a to bezpečnost organizace nebo firmy a informační bezpečnost. Jejich vzájemné vztahy nadřízenosti a podřízenosti jsou znázorněny na obrázku.[12]



Obr. č. 2: Vztah úrovní bezpečnosti v organizaci[13]

Nejvyšší kategorií je bezpečnost organizace. Její součástí je zajištění bezpečnosti objektů, majetku organizace jako ostraha přístupů apod. Některé její činnosti napomáhají zároveň i zajištění bezpečnosti IS a ICT jako např. kontrola oprávnění fyzického přístupu do budov. Její součástí kromě jiných je i informační bezpečnost. Cílem a úkolem řízení informační bezpečnosti je shrnout v sobě zásady bezpečné práce s informacemi všeho druhu a všech typů - tedy nejen s informacemi v digitální formě. Informační bezpečnost zahrnuje navíc proti bezpečnosti IS a ICT i způsob zpracování uložení a správy archivu nedigitálních dat, zásady skartace materiálů, nakládání s informacemi během jejich transportu na jiná místa, zásady pro poskytování informací novinářům, zásady pro veřejná vystupování pracovníků organizace apod. Samotná bezpečnost IS a ICT má za úkol chránit pouze ta aktiva, která jsou součástí informačního systému organizace podporovaného informačními a komunikačními technologiemi.[14]

[12] POŽÁR, Josef. *Manažerská informatika*. s. 254.
[13] tamtéž
[14] tamtéž

2.2.1. Bezpečnost v informatice

Problematika informační bezpečnosti patří, vzhledem ke standardizaci a nárůstu objemu výměny dat pomocí komunikačních sítí, k velmi aktuálním tématům. Organizace musí informační systémy zabezpečovat stejně jako kterékoli své investice. Celá oblast bezpečnosti a jejího zajištění je poměrně komplikovaná záležitost a skládá se z mnoha kroků a činností.[15]

Obr. č. 3: Oblasti řešení bezpečnosti[16]

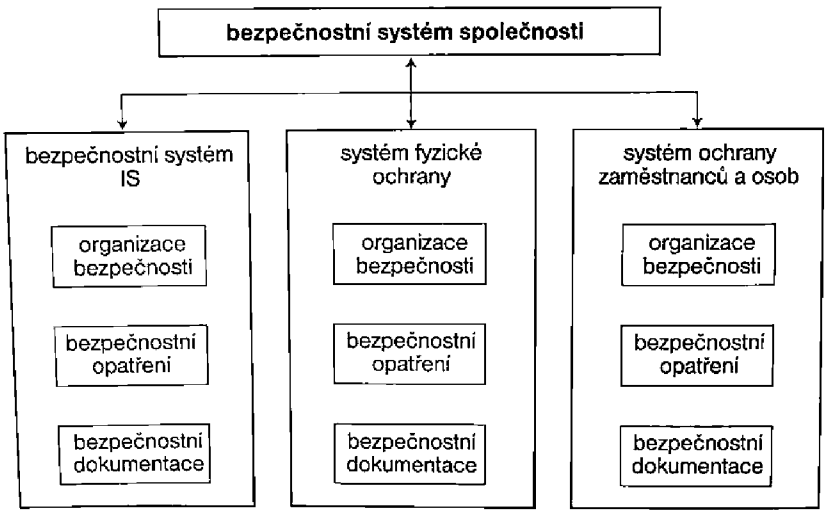
Obrázek ukazuje, že zajištění bezpečnosti IS/ICT se v různé míře promítá do řešení:

- bezpečnosti objektové, kde je řešena ochrana budov a prostor, tj. jejich ostraha včetně zajištění požární a další ochrany;
- bezpečnosti a ochraně zdraví při práci (BOZP), kde v závislosti na podmínkách a charakteru činnosti organizace dochází k zajištění ochrany zdraví pracovníků;
- bezpečnosti informační, zahrnující ochranu informačních aktiv organizace.[17]

Bezpečnostní cíle, celková bezpečnostní politika a veškeré aktivity v oblasti informační bezpečnosti musí být v souladu se strategickými cíli organizace. Procesy informační bezpečnosti jsou zaváděny s využitím modulu PDCA: plánování - zavedení - kontrola - využití. Informační bezpečnost se nedá zúžit jen na IS nebo ICT, ale musí se řešit všechny aspekty včetně organizačních procedur a chování jednotlivců. Informační bezpečnost je trvalý proces vzhledem k neustále probíhajícím změnám a nedá se zajistit na 100 % (vždy budou existovat nějaká zbytková rizika).[18]

[15] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika.* s. 377.
[16] tamtéž
[17] tamtéž
[18] POŽÁR, Josef. *Manažerská informatika*. s. 255.

Stále je však zapotřebí mít na paměti, že se jedná o součást celkové bezpečnosti společnosti a že ji nelze řešit izolovaně.[19]



Obr. č. 4: Schéma bezpečnostního systému společnosti[20]

2.3. PDCA model

Jde o metodu postupného zlepšování, která se dá použít téměř na cokoliv. Model obsahuje čtyři základní činnosti, které se stále opakují a tím dochází k neustálému zlepšování a rozvoji.[21]

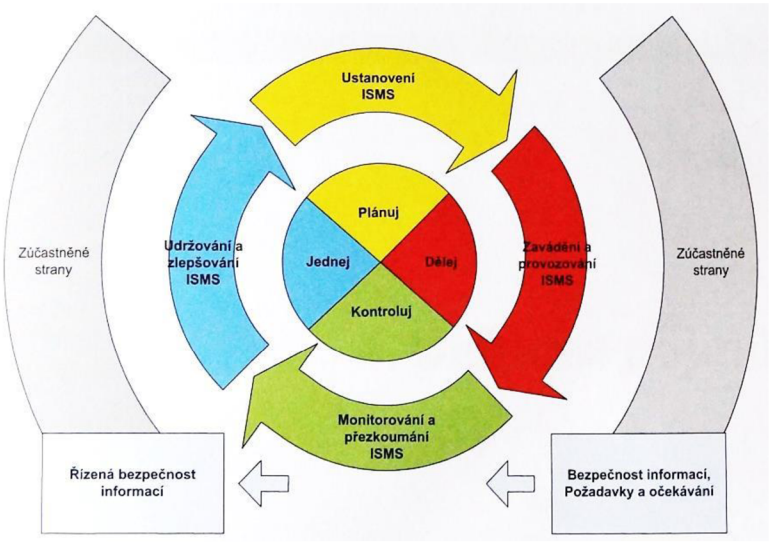
- Plan (plánuj) – naplánování zamýšleného zlepšení (záměr),
- Do (dělej) – realizace plánu,
- Check (kontroluj) – ověření výsledku realizace oproti původnímu záměru,
- Act (jednej) – úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe.[22]

Součástí modelu PDCA je také dokumentace každé jeho etapy, jako jedna z klíčových částí celého modelu.

[19] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. s. 11.
[20] tamtéž, s. 12.
[21] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*., s 24.
[22] tamtéž, s 25.

Procesy je třeba:

- identifikovat,
- popsat a zdokumentovat,
- řídit na základě dokumentace,
- následně optimalizovat jejich průběh.[23]



Obr. č. 5: Model PDCA v ISMS[24]

2.4. Definice ISMS

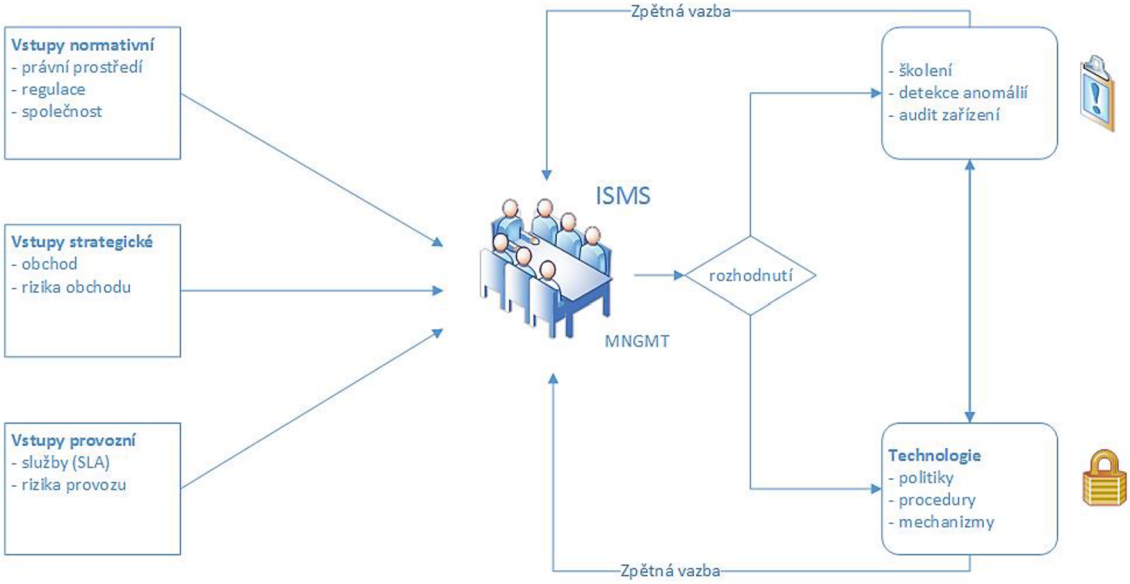
Již samotný název ISMS (Information Security Management Systém) napovídá, o co že se to vlastně jedná. Jedná se o Systém řízení informační bezpečnosti se všemi atributy, které to obnáší. Je třeba mít na paměti že ISMS je částí celkového systému řízení organizace.[25]

ISMS je v podstatě založeno na modelu PDCA a má následující čtyři etapy:

- Ustanovení ISMS (určuje rozsah a odpovědnosti)
- Zavádění a provoz ISMS (prosazení vybraných bezpečnostních opatření)
- Monitorování a přezkoumávání ISMS (zajištění zpětné vazby a hodnocení rizik)

[23] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*., s 25.
[24] tamtéž
[25] tamtéž, s. 14

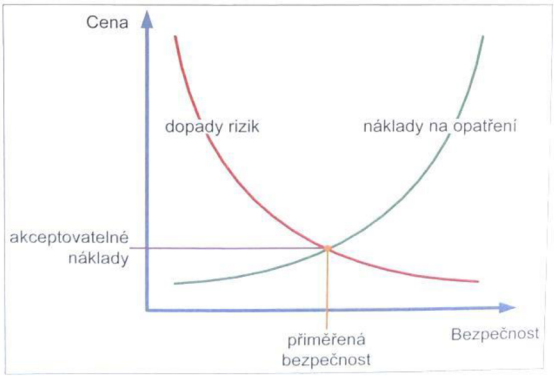
- Údržba a zlepšování (odstraňování slabin a soustavné zlepšování)[26]



Obr. č. 6: Struktura ISMS[27]

2.5. Přiměřená bezpečnost

Přiměřená bezpečnost vyjadřuje jakési optimum mezi bezpečností a vynaloženými prostředky. Vždy jde o to zvážit, jak velkou úroveň bezpečnosti skutečně potřebujeme, většinou máme totiž omezené zdroje. Na druhou stranu na bezpečnosti určitě není dobré šetřit.



Obr. č. 7: Graf přiměřené bezpečnosti za akceptovatelné náklady[28]

[26] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 14
[27] tamtéž, s. 15.
[28] tamtéž, s 36.

2.6. Normy a certifikace

Každá oblast lidské činnosti musí být řádně normalizována. Jen díky normám se mohou dorozumět informační systémy různých výrobců a různých zemí. Oblast počítačové bezpečnosti není výjimkou, i zde existují poměrně kvalitní normy.[29]

Existuje celá řada národních i mezinárodních organizací, které se vydáváním norem zabývají profesionálně a platí ve svém oboru za uznávanou autoritu. Řada norem těchto organizací je přebírána českým úřadem, samozřejmě po důsledném překladu do českého jazyka. S jakými normami se tedy můžete nejčastěji setkat:[30]

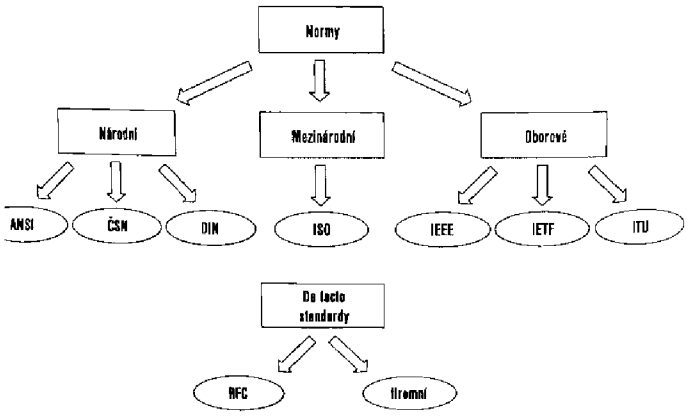
- **normy ISO:** vydává International Organisation for Standardisation
- **normy IEC:** vydává International Electrotechnical Commision
- **normy ITU:** vydává Mezinárodní telekomunikační unie[31]

Kromě těchto nadnárodních organizací existují národní úřady, které řadu těchto norem přebírají. Díky vývoji řady systémů v zahraničí se můžete nejčastěji setkat s těmito normami (například v dokumentaci):[32]

- **normy ANSI**: americké normy vydávané American National Standars Institute
- **normy DIN**: německý úřad Deutsche Institut for Normung[33]

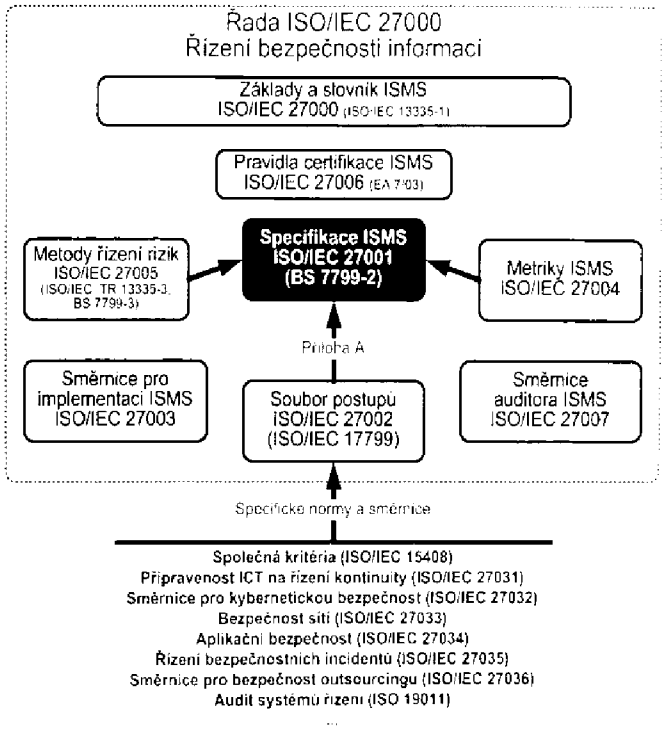
Existují také oborové organizace, které vydávají normy zaštítěné svou odbornou autoritou. Nejčastěji se sekáte s normami organizace IEEE (Institute of Eletrical and Electronics Engineers) či amerického NIST (National Institute for Standards and Technology).[34]

[29] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 17.
[30] tamtéž, s. 142.
[31] tamtéž
[32] tamtéž
[33] tamtéž
[34] tamtéž



Obr. č. 8: Struktura norem [35]

V České republice se normalizací zabývá Český normalizační institut (ČNI). Normy vydávané tímto úřadem nesou označení ČSN (Česká státní norma). Pokud se jedná o normu převzatou od některé mezinárodní organizace, zůstává i původní označení (samozřejmě je zachováno i původní číslování).[36]



Obr. č. 9: Vybrané normy řady ISO/IEC 27000[37]

[35] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 142.
[36] tamtéž, s. 143.
[37] DOUCEK, Petr. *Řízení bezpečnosti informací*. s. 83.

2.6.1. **ČSN ISO/IEC 27000**:2014 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Přehled a slovník

Tato mezinárodní norma poskytuje přehled systémů řízení bezpečnosti informací, které tvoří předmět rodiny norem ISMS a definuje související termíny. Termíny a definice uvedené v této normě se týkají termínů a definic obecně použitých v rodině norem ISMS, nikoliv všech termínů a definic. Rodina norem má pomoci organizacím všech typů a velikostí zavést a provozovat systém ISMS.[38]

2.6.2. **ČSN ISO/IEC 27001**:2013 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky

Norma poskytuje doporučení jak aplikovat vybraná opatření ISO/IEC 27002 v rámci procesu ustavení, provozu, údržby a zlepšování systému managementu bezpečnosti informací (Information Security Management Systém, ISMS) v organizaci. Norma prosazuje přijetí procesního přístupu k řešení ISMS a zavádí model známý jako Plánuj-Dělej-Kontroluj-Jednej (Plan-Do-Check-Act nebo zkratkou PDCA), který může být aplikován na všechny procesy ISMS tak, jak jsou definovány touto normou. Norma je propojena a harmonizována s normami ISO/IEC 9001:2000 a ISO/IEC 14001:2004 tak, aby bylo podpořeno jejich konzistentní a jednotné zavedení a provoz.[39]

V hlavní části normy jsou specifikovány požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a případnou certifikaci zdokumentovaného systému managementu bezpečnosti informací. Jsou zde specifikovány požadavky na výběr a zavedení bezpečnostních opatření chránících informační aktiva. V příloze jsou uvedeny cíle opatření a jednotlivá opatření, která jsou přímo propojena s cíly a opatřeními uvedenými v ISO/IEC 27002:20013.[40]

2.6.3. **ČSN ISO/IEC 27002**:2013 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů

Toto nové vydání mezinárodní normy obsahuje více než 114 strukturovaných oblastí doporučení rozdělených do 18 kapitol, ve kterých je obsaženo více než 5 000 přímých a

[38] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*., s 48.
[39] tamtéž, s 49.
[40] tamtéž

odvozených bezpečnostních opatření, podporujících dosahování podnikatelských cílů, přičemž odpovědnost za ně je možné jednoduše přiřadit osobám s odpovídajícími funkcemi. To umožňuje zjistit velmi rychle stav bezpečnosti informačního systému organizace a zároveň vytvořit východiska pro jeho zlepšení, zejména vymezením oblastí, které nejsou dostatečně zajištěny.[41]

2.6.4. **ČSN ISO/IEC 27005**:2011 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací

Tato mezinárodní norma poskytuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace, podporuje obecný koncept specifikovaný v ISO/IEC 27001 a je strukturována tak, aby dostatečně podporovala implementaci informační bezpečnosti založené na přístupu řízení rizik. Nicméně tato mezinárodní norma nenabízí konkrétní metodiku pro řízení rizik bezpečnosti informací. Záleží jen na organizaci, jaký přístup k řízení rizik zvolí, např. v závislosti na rozsahu ISMS, kontextu řízení rizik, průmyslovém odvětví. V souladu s přístupem k řízení rizik popsaným v této normě lze pro implementaci požadavků ISMS použít některou z celé řady existujících metodik pro řízení rizik.[42]

2.7. Bezpečnostní politika firmy

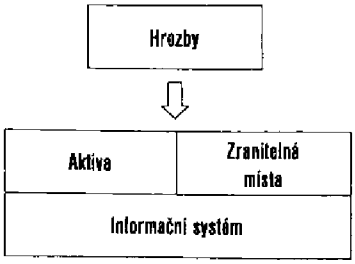
Základním dokumentem každé společnosti (z hlediska počítačové bezpečnosti) je takzvaná bezpečnostní politika. V každém případě by se mělo jednat o dokument písemný, ústní verze mají nepříjemný sklon k modifikaci, ať už chtěné či nechtěné. Bezpečnostní politika by měla odpovídat na několik základních otázek:[43]

- co chceme chránit
- proč to chceme chránit
- jak to chceme chránit
- jak ověříme, že je to opravdu chráněno
- co budeme dělat, když se něco pokazí[44]

---

[41] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*., s 49.
[42] tamtéž, s 51.
[43] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 168.
[44] tamtéž, s. 168.

V první řadě je tedy nezbytně nutné identifikovat, jaká data či jaké prostředky se v informačním systému firmy nacházejí. Ne všechna tato aktiva (souhrnné označení pro všechno cenné, co se v informačním systému nachází) je potřeba chránit, ne všechna je potřeba chránit stejně. Jak chceme konkrétní aktivum chránit, by mělo být odpovídat jeho hodnotě pro společnost.[45]

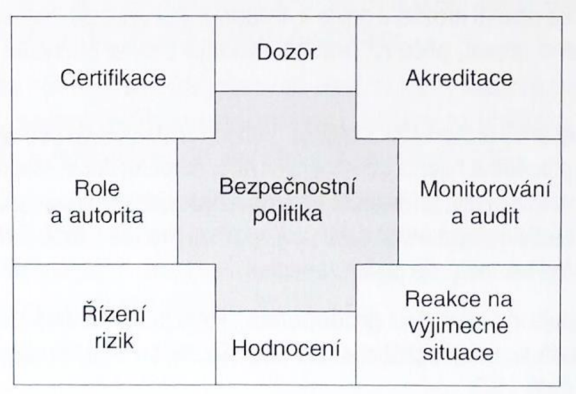


Obr. č. 10: Aktiva a hrozby[46]

Samotné zavedení bezpečnosti je jen první částí celého procesu. Předně je nutno správnost zavedení nějak zkontrolovat, abychom vyloučili úmyslné či neúmyslné lidské chyby. Kontrola by měla být prováděna periodicky, čímž zajistíme, že ochrana nebyla omylem či záměrně odstraněna, případně v kombinaci s jinými prostředky neztratila svou účinnost.[47]

Obrázek zachycuje základní přehled o obsahu řešení bezpečnosti IS/ICT. Vedle budování bezpečnostní politiky, patří k dalším významným úlohám analýza bezpečnostních rizik, návrh a implementace protiopatření, včetně implementace plánů pro řešení výjimečných situací. Tyto činnosti jsou zahrnuty do skupiny činností označených pojmem řízení rizik. Další činnosti se orientují na zajištění kontroly a auditu bezpečnosti a zahrnují monitorování, hodnocení, certifikaci a akreditaci bezpečnosti IS/ICT.[48]

[45] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 168.
[46] tamtéž
[47] tamtéž, s. 169.
[48] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika.* s. 380.



Obr. č. 11: Obsah řešení bezpečnosti IS/ICT[49]

Jaký stupeň zajištění bezpečnostních požadavků má být na konkrétní IS/ICT aplikován, definuje tzv. bezpečnostní politika.[50]

2.7.1. Obsah bezpečnostní politiky

Samotná bezpečnostní politika by neměla zůstat statickým dokumentem. Prostředí, ve kterém je informační systém umístěn, se v průběhu času mění. Je třeba čelit jiným hrozbám, chránit jiná aktiva a podobně. Sebelepší bezpečnostní politika by měla být čas od času aktualizována.[51]

Aby bylo prosazování bezpečnostních opatření snazší, měla by být celá politika vysvětlena kompletnímu vedení společnosti (tedy vedoucím jednotlivých oddělení). S bezpečnostní politikou se musí všichni dokonale ztotožnit a pochopit, proč se konkrétní věci provádějí konkrétním způsobem.[52]

2.7.2. Definice základních pojmů

Jako **informační systém** označujeme skupinu počítačů, serverů, disků a jiných záznamových médií, propojovacích a síťových kabelů, instalovaných programů a používaných dat. Je to zkrátka všechno, co běžní uživatelé většinou chápou pod pojmem „počítač".[53]

---

[49] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika.* s. 380.
[50] tamtéž, s. 380.
[51] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 169.
[52] tamtéž
[53] tamtéž

Informační bezpečnost (Information Security) jako obor zabývající se zabezpečením informací v informačních a komunikačních technologiích, lze chápat jako systém ochrany dat a informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, fyzických, technických, programových a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot.[54]

Aktivum (Asset). Nehmotný nebo hmotný statek mající v rámci IS určitou hodnotu.[55] Za nejcennější aktiva se považují peníze, majetek a především data a informace, jejichž zneužití, ztráta nebo modifikace by organizaci nebo osobě způsobily určitou škodu. Aktiva se dále dělí na hmotná a nehmotná[56]

Příklady aktiv jsou technické prostředky, softwarové prostředky, data, která informatika využívá a zpracovává, formalizované a neformalizované procesy a znalosti, které informatika zahrnuje, a také osoby, především provozní personál, jako jsou správci jednotlivých aplikací, komunikačních prostředků a další pracovníci oddělení informatiky.[57]

Bezpečnost (Security). Pod pojmem bezpečnost chápeme vlastnost nějakého objektu anebo subjektu (informačního systému či technologie), která určuje stupeň, míru jeho ochrany proti možným škodám a hrozbám.[58]

Citlivá data (Sensitive Data) jsou data informace, které vyžadují ochranu, poněvadž vždy existuje jistá pravděpodobnost působení hrozeb. V IS se především jedná o personální data, chráněná zákony, a o informace týkající se chodu organizace jako finanční agendy, informace o činnosti atd.[59]

Hrozba (Threat). Akce nebo událost, která může způsobit, že informace nebo zdroje zpracovávající informace budou záměrně nebo náhodně ztraceny, modifikovány, kompromitovány, stanou se nedostupnými nebo budou jinak negativně ovlivněny

---

[54] POŽÁR, Josef. *Manažerská informatika*. s. 252.
[55] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 17.
[56] POŽÁR, Josef. *Manažerská informatika*. s. 252.
[57] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika.* s. 377.
[58] POŽÁR, Josef. *Manažerská informatika*. s. 252.
[59] tamtéž

k újmě obchodní společnosti.[60] Hrozba může ohrozit bezpečnost (např. přírodní katastrofa, hacker, zaměstnanec aj.).[61]

Dokud zůstane hrozba hrozbou, je vše v pořádku. Vždy však musíme počítat s tím, že hrozba bude naplněna - v tomto případě už hovoříme o útoku.[62]

Ocenění rizik (Risk Assessment) je proces vyhodnocení hrozeb, které působí na informační systém, s cílem definovat úroveň rizika, kterému je systém vystaven. Cílem je zjištění, jsou-li bezpečnostní opatření dostatečná, aby snížila pravděpodobnost vzniku škody na přijatelnou úroveň. [63]

Riziko (Risk) je pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty.[64] Vyjadřuje tedy míru ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škod. [65]

Útokem, který nazýváme rovněž bezpečnostní incident, rozumíme buďto úmyslné využitkování zranitelného místa, tj. využití zranitelného místa ke způsobení škod/ztrát na aktivech IS, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. Při analýze možných forem útoků na IT je třeba typicky řešit problémy typu: jak se projevuje počítačová kriminalita, jaké jsou možné formy útoků, kdo útočí, kdo může páchat počítačový zločin, jaká rizika souvisí s používáním informačních technologií, jak se chránit před útoky apod. Útočit lze přerušením, odposlechem, změnou či přidáním hodnoty k datům.[66]

Zranitelnost (Vulnerability). Slabé místo IS pro bezpečnost hodnoceného aktiva (které vznikne například jako důsledek nedostatků v analýzách, návrzích, implementaci nebo provozu).[67] Každé aktivum je zranitelné, protože jeho hodnotu ohrožují různé vlivy.[68]

---

[60] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 17.
[61] POŽÁR, Josef. *Manažerská informatika*. s. 252.
[62] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 170.
[63] POŽÁR, Josef. *Manažerská informatika*. s. 252.
[64] tamtéž, s. 253.
[65] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 17.
[66] POŽÁR, Josef. *Manažerská informatika*. s. 253.
[67] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 18.
[68] POŽÁR, Josef. *Manažerská informatika*. s. 253.

Úroveň zranitelnosti aktiva se hodnotí podle jeho citlivosti, tj. náchylnosti aktiva, tj. že může být poškozeno, a kritičnosti, tj. důležitosti aktiva pro IS/ICT.[69]

Zranitelné místo. Slabinu informačního systému využitelnou ke způsobení škod nebo ztrát útokem na IS nazýváme zranitelné místo. Existence zranitelných míst je důsledek chyb, selhání v analýze, v návrhu a/nebo v implementaci IS, důsledek vysoké hustoty uložených informací, složitosti softwaru, existence skrytých kanálů pro přenos informace jinou než zamýšlenou cestou apod.[70]

Zranitelné místo je vlastně vždy jednou z vlastností IS/ICT. Takové zranitelné místo může být:[71]

- Fyzické, kdy je prvek IS/ICT fyzicky umístěn v prostředí, ve kterém může snadno dojít k jeho poškození, zničení či ztrátě.
- Přírodní, kdy prvek IS/ICT nemá schopnost se vyrovnat s některými objektivními faktory, jako je záplava, požár, blesk apod.
- Technologické, kdy prvek IS/ICT svými konstrukčními charakteristikami neumožňuje zajistit např. požadovaný trvalý plynulý provoz.
- Fyzikální, kdy prvek IS/ICT pracuje na takových fyzikálních principech, které umožňují jejich zneužití. Příkladem může být elektromagnetické vyzařování některých komponent, jako jsou monitory, kabeláž komunikační sítě apod,
- Lidské, kdy prvek IS/ICT je ohrožen působením lidí, jejich omylů a neznalosti.[72]

Útok na zranitelné místo označujeme termínem **bezpečnostní incident** („security incident"), což je jakákoli událost, která vede k porušení definovaných pravidel a postupů při provozování IS/ICT, včetně pokusů o tato porušení. Zároveň je za bezpečnostní incident označována jakákoli událost, která vede k ohrožení nastavených bezpečnostních vlastností. Hrozby a zranitelná místa využívají útočníci k vedení svého útoku.[73]

---

[69] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika.* s. 379.
[70] POŽÁR, Josef. *Manažerská informatika*. s. 253.
[71] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika.* s. 378.
[72] tamtéž
[73] tamtéž, s. 379.

Útočníkem může být osoba uvnitř organizace, nebo může jít o osobu mimo organizaci. Útok může mít jasný úmysl, nebo se jedná o neúmyslný útok. V případě osob, které realizují úmyslné útoky, se požívá pro jejich označení několik termínů, zejména:[74]

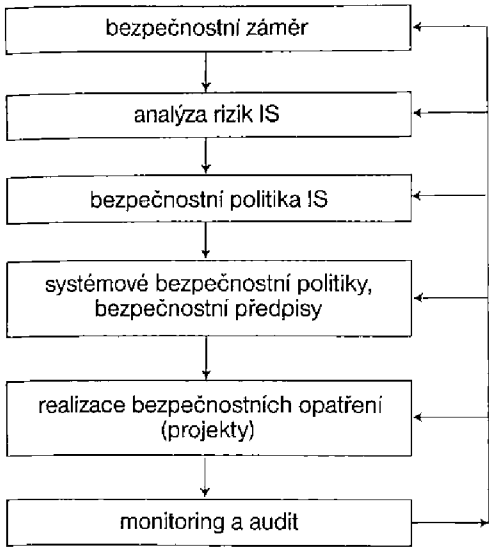
- Hacker - bere útok jako výzvu a prostředek získání prestiže.
- Vyzvědač („spy") - provádí útoky za účelem zisku informací, které jsou využívány pro různé politické účely.
- Terorista („terrorist") - provádí útoky za účelem vyvolání obavy a strachu.
- Kriminálník („criminal") - útočí na systémy pro svůj osobní finanční zisk.
- Vandal („vandal") - útočí na systémy s cílem systém zničit či poškodit.
- Cracker, zpravidla programátor - snaží se proniknout do systémů jiných vlastníků za účelem jejich krádeže. Typicky se orientuje na krádež duševního vlastnictví, tj. těch částí systémů, které jsou chráněny autorským zákonem.
- Phracker - jeho cílem je získání bezplatného přístupu k telefonním službám.
- Phreaker - jeho cílem jsou telekomunikační informace, které mu umožňují získávat přístup k dalším počítačům.[75]

Bezpečnostní opatření - prostředek sloužící ke zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby.[76] Vlastní opatření, která realizují zabezpečení aktiv, mohou být různého charakteru.[77]

[74] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika.* s. 379.
[75] tamtéž
[76] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 18.
[77] tamtéž, s. 11.

2.8. Postup realizace zabezpečení elektronických informací

Zavedení systémového zabezpečení IS je realizováno v několika návazných níže uvedených krocích (viz obrázek).[78]



Obr. č. 12: Proces zabezpečení IS[79]

2.8.1. Bezpečnostní záměr

Aby mohlo být ve společnosti postupně realizováno zabezpečení IS, musí být vedením společnosti tímto úkolem pověřen určitý útvar. Dále je nezbytným předpokladem úspěšného budování bezpečnostního systému podpora nejvyššího vedení (skutečná, nikoliv pouze formální, alibistická).[80]

Pověřený útvar zpracuje a předloží nejvyššímu vedení společnosti ke schválení dokument nazvaný bezpečnostní záměr. Tento dokument může být velmi stručný (rozsahem jedna až dvě strany formátu A4) a mělo by v něm být deklarováno, jakým způsobem bude informační bezpečnost řešena, jaký je cílový stav a jakým způsobem bude tohoto stavu dosaženo. Základním cílem každé společnosti je zamezení zneužití, neoprávněné modifikace, poškození, nedostupnosti a zničení informací za účelem minimalizace negativních dopadů. Dokument může případně obsahovat vybrané okruhy informací, které budou zabezpečeny (například z důvodu omezených finančních

[78] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. s. 13.
[79] tamtéž, s. 14.
[80] tamtéž

možností, dislokace některého pracoviště, z potřeby zabezpečit pouze vybranou skupinu informací).[81]

2.8.2. Analýza rizik

Na základě schválených cílů a postupů k dosažení bezpečnostního systému IS v dokumentu bezpečnostní záměr je potřebné, aby společnost zmapovala skutečný stávající stav v oblasti bezpečnosti IS. Proto je zapotřebí provést analýzu rizik IS z pohledu bezpečnosti. Analýzu rizik IS je nutno provádět odborníky. Rozhodně nedoporučujeme její provedení pouze vlastními zaměstnanci, kteří v dané oblasti nemají žádné praktické zkušenosti. Firmy obvykle provedení analýzy rizik IS řeší formou projektu, jehož řešitelský tým je složen z pracovníků externí specializované firmy v dané oblasti a vlastních pracovníků společnosti, o nichž se předpokládá, že budou členy útvaru řešícího bezpečnost IS a že budou v budoucnu provádět následné analýzy rizik.[82]

Výstupními materiály analýzy rizik je zpráva, která popisuje daný stav bezpečnosti v IS, obsahuje popis existujících bezpečnostních rizik a obvykle i návrh bezpečnostních opatření k eliminaci rizik na přijatelnou úroveň pro firmu.[83]

2.8.3. Bezpečnostní politika IS (dále BPIS)

V souladu se závěry analýzy rizik je vypracována BPIS. Tento dokument definuje východiska pro všechny další aktivity společnosti v oblasti informační bezpečnosti. Po schválení nejvyšším vedením obchodní společnosti je BPIS závazná pro všechny zaměstnance společnosti a pro pracovníky externích společností, kteří využívají IS dané společnosti.[84]

2.8.4. Systémové bezpečnostní politiky IS

Základní bezpečnostní principy a zásady obsažené v BPIS je zapotřebí rozpracovat podrobněji v systémových bezpečnostních politikách a v ostatních bezpečnostních předpisech.[85]

---

[81] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 14.
[82] tamtéž, s. 15.
[83] tamtéž
[84] tamtéž
[85] tamtéž

2.8.5. Bezpečnostní opatření

Zajištění postupné realizace doporučených bezpečnostních opatření, vyplývajících ze závěrů analýzy rizik IS a která jsou v souladu se zásadami platné BPIS, u některých opatření není náročná ani finančně, ani požadavky na lidské zdroje (například nastavení bezpečnostních parametrů operačního systému pro daný server), realizace jiných opatření může být nákladnější a často bývají řešeny formou projektů (za případné účasti specializované externí firmy).[86]

2.8.6. Monitoring a audit

Po zavedení bezpečnostních opatření je zapotřebí provádět kontrolu a audit stavu zabezpečení a dle potřeby odstraňovat zjištěné nedostatky.[87]

2.8.7. Akceptování nových potřeb zabezpečení IS

IS každé společnosti se průběžně mění především v důsledku změn v obchodních aktivitách společnosti a změn způsobených v důsledku rychlého vývoje informačních technologií. Proto je zapotřebí, aby společnost prováděla periodicky analýzy rizik IS, aktualizovala politiky a realizovala potřebná bezpečnostní opatření.[88]

2.9. Bezpečnostní hrozby

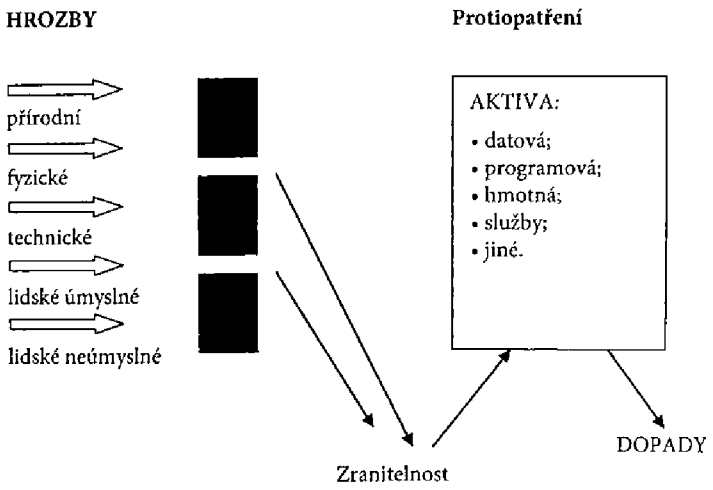
Hrozba má potenciální schopnost způsobit nežádoucí incident, který může mít za následek poškození systému nebo organizace a jejich aktiv.[89]

Pod hrozbou se pak také označuje jakákoliv okolnost či událost působící na zranitelné místo aktiva, která může způsobit potenciální škodu na aktivu.[90]

Základní schéma zajištění bezpečnosti IS a ICT představuje vztahy mezi aktivy organizace, hrozbami, které na ně mohou potenciálně působit, možnou zranitelností aktiv reálnými hrozbami, dopady reálných hrozeb na tato aktiva a možnostmi ochrany aktiv organizace formou bezpečnostních opatření.[91]

---

[86] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 16.
[87] tamtéž
[88] tamtéž
[89] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 86.
[90] POŽÁR, Josef. *Manažerská informatika*. s. 255.
[91] tamtéž, s. 256.



Obr. č. 13: Schéma zajištění bezpečnosti IS a IT - aktiva a hrozby[92]

Hrozby obvykle neexistují izolovaně, často se jedná o kombinace hrozeb, které představují riziko pro daný subjekt. Při provádění analýzy rizik je zapotřebí určit priority z pohledu dopadu a pravděpodobnosti jejich výskytu a zaměřit se na klíčové rizikové oblasti.[93]

2.9.1. Základní rozdělení hrozeb

Hrozby lze dělit podle hledisek zejména na:

- **přírodní a fyzické** (živelné pohromy a nehody, jako jsou např. poruchy v dodávce elektrického proudu, požáry, povodně apod.);
- **technické** (poruchy nosičů a počítačů, poruchy sítí);
- **technologické** (poruchy způsobené programy - viry, trojské koně apod.);
- **lidské**, tj.:
    - **neúmyslné,** které vyplývají z neznalosti, omylů nebo zanedbání;
    - **úmyslné,** které rozdělujeme na působící:
        - **zvenku systému** (hacker, terorista, špionáž apod.),
        - **zevnitř** (zlomyslní, zneuznaní, chamtiví zaměstnanci, hosté a návštěvníci organizace apod.).[94]

[92] POŽÁR, Josef. *Manažerská informatika*. s. 257.
[93] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 18.
[94] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika.* s. 381.

Pro úplnost je však třeba se zmínit o typických hrozbách, které mohou přicházet z internetu. Jsou to zejména tato rizika:

- hackeři, kteří způsobují jen 15-20 % prokázaných útoků na internetu;
- snadná možnost odposlechu - napíchnutí (wiretapping) na přenos a zneužití obsahu zprávy;
- krádež identity (Identity Theft) - získání adresy odesílatele, vydávání se za někoho jiného;
- neautorizované programy a možnost jejich modifikace, tzv. cracking;
- distribuce virů a červů;
- odmítnutí služby např. zahlcení elektronickou poštou, kdy je zahlcena služba či disková kapacita;
- dynamická změna hrozeb;
- hoaxy a spamy;
- spyware aj.[95]

Převážná většina hrozeb (více jak 50 % všech) patří do kategorie neúmyslných hrozeb. Mezi základní hrozby patří neoprávněné, náhodné nebo úmyslné:[96]

- **prozrazení** tajných informací - bezpečný systém nemůže povolit přístup nikomu (osobě, programu, zařízení), aniž by proběhla jejich autorizace;
- **upravení -** bezpečný systém pak musí zajistit, že nedojde k porušení integrity dat neautorizovaným, náhodným nebo úmyslným způsobem;
- **zničení -** bezpečný systém nesmí dovolit neautorizované zničení informací;
- **bránění** v dostupnosti informačního systému autorizovaným uživatelům - bezpečný systém nesmí dovolit, aby bylo autorizovaným uživatelům bráněno ve využití informačního systému a jeho zdrojů.[97]

[95] POŽÁR, Josef. *Manažerská informatika*. s. 259.
[96] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika.* s. 381.
[97] tamtéž

2.9.2. Posouzení hrozeb

Posouzení hrozeb provádíme vždy v závislosti na následujících otázkách:

- ztráta důvěrnosti - může vést například ke ztrátě důvěry vůči zákazníkům, právní odpovědnosti, ohrožení osobní bezpečnosti nebo finanční ztrátě;
- ztráta integrity - může vést například k přijetí nesprávných rozhodnutí, narušení
- funkčnosti organizace;
- ztráta dostupnosti - může vést například k neschopnosti vykonávat kritické činnosti organizace;
- ztráta individuální odpovědnosti - může vést například k podvodu, špionáži, krádeži;
- ztráta autentičnosti - může vést například k použití neplatných dat, která vedou k neplatným výsledkům;
- ztráta spolehlivosti - může vést například k nespolehlivým dodavatelům, demotivaci zaměstnanců.[98]

Nesmíme však nikdy zapomenut na tzv. následné efekty hrozby. Například výpadek elektrické energie neznamená jen nedostupnost dat, ale může vést při dlouhodobém výpadku k ohrožení činnosti organizace, případně i ohrožení fyzické integrity člověka (nemocnice, hasiči, policie). Vždy je třeba promyslet možné dopady hrozeb do nejmenších podrobností.[99]

2.10. Bezpečnostní incident

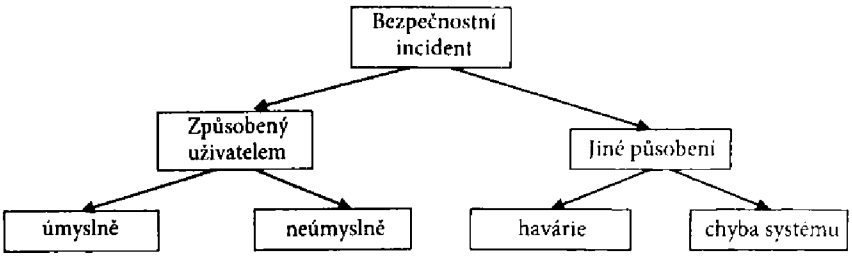
Poškození či ztráta datových souborů, delší vyřazení systému z provozu, rozšíření počítačových virů v síti nebo průnik do informačního systému je třeba považovat za bezpečnostní incident. Tato událost je vždy provázena informačními ztrátami. Po zjištění bezpečnostního incidentu je třeba vyšetřit jeho příčinu, podrobně analyzovat situaci s cílem zjištění zdrojů infiltrace a uvedení informačního systému do důvěryhodného stavu. Současně s odstraněním důsledků je třeba uskutečnit i opatření

[98] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 86.
[99] tamtéž

zamezující možnosti opakování tohoto jevu. Obecně by se při šetření bezpečnostního incidentu mělo postupovat následovně:[100]

- zjistit zdroj, podezření na napadení systému je nutné ihned hlásit;
- zajistit důkazy podrobným šetřením, všechny diskriminované účty musejí ihned změnit přístupová hesla;
- zjistit možnosti fyzického přístupu ke zdroji a osobní odpovědnost pracovníků;
- zpracovat protokol s osobami, které by, mohly nebo neměly být účastníky incidentu;
- po důkladném prošetření vyvodit disciplinární nebo kázeňská opatření s viníky, eventuálně ocenit přístup osob, které zabránily větším ztrátám apod.;
- přijmout technická, režimová a jiná preventivní opatření v informačním systému a na příslušných pracovištích.[101]

Bezpečnostní incidenty, které mohou být buď způsobené uživatelem, nebo vnějším i vnitřním působením, útokem jsou znázorněny na obrázku.



Obr. č. 14: Bezpečnostní incidenty[102]

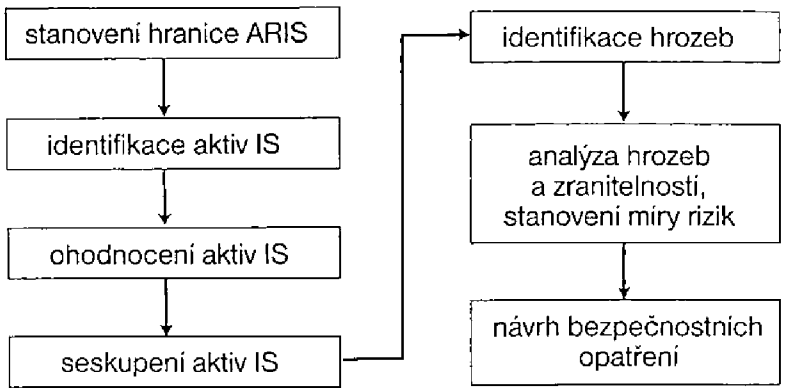
2.11. Analýza rizik

Při sestavování vlastní bezpečnostní politiky musí být nejprve provedena analýza rizik. Musíme tedy zjistit, co a proti čemu (tedy jaká aktiva proti jakým hrozbám) chceme chránit.[103]

[100] POŽÁR, Josef. *Manažerská informatika*. s. 259.
[101] tamtéž
[102] tamtéž, s. 260.
[103] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 170.

Analýza rizik slouží k odhadu ztrát, jež mohou vzniknout působením hrozeb na IS, a dává přehled o stupni nebezpečnosti jednotlivých hrozeb, slabých místech (zranitelnosti) hodnoceného IS a rizicích, jimž je hodnocený systém vystaven.[104]

V průběhu realizace každé podrobné analýzy rizik se provádějí obvykle na sebe navazující kroky znázorněné na obrázku.[105]



Obr. č. 15: Obecný postup realizace ARIS[106]

Hrozby obvykle neexistují izolovaně, často se jedná o kombinace hrozeb, které představují riziko pro daný subjekt. Při provádění analýzy rizik je zapotřebí určit priority z pohledu dopadu a pravděpodobnosti jejich výskytu a zaměřit se na klíčové rizikové oblasti.[107]

P - Pravděpodobnost vzniku a existence rizika

1) Nahodilá.
2) Nepravděpodobná.
3) Pravděpodobná.
4) Velmi pravděpodobná.
5) Trvalá.[108]

[104] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 18.
[105] tamtéž
[106] tamtéž, s. 19.
[107] tamtéž, s. 18.
[108] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 90.

R - Míra rizika

1) 0-10: Bezvýznamné riziko.
2) 11-20: Akceptovatelné riziko.
3) 21-30: Mírné riziko.
4) 31-60: Nežádoucí riziko.
5) 61-120: Nepřijatelné riziko.[109]

2.11.1. Stanovení hranic revize

Stanovení hranic revize bude provedeno ještě před identifikací a hodnocením aktiv. Pečlivá definice hranic nám umožní vyvarovat se zbytečných činností. Jinými slovy budeme definovat, kterých prvků se bude analýza rizik týkat, například aktiva IT (HW, SW, data a služby). [110]

2.11.2. Identifikace aktiv

Tento krok má jediný úkol - zjistit, jaká aktiva se v informačním systému vyskytují a jakou mají pro společnost hodnotu. Seznam aktiv je vhodné kompletovat v úzké spolupráci s oddělením IT. Jeho pracovníci velmi dobře vědí (nebo mají možnost to snadno zjistit), jaká data ukládají uživatelé na disky.[111]

Identifikace spočívá ve vytvoření seznamu aktiv, které leží uvnitř hranice analýzy rizik. Bude se tedy jednat o následující aktiva:[112]

a) informace (databáze, sestavy dat, dokumenty);
b) hardware - servery, pracovní stanice, směrovače, tiskárny, kabely;
c) software - operační systémy, aplikační programy;
d) budovy a místnosti, v nichž se aktiva typu a) až c) fyzicky nacházejí.[113]

Aby se dalo provést ohodnocení aktiv, je třeba nejprve aktiva identifikovat. V této etapě se doporučuje:[114]

---

[109] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 90.
[110] tamtéž, s. 93.
[111] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 171.
[112] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 19.
[113] tamtéž

- seskupit všechna aktiva, která k sobě logicky patří (programová aktiva, bezpečnostní aktiva, obchodní aktiva, služby apod.);
- identifikovat vlastníka každého daného aktiva (vlastníkem aktiva rozumíme přímo pověřenou osobu, plně odpovědnou za toto aktivum, s tímto vlastníkem se posléze určuje konkrétní hodnotu aktiva).[115]

2.11.3. Ohodnocení aktiv

Ve chvíli, kdy budeme mít identifikovaná aktiva, musíme k nim přiřadit hodnoty. Tyto hodnoty reprezentují význam aktiv pro činnost organizace. Vstupní údaje pro hodnocení aktiv budou zajištěny vlastníky a uživateli aktiv, například formou dotazníku, případně pomocí interview.[116]

Stanovení ohodnocení fyzických aktiv není obtížné, určíme ho na základě pořizovací ceny nového aktiva s přibližně stejnými parametry jako oceňované aktivum (takto lze odhadnout například cenu počítačového serveru).[117]

Při hodnocení aktiva bereme v úvahu celou řadu hledisek, např. nákupní nebo vývojové náklady, důležitost aktiva pro chod celého IS/ICT, cenu zpracovávaných informací, náklady na překlenutí případné škody na aktivu a samozřejmě i další hlediska, která mohou být specifická případ od případu.[118]

Dalším logickým krokem je stanovit stupnici a hodnotící kritéria, která budou použita k přiřazování ohodnocení určitého aktiva. Tato stupnice může být vyjádřena penězi nebo kvalitativními hodnotami.[119]

---

[114] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 82.
[115] tamtéž
[116] tamtéž, s. 93.
[117] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací.* s. 20.
[118] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika.* s. 378.
[119] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 82.

Příklad typické tabulky s termíny pro kvalitativní hodnocení (při napadení aktiva) jsou.

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

Obr. č. 16: Příklad hodnocení aktiv[120]

Důležité je také barevné odlišení. Máme-li mít rozsáhlé tabulky s hodnocením aktiv, pomohou vhodně zvolené barvy k jednodušší orientaci. Výběr a rozsah termínů, které si organizace zvolí, závisí na bezpečnostních potřebách organizace, její velikosti apod.[121]

2.11.4. Výpočet hodnoty aktiva

Pro výpočet ohodnocení aktiva je možno využít různé postupy. Nejjednodušším a také nejpoužívanějším je tzv. součtový algoritmus.[122]

Principem je součet: (Dostupnost + Důvěrnost + Integrita) /3.

2.11.5. Identifikace hrozeb

Mnohem složitější je identifikace hrozeb, které aktivům v informačním systému hrozí. Seznam hrozeb se navíc poměrně dynamicky vyvíjí, je tedy vysoká šance, že pokaždé na něco zapomeneme. K identifikaci hrozeb lze přistupovat několika způsoby. S největší pravděpodobností zvolíte ten první - intuitivní vyhledávání rizik.[123]

Jeho základem je důkladné přemýšlení nad všemi situacemi, které mohou v informačním systému nastat. Co když útočník provede to a to? A co když pronikne do serverovny voda? S největší pravděpodobností se při takovém přístupu na něco zapomene, což se podle Murphyho zákonů projeví v nejnevhodnější situaci. Pak nezbývá, než seznam hrozeb aktualizovat.[124]

---

[120] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 82..
[121] tamtéž, s. 83.
[122] tamtéž
[123] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 171.
[124] tamtéž, s. 171.

Druhým způsobem je inspirace jinými seznamy hrozeb. Pokud zvolíme seznam, který byl vytvořen pro podobné prostředí, může být úspěšnost poměrně vysoká. I zde sice hrozí jisté riziko omylu, není ale rozhodně tak vysoké.[125]

Třetím způsobem je využití podrobných dotazníků. Pro různé části prostředí jsou vytvořeny vysoce komplexní dotazníky. Při identifikaci rizik pak bezpečnostní expert prochází otázku za otázkou a zjišťuje, jak je na tom jeho systém v jeho prostředí. Výhodou tohoto přístupu je jeho vysoká kvalita — při dobře navrženém dotazníku jen stěží na něco zapomenete. Nevýhodou je poměrně vysoká časová náročnost a hlavně nedostupnost dotazníků.[126]

2.11.6. Hodnocení hrozeb

Hrozba představuje možnost poškodit zkoumaný systém IT a jeho aktiva. Hrozby mohou být přírodního nebo lidského původu a mohou být úmyslné nebo náhodné. Jako základní katalog hrozeb lze využít seznam uvedený v normě ČSN ISO/IEC TR 13335-3 v příloze C. Hodnocení hrozeb bude dáno do souvislosti s identifikovanými aktivy společnosti.[127]

2.11.7. Odhad zranitelnosti

Tento odhad odhalí slabá místa ve fyzickém prostředí, organizaci, postupech, personálu managementu, administraci HW, SW, nebo komunikačním zařízení, která mohou být využita zdrojem hrozby a způsobit tak škodu na aktivech.[128]

2.11.8. Vlastní analýza rizik

Nyní máme k dispozici dva seznamy - seznam aktiv, která se v systému vyskytují včetně jejich finančního ohodnocení, a seznam hrozeb, které informačnímu systému v daném prostředí hrozí. Úkolem analýzy rizik je nyní zjistit, jaká nebezpečí konkrétním aktivům hrozí.[129] Postupně tedy procházíme jednotlivá aktiva a rozhodujeme, které hrozby se na konkrétní aktivum vztahují.[130]

---

[125] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 171.
[126] tamtéž, s. 172.
[127] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 93.
[128] tamtéž
[129] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 172.
[130] tamtéž

Výsledkem je seznam aktiv, kterým jsou přiřazeny jednotlivé hrozby. Každé konkrétní dvojici aktivum-hrozba lze přiřadit pravděpodobnost, s jakou ke konkrétní hrozbě k danému aktivu dojde. Můžeme tedy kvalifikovaně rozhodnout, proti jaké pravděpodobnosti hrozeb budeme náš informační systém chránit.[131]

2.11.9. Identifikace plánovaných a existujících ochranných opatření

Součástí analýzy rizik je tzv. identifikace plánovaných nebo existujících bezpečnostních opatření. Výsledkem tohoto krokuje je seznam všech existujících a všech plánovaných bezpečnostních opatření.[132]

2.11.10. Výběr ochranných opatření

V předchozích krocích jsme zjistili, jakou hodnotu mají aktiva v našem informačním systému. Odhadli jsme také pravděpodobnost hrozeb a stanovili hranici pravděpodobnosti hrozeb, proti kterým se budeme chránit. Konkrétní hodnota této hranice závisí na finanční hodnotě chráněných aktiv.[133]

Princip ochranných opatření spočívá v minimalizaci případných rizik. Aby se usnadnil popis různých typů ochranných opatření, jsou v rámci normy zavedeny kategorie ochranných opatření. Mezi základní kategorie patří:[134]

- řízení a politiky bezpečnosti IT,
- kontrola bezpečnostní shody,
- řešení incidentů,
- personální opatření,
- provozní problémy,
- plánování kontinuity činnosti organizace,
- fyzická bezpečnost.[135]

Posledním krokem je navržení jednotlivých opatření. Opatření by měla být navržena pro každou dvojici aktivum-hrozba, často ale dojde k situaci, kdy jeden

---

[131] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 172.
[132] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 93.
[133] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 172.
[134] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 93.
[135] tamtéž

použitý bezpečnostní prostředek zajistí ochranu více takových dvojic. Jako ideální způsob návrhu se tedy jeví postup shora dolů. U každé dvojice navrhneme odpovídající opatření a vyčíslíme náklady na jeho zavedení a udržování.[136]

2.11.11. Odhad rizik

Cílem tohoto kroku je identifikovat a odhadnout rizika, kterými jsou aktiva vystavena. Tedy jednoduše řečeno, musíme zjistit, co nám hrozí a proč nám ta rizika hrozí.[137]

2.11.12. Přijetí rizik

Po identifikaci a odhadu rizik, po výběru a revizi ochranných opatření však vždy zůstávají tzv. zbytková rizika. Úplně bezpečný systém je pouze teoretická hypotéza, ke které se lze v reálném provozu pouze limitně blížit. Zbytková rizika mohou být rozdělena a být buď akceptována (akceptace rizika) nebo neakceptována. Jestliže riziko není akceptováno, probíhá znovu výběr ochranných opatření a odhadování rizik. Je zde vysoké riziko, že může být přijato dodatečně ochranné opatření, které je příliš nákladné nebo z hlediska bezpečnosti zbytečné.[138]

2.11.13. Politika bezpečnosti systému IT

Politika bezpečnosti systému IT by měla obsahovat podrobnosti požadovaných ochranných opatření a popis, proč jsou nezbytná.[139]

2.11.14. Plán bezpečnosti IT

Jedná se o shrnující dokument, který stručně popisuje veškeré akce, které se musí uskutečnit, aby mohla být implementována ochranná opatření.[140]

2.12. Realizace bezpečnostních opatření

Základním východiskem ISMS je norma ISO/IEC 27002:2013 - Soubor postupů pro řízení bezpečnosti informací. Ta obsahuje tzv. nejlepší zkušenosti řízení bezpečnosti informací.[141]

---

[136] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. s. 172.
[137] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 94.
[138] tamtéž
[139] tamtéž
[140] tamtéž
[141] DOUCEK, Petr. *Řízení bezpečnosti informací*. s. 125.

Obr. č. 17: Rozdělení oblastí bezpečnosti informací[142]

Jednotlivé oblasti obsahují:

- **Bezpečnostní politika** - definice základních pravidel bezpečnosti informací a vyjádření podpory vedením organizace.
- **Organizace bezpečnosti** - upřesnění struktury pro řízení bezpečnosti informací uvnitř organizace a řízení bezpečnosti ve vztahu k externím subjektům (zákazníkům, dodavatelům atd.).
- **Řízení aktiv** - udržování přehledu o existujících aktivech organizace a stanovení odpovědnosti za udržování přiměřené míry ochrany jednotlivých aktiv.
- **Bezpečnost z hlediska lidských zdrojů** - vymezení povinností za ochranu informací u všech pracovníků a zajištění potřebného bezpečnostního povědomí.
- **Fyzická bezpečnost** a **bezpečnost prostředí** - definice pravidel pro přístup osob do klíčových prostor organizace a ochrana zařízení, zejména zařízení ICT (prostředí)
- **Řízení komunikací a řízení provozu** - zajištěni spolehlivého a bezpečného chodu produkčních informačních a komunikačních systémů organizace.
- **Řízení přístupu** - pravidla pro přidělování přístupu ke všem prostředkům informačních a komunikačních systémů včetně sledování způsobu využívání dostupných prostředků.

[142] DOUCEK, Petr. *Řízení bezpečnosti informací.* s. 125.

- **Akvizice, vývoj a údržba informačních systémů** - prosazení principů bezpečnosti informací do projektů rozvoje ICT a dalších podpůrných aktivit.
- **Zvládání bezpečnostních incidentů** - pravidla a postupy určené pro řešení bezpečnostních incidentů včetně shromažďování potřebných důkazů.
- **Řízení kontinuity činnosti organizace** - postupy prevence a minimalizace škod plynoucích pro organizaci z havárií, živelných pohrom či jiných mimořádných událostí.
- **Soulad s požadavky** - organizace dokladuje naplnění požadavků vyplývajících z právních, smluvních a jiných závazků.[143]

Užitečný je přístup k formálnímu uspořádání normy. Ve starších verzích byla všechna bezpečnostní doporučení uvedena jako nestrukturovaný text, což nebylo pro uživatele příliš přehledné. Současná podoba rozlišuje následující tři typy popisu opatření:[144]

- Definice opatření jsou jednovětě specifikace bezpečnostních opatření, které jsou shodné s přílohou A normy ISO/IEC 27001.
- Směrnice pro zavedení obsahuje podrobný popis toho, co je opatřením myšleno a jakým způsobem by opatření mělo být implementováno a prosazováno. Uvedené informace nemusí být platné pro všechny případy nasazení a je přípustné aplikovat i jiné metody řešení.
- Další informace soustředí specifické údaje, které by měly být při implementaci zvažovány (např. právní důsledky, odkazy na specifické bezpečnostní normy apod.).[145]

Hlavním důvodem použití této vnitřní struktury je snaha o jednoznačné odlišení definice opatření od doporučení, jakou formou dané opatření zavádět a prosazovat. To velmi usnadňuje použití normy hlavně pro uživatele, jejichž hlavní profesní orientací není bezpečnost informací.[146]

---

[143] DOUCEK, Petr. *Řízení bezpečnosti informací*. s. 126.
[144] tamtéž
[145] tamtéž
[146] tamtéž

3. Analýza současného stavu

V analytické části bude provedena analýza současného stavu a informační bezpečnosti společnosti. Analýza bude odhalovat nedostatky současného řešení, ze kterých bude vyplývat návrh bezpečnostních opatření.

3.1. Popis společnosti

Společnost INNC s.r.o. je malá společnost, která má pět kmenových zaměstnanců, v případě větších projektů však spolupracuje s až třiceti externisty a její sídlo je v Hradci Králové.

Roční obrat společnosti je x – xx miliónů korun. Je držitelem řady certifikátů, od společností Microsoft, Red Hat, VM Ware, CISCO, ESET a dalších. Ve společnosti je zavedena norma ISO 9001 na řízení procesů.

Hlavní činností společnosti je výstavba a management počítačových sítí. Mezi reference společnosti můžeme zařadit vybudování infrastruktury pro akcenta.cz, včetně propojení se systémem České národní banky. A realizaci hostingového centra Energo klastr Jihlava s akcentem na využití moderních technologií – realizováno pro ČVUT a Fakultu ministerstva obrany.

Obr. č. 18: Logo společnosti INNC[147]

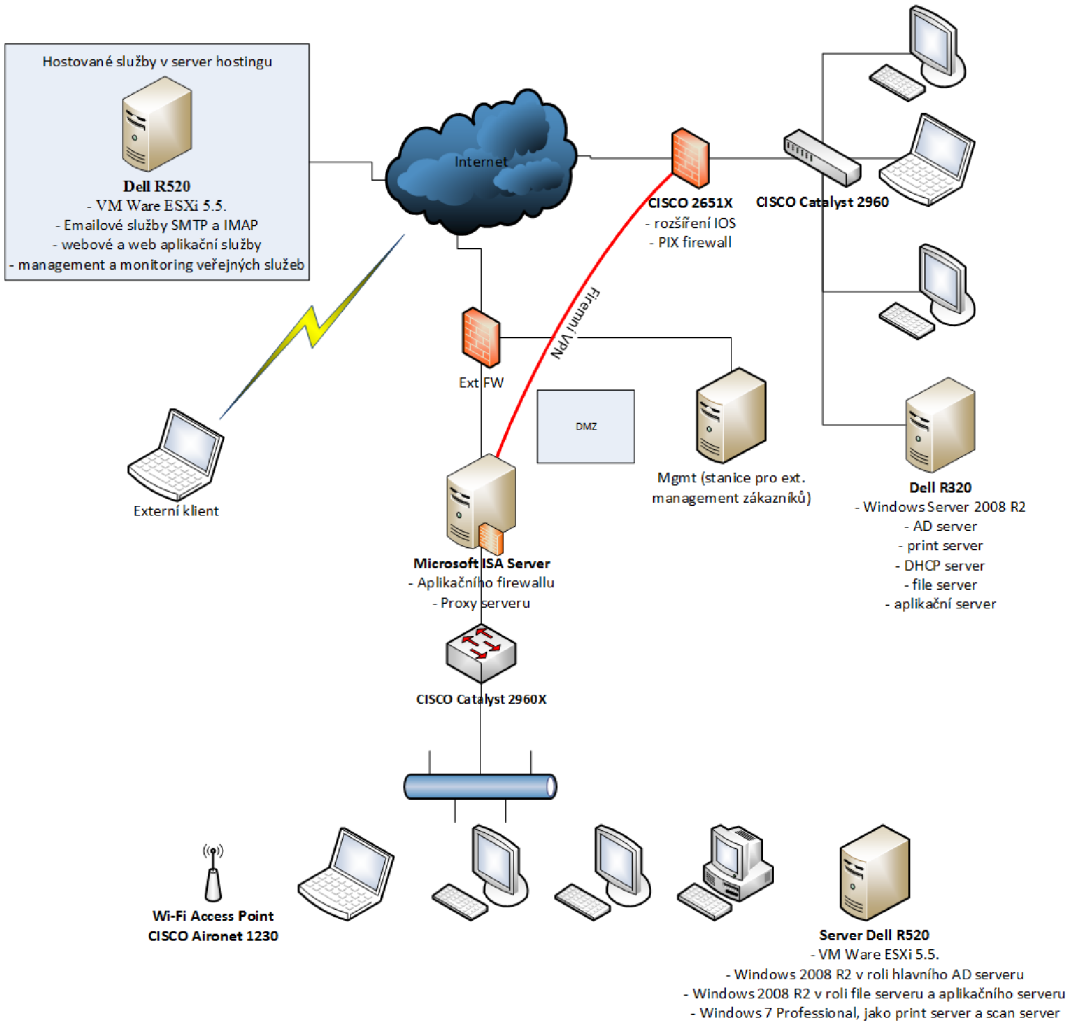
[147] INNC Network Communications. [online]. [cit. 2015-02-01].

3.2. Očekávání společnosti

Společnost se nechystá v současné době zavést ISMS a od práce očekává odhalení možných rizik a návrh opatření tak, aby byla řešena nejvyšší rizika (nepřijatelná a nežádoucí). V případě zbývajících finančních prostředků je ochotná řešit i nízká rizika, to však nemá být cílem této práce.

3.3. Infrastruktura společnosti

Infrastruktura společnosti je rozložena do tří vzájemně propojených částí, umístěných v geologicky odlišných oblastech. Sídlo společnosti, pobočka společnosti a hostingové centrum pro zajištění veřejných služeb.



Obr. č. 19: Síťová infrastruktura společnosti INNC s.r.o.[148]

[148] vlastní tvorba

3.3.1. Infrastruktura sídla společnosti

Firemní infrastruktura v sídle společnosti je rozdělena na tři bezpečnostní úseky, veřejná síť s hlavním firewallem, demilitarizovanou zónu (DMZ) zajišťující externí služby a přístup na internet a síť LAN.

LAN

V interní síti se nachází Server Dell R520 na kterém je provozován hypervizor VM Ware ESXi 5. 5. kde v rámci virtuálních serverů běží následující servery:

- Windows 2008 R2 v roli hlavního AD serveru.
- Windows 2008 R2 v roli file serveru a aplikačního serveru na kterém jsou hostovány ostatní interní služby společnosti, včetně informačního systému.
- Windows 7 Professional, jako print server a scan server.

Propojení LAN zajišťuje switch CISCO Catalyst 2960X. Na síti LAN je také Wi-Fi Access Point CISCO Aironet 1230. V rámci interní infrastruktury je i síťová tiskárna s kopírkou a scannerem a uživatelské stanice s Windows 7 Professional, které jsou součástí firemní domény. Na dalším PC je provozováno účetnictví společnosti.

Demilitarizovaná zóna (DMZ)

Jako hraniční firewall mezi LAN a DMZ je Microsoft ISA Server v režimu Aplikačního firewallu a Proxy serveru, který zajišťuje přístup klientům sítě LAN na internet a k externím službám.

Do DMZ je umístěno mgmt PC s operačním systémem Windows 7 Professional, které je určeno pro správu serverů klientů společnosti v rámci hlavní podnikatelské činnosti – správy sítí.

Jako hlavní firewall slouží PC s operačním systémem Red Hat Linux a nastavenými filtrovacími pravidly (IP filtring).

3.3.2. Infrastruktura pobočky

V síťové infrastruktuře pobočky je Windows Server 2008 R2 Dell R320, který zajišťuje AD server, print server, DHCP server, file server a aplikační server. Server je jištěný jednou UPS. Dále se zde nachází router/firewall CISCO 2651X s rozšířením IOS o PIX Firewall, který zajišťuje propojení klientů LAN do sítě internet a zamezuje neoprávněnému vstupu do interní sítě. Síť LAN je propojena pomocí switche CISCO Catalyst 2960.

Hostingové centrum

V rámci efektivního spojení byly veškeré veřejné služby společnosti odmigrovány do server hostingového centra. Veškeré služby jsou provozovány na vlastním hardware zařízení – serveru Dell R520. Tento hardware slouží jako podklad pro hypervizor VM Ware ESXi 5.5.

V rámci VM Ware infrastruktury jsou provozovány tři samostatné servery na platformě OS Linux. Jeden ze serverů zajišťuje emailové služby společnosti v rámci protokolu SMTP a IMAP a webové a web aplikační služby. Další server se stará o management a monitoring veřejných služeb zákazníků společnosti.

Mobilní klienti

V případě potřeby je možnost vzdáleného připojení do firemní infrastruktury pomocí VPN klientů. Přes mobilní telefon případně některou z veřejných wi-fi sítí. Přístup ke službám firmy je zabezpečen šifrovaným VPN kanálem pomocí technologie IPSEC.

3.4. Služby a jejich dostupnost

Základní skupiny síťových služeb můžeme rozdělit do tří kategorií. Interní služby pro kmenové pracovníky a ostatní zaměstnance společnosti. Interní služby pro externí pracovníky a externí – veřejné služby.

3.4.1. Interní služby v rámci LAN

Hlavní službou v rámci interní sítě je Active Directory. Dále DHCP služby, služby síťového serveru, služby DNS serveru a vzájemné sdílení. Z bezpečnostního pohledu jsou hlavními riziky, napadení virem, kontaminace v rámci přinesené USB flash paměti, zneužití důvěry v rámci interní lokální sítě a podobně. Tato bezpečnostní rizika částečně eliminuje nasazení struktury Active Directory, která přímo definuje uživatelská práva na jednotlivých stanicích i serverech. V rámci bezpečnostních politik jsou zakázána veškerá externí rozhraní pracovních stanic. Tedy, není-li definováno v AD politice jinak, nemůže běžný uživatel používat USB porty, CD/DVD mechaniky apod. Součástí AD je také monitoring. Virové nebezpečí služeb je eliminováno pomocí ESET NOD Antiviru v business verzi, který částečně zabraňuje metodám phishingu a malware.

Dalším uplatněným zabezpečením v síti LAN je aplikace zabezpečení na základě biometrických prvků, konkrétně otisku prstů, pro počítač účetního systému.

Posledním autorizačním faktorem je využití čipových karet s uživatelským certifikátem pro vzdálený přístup do bank, finančního úřadu, úřadu sociálního zabezpečení apod.

Jak vyplývá ze současného provozu je nejzásadnějším bezpečnostním rizikem prostředí internetu. S pohledu bezpečnostních děr v rámci browserů rozšiřujících pluginů, JavaScriptu nebo Javy jako takové. Dalším rizikem může být vynášení interních informací na externí servery pomocí služeb jako uloz.to, leteckaposta.cz a ostatní. Velká část těchto rizik je eliminována pomocí proxy serveru. Žádná veřejná komunikace tedy neprobíhá přímo, nýbrž pouze v rámci přesně daných protokolů a definovaných serverů. Každá komunikace je kontrolována dle RFC (seznam standardů jednotlivých protokolů), čímž je zabráněno jakémukoliv tunelování byť s použitím http protokolu nebo jiných tunelovacích prostředků k obejití proxy. Tento prostředek také

zabraňuje sdílení obrazovek, například pomocí Team Vieweru, přestože využívá k propojení jednotlivých spojení externí server.

Mgmt stanice u které je žádoucí přímý přístup do internetu je umístěna do DMZ a nejsou na ní již kladena tak závažná bezpečnostní opatření pro komunikaci v rámci interní sítě. Tato stanice může za určitých okolností přímo na internet. Díky zamezenému přístupu do sítě LAN, kde je v rámci druhého Firewallu proxy server, nepředstavuje toto připojení žádné bezpečnostní riziko pro interní síť, protože žádné připojení do vnitřní sítě neexistuje.

3.4.2. DMZ

V DMZ síti se nachází pouze mgmt počítač, který zprostředkovává služby vzdáleného dohledu jak pro síť LAN, tak pro externí přístup z mobilních klientů. Externí klienti se tedy pomocí IPSEC VPN přihlašují na mgmt PC a z něj dále mohou spravovat servery zákazníků.

Veškerý přístup na mgmt PC je zabezpečen z LAN pomocí jednoznačně definovaných prostupů v rámci proxy serveru. Z WAN je zabezpečení pomocí bezpečnostních pravidel definovaných v rámci hlavního firewallu společnosti a pomocí bezpečnostních politik definovaných přímo v rámci mgmt PC. Mgmt PC je instalováno v uzamčeném racku.

3.4.3. Hraniční Firewall

Hlavní zabezpečení sídla společnosti je založeno na externím firewallu, kde jsou definovány bezpečnostní politiky jednotlivých prostupů z a do sítě.

Přístup je umožněn výhradně pověřeným pracovníkům společnosti na základě prokázání šifrovacího klíče pro sestavení připojení. Firewall je umístěn v uzamčeném reku společně s ostatními prvky infrastruktury.

3.4.4. Služby v rámci pobočky

V rámci pobočky společnosti je infrastruktura řešená podobně jako v sídle, pouze se zde nenachází DMZ a hraniční firewall. Uživatelé mají přístup jen na služby, které mají povolené, vztahují se na ně tedy všechna bezpečnostní pravidla.

3.4.5. Interní služby v rámci obou lokalit (intranet)

Intranet je zajištěn pomocí IPSEC tunelů mezi proxy serverem na straně sídla společnosti a mezi firewallem na straně pobočky. Tím je zajištěna transparentní dostupnost lokálních služeb bez ohledu na umístění.

V rámci migrace mgmt pracovníků je akceptováno připojení přenosných PC do jedné i druhé sítě, přičemž jsou zachovány veškeré služby, tak jako by pracovník seděl na svém pracovišti.

3.4.6. Veřejné služby

E-mail server

E-mailové služby společnosti jsou zajištěny pomocí SMTP serveru POSTFIX a IMAP serveru DOVECOT. Již z charakteru služby SMTP vyplívají bezpečnostní rizika, kterým se v popisované společnosti předchází nasazením SSL certifikátů na obě služby.

http servery

V rámci serverů pro http a http aplikační služby je nainstalováno několik webových serverů využívajících interní databáze pro služby typu help desk pro zákazníky, statistické výstupy monitoringu zákaznických veřejných služeb a webové servery zákazníků.

U help deskové aplikace a dalších aplikací vyžadujících autorizaci je využíván SSL certifikát a přístup pomocí HTTPS.

Na serverech jsou jednoznačně definována přístupová pravidla k jednotlivým službám, na jednotlivé virtuální servery jsou vždy povoleny pouze prostupy na skutečně publikované služby, případně je prostup omezen pouze na zdrojové (source) adresy. Služby jsou zabezpečeny pravidelnými aktualizacemi.

Server hostingové centrum bylo zvoleno z důvodu vysokého zabezpečení hardwarových prostředků. Centrum má řešenu ochranu v rámci okolních faktorů, jako je pád letadla, bouře, povodně a podobně. V rámci nastavených bezpečnostních politik centra se vyžaduje autorizace přístupu do počítačového sálu, který je monitorován prostřednictvím video kamer. S ohledem na energetickou náročnost má centrum

samostatně řešené redundantní a plně zálohované zdroje elektrické energie s odlišnými dodavateli.

Hostingové centrum má vypracován požární plán včetně použití zplynovacích hasících technik, které jsou pro menší firmy z finančního hlediska nedostupné. Z tohoto pohledu je server hostingové centrum jednoznačnou výhodou a přínosem k umístění veřejně publikovaných síťových služeb.

3.5. Bezpečnost podniku

Bezpečnost podniku z pohledu fyzické a personální bezpečnosti.

3.5.1. Fyzická bezpečnost

Sídlo společnosti leží v nezáplavové oblasti a pro přístup do objektu je nutná karta zaměstnance. Prostor je chráněn kamerovým systémem a důležité prvky hardware jsou přesunuty do datového centra, čímž je zajištěno splnění vysokých bezpečnostních standardů. Společnost využívá klimatizaci a záložní zdroje pro případ výpadku energie.

3.5.2. Personální bezpečnost

Personální bezpečnost je zajištěna především pomocí smluv, nastavení práv a omezení v Active Directory (jednotliví zaměstnanci mají přístup pouze k věcem nezbytným pro svou činnost), osobními certifikáty, využíváním biometrických prvků, především otisků prstů (například pro přístup k účetnímu software) a pravidelným školením. Přístupu k citlivým službám je umožněn výhradně pověřeným pracovníkům společnosti na základě prokázání šifrovacího klíče.

3.6. Analýza rizik

V rámci analýzy rizik budou definována aktiva společnosti a případná rizika a hrozby, které mohou nastat.

3.6.1. Identifikace a ohodnocení aktiv

Identifikace aktiv a jejich zařezaní do kategorií.

Data

Velkou důležitost mají ve společnosti interní informace – tedy know-how společnosti, informace o zpracování síťových infrastruktur a podobně. Tyto informace jsou částečně uchovávány v tištěné a digitální podobě (dokumentace, návody) a jedná se především o vědomosti jednotlivých pracovníků společnosti.

Dalším důležitým prvek jsou smlouvy, které stanovují obchodní vztah mezi společností a jejími dodavateli a klienty. Jsou důležité především z právního hlediska, při řešení možných problémů.

Data zákazníků uložená v databázích a data, která byla poskytnuta společnosti a mohla by být zneužita neoprávněnou osobou.

Hardware

Mezi aktiva z hlediska hardware patří pracovní notebooky, kde má každý zaměstnanec k dispozici svůj přístroj, PC stanice, servery, síťová tiskárna, switche a routery.

Software

Do software patří operační systémy pro osobní počítače a servery, databázový software a účetní software společnosti.

Služby

Z hlediska aktiv do služeb spadá telefonní linka, zdroj elektrické energie a připojení k internetu.

Tab. č. 1: Identifikovaná aktiva[149]

Typ	Aktivum
Data	smlouvy
	data zákazníků
	interní informace
HW	notebooky
	servery
	PC stanice
	tiskárna
	switche
	routery
SW	operační systémy
	databázový software
	účetní software
Služby	telefonní linka
	zdroj elektrické energie
	připojení k internetu

Pomocná tabulka pro ohodnocení aktiv na základě dopadu na organizaci.

Tab. č. 2: Hodnocení rizik dle dopadu na organizaci[150]

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

Vzorec pro ohodnocení aktiv:

$$Hodnota\ aktiva = \frac{Dostupnost + Důvěrnost + Integrita}{3}$$

[149] vlastní tvorba
[150] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 82.

Tab. č. 3: Ohodnocení aktiv[151]

Typ	Aktivum	Dostupnost	Důvěrnost	Integrita	Hodnota aktiva
Data	smlouvy	5	5	5	5
	data zákazníků	3	5	4	4
	interní informace	5	5	5	5
HW	notebooky	3	5	4	4
	servery	3	5	4	4
	PC stanice	3	5	4	4
	tiskárna	2	1	3	2
	switche	3	4	4	3
	routery	3	4	3	3
SW	operační systémy	3	4	4	3
	databázový software	3	5	4	4
	účetní software	2	5	4	3
Služby	telefonní linka	2	2	2	2
	zdroj elektrické energie	3	1	2	2
	připojení k internetu	3	1	3	2

[151] vlastní tvorba

3.6.2. Identifikace hrozeb

K důležitým bezpečnostním rizikům ve společnosti patří prolomení zabezpečení na veřejné služby společnosti a částečná ztráta dat. Pro komplexnější pohled je zobrazena tabulka hrozeb.

Tab. č. 4: Identifikace a ohodnocení hrozeb dle ČSN ISO/IEC 27005[152]

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

[152] ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Řízení rizik bezpečnosti informací.*

3.6.3. Matice zranitelnosti a rizik

Na základě identifikovaných aktiv a hrozeb, byly sestaveny dvě matice. Matice zranitelnosti, zobrazuje zranitelnost aktiva vůči hrozbě. A matice rizik zobrazující velikost možného rizika. Pravděpodobnost i jednotlivé hodnoty byly stanoveny na základě logické úvahy.

Tab. č. 5: Stupnice pravděpodobnosti hrozeb[153]

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

[153] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 90.

Tab. č. 6: Matice zranitelnosti[154]

Zranitelnost (V)	Popis aktiva	smlouvy	data zákazníků	interní informace	notebooky	servery	PC stanice	tiskárna	switche	routery	operační systémy	databázový software	účetní software	telefonní linka	zdroj elektrické energie	připojení k internetu
	Hodnota aktiva (A)	5	4	5	4	4	4	2	3	3	3	4	3	2	2	2
Popis hrozby	Pravděpodobnost (T)															
Fyzické poškození																
Oheň	1	3	2	3	2	2	2	1	2	2	2	2	2	1	1	1
Poškození vodou	1	3	2	3	2	2	2	1	2	2	2	2	2	1	1	1
Znečištění	3		3	2	3	3	3	2	3	3				2		2
Zničení vybavení nebo médií	2		3	3	3	3	3	2	2	2						2
Prach, koroze, zamrznutí	2		3	2	3	3	3	2	2	2				2	2	2
Přírodní události																
Povodně	1	3	2	3	2	2	2	1	2	2	2	2	2	1	3	2
Ztráta klíčových služeb																
Selhání klimatizace nebo chladícího systému	2		3			3			2	2	3	2	2			
Ztráta energie	3		3		3	3	3	2	3	3	3	3	2	2	2	2
Kompromitování informací																
Špionáž a škodlivý kód	4	4	4	4	4	4	4		3	3	3	4	3			
Krádež média nebo dokumentu	3	4	3	3												
Krádež vybavení	2		3		3	3	3	2	2	2						2
Získání dat ze zničených médií	2	4	3	4							2	3	2			
Data z nedůvěryhodných zdrojů	2	3	3	3							3	3	2			
Manipulace s hardware	2		3	3	3	3	3	2	2	2	2	3	2			2
Manipulace se software	2	3	3	3							2	3	2			
Technická selhání																
Selhání zařízení	3		3	4	3	3	3	2	3	3	3	3	3	2	2	2
Selhání software	2		3	3					2	2	3	3	3			
Neoprávněné akce																
Neoprávněné použití zařízení	3	4	3	4	3	3	3	2	3	3	3	3	3			
Podvodné zkopírování software	2	3	3	3							2	3	2			
Použití ukradeného nebo zkopírovaného software	2	3	3	3							2	3	2			
Poškození dat	3	4	3	4							3	3	3			
Nezákonné zpracování dat	2	3	3	3												
Kompromitování funkcí																
Chybné použití	3		3	4							3	3	3			2
Zneužití práv	2		3	3							2	3	2			2
Padělání práv	2		3	3							2	3	2			

[154] vlastní tvorba

Matice rizik slouží pro výpočet míry rizika, za využití vzorce R = T*A*V, kde R označuje vypočtenou míru rizika, T je pravděpodobnost, že hrozba nastane, A je aktivum a V je zranitelnost.

Tab. č. 7: Míra rizika[155]

Míra rizika	Stupeň rizika	Dopad na organizaci
0 až 10	bezvýznamné	Nemá dopad na organizaci
10 až 20	akceptovatelné	Zanedbatelný dopad na organizaci
20 až 30	nízké	Mohou vzniknout potíže či finanční ztráty
30 až 60	nežádoucí	Vážné potíže a finanční ztráty
60 a více	nepřijatelné	Hrozí zaniknutí firmy

[155] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. s. 90.

Tab. č. 8: Matice rizik[156]

Riziko (R)	Popis aktiva	smlouvy	data zákazníků	interní informace	notebooky	servery	PC stanice	tiskárna	switche	routery	operační systémy	databázový software	účetní software	telefonní linka	zdroj elektrické energie	připojení k internetu
	Hodnota aktiva (A)	5	4	5	4	4	4	2	3	3	3	4	3	2	2	1
Popis hrozby	Pravděpodobnost (T)															
Fyzické poškození																
Oheň	1	15	8	15	8	8	8	2	6	6	6	8	6	2	2	2
Poškození vodou	1	15	8	15	8	8	8	2	6	6	6	8	6	2	2	2
Znečištění	3	0	36	30	36	36	36	12	27	27	0	0	0	12	0	12
Zničení vybavení nebo médií	2	0	24	30	24	24	24	8	12	12	0	0	0	0	0	8
Prach, koroze, zamrznutí	2	0	24	20	24	24	24	8	12	12	0	0	0	8	8	8
Přírodní události																
Povodně	1	15	8	15	8	8	8	2	6	6	6	8	6	2	6	4
Ztráta klíčových služeb																
Selhání klimatizace nebo chladícího systému	2	0	24	0	0	24	0	0	12	12	18	16	12	0	0	0
Ztráta energie	3	0	36	0	36	36	36	12	27	27	27	36	18	12	12	12
Kompromitování informací																
Špionáž a škodlivý kód	4	80	64	80	64	64	64	0	36	36	36	64	36	0	0	0
Krádež média nebo dokumentu	3	60	36	45	0	0	0	0	0	0	0	0	0	0	0	0
Krádež vybavení	2	0	24	0	24	24	24	8	12	12	0	0	0	0	0	8
Získání dat ze zničených médií	2	40	24	40	0	0	0	0	0	0	12	24	12	0	0	0
Data z nedůvěryhodných zdrojů	2	30	24	30	0	0	0	0	0	0	18	24	12	0	0	0
Manipulace s hardware	2	0	24	30	24	24	24	8	12	12	12	24	12	0	0	8
Manipulace se software	2	30	24	30	0	0	0	0	0	0	12	24	12	0	0	0
Technická selhání																
Selhání zařízení	3	0	36	60	36	36	36	12	27	27	27	36	27	12	12	12
Selhání software	2	0	24	30	0	0	0	0	12	12	18	24	18	0	0	0
Neoprávněné akce																
Neoprávněné použití zařízení	3	60	36	60	36	36	36	12	27	27	27	36	27	0	0	0
Podvodné zkopírování software	2	30	24	30	0	0	0	0	0	0	12	24	12	0	0	0
Použití ukradeného nebo zkopírovaného software	2	30	24	30	0	0	0	0	0	0	12	24	12	0	0	0
Poškození dat	3	60	36	60	0	0	0	0	0	0	27	36	27	0	0	0
Nezákonné zpracování dat	2	30	24	30	0	0	0	0	0	0	0	0	0	0	0	0
Kompromitování funkcí																
Chybné použití	3	0	36	60	0	0	0	0	0	0	27	36	27	0	0	12
Zneužití práv	2	0	24	30	0	0	0	0	0	0	12	24	12	0	0	8
Padělání práv	2	0	24	30	0	0	0	0	0	0	12	24	12	0	0	0

[156] vlastní tvorba

Z analýzy je patrné, že nejvyšší rizika se týkají kompromitování informací a neoprávněných akcí. Především těmto oblastem se tedy budu věnovat v návrhu řešení. Bude řešena i oblast týkající se zabezpečení externích pracovníků, protože jich společnost má celou řadu a mohli by být potencionálním rizikem.

3.6.4. Akceptace rizik a vyřešené hrozby

Společnost se rozhodla všechna bezvýznamná a akceptovatelná rizik akceptovat. Nízká nežádoucí a neakceptovatelná rizika pak akceptována nejsou.

Tab. č. 9: Akceptace rizik[157]

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

[157] vlastní tvorba

Téměř všechny hrozby jsou již z části nebo úplně řešeny. Řádky s hodnotou „Ne“ znázorňují, že řešení není dostatečné a budu se mu věnovat v rámci návrhu řešení.

Tab. č. 10: Vyřešené hrozby[158]

Hrozba	Zavedená opatření	Vyřešeno
Fyzické poškození		
Oheň	A.11.1.4	Ano
Poškození vodou	A.11.1.4	Ano
Znečištění		Ne
Zničení vybavení nebo médií	A.11	Ano
Prach, koroze, zamrznutí	A.11.2.4	Ano
Přírodní události		
Povodně	A.11.1.4; A.11.1.5; A.11.2.1	Ano
Ztráta klíčových služeb		
Selhání klimatizace nebo chladícího systému	A.11.2.2; A.11.2.4	Ano
Ztráta energie		Ne
Kompromitování informací		
Špionáž a škodlivý kód	A.9.1.1; A.9.2.2; A.9.2.3; A.9.2.4; A.9.4.1; A.11.2.6; A.12.2.1; A.12.6.2; A.14.1.2; A.14.1.3	Ne
Krádež média nebo dokumentu	A.6.2.1; A.8.3.3; A.9.1.1; A.9.1.2; A.9.2.2; A.9.2.3; A.9.4.1; A.11.2.5; A.11.2.6; A.11.2.8;A.12.2.1; A.13.2.1; A.13.2.2; A.14.1.2; A.14.1.3	Ne
Krádež vybavení	A.7.2.3; A.7.3.1; A.11.1.1; A.11.1.2; A.11.1.3; A.11.1.8; A.11.2.1; A.11.2.5	Ano
Získání dat ze zničených médií	A.11.2.7	Ano
Data z nedůvěryhodných zdrojů	A.12.6.2; A.13.1.1	Ano
Manipulace s hardware	A.11.1.1; A.11.1.3; A.11.1.8; A.11.2.1	Ano
Manipulace se software	A.6.2.2; A.9.1.1; A.9.2.2; A.9.2.3; A.11.2.9; A.12.2.1; A.12.5.1; A.12.6.2; A.14.2.4	Ano
Technická selhání		
Selhání zařízení	A.11.1.4; A.11.1.5; A.11.2.1;	Ne
Selhání software	A.12.4.4	Ne
Neoprávněné akce		
Neoprávněné použití zařízení	A.9.1.2; A.9.2.5; A.9.2.6; A.9.4.1 A.11.1.1; A.11.1.3; A.11.1.8; A.11.2.1; A.11.2.6; A.11.2.8; A.12.2.1; A.12.4.1; A.12.4.3; A.13.1.3	Ne
Podvodné zkopírování software	A.7.2.3; A.11.2.8; A.12.5.1; A.14.2.4	Ano
Použití ukradeného nebo zkopírovaného software	A.7.2.3; A.12.5.1; A.14.2.4	Ano
Poškození dat	A.9.1.2; A.9.4.1; A.11.2.8;A.12.3.1; A.12.2.1; A.12.6.2; A.14.1.3	Ne
Nezákonné zpracování dat	A.11.2.8; A.11.2.9; A.12.2.1; A.12.4.1; A.12.4.3; A.13.2.1; A.13.2.2; A.13.2.3; A.14.1.2; A.14.1.3	Ano
Kompromitování funkcí		
Chybné použití		Ne
Zneužití práv	A.7.2.3; A.9.1.1; A.9.2.1; A.9.2.2; A.9.2.3; A.9.2.5; A.9.2.6; A.9.4.1; A.9.4.3; A.12.4.1; A.12.4.3; A.13.1.3	Ano
Padělání práv	A.9.2.1; A.9.4.2	Ano

[158] vlastní tvorba

3.7. Zhodnocení stávajícího stavu

Přestože velká část bezpečnostních opatření je již zavedena, z analýzy vyplývá, že společnost v současnosti nemá řešen žádný komplexní systém řízení informační bezpečnosti.

Vzhledem k tomu, že společnost má zákazníky i mezi státními organizacemi, doporučuji jí certifikaci ISMS pro zachování současných klientů, celkové zvýšení bezpečnosti a udržení či zlepšení své pozice na trhu.

Dále analýza odhalila, že z hlediska aktiv je třeba nejvíce zabezpečit interní informace, data zákazníků, smlouvy a databázový software. Zneužití či poškození těchto aktiv by mohlo mít velmi velký až likvidační dopad na společnost. S tím souvisí i notebooky zaměstnanců, servery, PC stanice, operační systémy a účetní software. Z hlediska možných rizik je pak největším rizikem špionáž a škodlivý kód, společně s neoprávněným použitím zařízení, jeho selháním nebo ztrátou energie. Výrazným rizikem je také znečištění zařízení, jeho chybné použití a poškození nebo zneužití dat.

Největší pozornost by měla být v současnosti věnována zabezpečení a ochraně dat, školení uživatelů, aby se předešlo chybnému použití zařízení nebo neúmyslným incidentům, a péči o hardware. Protože společnost má řadu externích zaměstnanců, bude věnována pozornost opatřením s tím souvisejícím, jako je práce na dálku, politika mobilních zařízení a podobně.

4. Vlastní návrh řešení

V návrhu vlastního řešení, budou navržena, vybraná bezpečnostní opatření včetně finančních nákladů. A určena celková ekonomická náročnost.

4.1. Bezpečnostní opatření

Bezpečnostní opatření byla vybrána na základě výsledků analýzy a komunikace se společností. Všechna opatření jsou převzata z normy ČSN ISO/IEC 27001:2013, přílohy A. Pro realizaci jsem využil normu ČSN ISO/IEC 27002:2013.

Tabulka zobrazuje seznam vybraných opatření, která budou nově zavedena nebo revidována. Zavedení těchto opatření povede ke snížení rizik a zvýšení bezpečnosti.

Tab. č. 11: Opatření pro řešení hrozeb[159]

Hrozba	**Opatření**
Fyzické poškození	
Znečištění	A.11.2.4
Ztráta klíčových služeb	
Ztráta energie	A.11.2.2
Kompromitování informací	
Špionáž a škodlivý kód	A.6.2.1; A.6.2.2; A.9.3.1; A.9.4.2; A.9.4.4; A.10.1.1; A.12.5.1; A.13.1.1; A.13.2.3
Krádež média nebo dokumentu	A.6.2.2;A.9.3.1; A.9.4.2; A.9.4.4; A.10.1.1; A.11.2.9; A.13.1.1; A.13.2.3;
Technická selhání	
Selhání zařízení	A.11.2.2; A.11.2.4
Selhání software	A.11.2.4; A.12.2.1; A.12.5.1;
Neoprávněné akce	
Neoprávněné použití zařízení	A.6.2.1; A.6.2.2; A.9.3.1; A.9.4.2; A.9.4.3; A.9.4.4; A.11.2.9; A.12.5.1; A.13.1.1
Poškození dat	A.9.3.1; A.9.4.4; A.10.1.1; A.11.2.9
Kompromitování funkcí	
Chybné použití	A.7.2.2; A.7.3.1

4.1.1 Organizace bezpečnosti informací (A.6)

Cílem je ošetřit bezpečnost informací v organizaci vytvořením řídícího rámce pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci, včetně zajištění bezpečnosti při použití mobilních zařízení a práci na dálku.

[159] vlastní tvorba

Kontakt se zájmovými skupinami (A.6.1.4)

Doporučuji pravidelně sledovat stránky národního centra kybernetické bezpečnosti (www.govcert.cz) - především aktuální hrozby. Dále doporučuji účast na akcích zaměřených na bezpečnost, které jsou zde uváděny v sekci Akce / Události. Nezbytné je též sledování informací o aktuální legislativě týkající se bezpečnosti a významných bezpečnostních incidentů a reagovat na ně co nejdříve zavedením bezpečnostních opatření ve vlastní společnosti Dalším užitečným zdrojem informací týkajících se bezpečnosti jsou stránky www.csirt.cz.

Hlavní výhodou tohoto opatření je, že společnost získá přehled o aktuálních trendech v oblasti bezpečnosti informací. Může navázat kontakt nebo spolupráci s odborníky na bezpečnost. A při pravidelném sledování stránek bude včas informována a o aktuálních bezpečnostních hrozbách a způsobu jejich řešení.

Politika mobilních zařízení (A.6.2.1)

Pro dosažení dostatečné bezpečnosti je třeba vždy používat bezpečné prostředí, ideálně tedy neveřejné místo s kontrolou vstupu a zabezpečeným přístupem. Mobilní zařízení je vždy nutné bezpečně skladovat a nenechávat je na veřejně přístupných místech (pokojový stůl, nemocniční pokoj, zasedací místnost,…).

Na každém zařízení musí být nainstalovaný antivirový program. Doporučuji Kaspersky Internet Security pro Android nebo ESET Mobile Security pro Android. Vzhledem k tomu, že společnost má řešení od společnosti ESET, předpokládám, že toto řešení zvolí i pro mobilní zařízení.

ESET Mobile Security pro Android

1. Ochrana koncových zařízení

1.1. Ochrana v reálném čase

Kontroluje všechny aplikace a navázané komunikace na přítomnost škodlivého kódu. Chrání před online i offline hrozbami, detekuje útoky USSD.

1.2. Kontrola při nabíjení

Umožňuje provést kontrolu v případech, kdy se zařízení nabíjí nebo je zamknutá obrazovka.

1.3. *Anti-Phishing*

Chrání před podvodnými stránkami, které se snaží získat citlivé informace jako je uživatelské jméno, heslo, podrobnosti o kreditních kartách nebo bankovnictví.

1.4. Filtr volání a SMS

Na zařízení se dovolá a pošle zprávu jen určená osoba. Definovat lze také čas, kdy je zařízení dostupné.

2. Bezpečnost zařízení

Mobile Device Management (MDM)

Administrátor má možnost uplatňovat na zařízení základní bezpečnostní politiky pro mobilní zařízení. Produkt automaticky upozorňuje uživatele a správce v případech, které nejsou v souladu s firemní politikou, a doporučuje provést změny.

Nastavení umožňuje:

- Definovat požadavek na silné heslo
- Určit maximální počet pokusů pro odemknutí zařízení. Při překročení dojde automaticky k přechodu do továrního nastavení
- Určit maximální dobu platnosti hesla
- Určit čas pro zamknutí obrazovky při nečinnosti
- Vyzvat uživatele k šifrování zařízení
- Zablokovat integrovanou kameru

3. Kontrola aplikací

Umožňuje administrátorovi monitorovat instalované aplikace, blokovat přístup k definovaným aplikacím a vyzve uživatele k odinstalaci určité aplikace.

Nastavení kontroly aplikací:

- Umožňuje zablokovat definované aplikace
- Blokovat dle kategorií - hry, sociální sítě atd.
- Blokovat dle práv – kam aplikace přistupují
- Blokovat dle zdroje – mimo Google play apod.
- Umí vytvořit výjimky na základě whitelistů a seznam povinně instalovaných aplikací.

4. Anti-Thief

4.1. *Událost*

Všechny vzdálené příkazy provádí správce pomocí ESET Remote Administrator nebo přes SMS s dvoufaktorovou autentizací, případně přímo z grafického rozhraní.

4.2. *Zpráva na obrazovku*

Odešle libovolnou zprávu např. s kontaktními informacemi na ztracené zařízení. Zpráva se zobrazí na obrazovce formou vyskakovacího okna.

4.3. *Admin kontakty*

Obsahují seznam důvěryhodných telefonních čísel chráněných administrátorským heslem. SMS příkazy je poté možné odesílat jen z těchto čísel. Uvedené kontakty dostávají upozornění z Anti-Thiefu.

4.4. *Informace na zamknuté obrazovce*

Správce může vytvořit a odeslat na zařízení vlastní zprávu (např. s kontaktními informace). Zpráva se zobrazí na obrazovce i v případě, že je zařízení zablokováno.

4.5.Základní vzdálené akce

Správce může vzdáleně zamknout/ odemknout zařízení, spustit zvukovou sirénu, lokalizaci, smazat data a podobně.[160]

Po instalaci antiviru je tedy nutné okamžitě aktivovat a nastavit všechny bezpečnostní prvky. K tomu účelu je přímo v aplikaci průvodce, který uživatele postupně a přehledně provede všemi důležitými kroky. Pro ještě větší zefektivnění pak doporučuji tuto službu spojit ještě se službou ESET Remote Administrator 6 pro vzdálenou správu.

Doporučení pro práci s mobilními zařízeními:

- vyhnout se odpozorování hesla nežádoucími osobami
- pravidelně aktualizovat antivirový program
- pravidelně vytvářet zálohy důležitých informací
- automaticky zamykat zařízení
- zařízení by mělo být vhodně chráněno proti krádeži nebo ztrátě (aktivovaný Anti-Thief, heslo, PIN, šifrování dat)
- vzdálený přístup by měl být umožněn pouze po úspěšné identifikaci a autorizaci

Postup v případě krádeže nebo ztráty:

1) Okamžitě informujte administrátora
2) Využijte funkce Anti-Thief (zamknout zařízení, lokalizovat, poslat zprávu a případně smazat data)
3) Změna přístupových údajů souvisejících s daným zařízením
4) Zakázat všechny přístupy do systému z daného zařízení
5) Informovat klienty v případě nebezpečí úniku jejich dat

Pro zvyšování povědomí zaměstnanců o bezpečnosti mobilních zařízení doporučuji pravidelně organizována školení.

Náklady

5x ESET Mobile Security pro Android	1 422.00 Kč

[160] *ESET Endpoint Security pro Android* [online]. [cit. 2016-05-11].

Práce na dálku (A.6.2.2)

Pro práci na dálku doporučuji používat pouze firemní předem nastavená zařízení, u nichž bude probíhat monitoring činnosti a zaznamenávání formou logů. Část opatření je řešena již v A.6.2.1.

Protože v současné době probíhá vzdálené přihlášení přes VPN pouze pomocí jednofaktorové autentizace, navrhuji pro zvýšení bezpečnosti zavést dvoufaktorovou autentizaci ESET Secure Authentication čímž bude zvýšeno zabezpečení pro vzdálený přístup i v případě zcizení zařízení nebo vyzrazení hesla.

ESET Secure Authentication

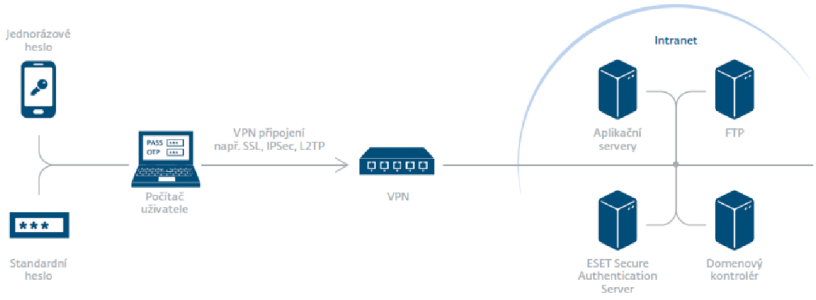
Poskytuje silné ověření oprávnění přístupu do firemní sítě a k jejímu obsahu. Jde o mobilní řešení, které používá dvou faktorové ověření s jednorázovým heslem (2FA OTP). Výhodou jednorázových hesel je jejich náhodnost, proto je nelze předvídat ani znovu použít.

ESET Secure Authentication chrání:

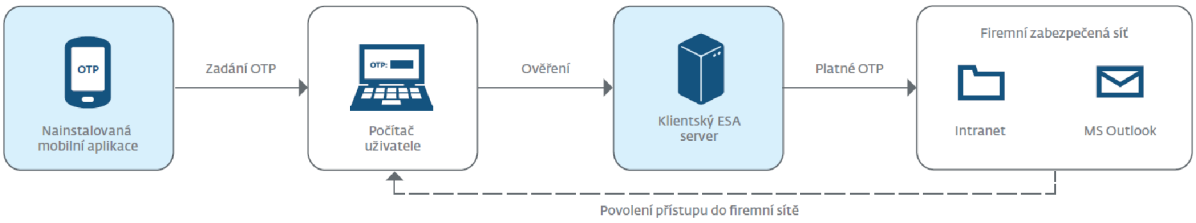
- Přístup do firemní VPN
- Remote Desktop protokol
- Lokální přihlášení do počítače
- Webové a cloudové služby přes Microsoft ADFS 3.0, například Office 365
- Webové aplikace Microsoft, například OWA
- Exchange Control Panel & Exchange Administrator Center 2013
- VMware Horizon View
- Služby založené na RADIUS

Řešení můžete jednoduše implementovat do RADIUS služeb nebo použít API a integrovat řešení do existujícího autentifikačního systému, založeném na Active Directory. Aplikace obsahuje nástroje SDK, pomocí kterých můžete řešení

implementovat do libovolného vlastního systému, bez potřeby použití Active Directory.[161]



Obr. č. 20: VPN s ESET Secure Authentication[162]



Obr. č. 21: Komunikace na straně uživatele[163]

Další doporučení:

- pracovat z fyzicky bezpečného prostředí (ideálně uzamykatelná kancelář bez přístupu dalších osob)
- vždy kontrolovat že je nastavený firewall a aktuální antivirový program
- pracovat pouze z firemních zařízení a nesnažit se o přístup ze zařízení, které není dostatečně zabezpečeno
- pokud je to možné používat pro přihlášení do zařízení otisk prstu

Náklady

5x ESET Secure Authentication	8 428.00 Kč

[161] *Dvoufaktorová autentizace* [online]. [cit. 2016-05-11].

[162] tamtéž

[163] tamtéž

4.1.2 Bezpečnost lidských zdrojů (A.7)

Opatření pro bezpečnost lidských zdrojů jsou v případně zpracovávané společnosti velmi podstatná vzhledem k velkému počtu externích pracovníků. Právě pracovníci jsou často jednou z hlavních příčin hrozeb a rizik. Bude ošetřeno dodržování povinností smluvních stran a výběr vhodných kandidátů na jednotlivé role a zajištění vědomí vlastních povinností v oblasti bezpečnosti informací. V neposlední řadě se budou opatření věnovat i celému životnímu cyklu zaměstnance, tedy od výběru přes pracovní vztah až po ukončení pracovního vztahu.

Povědomí, vzdělávání a školení bezpečnosti informací (A.7.2.2)

Společnost v současnosti pořádá školení zaměřená na zvýšení odbornosti zaměstnanců. Neorganizuje však školení zaměřená na bezpečnost informací. Doporučuji tedy současná školení rozšířit o školení zaměřená na bezpečnost informací, v rámci kterých bude v zaměstnancích budováno povědomí o bezpečnosti informací. Mimo jiné budou zaměstnanci v rámci školení seznamováni s aktuální firemní bezpečností politikou, novými trendy v bezpečnosti, případně v oblasti možných hrozeb a rizik, a také se změnami v bezpečnosti společnosti a bezpečnostních postupech.

Doporučuji také, aby byl každý zaměstnanec (nový i stávající) seznámen s bezpečnostní politikou, odpovědnostmi, bezpečnostním očekáváním, případnými sankcemi při porušení nebo nedodržení a prošel dostatečným vstupním školením vzhledem k jeho pozici a náplni práce. Teprve poté by mu měl být umožněn přístup k aktivům společnosti. Tímto postupem by se mělo předejít mnohým incidentům způsobeným nedostatečnou informovaností.

Pro realizaci školení bych doporučil společnost ESET vzhledem k tomu, že s ní již je rozvinuta spolupráce a patří mezi špičky na trhu, případně společnost COMGUARD.

Školení ESET Services

Společnost ESET nabízí „školení na míru“, kdy je možné se předem domluvit na obsahu školení na základě specifických požadavků společnosti. Školení je realizováno na základě nejnovějších bezpečnostních norem a standardů. Hlavním cílem je vzdělávat

a obeznamovat zaměstnance společnosti s bezpečnostními riziky, vnitřními předpisy a dobrou praxí při používání IT prostředků a nakládáním s informacemi.

Náplň a rozsah školení je stanovena na základě konkrétních potřeb a požadavků zákazníka. Předmětem školení mohou být následující oblasti:

- Vnitřní předpisy
- Fyzická bezpečnost
- Ochrana IT prostředků (počítače, telefony,...)
- Používání hesel
- Bezdrátové sítě
- Přenosná média
- Internetové služby (e-mail, web, sociální sítě,...)
- Škodlivý kód a jeho šíření
- Zvládání bezpečnostních incidentů
- Nakládání s citlivými informacemi
- Autorská práva a IT
- Ochrana osobních údajů

Nabízené služby

- Návrh a příprava vzdělávacího programu
- Příprava a realizace školení[164]

Cena školení je řešena individuálně na základě požadavků společnosti.

Školení COMGUARD

Společnost COMGUARD nabízí širokou škálu školení, kdy jsou však předem dané kurzy i jejich cena. Toto řešení tedy může společnost zvolit v případě, že jí bude vyhovovat některý z nabízených kurzů a chce předem znát cenu za školení.

[164] *Řízení informační bezpečnosti* [online]. [cit. 2016-05-11].

Některá z nabízených školení:

- Penetrační testování a etický hacking v sítích LAN
- Penetrační testování a etický hacking v sítích WAN
- Penetrační testování a etický hacking webových aplikací
- Bezpečnost v prostředí Windows a internetových služeb
- Bezpečnost v prostředí WWW aplikací a internetových služeb
- Windows Server 2008/2012 - Praktická ochrana serverů a sítí
- Zabezpečení bezdrátových sítí - WiFi
- VMware vSphere – Security
- LINUX – Zabezpečení systému a sítě
- PKI – Elektronický podpis v praxi administrátora
- Troubleshooting a analýza sítě s využitím Snifferu
- SQL Server 2014/2012 - komplexní zabezpečení
- Zabezpečení platforem iOS a Android ve firemním prostředí[165]

Více informací je možné nalézt přímo na oficiálních stránkách (www.comguard.cz) v sekci „Školící centrum“, kde je možno si detailně zobrazit obsah jednotlivých kurzů.

Náklady na školení pro příští rok:

VMware vSphere – Security	13 900.00 Kč
Windows Server 2008/2012 - Praktická ochrana serverů a sítí	13 900.00 Kč
Penetrační testování a etický hacking v sítích LAN	13 900.00 Kč

Disciplinární řízení (A.7.2.3)

Společnost v současné době nemá žádný plán pro disciplinární řízení. Uvádím zde tedy doporučení pro dokument „*Disciplinární řízení*“, který je možné uložit do IS společnosti a v případě potřeby následně upravit.

[165] *COMGUARD - Školicí centrum* [online]. [cit. 2016-05-11].

1. Úvodní ustanovení

Disciplinární řád pro zaměstnance INNC, s.r.o. ustanovuje postup a sankce v případě přestupků. Řád je v souladu s bezpečnostní politikou společnosti a se zákony ČR. Upravuje podrobnosti o disciplinárních přestupcích zaměstnanců a stanovuje postup pro projednávání disciplinárních přestupků a následné ukládání sankcí.

2. Postup před zahájením disciplinárního řízení:

Před zahájením samotného disciplinárního řízení je třeba prověřit následující faktory:

- ověřit, že se skutečně jedná o narušení bezpečnosti
- zjistit, zda jde o první nebo opakovanou událost
- ověřit, zda byla daná osoba dostatečně informována o svých odpovědnostech, povinnostech a případně důsledcích svého jednání z hlediska bezpečnosti informací a zda byla řádně proškolena
- znovu projít a ověřit podepsané smlouvy
- zjistit, zda byl incident způsoben záměrně

3. Disciplinární přestupek

Disciplinárním přestupkem je zaměstnancem zaviněné porušení povinností stanovených v dokumentech „*Manuál uživatele*“ nebo „*Oprávnění a zodpovědnosti*“ uváděných v IS nebo jiných interních směrnic společnosti. Dále se pak jedná o porušení smluvních nebo zákonných ustanovení.

4. Sankce

Za disciplinární přestupek lze zaměstnanci uložit některou z těchto sankcí:

a) napomenutí,
b) udělení finanční pokuty dle závažnosti přestupku až do výše 100 000 Kč,
c) ukončení pracovního poměru,
d) řešení soudní cestou

Při ukládání sankcí se přihlíží k charakteru jednání, jímž byl přestupek spáchán, k okolnostem, za nichž k němu došlo, ke způsobeným následkům, k míře zavinění, jakož i k dosavadnímu chování zaměstnance, který se přestupku dopustil, a k jeho snaze o nápravu následků.

Od uložení sankce je možné upustit, jestliže samotné projednání přestupku vede k nápravě, zejména jde-li o přestupek spáchaný z nedbalosti anebo o přestupek méně závažný.

Sankce je buď neveřejná a oznamuje se pouze zaměstnanci, nebo je řešena veřejně pro výstrahu ostatním. O způsobu řešení rozhoduje komise.

Napomenutí

Napomenutí lze uložit pouze za méně závažný přestupek nebo za přestupek spáchaný z nedbalosti.

Udělení finanční pokuty

Finanční pokutu lze udělit v případě, že daný přestupek způsobil společnosti finanční ztrátu a zároveň se jedná o nezáměrný přestupek (například z nedbalosti). Výše finanční pokuty je stanovena do 100 000kč ve speciálních případech však může být stanovena i jinak. Je zohledňována především závažnost přestupku a dopad na společnost.

Ukončení pracovního poměru

V případě úmyslného porušení stanov společnosti nebo zákona ČR, může být zaměstnanci bezpodmínečně a s okamžitou platností ukončen pracovní poměr bez nároku na odstupné. A dále pak udělena finanční pokuta či zahájeno soudní stíhání.

Soudní stíhání

Pokud se jedná o záměrný přestupek s cílem poškodit společnost, bude tento přestupek řešen soudní cestou.

5. Lhůta k projednání disciplinárního přestupku

Disciplinární přestupek je nutné projednat nejpozději do 30 dní od jeho zjištění a to k tomu určenou komisí.

6. Disciplinární komise

Disciplinární komise je tvořena ředitelem společnosti a dvěma vybranými zaměstnanci (určuje ředitel společnosti), kteří rozumí dané problematice. V případě přestupku, který má vliv na některého z klientů společnosti může být přizván i zástupce dané společnosti. Rozhodující slovo v komisi má ředitel společnosti (pokud sám není předmětem disciplinárního řízení) a celé jednání je neveřejné a jeho obsah musí být udržován v tajnosti.

V případě, že se jeden ze dvou vybraných pracovníků nemůže jednání zúčastnit, je možné za něj vybrat náhradu. Je vyžadována účast všech členů komise a rozhodnutí je přijato pouze v případě souhlasu nadpoloviční většiny, jinak je posunuto k dalšímu projednání.

V případě prokázání předpojatosti nebo jakékoliv negativní angažovanosti jednoho z členů komise musí být tento člen nahrazen.

7. Zahájení disciplinárního řízení

Disciplinární řízení je zahájeno na základě informace o možném porušení interních směrnic společnosti nebo zákonu ČR. A to až poté, co je pečlivě přezkoumáno (viz. postup před zahájením disciplinárního řízení).

Disciplinární řízení je zahájeno, pokud došlo k závěru, že byl spáchán přestupek, na nějž se vztahuje disciplinární řád a to nejpozději do 30 dnů od zjištění daného přestupku.

8. Proces disciplinárního řízení

1. Je svolána disciplinární komise a předloženy zjištěné důkazy.
2. Daný problém je projednáván komisí a jsou stanoveny návrhy na možné sankce.

3. Komise určí datum projednání s osobou, která se přestupku dopustila. Daná osoba pak musí být včas informována o tom, že se vyžaduje její účast. V případě opakované neúčasti pozvané osoby má komise právo rozhodnout bez ní.
4. Osoba, která je předmětem řízení má možnost se vyjádřit a případně předložit důkazy.
5. Opětovné jednání komise a zvážení předložených důkazů a nových skutečností
6. Komise rozhodne o sankci.
7. Rozhodnutí komise je oznámeno zaměstnanci a jsou vykonány potřebné kroky.

Během procesu disciplinárního řízení, může být toto řízení zastaveno nebo zrušeno, pokud se tak komise rozhodne. Z každého řízení pak musí být veden a uchováván zápis.

Odpovědnosti při ukončení nebo změně pracovního vztahu (A.7.3.1)

Při zrušení pracovního vztahu doporučuji aplikovat následující postup:

1. Zaměstnanec musí navrátit veškerá zapůjčená aktiva (mobilní telefon, notebook tablet, klíče od společnosti a podobně).
2. Ve všech systémech musí být zrušena veškerá přístupová práva daného zaměstnance (firemní systém, vzdálený přístup, přístup do budovy společnosti a podobně).
3. Bude podepsána smlouva o ukončení pracovního poměru, jejíž součástí je požadování mlčenlivosti o firemních procesech a citlivých informacích.
4. Pokud byl pracovní poměr ukončen na základě disciplinárního řízení nebo za jiných nepříznivých okolností, může být zaměstnanec okamžitě vyveden z budovy a mohou být navržena zvláštní opatření.
5. O skutečnosti budou informováni další zaměstnanci.

4.1.3 Řízení přístupu (A.9)

Opatření se snaží omezit přístup k informacím a vybavení pro zpracování informací tím, že se snaží zajistit přístup pouze oprávněným uživatelům a naopak předcházet neoprávněnému přístupu. Uživatelé jsou činěni odpovědnými za ochranu svých autentizačních informací. A jsou navrženy vhodné postupy pro dodržení dostatečné bezpečnosti přístupu.

Používání tajných autentizačních informací (A.9.3.1)

Pro společnost je velmi důležité používání kvalitních autentizačních informací tak, aby bylo maximálně zabráněno neoprávněnému přístupu. Doporučuji, aby s těmito doporučeními byl seznámen každý zaměstnanec a bylo vyžadováno jejich plnění.

Doporučení pro vytvoření bezpečného hesla:

- délka hesla minimálně 8-10 znaků
- kombinace malých i velkých písmen a speciálních znaků
- nepoužívat diakritiku
- nepoužívat hesla související s nějakou reálnou skutečností (jméno psa, číslo domu a podobně)
- nepoužívat reálná slova (heslo by nemělo mít žádný jazykový význam)
- střídat písmena, znaky a číslice

Čeho se vyvarovat:

- nezapisovat si hesla na místa přístupná dalším osobám (ideálně si heslo nezapisovat nikam, to však při větším množství hesel nemusí být možné)
- heslo nesmí být s nikým sdíleno
- nepoužívat jedno heslo pro více přístupů
- nepoužívat stejná hesla pro osobní i pracovní účely
- neukládat hesla v rámci přihlašování (například na webových stránkách, do mailu, interního systému a podobně)

Pro zvýšení bezpečnosti autentizačních informací dále navrhuji následující doporučení:

- využívání dvoufaktorové autentizace (již bylo řešeno v rámci A.6.2.2) tam, kde je to možné
- používání otisků prstů a jiných unikátních identifikátorů (případně ještě doplněné o heslo)

Nadále je třeba hesla měnit v pravidelných intervalech, nebo pokaždé v případě náznaku možné kompromitace. Také doporučuji, aby ke každé službě bylo unikátní heslo a nedocházelo tak k duplicitám hesel. Pro zvýšení bezpečnosti může být omezen

počet pokusů pro přihlášení. A odpovědná osoba by měla být informována, o již nepoužívaných heslech, aby se předešlo nebezpečí útoku v případě jejich vyzrazení.

Bezpečné postupy přihlášení (A.9.4.2)

Pro přihlašování k systémům a aplikacím doporučuji používat pouze zařízení společnosti s dostatečně nastavenou bezpečnostní ochranou (viz. A.6.2.1 a A.6.2.2) a také bezpečná hesla (viz. A.9.3.1).

Pravidla pro bezpečné přihlášení:

- nikdy neukládat hesla a nepovolovat automatické přihlášení
- v rámci přihlašování by mělo být zobrazováno pouze minimum informací
- neměly by být přítomny žádné nápovědy nebo cokoliv co by se dalo zneužít
- proces přihlašovaní vykonávat až v případě, že jsou vyplněny všechny potřebné údaje
- v případě opakovaného přihlášení vytvořit bezpečnostní událost, a pokud bude překročen nastavený počet pokusů (obvykle tři), tak přihlašování zablokovat a informovat zodpovědnou osobu
- nemělo by být zobrazováno heslo ani počet jeho znaků
- používat vhodné a dostatečně bezpečné šifrování

Pro přihlašování k webovým aplikacím a službám doporučuji zavést True Key od společnosti Intel. Čímž bude dosaženo vícefaktorové autentizace a tedy větší bezpečnosti i v případě odhalení hesla.

True Key

Ochrana pomocí šifrování

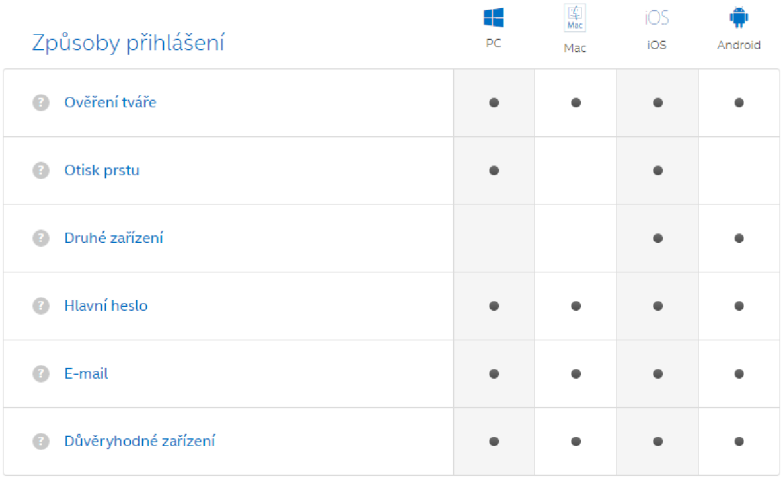
Aplikace True Key chrání hesla tak, že je zakóduje pomocí technologie AES-256, což je jeden z nejsilnějších dostupných šifrovacích algoritmů. Údaje pak může dešifrovat a získat k nim přístup pouze oprávněná osoba, a to pomocí vybraných faktorů.

Ověřování pomocí více faktorů

V aplikaci True Key se standardně používá ověřování pomocí více faktorů. Před přihlášením bude identita uživatele vždy ověřena na základě nejméně dvou faktorů. Do uživatelského profilu je možné přidat další faktory. Čím víc faktorů uživatel zvolí, tím silnější profil bude.

Jednoduchost a bezpečnost

Přihlášení v důvěryhodném zařízení může spočívat pouze v tom, že uživatel použije pouze jeden vybraný faktor, jako například tvář, otisk prstu nebo hlavní heslo. Když není používáno důvěryhodné zařízení (například při použití telefonu známého, osobního nebo půjčeného notebooku a podobně), bude identita vždy ověřena pomocí dvou uživatelem vybraných dalších faktorů.[166]

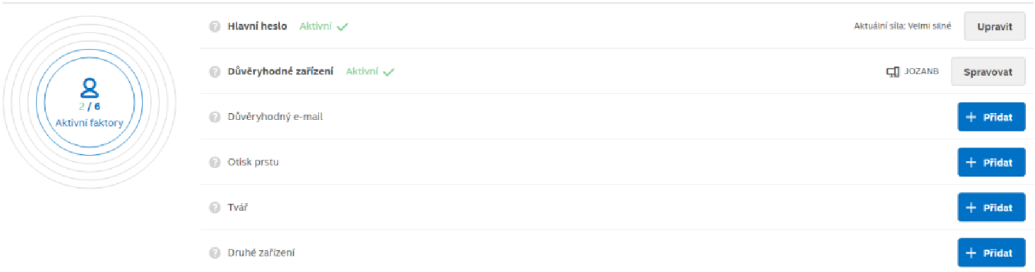


Obr. č. 22: Způsoby přihlášení v True Key[167]

Pro nejvyšší bezpečnost je možné zvolit i všech šest faktorů. Tuto technologii je možné zavést i pro přihlašování do Windows. Cena tohoto řešení je do patnácti hesel zdarma, dále pak za 20 USD ročně až do 2 000 hesel.

[166] *Snadné a bezpečné přihlašování v digitálním prostředí* [online]. [cit. 2016-05-11].

[167] vlastní tvorba



Obr. č. 23: Úrovně bezpečnosti v True Key[168]

K přihlašování do systému a aplikací, kde není možné zavést True Key doporučuji také používat vícefaktorovou autentizaci (například heslo ve spojení s otiskem prstu, zvláštním tokenem a podobně). A při vzdáleném přihlášení doporučuji použití šifrovaného protokolu SSH (v Linuxu možné zadávat příkazy z terminálu, ve Windows například pomocí PuTTY).

Systém správy hesel (A.9.4.3)

Společnosti doporučuji používat systém správy hesel KeePass (zdarma), 1Password (5 USD měsíčně) nebo Sticky Password (zdarma s možností rozšíření za 690 Kč ročně).

Všeobecná doporučení pro systém správy hesel:

a) prosazovat používání individuálních hesel a uživatelských ID pro udržení odpovědnosti
b) umožnit uživatelům volit a měnit si své vlastní heslo a zahrnout do systému postup pro potvrzení hesla, který by zamezoval možným překlepům
c) prosazovat výběr kvalitních hesel (viz A.9.3.1)
d) prosazovat obměnu hesel
e) donutit uživatele změnit si dočasně přidělené heslo při prvním přihlášení
f) udržovat záznam předchozích uživatelských hesel a zabránit uživatelům znovu je použít
g) při zadávání hesla nezobrazovat heslo na obrazovce
h) ukládat soubory hesel odděleně od dat aplikace
i) ukládat a přenášet hesla v chráněné podobě (např. v zašifrovaná nebo hashovaná)

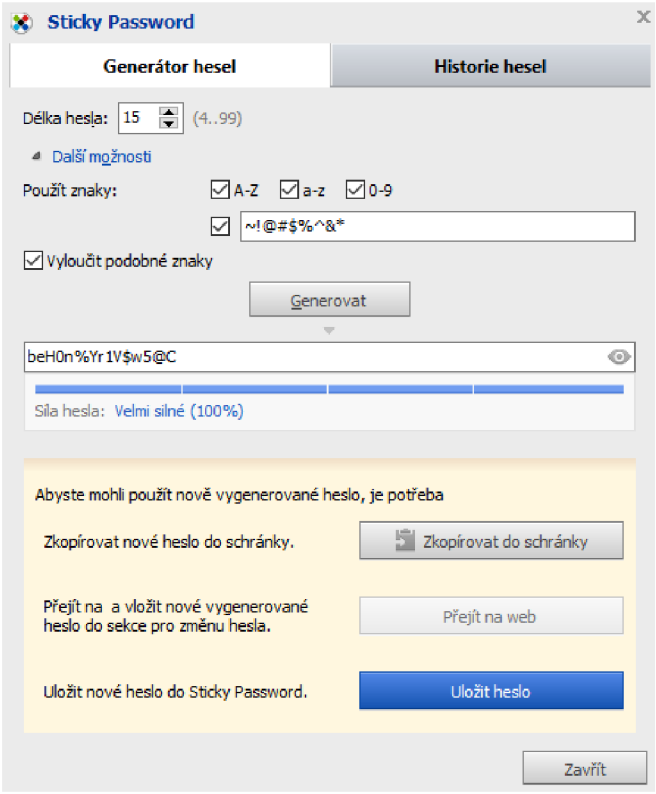
[168] vlastní tvorba

Většinu těchto doporučení všechny tři navrhované produkty splňují. Společnosti bych doporučil zvolit Sticky Password, protože oproti KeePass má lepší grafické rozhraní, zároveň však srovnatelnou funkcionalitu a oproti 1Password je zdarma.

Sticky Password

Sticky Password používá jedno hlavní heslo, které musí být dostatečně bezpečné (viz. A.9.3.1) a které musí být udržováno v tajnosti. Data jsou šifrována pomocí AES-256 a je možné nastavit přístup pomocí biometrických prvků (otisk prstu).

Program umožňuje generovat unikátní a bezpečná hesla na základě zadaných požadavků. To může být využito především při tvorbě nových účtů nebo aktualizaci hesel u již vytvořených účtů.



Obr. č. 24: Generátor hesla v StickyPassword[169]

Použití této aplikace, tedy společnosti umožní, používat dostatečně bezpečná hesla, unikátní pro každou aplikaci.

[169] vlastní tvorba

Použití privilegovaných programových nástrojů (A.9.4.4)

Počítače někdy mohou obsahovat programové nástroje, které jsou schopné překonat aplikační nebo systémové kontroly a to již v defaultní instalaci systému. Je tedy nutné tyto nástroje identifikovat a buď odstranit, nebo nastavit dostatečná bezpečnostní opatření.

Společnost zatím toto opatření řeší tak, že má definovány role, kterým je přístup k těmto nástrojům umožněn a všem ostatním je zakázán. To je řešeno pomocí nastavení v Active Directory. Dále jsou všechny defaultně nainstalované programové nástroje, které by mohly ohrozit bezpečnost buď odinstalovány, nebo je k nim zakázán přístup (opět pomocí Active Directory). Všeobecně platí zásada, že je povoleno jen to nejnutnější a vše ostatní je zakázáno. Není však řešena bezpečnost u privilegovaných uživatelů, kteří mají k těmto nástrojům přístup. Proto bych doporučoval zavést monitoring privilegovaných osob například pomocí řešení Privileged Session Manager od společnosti CyberArk.

Privileged Session Manager (PSM)

Izoluje, kontroluje a monitoruje přístup privilegovaných uživatelů a stejně tak i jejich aktivitu na kritických systémech včetně Unixu, Linuxu, Windows, databázích a virtuálních strojích.

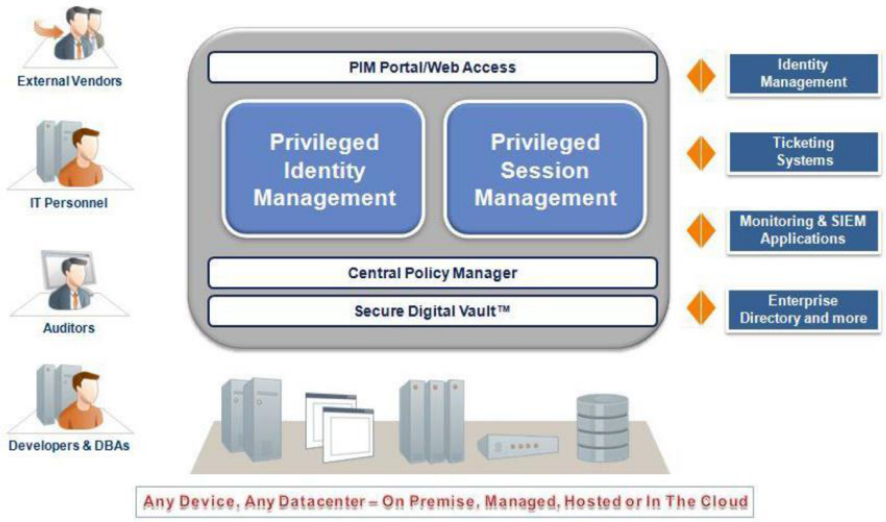
Monitorování v reálném čase umožňuje vedoucímu bezpečnosti sledovat činnost uživatele a odhalovat podezřelé události v reálném čase.

Vzdálená kontrola umožňuje okamžitě ukončit aktivitu podezřelého privilegovaného sezení, přímo z konzoly CyberArk.

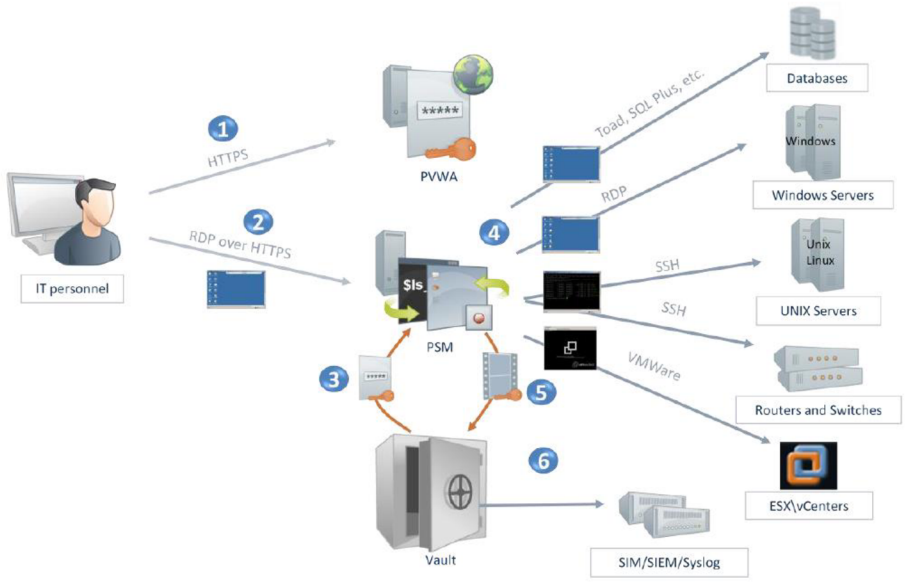
Detailní logy a video záznamy umožňují určit okamžik incidentu, jak začal a čím a kým byl způsoben. K těmto záznamům pak má přístup pouze správce a uživatelé do nich již nemohou zasahovat.

Bezpečnostní proxy server vytváří bezpečné, izolované prostředí pro oddělení uživatelských a koncových zařízení. Veškerá komunikace probíhá přes proxy server bez

použití agenta a je tedy jediným přístupovým bodem. Jsou tak monitorovány všechny privilegované aktivity.[170]



Obr. č. 25: Ochrana kritických aktiv před vnitřními a vnějšími hrozbami[171]

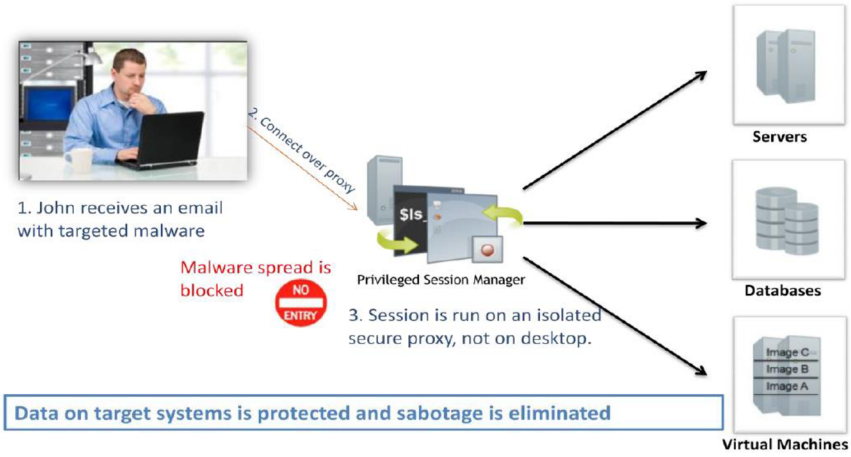


Obr. č. 26: PSM Architektura[172]

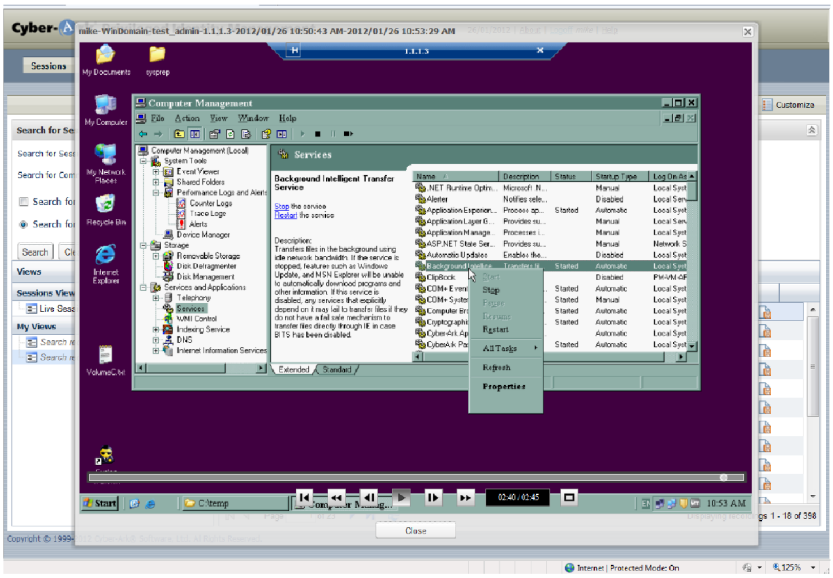
[170] *Privileged Session Manager* [online]. [cit. 2016-05-11].

[171] tamtéž

[172] tamtéž



Obr. č. 27: Oddělení klientů od cílových zařízení[173]



Obr. č. 28: Přehrání zaznamenané nahrávky[174]

Náklady

3x PSM for Servers - per-target Server Licenses	9 950 Kč
V případě zabezpečení i hypervizorů a databází	
5x PSM Concurrent User Licenses (Servers, DB and VM)	204 770 Kč

[173] *Privileged Session Manager* [online]. [cit. 2016-05-11].

[174] tamtéž

4.1.4 Kryptografie (A.10)

Používání kryptografie je vhodné pro zvýšení bezpečnosti při ochraně důvěrnosti, autentičnosti a integrity informací.

Politika pro použití kryptografických opatření (A.10.1.1)

Společnost už některá kryptografická opatření využívá a má i politiku pro jejich používání. Konkrétně využívá elektronických podpisů, šifrování (disku, dat) a SSH (pro vzdálenou správu a podobně). Pro zvýšení efektivity doporučuji zavést aplikaci I.CA Secom 2, pro práci s elektronickými podpisy, kterou nabízí První certifikační autorita, A.S. Pro generování klíčů pak opět doporučuji První certifikační autoritu, A.S.

I.CA Secom 2

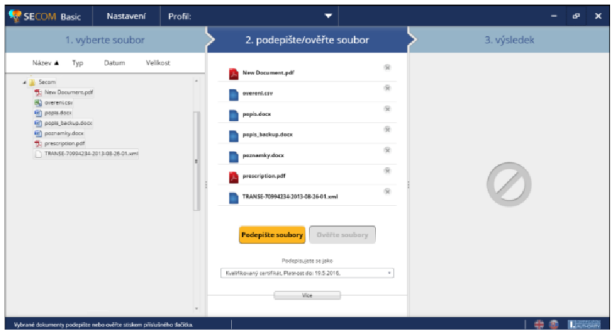
Software umožňuje vytváření a ověřování elektronických podpisů (až po dobu platnosti časového razítka). Dále je možné podepsat všechny typy souborů: textové soubory, obrázky v libovolných formátech, různé texty či binární soubory apod.

Základní přehled funkcí aplikace:

- Vytváření podpisů PAdES (podpis souborů typu PDF)
- Vytváření podpisů CAdES (podpis ostatních libovolných souborů)
- Možnost přidání kvalifikovaných časových razítek I.CA k elektronickému podpisu
- Viditelná prezentace podpisu PAdES v PDF dokumentech s variabilními texty a položkami převzatými z certifikátu
- Možnost podepisování a razítkování přímo z MS Word
- Hromadné podepisování dokumentů - složkové podepisování
- Vícenásobné podepisování dokumentů - podepsání již podepsaných dokumentů
- Hromadné ověřování dokumentů s elektronickým podpisem a časovým razítkem
- Možnost automatického zálohování podepsaných dokumentů
- Uživatelské profily - v jedné aplikaci lze podepisovat více certifikáty I.CA
- Možnost nastavení historie podepisování

- Automatické online aktualizace[175]

Aplikace vyhovuje požadavkům aktuálních technických standardů a norem ETSI a plně respektuje požadavky dané evropským Nařízením eIDAS (Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu).



Obr. č. 29: Hlavní okno aplikace Secom 2[176]

Obr. č. 30: Podpis více souboru[177]

Obr. č. 31: Informace o časovém razítku v elektronickém podpisu[178]

---

[175] *I.CA Secom* [online]. [cit. 2016-05-11].

[176] *I.CA Secom - popis* [online]. [cit. 2016-05-11].

[177] tamtéž

Všeobecně vzato tím, že jsou zavedeny tyto prostředky, je dosaženo vyšší důvěrnosti, integrity a bezpečnosti předávaných informací. Využití kryptografických technik je také možné předložit jako důkaz v případě bezpečnostních incidentů. Všechny techniky musí být v souladu s legislativou.

Náklady

Aplikace I.CA Secom	1 960,20Kč

4.1.5 Fyzická bezpečnost a bezpečnost prostředí (A.11)

Opatření mají zabraňovat neautorizovanému fyzickému přístupu do společnosti a možnému poškození či zásahům do informací a dalších aktiv společnosti. Dále mají chránit před ztrátou, poškozením, krádeži nebo kompromitaci aktiv a možnému přerušení činností organizace.

Podpůrné služby (A.11.2.2)

Společnost v současné době využívá UPS pro zajištění serverů v případě výpadku energie. Doporučuji však přikoupení a zavedení dvou dalších UPS k serverům Dell R320 a Dell R520, které jsou umístěny v sídle společnosti a na pobočce. Bude tak dosaženo větší spolehlivosti v případě, že by jeden ze záložních zdrojů selhal. Záložní zdroj APC Smart-UPS 1000VA LCD RM nabízí 10 minut provozu při plné zátěži a až 31 minut při zátěži na 50%. Doporučuji také pravidelnou osobní kontrolu UPS 1x za dva týdny. Pravidelnější kontroly a případná nastavení je možné realizovat pomocí vzdálené správy nebo přímo na zařízení.

Náklady

2x APC Smart-UPS 1000VA LCD RM	24 980 Kč

Údržba zařízení (A.11.2.4)

Doporučuji, aby zařízení společnosti byla z důvodu udržení stálé dostupnosti a integrity kontrolována v pravidelných intervalech (1x měsíčně). V rámci kontroly se bude zjišťovat, zda je zařízení používáno v souladu s doporučeními výrobce a zda je vše plně

[178] *I.CA Secom - popis* [online]. [cit. 2016-05-11].

funkční, případně jestli nehrozí nějaké možné riziko. Pokud bude zjištěna závada, doporučuji, aby opravu prováděl pouze zaškolený technik, čímž by se mělo předejít možných chybám v rámci servisu. Odpovědnost za kontrolu by měl vlastník aktiva.

Dále doporučuji, aby byly vedeny a uchovávány záznamy o tom, kdy byla kontrola provedena, kým byla provedena a její konkrétní popis. Předpokládá se, že společnost si kontrolu a údržbu bude zajišťovat sama. V případě, že by se rozhodla svěřit údržbu externí firmě, je třeba dát důraz na dostatečnou bezpečnost a důvěryhodnost.

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

Pro zvýšení bezpečnosti doporučuji přijmout zásadu prázdného stolu a obrazovky monitoru.

Doporučení:

- nastavit automatické zamykání obrazovky při nečinnosti a uzamčení PC vždy při odchodu (například pomocí kláves Win+L)
- odstranění všech prvků obsahujících informace, které by bylo možné zneužít, ať už se jedná o různá paměťová média, bloky, kousky papíru s informacemi a podobně
- všechny kritické dokumenty firmy, by měly být vždy bezpečně uzamčeny a nikdy neponechány volně bez dozoru
- při tisku důležitých dokumentů je ihned odebrat z tiskárny a při odchodu zkontrolovat, že nezůstaly důležité dokumenty v tiskárně nebo scanneru

Tyto zásady by měly být platné i pro práci na dálku, tedy mimo prostory organizace. A měly by s nimi být seznámeni všichni zaměstnanci.

4.1.6 Bezpečnost provozu (A.12)

Společnost už má poměrně velkou část bezpečnosti provozu pokrytou. Budu se tedy věnovat jen opatřením, která ještě nejsou zavedená, nebo která bych doporučoval revidovat. Cílem všech opatření této kategorie je především ochrana informací a vybavení proti poškození, ztrátě a využívání technických zranitelností.

Instalace softwaru na provozní systémy (A.12.5.1)

Doporučuji, aby každý zaměstnanec dostal zařízení s již předinstalovaným a nastaveným software. Sám by pak neměl právo žádný software instalovat a v případě potřeby instalace by musel požádat zodpovědnou osobu.

Pro zodpovědné osoby, které mají oprávnění pro instalaci a přístup i na provozní systémy doporučuji následující opatření:

- Před instalací nebo aktualizací software zvážit nutnost instalace a případná bezpečnostní rizika.
- Vést seznam instalovaného programového vybavení včetně aktuálních verzí.
- Před instalací, která by mohla mít dopad na celý systém provést komplexní zálohu zařízení.
- O každé aktualizaci nebo nové instalaci software vést záznam v IS.
- Řídit se postupy od dodavatele softwaru.
- Pravidelně kontrolovat (alespoň 1x ročně) podporu současného programového vybavení (hlavně u systémů) a v případě ukončení podpory informovat ředitele společnosti.

Před každou instalací nebo aktualizací software, doporučuji zvážit, zda je opravdu nutná. Nedoporučuji provádět instalaci pouze na základě toho, že vyšla nová verze softwaru, pokud tím nejsou řešeny nějaké zásadní nedostatky. Důraz by měl být dán na bezpečnost a stabilitu.

4.1.7 Bezpečnost komunikací (A.13)

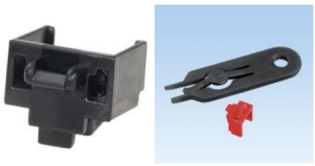
Cílem bezpečnosti komunikací je zajistit ochranu informací přenášených a používaných v sítích a jejich podpůrných prostředích. Tuto část má společnost již zavedenou a zvládnutou. Další částí je však ochrana bezpečnosti informací při přenosu v rámci organizace a s externími subjekty a této se budu nyní především věnovat.

Opatření v sítích (A.13.1.1)

Protože návrh a správa sítí je hlavní podnikatelskou činností společnosti, navrhuje a spravuje si společnost síť sama. Hlavní dohled na síť zabezpečuje ředitel společnosti. Schéma sítě je možné vidět v analytické části této práce.

Doporučuji, aby ředitel předal dohled nad sítí jednomu ze zaměstnanců, který by byl zodpovědný za monitoring sítě a kontrolu log souborů. Dále doporučuji aplikovat blokátory na nevyužité porty, zámky na již zavedené kabely a štítky s popisem na jednotlivé kabely, pro zvýšení přehlednosti.

Obr. č. 32: Zámek na konektor RJ45[179]



Obr. č. 33: Zámek portu RJ45[180]

Obr. č. 34: Štítky pro popis kabelů[181]

Další důležité prvky, jako je monitoring, správa zařízení, vzdálený přístup, servis a údržba zařízení a další, jsou řešeny v rámci jiných opatření nebo je společnost již má zavedeny.

Náklady

5x Panduit RJ45, Zámek na konektor RJ45 (PSL-DCPL)	4 380 Kč
5x Panduit RJ45, Zámek portu RJ45 černý (PSL-DCJB-BL)	3 355 Kč
1x Panduit, Štítky pro popis kabelů 200ks (S100X150VBC)	1 150 Kč

[179] *Standard Lock-in Device* [online]. [cit. 2016-05-11].

[180] *Jack module block-out device* [online]. [cit. 2016-05-11].

[181] *P1 Cassette* [online]. [cit. 2016-05-11].

Elektronické předávání zpráv (A.13.2.3)

Toto opatření je již řešeno v rámci jiných opatření, jako je Politika mobilních zařízení (A.6.2.1), Práce na dálku (A.6.2.2), Používání tajných autentizačních informací (A.9.3.1), Bezpečné postupy přihlášení (A.9.4.2) a Politika pro použití kryptografických opatření (A.10.1.1). Při aplikaci zmíněných opatření by mělo dojít k bezpečnému předávání elektronických zpráv.

Pro zvýšení bezpečnosti elektronické komunikace doporučuji:

- Nereagovat na žádné emaily vyzívající ke změně hesla, poslání důležitých informací nebo změně nastavení.
- Neuvádět svou e-mailovou adresu, pokud to není nutné a neposkytovat ji osobám, které jsou nedůvěryhodné (případně informovat osoby, kterým je poskytována e-mailová adresa, aby ji dále nešířily).
- Při náznaku zneužití adresy ihned informovat správce.
- Nekomunikovat přes sociální média (Messenger a podobně).
- Nenahrávat citlivé informace na veřejná uložiště (leteckaposta.cz, uloz.to).

Také mohu společnosti doporučit řešení GFI MailEssentials pro posílení ochrany před malware a GFI Archiver pro archivaci e-mailů.

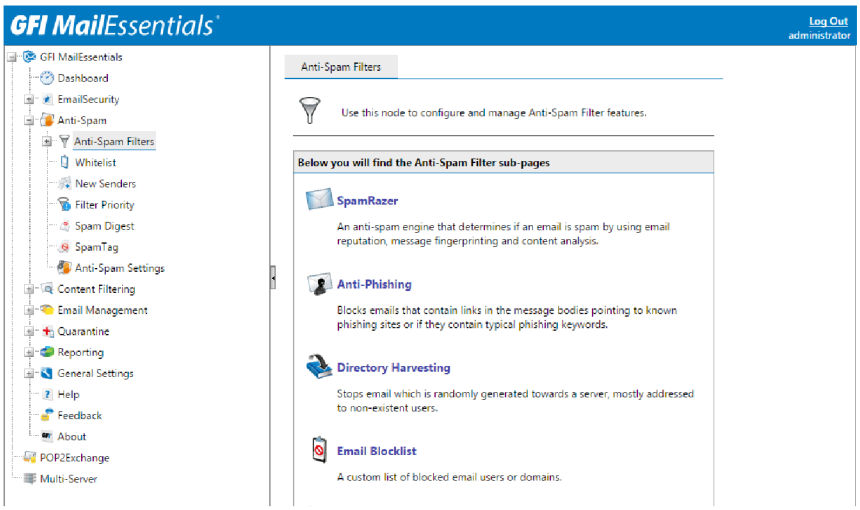
GFI MailEssentials

Nabízí zabezpečení poštovních serverů a ochranu před spamem.

Výkonný nástroj pro ochranu před spamem pro podniky

Toto řešení certifikované podle VBSpam používá několik anti-spamových filtrů, které kombinují techniku SpamRazer, greylisting, filtraci dle reputace IP adres, bayesovskou filtraci a další pokročilé techniky k zajištění úspěšnosti zachycení spamu vyšší než 99 % a minimálního počtu falešných pozitiv. To zaručuje bezpečné doručení důležitých emailů.[182]

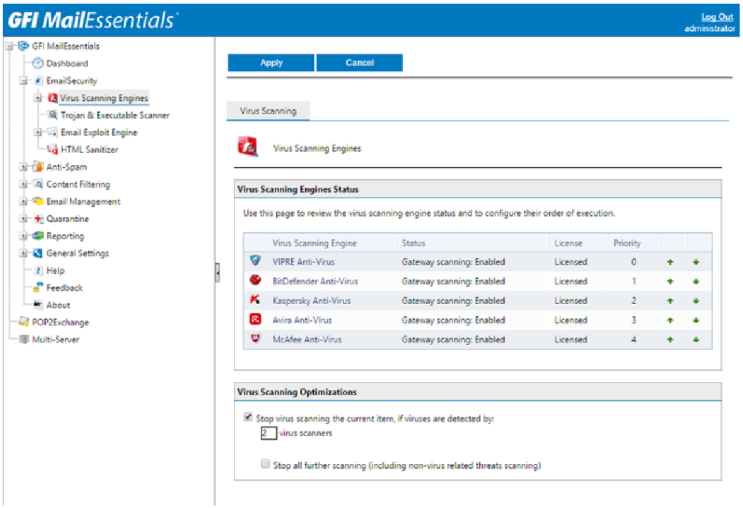
[182] *GFI MailEssentials* [online]. [cit. 2016-05-11].



Obr. č. 35: GFI MailEssentials Anti-Spam[183]

Použití několika antivirových enginů

Více antivirových enginů drasticky zkracuje čas, který je potřebný pro získání nejnovějších definic virů, a tak umožňuje rychleji reagovat na nejnovější hrozby. Protože každý engin má své vlastní metody heuristik a detekce, získáte maximální ochranu svého emailového prostředí.[184]



Obr. č. 36: GFI MailEssentials Virus Scanning Engine[185]

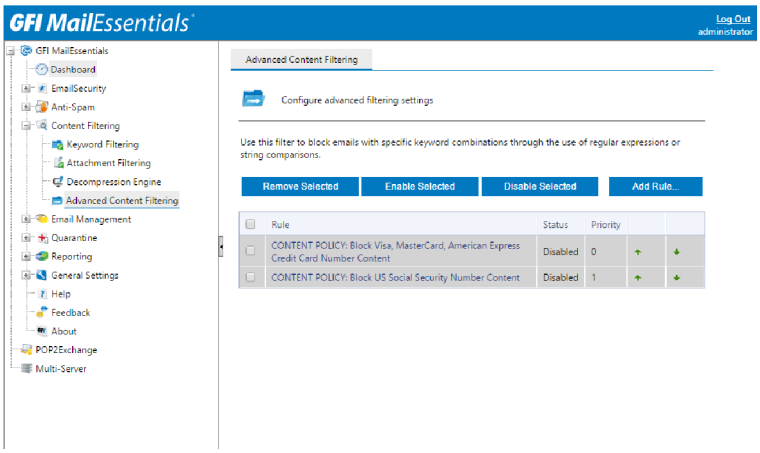
[183] *GFI MailEssentials* [online]. [cit. 2016-05-11].

[184] tamtéž

[185] tamtéž

Vynucení pravidel pro povolený obsah zpráv

Granulární vynucování zásad práce s obsahem emailů podle uživatele umožňuje mít pod kontrolou obsah, který prostřednictvím emailu vstupuje do sítě, anebo ji opouští. Tato funkce je založena na skutečných typech souborů, kontrole klíčových slov ze slovníku a kontrole regulárních výrazů, což pomáhá chránit Vaši společnost před nechtěnými nebo záměrnými úniky dat, čímž Vám pomáhá splnit zákonné požadavky.[186]



Obr. č. 37: GFI MailEssentials Advanced Content Filtering[187]

GFI Archiver

Archivace pro zvýšení produktivity, zlepšení správy a splnění zákonných požadavků.

Archivace emailů, souborů a kalendářů

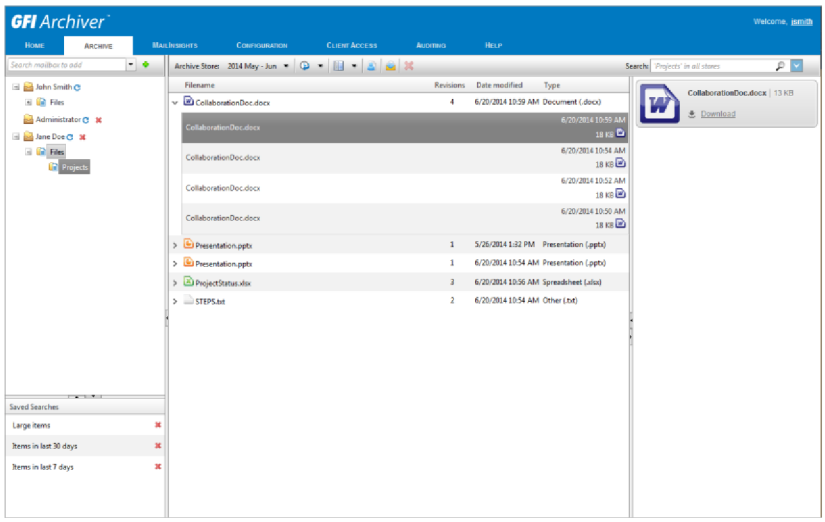
GFI Archiver archivuje emaily, soubory a záznamy z kalendářů. Jeho doplněk File Archiving Assistant (FAA) umožňuje sdílet soubory mezi uživateli a ukládat je centrálně a bezpečně bez toho, aniž byste museli spoléhat na poskytovatele online úložišť.[188]

---

[186] *GFI MailEssentials* [online]. [cit. 2016-05-11].

[187] tamtéž

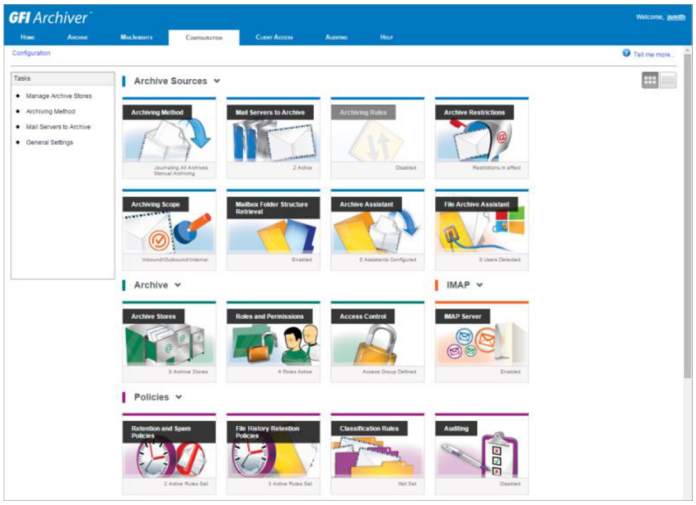
[188] tamtéž



Obr. č. 38: GFI Archiver File Archiving Assistant[189]

Bezpečná archivace docílí splněný zákonných požadavků

Minimalizujte právní riziko. Archivujte emaily i soubory v jejich původním stavu – v centralizovaném úložišti chráněném před falšováním – což Vám pomůže nejen splnit zákonné požadavky, ale také při interním vyšetřování.[190]



Obr. č. 39: GFI Archiver Archive Sources[191]

---

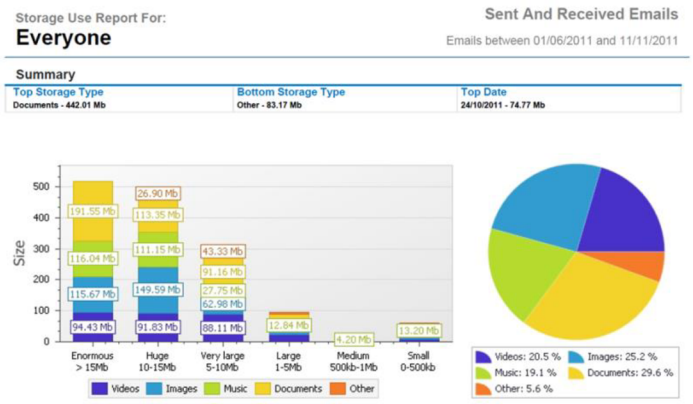
[189] *GFI MailArchiver* [online]. [cit. 2016-05-11].

[190] tamtéž

[191] tamtéž

Identifikace podnikových problémů

Váš archiv je zdrojem neuvěřitelných obchodních informací. Pomocí reportů můžete identifikovat zákonná rizika a zvýšit produktivitu. [192]



Obr. č. 40: GFI Archiver Report[193]

Náklady

5x GFI MailEssentials	2060 Kč / rok
5x GFI Archiver	2050 Kč / rok

[192] *GFI MailArchiver* [online]. [cit. 2016-05-11].

[193] tamtéž

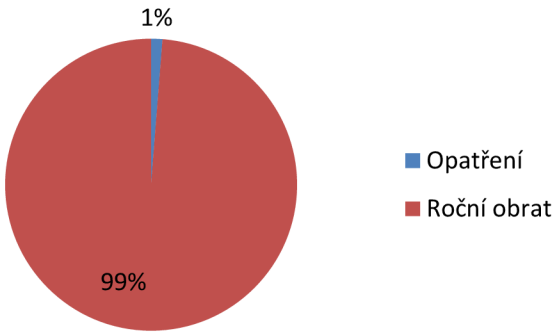
4.2. Ekonomické zhodnocení

Jednorázové náklady na zavedení opatření do společnosti činní 101 435 Kč. Každoročně pak údržba opatření přijde společnost na 65 610 Kč. Velká část nákladů je složena z licencí na software, asi třetinu tvoří náklady na školení a nejmenší část tvoří prvky na síťová opatření. Nejsou započteny žádné náklady na práci, protože společnost si vše bude realizovat sama.

Tab. č. 12: Náklady na zavedení opatření[194]

Opatření	Popis	Jednorázově	Každoročně
A.6.2.1	5x ESET Mobile Security pro Android	1 422 Kč	1 422 Kč
A.6.2.2	5x ESET Secure Authentication	8 428 Kč	8 428 Kč
A.7.2.2	VMware vSphere – Security	13 900 Kč	13 900 Kč
	Windows Server 2008/2012 - Praktická ochrana serverů a sítí	13 900 Kč	13 900 Kč
	Penetrační testování a etický hacking v sítích LAN	13 900 Kč	13 900 Kč
A.9.4.4	3x PSM for Servers - per-target Server Licenses	9 950 Kč	9 950 Kč
A.10.1.1	Aplikace I.CA Secom	1 960,20 Kč	0,00 Kč
A.11.2.2	2x APC Smart-UPS 1000VA LCD RM	24 980 Kč	0 Kč
A.13.1.1	5x Panduit RJ45, Zámek na konektor RJ45 (PSL-DCPL)	4 380 Kč	0 Kč
	5x Panduit RJ45, Zámek portu RJ45 černý (PSL-DCJB-BL)	3 355 Kč	0 Kč
	1x Panduit, Štítky pro popis kabelů 200ks (S100X150VBC)	1 150 Kč	0 Kč
A.13.2.3	5x GFI MailEssentials	2 060 Kč	2 060 Kč
	5x GFI Archiver	2 050 Kč	2 050 Kč
Celkem		**101 435 Kč**	**65 610 Kč**

Procentní vyjádření nákladů na zavedení opatření.



Graf č. 1: Náklady na zavedení opatření

[194] vlastní tvorba

5. Závěr

Cílem práce bylo navrhnout bezpečnostní opatření pro malou společnost na základě norem ISO 27 000. Společnost v současné době neuvažuje o certifikaci ISMS. Tato práce jí však poskytuje praktická doporučení pro zvýšení bezpečnosti na základě norem ČSN ISO/IEC 27 001:2013 a ČSN ISO/IEC 27 002:2013.

Pro přehlednost je práce rozdělena do tří částí.

První část obsahuje teoretická východiska a definuje obecné pojmy jako informace, bezpečnost organizace a bezpečnost informací. Popisuje PDCA model, definuje ISMS a vysvětluje pojem přiměřené bezpečnosti. Jsou zde také popsány vybrané normy z řady ISO/IEC 27 000, které byly využívány v práci a objasněn pojem bezpečnostní politiky firmy. Největší část pak byla věnována postupu realizace zabezpečení elektronických informací a analýze rizik.

Druhá část je zaměřena na analýzu společnosti – popis infrastruktury společnosti a spektra nabízených služeb. V rámci analýzy rizik byla identifikována a ohodnocena aktiva společnosti, stanovena rizika, hrozby a matice zranitelnosti a rizik. Při realizaci analýzy rizik jsem využíval normu ČSN ISO/IEC 27 005:2011. Analýza odhalila, že z hlediska aktiv jsou nejvíce ohroženou oblastí interní informace, data zákazníků, smlouvy a databázový software. Přičemž právě zneužití či poškození těchto aktiv by mohlo mít velmi velký až likvidační dopad na společnost. Z hlediska možných rizik, pak vystupuje do popředí riziko špionáže a škodlivého kódu, společně s neoprávněným použitím zařízení, jeho selháním nebo ztrátou energie. Výrazné bylo také riziko znečištění zařízení, jeho chybné použití, a poškození nebo zneužití dat. Analýza tedy odhalila, že největší pozornost by měla být věnovat zabezpečení a ochraně dat, školení uživatelů a péči o hardware.

Třetí část práce je věnována návrhu bezpečnostních opatření:

Pro zvyšování povědomí o bezpečnosti u zaměstnanců i v celé společnosti doporučuji navázat kontakt s odbornými fóry, účastnit se odborných událostí zaměřených na bezpečnost, které jsou dostupné na stránkách národního centra kybernetické bezpečnosti (www.govcert.cz) a každoročně absolvovat alespoň tři školení týkající se bezpečnosti. Jako vhodné organizace pro realizaci školení uvádím společnosti ESET a COMGUARD.

Pro zvýšení zabezpečení a ochrany dat doporučuji v rámci opatření zavést a používat produkt ESET Mobile Security pro Android, který umožňuje nastavit mobilní zařízení dle potřeb společnosti. Pro práci na dálku navrhuji zavedení produktu ESET Secure Authentication, který poskytuje vícefaktorovou autentizaci a umožňuje zajištění větší bezpečnost i v případě prozrazení hesla. Uvádím postupy pro vytvoření dostatečně bezpečného hesla a pro správu hesel doporučuji program Sticky Password. Byly stanoveny postupy pro bezpečné přihlášení a doporučena aplikace True Key pro bezpečné přihlašování do internetových aplikací. Tato aplikace chrání hesla pomocí šifrování AES-256 a vícefaktorové autentizace. Pro kontrolu privilegovaných uživatelů doporučuji použití software Privileged Session Manager (PSM) od společnosti CyberArk, který umožňuje monitorovat a spravovat privilegované uživatele. Doporučil jsem také software I.CA Secom 2 pro zjednodušení práce s elektronickými podpisy a navrhl přijetí zásady prázdného stolu a obrazovky monitoru a postupy pro instalaci softwaru na provozní systémy. Zvýšení bezpečnosti e-mailové komunikace doporučuji zajistit aplikacemi GFI MailEssentials pro posílení ochrany před malware a GFI Archiver pro archivaci e-mailů. Pro případ porušení bezpečnostních zásad společnosti navrhuji plán pro disciplinární řízení.

Z hlediska péče o hardware a fyzické bezpečnosti doporučuji přikoupení dvou UPS zdrojů APC Smart-UPS 1000VA LCD RM, čímž by měla být eliminována rizika spojená s výpadkem energie. Doporučil jsem také postup pro údržbu zařízení. V rámci síťových opatření doporučuji aplikovat blokátory na nevyužité porty, zámky na již zavedené kabely a štítky s popisem na jednotlivé kabely, pro zvýšení přehlednosti.

Bezpečnostní opatření byla navržena tak, aby snížila nebo úplně eliminovala rizika vycházející z analýzy a k jejich realizaci byly využity normy ČSN ISO/IEC 27 001:2013 a ČSN ISO/IEC 27 002:2013. Pro zavedení těchto opatření byla stanovena částka 101 435 Kč a pro každoroční údržbu pak 65 610 Kč. Z hlediska celkového obratu společnosti se jedná asi o 1%. Doporučuji tedy společnosti tato opatření zavést.

V příloze práce je vypracováno prohlášení o aplikovatelnosti, pro celistvý pohled na bezpečnost ve společnosti, podle normy ČSN ISO/IEC 27001:2013, přílohy A.

Stanovený cíl práce - návrh bezpečnostních opatření pro malou společnost, která v současné době neuvažuje o certifikaci ISMS, na základě norem ISO 27 000 – byl naplněn. Společnost obdržela analýzu rizik z nezávislého zdroje a návrh praktických opatření vedoucích k eliminaci současných rizik. Práce bude společnosti poskytnuta jako možný podklad pro další rozhodování.

Seznam použité literatury

[1] COMGUARD . *COMGUARD - Školicí centrum* [online]. [cit. 2016-05-11]. Dostupné z: https://www.comguard.cz/skolici-centrum/

[2] Cyberark. *Privileged Session Manager* [online]. [cit. 2016-05-11]. Dostupné z: http://www.cyberark.com/products/privileged-account-security-solution/privileged-session-manager/

[3] ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Řízení rizik bezpečnosti informací.* 2013. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

[4] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.

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

[6] ESET. *ESET Endpoint Security pro Android* [online]. [cit. 2016-05-11]. Dostupné z: http://www.eset.com/cz/firmy/produkty/android-security/

[7] ESET. *Dvoufaktorová autentizace* [online]. [cit. 2016-05-11]. Dostupné z: http://www.eset.com/cz/firmy/produkty/two-factor-authentication/

[8] ESET. *Řízení informační bezpečnosti* [online]. [cit. 2016-05-11]. Dostupné z: http://www.eset.com/cz/firmy/eset-services/rizeni-informacni-bezpecnosti/skoleni/

[9] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky*. Praha: Grada, 2006. Management v informační společnosti. 482 s. ISBN 80-247-1278-4.

[10] GFI. *GFI MailEssentials* [online]. [cit. 2016-05-11]. Dostupné z: http://gfi-software.cz/gfi-mailessentials/

[11] GFI. *GFI MailArchiver* [online]. [cit. 2016-05-11]. Dostupné z: http://gfi-software.cz/gfi-mailarchiver/

[12] INNC Network Communications. [online]. [cit. 2015-02-01]. Dostupné z: http://www.innc.cz/

[13] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Vyd. 1. Brno: Computer Press, 2007. 154 s. ISBN 978-80-251-1511-4.

[14] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013, 377 s. ISBN 9788072048724.

[15] PANDUIT. *Jack module block-out device* [online]. [cit. 2016-05-11]. Dostupné z: http://www.panduit.com/en/products-and-services/products/safety-and-security

[16] PANDUIT. *Standard Lock-in Device* [online]. [cit. 2016-05-11]. Dostupné z: http://www.panduit.com/en/products-and-services/products/safety-and-security

[17] PANDUIT. *P1 Cassette* [online]. [cit. 2016-05-11]. Dostupné z: http://www.panduit.com/en/products-and-services/products/safety-and-security

[18] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. 357 s. ISBN 978-80-7380-276-9.

[19] První certifikační autorita. *I.CA Secom* [online]. [cit. 2016-05-11]. Dostupné z: https://www.ica.cz/Secom

[20] První certifikační autorita. *I.CA Secom - popis* [online]. [cit. 2016-05-11]. Dostupné z: http://www.ica.cz/Secom-popis

[21] TrueKey . *Snadné a bezpečné přihlašování v digitálním prostředí* [online]. [cit. 2016-05-11]. Dostupné z: https://www.truekey.com/

Seznam použitých zkratek

AD	Active Directory
ČSN	Česká technická norma
DMZ	Demilitarizovaná zóna
HW	Hardware
ICT	Informační a komunikační technologie
IEEE	Institut pro elektrotechnické a elektronické inženýrství
IS	Informační systém
ISO	Mezinárodní organizace pro normalizaci
ISMS	Systém řízení bezpečnosti informací
IT	Informační technologie
LAN	Lokální síť
MGMT	Management
PDCA	Demingův cyklus (Plánuj, dělej, kontroluj, jednej)
SW	Software
VPN	Virtuální privátní síť
WAN	Počítačová síť na dlouhou vzdálenost

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam příloh

Příloha č. 1: Prohlášení o aplikovatelnosti

A.5 Politiky bezpečnosti informací

A.5.1 Směřování bezpečnosti informací vedením organizace

Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkající se činnosti organizace, příslušnými zákony a směrnicemi.

A.5.1.1 Politiky pro bezpečnost informací

Opatření: Soubor politik pro bezpečnost informací musí být definován, schválen vedením organizace, vydán a dán na vědomí všem zaměstnancům a relevantním externím stranám.

Vyloučeno: Ano

Způsob plnění požadavku: politika ISMS

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Opatření: Pro zjištění neustálé vhodnosti, přiměřenosti a efektivnosti musí být politiky pro bezpečnost informací přezkoumávány v plánovaných intervalech vždy, když nastane významná změna.

Vyloučeno: Ano

Způsob plnění požadavku: příručka ISMS

A.6 Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: Ustanovit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci.

A.6.1.1 Role a odpovědnosti bezpečnosti informací

Opatření: Musí být definovány a přiděleny odpovědnosti v oblasti bezpečnosti informací.

Vyloučeno: Ne

Způsob plnění požadavku: příručka ISMS

A.6.1.2 Princip oddělení povinností

Opatření: Pro snížení příležitostí k neoprávněné nebo neúmyslné modifikaci nebo zneužití aktiv organizace musí být zajištěno oddělení neslučitelných povinností a odpovědností.

Vyloučeno: Ano

Způsob plnění požadavku: Pro každého zaměstnance je vytvořen dokument s jeho povinnostmi a odpovědnostmi. Tento dokument je tvořen a schvalován vedením. Je přístupný z IS společnosti a po domluvě je možné ho modifikovat. Podle funkce jsou každému zaměstnanci přidělena práva a daná role. Pro jednotlivé role je definováno nastavení v Active direktory.

A.6.1.3 Kontakt s příslušnými orgány a autoritami

Opatření: Musí být udržovány přiměřené vztahy s příslušnými orgány a autoritami.

Vyloučeno: Ano

Způsob plnění požadavku: Protože se jedná o malou společnost, probíhá komunikace na denní bázi.

A.6.1.4 Kontakt se zájmovými skupinami

Opatření: Musí být udržovány přiměřené vztahy s odbornými zájmovými skupinami nebo ostatními odbornými fóry na bezpečnost a profesními sdruženími.

Vyloučeno: Ne

Způsob plnění požadavku: Pravidelné sledování stránek národního centra kybernetické bezpečnosti a účastnění se akcí.

A.6.1.5 Bezpečnost informací v řízení projektů

Opatření: Bezpečnost informací musí být zohledněna v řízení projektů nezávisle na typu projektu.

Vyloučeno: Ano

Způsob plnění požadavku: společnost každý projekt sestavuje na základě norem

A.6.2 Mobilní zařízení a práce na dálku.

Cíl: Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku.

A.6.2.1 Politika mobilních zařízení

Opatření: Musí být přijata politika a relevantní bezpečnostní opatření pro zvládání rizik spojených s používáním mobilních zařízení.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: manuál uživatele

A.6.2.2 Práce na dálku

Opatření: Musí být implementována politika a relevantní bezpečnostní opatření na ochranu informací, které jsou přístupné, zpracované nebo ukládané v místech pro práci na dálku.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: manuál uživatele

A.7 Bezpečnost lidských zdrojů

A.7.1 Před vznikem pracovního vztahu

Cíl: Zajistit, aby zaměstnanci a smluvní strany byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybráni vhodní kandidáti.

A.7.1.1 Prověřování

Opatření: Všichni uchazeči o zaměstnání musí být prověřeni podle platných zákonů, předpisů a v souladu s etikou. Prověření musí být prováděna na základě požadavků, týkajících se činnosti organizace, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, a také z hlediska potenciálních rizik.

Vyloučeno: Ano

Způsob plnění požadavku: Společnost si své zaměstnance vybírá pečlivě a výběrové řízení má několik kol, kdy uchazeč o zaměstnání komunikuje přímo s vedením společnosti a jsou prověřovány jeho znalosti a kompetence.

A.7.1.2 Podmínky pracovního vztahu

Opatření: Pracovní smlouvy uzavřené se zaměstnanci a smluvními stranami musí obsahovat ustanovení o jejich odpovědnostech a odpovědnostech organizace za bezpečnost informací.

Vyloučeno: Ano

Způsob plnění požadavku: pracovní smlouva

A.7.2 Během pracovního vztahu

Cíl: Zajistit, aby si zaměstnanci a smluvní strany byli vědomi a plnili si svoje povinnosti v oblasti bezpečnosti informací.

A.7.2.1 Odpovědnosti vedení organizace

Opatření: Vedení organizace musí po všech zaměstnancích a smluvních stranách požadovat dodržování bezpečnosti informací v souladu s ustanovenými politikami a postupy v organizaci.

Vyloučeno: Ne

Způsob plnění požadavku: příručka ISMS

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Opatření: Všichni zaměstnanci organizace, a je-li to relevantní i smluvní strany, musí s ohledem na svou pracovní náplň dostávat odpovídající vzdělávání a školení pro zvyšování povědomí bezpečnosti informací a musí být pravidelně informováni o změnách v politikách a postupech bezpečnosti informací.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: Ve společnosti probíhají pravidelná školení pro zvyšování kvalifikace zaměstnanců a jejich povědomí o bezpečnosti informací.

A.7.2.3 Disciplinární řízení

Opatření: Musí existovat formální proces disciplinárního řízení k přijetí opatření vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací.

Vyloučeno: Ne

Způsob plnění požadavku: příručka ISMS

A.7.3 Ukončení a změna pracovního vztahu

Cíl: Chránit zájmy organizace v rámci procesu změny nebo ukončení pracovního vztahu.

A.7.3.1 Odpovědnosti při ukončení nebo změně pracovního vztahu

Opatření: Odpovědnosti a povinnosti v oblasti bezpečnosti informací, které zůstávají platné po ukončení nebo změně pracovního vztahu, musí být definovány, komunikovány se zaměstnanci nebo smluvními stranami a prosazovány.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: smlouva; postup co dělat je v dokumentu „*Ukončení pracovního vztahu*“ v IS

A.8 Řízení aktiv

A.8.1 Odpovědnost za aktiva

Cíl: Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně.

A.8.1.1 Seznam aktiv

Opatření: Aktiva související s informacemi a vybavení pro zpracování informací musí být identifikována a seznam těchto aktiv musí být vytvořen a udržován aktuální.

Vyloučeno: Ano

Způsob plnění požadavku: Seznam aktiv je součástí analýzy této práce a bude zapsán do IS společnosti a udržován aktuální; účetnictví

A.8.1.2 Vlastnictví aktiv

Opatření: Aktiva udržovaná v seznamu musí mít určeného vlastníka.

Vyloučeno: Ano

Způsob plnění požadavku: plyne z účetnictví

A.8.1.3 Přípustné použití aktiv

Opatření: Musí být určena, dokumentována a implementována pravidla pro přípustné použití informací a aktiv souvisejících s informacemi a vybavením pro zpracování informací.

Vyloučeno: Ano

Způsob plnění požadavku: v rámci interní normy (například pro půjčení vozidla, apod.)

A.8.1.4 Navrácení aktiv

Opatření: Při ukončení pracovního vztahu, smluvního vztahu nebo dohody musí zaměstnanci pracovníci externích stran odevzdat veškerá jim svěřená aktiva, která jsou majetkem organizace.

Vyloučeno: Ano

Způsob plnění požadavku: smlouva; postup v IS co dělat při ukončení pracovního vztahu

A.8.2 Klasifikace informací

Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci.

A.8.2.1 Klasifikace informací

Opatření: Informace musí být klasifikovány s ohledem na zákonné požadavky, jejich hodnotu, kritičnost a citlivost vůči neoprávněnému prozrazení nebo modifikaci.

Vyloučeno: Ano

Způsob plnění požadavku: dokument „*Klasifikace informací*“ v IS; smlouvy o mlčenlivosti s bankami

A.8.2.2 Označování informací

Opatření: Pro označování informací musí být vytvořen a implementován vhodný soubor postupů, které jsou v souladu se schématem klasifikace informací přijatým organizací.

Vyloučeno: Ano

Způsob plnění požadavku: na základě dokumentu „*Klasifikace informací*“ v IS jsou informace označovány

A.8.2.3 Manipulaci s aktivy

Opatření: Pro manipulaci s aktivy musí být vytvořený a implementovány postupy v souladu se schématem klasifikace informací přijatým organizací.

Vyloučeno: Ano

Způsob plnění požadavku: na základě dokumentu „*Klasifikace informací*“ v IS jsou vedeny záznamy o manipulaci s aktivy

A.8.3 Manipulace s médii

Cíl: Předcházet neoprávněnému vyzrazení, modifikaci, odstranění nebo zničení informací uložených na médiích.

A.8.3.1 Správa výměnných médií

Opatření: Musí být implementovány postupy pro správu výměnných médií v souladu se schématem klasifikace informací přijatým organizací.

Vyloučeno: Ano

Způsob plnění požadavku: součástí dokumentu „*Klasifikace informací*“ v IS

A.8.3.2 Likvidace médií

Opatření: Média, pokud nejsou dále upotřebitelná, musí být bezpečně zlikvidována v souladu s formalizovanými postupy.

Vyloučeno: Ano

Způsob plnění požadavku: . Znehodnocuje se buď úplným fyzickým zničením nebo pokud je zařízení ještě funkční, např. disk, vícenásobným nulovým přepisem. (data nelze rekonstruovat)

A. 8.3.3 Přeprava fyzických médií

Opatření: Média obsahující informace musí být během přepravy chráněna proti neoprávněnému přístupu, zneužití nebo narušení.

Vyloučeno: Ano

Způsob plnění požadavku: dokument „*Manipulace s médii*“ v IS

A.9 Řízení přístupu

A.9.1 Požadavky organizace na řízení přístupu

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

A.9.1.1 Politika řízení přístupu

Opatření: Musí být ustanovena, dokumentována a přezkoumávána politika řízení přístupu v závislosti na požadavcích na činnosti organizace a bezpečnosti informací.

Vyloučeno: Ano

Způsob plnění požadavku: dokument „*Řízení přístupu*“ v IS

A.9.1.2 Přístup k sítím a síťovým službám

Opatření: Uživatelé musí mít přístup pouze k těm sítím a síťovým službám, pro jejichž použití byli zvlášť oprávněni.

Vyloučeno: Ano

Způsob plnění požadavku: Na základě dokumentu „*Oprávnění a role*“, který se nachází v IS, je nastaveno Active Directory i další služby tak, aby uživatel měl přístup pouze k prvkům nezbytně nutným pro svou činnost a vše ostatní měl zakázáno.

A.9.2 Řízení přístupu uživatelů

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

A.9.2.1 Registrace a zrušení registrace uživatele

Opatření: Pro přidělování přístupových práv musí být implementován proces formalizované registrace uživatele včetně jejího zrušení.

Vyloučeno: Ano

Způsob plnění požadavku: dokument „*Řízení přístupu*“ v IS

A.9.2.2 Správa uživatelských přístupů

Opatření: Pro přidělování a odebírání přístupových práv všem typům uživatelů ke všem systémům a službám musí být implementován formalizovaný proces správy uživatelských přístupů.

Vyloučeno: Ano

Způsob plnění požadavku: součástí dokumentu „*Řízení přístupu*“ v IS

A.9.2.3 Správa privilegovaných přístupových práv

Opatření: Musí být omezeno a řízeno přidělování a používání privilegovaných přístupových práv.

Vyloučeno: Ano

Způsob plnění požadavku: řešeno v dokumentu „*Oprávnění a role*“ v IS

A.9.2.4 Správa tajných autentizačních informací uživatelů

Opatření: Přidělování tajných autentizačních informací musí být řízeno formalizovaným procesem.

Vyloučeno: Ano

Způsob plnění požadavku: Zásady pro bezpečné heslo jsou sepsány v dokumentu „*Manuál uživatele*“ v IS a jsou doporučeny i některé generátory, které sami z části už tuto bezpečnost řeší.

A.9.2.5 Přezkoumání přístupových práv uživatelů

Opatření: Vlastníci aktiv musí v pravidelných intervalech přezkoumávat přístupová práva uživatelů.

Vyloučeno: Ano

Způsob plnění požadavku: vlastníci aktiv přezkoumávají přístupová práva uživatelů;

A.9.2.6 Odebrání nebo úprava přístupových práv

Opatření: Při ukončení nebo změně pracovního vztahu, smluvního vztahu nebo dohody musí být všem zaměstnancům a externím stranám odejmuta nebo pozměněna přístupová práva k informacím a vybavení pro zpracování informací.

Vyloučeno: Ano

Způsob plnění požadavku: smlouva; postup co dělat je v dokumentu „*Ukončení pracovního vztahu*“ v IS

A.9.3 Odpovědnosti uživatelů

Cíl: Učinit uživatele odpovědné za ochranu jejich autentizačních informací.

A.9.3.1 Používání tajných autentizačních informací

Opatření: Při používání tajných autentizačních informací musí být po uživatelích vyžadováno, aby dodržovali postupy stanovené organizací.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: smlouva; součástí dokumentu „*Manuál uživatele*“ v IS

A.9.4 Řízení přístupu k systémům a aplikacím

Cíl: Předcházet neautorizovanému přístupu k systémům a aplikacím.

A.9.4.1 Omezení přístupu k informacím

Opatření: V souladu s politikou řízení přístupu musí být omezen přístup k informacím a funkcím aplikace.

Vyloučeno: Ano

Způsob plnění požadavku: Na základě dokumentu „*Oprávnění a role*“, který se nachází v IS, je nastaveno Active Directory i další služby tak, aby uživatel měl přístup pouze k prvkům nezbytně nutným pro svou činnost a vše ostatní měl zakázáno.

A.9.4.2 Bezpečné postupy přihlášení

Opatření: Pokud to politika řízení přístupu vyžaduje, musí být přístup k systémům a aplikacím řízen postupy bezpečného přihlášení.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: součástí dokumentu „*Manuál uživatele*“ v IS, případně obsaženo v manuálech k jednotlivým aplikacím a službám (manuály se nachází také v IS)

A.9.4.3 Systém správy hesel

Opatření: Systémy správy hesel musí být interaktivní a musí zajišťovat použití kvalitních hesel.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: součástí dokumentu „*Manuál uživatele*“ v IS

A.9.4.4 Použití privilegovaných programových nástrojů

Opatření: Musí být omezeno a přísně kontrolováno použití programových nástrojů, které mohou být schopné překonat systémové nebo aplikační kontroly.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: Používání nástrojů, které jsou schopné překonat systémové, nebo aplikační kontroly je přísně kontrolováno vedením společnosti.

A.9.4.5 Řízení přístupu ke zdrojovým kódům

Opatření: Musí být omezen přístup ke zdrojovým kódům programů.

Vyloučeno: Ano

Způsob plnění požadavku: Nevztahuje se na společnost.

A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: Zajistit řádné a efektivní používání kryptografie k ochraně důvěrnosti, autentičnosti a / nebo integrity informací.

A.10.1.1 Politika pro použití kryptografických opatření

Opatření: Musí být vytvořena a implementována politika pro užívání kryptografických opatření na ochranu informací.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: součástí dokumentu „*Manuál uživatele*“ v IS

A.10.1.2 Správa klíčů

Opatření: Politika pro používání, ochranu a dobu existence kryptografických klíčů musí být vytvořena a implementována po celou dobu jejich životního cyklu.

Vyloučeno: Ano

Způsob plnění požadavku: Společnost správu klíčů nevyužívá.

A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.1 Bezpečnost oblasti

Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace.

A.11.1.1 Fyzický bezpečnostní perimetr

Opatření: Bezpečnostní perimetry musí být definovány a používány k ochraně oblastí, které obsahují citlivé nebo kritické informace a vybavení pro zpracování informací.

Vyloučeno: Ano

Způsob plnění požadavku: zásady pro fyzickou bezpečnost jsou v dokumentu „*Manuál uživatele*“; servery jsou umístěny v uzamčených místnostech nebo odmigrovány do datového centra, kde jsou vysoké standarty fyzické bezpečnosti; pro vstup do budovy je vyžadována autentizace a projití přes recepci, navíc je celý objekt střežen kamerovým systémem;

A.11.1.2 Fyzické kontroly vstupu

Opatření: Aby bylo zajištěno, že je přístup do bezpečných oblastí povolen pouze oprávněným osobám, musí být tyto oblasti chráněny vhodným systémem vstupních kontrol.

Vyloučeno: Ne

Způsob plnění požadavku: kontrola na recepci; autentizace pomocí vstupních karet; při vstupu k prvkům umístěným v datovém centru jsou přísné kontroly vstupu

A11.1.3 Zabezpečení kanceláří, místností a vybavení

Opatření: Musí být navržena a aplikována fyzická bezpečnost kanceláří, místností a vybavení.

Vyloučeno: Ano

Způsob plnění požadavku: řešeno v dokumentech „*Manuál uživatele*“ a „*Odpovědnosti a povinnosti*“

A.11.1.4 Ochrana před vnějšími hrozbami a hrozbami prostředí

Opatření: Musí být navržena a aplikována fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím.

Vyloučeno: Ano

Způsob plnění požadavku: migrace kritických prvků do server hostingového centra; v oblasti společnosti se přírodní katastrofy nevyskytují; zabezpečení pomocí CCTV, kontroly vstupu; pro případ havárii má firma havarijní plány

A.11.1.5 Práce v bezpečných oblastech

Opatření: Musí být navrženy a aplikovány postupy pro práci v bezpečných oblastech.

Vyloučeno: Ano

Způsob plnění požadavku: společnost se nachází v bezpečné oblasti; jsou vyžadovány karty pro vstup a fyzická kontrola; autentizace pro přístup k zařízením; další bezpečnostní zásady jsou v dokumentu „*Manuál uživatele*“ v IS

A.11.1.6 Oblasti pro nakládku a vykládku

Opatření: Přístupové body, jako oblasti pro nakládku a vykládku a další místa, kde se mohou neoprávněné osoby dostat do prostor organizace, musí být kontrolovány, a pokud je to možné, izolovány od vybavení pro zpracování informací, aby se zabránilo neoprávněnému přístupu k nim.

Vyloučeno: Ne

Způsob plnění požadavku: neoprávněné osoby se dostanou pouze na recepci a to až poté co je recepční pustí, celý prostor je střežen kamerovým systémem a protože společnost nemá velké prostory, není těžké sledovat pohyb osob po objektu

A.11.2 Zařízení

Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace.

A.11.2.1 Umístění zařízení a jeho ochrana

Opatření: Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.

Vyloučeno: Ano

Způsob plnění požadavku: zařízení umístěna v server hostingovém centru, nebo na zabezpečených místech uvnitř budovy

A.11.2.2 Podpůrné služby

Opatření: Zařízení musí být chráněno před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: zařízení u kterých je požadován nepřetržitý provoz mají UPS

A.12.2.3 Bezpečnost kabelových rozvodů

Opatření: Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat nebo podporu informačních služeb, musí být chráněny před odposlechem, rušením či poškozením.

Vyloučeno: Ano

Způsob plnění požadavku: Přístup k rozvaděčům a kabelovým trasám. Monitoring výpadků, kdy by se poznalo i krátkodobé přepojení.

A.11.2.4 Údržba zařízení

Opatření: Zařízení musí být správně udržováno pro zajištění jeho stálé dostupnosti a integrity.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: v dokumentu „*Povinnosti a odpovědnosti*“ jsou zakomponovány povinnosti související s údržbou konkrétních zařízení

A.11.2.5 Přemístění aktiv

Opatření: Zařízení, informace nebo software nesmí být přemísťováno mimo prostory organizace bez předchozího schválení.

Vyloučeno: Ano

Způsob plnění požadavku: Přemístění větších zařízení jako je server a podobně je vždy nejprve projednáno a musí být schváleno vedením. Pro mobilní zařízení a notebooky jsou uvedeny bezpečnostní postupy v dokumentu „*Manuál uživatele*“ v IS

A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace

Opatření: Aktiva mimo prostory organizace musí být zabezpečena s přihlédnutím k rozdílným rizikům, která vyplívají z jejich použití mimo organizaci.

Vyloučeno: Ano

Způsob plnění požadavku: pojištění; standardy server hostingového centra

A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení

Opatření: Všechny prvky zařízení obsahující paměťová média musí být zkontrolovány tak, aby bylo zajištěno, že před jejich likvidací nebo opakovaným použitím budou jakákoliv citlivá data a licencovaný software odstraněny nebo bezpečně přepsány.

Vyloučeno: Ano

Způsob plnění požadavku: Znehodnocuje se buď úplným fyzickým zničením, nebo pokud je zařízení ještě funkční, např. disk, vícenásobným nulovým přepisem (data nelze rekonstruovat)

A.11.2.8 Uživatelská zařízení bez obsluhy

Opatření: Uživatelé musí zajistit přiměřenou ochranu zařízení bez obsluhy.

Vyloučeno: Ano

Způsob plnění požadavku: dokument „*Manuál uživatele*“ v IS

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Opatření: Musí být přijata zásada prázdného stolu ve vztahu k dokumentům a výměnným paměťovým médiím a zásad prázdné obrazovky monitoru u vybavení pro zpracování informací.

Vyloučeno: Ne

Způsob plnění požadavku: dokument „*Manuál uživatele*“ v IS

A.12 Bezpečnost provozu

A.12.1 Provozní postupy a odpovědnosti

Cíl: Zajistit správný a bezpečný provoz vybavení pro zpracování informací.

A.12.1.1 Dokumentované provozní postupy

Opatření: Provozní postupy musí být dokumentovány a musí být dostupné uživatelům podle potřeby.

Vyloučeno: Ano

Způsob plnění požadavku: společnost má dokumentaci sítě a měla i ISO – Příručku kvality

A.12.1.2 Řízení změn

Opatření: Změny v organizaci a jejích procesech, v prostředích pro zpracování informací a systémech, které ovlivňují bezpečnost informací, musí být řízeny.

Vyloučeno: Ano

Způsob plnění požadavku: změny jsou komunikovány a řízeny vedením

A.12.1.3 Řízení kapacit

Opatření: Pro zajištění požadovaného výkonu systému, s ohledem na budoucí kapacitní požadavky, musí být monitorováno, nastaveno a předvídáno využití zdrojů.

Vyloučeno: Ano

Způsob plnění požadavku: monitoring a zajištění požadovaného výkonu vykonává přímo ředitel společnosti; denní komunikace ve společnosti umožňuje odhalit případné nedostatky

A.12.1.4 Princip oddělení prostředí vývoje, testování a provozu

Opatření: Pro snížení rizika neoprávněného přístupu nebo změn provozního prostředí musí být odděleno prostředí vývoje, testování a provozu.

Vyloučeno: Ano

Způsob plnění požadavku: Nevztahuje se na společnost

A.12.2 Ochrana proti malwaru

Cíl: Zajistit, aby informace a vybavení pro zpracování informací byly chráněny proti malwaru.

A.12.2.1 Opatření proti malwaru

Opatření: Na ochranu proti malwaru musí být implementována opatření na jeho detekci, prevenci a obnovu, a to ve spojení s odpovídajícím bezpečnostním povědomím uživatelů.

Vyloučeno: Ano

Způsob plnění požadavku: bezpečnostní software od firmy ESET; nastavení firewallu; pravidelné zálohy; dokument „*Manuál uživatele*“ v IS; řešeno i v rámci jiných opatření

A.12.3 Zálohování

Cíl: Chránit proti ztrátě dat.

A.12.3.1 Zálohování informací

Opatření: Záložní kopie informací, softwaru a binárních obrazů systému musí být pořizovány v pravidelných intervalech v souladu se schválenou politikou zálohování.

Vyloučeno: Ano

Způsob plnění požadavku: je sestaven denní, týdenní a měsíční plán, jak na fyzická média, tak po síti s různou geolokací.

A.12.4 Zaznamenávání formou logů a monitorování

Cíl: Zaznamenávat události a vytvářet záznamy.

A.12.4.1 Zaznamenávání událostí formou logů

Opatření: Musí být pořizovány, uchovávány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.

Vyloučeno: Ano

Způsob plnění požadavku: součástí záloh

A.12.4.2 Ochrana logů

Opatření: Prostředky pro zaznamenávání formou logů a logy musí být chráněny proti zfalšování a neoprávněnému přístupu.

Vyloučeno: Ano

Způsob plnění požadavku: zálohy jsou geolokačně na různých místech, k části záloh je nutné zvláštní oprávnění – SW přístup

A.12.4.3 Logy o činnosti administrátorů a operátorů

Opatření: Aktivity systémového administrátora a systémového operátora musí být logovány a logy chráněny a pravidelně přezkoumávány.

Vyloučeno: Ano

Způsob plnění požadavku: opět součástí záloh

A.12.4.4 Synchronizace hodin

Opatření: Hodiny všech důležitých systémů pro zpracování informací musí být v rámci organizace nebo bezpečnostních domén synchronizovány s jediným referenčním zdrojem času.

Vyloučeno: Ano

Způsob plnění požadavku: synchronizace se světovými atomovými hodinami

A.12.5 Správa provozního softwaru

Cíl: Zajistit integritu provozních systémů.

A.12.5.1 Instalace softwaru na provozní systémy

Opatření: Musí být implementovány postupy řízené instalace softwaru na provozních systémech.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: Na základě dokumentu „*Oprávnění a role*“, který se nachází v IS, je nastaveno Active Directory i další služby tak, aby uživatel měl přístup pouze k prvkům nezbytně nutným pro svou činnost a vše ostatní měli zakázáno; pro důležité instalace jsou vypracovány postupy v IS

A.12.6 Řízení technických zranitelností

Cíl: Zabránit využívání technických zranitelností.

A.12.6.1 Řízení technických zranitelností

Opatření: Musí být zajištěno včasné získání informací o existenci technických zranitelností provozovaných informačních systémů, vyhodnocena úroveň ohrožení organizace vůči těmto zranitelnostem a přijata příslušná opatření na zvládání souvisejících rizik.

Vyloučeno: Ano

Způsob plnění požadavku: zdvojení kritických systémů (redundance)

A.12.6.2 Omezení instalace softwaru

Opatření: Musí být ustanovena a implementována pravidla ohledně instalace softwaru uživateli.

Vyloučeno: Ano

Způsob plnění požadavku: součástí dokumentu „*Oprávnění a role*“, který se nachází v IS; pro důležité instalace jsou vypracovány postupy v IS

A.12.7 Hlediska auditu informačních systémů

Cíl: Minimalizovat dopady auditních činností na provozní systémy.

A.12.7.1 Opatření k auditu informačních systémů

Opatření: Požadavky auditu a činnosti zahrnující verifikaci provozních systémů musí být pečlivě naplánovány a schváleny, aby se minimalizovalo narušení procesů organizace.

Vyloučeno: Ano

Způsob plnění požadavku: společnost si zajišťuje audit sama (provádí ředitel společnosti)

A.13 Bezpečnost komunikací

A.13.1 Správa bezpečnosti sítě

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

A.13.1.1 Opatření v sítích

Opatření: K ochraně informací v systémech a aplikacích musí být sítě řízeny, spravovány a kontrolovány.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: společnost si bezpečnost sítě spravuje a řídí

A.13.1.2 Bezpečnost síťových služeb

Opatření: Musí být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní mechanismy, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb, ať už jsou zajišťovány interně nebo cestou outsourcingu.

Vyloučeno: Ano

Způsob plnění požadavku: společnost do dohod zahrnuje bezpečnostní mechanizmy dle domluvy se zákazníkem; svoji bezpečnost si řeší společnost sama (viz. analýza v této práci)

A.13.1.3 Princip oddělení v sítích

Opatření: V sítích musí být odděleny skupiny informačních služeb, uživatelů a informačních systémů.

Vyloučeno: Ano

Způsob plnění požadavku: několik virtuálních sítí, VLAN

A.13.2 Přenos informací

Cíl: Zajistit bezpečnost informací při jejich přenosu v rámci organizace a s externími subjekty.

A.13.2.1 Politiky a postupy při přenosu informací

Opatření: Musí existovat formalizované politiky, postupy a opatření k ochraně přenosu informací pomocí jakéhokoliv typu komunikačního vybavení.

Vyloučeno: Ano

Způsob plnění požadavku: součástí dokumentu „*Manuál uživatele*“ v IS

A.13.2.2 Dohody o přenosu informací

Opatření: Dohody se musí zabývat zabezpečeným přenosem informací týkající se činností organizace mezi organizací a externími stranami.

Vyloučeno: Ano

Způsob plnění požadavku: společnost sepisuje dohody vždy dle zákazníka a důležitosti informace

A.13.2.3 Elektronické předávání zpráv

Opatření: Musí být vhodným způsobem chráněny elektronicky přenášené informace.

Vyloučeno: Ne (revidovat)

Způsob plnění požadavku: elektronický podpis, šifrování

A.13.2.4 Dohody o utajení nebo mlčenlivosti

Opatření: Musí být identifikovány, pravidelně přezkoumávány a dokumentovány požadavky na dohody o utajení nebo na dohody o mlčenlivosti reflektující potřeby organizace na ochranu informací.

Vyloučeno: Ano

Způsob plnění požadavku: uzavřené smlouvy; zákon č. 101/2000 Sb., o ochraně osobních údajů; ustanoveními občanského zákoníku o ochraně vlastnictví

A.14 Akvizice, vývoj a údržba systémů

A.14.1 Bezpečnostní požadavky informačních systémů

Cíl: Zajistit, aby se bezpečnost informací stala nedílnou součástí informačních systémů v jejich celém životním cyklu. To zahrnuje i požadavky na informační systémy, které poskytují služby ve veřejných sítích.

A.14.1.1 Analýza a specifikace požadavků bezpečnosti informací

Opatření: V požadavcích na nové informační systémy nebo na rozšíření existujících systémů musí být obsaženy také požadavky týkající se bezpečnosti informací.

Vyloučeno: Ano

Způsob plnění požadavku: Nesouvisí se společností

A.14.1.2 Zabezpečení aplikačních služeb ve veřejných sítích

Opatření: Informace přenášené ve veřejných sítích v rámci aplikačních služeb musí být chráněny před podvodnými aktivitami, zpochybňováním smluv, neoprávněným vyzrazením a modifikací.

Vyloučeno: Ano

Způsob plnění požadavku: transakční zpracování, elektronické podpisy, šifrování mailu

A.14.1.3 Ochrana transakcí aplikačních služeb

Opatření: Musí být zajištěna ochrana informací přenášených při transakcích aplikačních služeb tak, aby se zabránilo neúplnému přenosu informací, chybnému směrování,

neoprávněné změně zpráv, neoprávněnému vyzrazení, neoprávněné duplikaci nebo opakování přenosu zpráv.

Vyloučeno: Ano

Způsob plnění požadavku: transakční zpracování, elektronické podpisy, šifrování mailu

A.14.2 Bezpečnost v procesech vývoje a podpory

Cíl: Zajistit, aby bezpečnost informací byla navrhována a implementována v životním cyklu vývoje informačních systémů.

A.14.2.1 Politika bezpečného vývoje

Opatření: Musí být ustanovena v rámci organizace aplikována pravidla pro vývoj softwaru a systémů.

Vyloučeno: Ano

Způsob plnění požadavku: Nesouvisí se společností

A.14.2.2 Postupy řízení změn systému

Opatření: Pomocí formalizovaných postupů řízení změn musí být řízeny změny systémů v rámci jejich životního cyklu vývoje.

Vyloučeno: Ano

Způsob plnění požadavku: Nesouvisí se společností

A.14.2.3 Technické přezkoumání aplikací po změnách provozní platformy

Opatření: V případě změny provozní platformy musí být přezkoumány a otestovány aplikace kritické pro činnost organizace, aby se zajistilo, že změny nemají nepříznivý dopad na provoz nebo bezpečnost organizace.

Vyloučeno: Ano

Způsob plnění požadavku: Nesouvisí se společností

A.14.2.4 Omezení změn softwarových balíků

Opatření: Modifikace softwarových balíků musí být omezeny na nezbytné změny a veškeré provádění změny musí být přísně řízeny.

Vyloučeno: Ano

Způsob plnění požadavku: Na základě dokumentu „*Oprávnění a role*“, který se nachází v IS, je nastaveno Active Directory i další služby tak, aby uživatel měl přístup pouze k prvkům nezbytně nutným pro svou činnost a vše ostatní měl zakázáno

A.14.2.5 Principy budování bezpečných systémů

Opatření: Principy budování bezpečných systémů musí být ustanoveny, dokumentovány, udržovány a aplikovány při implementaci informačních systémů.

Vyloučeno: Ano

Způsob plnění požadavku: Nesouvisí se společností

A.14.2.6 Prostředí bezpečného vývoje

Opatření: Pro vývoj systémů a jejich integraci, pokrývající celý životní cyklus vývoje systémů, musí organizace vytvořit a přiměřeně chránit prostředí bezpečného vývoje systémů.

Vyloučeno: Ano

Způsob plnění požadavku: Nesouvisí se společností

A.14.2.7 Outsourcovaný vývoj

Opatření: Organizace musí dohlížet a monitorovat činnosti outsourcovaného vývoje systému.

Vyloučeno: Ano

Způsob plnění požadavku: Nesouvisí se společností

A.14.2.8 Testování bezpečnosti systému

Opatření: Během vývoje musí být prováděno testování funkčnosti bezpečnosti.

Vyloučeno: Ano

Způsob plnění požadavku: Nesouvisí se společností

A.14.2.9 Testování akceptace systémů

Opatření: Pro nové informační systémy, aktualizace a nové verze musí být ustanoveny testovací postupy a odpovídající kritéria a akceptace.

Vyloučeno: Ano

Způsob plnění požadavku: Nesouvisí se společností

A.14.3 Data pro testování

Cíl: Zajistit ochranu dat používaných pro testování.

A.14.3.1 Ochrana dat pro testování

Opatření: Data pro testování musí být pečlivě vybrána, chráněna a kontrolována.

Vyloučeno: Ano

Způsob plnění požadavku: Nesouvisí se společností

A.15 Dodavatelské vztahy

A.15.1 Bezpečnost informací v dodavatelských vztazích

Cíl: Zajistit ochranu aktiv organizace, ke kterým mají dodavatelé přístup.

A.15.1.1 Politika bezpečnosti informací pro dodavatelské vztahy

Opatření: Požadavky bezpečnosti informací na snížení rizik spojených s přístupem dodavatelů k aktivům organizace musí být odsouhlaseny s dodavateli a dokumentovány.

Vyloučeno: Ano

Způsob plnění požadavku: Dodavatelé nemají přístup k aktivům společnosti.

A.15.1.2 Bezpečnostní požadavky v dohodách s dodavateli

Opatření: Všechny požadavky relevantní bezpečnosti informací musí být ustanoveny a odsouhlaseny s každým dodavatelem, který může přistupovat k informacím organizace, zpracovávat je, ukládat, komunikovat nebo je zajišťovat prvky IT infrastruktury.

Vyloučeno: Ano

Způsob plnění požadavku: Spíše ze strany dodavatele. Dohody o vývozu šifrování apod. Viz. podmínky Cisco, Dell, Microsoft …

A.15.1.3 Dodavatelský řetězec informačních a komunikačních technologií

Opatření: Dohody s dodavateli musí zahrnovat požadavky na rizika bezpečnosti informací spojená s dodavatelským řetězcem služeb a produktů informačních a komunikačních technologií.

Vyloučeno: Ano

Způsob plnění požadavku: Společnost není schopna ovlivnit z důvodu své malé velikosti a naopak velké síly dodavatele.

A.15.2 Řízení dodávek služeb dodavatelů

Cíl: Udržovat dohodnutou úroveň bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami.

A.15.2.1 Monitorování a přezkoumávání služeb dodavatelů

Opatření: Organizace musí pravidelně monitorovat, přezkoumávat a auditovat dodávky služeb dodavatelů.

Vyloučeno: Ne

Způsob plnění požadavku: V současnosti se kontroluje, zda víckrát v dodávce dodavatel neselhal.

A.15.2.2 Řízení změn ve službách dodavatelů

Opatření: Změny v poskytování služeb dodavateli, včetně změn v udržování a zlepšování existujících politik, postupů a opatření bezpečnosti informací, musí být řízeny s ohledem na kritičnost informací, systémů a procesů organizace, které jsou součástí těchto změn, a s ohledem na opakované posouzení rizik.

Vyloučeno: Ne

Způsob plnění požadavku: Stanoveno smlouvou.

A.16 Řízení incidentů bezpečnosti informací

A.16.1 Řízení incidentů bezpečnosti informací a zlepšování

Cíl: Zajistit odpovídající a efektivní přístup ke zvládání incidentů bezpečnosti informací zahrnujícímu komunikaci ohledně bezpečnostních událostí a slabých míst.

A.16.1.1 Odpovědnosti a postupy

Opatření: Pro zajištění rychlé, efektivní a systematické reakce na incidenty bezpečnosti informací musí být ustaveny odpovědnosti a postupy pro zvládání incidentů bezpečnosti informací.

Vyloučeno: Ano

Způsob plnění požadavku: dokument „*Odpovědnosti a povinnosti*“ v IS

A.16.1.2 Hlášení událostí bezpečnosti informací

Opatření: Události bezpečnosti informací musí být co nejrychleji hlášeny příslušnými řídícími kanály.

Vyloučeno: Ano

Způsob plnění požadavku: události jsou hlášeny hned pomocí mobilního telefonu, Skype nebo e-mailu

A.16.1.3 Hlášení slabých míst bezpečnosti informací

Opatření: Po zaměstnancích a smluvních stranách používající informační systémy a služby musí být vyžadováno, aby si všímali a hlásili jakákoliv slabá místa bezpečnosti informací v systémech nebo službách nebo podezření na ně.

Vyloučeno: Ano

Způsob plnění požadavku: řešeno v dokumentech „*Manuál uživatele*“ a „*Odpovědnosti a povinnosti*“ v IS

A.16.1.4 Posouzení a rozhodnutí o událostech bezpečnosti informací

Opatření: Události bezpečnosti informací musí být posouzeny a musí být rozhodnuto, zda mají být klasifikovány jako incidenty bezpečnosti informací.

Vyloučeno: Ano

Způsob plnění požadavku: posuzování a rozhodování provádí ředitel společnosti nebo k tomu určený pracovník, na základě dokumentu „*Odpovědnosti a povinnosti*“ v IS

A.16.1.5 Reakce na incidenty bezpečnosti informací

Opatření: Reakce na incidenty bezpečnosti informací musí být v souladu s dokumentovanými postupy.

Vyloučeno: Ano

Způsob plnění požadavku: Záleží na požadavku a času na řešení. V případě napadnutí – např. hackerský útok se musí jednat rychle – v minutách. Jinak se jen zaznamenává průběh formou logů.

A.16.1.6 Ponaučení z incidentů bezpečnosti informací

Opatření: Znalosti získané z analýzy a řešení incidentů bezpečnosti informací musí být použity ke snížení pravděpodobnosti nebo dopadu následných incidentů.

Vyloučeno: Ano

Způsob plnění požadavku: Zavádí se opatření – omezení práv uživatele, nastavení firewallu, různý antivir – např. na serveru a pak u uživatele

A.16.1.7 Shromažďování důkazů

Opatření: Organizace musí definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování informací, které můžou sloužit jako důkazy.

Vyloučeno: Ano

Způsob plnění požadavku: Archivují se logy

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

A.17.1 Kontinuita bezpečnosti informací

Cíl: Kontinuita bezpečnosti informací musí být součástí systémů řízení kontinuity činnost organizace.

A.17.1.1 Plánování kontinuity bezpečnosti informací

Opatření: Organizace musí určit svoje požadavky na bezpečnost informací a kontinuitu řízení bezpečnosti informací při nepříznivých situacích, například během krizí, katastrof nebo havárií.

Vyloučeno: Ano

Způsob plnění požadavku: Společnost má určeny požadavky na bezpečnost informací a kontinuitu řízení bezpečnosti informací při nepříznivých situacích, ze kterých vychází i zálohovací plán – různá geolokace

A.17.1.2 Implementace kontinuity bezpečnosti informací

Opatření: Organizace musí ustavit, dokumentovat, implementovat a udržovat procesy, postupy a opatření k zajištění požadované úrovně kontinuity pro bezpečnost informací během nepříznivých situací.

Vyloučeno: Ano

Způsob plnění požadavku: řešeno smluvně; částečně také v rámci ISO 9001

A.17.1.3 Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací

Opatření: Organizace musí v pravidelných intervalech verifikovat ustavená a implementovaná opatření kontinuity bezpečnosti informací, aby zajistila, že jsou dostatečná a efektivní během nepříznivých situací.

Vyloučeno: Ano

Způsob plnění požadavku: Sledují se předem smluvené postupy (např. otázkou na poradách apod.), dále jsou dělány a sledovány zápisy ze společných porad.

A.17.2 Redundance

Cíl: Zajistit dostupnost vybavení pro zpracování informací.

A.17.2.1 Dostupnost vybavení pro zpracování informací

Opatření: Vybavení pro zpracování informací musí být implementováno s dostatečnou redundancí, aby byly splněny požadavky na dostupnost.

Vyloučeno: Ano

Způsob plnění požadavku: redundance je zajištěna pouze u vybraných prvků; vícenásobné připojení k internetu apod.

A.18 Soulady s požadavky

A.18.1 Soulad s právními a smluvními požadavky

Cíl: Vyvarovat se porušení zákonných, předpisových nebo smluvních povinností týkající se bezpečnosti informací a jakýchkoliv bezpečnostních požadavků.

A.18.1.1 Identifikace odpovídající legislativy a smluvních požadavků

Opatření: Pro každý informační systém a organizace musí být jednoznačně identifikovány, dokumentovány a udržovány aktuální veškeré relevantní zákonné, předpisové a smluvní požadavky a způsob, jakým je organizace dodržuje.

Vyloučeno: Ano

Způsob plnění požadavku: společnost dohlíží na dodržování odpovídající legislativy a smluvních požadavků a případné nejasnosti konzultuje s právníky

A.18.1.2 Ochrana duševního vlastnictví

Opatření: Pro zajištění souladu se zákonnými, předpisovými a smluvními požadavky, které jsou relevantní ochraně duševního vlastnictví a používání proprietárních softwarových produktů, musí být implementovány vhodně postupy.

Vyloučeno: Ne

Způsob plnění požadavku:

A.18.1.3 Ochrana záznamů

Opatření: Záznamy musí být chráněny proti ztrátě, zničení, padělání a neautorizovanému přístupu a zveřejnění, a to v souladu se zákonnými, předpisovými a smluvními požadavky a požadavky týkající se činnosti organizace.

Vyloučeno: Ano

Způsob plnění požadavku: digitální záznamy se zálohují, písemné se skenují

A.18.1.4 Soukromí a ochrana osobních údajů

Opatření: Soukromí a ochrana osobních údajů musí být zajištěny v souladu s odpovídající legislativou a s předpisy, pokud je to použitelné.

Vyloučeno: Ano

Způsob plnění požadavku: řešeno smluvně

A.18.1.5 Regulace kryptografických opatření

Opatření: Kryptografická opatření musí být používána v souladu s příslušnými úmluvami, legislativou a předpisy.

Vyloučeno: Ano

Způsob plnění požadavku: součástí dokumentu „*Manuál uživatele*“ v IS

A.18.2 Přezkoumání bezpečnosti informací

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

A.18.2.1 Nezávislá přezkoumání bezpečnosti informací

Opatření: Přístup organizace k řízení a implementaci bezpečnosti informací (tj. cílů opatření, jednotlivých opatření, politik, procesů a postupů bezpečnosti informací) musí být nezávisle přezkoumáván v plánovaných intervalech, nebo když nastane významná změna.

Vyloučeno: Ne

Způsob plnění požadavku:

A.18.2.2 Shoda s bezpečnostními politikami a normami

Opatření: Vedoucí pracovníci musí pravidelně přezkoumávat shodu zpracování informací a postupů v rozsahu jejich odpovědnosti s odpovídajícími bezpečnostními politikami, normami a dalšími požadavky na bezpečnost.

Vyloučeno: Ano

Způsob plnění požadavku: určení pracovníci pravidelně přezkoumávají shodu zpracování informací s odpovídajícími bezpečnostními politikami, normami a dalšími požadavky na bezpečnost, ale jen v rámci společnosti nebo po dohodě se zákazníkem. Společnost nemá prověrky ani na důvěrné ani na tajné informace v rámci veřejné správy.

A.18.2.3 Přezkoumání technické shody

Opatření: Informační systémy musí být pravidelně přezkoumávány, zda jsou v souladu s politikami a normami bezpečnosti informací organizace.

Vyloučeno: Ne

Způsob plnění požadavku: společnost si kupuje normy a každý nový projekt nastavuje dle nich (staré projekty už neupravuje)