Analýza rizik IT bezpečnosti ve společnosti XY

Ondřej Hubáček

Bakalářská práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2014/2015

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Ondřej Hubáček**
Osobní číslo:	**L12224**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**
Téma práce:	**Analýza rizik IT bezpečnosti ve společnosti XY**

Zásady pro vypracování:

1. **Zpracujte teoretické pojednání zabývající se problematikou zvoleného tématu bakalářské práce.**
2. **Analyzujte rizika IT bezpečnosti ve vybraném podniku.**
3. **Vymezte problematické oblasti a navrhněte opatření vedoucí k minimalizaci rizik.**
4. **Zhodnoťte navržená opatření a naplnění cíle bakalářské práce.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] SMEJKAL, V., RAIS, K. Řízení rizik ve firmách a jiných organizacích. Expert. Praha: Grada Publishing, 2013. ISBN: 978-80-247-4644- 9.

[2] DOSEDĚL, T. Počítačová bezpečnost a ochrana dat, Brno 1.vyd., Computer Press, 2004, ISBN-80-251-0106-1.

[3] PROSISE, C., MANDIA, K. Počítačový útok detekce, obrana a okamžitá náprava. Praha: Computer Press, 2002. ISBN 80-7226682-9.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce:	**Ing. et Ing. Jiří Konečný, Ph.D.** Ústav krizového řízení
Datum zadání bakalářské práce:	**6. února 2015**
Termín odevzdání bakalářské práce:	**16. května 2015**

V Uherském Hradišti dne 20. února 2015

L.S.

doc. RNDr. Jiří Dostál, CSc.
děkan

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v archivu Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval/a samostatně a použitou literaturu jsem citoval/a. V případě publikace výsledků budu uveden/a jako spoluautor/ka
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Uherském Hradišti dne 11.5.2015

.....

podpis studenta/ky

ABSTRAKT

Analýza rizik je nástroj pomáhající odhalit bezpečnostní rizika systému a návrhu jeho bezpečnostních opatření. Právě analýza rizik je hlavním tématem této bakalářské práce. V první, teoretické části jsou popsány obecné pojmy bezpečnosti informačních systémů, kterou popisuje směrnice ISO 27000 a teorie analýzy rizik. V praktické části jsou zkoumány vybrané oblasti informačního prostředí IT společnosti pomocí nástrojů pro analýzu rizika. Ze zjištěných závěrů je vypracováno závěrečné vyhodnocení a jsou navržena vhodná opatření řídící se podle norem ISO 27000.

Klíčová slova: bezpečnost informací, rizika, aktiva, hrozby, proces, analýza rizik, ochranné opatření

ABSTRACT

Risk analysis is a tool which helps to detect security risks on the system and the design of its security measures. It is the risk analysis which is the main topic of this thesis. The first, theoretical part deals with the general concepts of information systems security, which describes the directive ISO 27000, and the theory of risk analysis. The practical part investigates selected areas of the information environment of the IT company, using the tools for the analysis of risk. Finally on the basis of the conclusions of this research is suggested the final assessment and designed appropriate measure following the standards ISO 27000.

Keywords: Information Security, Risks, Actives, Threats, Process, Risk Analysis, Safeguards

Na tomto místě bych rád poděkoval svému vedoucímu bakalářské práce panu Ing. et Ing. Jiřímu Konečnému, Ph.D. za jeho odborné rady, připomínky a konzultace. Dále bych chtěl poděkovat své rodině a přítelkyni za velkou podporu po celou dobu mého studia.

OBSAH

ÚVOD

Řízení rizik IT bezpečnosti je v dnešní době velmi diskutovaným tématem moderních organizací, protože stále více ovlivňuje firemní procesy těchto organizací. Implementace správných postupů při řízení bezpečnosti informací přináší podstatnou konkurenční výhodu dané společnosti a pomáhá podporovat její obchodní cíle. Naopak nevhodná implementace postupů informační bezpečnosti může zvýšit náklady organizace a vést až k její likvidaci. Z tohoto důvodu je řízení bezpečnosti mnoha organizacemi vnímáno jako přítěž pro podnikání doprovázená zvýšením nákladů. Proto je nutné si uvědomit, že je důležité zvolit vhodná pravidla a postupy, které budou na míru určeny pro konkrétní organizaci a budou mít minimální dopad a zároveň maximální přínos pro její fungování.

Podstatou bezpečnosti informací je ochraňovat důležité zdroje organizace, jako například hardware, software a informace v nich obsažené. Za tímto účelem je tedy vhodné použít konkrétní ochranná opatření tak, aby byla nápomocná organizaci a chránila její fyzické, finanční, zaměstnanecké a další informační zdroje.

Pro účel výběru vhodných opatření existuje sada norem mezinárodní standardizační organizace, zkr. ISO, konkrétně norma ČSN ISO/IEC 27000, která specifikuje náležitosti řízení informační bezpečnosti, anglická zkratka ISMS. Po nasazení opatření odpovídajících této řadě směrnic je možné získat odpovídající certifikaci o splnění všech náležitostí ve směrnici ISO obsažených. To však není bezpodmínečně nutné a není to mnohokrát ani záměrem organizace. Záměrem tak hlavně bývá nasazení odpovídajících opatření dle směrnice a zvýšení informační bezpečnosti.

Cílem této bakalářské práce je vymezit problematické oblasti informační bezpečnosti, analyzovat rizika, navrhnout opatření vedoucí k minimalizaci rizik a tato opatření zhodnotit.

I. TEORETICKÁ ČÁST

1 CO JE RIZIKO?

Pojem riziko je spojen s pravděpodobností nebo možností škody. Jinými slovy je to očekávaná hodnota škody. Je to vlastně výsledek aktivace určitého nebezpečí, která vyústí v určitý negativní následek, škodu. Je to kvantitativní a kvalitativní vyjádření ohrožení, vyjadřující **míru ohrožení, stupeň ohrožení**. [8]

Neexistuje jedna obecně uznávaná definice, pojem riziko je definován různě:

1. Pravděpodobnost či možnost vzniku ztráty, obecně nezdaru.
2. Odchýlení skutečných a očekávaných výsledků.
3. Nebezpečí negativní odchylky od cíle (tzv. čisté riziko)
4. Nebezpečí chybného rozhodnutí.
5. Možnost, že specifická hrozba využije specifickou zranitelnost systému

Obecně existuje několik druhů rizik, například:

- Politická a teritoriální
- Ekonomická – makroekonomická a mikroekonomická, například tržní, inflační, úvěrová
- Bezpečnostní
- Právní a spojená s odpovědností za škodu
- Předvídatelná a nepředvídatelná
- Specifická – například pojišťovací, manažerská, informační

S rizikem jsou tedy těsně spjaty dva pojmy:

1. Pojem **neurčitého výsledku**, o němž se implicitně uvažuje ve všech definicích rizika: **výsledek musí být nejistý.** Máme-li hovořit o riziku, musí existovat alespoň dvě varianty řešení.
2. **Alespoň jeden z možných výsledků je nežádoucí.** V obecném slova smyslu může jít o ztrátu, kdy jistá část majetku jednotlivce je ztracena. Může jít o výnos, který je nižší, než možný výnos. [1]

1.1 Analýza rizik

Prvním krokem procesu snižování rizik je přirozeně jejich analýza. Analýza rizik je obvykle chápána jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich závažnosti.

Analýza rizik zpravidla zahrnuje:

1. **Identifikaci aktiv** – vymezení posuzovaného subjektu a popis aktiv, které vlastní
2. **Stanovení hodnoty aktiv** – určení hodnoty aktiv a jejich význam pro subjekt, ohodnocení možného dopadu jejich ztráty, změny či poškození na existenci či chování subjektu
3. **Identifikaci hrozeb a slabin (zranitelnosti)** – určení druhů událostí a akcí, které mohou ovlivnit negativně hodnotu aktiv, určení slabých míst subjektu, která mohou umožnit působení hrozeb.
4. **Stanovení závažnosti hrozeb a míry zranitelnosti** – určení pravděpodobnosti výskytu hrozby a míry zranitelnosti subjektu vůči dané hrozbě [1]

1.2 Základní pojmy analýzy rizik

1.2.1 Aktivum

Aktivum je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby. Aktiva se dělí na **hmotná** (nemovitosti, peníze) a na **nehmotná** (informace, autorské práva). Aktivem může být sám subjekt, neboť hrozba může působit na celou jeho existenci. Identifikace aktiv je závislá na úrovni podrobnosti, která je zvolena.

Základní charakteristikou aktiva je **hodnota aktiva,** která je založena na objektivním vyjádření obecně vnímané ceny, nebo na subjektivním ocenění důležitosti (kritičnosti) v závislosti na úhlu pohledu hodnocení.

1.2.2 Hrozba

Hrozba je síla, událost, aktivita, nebo osoba, která má nežádoucí vliv na aktiv, nebo může způsobit škodu, resp. poškodit organizaci jako celek. Hrozby mohou být přírodního, nebo lidského původu a mohou být náhodné nebo úmyslné. Mohou pocházet zevnitř i zvenčí organizace. Hrozbou může být například krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy apod.

Škoda, kterou způsobí hrozba se nazývá **dopad hrozby**. Dopad hrozby může být odvozen od absolutní hodnoty ztrát, do které jsou zahrnuty náklady na znovuobnovení činnosti aktiva nebo náklady na odstranění následků škod způsobených subjektu hrozbou.

1.2.3 Zranitelnost

Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby. Výskyt zranitelnosti nepůsobí škodu jako takový, protože musí existovat hrozba, která ho využije. Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem. Základní charakteristikou zranitelnosti je její úroveň.

1.2.4 Protiopatření

Protiopatření je postup, process, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby. Protiopatření se navrhují s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody. Z hlediska analýzy rizik je protiopatření charakterizováno **efektivitou** a **náklady**.

1.2.5 Riziko

Riziko vzniká vzájemným působením hrozby a aktiva. Hrozba, která nepůsobí na žádné aktivum, nemusí být při analýze rizik brána v úvahu. Aktivum, na které nepůsobí žádná hrozba není předmětem analýzy rizik.

Úroveň rizika je určena hodnotou aktiva, resp. Následkem pro jeho vlastníka či celou organizaci, zranitelností aktiva a úrovní hrozby.

Zbytkové riziko je takové riziko, které je tak malé (nepřesáhne referenční úroveň), že je pro subjekt přijatelné a není nutné podnikat další protiopatření k jeho snížení.

Referenční úroveň je hranice míry rizika (stanovená hodnota velikosti rizika), která rozhoduje o tom, zda je riziko zbytkové (velikost rizika je menší, než referenční úroveň), či není zbytkové (velikost rizika je větší než referenční úroveň).[1]

2 VZTAHY V ANALÝZE RIZIK

Správné pochopení vztahů v analýze rizik je pro úspěšné provedení analýzy klíčové.

Mechanismus uplatnění rizika probíhá následujícím způsobem:

- Hrozba využije zranitelnosti, překoná protiopatření a působí na aktivum, kde způsobí škodu (dopad).
- Aktivum (svou hodnotou) motivuje útočníka k aktivaci hrozby. Vůči působení hrozby se aktivum vyznačuje určitou zranitelností. Aktivum je zároveň chráněno protiopatřeními před hrozbami.
- Protiopatření chrání aktiva, detekuje hrozby a zmírňuje nebo zcela zabraňuje jejich působení na aktiva. Protiopatření zároveň odrazují od aktivování hrozeb.
- Hrozba působí přímo na aktivum nebo na protiopatření s cílem získat přístup k aktivu. Aby mohla hrozba působit, musí být aktivována. Pro svou aktivaci vyžaduje zdroje (vytvoření podmínek pro její působení).[1]

Obrázek 1. Vztahy při analýze rizik [9]

3 BEZPEČNOST V IT

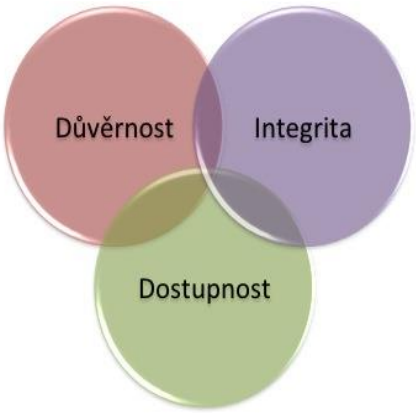
Užívání informačních a komunikačních technologií přináší do lidského života mnoho výhod, ale zároveň také vytváří určitou závislost na službách poskytovaných těmito technologiemi. Možná dlouhodobá nedostupnost těchto služeb může způsobovat problémy na straně fyzických osob, ale hlavně na straně osob právnických.

Dříve se managementy firem nezabývaly informační bezpečností, protože její důležitost nebyla až taková, jako dnes. IT systémy byly daleko menší, jednodušší a nebyly součástí hlavních aktiv společností. V dnešní době se však jejich role úplně změnila a to si začíná uvědomovat každá moderní firma. Informační bezpečnost se stává jedním z hlavních pilířů každé společnosti.

Bezpečnost informací

Bezpečnosti informací zahrnuje tři hlavní aspekty: důvěrnost, dostupnost a integritu. Aby mohla zajistit úspěch v činnosti organizace a kontinuitu této činnosti a minimalizovat dopady incidentů bezpečnosti informací, vyžaduje bezpečnost informací použití a řízení vhodných opatření bezpečnosti informací, zohledňujících široký rozsah hrozeb.

Bezpečnost informací se dosáhne implementací použitelné sady opatření, vybraných zvoleným procesem řízení rizik a řízených pomocí ISMS, včetně politik, procesů, postupů, organizačních struktur, softwaru a hardwaru, aby byla zajištěna ochrana identifikovaných informačních aktiv. Tato opatření je nutné specifikovat, implementovat, monitorovat, přezkoumávat a zlepšovat tam, kde je to nezbytné, aby se zajistilo, že jsou splněny specifické cíle bezpečnosti informací a podnikatelské cíle organizace. Příslušná opatření bezpečnosti informací by měla být uceleně začleněna do procesů činnosti organizace.[2]



Obrázek 2. Bezpečnost informací[10]

4 SYSTÉMY ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

4.1 Co je ISMS?

ISMS (Systém řízení bezpečnosti informací) sestává z politik, postupů, směrnic a příslušných zdrojů a činností, které organizace řídí, aby zajistila ochranu informačních aktiv. ISMS představuje systematický přístup k ustanovení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací organizace tak, aby byly dosaženy její cíle. Je založen na posuzování rizik a na úrovních přijetí rizik organizace, které byly navrženy pro efektivní ošetření rizik a pro jejich řízení. K úspěšné implementaci ISMS přispívá analýza požadavků na ochranu informačních aktiv a aplikace příslušných opatření s cílem zajistit ochranu těchto informačních aktiv v souladu s požadavky. K úspěšné implementaci ISMS rovněž přispívají dále uvedené základní principy:

- povědomí o potřebě bezpečnosti informací
- určení odpovědnosti za bezpečnost informací
- začlenění závazku vedení a zájmu zúčastněných stran
- zvýšení společenských hodnot
- posouzení rizika, na základě kterého budou stanovena příslušná opatření, aby bylo dosaženo přijatelných úrovní rizika
- bezpečnost začleněná jako základní prvek do informačních sítí a systémů
- aktivní prevence a detekce incidentů bezpečnosti informací
- zajištění komplexního přístupu k řízení bezpečnosti informací
- neustálé opakované posuzování bezpečnosti informací a provádění modifikací dle potřeby [2]

4.2 Proč je ISMS důležitý

Riziky spojenými s informačními aktivy organizace je třeba se zabývat. Dosažení bezpečnosti informací vyžaduje řízení rizik a zahrnuje rizika plynoucí z hrozeb fyzických, hrozeb souvisících s lidským faktorem, nebo s technologií, spojených se všemi druhy informací uvnitř organizace nebo používanými organizací.

Zavedení ISMS by mělo být pro organizaci strategické rozhodnutí a je nutné, aby toto rozhodnutí bylo uceleně začleněno, odstupňováno a aktualizováno v souladu s potřebami

organizace. Bezpečnost informací není vždy při návrhu a vývoji informačních systémů brána v úvahu. Často je také považována jen za technické řešení. Avšak bezpečnost, která může být dosažena technickými prostředky, je omezená a může být neúčinná, není-li podporována příslušným řízením a postupy v kontextu ISMS. Začlenění bezpečnosti do informačního systému, je-li již vytvořený, může být obtížné a nákladné. ISMS zahrnuje identifikaci zavedených opatření a vyžaduje pečlivé plánování a věnování pozornosti detailům. Například řízení přístupu, která mohou být technická, fyzická, administrativní nebo kombinovaná, poskytují prostředky zajišťující, že přístup k informačním aktivům je oprávněný a omezený, a že vychází z požadavků činnosti organizace a bezpečnostních požadavků.[2]

4.3 Posuzování rizik bezpečnosti informací

Posuzování rizik by mělo identifikovat, kvantifikovat a stanovit prioritu rizika v porovnání s kritérii pro přijetí rizika a cílů závažných pro organizaci. Výsledky by měly nasměřovat a určit příslušnou činnost managementu a systém preferencí pro řízení rizik bezpečnosti informací a pro implementaci opatření vybraných k ochraně před těmito riziky. Posuzování rizik by mělo zahrnovat systematický přístup k předběžnému odhadu velikosti rizik (analýza rizik) a porovnání odhadnutých rizik s kritérii rizik, aby se stanovila závažnost rizik (hodnocení rizik).

Posuzování rizik by mělo být prováděno periodicky, aby reflektovalo změny požadavků na bezpečnost informací a na stav rizik například v aktivech, hrozbách, zranitelnostech, dopadech hodnoceních rizik a ve výskytu závažných změn. Odhady rizik by měly být prováděny metodicky tak, aby výsledky byly porovnatelné a reprodukovatelné. Aby bylo efektivní, mělo by mít posuzování rizik bezpečnosti informací návaznosti na posuzování rizik v ostatních oblastech.[2]

4.4 Ošetřování rizik bezpečnosti informací

Organizace by měla před zvážením, jak ošetřit určité riziko, stanovit kritéria, určující, zda rizika mohou, nebo nemohou být akceptována. Rizika mohou být akceptována, jestliže je například odhadnuto, že riziko je nízké, nebo že náklady na ošetření rizika nejsou pro organizaci rentabilní. Akceptovaná rozhodnutí by měla být zaznamenána.

Pro každé identifikované riziko je po posuzování rizika nutné rozhodnout o ošetření rizika. Možná ošetření rizika zahrnují:

- použití vhodných opatření vedoucích ke snížení rizik
- vědomé a objektivní přijetí rizika, za předpokladu, že srozumitelným způsobem naplňují politiku a kritéria organizace pro přijetí rizika
- vyhnutí se rizikům tím, že nebudou přípustné činnosti, které by mohly vyvolat výskyt rizik
- sdílení rizik s jinými stranami, například s pojišťovnami a dodavateli

Pro ta rizika, kde rozhodnutí o ošetření rizika znamená aplikaci vhodných opatření, by měla být tato opatření vybrána a implementována.[2]

4.5 Výběr a implementace opatření

Pro identifikaci požadavků na bezpečnost informací, po určení a posouzení rizik bezpečnosti informací vůči identifikovaným informačním aktivům a po přijetí rozhodnutí o ošetření rizik bezpečnosti informací je třeba vybrat a implementovat příslušná opatření vedoucí ke snížení rizik.

Opatření by měla zajistit snížení rizik na přijatelnou úroveň se zohledněním:

- požadavků a omezení daných národní a mezinárodní legislativou a předpisy
- cílů organizace
- provozních požadavků a omezení
- nákladů na zavedení a provoz souvisících se snížením rizik, při současném zachování proporcionality a k požadavkům a omezením organizace
- potřeby uvést do rovnováhy investice spojené se zavedením a provozem opatření a ztrátu, která by pravděpodobně vznikla jako důsledek incidentů v oblasti bezpečnosti informací

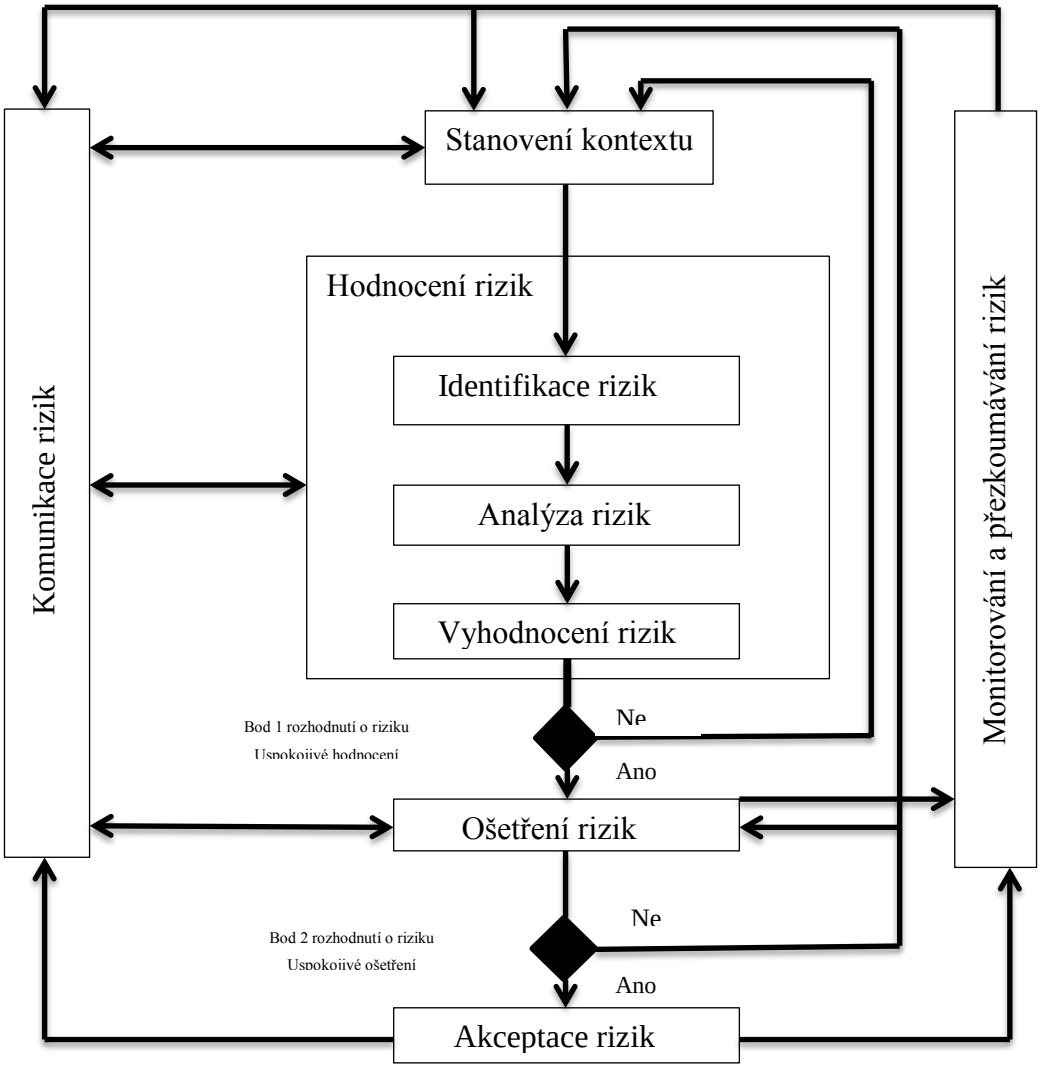
Opatření bezpečnosti informací by měla být zvažována při specifikaci požadavků systémů a projektů, a ve stadiu návrhu. Jestliže se to opomine, výsledkem mohou být dodatečné náklady a méně efektivní řešení, a v nejhorším případě i nemožnost dosáhnout adekvátní bezpečnosti. Je třeba si uvědomit, že některá opatření nemusí být aplikovatelná na každý informační systém, nebo prostředí a nemusí být proveditelná pro všechny organizace. Je nutné mít na paměti, že žádný soubor opatření nemůže docílit úplnou bezpečnost informací. K podpoře cílů organizace by měly být implementovány další řídící činnosti sloužící k monitorování, hodnocení a zlepšování účinnosti a efektivnosti opatření bezpečnosti informací.[2]

5 ANANÝZA RIZIK IT BEZPEČNOSTI POMOCÍ NORMY ISO/IEC 27005

V následující kapitole se budu zabývat popisem obecných doporučení pro řízení rizik bezpečnosti informací v rámci organizace, zvláště pak doporučení na požadavky řízení bezpečnosti informací, kterou popisuje norma ISO/IEC 27005.

5.1 Jak mezinárodní norma aplikuje proces řízení rizik?

Proces řízení rizik bezpečnosti informací sestává ze stanovení kontextu, posouzení rizik, ošetření rizik, akceptace rizik, komunikace rizik a monitorování a přezkoumávání rizik.



Obrázek 3. Znázornění procesu bezpečnosti informací [3]

Jak ukazuje obrázek 3, proces řízení rizik bezpečnosti informací se může u činností posouzení rizik a/nebo ošetření rizik opakovat. Opakující se přístup k provádění posouzení

rizik může při každém opakování hloubku a podrobnosti posouzení zvyšovat. Opakující se přístup zajišťuje správnou rovnováhu mezi minimalizací času a vynaloženého úsilí potřebného k identifikaci opatření, přičemž stále zajišťuje, že vysoká rizika jsou náležitě posouzena.

Nejdřív se stanoví kontext. Pak se provádí posouzení rizik. Pokud toto poskytne informací pro efektivní určení akcí nutných pro modifikaci rizik na přijatelnou úroveň, pak je úkol dokončen a následuje ošetření rizik. Jestliže jsou informace nedostatečné, musí být provedeno další opakování posouzení rizik s revidovaným kontextem (např. kritérii posouzení rizik, kritérii akceptace rizik nebo kritérii dopadu), možná jen na omezených částech celkového rozsahu (viz obrázek 3, bod 1 rozhodnutí o riziku. Účinnost ošetření rizik závisí na výsledcích posouzení rizik.[3]

Všimněme si, že ošetření rizik zahrnuje cyklický proces:

- posouzení ošetření rizik
- rozhodnutí, zda úroveň zbytkových rizik je akceptovatelná
- vytvoření nového ošetření rizik, pokud úrovně ošetření rizik nejsou akceptovatelné
- posouzení účinnosti ošetření rizik

Je možné, že ošetření rizik nepovede okamžitě k přijatelné úrovni zbytkového rizika. V takové situaci může být v případě nutnosti provedeno opakované posouzení rizik se změněnými parametry kontextu, po němž bude následovat další ošetření rizik (viz obrázek 3, bod 2 rozhodnutí o riziku).

Činnosti akceptace rizik musí zajistit, aby vedoucí pracovníci organizace zbytková rizika explicitně přijali. To je důležité zejména v situaci, kdy je zavedení opatření opomenuto, nebo odloženo, např. kvůli nákladům. Během celého procesu řízení rizik bezpečnosti informací je důležité, aby byli o rizicích a jejich ošetření informováni příslušní vedoucí pracovníci a zaměstnanci provozu. I před ošetřením rizik mohou být informace o identifikovaných rizicích pro zvládání incidentů velmi cenné a mohou pomoci snížit potenciální škodu. [3]

5.2 Čtyři fáze činnosti řízení bezpečnosti informací

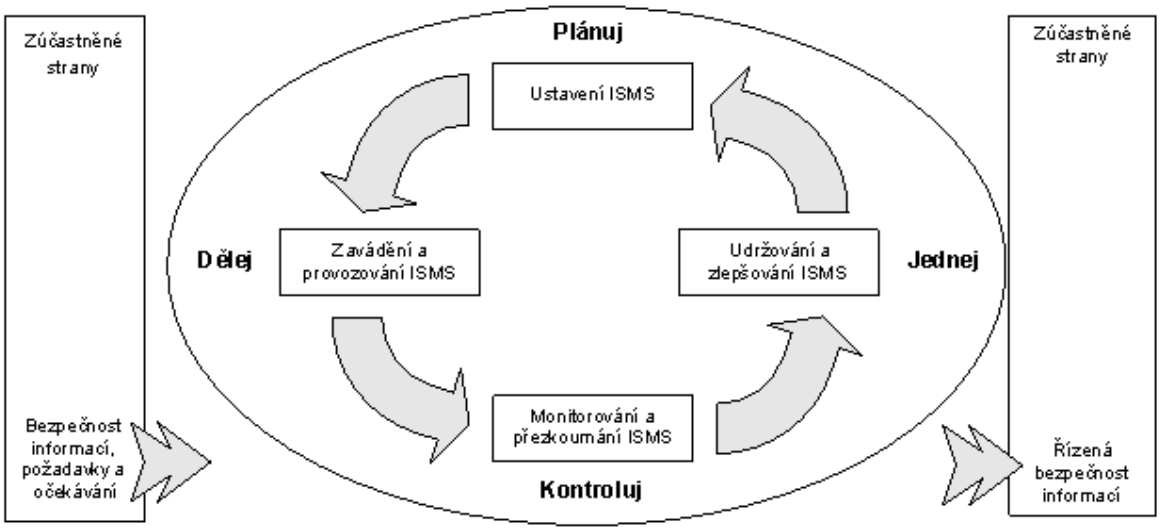
V ISMS tvoří stanovení kontextu, posouzení rizik, vývoj plánu ošetření rizik a akceptace rizik součást fáze „plánuj“. Ve fázi „dělej“ se akce opatření potřebná k redukci rizika na přijatelnou úroveň uplatňují v souladu s plánem ošetření rizik. Ve fázi „kontroluj“ ISMS musí vedoucí pracovníci určit potřebu přezkoumání posouzení a ošetření rizik ve světle incidentů a změn okolností. Ve fázi „jednej“ se provádějí všechny požadované akce, včetně dodatečného použití procesu řízení rizik bezpečnosti informací. [3]

Následující tabulka shrnuje činnosti řízení rizik bezpečnosti informací k těmto čtyřem fázím procesu ISMS:

Proces ISMS	**Proces řízení rizik bezpečnosti informací**
Plánuj	Stanovení kontextu Posouzení rizik Příprava plánu ošetření rizik Akceptace rizik
Dělej	Implementace plánu ošetření rizik
Kontroluj	Kontinuální monitorování a přezkoumávání rizik
Jednej	Udržování a zlepšování procesu řízení rizik bezpečnosti informací

Tabulka 1. Propojení ISMS a procesu řízení rizik bezpečnosti informací

Model známý jako „Plánuj-Dělej-Kontroluj-Jednej“ (Plan-Do-Check-Act nebo PDCA) může být aplikován na všechny procesy ISMS tak, jak jsou zavedeny touto normou. obrázek 4 znázorňuje, jak ISMS přijímá požadavky bezpečnosti informací a očekávání zainteresovaných stran jako vstup, a jak pomocí činností a procesů vytváří výstupy bezpečnosti informací, které splňují tyto požadavky a očekávání. [11]



Obrázek 4. PDCA model aplikovaný na procesy ISMS [11]

5.3 Stanovení kontextu

Nejdůležitější je určit účel řízení rizik bezpečnosti informací, protože toto ovlivňuje celý proces a zejména stanovení kontextu. Tím účelem může být:

- podpora ISMS
- příprava plánu kontinuity činností organizace
- příprava plánu reakce na incident
- popis požadavků na bezpečnost informací u produktu, služby, nebo mechanismu[3]

5.3.1 Přístup k řízení rizik

Měl by být vybrán a vhodně přizpůsoben přístup k řízení rizik, který řeší základní kritéria: kritéria hodnocení rizik, kritéria dopadu, kritéria akceptace rizik. Kromě toho by měla organizace zhodnotit, zda jsou k dispozici potřebné zdroje pro:

- provedení posouzení rizik a stanovení plánu ošetření rizik
- definování a zavedení politik a postupů, včetně implementace vybraných opatření
- opatření pro monitorování
- monitorování procesu řízení rizik bezpečnosti informací[3]

5.3.2 Kritéria hodnocení rizik

Měla by být vytvořena kritéria hodnocení rizik bezpečnosti informací zohledňující např:

- strategické hodnoty procesu informací o činnostech organizace
- kritičnosti informačních aktiv
- důležitost dostupnosti, důvěrnosti a integrity provozu a obchodních činností
- očekávání a představy zainteresovaných stran, negativní následky ztráty důvěryhodnosti a pověsti

5.3.3 Kritéria dopadu

Měla by být vytvořena kritéria dopadu, která by měla být specifikována na základě stupně škod nebo ztrát organizace způsobených bezpečnostní událostí, s ohledem na:

- úroveň klasifikace ovlivněného informačního aktiva
- narušení bezpečnosti informací
- ztrátu činností organizace a finanční hodnoty
- požkození pověsti

5.3.4 Kritéria akceptace

Měla by být vytvořena a určena kritéria akceptace rizik. Tato kritéria často závisí na politikách, záměrech a cílech organizace a zájmech zainteresovaných stran. Kritéria akceptace rizik se mohou lišit podle toho, jak dlouho se očekává, že riziko bude existovat, např. riziko může být spojeno s dočasnou nebo krátkodobou činností. Kritéria akceprace rizik by se měla stanovit s přihlédnutím k:

- obchodním kritériím
- právním a regulačním aspektům
- provozu
- technologiím
- financím
- sociálním a humanitárním faktorům. [3][4]

5.4 Posouzení rizik bezpečnosti informací

Posouzení rizik určuje hodnotu informačních aktiv, identifikuje možné hrozby a zranitelnosti, které existují, identifikuje stávající opatření a jejich účinek na identifikované riziko, určuje potenciální dopady a nakonec stanoví prioritu určených rizik a řadí je proti kritériím hodnocení rizik určeným ve stanovení kontextu. Posouzení rizik se často provádí ve dvou, nebo vice opakováních.[3]

5.5 Identifikace rizik

Účelem identifikace rizik je určit, co by se mohlo stát, aby byla způsobena potenciální ztráta, a porozumět tomu jak, kde a proč ke ztrátě může dojít.

5.5.1 Identifikace aktiv

U identifikace aktiv je třeba mít na paměti, že informační systém se skládá z něčeho víc, než jen z hardwaru a software. U každého aktiva by měl být identifikován vlastník aktiva k zajištění záruky a odpovědnosti za aktivum. Vlastník aktiva je často nejvhodnější osobou pro určení hodnoty aktiva pro organizaci.

5.5.2 Identifikace hrozeb

Hrozba má potenciál poškodit aktiva jakou jsou informace, procesy a systémy, tedy poškodit samotnou organizaci. Hrozba může vyvstat zevnitř i zvenčí organizace. Hrozby by se měly identifikovat obecně podle typu (např. neoprávněné akce, fyzické zničení, technické poruchy) a pak, v případě potřeby by se měly v rámci obecné třídy identifikovat jednotlivé hrozby. Některé hrozby můžou poskytnout vice než jedno aktivum. V takových případech mohou mít různý dopad v závislosti na tom, která aktiva jsou postižena.

5.5.3 Identifikace stávajících opatření

Aby se předešlo zbytečné práci nebo nákladům, např. při duplikaci opatření, měla by být provedena identifikace stávajících opatření. Mimo to je třeba při identifikaci stávajících opatření provést kontrolu správné funkčnosti stávajících opatření. Pokud opatření nefunguje dle předpokladů, může způsobit zranitelnost. [3][4]

5.5.4 Identifikace zranitelnosti

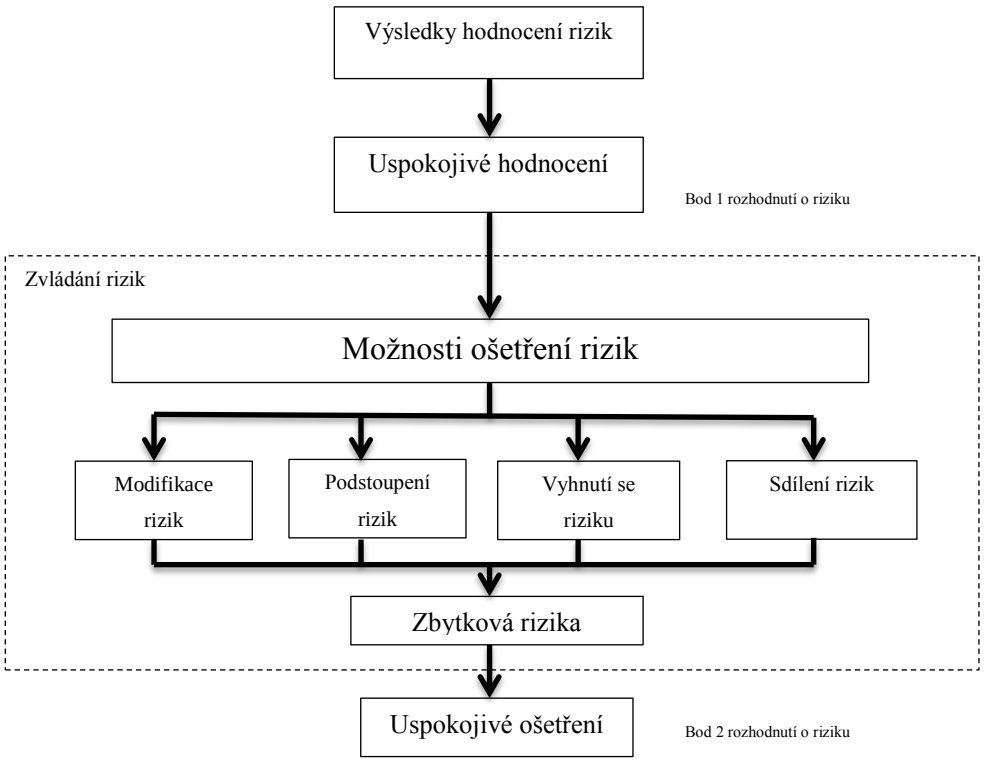
Výskyt zranitelnosti sám o sobě škodu nezpůsobí, protože musí existovat hrozba, která ho využije. Zranitelnost, která nemá odpovídající hrozbu, nemusí vyžadovat příjetí opatření, ale měla by být rozpoznána a monitorována.

5.5.5 Identifikace následků

Nádledkem může být ztráta účinnosti, nepříznivé provozní podmínky, ztráta obchodu, pověsti, škoda atd. Je nutno určit následek incidentu a posuzovat přitom kritéria dopadu definovaná během činnosti stanovení kontextu. Následek může ovlivnit jedno nebo vice aktiv nebo jen část aktiva.

5.6 Ošetření rizik bezpečnosti informací

K dispozici jsou čtyři volby pro ošetření rizik: modifikace rizika, podstoupení rizika, vyhnutí se riziku a sdílení rizika. Tyto čtyři způsoby ošetření rizik se vzájemně nevylučují. Někdy může organizace získat podstatnou výhodu kombinací způsobů, jako je snížení pravděpodobnosti rizik, snížení jejich následků a sdílení nebo podstoupení jakéhokoliv zbytkového rizika.[3]



Obrázek 5. Ošetření rizik [3]

5.6.1 Modifikace rizik

Úroveň rizik by měla být řízena zavedením, odstraněním nebo provedením změny opatření tak, aby mohlo být zbytkové riziko přehodnoceno jako přijatelné. Opatření může zajistit jeden nebo vice z následujících typů ochrany: nápravu, vyloučení, prevenci, minimalizaci dopadu, odstrašování, odhalení, obnovení, monitorování a povědomí. Během výběru opatření je důležité zvážit náklady na získání, zavedení, spravování, provozování, monitorování a údržbu opatření ve vztahu k hodnotě chráněných aktiv.

5.6.2 Podstoupení rizik

Rozhodnutí o podstoupení rizika bez další akce by mělo být učiněno v závislosti na hodnocení rizik. Jestliže úroveň rizik splňuje kritéria akceptace rizik, není zapotřebí přijímat další opatření a riziko lze podstoupit.

5.6.3 Vyhnutí se riziku

Když jsou identifikovaná rizika považována za příliš vysoká, nebo když náklady na uplatnění jiných způsobů ošetření rizik převyšují přínosy, organizace může přijmout rozhodnutí o celkovém vyhnutí se riziku tím, že upustí od plánované nebo existující činnosti nebo souboru činností, nebo změní podmínky, za nichž tuto činnost provozuje. Například u rizik způsobených přírodou může být z hlediska nákladů nejúčinnější alternativou fyzicky odstěhovat zařízení zpracovávající informace na místo, kde toto riziko neexistuje nebo je pod kontrolou.

5.6.4 Sdílení rizik

Sdílení rizik zahrnuje rozhodnutí sdílet určitá rizika s externími stranami. Sdílení rizik může vytvářet nova rizika nebo měnit existující, identifikovaná rizika. Sdílení lze provést pojištěním,, které bude pokrývat následky, nebo uzavřením smlouvy s obchodním partnerem, jehož úkolem bude monitorovat informační system a přijmout okamžitá opatření k zastavení útoku, než bude způsobena škoda určité úrovně. Je však nutné pamatovat na to, že je možné sdílet odpovědnost za zvládnutí rizika, ale obvykle není možné sdílet odpovědnost za dopad.[3]

5.7 Akceptace rizik bezpečnosti informací

Měla by být učiněna a formálně zaznamenána rozhodnutí akceptovat rizika a odpovědnosti za tato rozhodnutí. Kritéria akceptace rizik mohou být komplexnější, než aby jen určovala, zda zbytkové riziko spadá, nebo nespadá nad nebo pod určitou prahovou úroveň. V některých případech nemusí úroveň zbytkového rizika vyhovovat kritériím akceptace rizik, protože uplatňovaná kritéria neberou v úvahu převažující okolnosti. Například lze argumentovat tím, že je nutné akceptovat rizika, protože přínosy doprovázející rizika jsou velmi atraktivní, anebo protože náklady na modifikaci rizik jsou velmi vysoké. Tyto okolnosti naznačují, že jsou kritéria akceptace rizik nepřiměřená a měla by být revidována, je-li to možné. Avšak pokaždé není možné revidovat kritéria akceptace rizik včas. V takových případech ti, co rozhodují mohou být nuceni akceptovat rizika, která nesplňují běžná kritéria akceptace.

5.8 Komunikace a konzultace rizik bezpečnosti informací

Komunikace rizik je činnost vedoucí k získání dohody o tom, jak řídit rizika výměnou a/nebo sdílením informací o rizicích mezi těmi, co rozhodují a ostatními zainteresovanými stranami. Tyto informace zahrnují mimo jiné existence, character, formu, pravděpodobnost, závažnost, ošetření a přijatelnost rizik.

Komunikace rizik by měl být prováděna za účelem:

- poskytování záruky výstupu řízení rizik organizace
- shromažďování informací o rizicích
- sdílení výsledků plynoucích z posouzení rizik a prezentace plánu ošetření rizik
- podpory činit rozhodnutí
- koordinace zúčastněných stran a plánování reakcí s cílem snížení následků jakéhokoliv incident
- poskytování pocitu odpovědnosti za rizika těm, co rozhodují, a zainteresovaným stranám
- zvyšování povědomí

Organizace by měla vytvářet plány komunikace rizik pro běžné operace, jakož i pro nouzové situace. Proto by měla být činnost komunikace rizik prováděna nepřetržitě.[3][4]

5.9 Monitorování a přezkoumávání rizik bezpečnosti informací

5.9.1 Monitorování a přezkoumávání rizikových faktorů

Rizika nejsou stálá. Hrozby, zranitelnosti, pravděpodobnost nebo následky se mohou změnit náhle, bez jakéhokoliv předchozího náznaku. Proto je pro detekování těchto změn nutné neustálé monitorování.

Organizace by měla zajistit neustálé monitorování:

- nových aktiv, která byla zařazena do rozsahu řízení rizik
- nových hrozeb, které by mohly působit zvenčí i uvnitř organizace a které ještě nebyly hodnoceny
- možnosti, že by nové nebo zvýšené zranitelnosti mohly umožnit hrozbám tyto nové nebo změnené zranitelnosti zneužít
- zvýšeného dopadu nebo následků hodnocených hrozeb, zranitelností a rizik, které dohromady způsobují nepřijatelnou úroveň rizik
- incidentů bezpečnosti informací

Nové hrozby, zranitelnosti, nebo změny pravděpodobností nebo následků mohou zvýšit rizika, která byla dříve hodnocena jako nízká. V rámci přezkoumávání nízkých a akceptovaných rizik by mělo být každé riziko posuzováno zvlášť a take všechna tato rizika jako celek, a měl by být vyhodnocen jejich potenciální celkový dopad.

5.9.2 Monitorování, přezkoumávání a zlepšování řízení rizik

Organizace by měla zajistit, aby proces řízení rizik bezpečnosti informací a relevantní činnosti zůstaly přiměřené současným okolnostem a byly naplňovány. Všechna dohodnutá zdokonalení procesu nebo akcí nutných pro zvýšení souladu s procesem by měla být sdělena příslušným vedoucím pracovníkům, aby byla jistota, že žádné riziko, nebo prvek rizika nebyly přehlédnuty nebo podceněny a že jsou prováděny nutné akce a činěna rozhodnutí k zajištění reálného pochopení rizika a schopnosti reagovat. [3][5]

6 IDENTIFIKACE, OHODNOCENÍ AKTIV A ZJIŠŤOVÁNÍ DOPADU

6.1 Příklady identifikace aktiv

Pro stanovení hodnoty potřebuje organizace nejprve svá aktiva identifikovat. Lze rozlišovat dva druhy aktiv.

1. Primární aktiva
- obchodní procesy a činnosti
- informace
2. Podpůrná aktiva
- hardware
- software
- sítě
- pracovníci
- lokalita
- organizace

6.1.1 Identifikace primárních aktiv

Identifikaci primárních aktiv provádějí společné pracovní skupiny zástupců procesu (vedoucí pracovníci, odborníci v oblasti informačních systémů a uživatelé). Primárními aktivy jsou obvykle hlavní procesy a informace o činnosti v rámci rozsahu.

Existují dva typy primárních aktiv:

1. Obchodní procesy a činnosti, například:

- procesy, jejichž ztráta, nebo omezení neumožňuje plnit poslání organizace
- procesy, které obsahují tajné procesy nebo procesy zahrnující patentované nebo jinak chráněné technologie¨
- procesy, které jsou-li pozměněny, mohou významně ovlivnit plnění poslání organizace [5][3]

2. Informace

- životně důležité informace pro plnění poslání, nebo činností organizace
- strategické informace vyžadované pro dosažení cílů určených strategickými orientacemi
- velmi nákladné informace, jejichž shromažďování, skladování, zpracovávání a přenos vyžaduje hodně času a/nebo je na jejich získání zapotřebí vysokých nákladů[5]

6.1.2 Seznam a popis podpůrných aktiv

Tato aktiva mají zranitelnosti, jež jsou zneužitelné hrozbami, jejichž cílem je poškodit primární aktiva v rámci rozsahu. Jsou různého typu:

Hardware

Hardware sestává ze všech procesů podporujících fyzické prvky.

Zařízení pro zpracování dat (aktivní) – Zařízení pro automatické zpracování informací včetně položek požadovaných pro samostatný provoz.

Přenosná zařízení – Přenosná počítačová zařízení. Příklady: notebook, mobilní telefon

Procesní periférie - Zařízení připojené k počítači přes komunikační port. Příklady: tiskárna, vyjímatelná disková jednotka

Nosiče dat – Nosič informací, který lze připojit k počítači nebo počítačové síti pro uchovávání dat. Příklady: disketa, CD ROM, vyjímatelný pevný disk, flash disk, paměťový klíč, páska.

Ostatní nosiče – Statická média, neelektronické nosiče obsahující data. Příklady: papír, diapozitiv, dokumentace, fax.

Software

Software sestává ze všech programů přispívajících k provozu hardwaru pro zpracování dat.

Operační systém – Zahrnuje všechny programy základního operačního systému, z kterého se spouštějí všechny ostatní programy. Zahrnuje jádro a základní funkce nebo služby.

Software pro služby, údržbu nebo správu – Software je charakterizován tím, že doplňuje služby operačního systému a není přímo ve službách uživatelů a aplikací.[5][3]

Softwarové balíky nebo standartní software – Kompletní produkty, které jsou obchodně využívány jako takové s nosičem a údržbou. Příklady: databázový software, software pro zasílání elektronických zpráv, adresářový software.

Podnikové aplikace

Standartní podnikové aplikace – Komerční software navržený k tomu, aby umožňoval uživatelům přístup ke službám a funkčním, které požadují od svého informačního systému. Příklady: účetní software, software pro řízení obráběcích strojů, software péče o zákazníka.

Specifické podnikové aplikace - Software, v němž byly různé aspekty specificky vyvinuty, aby umožnil uživatelům přímý přístup ke službám a funkcím, které vyžadují od svého informačního systému.

Sítě

Sítě jsou sestaveny ze všech telekomunikačních zařízení využívaných k propojení několika fyzicky vzdálených počítačů nebo prvků informačního systému.

Médium a podpory – Komunikační a telekomunikační média jsou charakteristická hlavně fyzickými a technickými parametry zařízení a komunikačními protokoly. Příklady: Ethernet, ADSL, WiFi, Bluetooth.

Pasivní nebo aktivní přenos – Všechna zařízení, která nejsou logickým zakončením komunikací, ale jsou to zprostředkující nebo transportní zařízení. Příklady: Směrovač (router), rozbočovač (hub), přepínač (switch).

Pracovníci

Skupiny lidí zabývajících se informačním systémem.

Ti, kteří rozhodují – jsou vlastníky primárních aktiv a vedoucí pracovníci organizace nebo projektu. Příklady: nejvyšší vedení organizace, vedoucí projektu.

Uživatelé – pracovníci, kteří manipulují s citlivými prvky z rozsahu své činnosti a kteří mají zvláštní zodpovědnost. K plnění svých úkolů mohou mít zvláštní přístupová práva k informačnímu systému. Příklady: management financí, manažer pro řízení rizik.

Pracovníci provozu – jedná se o pracovníky zabývající se provozem a údržbou informačního systému. Aby mohly plnit své každodenní úkoly, mohou mít zvláštní přístupová práva k informačnímu systému. Příklady: správce systému, záloha, Help Desk, bezpečnostní technici.[5][3]

Lokalita

Zahrnuje všechna místa obsažená zcela, nebo zčásti v rozsahu a fyzické prostředky potřebné pro její provoz.

Vnější prostředí – Všechna místa, na kterých nemohou být uplatněny bezpečnostní prostředky organizace. Příklady: domovy pracovníků, prostředí mimo pracoviště.

Areál – Místo, které hraničí obvodem přímo s vnějším prostředím. Může se jednat o fyzickou ochrannou hranici získanou vytvořením fyzických bariér nebo prostředků dohledu okolo budov.

Zóna – Zónu tvoří fyzická ochranná hranice rozdělující prostory uvnitř areálu organizace. Získá se vytvořením fyzických bariér okolo infrastruktury pro zpracování informací organizace. Příklad: vyhrazená přístupová zóna.

Komunikace – Telekomunikační služby a zařízení poskytované operátorem. Příklad: telefonní linka

Vybavení – Služby a prostředky požadované pro zajištění elektrické energie pro zařízení a periferie IT.

Organizace

Organizace popisuje organizační rámec sestávající ze všech struktur pracovníků přidělených k úkolu a postupů kontrolujících tyto struktury.

Řídící orgány – Jsou to organizace, od nichž analyzovaná organizace odvozuje svoji pravomoc. Mohou být právně sdružené nebo externí. To určuje pro analyzovanou organizaci omezení na základě předpisů rozhodnutí a akcí. Příklady: správní orgán, hlavní ředitelství organizace.

Organizační struktura organizace – Skládá se z různých útvarů organizace, včetně jejich propojených aktivit, pod kontrolou vedení. Příklady: řízení lidských zdrojů, řízení IT, bezpečnostní služba budovy.

Subdodavatelé / dodavatelé / výrobci - Jedná se o organizace, které poskytují organizaci službu nebo zdroje a jsou k tomu zavázány smlouvou. Příklady: společnost zajišťující správu areálu, společnost zajišťující nákup služeb mimo organizaci. [5][3]

6.2 Ohodnocení aktiv

Kvůli různorodosti aktiv vyskytujících se ve většině organizací je pravděpodobné, že některá aktiva, která mají známou peněžní hodnotu, budou ohodnocena v místní měnové jednotce, zatímco ostatní aktiva, která mají kvalitativnější hodnotu, mohou být seřazena podle hodnoty, například od „velmi nízké“ po „velmi vysokou“. Pro jedno a totéž aktivum lze použít oba typy hodnocení.

6.2.1 Kritéria

Možná kritéria používaná k určení hodnoty aktiva zahrnují původní cenu, náhradu aktiva nebo jeho opětovné vytvoření, nebo jeho hodnota může být abstraktní, např. hodnota pověsti organizace. Dalším základem pro stanovení hodnoty aktiv jsou náklady vzniklé v důsledku ztráty důvěrnosti, integrity a dostupnosti jako výsledek incidentu. V konečné analýze by mělo být pečlivě určeno, která hodnota, nebo hodnoty budou aktivu přiřazeny, protože konečná přiřazená hodnota vstupuje do rozhodování o zdrojích, jež mají být vynaloženy na ochranu aktiv.

6.2.2 Redukce na společný základ

Nakonec musí být všechna ohodnocení aktiv redukována na společný základ. To lze provést pomocí kritérií, jako jsou ta níže uvedená. Kritéria, jež mohou být použita pro posouzení možných následků vyplívajících ze ztráty důvěrnosti, integrity, dostupnosti, nepopiratelnosti, odpovědnosti, autentičnosti nebo spolehlivosti aktiv jsou například tato:

- porušení legislativy nebo předpisů
- ztráta důvěry/negativní dopad na pověst
- narušení veřejného pořádku
- ohrožení osobní bezpečnosti
- finanční ztráta
- přerušení obchodních činností
- ztráta důvěry zákazníků
- narušení vnitřního provozu
- ztráta konkurenční výhody
- ztráta technické pověsti
- materiální škoda [4][3]

6.2.3 Škála

Organizace může definovat své vlastní limity pro hodnoty aktiv, jako „nízká“, „střední“ nebo „vysoká“. Tyto limity by měly být stanoveny podle vybraných kritérií. Musíme však podotknout, že je výhradně na organizaci, aby rozhodla, co je považováno za „nízký“ nebo „vysoký“ následek. Následek, který může být katastrofální pro malou organizaci, může být zanedbatelný pro velmi velkou organizaci.

6.2.4 Závislosti

Čím jsou obchodní procesy podporované aktivem důležitější a početnější, tím větší je hodnota takového aktiva. Měly by být také identifikovány závislosti aktiv na obchodních procesech a ostatních aktivech, protože by to mohlo ovlivnit hodnoty aktiv. Hodnoty aktiv, na nichž jsou závislá jiná aktiva, lze modifikovat tímto způsobem:

1. Jsou-li hodnoty závislých aktiv (např. dat) nižší, nebo se rovnají hodnotě posuzovaného aktiva (např. softwaru), jeho hodnota zůstane stejná

2. Jsou-li hodnoty závislých aktiv (např. dat) vyšší, pak by se hodnota posuzovaného aktiva (např. softwaru) měla zvýšit podle:

- stupně závislosti
- hodnot těch ostatních aktiv

6.2.5 Výstup

Konečným výstupem těchto kroků je seznam aktiv a jejich hodnot vztahující se k vyzrazení, modifikaci, nedostupnosti, destrukci a nákladům na výměnu.

6.3 Posouzení dopadu

Incident bezpečnosti informací může mít dopad na více než jedno aktivum nebo pouze část aktiva. Dopad se vztahuje ke stupni úspěchu incidentu. Dopad se považuje za takový, který má buď okamžitý, nebo budoucí účinek, který zahrnuje finanční a tržní následky.

Okamžitý dopad je buď přímý, nebo nepřímý.

Přímý dopad:

- náklady na získání, konfiguraci a instalaci nového aktiva nebo zálohy
- finanční hodnota výměny ztraceného aktiva [3][4]

- náklady na přerušení provozu v důsledku incidentu do obnovení služby poskytované tímto aktivem
- výsledky dopadu při narušení bezpečnosti informací

Nepřímý dopad:

- náklady na přerušení provozu
- potenciální zneužití informací získaných porušením bezpečnosti
- nedodržení zákonných, nebo regulatorních povinností

Jako takové, první posouzení odhadne dopad jako velmi blízký příslušné hodnotě aktiva. Při jakémkoliv dalším opakování u tohoto aktiva bude dopad v důsledku přítomnosti a účinnosti přijatých opatření jiný (obvykle mnohem nižší).[3][6]

7 PŘÍKLADY TYPICKÝCH HROZEB

Následující tabulka ukazuje příklady typických hrozeb. Seznam může být využit v rámci procesu posouzení hrozeb. Hrozby mohou být úmyslné, náhodné nebo environmentální a mohou způsobovat např. narušení nebo ztrátu důležitých služeb. Následující seznam pro každou hrozbu ukazuje typ relevantního zdroje: A (accidental – náhodný), D (deliberate – úmyslný), E (enviromental – environmentální). Typ zdroje D je použit pro úmyslné akce zaměřené na aktiva. A je pro lidské činnosti, které mohou náhodně poškodit informační aktiva, a E je pro všechny incidenty, které nejsou založeny na lidské činnosti. Pořadí skupin hrozeb nereflektuje žádné priority. [3][6]

Typ	Hrozby	Zdroj
Fyzické poškození	Požár	A, D, E
	Poškození vodou	A, D, E
	Zničení zařízení nebo médií	A, D, E
	Prach, koroze, zamrznutí	A, D, E
Přírodní události	Klimatický jev	E
	Seismický jev	E
	Meteorologický jev	E
	Povodeň	E
Ztráta základních služeb	Selhání klimatizace nebo dodávky vody	A, D
	Přerušení dodávky elektřiny	A, D, E
	Selhání telekomunikačního zařízení	A, D
Poruchy způsobené zářením	Elektromagnetické záření	A, D, E
	Elektromagnetické impulzy	A, D, E
Ohrožení informací	Vzdálená špionáž	D
	Odposlech	D
	Krádež médií nebo dokumentů	D
	Krádež zařízení	D
	Vyzrazení	A, D
	Falšování pomocí technického vybavení	D
	Falšování pomocí aplikačního program. Vybavení	A, D
Technická selhání	Selhání zařízení	A
	Přetížení informačního systému	A, D
	Chyba údržby	A, D
Neoprávněné činnosti	Neoprávněné použití zařízení	D
	Poškození dat	D
Ohrožení funkčnosti	Chyba v používání	A
	Zneužití oprávnění	A, D
	Falšování práv	D

Tabulka 2. Příklady typických hrozeb [3]

Zdroj hrozby	Motivace	Možné důsledky
Hacker, cracker	Výzva Rebelie Peníze	Hacking Narušení a prolomení systému Neoprávněný přístup
Počítačová kriminalita	Zničení informací Nezákonné prozrazení informací Finanční prospěch	Počítačový zločin Získání informace za úplatu Průnik do systému
Terorismus	Vydírání Vykořisťování Politický prospěch Zviditelnění v médiích	Bombové útoky Informační válka Průnik do systému Porušení systému
Průmyslová špionáž (zpravodajské služby, společnosti, zahraniční vlády, ostatní vládní zájmy)	Konkurenční výhoda Ekonomická špionáž	Politické zvýhodnění Ekonomické zneužití Krádež informací Průnik do soukromí
Interní pracovníci (špatně zaškolení, nespokojení, škodolibí, nedbalí, nečestní nebo zaměstnanci s ukončeným pracovním poměrem)	Zvědavost Ego Finanční prospěch Odplata Neúmyslné chyby a opomenutí	Napadení zaměstnance Prohlížení chráněných informací Zneužití počítačů Škodlivý kód (virus) Narušení komunikace Sabotáž systému

Tabulka 3. Příklady zdrojů hrozeb [3]

8 PŘÍKLADY ZRANITELNOSTÍ

Následující tabulka ukazuje příklady zranitelností pro různé oblasti bezpečnosti, včetně příkladů hrozeb, které dané zranitelnosti mohou využít

Hardware	Nedostatečná údržba záznamových médií	Chyba údržby systému
	Citlivost na vlhkost, prach, zašpinění	Prach, koroze, zamrznutí
	Citlivost na změny napětí	Přerušení dodávky elektřiny
	Nechráněné uskladnění	Krádež médií nebo dokum.
Software	Známé chyby v programech	Zneužití oprávnění
	Neodhlášení při opouštění pracovní stanice	Zneužití oprávnění
	Široce rozšířené programy	Poškození dat
	Špatné nastavení parametrů	Chyba použití
	Špatná správa hesel	Falšování práv
	Nedostatečná fyzická ochrana budov	Krádež médií nebo dokum.
Sítě	Nechráněné komunikační linky	Odposlech
	Nekvalitní kabelové spojení	Selhání telekomun. zařízení
	Nedostatečná autentizace uživatele	Falšování práv
	Nedostatečně bezpečná síťová architektura	Vzdálená špionáž
	Přenos odkrytých hesel	Vzdálená špionáž
Zaměstnanci	Nedbalá kontrola fyzického přístupu budov	Nedostatek personálu
	Nedostatečné bezpečnostní školení	Chyba použití
	Nedostatek povědomí o bezpečnosti	Chyba použití
	Nedostatečná kontrola práce exter. zaměst.	Krádež médií nebo dokum.
Lokality	Nedbalá kontrola fyz. přístupu do budov	Zničení zařínení nebo médií
	Poloha v zátopové oblasti	Povodeň
	Nedostatečná fyz. ochrana budov	Krádež zařízení
Organizace	Nedostatečný fotmální postup při reg. uživ.	Zneužití oprávnění
	Nedostatky v postupech pro zprac. Informací	Zneužití oprávnění
	Nedostatky v postupech pro identifik. Rizik	Zneužití oprávnění
	Nedostatky v postupech pro řízení změn	Chyba údržby systému
	Nedostatky v postup. při zacházení s inform.	Chyba použití
	Nedostatek v přezkoumáních management.	Neoprávněné použití zař.
	Nedostatečné zajištění ve smlouv. se zaměst.	Nezákonné zpracování dat

Tabulka 4. Příklady zranitelností [3]

II. PRAKTICKÁ ČÁST

9 POPIS ZKOUMANÉ SPOLEČNOSTI

Zkoumaná společnost funguje v oblasti IT šestým rokem. Zabývá se poskytováním IT služeb významnému českému podnikatelskému subjektu. Mezi její hlavní činnosti patří návrhy, realizace, správa IT řešení a správa NON-IT technologií, jako jsou chladící systémy a záložní zdroje. Dalšími činnosti tohoto podniku je řešení problémů a požadavků zákazníků a dohled nad dodržováním bezpečnosti informací. Nejdůležitější činností je však provozování všech informačních aktiv společnosti.

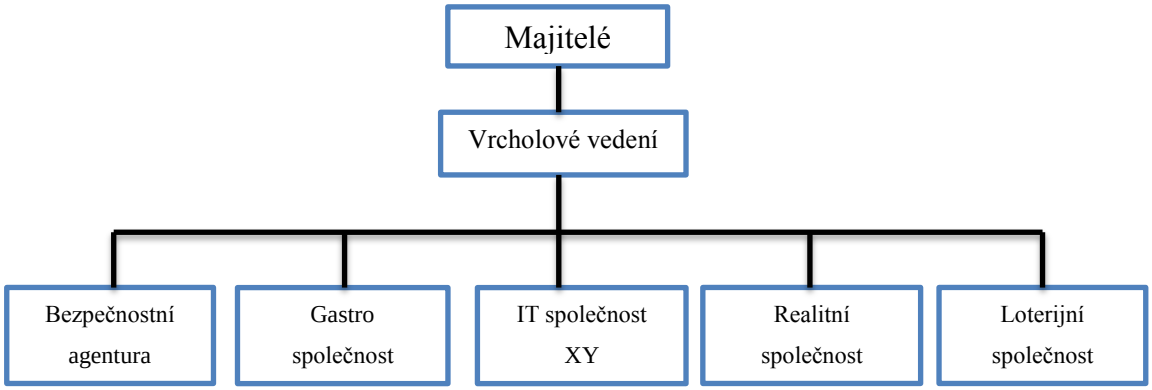
Podnik je součástí velkého holdingu, do kterého patří například organizace zajišťující bezpečnostní služby, organizace obchodující s realitami, organizace podnikající v gastronomickém průmyslu a organizace provozující loterie a hry. Pro všechny tyto organizace námi zkoumaná společnost zajišťuje služby v oblasti IT a dohlíduje dodržování informační bezpečnosti.

Všechny tyto organizace sídlí v jednom areálu a z hlediska IT bezpečnosti podléhají nařízením a směrnicím společnosti XY.

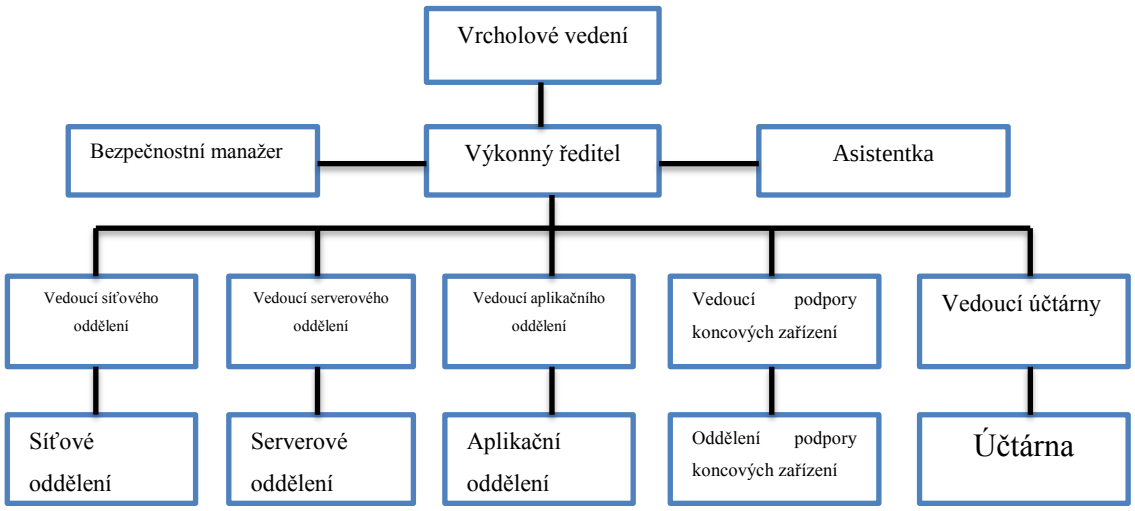
9.1 Statistické ukazatele

- počet všech společností holdingu: 5
- počet zaměstnanců holdingu: cca 400
- počet zaměstnanců IT společnosti XY: 40
- počet správců sítě: 5
- počet správců serverů: 5
- počet správců aplikací: 3
- počet správců koncových zařízení: 4
- externí podpora IT: poskytována ve formě výměny poškozeného HW

9.2 Organizační struktura holdingu



9.3 Organizační struktura IT společnosti XY



10 STÁVAJÍCÍ ŘEŠENÍ BEZPEČNOSTI VE SPOLEČNOSTI XY

10.1 Fyzická bezpečnost

Celý areál firmy i její budovy jsou nepřetržitě monitorovány bezpečnostní agenturou, která sídlí přímo v budově společnosti. Každá budova je vybavena elektronickým zabezpečovacím systémem, kamerovým systémem a elektronickými zámky vstupních a vnitřních dveří, které se otevírají čipovými kartami. Tyto karty má k dispozici každá zaměstnanec, avšak u každého je přístup řešen individuálně dle potřeb. Veškeré pohyby v areálu a budovách jsou monitorovány a nahrávány.

Cizí příchozí návštěvníci jsou u vstupu evidováni pomocí skenerů identifikačního dokladu. Zároveň návštěvníkovi není umožněn přístup do areálu bez doprovodu firemního zaměstnance, který je k tomuto účelu určen.

10.2 Požární bezpečnost

První úroveň detekce požáru v objektu zajišťuje laserová detekce. Laserové hlásiče jsou aktivními hlásiči detekce kouře ve vzduchu. Fungují na principu rozptylu světelného paprsku, který je detekován na senzoru. Druhou úrovní detekce jsou klasická kouřová čidla. První úroveň detekce slouží pouze jako informativní pro dohledové centrum, pokud však dojde ke zdetekování kouřovými čidly, automaticky se aktivuje hasící zařízení. Pro hašení IT techniky je použito plynové hasící zařízení, aby nedošlo k jejímu následnému poškození.

10.3 Napájení a chlazení IT

Pro zajištění nepřetržitého napájení jsou v areálu společnosti umístěny dva dieselgenerátory. Při výpadku elektrické energie dojde k automatickému nastartování jednoho ze záložních generátorů. Druhý generátor slouží jako záloha při nenastartování prvního generátoru. Po nastartování jsou generátory schopny dodávat elektrickou energii do 30 sekund.

Aby nedošlo k výpadku ani na těchto 30 sekund, je všechna technika nutná k provozu společnosti připojena na náhradní bateriové zdroje, které jsou schopny udržet zařízení v provozu až po dobu tří hodin.

Aby nedocházelo k přehřívání IT techniky, jsou místnosti, kde je tato technika umístěná, vybaveny moderními vzduchovými chladícími systémy.

10.4 Síťová bezpečnost

10.4.1 Ochrana před vnějšími vlivy

V současnosti je ochrana před vnějšími vlivy a útoky řešena pomocí firewallů. Tyto firewally jsou buď osobní softwarové, nebo hardwarové. Osobní softwarové firewally jsou umístěny především v operačních systémech osobních počítačů a zajišťují síťovou bezpečnost v rámci vnitřní sítě. V kooperaci s antivirovými softwary vytvářejí ochranu dat v PC tak, aby nedocházelo k infikaci škodlivými sofwary a neoprávněným vniknutím do uživatelské stanice.

Hardwarové firewally jsou umístěny mezi jednotlivými sítěmi tak, aby mohli správci sítí řídit provoz mezi těmito sítěmi. Hlavním úkolem hardwarových firewallů je však oddělení vnitřních sítí společnosti od veřejné sítě Internet.

Softwarové i hardwarové firewally se v principu moc neliší. Dokážou hlavně omezovat komunikaci na základě služeb, portů a IP adres.

10.4.2 Ochrana před vnitřními vlivy

Všechny uživatelské přístupy ve společnosti XY, jakožto i v celém holdingu jsou řízeny pomocí služby Active Directory. Active Directory je nástroj, který pomáhá administrátorům sítě řídit její provoz pomocí politik, které určují, kam má který uživatel přístup a jaké aplikace smí nebo nesmí používat. Uživatel je povinen mít svou stanici chráněnou heslem, které mu zároveň slouží k přístupu do aplikací, jež jsou určeny k výkonu jeho práce.

Obrázek 6. Síťová bezpečnost [12]

11 ANALÝZA RIZIK

V následující části práce se budu zabývat analýzou konkrétních rizik IT bezpečnosti ve společnosti XY.

11.1 Stanovení hranice analýzy rizik

Při stanovení hranice analýzy rizik určujeme, která aktiva budou zahrnuta do analýzy rizik a která ne. Analýza rizik nebude probíhat u všech aktiv, nýbrž hlavně u aktiv, které byly ze strany organizace určeny jako nejdůležitější vzhledem probíhajícímu procesu snižování rizik. Určená aktiva budou identifikována a ohodnocena v následující kapitole.

11.2 Identifikace a hodnocení aktiv

Jednotlivé hodnoty aktiva budou určovány podle stupnice **„nízká“ - 1**, **„střední“ - 2** nebo **„vysoká“ - 3**.

Nízká (1):

- nulový dopad pro společnost
- minimální dopad pro společnost

Střední (2):

- problémy a finanční ztráty organizace

Vysoká (3):

- velké problémy a finanční ztráty organizace
- ohrožení dalšího fungování organizace

11.3 Ohodnocení aktiv

Primární aktiva	
Aktivum	**Hodnota**
Proces Core Bussinessu společnosti	Vysoká (3)
Know-how	Vysoká (3)
Informace o zákaznících	Střední (2)
Smlouvy se zákazníky	Vysoká (3)
Dokumentace k systémům	Vysoká (3)
Pracovní smlouvy se zaměstnanci	Vysoká (3)
Podpůrná aktiva	
Pevné pracovní stanice	Střední (2)
Přenosná zařízení určená k výkonu práce	Střední (2)
Stolní telefony	Nízká (1)
Nosiče dat (pasivní)	Střední (2)
Tiskárny	Nízká (1)
Ostatní nosiče dat	Střední (2)
Řídící orgány podniku	Vysoká (3)
Standartní softwarové vybavení	Střední (2)
Speciální podnikové aplikace	Střední (2)
Síťový hardware (serverovny)	Vysoká (3)
Síťový hardware (uživatelé)	Střední (2)
Servery informačního systému	Vysoká (3)
Internetová konektivita	Vysoká (3)
Budova podniku	Vysoká (3)

Tabulka 5. Ohodnocení aktiv

11.4 Identifikace hrozeb

V tabulce níže můžeme vidět námi identifikované hrozby, příklady zranitelností a pravděpodobnosti výskytu hrozeb, které jsou značeny stupnicí **„nízká“ – 1, „střední“ – 2 nebo „vysoká“ - 3.**

Hrozba	Příklady zranitelnosti	Pravděpodobnost výskytu hrozby celková - P
Povodeň	Poloha v zátopové oblasti	Nízká (1)
Požár	Shoření	Nízká (1)
Prach, koroze	Citlivost na prach, vlhkost	Střední (2)
Zničení zařízení nebo médií	Špatná údržba, neodborné zacházení	Střední (2)
Přerušení dodávky elektřiny	Nestabilní síť	Střední (2)
Krádež médií, nebo dokumentů	Nechráněné uskladnění	Střední (2)
Krádež zařízení	Nedbalost při zacházení se svěřeným zařízením	Střední (2)
Zneužití oprávnění	Neodhlášení se při opouštění pracovní stanice	Vysoká (3)
Poškození dat	Nedostatky v postupech pro řízení dokumentace	Vysoká (3)
Přetížení informačního systému	Nedostatečná odezva pracovníků údržby	Vysoká (3)
Falšování práv	Nedostatečná identifikace a autentizace uživatele	Střední (2)
Chyba použití	Špatné nastavení parametrů	Vysoká (3)
Odposlech	Nechráněný přenos dat	Vysoká (3)
Neoprávněné použití zařízení	Nedostatek politik pro použití telekomunikačních prostředků	Vysoká (3)
Selhání telekomunikačního zařízení	Bod totálního selhání	Střední (2)

Tabulka 6. Identifikace hrozeb

11.5 Analýza zranitelnosti aktiva při výskytu hrozby

V tomto bodě bude sestavena tabulka, ve které budou porovnány závažnosti hrozeb a hodnoty aktiv. Pro každé aktivum bude stanovena hodnota zranitelnosti při výskytu dané hrozby - **PD**. Tato hodnota bude určována pomocí stupnice **„nízká“ – 1, „střední“ - 2 a „vysoká“ – 3**. Hodnota aktiva - **A**. Pravděpodobnost výskytu hrozby - **PC**.

Matice zranitelnosti	**Hrozba**	Povodeň	Požár	Prach, koroze	Zničení zařízení nebo médií	Přerušení dodávky elektřiny	Krádež médií nebo dokum.	Krádež zařízení	Zneužití oprávnění	Poškození dat	Přetížení informačního sys.	Falšování práv	Chyba použití	Odposlech	Neoprávněné použití zaříz.	Selhání telekomun. zaříz.
Aktivum	PC	1	1	2	2	2	2	2	3	3	3	2	3	3	3	2
	A															
Proces Core Bussinessu společnosti	3	1	2	x	2	2	3	3	3	2	3	2	x	x	2	3
Know-how	3	x	x	x	x	x	3	x	2	2	x	x	x	3	x	x
Informace o zákaznících	2	x	x	x	1	x	2	1	2	2	x	2	x	3	2	x
Smlouvy se zákazníky	3	1	1	x	x	x	3	x	2	x	x	x	1	x	x	x
Dokumentace k systémům	3	1	1	x	2	x	3	x	2	2	x	2	1	3	3	x
Pracovní smlouvy se zaměstnanci	3	1	1	x	x	x	2	x	2	x	x	2	x	x	x	x
Pevné pracovní stanice	2	1	1	3	3	3	2	3	2	3	x	2	3	x	3	x
Přenosná zařízení určená k výkonu práce	2	1	1	1	3	x	3	3	2	2	x	2	2	x	3	x
Stolní telefony	1	1	1	2	2	x	x	1	x	x	x	x	1	3	1	1
Nosiče dat (pasivní)	2	1	1	1	3	x	3	3	2	3	x	x	2	x	2	x
Tiskárny	1	1	1	3	1	1	x	1	x	x	x	x	1	x	1	1
Ostatní nosiče dat	2	1	1	2	3	x	3	x	2	2	x	2	1	x	x	x
Řídící orgány podniku	3	1	1	x	x	x	x	x	2	x	x	2	1	2	2	x
Standartní softwarové vybavení	2	x	x	x	x	x	2	2	x	2	x	x	3	x	2	x
Speciální podnikové aplikace	2	x	x	x	x	x	2	2	2	2	3	2	2	x	2	x
Síťový hardware (serverovny)	3	1	1	2	1	1	x	1	1	2	3	2	3	x	2	3
Síťový hardware (uživatelé)	2	1	2	2	1	2	2	1	2	2	3	2	2	x	2	3
Servery informačního systému	3	1	1	2	1	1	x	1	2	2	3	2	2	x	2	3
Internetová konektivita	3	x	x	x	x	2	x	x	2	3	2	x	x	3	2	3
Budova podniku	3	2	2	x	1	2	x	x	1	x	x	2	x	x	x	x

Tabulka 7. Matice zranitelnosti

11.6 Analýza rizika a míry dopadu

Matice rizik	**Hrozba**	Povodeň	Požár	Prach, koroze	Zničení zařízení nebo médií	Přerušení dodávky elektřiny	Krádež médií nebo dokum.	Krádež zařízení	Zneužití oprávnění	Poškození dat	Přetížení informačního sys.	Falšování práv	Chyba použití	Odposlech	Neoprávněné použití zařiz.	Selhání telekomun. zařiz.
Aktivum	PC	1	1	2	2	2	2	2	3	3	3	2	3	3	3	2
	A															
Proces Core Bussinessu společnosti	3	3	6	x	12	12	18	18	27	18	27	12	x	x	18	18
Know-how	3	x	x	x	x	x	18	x	18	18	x	x	x	27	x	x
Informace o zákaznících	2	x	x	x	4	x	8	4	12	12	x	8	x	18	12	x
Smlouvy se zákazníky	3	3	3	x	x	x	18	x	18	x	x	x	9	x	x	x
Dokumentace k systémům	3	3	3	x	12	x	18	x	18	18	x	12	9	27	27	x
Pracovní smlouvy se zaměstnanci	3	3	3	x	x	x	12	x	18	x	x	12	x	x	x	x
Pevné pracovní stanice	2	2	2	12	12	12	8	12	12	18	x	8	18	x	18	x
Přenosná zařízení určená k výkonu práce	2	2	2	4	12	x	12	12	12	12	x	8	12	x	18	x
Stolní telefony	1	1	1	4	4	x	x	2	x	x	x	x	3	9	3	2
Nosiče dat (pasivní)	2	2	2	4	12	x	12	12	12	18	x	x	12	x	12	x
Tiskárny	1	1	1	6	2	2	x	2	x	x	x	x	3	x	3	2
Ostatní nosiče dat	2	2	2	8	12	x	12	x	12	12	x	8	6	x	x	x
Řídící orgány podniku	3	3	3	x	x	x	x	x	18	x	x	12	9	18	18	x
Standartní softwarové vybavení	2	x	x	x	x	x	8	8	x	12	x	x	18	x	12	x
Speciální podnikové aplikace	2	x	x	x	x	x	8	8	12	12	18	8	12	x	12	x
Síťový hardware (serverovny)	3	3	3	12	6	6	x	6	9	18	27	12	27	x	18	18
Síťový hardware (uživatelé)	2	2	2	8	4	8	8	4	12	12	18	8	12	x	12	12
Servery informačního systému	3	3	3	12	6	6	x	6	18	18	27	12	18	x	18	18
Internetová konektivita	3	x	x	x	x	12	x	x	18	27	18	x	x	27	18	18
Budova podniku	3	6	6	x	6	12	x	x	9	x	x	12	x	x	x	x

Tabulka 8. Matice rizik

V tabulce č.8 (matice rizik) můžeme vidět hodnoty, které jsme zjistili pomocí vzorce A* PC*PD, kde A vyjadřuje hodnotu rizika (určenou v tabulce č.5), PC vyjadřuje celkovou pravděpodobnost výskytu hrozby (určenou v tabulce č.6) a PD vyjadřuje dílčí pravděpodobnost zranitelnosti aktiva na danou hrozbu (určenou v tabulce č.7).

Tímto krokem jsme zjistili, jak jsou která aktiva důležitá, náchylná na využití zranitelnosti a na které aktiva by mohlo působení hrozby mít největší dopad.

Z hlediska přehlednosti a kvůli určení teoretické hodnoty každého aktiva pro společnost je vhodné sjednotit hodnoty zjištěné v tabulce č. 8 pomocí aritmetického průměru. Zjištěné hodnoty budou zaokrouhleny na celá čísla.

AKTIVUM	ARITMETICKÝ PRŮMĚR
Proces Core Bussinessu společnosti	**16**
Know-how	**20**
Informace o zákaznících	**10**
Smlouvy se zákazníky	**10**
Dokumentace k systémům	**15**
Pracovní smlouvy se zaměstnanci	**10**
Pevné pracovní stanice	**11**
Přenosná zařízení určená k výkonu práce	**10**
Stolní telefony	**3**
Nosiče dat (pasivní)	**10**
Tiskárny	**2**
Ostatní nosiče dat	**8**
Řídící orgány podniku	**12**
Standartní softwarové vybavení	**12**
Speciální podnikové aplikace	**11**
Síťový hardware (serverovny)	**13**
Síťový hardware (uživatelé)	**9**
Servery informačního systému	**13**
Internetová konektivita	**20**
Budova podniku	**9**

Tabulka 9. Hodnota aktiva

12 ZAVEDENÍ OCHRANNÝCH OPATŘENÍ

Účinná bezpečnost zpravidla vyžaduje kombinaci různých opatření, aby poskytovala aktivům určitý stupeň bezpečnosti. Ochranné opatření jsou nástrojem ke snižování míry výsledného rizika.

Opatření jdou definovány jako praktiky, postupy nebo mechanizmy, které můžou:

- snížit zranitelnost
- poskytovat ochranu před hrozbami
- snížit dopad nežádoucího incidentu
- identifikovat nežádoucí incidenty
- ulehčit obnovu

Hlavním cílem bezpečnostních opatření je eliminovat působení hrozeb na aktiva informačního systému. Ochranné opatření můžou rizika působící na informační systém:

- eliminovat
- snížit
- přesunout
- akceptovat

Zanedbání nebo opomenutí některého z opatření může mít za následek oslabení nebo dokonce narušení celého informačního systému. Zároveň platí pravidlo, že informační systém je natolik bezpečný, nakolik je bezpečný jeho nejslabší článek

Ochranné opatření zpravidla členíme na:

- **opatření v oblasti fyzické bezpečnosti**
- **organizační a režimové opatření**
- **opatření v oblasti informační bezpečnosti**

12.1 Opatření v oblasti fyzické bezpečnosti

Oblast fyzické bezpečnosti zahrnuje tyto námi zkoumané aktiva:

Smlouvy se zákazníky - 10
Dokumentace k systémům - 15
Pracovní smlouvy se zaměstnanci - 10
Pevné pracovní stanice - 11
Přenosná zařízení určená k výkonu práce - 10
Stolní telefony - 3
Nosiče dat (pasivní) - 10
Tiskárny - 2
Ostatní nosiče dat - 8
Síťový hardware (serverovny) - 13
Síťový hardware (uživatelé) - 9
Servery informačního systému - 13
Budova podniku - 9

Opatření v oblasti fyzické bezpečnosti zahrnují:

1. **Fyzickou ochranu**

Fyzické ochranné opatření zahrnují oplocení areálu společnosti, nepřetržité monitorování budov, uchovávání záznamů, řízení fyzického přístupu do budov, rackové skříně pro ochranu IT techniky apod.

2. **Protipožární ochranu**

Vybavení a okolní prostory, včetně přístupů k nim by měly být chráněné před rozšířením požáru z budovy. Rizika požáru u prostorů s důležitým vybavením by měly být minimalizovány. Ochranné opatření by měly zahrnovat detekci ohně a dýmu, poplachy a zneškodnění požáru. Důležité je, aby byly k hašení použity takové prostředky, které nezpůsobí poškození IT techniky.

3. **Ochranu proti vodě**

Důležité zařízení by měly být umístěny v prostorech, kde není pravděpodobný výskyt záplav způsobených klimatickými změnami, nebo zaplavení z důvodu např. prasknutí vodovodního potrubí.

4. **Ochranu před ostatními přírodními vlivy**

Důležité zařízení by měly být chráněny před účinkem změny napětí způsobeného například bleskem. K tomu mohou dopomoci například přepěťové ochrany.

5. **Ochranu před krádeží**

Všechny vybavení by měly mít jedinečné identifikační označení a měl by být udržovaný soupis tohoto vybavení s pravidelnou kontrolou stavu. Stálá dohledová služba by měla zajišťovat kontrolu všech zařízení a médií, které opouštějí budovy organizace.

6. **Ochranu napájení a klimatizace důležitých prvků IS**

Všechny důležité IT prvky by měly být chráněny před chybami v napájení. Měl by být zajištěný vhodný zdroj napájení a záložní zdroj napájení Uninterruptible Power Suply (UPS). U techniky, která je důležitá pro chod celého IS je vhodné použít UPS s větším výkonem, které jsou schopny napájet IS po dlouhou dobu. U kancelářských IT zařízení, které mají větší hodnotu stačí použít menších UPS, které zajistí ochranu před změnami v elektrické síti, krátkodobými výpadky a dopomohou tak k tomu, že nedojde k poškození zařízení, nebo ztrátě neuložených dat.

Obrázek 7. Skříně rack

Obrázek 8. Záložní zdroj

<u>Návrh konkrétních opatření fyzické bezpečnosti u aktiv</u>:
Smlouvy se zákazníky - 10
Dokumentace k systémům - 15
Pracovní smlouvy se zaměstnanci - 10
Ostatní nosiče dat - 8

Jedná se o aktiva, které svojí hodnotou patří mezi významnější a můžou se vyskytovat jak v papírové, tak v elektronické podobě. U papírové formy je vhodné tato aktiva uchovávat v archivech, popřípadě trezorech s omezeným přístupem pouze pro vedení organizace. To stejné platí i u elektronické podoby. I zde je nutné řídit přístupy pomocí práv a hesel, kterými disponuje pouze určitá skupina lidí. Také je vhodné tyto dokumenty v elektronické podobě zálohovat na jiné úložiště, aby nedošlo k jejich ztrátě.

Návrh konkrétních opatření fyzické bezpečnosti u aktiv:
Pevné pracovní stanice - 11
Přenosná zařízení určená k výkonu práce - 10
Stolní telefony - 3
Nosiče dat (pasivní) - 10
Tiskárny - 2

Aktiva **stolní telefony** a **tiskárny** mají z hlediska bezpečnosti malý význam a jejich nahrazení může být takřka okamžité a ztráta při jejich výpadku minimální. Jejich hodnota přesto nebývá malá. Ochranu těchto zařízení můžeme zajistit především pravidelnou údržbou a správným používáním. U tiskáren z hlediska šetření nákladů zřídit evidenci tisku oproti uživatelským účtům.

Narušení bezpečnosti u aktiv **pevné pracovní stanice, přenosná zařízení určená k výkonu práce a nosiče dat** může mít pro firmu z hlediska jejich hodnoty vyšší dopad. Tyto zařízení jsou hlavně ve správě uživatelů, a proto by tito uživatelé za ně měli mít patřičnou odpovědnost. Vzhledem k tomu, že data obsažená na těchto zařízeních mohou být velmi citlivá, je důležité jejich obsah chránit silným heslem a také zálohovat nejlépe na firemní file servery s řízeným přístupem do složek.

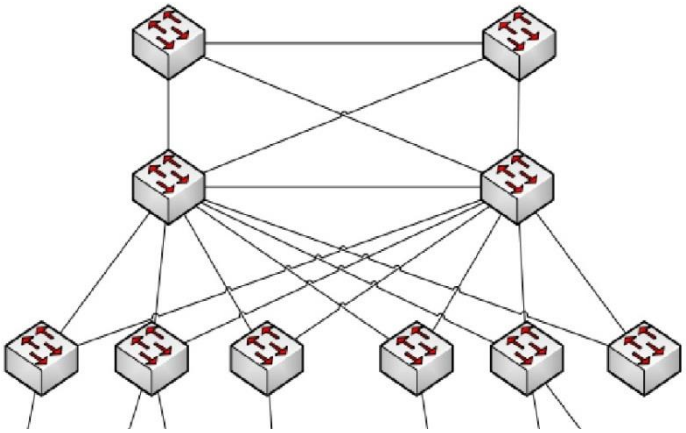
Návrh konkrétních opatření fyzické bezpečnosti u aktiv:
Síťový hardware (serverovny) - 13
Síťový hardware (uživatelé) - 9
Servery informačního systému - 13
Budova podniku - 9

Budova podniku je důležité aktivum a je nutné ji chránit především perimetrickou ochranou, fyzickou ochranou, režimovou ochranou a protipožární ochranou. Všechny tyto oblasti námi zkoumaná společnost má řešeny dobře. Perimetrickou ochranu zajišťují ploty s ostnatými dráty a budova s řízeným přístupem. Fyzickou ochranu zajišťuje bezpečnostní služba jak na úrovni vjezdu do areálu, tak na úrovni vchodu budovy. Celý prostor je monitorován a nahráván kamerovým systémem a přístupy ve vnitřních prostorách jsou řízeny čipovými kartami. Protipožární ochranou je pokryta celá budova a to jak aktivními hasícími systémy, tak pasivními kouřovými detektory.

Síťový hardware (uživatelé) je také velmi důležité a cenné aktivum, avšak pro chod hlavních informačních systémů ne až tak důležité, protože není na těchto zařízeních závislý. Při dlouhodobějším výpadku by však mohly nastat potíže, kdy by uživatelé nemohli pracovat a starat se o chod společnosti. Vhodná opatření jsou uzamknout tyto

zařízení v prostorech s řízeným přístupem, popřípadě používat uzamykatelných rack skříní. Dále se doporučuje používat zdvojených tras propojení a zdvojení (redundanci) samotných prvků. Při výpadku jedné trasy nebo jednoho prvku tak nedojde k výpadku sítě. Posledním vhodným opatřením je záloha konfigurace zařízení a placená podpora od dodavatele (např. rychlá výměna prvku).

Síťový hardware (serverovny) a Servery informačního systému – tato aktiva jsou životně důležitá pro chod informačního systému. V případě výpadku těchto zařízení může dojít k velkým finančním a jiným ztrátám společnosti. Opatření pro bezvýpadkový chod informačního systému je omezení přístupu pouze pro správce systému, uzamknutí zařízení ve skříních rack, zdvojení síťových tras, včetně internetové konektivity, fyzická redundance prvků, záloha konfigurací, podpora od dodavatele techniky, chlazení a protipožární zařízení, které nezpůsobí škody na technice.



Obrázek 9. Zdvojení (Redundance)

12.2 Opatření v oblasti informační bezpečnosti

Oblast informační bezpečnosti zahrnuje tyto námi zkoumané aktiva:

Proces Core Bussinessu společnosti – 16
Know-how – 20
Informace o zákaznících – 10

Standartní softwarové vybavení - 12

Speciální podnikové aplikace – 11

Dokumentace k systémům - 15

Síťový hardware (serverovny) - 13
Síťový hardware (uživatelé) - 9
Servery informačního systému - 13
Internetová konektivita – 20

Do okruhu informační bezpečnosti spadá především kontrola uživatelských přístupů k datům, ochrana uložených dat a ochrana dat přenášených po síti.

1. Kontrola uživatelských přístupů k datům – k ohrožení informací může dojít kupříkladu neoprávněným prolomením hesla. To může ohrozit velkou část informačních aktiv. Základní ochranou proti takovému typu útoku je dostatečně silné heslo, které je kombinací malých a velkých písmen, číslic a speciálních znaků. Dalším typem opatření může být řízení přístupů pomocí doménového řadiče, který umožňuje rozpoznávání uživatele a umožní mu tak přístup pouze k souborům, ke kterým mu byl v rámci jeho pracovní náplně povolen. Posledním typem je zabezpečení pomocí protokolu 802.1X, který řídí přístup jak uživatelské stanice, tak uživatele. Funguje tak, že rozpozná firemní zařízení, které má uložené v databázi plus přihlášení uživatele a povolí mu zdroje, ke kterým má mít přístup. Pokud se v síti objeví zařízení, které protokol 8021.X nerozpozná, nepovolí mu přístup k žádným zdrojům. Návrh opatření je použít všech těchto možností a docílit tak maximálního možného zabezpečení.

<u>Doporučení v bodě 1 se týkají aktiv</u>:
Know-how – 20
Informace o zákaznících – 10

Standartní softwarové vybavení - 12

Speciální podnikové aplikace – 11

Dokumentace k systémům - 15

Síťový hardware (serverovny) - 13
Síťový hardware (uživatelé) - 9
Servery informačního systému - 13

2. Ochrana uložených dat

K ochraně uložených dat patří kontrola uživatelských přístupů k datům, která je uvedena v bodě jedna, ale také fyzická bezpečnost zařízení, na kterých jsou cenná data uložena uvedená v kapitole 12.1 o fyzické bezpečnosti.

Hlavním bodem ochrany uložených dat je však jejich zálohování. Doporučení je zálohovat data minimálně na dvě nezávislé aktivní diskové pole, u kterých jsou tyto data v jeden čas dostupné tak, aby při výpadku jednoho nedošlo k dočasnému omezení procesů společnosti. Dalším doporučením je zálohování na magnetické pásky, na kterých lze data uchovávat po velmi dlouhou dobu. Důležitým krokem je však také zálohovat konfigurace všech síťových prvků, aby mohlo v případě problému dojít k rychlému obnovení požadované funkce.

Doporučení v bodě 2 se týkají aktiv:
Know-how – 20
Informace o zákaznících – 10

Proces Core Bussinessu společnosti – 16
Speciální podnikové aplikace – 11

Dokumentace k systémům - 15

Síťový hardware (serverovny) - 13
Síťový hardware (uživatelé) - 9
Servery informačního systému – 13

3. Ochrana dat přenášených po síti

Ochrana dat přenášených po síti hlavně závisí na tom, zda jsou data přenášena po vnitřní síti (LAN), nebo po síti Internet (WAN).

Komunikace ve vnitřní síti – základním doporučením je oddělení uživatelských sítí a sítí pro servery do samostatných broadcastových domén (vlan), aby nedocházelo k možnosti přetížení důležitých informačních systémů neúměrným množstvím dotazů. Stejně důležité je řízení provozu pomocí IP adres a portů, k čemuž slouží interní stavové firewally. Pravděpodobnost odposlouchávání komunikace ve vnitřní síti je malá, takže není důvod zde používat šifrování komunikace.

Komunikace se sítí Internet – tento bod je z hlediska bezpečnosti a procesu funkce core bussinesu společnosti nejkritičtější, protože se jedná o nejméně bezpečnou komunikaci, avšak životně důležitou pro chod organizace. Základní doporučení je používat šifrovacích protokolů SSH, SSL či podobných, nebo tunelového spojení VPN.

SSH – (Secure Shell) – je protokol založený na principu šifrování veřejným klíčem. To znamená, že pracuje s dvojicí klíčů, soukromým a veřejným. Je to základní nástroj používaný hlavně ke vzdáleným konfiguracím zařízení, nebo datovému přenosu.

SSL – (Secure Socket Layer) – je podobně založený jako SSH a poskytuje bezpečnou komunikaci mezi klientem a serverem.

VPN - (Virtual Private Network) - je prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, dojde k autentizaci, veškerá komunikace je šifrována, a proto můžeme takové propojení považovat za bezpečné. [13]

Komunikace po beztrátové síti - doporučení pro komunikaci po bezdrátové síti je používat zabezpečení WPA2 se šifrováním AES, které bezpečně zamezí odposlechům bezdrátového provozu. Pro samotné připojení do bezdrátu není vhodné používat Preshared-key, protože může dojít k jeho snadnému šíření, ale doporučením je spíše používat protokoly PEAP, či EAP-TLS, které ověřují uživatele a koncové stanice oproti radius serveru pomocí důvěryhodných certifikátů , dohromady ověřením proti AD.

Obrázek 10. Virtual Private Network[15]

Další doporučené možnosti ochrany vnitřních sítí jsou například L3 firewally, které jsou ovšem standardem ve všech sítích, dále proxy servery a IPS/IDS sondy, které jsou tím nejlepším, co lze k ochraně v před vnějším prostředím v dnešní době použít.

L3 Firewally - Firewall je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. [14]

Proxy server - je počítač, který funguje jako prostředník mezi webovým prohlížečem (jako je například aplikace Internet Explorer) a Internetem. Proxy servery pomáhají zlepšit výkon webu ukládáním kopií často navštěvovaných webových stránek. Pokud prohlížeč požaduje webovou stránku uloženou ve sbírce proxy serveru (v jeho mezipaměti), proxy server ji poskytne sám, což je rychlejší než připojení k příslušnému webu. Proxy servery také pomáhají zlepšit zabezpečení filtrováním obsahu webu a nebezpečného softwaru.[16]

IPS/IDS sonda - Intrussion Detection System je systém, který detekuje narušení (potencionální útok). IDS jsou centrálně orientované systémy, které se skládají ze sond detekujících útoky, databáze, do které jsou tyto záznamy ukládány a centrální management konzole, ze které je možné do databází nahlížet, ale také generovat výstupy. Tyto výstupy mají formu, kterou si stejně jako typ informací, které obsahují, může administrátor přizpůsobit. Některé tyto konzole disponují vyspělými analytickými nástroji.

Pod pojmem IPS (Intrussion Prevention systém) je pokračování IDS. Zatímco úkolem IDS je útoky detekovat, pak úkolem IPS, je útoky detekovat a zastavit. Na první pohled to vypadá, že IDS nemají na trhu již místo. Realita je ale zcela odlišná. IPS rozhodně není vhodným řešením pro každou implementaci.[17]

V posledním bodě je nutné dodat, že je důležité, aby byl celkový provoz sítí logován pomocí vhodného log management nástroje, který bude administrátorům nápomocen při řešení jakékoliv bezpečnostní události.

Toto jsou doporučené nástroje, které jsou vhodné k zajištění dostatečně bezpečného fungování informačního systému.

Tato opatření jsou vhodná pro všechna aktiva uvedená v bodě 12.2.

12.3 Organizační a režimové opatření

Tato kapitola se dotýká bezpečnosti všech zkoumaných aktiv

Režimové opatření jsou kroky, které je potřeba přijmout, aby byly prostředky přijaté ve fyzické a informační bezpečnosti maximálně využity a nebyly oslabovány, nebo znehodnocovány působením lidského faktoru. Mezi tyto opatření patří :

- vytváření bezpečnostního povědomí ve firmě – je vhodné, aby byli zaměstnanci zapojeni do procesu vytváření bezpečnostního povědomí a byli s ním patřičně seznámeni
- školení zaměstnanců – pravidelné školení zaměstnanců v oblasti bezpečnosti a v oblasti znalosti informačních systému napomáhá zvýšení efektivity práce a snížení počtu uživatelských chyb
- úprava pracovních smluv – práva a povinnosti musí být zakotveny přímo v pracovních smlouvách (smlouva o mlčenlivosti).
- podnikové bezpečnostní směrnice – důležitou součástí ochrany informačního systému je přijetí odpovídající bezpečnostní směrnice. Návrh, jak by měla tato bezpečnostní směrnice vypadat je umístěn v **příloze P I**.

12.4 Bezpečnostní směrnice

Bezpečnostní směrnice je další opatření, které je vhodné přijmout, aby došlo ke zvýšení povědomí všech uživatelů, ochraně informací, hlášení bezpečnostních incidentů, pravidel používání, pravidel přístupů a správnému řízení procesů.

Doporučení pro společnost XY, ale i každou IT organizaci je přijmout bezpečnostní směrnici sestavenou dle ISO 27000 a tím zvýšit svou konkurenceschopnost ve světě informačních technologií. Jak by měla vypadat taková bezpečnostní směrnice je uvedeno v příloze P I.

ZÁVĚR

Zadáním práce bylo analyzovat rizika IT bezpečnosti společnosti XY. Tuto analýzu jsem prováděl pomocí nástrojů sady norem ISO 27000. V teoretické části práce jsem popsal obecnou teorii analýzy rizika a vymezil jednotlivé pojmy. Za další jsem uvedl, co je PDCA cyklus, kterým se celý systém řídí. Bylo popsáno, co je ISMS a proč je důležité jej provádět. Největší část teorie byla však věnována doporučenému postupu analýzy rizika podle normy ISO 27005 a to jak identifikovat a ohodnocovat aktiva, hrozby, zranitelnosti a jakým způsobem provádět samotnou analýzu rizika. V poslední části byly uvedeny, jaké hrozby a zranitelnosti se můžou objevovat v oblasti informační bezpečnosti.

V praktické části jsem začal popisem zkoumané společnosti, čím se tato společnost zabývá, jaká je její organizační struktura a zhodnotil aktuální stav informační bezpečnosti. Dále jsem identifikoval a ohodnotil její důležitá aktiva, možné hrozby a zranitelnosti aktiv při působení hrozeb. Hodnocení aktiv, hrozeb a zranitelností jsem prováděl podle několikaleté osobní zkušenosti z praxe. Samotný postup analýzy rizika jsem prováděl dle doporučení směrnice ISO 27005 pomocí matice rizik. Touto maticí jsem zjistil, jakou mají jednotlivé aktiva pro společnost hodnotu a na které by mohlo mít působení hrozeb největší dopad. Na závěr jsem určil, jaké náležitosti je nutné splnit, aby došlo ke zvýšení IT bezpečnosti společnosti XY.

Díky této práci jsem si více uvědomil, která aktiva informačního systému jsou důležitá, jaké možné hrozby na ně mohou působit, přišel na mnoho možností ošetřování rizik informační bezpečnosti a pochopil důležitost provádět kroky analýzy rizika.

SEZNAM POUŽITÉ LITERATURY

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

[2] ČSN ISO/IEC 27000 (36 9790) *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací* - Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010, 23 s.

[3] ČSN ISO/IEC 27005 (36 9790) *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013, 63 s. Česká technická norma.

[4] HANÁČEK, Petr a Jan STAUDEK. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém, 2000, 127 s. ISBN 80-238-5400-3.

[5] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, ix, 190 s. ISBN 8025101061.

[6] PROSISE, Chris a Kevin MANDIA. *Počítačový útok: detekce, obrana a okamžitá náprava*. Vyd. 1. Praha: Computer Press, 2002, xxii, 410 s. ISBN 8072266829.

[7] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí (praktické rady a návody)*. 1. vyd. Praha: Grada, 2003, 200 s. ISBN 80-247-0663-6.

[8] ŠEFČÍK, Vladimír. *Analýza rizik*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 8073186969.

[9] *Storagecraft* [online]. 2013 [cit. 2015-02-18]. Dostupné z WWW: <http://www.zalohovani.net/zalohovani-a-archivace-dat-v-podnikovem-prostredi-6-dil-cast-13-business-continuity-management-bcm >.

[10] *Vlastní cesta* [online]. 2011 [cit. 2015-03-05]. Dostupné z WWW: <http://www.vlastnicesta.cz/clanky/informace-a-bezpecnost/>.

[11] *Český normalizační institut* [online]. 2006 [cit. 2015-03-19]. Dostupné z WWW: <http://csnonlinefirmy.unmz.cz/html_nahledy/36/76533/76533_nahled.htm/>.

[12] *University of Riverside* [online]. 2015 [cit. 2015-04-06]. Dostupné z WWW: <http://www.uofriverside.com/conferences/management-conferences/global-symposium-on-information-and-network-security/2015-fall-global-symposium-on-information-and-network-security/>.

[13] *Attel* [online]. 2015 [cit. 2015-04-10]. Dostupné z WWW: <http://www.attel.cz/cz/produkty-a-reseni/typova-reseni/vpn-virtualni-privatni-sit/23-definice-vpn/>.

[14] *Lucie Zolta* [online]. 2015 [cit. 2015-04-10]. Dostupné z WWW: <http://lucie.zolta.cz/index.php/pocitace-a-site/178-stavovy-firewall/>.

[15] *Netkrom Solution* [online]. 2015 [cit. 2015-04-10]. Dostupné z WWW: <http://netkromsolution.com/?portfolio=portfolio-3/>.

[16] *Windows* [online]. 2015 [cit. 2015-04-10]. Dostupné z WWW: <http://windows.microsoft.com/cs-cz/windows-vista/what-is-a-proxy-server/>.

[17] *4safety* [online]. 2015 [cit. 2015-04-10]. Dostupné z WWW: < http://www.4safety.cz/text/ids/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ISO International Organization of Standardization

IS Informační systém

PDCA Plan Do Check Act

ISMS Information Security Management System

IT Informační technologie

UPS Uninterruptible Power Suply

LAN Local Area Network

VLAN Virtual Local Area network

WAN Wide Area Network

SSH Secure Shell

SSL Secure Socket Layer

VPN Virtual Private Network

IDS Intrusion Detection System

IPS Intrusion Prevention Systém

AD Active Directory

WPA2 Wi-Fi Protected Access Version 2

AES Advanced Encryption Standard

PEAP Protected Extensible Authentication Protocol

EAP-TLS Extensible Authentication Protocol – Transport Layer Security

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: BEZPEČNOSTNÍ SMĚRNICE SPOLEČNOSTI XY

Bezpečnostní směrnice

1 Základní ustanovení

1.1 Preambule

Představenstvo společnosti XY (dále jen „společnost“) vydává prostřednictvím tohoto interního dokumentu Bezpečnostní směrnici své společnosti. Stanovení podmínek, limitů a lhůt, specifických pro konkrétní společnost pro potřeby této směrnice je možné ustanovit písemným dodatkem Rámcové smlouvy. Při zabezpečení cílů stanovených vedením společnosti v rámci této směrnice je využívána jako poradenská a servisní entita Společnost XY (dále jen „Společnost XY“).

1.2 Význam zkratek a výrazů

PS prostředky ve vlastnictví společnosti XY.

BYOD prostředky ve vlastnictví zaměstnance

ITPKU oddělení Podpora koncových uživatelů společnosti XY

IT DKI oddělení správy Datové a komunikační infrastruktury společnosti XY

PC osobní počítač

IS informační systém

SW programové vybavení výpočetní techniky

zaměstnanec osoba, které trvá pracovní poměr se společností XY.

1.3 Úvodní ustanovení

Společnosti vlastní nebo disponují prostředky (dále jen PS), kterými vytváří hodnoty v rámci své podnikatelské činnosti. Ve smyslu této směrnice se jedná o informační a telekomunikační technologie, které slouží k získávání, zpracování, uchovávání, přenos a sdílení informací v elektronické a jiné podobě.

PS jsou v užívání společností a odpovědnost za ně nesou zaměstnanci, jimž byly tyto PS svěřeny k užívání. Zaměstnanci jsou zavázáni se chovat tak, aby svým počínáním neumožnili či neusnadnili přístup k PS nepovolaným osobám, a to jak po dobu trvání pracovněprávního vztahu, tak i po jeho skončení. Zneužití PS zaměstnancem je posuzováno jako porušení vnitřních předpisů, které je považováno za porušování pracovních povinností a může mít pracovněprávní důsledky.

2 Bezpečnostní incidenty

Za bezpečnostní incident jsou považovány všechny události, při nichž dojde k ohrožení dostupnosti, integrity a důvěrnosti informací, stejně jako zneužití, zcizení, ztráty či poškození dat.

Bezpečnostní incidenty (dále jen BI) zahrnují, ale nejsou omezeny pouze na:

- Ztráta PS nebo BYOD
- Zcizení PS nebo BYOD
- Zneužití PS nebo BYOD (zcizení, kompromitace nebo poskytnutí hesla)

2.1 Hlášení bezpečnostních incidentů

Zaměstnanec je povinen každý zjištěný bezpečnostní incident neprodleně ohlásit.

Ohlášení BI je možné provést:

- Web http:\\hlaseni
- Telefonicky 522 xxx xxx
- Emailem podpora@spolecnost.cz

2.2 Řešení bezpečnostních incidentů

Za řešení BI je odpovědný bezpečnostní manažer společnosti XY podle odpovídající směrnice. Výsledek šetření BI spolu s návrhem nápravného opatření pak předává na vedení dotčené společnosti.

3 Bezpečnost informací

3.1 Klasifikace informací

Zaměstnanci klasifikují data do skupin podle tabulky č. 1.

Typ dat	Popis	Cílová skupina
4. Diskrétní	Přístupová hesla do systémů, šifrovací klíče, Informace o mzdách a další, o nichž tak stanoví vedení. Tištěné dokumenty obsahující taková data musí být v záhlaví označeny.	zaměstnanci pověření vedením, případně ad hoc pověření zaměstnanci
3. Citlivá	Osobní údaje zaměstnanců, obchodní smlouvy. Tištěné dokumenty obsahující taková data musí být v záhlaví označeny.	skupina zaměstnanců určená vedením
2. Interní	Data přístupná všem zaměstnancům (interní předpisy, dokumenty) Pracovní postupy, které nejsou klasifikovány jako Know-How. Tištěné dokumenty obsahující taková data mohou být označeny	zaměstnanci
1. Veřejná	Informace zveřejnitelné, dostupné na webových stránkách. Tištěné dokumenty nemusí být nijak označeny.	veřejnost

Tabulka 1.

V případě, že nebude spolehlivě určeno zařazení dat do některé ze skupin informací, bude takto o jejich zařazení rozhodnuto vedením. Do doby než se tak stane, se považují tato data, za data skupiny 3, tedy Citlivá.

3.2 Ochrana Informací

Zaměstnanci mohou informace kategorií 2, 3 a 4 využívat výhradně k pracovním účelům. Nakládání s informacemi pro osobní účely, nebo pro účely třetí strany, pokud není tato činnost pracovní náplní zaměstnance, se považuje za porušení interních směrnic. Při práci nesou zaměstnanci odpovědnost ve věci bezpečnosti za data, se kterými se dostávají do styku. Zaměstnanci jsou zavázáni s informacemi nakládat tak, aby nedošlo k narušení jejich dostupnosti, důvěrnosti, integrity, stejně jako je nutné zamezit ztrátě, zcizení či zneužití.

4 Pravidla pro používání prostředků Společnosti

4.1 Ochrana přístupu k PS

Zaměstnanci jsou zodpovědní za jim svěřené PS, čímž jsou zavázáni dodržovat a dbát následující:

- PS nebo BYOD nesmí být ponecháno volně dostupné neoprávněné osobě
- V případě nepřítomnosti uživatele musí být PS nebo BYOD zabezpečeno proti zcizení, zneužití
- Informace nacházející se v PS nebo BYOD musí být chráněny proti zcizení, ztrátě, zneužití a poškození podle pravidel a opatření uvedených v bezpečnostních směrnicích
- Dodržovat politiku hesel (viz. kapitola Politika hesel)
- Pracovní stanice musí být přidány do domény (výjimky uděluje výkonný ředitel společnosti na základě konzultace s bezpečnostním manažerem.)

4.2 Ochrana autorských práv

Zaměstnancům je zakázáno pořizovat, uchovávat nebo sdílet nelegální kopie produktů, které jsou chráněny autorskými právy. Zaměstnanci jsou zodpovědní za dodržování autorských práv a licenčních podmínek, které se vztahují k programům, souborům, grafice, dokumentům, audio a video souborům, zprávám a ostatním materiálům, které mají v úmyslu stahovat nebo kopírovat. Je zakázáno vyslovit souhlas s licenčními podmínkami nebo stahovat jakýkoli materiál, za který se vybírají poplatky, bez předchozího doložitelného souhlasu zaměstnavatele, v případě programového vybavení i souhlasu IT bezpečnostního manažera společnosti XY.

4.3 Zakázaný obsah

Je zakázáno používat PS k shromažďování, uchovávání, rozesílání a sdílení materiálů, které zahrnují, ale neomezují se pouze na:

- Podvodné dokumenty
- Omezování lidských práv a svobod
- Omezující práva menšin
- Rasistická tématika
- Neuctivá, pornografická, nemravná, výhružná, hanlivá tématika

Soubory získané ze zdrojů mimo společnost, včetně přenosných médií z domova, souborů stažených z Internetu, získaných z diskusních skupin a ostatních on-line služeb, souborů připojených k e-mail zprávám a souborů získaných ze zdrojů mimo Společnost, včetně přenosných médií z domova, souborů stažených z internetu, získaných z diskusních skupin a ostatních on-line služeb, souborů připojených k e-mail zprávám a souborů získaných od zákazníků a dodavatelů, mohou obsahovat škodlivé kódy, které mohou poškodit zařízení v interní počítačové síti firmy. Zaměstnanci nesmí stahovat soubory z volně dostupných zdrojů v Internetu, včetně souborů získaných jako příloha v e-mail zprávě od osoby zvenčí nebo použít disk, disketu, flash memory, nebo jiné médium z jiného než firemního zdroje, aniž by nejdříve provedli detekci škodlivých kódů v těchto materiálech a to pomocí firmou schváleného antivirového programu. Pokud má zaměstnanec podezření na přítomnost viru na zařízení umístěném v interní síti, je povinen okamžitě nahlásit bezpečnostní incident na podpora@spolecnost.cz (viz. kapitola Bezpečnostní incidenty).

4.4 Soukromé aktivity na PS

Společnosti jsou oprávněny ke sledování materiálů, jež byly vytvořeny, uloženy, rozeslány, anebo sdíleny uživatelem prostřednictvím PS, dále k monitorování obsahu PS, stejně jako veškeré komunikace odeslané a přijaté prostřednictvím PS, není-li právními předpisy stanoveno jinak.

Výše uvedená práva jsou společnosti oprávněny použít v případě podezření na zneužívání PS, nedodržování interních směrnic, ale i v případě náhodných preventivních opatření. Společnost je oprávněna stanovit rozsah užívání PS ze strany zaměstnance i pro soukromé účely zaměstnance, kterému bylo PS přiděleno.

Soukromé aktivity na BYOD zařízení nepodléhají kontrole společnosti a společnost se distancuje od škod, které zaměstnanec soukromým používáním BYOD způsobí, a jejich následků.

5 Pravidla pro přístup do vnitřní sítě

Zaměstnancům je přístup do vnitřní sítě zřízen výhradně k pracovním účelům. Zaměstnanci jsou odpovědní za své chování ve vnitřní síti a nesou za něj plnou zodpovědnost.

5.1 Přístup do vnitřní sítě

Pro přístup do vnitřní sítě jsou zaměstnanci povinni používat pouze PS, které jsou v majetku společnosti XY. Použití jakýchkoliv jiných prostředků, které jsou v soukromém vlastnictví zaměstnance nebo jsou mu zapůjčeny třetí stranou, je možné pouze po konzultaci a se souhlasem ředitele společnosti XY a bezpečnostního manažera společnosti XY. Ostatní zařízení mohou být blokována pravidly identity managementu a bude na ně pohlíženo jako na zařízení externích pracovníků a hostů společnosti.

5.2 Vzdálený přístup do vnitřní sítě

Pro zřízení jiného druhu vzdáleného přístupu do vnitřní sítě než je uveden v této kapitole, je nutné mít tento druh přístupu schválený výkonným ředitelem. Vzdálený přístup do vnitřní sítě je zřízen výhradně přes webový server přístupný na adrese https://hlaseni. Zřízení přístupu provádí systémový administrátor, na základě požadavku.

Žádost o přístup zaměstnance do vnitřní sítě se řídí podle těchto kroků:

1. Nadřízený zaměstnance zadá požadavek, který musí obsahovat:
    1. Jméno uživatele a kontakt na uživatele, pro něhož je vzdálený přístup požadován
    2. Název společnosti, oddělení
    3. Důvod pro zřízení vzdáleného přístupu
    4. Systémy, do kterých potřebuje mít uživatel udělen přístup
2. Nadřízený zaměstnance zasílá požadavek na schválení výkonnému řediteli

3. Výkonný ředitel schválí/neschválí požadavek
4. Výkonný ředitel o rozhodnutí vyrozumí žadatele
5. V případě schválení požadavku výkonným ředitelem, nadřízený zaměstnance zadává schválený požadavek
6. Systémový administrátor nastaví přístup podle definovaného požadavku

6 Pravidla pro přístup externích uživatelů do vnitřní sítě

Externím uživatelem se rozumí osoba, která není zaměstnancem společnosti XY.

Externí uživatelé mohou být připojeni do vnitřní sítě pouze podle pravidel uvedených níže a za předpokladu, že je mezi tímto zaměstnancem a společností XY uzavřena písemná smlouva nebo jinak zajištěno dodržení standardů bezpečnosti dat v rozsahu této směrnice.

6.1 Přístup do vnitřní sítě

Externí uživatelé budou připojeni do vnitřní sítě pouze na základě požadavku zaslaného na podpora@spolecnost.cz . Požadavek zasílá člen vedení, který spolupracuje s externím uživatelem, spolu se zdůvodněním proč je nutné zřídit přístup pro externího uživatele do interní sítě. Dále je potřeba uvést:

- Důvod udělení přístupu
- Na jaké systémy žádá přístup
- Jaké porty je třeba povolit pro komunikaci
- Na jak dlouho požaduje přístup
- Z jakého místa žádá přístup do sítě

Zaměstnanci společnosti XY připraví datovou zásuvku pro připojení tohoto uživatele. Odpovědnost za jednání externího uživatele nese člen vedení, na základě jehož žádosti byl přístup do vnitřní sítě povolen.

6.2 Vzdálený přístup do vnitřní sítě

Vzdálený přístup do vnitřní sítě Společnosti je zřízen výhradně přes webový server přístupný na adrese https://hlaseni. Schválení zřízení vzdáleného přístupu do vnitřní sítě se musí řídit podle procesu popsaného v kapitole Vzdálený přístup do vnitřní sítě. Mimo body uvedené v této kapitole je nutné dále uvést:

- Jaké porty bude v komunikaci využívat
- Na jak dlouho požaduje přístup

Pro zřízení jiného druhu vzdáleného přístupu do vnitřní sítě než je uveden v této kapitole, je nutné mít tento druh přístupu schválený výkonným ředitelem.

6.3 Přístup k bezdrátové síti

Pro přístup k PS je možné použít bezdrátovou síť wi-fi, kterou jsou pokryty všechny prostory areálu.

K přístupu využijí hosté a externí pracovníci Guest portál společnosti XY, přičemž heslo pro přístup smí externímu uživateli předat jen osoba k tomu určená, což je buď administrátor sítě, jeho nadřízený nebo asistentka ředitele.

Přístup k bezdrátové síti opravňuje uživatele k využití internetové konektivity. V případě požadavku na připojení k uživatelské síti a sdílení zdrojů je možné použít pouze PS společnosti.

Zaměstnanci a externí pracovníci s oprávněním k přístupu ke zdrojům společnosti XY budou prostřednictvím Guest portálu připojeni k interním sítím automaticky ve kterékoliv lokalitě wi-fi sítí pokryté.

7 Politika přístupových práv

7.1 Doménoví administrátoři

Činnost doménových administrátorů vykonávají pouze zaměstnanci společnosti XY pracující v oddělení IT Servery. Přidání jiného uživatele do skupiny doménoví administrátoři je možné pouze s výjimkou, kterou uděluje výkonný ředitel společnosti XY. Tato výjimka se uděluje pouze v případě, kdy není možné využít jiné řešení. Výkonný ředitel společnosti XY musí před udělením této výjimky posoudit všechna bezpečnostní rizika spojená s tímto krokem. Udělená výjimka má pouze dočasný charakter, nezbytný k provedení prací nebo úkonů, k nimž jsou oprávnění nezbytná.

7.2 Udělování přístupových práv

Zaměstnanec při svém nástupu obdrží přihlašovací údaje ke svému účtu a přístupová práva k systémům pro svou pracovní činnost (viz. kapitola Nástup nového zaměstnance). Jestliže zaměstnanec potřebuje povolit přístup na některý ze systémů, které společnost využívá,

musí jeho nadřízený poslat požadavek na podpora@spolecnost.cz. Požadavek na změnu pravidel přístupů pro zaměstnance musí obsahovat:

- Jméno, Příjmení
- Název společnosti, oddělení
- Pracovní pozice
- Systémy, do kterých má mít zaměstnanec přístup
- Důvod pro zpřístupnění těchto systémů

Vedoucí pracovník je povinen projednat povolení přístupu k systému v rámci vedení společnosti, které si může vymínit povolení přístupu provedením bezpečnostní prověrky pracovníka.

Jestliže pomine důvod pro zpřístupnění některého ze systémů zaměstnanci, je jeho nadřízený povinen tuto skutečnost oznámit formou požadavku na odebrání přístupového oprávnění pro zaměstnance. Tento požadavek musí obsahovat:

- Jméno, Příjmení
- Název společnosti, oddělení
- Pracovní pozice
- Systémy, do kterých má být zaměstnanci odebrán přístup

8 Politika hesel

Zaměstnanci jsou plně zodpovědní za jim svěřené přístupové údaje do osobního účtu, systémů, aplikací. Jsou povinni své přihlašovací údaje zabezpečit proti vyzrazení, ztrátě, zcizení, či jinému zneužití. Z toho vyplývá, že zaměstnanci mají zakázáno:

- Vyzradit své přihlašovací údaje jiné osobě
- Nechat své přihlašovací údaje volně dostupné jiné osobě
- Opouštět pracoviště bez zabezpečení PC
    - Uzamknutí obrazovky
    - Odhlášení ze systému
    - Ukončení relace

Hesla a přihlašovací údaje uživatelů nesmí být uloženy v tištěné podobě a být volně přístupné. Administrace hesel musí být přístupná pouze stanovenému systémovému administrátorovi. Pro případ opomenutí uzamčení relace při odchodu od PS dojde po 30-ti minutách k jejímu vynucenému automatickému uzamčení.

8.1 Úroveň zabezpečení hesla

- Heslo musí obsahovat minimálně 8 znaků, povoleny jsou alfanumerické znaky, speciální znaky a je rozlišováno použití malých a velkých písmen
- Maximální stáří hesla je 6 měsíců
- Při změně hesla není povoleno použít žádné ze 4 předchozích hesel

8.2 Změna hesla

Zaměstnanec při svém nástupu obdrží přihlašovací údaje ke svému účtu. Maximální stáří hesla může být 6 měsíců. Poté bude heslo automaticky deaktivováno a přístup na účet zablokován.

Zaměstnanec je povinen změnit heslo:

- Při prvním přihlášení, vždy po obdržení dočasného hesla od systémového administrátora (je vyžadováno systémem, pokud si uživatel heslo nezmění, dojde k blokaci jeho účtu)
- Minimálně 1x za 6 měsíců (tento interval je vyžadován systémem, pokud si uživatel heslo nezmění, dojde k blokaci jeho účtu)
- V případě vygenerování nového hesla administrátorem
- V případě vyzrazení, či podezření na vyzrazení hesla
- pokud bylo heslo svěřeno jiné osobě v souvislosti se zásahem na uživatelském účtu, je uživatel povinen, po ukončení tohoto zásahu, své heslo neprodleně změnit

9 Bezpečnostní pravidla pro životní cyklus zaměstnance

Při nástupu je nový zaměstnanec povinen se seznámit s Bezpečnostní politikou a Bezpečnostní směrnicí a dalšími souvisejícími předpisy Společnosti, které jsou závazné

pro nadřízeného zaměstnance. Za seznámení zaměstnance s těmito předpisy je odpovědný nadřízený nastupujícího zaměstnance.

Předpisy se zabývají udělením/odebráním přístupu do vnitřní sítě Společnosti. Dále nastavením přístupů do systémů. Předpisy se zaměřují na tři varianty životního cyklu zaměstnance:

- Vznik pracovního poměru zaměstnance
- Ukončení pracovního poměru zaměstnance

10 Zabezpečení dat a osobních údajů:

Shromažďování a použití osobních údajů

Osobní údaje jsou údaje, které mohou být použity k osobní identifikaci nebo kontaktování konkrétní osoby. Osobní údaje, které Společnost shromažďuje, slouží výlučně pro potřebu společnosti a souvisejí s realizací jejího podnikání. Příslušný vedoucí pracovník je povinen před zpřístupněním osobních údajů zajistit proškolení jednotlivých zaměstnanců, kteří budou pracovat s osobními údaji o jejich povinnostech.

Shromažďování a použití jiných než osobních údajů

Shromažďujeme také údaje jiné než osobní povahy − data ve formě, která neumožňuje přímé spojení s jakoukoliv konkrétní osobou. Informace neosobní povahy můžeme shromažďovat, používat, předávat a sdělovat za jakýmkoliv účelem. Tímto shromažďováním dat neosobní povahy je možno chápat výkon jednotlivých provozů, zařízení, jejich energetickou náročnost a podobně. Tato data pak mohou být využívána v rámci optimalizace provozu a podnikání Společnosti např. formou souhrnných dat. Souhrnná data jsou pro účely tohoto Předpisu o ochraně osobních údajů považována za neosobní údaje.

Osobní údaje, které nejsou veřejně dostupné, bude společnost po celou dobu jejich uchování uchovávat plně v souladu se zákonem č. 101/2000 Sb. o ochraně osobních údajů. Za osobní údaj se považuje jakákoliv informace týkající se stanoveného subjektu informací. Subjekt informací se považuje za stanovený, jestliže lze subjekt informací přímo nebo nepřímo identifikovat zvláště na základě čísla, kódu nebo jedné či více složek, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

Pracovat s těmito daty mohou pouze osoby k tomu určené a v rozsahu nutném pro plnění jejich pracovních povinností. Každý z těchto pracovníků je povinen zajistit splnění zákonných regulativ a podmínek pro práci s těmito daty.

Pokud dojde ke zkombinování neosobních údajů s osobními údaji, budou výsledné sloučené informace považovány za osobní údaje po celou dobu trvání takového sloučení.

Sdělování údajů třetím stranám

Zaměstnanci nejsou oprávnění poskytnout jakékoliv osobní či neosobní údaje ostatních zaměstnanců či klientů/zákazníků třetím osobám mimo Společnost, pokud se tak neděje v rámci plnění pracovních úkolů na straně zaměstnance. V případě uplatnění vzniku jakéhokoliv nároku třetí strany (pokuta, náhrada škody či jiné újmy), je výkonný ředitel Společnosti oprávněn rozhodnout o dočasném odejmutí přístupových práv k IS příslušného zaměstnance včetně rozsahu a doby trvání tohoto odejmutí práv.

Uložení a ochrana údajů

Společnost činí opatření, včetně administrativních, technických a fyzických, k tomu, aby vaše osobní a jiné údaje ochránila před ztrátou, krádeží a zneužitím i před neoprávněným přístupem, sdělením, úpravou a zničením.

Společnost ve spolupráci s bezpečnostním manažerem stanoví vhodné umístnění úložiště osobních a údajů, jakož i dalších informací včetně stanovení lhůt archivace jednotlivých dokumentů v závislosti na trvání obchodních vztahů, jakož i dle zákonných regulativ pro jednotlivé druhy dokumentů. Údaje a informace které nespadají do některé z kategorií dokumentů a informací k archivaci je nutno skartovat či jinak odstranit. Vedení společnosti je oprávněno stanovit osobu ke kontrole plnění této povinnosti.

Jiné

Společnost může být povinna poskytnout osobní a jiné údaje, ať již ze zákona, v rámci soudního řízení, sporu a/nebo na žádost státních orgánů a úřadů. Údaje může společnost také poskytnout v případě, že se bude důvodně domnívat, že jejich sdělení je nutné k vymáhání plnění z titulu smlouvy, jakož i pohledávek apod. či k ochraně provozní činnosti nebo partnerů Společnosti.

Ve vztahu k archivaci dat a dokumentů jakož i k jejich skartaci bude tato otázka upravena samostatnou směrnicí o archivaci a skartaci.

11 Závěrečná ustanovení

V případě nedodržení pravidel uvedených v jednotlivých kapitolách tohoto dokumentu, mohou být zaměstnanci odebrány přístupy na osobní účet, do systémů, do sítě apod.

V případě závažných porušení pravidel jsou tato považována za porušování pracovních povinností a vůči zaměstnanci mohou být vyvozeny pracovněprávní důsledky.

Proškolení zaměstnanců společnosti o obsahu této směrnice zajistí vedení společnosti XY.