Implementace systému řízení bezpečnosti informací ve výrobním podniku dle ČSN ISO/IEC 27001

Bc. Jitka Mičulková

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

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

Jméno a příjmení:	**Bc. Jitka Mičulková**
Osobní číslo:	**A16238**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Implementace systému řízení bezpečnosti informací ve výrobním podniku dle ČSN ISO/IEC 27001**
Téma anglicky:	**The Implementation of an Information Security Management System in a Production Enterprise According to ČSN ISO / IEC 27001 Norms**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na téma řízení bezpečnosti informací.**
2. **Popište systém managementu bezpečnosti informací.**
3. **Analyzujte současný stav řízení bezpečnosti informací v podniku.**
4. **Navrhněte optimalizaci procesů řízení bezpečnosti informací za účelem zvýšení bezpečnosti podniku a proveďte diskuzi nad tímto výstupem.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.**
2. **DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.**
3. **NENADÁL, Jaroslav. Moderní management jakosti: principy, postupy, metody. Praha: Management Press, 2008. ISBN 978-80-7261186-7.**
4. **DRASTICH, Martin. Systém managementu bezpečnosti informací. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9.**
5. **ČSN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.**

Vedoucí diplomové práce: **doc. Ing. Jiří Gajdošík, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. prosince 2017**

Termín odevzdání diplomové práce: **28. května 2018**

Ve Zlíně dne 8. prosince 2017

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové 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 diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové 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 diplomové práci pracovala samostatně a použitou literaturu jsem citovala. V případě publikace výsledků budu uvedena jako spoluautorka.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 14. 5. 2018

.....
podpis diplomanta

ABSTRAKT

Diplomová práce se zaměřuje na návrh zavedení systému řízení bezpečnosti informací ve výrobním podniku. V teoretické části jsou definovány základní teoretické poznatky a pojmy z bezpečnosti informační bezpečnosti.

Praktická část řeší analýzu a zhodnocení současného stavu bezpečnosti. Vlastní návrh řešení obsahuje analýzu rizik, návrh opatření pro zvládání rizik a ekonomické zhodnocení.

Klíčová slova:

informační bezpečnost, aktivum, hrozba, zranitelnost, riziko, analýza rizik, bezpečnostní opatření

ABSTRACT

The master's thesis is aimed at proposing an implementation of an information security management system in a company. The theoretical section defines a basic theoretical background and concepts of information security.

The practical section deals with the analysis and assessment of the current security situation in the company. The solution proposal contains the risk analysis, the proposal of security measures for risk treatment and economic evaluation.

Keywords:

information security, asset, threat, vulnerability, risk, risk analysis, security measures

Děkuji vedoucímu diplomové práce panu doc. Ing. Jiří Gajdošík, CSc. za cenné rady a inspirativní podněty a konzultace.

Děkuji rodině za veškerou podporu a trpělivost během mého studia.

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

OBSAH

ÚVOD

Účelem této diplomové práce je definice a implementace systému managementu bezpečnosti ve výrobním podniku, určení jednotlivých oblastí, ve kterých je nutné aplikovat procesy bezpečnosti s cílem efektivně zajistit bezpečnost zvolených oblastí a dosáhnout trvalé pozice důvěryhodného obchodního partnera na tuzemských i zahraničních trzích.

Cílem je zvýšení bezpečnosti informací, ve smyslu zvýšení míry dostupnosti a důvěrnosti informací (optimalizace ICT procesů, předcházení bezpečnostním incidentům, zvýšení kredibility vůči partnerům) a splnění požadavků relevantní legislativy.

V analýze současného stavu přiblížím společnost, pro kterou návrh zavedení bezpečnostních opatření zpracovávám, analyzuji současný stav bezpečnosti a kriticky jej zhodnotím.

Vypracuji analýzu rizik a navrhnu opatření pro jejich zvládání. Navržená bezpečnostní opatření detailně popíšu a nastíním jejich implementaci. Odhadnu časovou náročnost a náklady na implementaci jednotlivých opatření.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST INFORMACÍ

Problematika informační bezpečnosti je velmi široká, zahrnuje všechny faktory, které se podílejí na zabránění přístupu k citlivým informacím nepovolaným osobám. Samotné informace musí být chráněny proti zneužití ve všech etapách jejich zpracování. Zároveň musí být také zabezpečena jejich dostupnost.

Do informační bezpečnosti patří nejen problematika datových přenosů, ochrana sítí, propojení, ale také například fyzická ochrana budov, pravidelné školení a analýza rizik.

Řešení informační bezpečnosti na obecné úrovni je rozsáhlá záležitost. Každá organizace má odlišný soubor požadavků na bezpečnostní opatření, který se odvíjí od úrovně důvěrnosti informací, nároků na integritu a dostupnost.

Informační bezpečnost není pouze interní věcí podniku, ale v době elektronických komunikací, také věcí mezi podnikem a státní správou. Informační bezpečnost podniku také dopadá na jeho obchodní partnery. Je proto běžné, že se požaduje v rámci dobrých obchodních vztahů, aby si obchodní partneři navzájem demonstrovali, jaké mechanismy používají k zabezpečení informací a informačních systémů. Společnosti toto řeší zavedením bezpečnostních standardů a některé i certifikací. [11]

Co bezpečnost informací přináší?

- Ochrana existujících dat proti ztrátě, zničení nebo zneužití;
- Výchova personálu k šetrnému zacházení s daty;
- Optimalizace sběru, přenosu a ochrany dat;
- Zvýšení povědomí a zlepšení řídících mechanizmů;
- Zajištění shody s právními předpisy.

Bezpečnost informací ochraňuje informace před širokou škálou hrozeb pro zachování kontinuity podnikání, minimalizuje pravděpodobnost poškození podniku a maximalizuje návratnost investic a podnikatelských příležitostí.

1.1 Informace

Informace je význam přisouzený datům. Jsou to sdělení (zpracovaná do podoby užitečné pro příjemce), z nichž se dovídáme něco nového, a tím dochází ke snižování dosavadní neurčitosti, o nějakém jevu nebo události. Každá informace je tedy datem, ale naopak neplatí, že jakákoliv data jsou zároveň informacemi. Těmito se stávají až v okamžiku, kdy příjemci přinesou nějaké poznání. [11]

Záleží také na aktuálnosti informace. Každá informace je aktuální a užitečná pouze po určitý časový úsek, prochází životním cyklem.

Termín informace není synonymum termínu data. Data jsou vyjádření události formálním způsobem, v odpovídajícím syntaxu. Rozdíl oproti informaci je ten, že označujeme informace jako užší množinu dat, které je přiřazen význam. [10] Z toho vyplývá, že informací se data stávají až v procesu interpretace.

Životní cyklus informace

Obrázek č. 1 znázorňuje životní cyklus informace. Informace vznikne v určitém bodě na časové ose, po které se pohybuje až po svůj zánik. V tomto časovém období prochází různými změnami. Jsou modifikovány, aby si zachovaly nebo zvýšili svou užitečnost, jsou předávány jiným uživatelům, nebo jsou určeny pouze ke čtení a jejich podoba zůstává neměnná. Variant je spousta, ale společné mají tyto aktivity to, že musejí být informace někde uloženy.

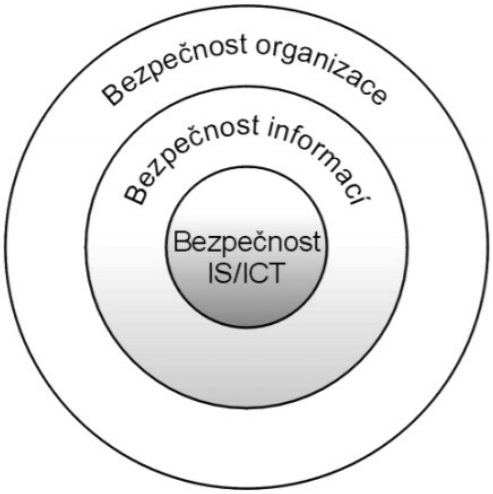
Obr. 1 Životní cyklus informace [15]

Informace je potřeba chránit v úložišti, při přenosu a během uživatelské manipulace. Tyto aktivity se provádí za účelem zajištění a zachování jejich dostupnosti, důvěryhodnosti a integrity. Důležitá je také likvidace informací, kdy se snažíme, aby již s daty nebylo možné, jakkoliv nakládat. Jejich zneužitím by mohlo dojít ke způsobení újmy vlastníkovi např. prozrazení know-how, obchodních informací, získání kontaktů na zákazníky.

1.2 Bezpečnost

Bezpečnost je důležitý pojem bezpečnostní terminologie. Ve slovníku je bezpečnost vymezena u přídavného jména „bezpečný“; a jako synonymum se uvádí slovo jistota. Bezpečný je ten, kdo není vystaven nebezpečí („být bezpečný před zloději“), popř. poskytuje ochranu před nebezpečím („bezpečný úkryt“) nebo je nepochybný, zaručený, důvěryhodný („bezpečný pramen informací“). [9]

V pojetí bezpečnosti podniku (organizace) existuje vzájemný vztah mezi bezpečnosti informací a bezpečnosti IS/ICT. Všechny kategorie bezpečnosti jsou vzájemně propojeny. Následující obrázek znázorňuje vztah těchto tří úrovní bezpečnosti.



Obr. 2 Vztah úrovní bezpečnosti [2]

Bezpečnost organizace

Bezpečnost organizace je na nejvyšší úrovni bezpečnosti. Spadá tady zajištění bezpečnosti objektu nebo majetek organizace. [2]

Klíčové okruhy řízení bezpečnosti v organizacích jsou fyzická bezpečnost (majetku, osobní), informační bezpečnost, ICT bezpečnost, bezpečnost práce a ochrana zdraví, forenzní audit apod.

Zároveň může pomoct ostatním úrovním jako například bezpečnosti IS/ICT tím, že se bude kontrolovat fyzický přístup do objektu/budovy. [2]

Bezpečnost informací

Bezpečností v tomto smyslu je myšleno ochrana informačních systémů a informací, které jsou uloženy, zpracovávány a transportovány. Shrnuje zásady bezpečnosti práce s informacemi, způsob zpracování dat, ukládání a uchovávání, skartace aj. Obsahuje proces ochrany důvěrnosti, integrity a dostupnosti.

Důvěrnost – informační aktivum není dostupné nepovolaným osobám nebo procesům, zajištění přístupu k informacím pouze autorizovaným jedincům a procesům, tedy poskytnutí přístupu k informaci pouze oprávněné osobě. V praxi, zejména ve větších organizacích, není snadné bez řízení oprávnění přístupu k datům toto zajistit. Společnost pracuje s daty různé úrovně důležitosti a každý pracovník má mít přístup pouze k těm informacím, které potřebuje ke své pracovní činnosti. Je nutné definovat skupiny a přiřadit k nim data dle důležitosti. Skupiny musejí být přehledné a srozumitelné tak, aby přiřazení informace do určité skupiny bylo jednoznačné pro všechny.

Integrita – znamená ochranu, zajištění správnosti, přesnosti a úplnosti informací. Informační aktivum nemůže být při zachování integrity neoprávněné modifikováno. Neúmyslné narušení původního stavu dat má na svědomí většinou nějaká technická závada. Úmyslné narušení nebo modifikaci dat má naopak na svědomí cílený útok se záměrem poškodit hodnotu informace. Vždy je důležité včas rozpoznat narušení integrity.

Dostupnost – představuje poskytování informací a přístup k informacím všem oprávněným uživatelům v okamžiku, kdy je potřebují. Narušení dostupnosti mohou způsobit různé druhy incidentů, jako jsou porucha HW, OS, aplikace, problém v komunikační síti, fyzický útok na systém apod.

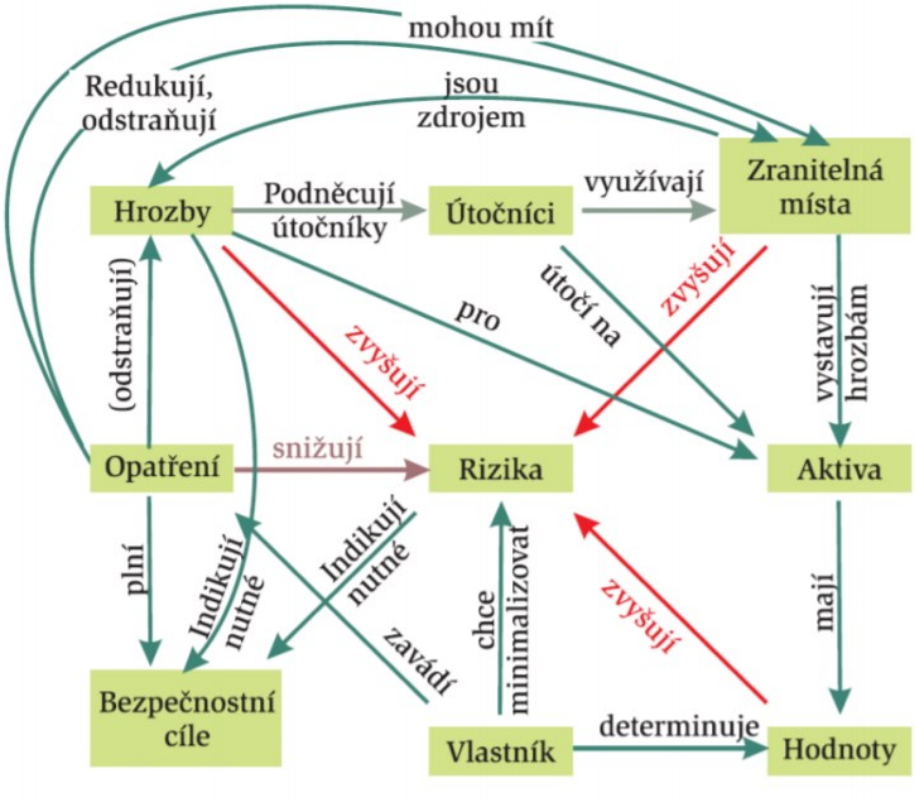
Bezpečnost IS/ICT

Bezpečnost IS/ICT je již konkrétní ochrana aktiv, která jsou součástí informačního systému podniku. [2] Dlouhodobá nedostupnost služeb způsobuje značné problémy.

Bezpečnost informačních technologií je nikdy nekončící proces, jehož hlavním cílem je neustále se zlepšovat, reagovat a řešit nově vzniklá rizika. Hlavním požadavkem je vybudování

sítí a zajištění jejich funkčního chodu. Informační bezpečnost se v současnosti patří mezi stěžejní body v budování ICT struktur.

Následující obrázek znázorňuje obecný model bezpečnosti, jeho hlavní prvky a vztahy mezi nimi.



Obr. 3 Obecný model bezpečnosti [13]

Aktiva, hodnoty organizace jsou vystavena hrozbám (vnější, vnitřní), které se snaží využít zranitelnosti organizace a překonat bezpečnostní opatření. Působí na aktiva a způsobují škody. Riziko vzniká vzájemným působením hrozby a aktiva a můžeme ho chápat jako kvantifikaci působení hrozby na aktivum. [7]

2 ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Bezpečnost informačních systémů by měla být základem v podnicích, kde se používají informační systémy. Řízení bezpečnosti informací musí zajistit ochranu aktiv před hrozbami ať již vnějšími nebo vnitřními s minimálními náklady.

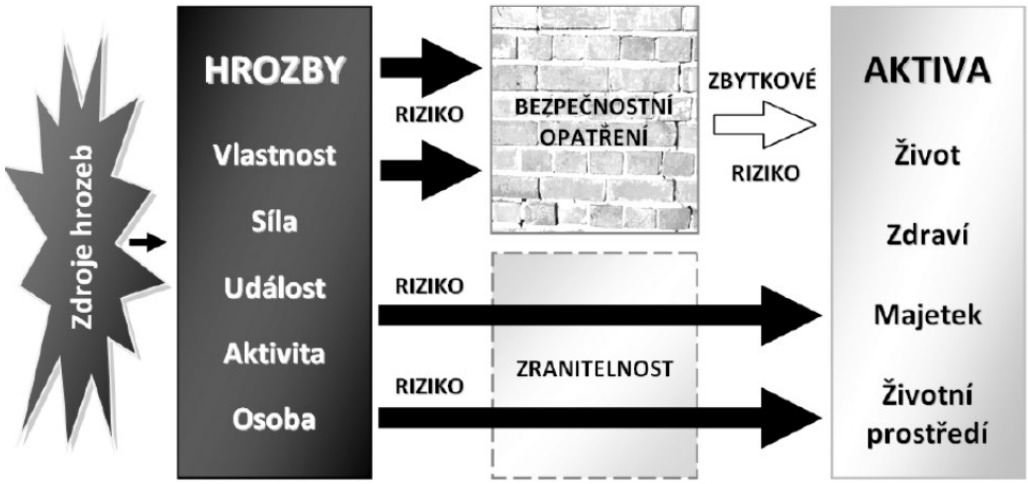
2.1 Pojmy z oblasti bezpečnosti informací

Aktivum – je vše, co má pro daný podnik nějakou hodnotu, která může být snížena působením hrozby.

Hrozba – je nějaká skutečnost, síla, událost nebo osoba, která působí na aktivum s cílem ho ovládnout, získat ho. Hrozby mohou být vnější (politické, ekonomické, sociální, technologické, legislativní, ekologické) nebo vnitřní (procesní, personální, věcné – mechanické).

Riziko – vzniká působením hrozby na aktiva. Je to možnost, že i při zajišťování činnosti podniku s nějakou pravděpodobností může nastat nějaká událost s nežádoucími dopady na plnění cílů podniku. [7]

Zranitelnost – je nějaký nedostatek, slabina nebo stav aktiva, které může hrozba zneužít pro uplatnění nežádoucího vlivu.



Obr. 4 Vztah mezi základními termíny v oblasti řízení rizik [7]

2.2 ISMS

Rozvoj počítačových technologií a informačních systémů s sebou přináší zavedení ochrany dat a účinného systému managementu informací. Management bezpečnosti informací je především určen pro organizace, které pracují s informacemi. Cílem je zamezit jejich ztrátě,

odcizení nebo zneužití. Zejména se zaměřuje na ochranu osobních údajů, firemních údajů, dat zákazníků a dodavatelů, know-how.

Systém managementu bezpečnosti informací ISMS (Information Security Management System) je část celkového systému řízení organizace, založená na přístupu k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání údržbu a zlepšování bezpečnosti informací. Řízení ISMS je založeno na modelu PDCA. [2]

ISMS je soubor pravidel a opatření, po jejichž zavedení má správné a úplné informace (princip integrity) včas k dispozici ten, kdo je skutečně potřebuje (princip dostupnosti) a pouze ten, kdo je k přístupu k nim oprávněn (princip důvěrnosti).

Pro ISMS v rámci podniku musí být jednoznačně popsána organizace řízení, odpovědnost za informační bezpečnost řídících pracovníků všech stupňů, odborných orgánů a rolí v systému bezpečnosti informací.

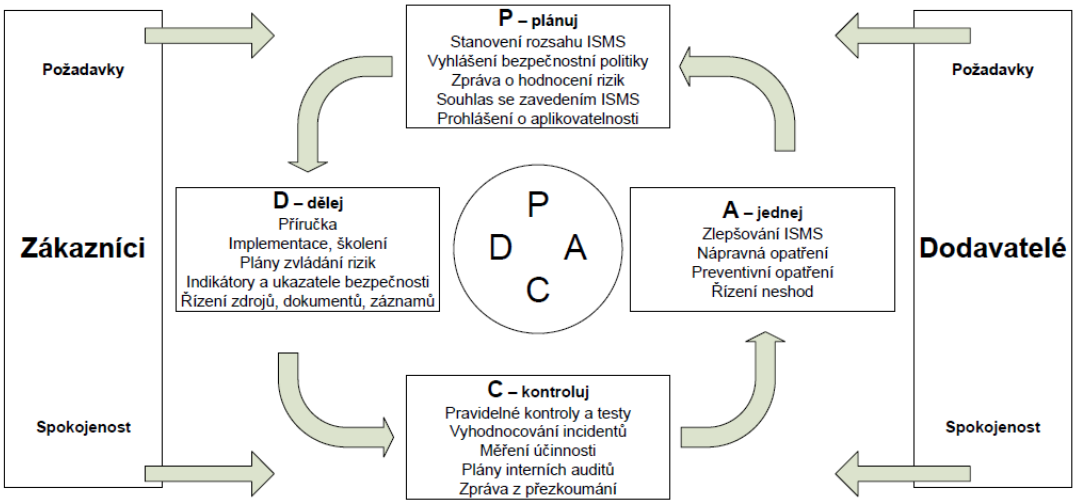
Certifikace systému managementu bezpečnosti informací

Certifikace dle normy ČSN ISO/IEC 27001 prosazuje přijetí procesního přístupu pro ustanovení, zavádění, provozování, monitorování, udržování a zlepšování ISMS v organizaci.

Certifikace je aplikovatelná v jakékoliv organizaci. Podle ní se posuzuje systém informační bezpečnosti. Certifikace přináší společnostem konkurenční výhodu.

2.3 PDCA model

Informační bezpečnost musí být řízena a je jedno, zda se jedná o firmu s 20 nebo s 1000 zaměstnanci. Rozdílné mohou být pouze časové lhůty, množství práce a výklady jednotlivých doporučení a postupů, jak toho dosáhnout. Principem celého ISMS je tzv. PDCA model. Tento model zavádí souvislý systém řízení bezpečnosti informací v podniku. Jeho jednotlivé kroky (Plan, Do, Check a Act) zaručují, že zavedení systému nebude jen jednorázovou aktivitou, ale neustálým koloběhem. Norma ISO/IEC 27001 jasně popisuje, postup při zavádění ISMS a nařizuje, kterých cílů a bezpečnostních opatření musí být dosaženo.



Obr. 5 Model PDCA [4]

Plánuj – Plan – Ustanovení ISMS

V prvním kroku je nutné získat souhlas vedení společnosti s nasazením systému. Norma tento souhlas požaduje a zavádění ISMS musí být prováděno směrem od vrchu dolů. Podnik musí dále:

- Stanovit hranice a rozsah ISMS dle činnosti svého podnikání, stanovit politiku ISMS, její cíle, stanovit kritéria pro hodnocení rizik;
  Definice rozsahu ISMS - V této části se určí rozsah a hranice, ve kterých je ISMS uplatňováno. Nejprve je potřeba získat dostatek informací, nebo provést úvodní analýzu, ze které vyplyne, které části organizace je nutno chránit. ISMS nemusí vždy pokrývat celou organizaci;
  Definice politiky ISMS - Dalším krokem je stanovení politiky ISMS. Jde o krátký, ale důležitý dokument, který prezentuje zájem vedení organizace o řízení bezpečnosti informací a definuje klíčové zásady bezpečnosti. Dokument musí být schválen vedením a také s ním musí být seznámeni všichni zaměstnanci. Bez podpory vedení není implementace, provoz a údržba ISMS reálná; [12]
- Stanovit systematický přístup k hodnocení rizik, metodiku hodnocení rizik, zajistit porovnatelnost a reprodukovatelnost výsledků hodnocení;
- Identifikovat rizika aktiv, hrozby pro tyto aktiva, zranitelnosti, které by mohly být hrozbami využity, dopady na aktiva;

- Analyzovat a vyhodnocovat rizika, posoudit dopady na činnosti podniku při selhání bezpečnosti, pravděpodobnost selhání, analyzovat zranitelnost, odhadnout úrovně rizika;
- Postupy pro řízení rizik;
  Řízení rizik je základem každého systému řízení bezpečnosti informací a podstatným způsobem ovlivňuje efektivitu fungování celého ISMS. Nezbytnými kroky pro systematické řízení rizik je výběr vhodné metody hodnocení rizik, provedení analýzy rizik a návrh způsobů řízení rizik;
- Souhlas vedení organizace s opatřeními a zbytkovými riziky;
  V této části vedení odsouhlasí navrhnutá opatření pro snižování rizik a přebírá na sebe zodpovědnost za zbytková rizika. Pokud k souhlasu nedojde, je potřeba opatření upravit;
- Prohlášení o aplikovatelnosti;
  Je důležitý dokument, který zdůvodňuje výběr jednotlivých opatření a zachycuje matici vztahů mezi hrozbami a jednotlivými opatřeními navrhnutými pro jejich účinné a efektivní snižování. Je z něj jasně patrné, která opatření budou v dané organizaci přijata, a která ne.

Dělej – Do – Zavádění a provoz ISMS

Cílem je systematické zavádění bezpečnostních opatření do chodu podniku. Určit a zavést plán zvládání rizik, určit priority a odpovědnosti, zavést bezpečnostní opatření a metodiku měření jejich účinností.

- Plán zvládání rizik;

Tento dokument popisuje veškeré činnosti spojené s ISMS jejich potřebné zdroje. Jednoznačně určuje osobní odpovědnosti za provádění plánovaných činností. Východiskem pro tento plán jsou především výsledky řízení rizik a podněty získané pravidelným vyhodnocováním stavu ISMS vedením organizace. Plán zvládání rizik obsahuje výčet činností, aktivit a projektů vedoucích k potřebnému snižování bezpečnostních rizik.

- Příručka bezpečnosti informací;

Příručka bezpečnosti slouží k podpoře prosazování ISMS a definuje dílčí procesy i postupy, které zajišťují efektivní prosazení bezpečnostních opatření.

Tato příručka patří mezi důležité dokumenty pro úspěšné nastavení, provoz a zlepšování ISMS v podniku. Patří sem definice rozsahu ISMS, politika ISMS, hodnocení rizik a zvládání rizik.

Dále zde řadíme dokumentaci sloužící jako podpora ISMS, která je přizpůsobená potřebě konkrétní organizace. Tento dokument se nazývá příručka bezpečnosti informací a definuje dílčí procesy a postupy k zajištění jednotlivých bezpečnostních opatření.

Na nejnižší úrovni bezpečnostní dokumentace jsou pracovní příručky. Tato dokumentace není povinná lze ji nahradit konkrétní dokumentací patřící k příslušným systémům.

Struktura příručky bezpečnosti informací vychází z normy ISO/IEC 27001 a její struktura je následující:

- Předmět normy;
- Normativní odkazy;
- Termíny a definice;
- Systém managementu bezpečnosti informací;
- Odpovědnost vedení;
- Interní audit ISMS;
- Přezkoumání ISMS vedením organizace;
- Zlepšování ISMS;
- Prohlubování bezpečnostního povědomí zaměstnanců. [5]

Je potřeba zajistit promítnutí všech definovaných pravidel a postupů do skutečného chování odpovědných pracovníků a uživatelů. Je nutné jim srozumitelně vysvětlit bezpečnostní principy a pravidla a seznámit je s bezpečnostními riziky tak, aby byli schopni správně reagovat na nenadálé situace a hrozby. Tak je možné zajistit větší odolnost nejslabšího článku v řetězci ISMS, kterým je vždy lidský faktor.

- Měření provozu ISMS (indikátory a metriky prokazující účinnost ISMS);

Zavádí pravidelné sledování objektivních údajů o skutečném fungování systému řízení bezpečnosti. Využívá se k tomu sada ukazatelů pro oblasti finanční, personální a technické;

- Řízení zdrojů, dokumentace a záznamů ISMS;

Tento krok vyžaduje provádění všech činností řízeným a dokumentovaným způsobem. Je nutné shromažďovat podklady pro další fázi, tedy monitorování. Cílem je vytvořit pravidla pro tvorbu, schvalování a aktualizaci dokumentace řízení bezpečnosti. Současně je důležité vytvářet záznamy o všech provedených úkonech včetně identifikace osoby, která úkon provedla, kdy a kde byl realizován;

Z pohledu zdrojů je potřeba sledovat, zda potřeby ISMS pokrývá odpovídající množství lidských, finančních a technologických zdrojů a účelně tyto zdroje řídit.

Kontroluj – Check – Monitorování a přezkoumání ISMS

Hlavním cílem tohoto kroku je zajištění monitorování a přezkoumávání ISMS. Podnik musí zavést následující doporučení:

- Zavést opatření pro včasnou detekci chyb – detekce bezpečnostních incidentů, vyhodnocování účinnosti opatřeních při narušení, měřit jejich účinnost, pravidelně přezkoumávat účinnost ISMS;
- Monitorování a provádění kontrol;
  Tento krok zahrnuje vykonávání nezbytných kontrol a testů, které poskytují zpětnou vazbu, nezbytnou pro fungování ISMS. Je potřeba dohlížet na to, zda bezpečnostní opatření naplňují očekávání, která do nich byla při zavádění vkládána. Součástí je také detekce chyb a zaznamenávání úspěšných i neúspěšných pokusů o narušení bezpečnosti. Výsledky těchto měření jsou podnětem pro přehodnocení výsledků hodnocení rizik;
- Interní audity ISMS;
  Zajišťují nezávislý pohled na fungování ISMS a jsou důležitou zpětnou vazbou;
- Přezkoumání ISMS vedením;
  Podněty a připomínky k fungování ISMS získané během jeho monitorování slouží pro přezkoumání ISMS vedením organizace. Výstupem bývá zpráva o stavu ISMS, která shrnuje, co v systému funguje dobře a je možné se o tyto části opírat, a zároveň rozebere skutečnosti, které optimálně nefungují a je nutné se na ně zaměřit.

Jednej – Act – Údržba a zlepšování

Poslední etapa zahrnuje realizaci možností udržování a zlepšování ISMS a odstraňování nedostatků.

- Soustavné zlepšování ISMS;

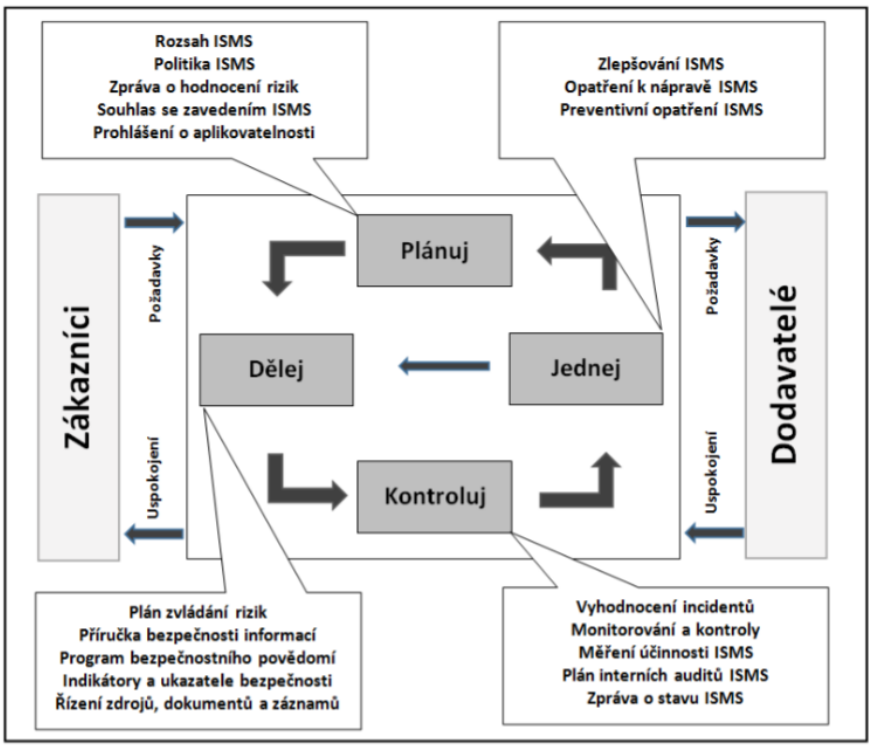
Důležitým prvkem zlepšování je využití zpětné vazby a zkušenosti účastníků tohoto procesu. Zjištění přicházející z praxe jsou přínosné a je potřeba je analyzovat a následně po zvážení jejich dopadů na organizaci zapracovat do systému řízení bezpečnosti.

- Odstraňování neshod ISMS;

Do tohoto kroku patří opatření k nápravě, které je reakcí na řešení nedostatků ISMS, kdy se nedostatek již projevil a je potřeba na něj vhodným způsobem reagovat a také preventivní opatření, které umožňuje zabránit případnému vzniku nedostatků, které by mohly mít vliv na ISMS.

Podnik by měl provádět:

- Preventivní a nápravnou činnost;
- Analyzovat návrhy na zlepšení;
- Navrhovat postupy pro zlepšení. [4]



Obr. 6 Model PDCA pro řízení bezpečnosti informací [2]

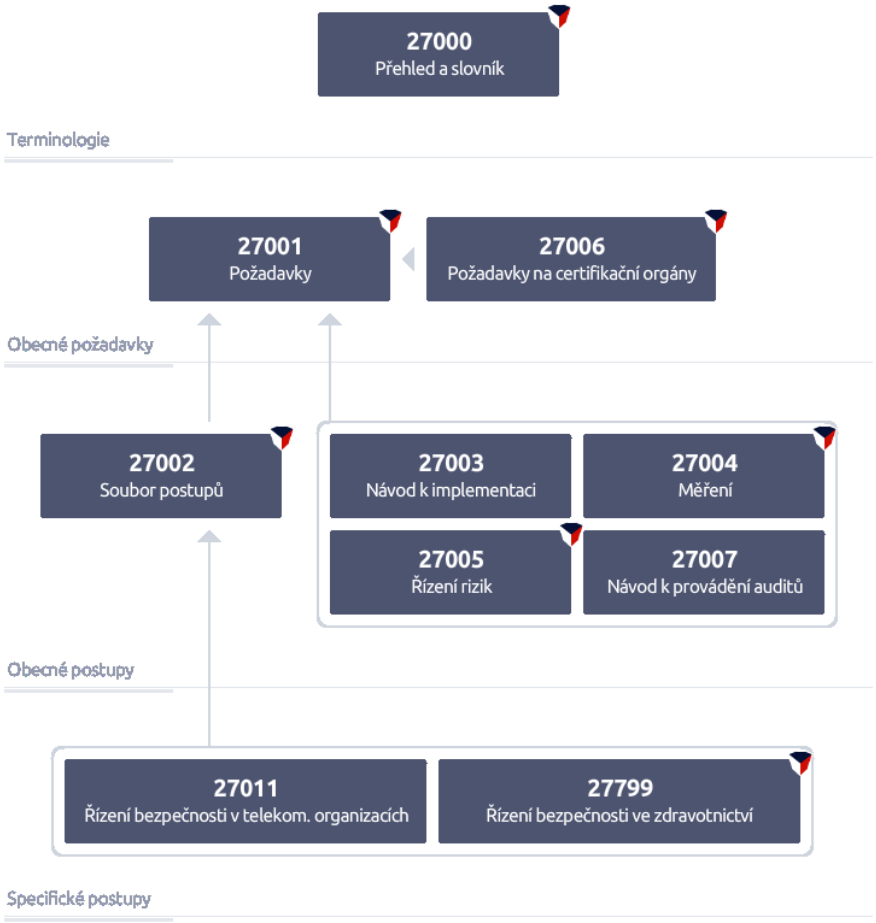
3 ZÁKONY A NORMY V OBLASTI BEZPEČNOSTI IT

3.1 Sada norem řady ISO/IEC 27000

Tyto normy jsou zaměřeny na faktory dostupnosti, důvěrnosti a integrity informací a informačních systémů v podniku. Normy se snaží komplexně řešit obranu proti možným hrozbám a nebezpečím, které byly v podniku identifikovány, oceněny a mohou mít dopady na aktiva podniku. Tvůrcem těchto norem je mezinárodní organizace pro standardizaci. Z hlediska řízení informační bezpečnosti je tato řada norem zásadní. Důvodem je jejich univerzalita, rozšířenost a přímá specializace na ISMS.

ISO/IEC 27000

Definuje a zavádí pojmy a terminologický slovník pro všechny ostatní normy z této řady.



Obr. 7 Řada norem ISO 27000 [5], upravila Mičulková 2018

ISO/IEC 27001

Toto je hlavní norma pro ISMS podle ní jsou systémy certifikovány. Systém řízení informační bezpečnosti je sada pravidel zabývajících se řízením informační bezpečnostní politiky nebo rizik souvisejících s IT a je definována v rámci této normy.

Rozvoj ISMS na základě normy zahrnuje následujících šest kroků:

- Definice bezpečnostní politiky;
- Definice ISMS rozsahu;
- Posouzení rizik;
- Řízení rizik;
- Výběr vhodných kontrol;
- Prohlášení o aplikovatelnosti.

ISO/IEC 27002

Obsahuje přehled nejdůležitějších bezpečnostních postupů a opatření, které jsou vhodné pro bezpečnost informací v podniku provést. Hlavní oblasti jsou:

- Bezpečnostní politika;
- Organizace bezpečnosti;
- Klasifikace a řízení aktiv;
- Bezpečnost lidských zdrojů;
- Fyzická bezpečnost a bezpečnost prostředí;
- Řízení komunikací a provozu;
- Řízení přístupu;
- Akvizice, vývoj a údržba IS;
- Zvládání bezpečnostních incidentů;
- Řízení kontinuity činnosti organizace;
- Soulad s požadavky.

ISO/IEC 27003

Poskytuje návody, podporu a doporučení pro implementaci ISMS.

ISO/IEC 27004

Obsahuje přehled měření a metrik k provádění pravidelných přezkumů účinnosti ISMS a měření účinnosti zavedených opatření za účelem ověření, zda jsou definované bezpečnostní požadavky v organizaci naplněny.

ISO/IEC 27005

Doporučení pro oblast řízení rizik v oboru bezpečnosti informací.

3.2 Zákony a nařízení

Některé zákony související s oblastí řízení bezpečnosti informací v podniku:

- zákon č. 101/2000 Sb., o ochraně osobních údajů;
- Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů;
- zákon č. 148/1998 Sb., o ochraně utajovaných skutečností;
- zákon č. 480/2004 Sb., o některých službách informační společnosti;
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti;
- Zákon č. 227/2000 Sb., o elektronickém podpisu;
- Zákon č. 513/1991 Sb., Obchodní zákoník;
- Zákon č. 240/2000 Sb., o krizovém řízení;
- Zákon č. 181/2014 Sb. o kybernetické bezpečnosti.

3.2.1 Obecné nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů (anglicky General Data Protection Regulation) nabývá účinnosti dne 25. května 2018 a platí pro všechny organizace nabízející zboží nebo služby v rámci EU a manipulující s osobními údaji subjektů (fyzických osob). Jedná se o účinné nařízení EU, což znamená, že má přednost před národní legislativou. Osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity

této fyzické osoby. [17] Obecné nařízení o ochraně osobních údajů ukládá správcům osobních údajů např.:

- povinnost zabezpečit zpracování osobních údajů;
- povinnost provádět posouzení vlivu na ochranu osobních údajů;
- povinnost ohlašovat porušení zabezpečení osobních údajů;
- povinnost jmenovat pověřence pro ochranu osobních údajů;
- povinnost vést záznamy o činnostech zpracování osobních údajů (včetně povinnosti zaznamenávat i přístupy ke čtení osobních údajů). [17]

Subjekt údajů (fyzická osoba) má dle tohoto nařízení např.:

- právo na přístup k osobním údajům;
- právo na opravu nebo výmaz („právo být zapomenut“);
- právo na omezení zpracování;
- právo na přenositelnost údajů;
- právo vznést námitku. [17]

4 ŘÍZENÍ RIZIK

Řízení rizik je jedním ze základních manažerských nástrojů efektivního systému řízení společnosti, jehož cílem je podpora při naplňování vize a strategie společnosti. Řízení rizik je koncipováno v souladu s nejlepší mezinárodní praxí v oblasti řízení a správy společnosti jako proaktivní, dynamický a sebezdokonalující se systém, který je primárně zaměřen na eliminaci nebo snížení negativních dopadů rizik působících vně i uvnitř společnosti a na maximální využívání pozitivních dopadů rizik pro společnost. Řízení rizik je nedílnou součástí strategického řízení společnosti.

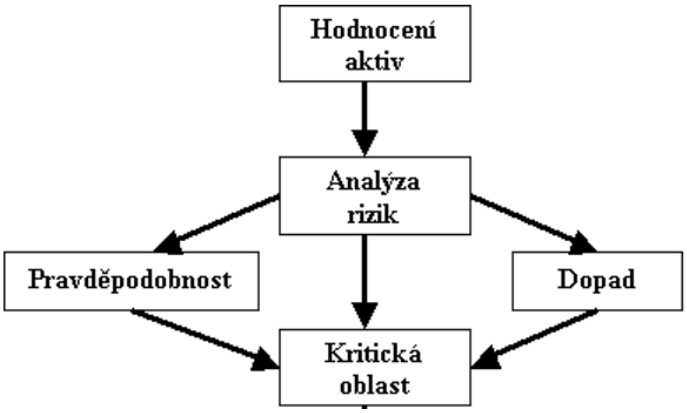
Efektivní řízení rizik se týká každého zaměstnance společnosti.

4.1 Analýza rizik

Analýza rizik slouží k stanovení míry rizika. Na základě ohodnocení aktiv analyzujeme hrozby, u kterých stanovíme míru pravděpodobnosti výskytu. Výsledkem analýzy rizik, je tedy seznam hrozeb. Pro hrozby, které jsou pro podnik nebezpečné, se navrhuje bezpečnostní opatření, které zvyšuje míru bezpečnosti aktiva.

Analýza rizik IS je klíčovou aktivitou v procesu řešení bezpečnosti, která musí poskytnout odpověď na následující tři otázky:

- Co se stane, když nebudou informace chráněny?
- Jak může být porušena bezpečnost informací?
- S jakou pravděpodobností se to stane? [8]



Obr. 8 Analýza rizik [8]

4.2 Přístupy analýzy rizik

Základní přístup

Tato metoda rychle zavádí bezpečnostní opatření bez podrobnější analýzy. Aplikovaná opatření bývají převzata ze standardů v oblasti informační bezpečnosti. Výhoda je rychlost nasazení. Jde o úspornou metodu, protože při implementaci je použito standardní řešení. Tento přístup je vhodný pro organizace s malou vazbou na IT.

Neformální přístup

Tento přístup není založen na předem definovaných metodách, vychází ze zkušeností osob a znalostí konkrétního prostředí. Výhodou je rychlost a nenákladnost.

Podrobná analýza rizik

Považuje se za nejpřesnější přístup, ale je časově a finančně náročná. Postupuje se od identifikace a hodnocení aktiv přes posouzení hrozeb na aktiva a odhad zranitelnosti. Na základě toho jsou poté nadefinována bezpečnostní opatření.

Kombinovaný přístup

Používá se při analýze rizik ve velkých organizacích. Vybraná aktiva se analyzují pomocí podrobného přístupu, ostatní části IS podle základního přístupu. Získáme rychlý přehled o rizicích, která hrozí IS jako celku a rovněž získáme podrobné informace o rizicích, které hrozí kritickým částem IS. [8]

4.3 Metody řízení rizik

Analytické

Jsou metody zaměřené na identifikaci zdrojů rizika. Analyzují příčiny vzniku nebezpečných událostí a scénáře rozvoje nebezpečné události.

- Delfská metoda – patří mezi nejpoužívanější metody kvalitativní analýzy rizik, mezi metody expertního odhadování. Používá se pro podporu provádění kvantitativní analýzy rizik. Pro analýzu rizik je vhodná především proto, že určuje, co se může stát a za jakých podmínek.

- Check list – analýza pomocí kontrolního seznamu, je velmi jednoduchá technika využívající seznam položek, kroků či úkolů podle kterých se ověřuje správnost či úplnost postupu.
- What If – co se stane, když? Je postup na hledání možných dopadů vybraných situací.

  Je to diskuse a hledání nápadů, ve které skupina zkušených lidí obeznámených s procesem klade otázky nebo vyslovuje úvahy o možných nehodách.

- Maticový diagram – používá se k posouzení vzájemných souvislostí mezi dvěma nebo více oblastmi problému. [3]
- ETA – analýza stromu událostí – analytická technika, která se používá pro vyhodnocení průběhu procesu a jeho událostí vedoucích k možné nehodě.
- HAZOP – analýza ohrožení a provozuschopnosti, jde o systematickou identifikaci nebezpečných stavů složitých procesních zařízení, včetně prověření stávajících bezpečnostních funkcí a formulace opatření snižující míru rizika.
- SWOT analýza – jádro této metody spočívá v klasifikaci a ohodnocení jednotlivých faktorů, které jsou rozděleny do 4 základních skupin (silné a slabé stránky subjektu a faktory vyjadřující příležitosti a nebezpečí jako vlastnosti vnějšího prostředí). [6]

Srovnávací

Srovnávací metody jsou zaměřeny na identifikaci zdrojů rizika. Většinou se provádějí na základě porovnávání a aplikování provozních zkušeností získaných z provozu nebezpečných zařízení a doplněné prohlídkou zařízení. Jejich cílem je odhalení slabin nebezpečného zařízení.

- Indexové metody (RR – Relative Ranking) - jedná se o metody rychlého posuzování bezpečnosti procesu s využitím indexů pro oceňování nebezpečných vlastností procesu. Princip metod je bodové ohodnocení jednotlivých operací procesu a procesních podmínek na základě stanovených výpočtů.
- Revize bezpečnosti (SR – Safety Review) - Revize bezpečnosti je určena pro identifikaci podmínek nebo provozních činností v podniku, které by mohly vést k nehodě a následně ke zranění, újmě na majetku nebo na životním prostředí. Revize bezpečnosti zahrnuje rozhovory s lidmi v podniku. Na základě zjištěných informací je revizor bezpečnosti schopen vytvořit odhad možných situací a scénářů, které mohou způsobit újmu.

- Kontrolní seznam (CL – Checklist Analysis) - k analýze kontrolním seznamem se používá psaný seznam položek nebo kroků k ověření stavu systému. Kontrolní seznam poskytuje základ pro zhodnocení procesních zdrojů rizika. Měl by odhalit problémy, které vyžadují pozdější podrobnou analýzu.

4.4 Postup při analýze rizik

Při řešení ISMS je důležitým krokem v prvních fázích procesu analýza rizik. Analýza rizik je klíčový prvek a stojí na vrcholu pyramidy zavádění systému ISMS. [1]

Analýza rizik obsahuje tyto kroky:

- Stanovení hranice analýzy rizik – je třeba určit, která aktiva budou do analýzy rizik zahrnuta a která budou vyloučena. Tímto krokem je jednoznačně dán výsledný rozsah analýzy. Tato hranice je převážně stanovována vedením podniku na základě vytvořené úvodní studie či sledovaná oblast obsahuje aktiva podniku, která se přímo podílejí na jeho činnosti nebo tvoří jeho konkurenční výhodu apod.
- Identifikace aktiv – vytváří se soupis všech identifikovaných aktiv uvnitř definované hranice pro analýzu rizik.
- Stanovení hodnoty a seskupování aktiv – při stanovení hodnoty aktiv se může vycházet z různých hledisek. Tato hlediska lze rozdělit na zkoumání nákladových či výnosových charakteristik aktiva. Použijí se ty charakteristiky, které odpovídají vyšší hodnotě pro podnik. Patří sem např. pořizovací cena, zisky z aktiva, ochranná známka, patent, průmyslový vzor, kvalifikace, know-how, technologie atd. Do hodnoty je třeba započítat, jak podnik je moc závislý na daném aktivu, co se v podniku stane v případě ztráty, nedostupnosti, zničení aktiva. Protože aktiv může být v podniku identifikováno velké množství, je vhodné tyto aktiva shlukovat do určitých celků podle jejich povahy.
- Identifikace hrozeb – v tomto kroku analýzy rizik se vyhledávají hrozby, pro které musí být v dalších krocích následně nalezeno odpovídající protiopatření. Výběr možných hrozeb je třeba provádět tak, aby tyto hrozby ohrožovaly alespoň jedno z identifikovaných aktiv. Hrozby lze získat z mnoha zdrojů, především z literatury, oborových zkušeností, případně z provedených analýz.
- Analýza hrozeb a zranitelnosti – každou identifikovanou hrozbu je třeba hodnotit vůči všem skupinám aktiv, které jsme předchozími kroky vytvořili. Je třeba, aby pro

aktiva, u kterých se může daná hrozba uplatnit, byla určena úroveň hrozby vůči aktivu a také úroveň zranitelnosti aktiva vůči této hrozbě.

- Pravděpodobnost jevu – musíme zvážit pravděpodobnost výskytu dané hrozby. Je tedy potřeba při analýze hrozeb tyto identifikované hrozby doplnit pravděpodobností jejich výskytu a tuto hodnotu pak brát v potaz při vytváření protiopatření. Je potřeba také zkoumat, zda se jedná o jevy náhodné nebo ne.
- Měření rizika – výše rizika vyplývá z hodnoty aktiva, úrovně hrozby a zranitelnosti aktiva.

4.5 Druhy rizika

Každé riziko má neblahý vliv na finanční oblast organizace, je tedy nutné rozlišovat, o jakou úroveň ohrožení se jedná. Úrovně rizik mohou být:

Nízké – v tomto případě je riziko pro podnik obvykle akceptovatelné, jeho působením nedochází k téměř žádným citelným ztrátám. Je ale nutné jej monitorovat a rozhodně nesmí být ignorováno. Opatření proti nízkým rizikům je možno zavádět řádově v měsících.

Střední – zde je již nutností zavést opatření, která ovšem minimalizují riziko jen z části. Opatření bývají zaváděna řádově v týdnech.

Vysoké – jde o úroveň, kdy je nezbytné co nejdříve přijmout taková opatření, aby došlo k výraznému snížení úrovně rizika. Zavedení probíhá řádově ve dnech.

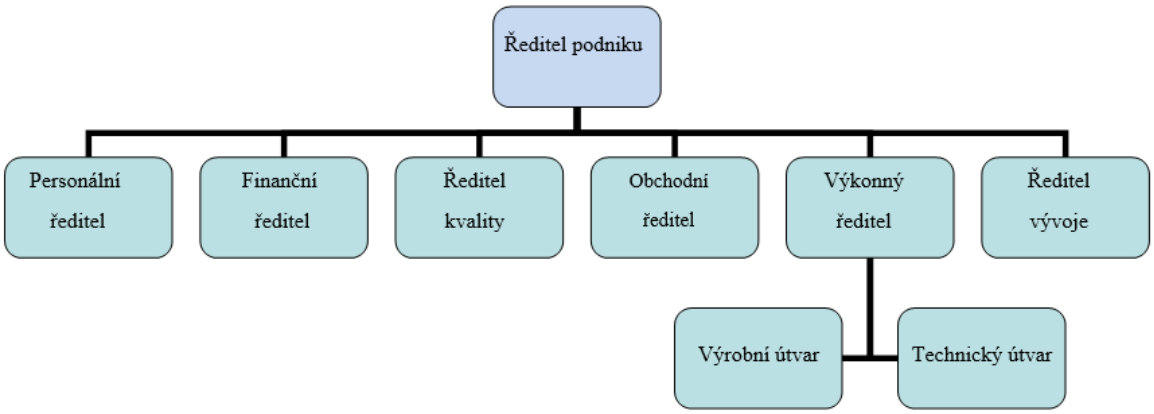
Kritické – probíhající proces musí být ukončen do doby, než budou zavedena opatření, která toto riziko sníží. Navrhují se jednoduchá a rychle aplikovatelná opatření, která je možno zavést během několika hodin. [14]

V procesu snižování rizika je třeba brát v úvahu, že riziko nikdy zcela neeliminujeme. Často nastane situace, že zavedením opatření vzniknou další typy rizik.

II. PRAKTICKÁ ČÁST

5 PŘEDSTAVENÍ PODNIKU

Společnost, na kterou je zaměřena tato práce, je podnikem, který se profiluje v oblasti, strojírenské výroby a vývoje. Zaměstnává více než 800 zaměstnanců, kteří dohromady nabízí široké portfolio profesionálních služeb.



Obr. 9 Organizační struktura podniku, Mičulková 2018

Hlavní odpovědnost za provádění činností spojených s managementem bezpečnosti v tomto podniku, má ředitel podniku, který má v pravomoci schvalovat politiku a cíle managementu bezpečnosti, rozhodovat o prioritách a změnách jednotlivých oblastí. Výkonem odpovědné osoby za ochranu utajovaných informací je pověřen ředitelem podniku bezpečnostní ředitel.

Odpovědnost za zpracování a aplikaci jednotlivých oblastí managementu bezpečnosti mají představitelé top managementu, kteří jsou majitelé daného procesu. Tito majitelé procesů mají v pravomoci vytvářet vhodné prostředí, podmínky a zásady k realizaci managementu bezpečnosti v oblastech jejich podřízenosti a jsou také odpovědni za efektivní a kvalitní naplňování tohoto cíle.

Ve společnosti platí vnitřní směrnice, která stanovuje pravidla pro používání informačních technologií v prostředí společnosti jako např. pravidla pro uživatelské účty, software nebo ukládání dat. Společnost má dále zavedenou směrnici týkající se bezpečnosti informací, která se zabývá také ochranou důvěrných informací a osobních údajů. Určuje postupy, jak s informacemi nakládat, a povinnosti zaměstnanců při práci s nimi.

5.1 Politika managementu bezpečnosti

Politika managementu bezpečnosti je stanovena top managementem podniku jako podpůrný program stanovených strategických cílů podniku, neboť bezpečnost se ve svém širokém pojetí prolíná do všech procesů probíhajících v podniku při zajišťování svých podnikatelských aktivit.

Realizace procesů managementu bezpečnosti je především preventivním prvkem směřujícím k zajištění možných rizikových oblastí, jejich vyhledávání, identifikování, monitorování, vyhodnocování a řešení konkrétních oblastí. V globálním efektu management bezpečnosti zvyšuje konkurenceschopnost podniku a přináší mu tak prestižní postavení v obchodní sféře.

5.2 Oblasti managementu bezpečnosti

Management bezpečnosti je zaměřen do těchto oblastí:

Bezpečnost obchodních informací

Zahrnuje oblast ochrany obchodního tajemství, důvěrných informací a know-how, které má podnik ve vlastním zájmu a zájmu obchodních aktivit ochraňovat.

Bezpečnost utajovaných informací

Představuje oblast ochrany utajovaných informací, které jsou označeny stupněm utajení a jejichž vyzrazení by způsobilo újmu zájmům ČR nebo by bylo pro zájmy ČR nevýhodné a utajovaných informací poskytovaných v mezinárodním styku.

Bezpečnost personálních informací

Jedná se o bezpečnost osobních údajů a citlivých údajů zaměstnanců podniku, se kterými je nutné manipulovat při jejich zpracování. Tato bezpečnost se prolíná i do formy zpracování, tj. do oblasti bezpečnosti informační techniky a bezpečnosti provozování kamerového systému v podniku.

Bezpečnost informačních systémů certifikovaných

Představuje oblast zpracování utajovaných informací na určených certifikovaných objektech a aktivech určeného informačního systému, který je certifikovaný NÚKIB a doložen odpovídajícím certifikátem s uvedenou dobou platnosti certifikovaného systému.

Bezpečnost informačních systémů podniku

Jedná se o oblast, která zavádí systémový přístup k bezpečnému zajištění podnikových informací zpracovávaných v prostředí informačního systému.

Bezpečnost fyzická

Bezpečnost fyzická zahrnuje několik samostatných oblastí, u kterých je nezbytné aplikovat prvky bezpečnosti v souladu s legislativou anebo na základě interních požadavků.

Jedná se o tyto oblasti:

- Ochrana majetku, bezpečnost areálů, bezpečnost objektů a zabezpečených oblastí, výkon ostrahy;
- Režimová pracoviště;
- Speciální přeprava vyžadující si specifické podmínky nebo utajení (techniky, materiálu, munice, výbušnin, chemikálií, odpadu, peněz a podobně);
- Manipulace se specifickým materiálem (zbraně, munice, výbušniny, chemikálie, nebezpečné odpady a podobně).

Bezpečnost průmyslová

Představuje aplikování prvků bezpečnosti při provozování citlivé činnosti podniku.

6 VSTUPNÍ ANALÝZA SOUČASNÉHO STAVU

V této kapitole je analyzován současný stav informační bezpečnosti ve společnosti, na základě, kterého se stanoví opatření pro zvýšení bezpečnosti.

V prostředí společnosti se používají počítače na platformě společnosti Microsoft a technologie Hyper-V, která platformu společnosti Microsoft zachovává. Jedná se tedy o unifikované řešení. Jiné operační systémy se v prostředí společnosti nepoužívají, nebezpečí napadení jiných operačních systémů tedy nehrozí. Všechny síťové prvky jsou od firmy CISCO. Servery jsou napájené přes zdroj nepřerušovaného napájení (UPS), který je v případě výpadku elektřiny vydrží napájet po dobu 45 minut. Počítače jsou převážně značky HP a je jich přibližně 250 a notebooky značky DELL a Lenovo, těch je přibližně 50. V nich je nainstalovaný OS Windows 7 z 80 % a novější již mají Windows 10.

Každý zaměstnanec má v adresářové službě Active Directory vytvořen účet s vhodným nastavením práv přístupu k podnikovým prostředkům, čímž je mu umožněn přístup pouze k firemním službám a prostředkům, které potřebuje k vykonávání své práce.

Ve společnosti platí vnitřní směrnice, které stanovují pravidla pro používání informačních technologií v prostředí společnosti jako např. pravidla pro uživatelské účty, software nebo ukládání dat. Předpokládám, že bude potřeba vytvořit nové směrnice nebo upravit ty stávající tak, aby odpovídaly požadavkům jednotlivých opatření, které vyplynou z analýzy rizik.

6.1 Rozsah analýzy

Data, aplikace a technické prostředky IS tvoří základní podpůrná aktiva, prostřednictvím kterých se zpracovávají primární aktiva. Tato aktiva mají pro společnost svoji hodnotu a je nutné zajistit jejich adekvátní ochranu. Cílem analýzy je zjistit podmínky a současný stav realizace informační bezpečnosti ve firmě pro následnou aktualizaci systému řízení bezpečnosti informací.

Hlavním důvodem pro ochranu informací podniku je zabezpečení jeho strategických zájmů, a to zejména zajištění dostupnosti služeb informačního systému, ochrany důležitých informací, ochrany osobních údajů a také zajištění dobrého jména.

Analýza informačních aktiv má za úkol získat přehled o zpracovávaných informacích a určení důležitých služeb a aplikací informačního systému. Při přípravě analýzy byla brána v úvahu hodnota zabezpečovaných aktiv a jejichž ohrožení (např. dočasná nedostupnost,

nepřípustná modifikace, zneužití, ztráta případně zničení), které by mohly vést k vážným následkům, jako je např. únik citlivých informací, porušení právních norem nebo přerušení aktivit podniku s tím, že nebudou dostupné služby informačního systému.

Rozsah požadované úrovně bezpečnosti je ve své podstatě závislý na rozsahu a hranicích bezpečnosti informací a hodnotě aktiv, která mají být chráněna. Míra ochrany musí být úměrná jejich hodnotě a předpokládaným hrozbám, kterým je informační systém vystaven.

6.2 Analýza rizik

Analýza rizik bude vypracována podle maticové metody analýzy rizik.

Tato analýza využívá tři parametry aktivum, hrozba a zranitelnost. Matice zranitelnosti se vytvoří spojením tabulky hodnocení aktiv, tabulky hrozeb a zranitelností. Poté se jednotlivé zranitelnosti aktiv posoudí a doplní do matice. Dále se pomocí vzorce vypočítá míra rizika a zanese se do nové matice rizik a podle stanovených hranic rizika se stanoví jeho závažnost.

Návrh bezpečnostních opatření k minimalizaci největších rizik v podniku:

- Analýza rizik:
    - Analýza aktiv;
        - identifikace aktiv;
        - ohodnocení aktiv;
    - Analýza hrozeb;
        - identifikace hrozeb;
        - pravděpodobnost hrozeb;
        - ohodnocení hrozeb;
        - analýza zranitelnosti;
    - hodnocení zranitelnosti aktiv vůči možným hrozbám;
    - hodnocení, akceptace rizik;
- výběr vhodných bezpečnostních opatření, k zajištění akceptovatelné bezpečnosti.

6.2.1 Analýza aktiv

V první části analýzy byla identifikována aktiva společnosti. Tabulka 1 byla stanovena na základě komunikace s top managementem firmy. Dále bylo provedeno ohodnocení aktiv, a to vzhledem k dopadu na podnik, který se děje v důsledku porušení důvěrnosti, integrity

a dostupnosti daných aktiv. Pro hodnocení aktiv je použita škála 1–4 a nejdůležitější aktiva jsou ohodnocena „4“.

Tab. 1 Škála ohodnocení aktiv, Mičulková 2018

Popis dopadu	Hodnota aktiva
Nízký	1
Střední	2
Vysoký	3
Kritická úroveň	4

Stupnice pro hodnocení jednotlivých parametrů (důvěrnost, integritu, dostupnost) jsou uvedeny v tabulkách níže dle Vyhlášky č. 316/2014 Sb.

Tab. 2 Stupnice pro hodnocení důvěrnosti [16]

Úroveň	Popis	Ochrana
1 - Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění (např. na základě zákona č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů). Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Není vyžadována žádná ochrana.
2 - Střední	Aktiva nejsou veřejně přístupná a tvoří know-how orgánu a osoby uvedené v § 3 písm. c) až e) zákona, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.
3 - Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství podle zákona č. 89/2012 Sb., občanský zákoník, osobní údaje podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací vnější komunikační sítí jsou chráněny pomocí kryptografických prostředků.
4 – Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. strategické obchodní tajemství, citlivé osobní údaje).	Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.

Tab. 3 Stupnice pro hodnocení integrity [16]

Úroveň	Popis	Ochrana
1 - Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Není vyžadována žádná ochrana.
2 - Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (např. omezení přístupových práv pro zápis).
3 - Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených vnějšími komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
4 - Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. pomocí technologie digitálního podpisu).

Tab. 4 Stupnice pro hodnocení dostupnosti [16]

Úroveň	Popis	Ochrana
1 - Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
2 - Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
3 – Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona. Aktiva jsou považována jako velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
4 – Kritická	Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona. Aktiva jsou považována jako kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

6.2.2 Ohodnocení aktiv

Dále byla aktiva ohodnocena pomocí algoritmu: Hodnota aktiva = (Důvěrnost + Integrita + Dostupnost) / 3.

Tab. 5 Přehled identifikovaných aktiv a jejich ohodnocení, Mičulková 2018

Skupina	Poř.č.	Název aktiva	Důvěr-nost	Inte-grita	Dostup-nost	Hodnota aktiva
Listiny	**1**	Listiny – standardní důvěrnost	3	3	2	3
	2	Listiny – vysoká důvěrnost	4	3	2	3
	3	Sklad důvěrný	3	3	2	3
	4	Sklad standard	3	3	2	3
Data	**5**	Elektronická data	3	3	2	3
	6	Elektronická data-důvěrná	4	3	2	3
Aplikace	**7**	Provozní SW	3	3	2	3
	8	Systémový SW	4	4	3	4
Operační systém	**9**	Operační systémy	4	4	3	4
	10	Server	3	4	4	4
Hardware a podpůrná zařízení	**11**	Čtečky/Av technika/média	3	3	2	3
	12	UPS, EZS	4	3	3	3
	13	Kamery	2	2	3	2
	14	Tiskárny	2	2	3	2
	15	Switche	4	4	3	4
	16	Síťová infrastruktura	4	4	3	4
	17	Pracovní stanice/notebooky	3	3	2	3
Kabeláž	**18**	Datová kabeláž	3	3	2	3
	19	Elektrické rozvody	3	2	3	3
Lidé	**20**	Lidé – standardní důvěrnost	3	3	2	3
	21	Lidé – vysoká důvěrnost	4	3	2	3
Budovy, serverovny, kanceláře	**22**	Budovy	3	3	2	3
	23	Datové centrum	4	4	3	4
	24	Kanceláře	3	3	2	3
	25	Příruční archiv	3	3	2	3
Služby	**26**	Elektronická pošta	3	3	2	3
	27	Webové stránky	3	3	3	3
	28	Připojení k internetu	3	4	3	3

6.2.3 Analýza hrozeb

Na aktiva působí mnoho druhů hrozeb. Hrozby můžou způsobit nežádoucí incident, který může mít za následek poškození aktiv a tím i poškození organizace. K tomuto poškození může dojít např. v důsledku kybernetického útoku na informace organizace a výsledkem takovéhoto útoku může být např. nedovolené prozrazení, modifikace, zkomolení, zničení, nedostupnost nebo ztráta informací. Hrozby mohou vzniknout z náhodných, neúmyslných nebo úmyslných příčin či událostí.

Aby došlo k poškození aktiva, využívá hrozba jedné nebo i více zranitelností systémů, aplikací nebo služeb využívaných organizací. Hrozby mohou působit z vnějšku nebo vnitřku organizace. Hrozby a zranitelnosti musí působit současně, aby způsobily incidenty, které by mohly poškodit aktiva.

Pro analýzu rizik je použit katalog hrozeb, který vychází z katalogu hrozeb Vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech a je uveden v příloze P I.

Škála pro pravděpodobnost hrozeb. Škála 1-4, jedna je velmi nízká pravděpodobnost hrozby a čtyři je nejvyšší pravděpodobnost hrozby.

Tab. 6 Škála pravděpodobnosti hrozeb, Mičulková 2018

Popis	Hodnota
Velmi nízká pravděpodobnost hrozby	1
Nízká pravděpodobnost hrozby	2
Střední pravděpodobnost hrozby	3
Vysoká pravděpodobnost hrozby	4

Tab. 7 Identifikace a pravděpodobnost hrozeb, Mičulková 2018

Poř.č.	Hrozba	Pravděpodobnost
1	Zemětřesení	1
2	Povodně	1
3	Hurikán / Přívalový déšť	1
4	Blesk	2
5	Průmyslová akce	2
6	Nedostatečná ochrana vnějšího perimetru / krádež	2
7	Použití zbraní / bomby	1

8	Škoda způsobená průnikem neoprávněné osoby	3
9	Nedostatek zaměstnanců s potřebnou odbornou úrovní	3
10	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	4
11	Provedení neoprávněných činností	2
12	Zneužití oprávnění ze strany uživatelů	3
13	Zneužití oprávnění ze strany administrátorů	2
14	Zneužití identity jiné fyzické osoby	3
15	Zneužití nebo modifikace údajů	1
16	Zneužití vnitřních prostředků, sabotáž	1
17	Užívání software v rozporu s licenčními podmínkami	3
18	Pochybení ze strany zaměstnanců a neschopnost jeho včasného odhalení	2
19	Zneužití vyměnitelných paměťových médií	2
20	Odcizení nebo poškození aktiva	2
21	Poškození, nebo selhání technického, nebo programového vybavení	4
22	Škodlivý kód (např. viry, spyware, trojské koně)	2
23	Nedostatky při poskytování služeb informačního systému	2
24	Přerušení dodávky komunikačních služeb nebo elektrické energie	3
25	Nedostatečná údržba	3
26	Chyba údržby informačního systému	3
27	Kybernetický útok z vnější komunikační sítě	2
28	Kybernetický útok z vnitřní sítě	1
29	Cílený kybernetický útok (pomocí sociálního inženýrství, použití špionážních technik)	2
30	Nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů	4
31	Nepřesné nebo nejednoznačné vymezení práv a povinností administrátorů	2
32	Nepřesné nebo nejednoznačné vymezení práv a povinností bezpečnostních rolí	2
33	Nevhodné nastavení přístupových oprávnění	3
34	Nedostatečné postupy při identifikování a ošetřování bezpečnostních událostí a incidentů	3
35	Nedostatečné monitorování činnosti uživatelů	4
36	Nedostatečné monitorování činnosti administrátorů	3
37	Nevhodná bezpečnostní architektura	2
38	Nedostatečná míra nezávislé kontroly	3

6.2.4 Posouzení zranitelnosti jednotlivých aktiv jednotlivými hrozbami

Pro hodnocení hrozeb je důležité stanovit předpokládaný dopad na aktivum při vzájemné interakci hrozby a zranitelnosti. Současně je určena míra možného dopadu hrozby v případě její realizace na dostupnost, důvěrnost a integritu aktiva.

Jednotlivé parametry pro stanovení dopadů jsou uvedeny v následující tabulce.

Tab. 8 Škála dopadu na aktivum, Mičulková 2018

Popis	Hodnota
Žádný dopad na organizaci	1
Minimální dopad na organizaci	2
Střední potíže a možnost finanční ztráty	3
Velké potíže a finanční ztráty	4

Tab. 9 Dopad hrozby na dostupnost, důvěrnost a integritu, Mičulková 2018

Poř.č.	Hrozba	Důvěrnost	Inte-grita	Dostup-nost
1	Zemětřesení	1	3	2
2	Povodně	2	3	2
3	Hurikán / Přívalový déšť	1	3	2
4	Blesk	1	2	2
5	Průmyslová akce	1	3	2
6	Nedostatečná ochrana vnějšího perimetru / krádež	1	2	1
7	Použití zbraní / bomby	1	3	3
8	Škoda způsobená průnikem neoprávněné osoby	2	2	2
9	Nedostatek zaměstnanců s potřebnou odbornou úrovní	3	1	2
10	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	4	3	3
11	Provedení neoprávněných činností	1	3	3
12	Zneužití oprávnění ze strany uživatelů	2	2	4
13	Zneužití oprávnění ze strany administrátorů	2	3	3
14	Zneužití identity jiné fyzické osoby	2	3	3
15	Zneužití nebo modifikace údajů	2	3	3
16	Zneužití vnitřních prostředků, sabotáž	1	3	3
17	Užívání software v rozporu s licenčními podmínkami	2	1	3
18	Pochybení ze strany zaměstnanců a neschopnost jeho včasného odhalení	2	3	2
19	Zneužití vyměnitelných paměťových médií	1	3	1
20	Odcizení nebo poškození aktiva	2	4	3
21	Poškození, nebo selhání technického, nebo programového vybavení	3	1	2
22	Škodlivý kód (např. viry, spyware, trojské koně)	2	3	2
23	Nedostatky při poskytování služeb informačního systému	2	3	3
24	Přerušení dodávky komunikačních služeb nebo elektrické energie	3	1	3
25	Nedostatečná údržba	2	1	3
26	Chyba údržby informačního systému	2	1	3
27	Kybernetický útok z vnější komunikační sítě	2	4	3
28	Kybernetický útok z vnitřní sítě	2	3	2

29	Cílený kybernetický útok (pomocí sociálního inženýrství, použití špionážních technik)	2	3	3
30	Nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů	1	2	3
31	Nepřesné nebo nejednoznačné vymezení práv a povinností administrátorů	4	3	3
32	Nepřesné nebo nejednoznačné vymezení práv a povinností bezpečnostních rolí	2	2	4
33	Nevhodné nastavení přístupových oprávnění	2	3	2
34	Nedostatečné postupy při identifikování a ošetřování bezpečnostních událostí a incidentů	4	3	3
35	Nedostatečné monitorování činnosti uživatelů	3	1	2
36	Nedostatečné monitorování činnosti administrátorů	2	3	2
37	Nevhodná bezpečnostní architektura	2	3	3
38	Nedostatečná míra nezávislé kontroly	2	1	3

6.2.5 Matice zranitelnosti

Zranitelnosti jsou bezpečnostně slabá místa spojená s aktivy organizace. Tato slabá místa mohou být využita jednou nebo více hrozbami, což zapříčiní nežádoucí incident, který může vyústit ve ztrátu, zničení nebo poškození těchto aktiv a činnosti organizace. Zranitelnost sama o sobě nezpůsobuje poškození, je to pouze okolnost nebo soubor okolností, které mohou umožnit hrozbě, aby se realizovala a zapříčinila poškození aktiv a činnosti, které jsou těmito aktivy podporovány. Identifikace zranitelnosti musí zjistit slabá místa, která se vztahují k aktivům.

Tab. 10 Škála posouzení zranitelnosti, Mičulková 2018

Úroveň	Hodnota	Popis
Nízká	1	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, které jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
Střední	2	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	3	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	4	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Tab. 11 Matice zranitelnosti, Mičulková 2018

	Popis aktiva	Listiny - standardní důvěrnost	Listiny - vysoká důvěrnost	Sklad důvěrný	Sklad standard	Elektronická data	Elektronická data-důvěrná	Provozní SW	Systémový SW	Operační systémy	Server	Čtečky/Av technika/média	UPS, EZS	Kamery	Tiskárny	Switche	Síťová infrastruktura	Pracovní stanice/notebooky	Datová kabeláž	Elektrické rozvody	Lidé - standardní důvěrnost	Lidé - vysoká důvěrnost	Budovy	Datové centrum	Kanceláře	Přírůční archiv	Elektronická pošta	Webové stránky	Připojení k internetu
	Hodnota aktiva (A)	3	3	3	3	3	3	3	4	4	4	3	3	2	2	4	4	3	3	3	3	3	3	4	3	3	3	3	3
Popis hrozby	**Pravděpodobnost hrozby (T)**																												
Zemětřesení	1						1	1	1	1	1		1	1	1	1	1	1	1	1			2	1	1	1		2	1
Povodně	1	1	2	1	1			1	1	1	2	1	1	3	1	2	1	1	2	2			2	2	1	1			1
Hurikán / Přívalový déšť	1			1							2		1	2	2		1		1	2			2	1	1	1			1
Blesk	2							1	1	1	2	1	2	3	2	2	1	2	1	1	1	1	1	1	1				1
Průmyslová akce	2																2												1
Nedostatečná ochrana vnějšího perimetru / krádež	2	1	3		1	3						2						1											
Použití zbraní / bomby	1	1	2	1	1					1	1		1	1	1	1	1	1	1	1	2	3	1	1	1	1			
Škoda způsobená průnikem neoprávněné osoby	3	2	4	2	1	3												2								1			
Nedostatek zaměstnanců s potřebnou odbornou úrovní	3					2	3	1	1												3	4							
Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	4					1	2			2																	4		
Provedení neoprávněných činností	2	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1
Zneužití oprávnění ze strany uživatelů	3	3	4	4	2	2	4					2						2			2	3					3		2
Zneužití oprávnění ze strany administrátorů	2					2	3							2				2			1	3		2			3		
Zneužití identity jiné fyzické osoby	3	2	3			2	3											2											
Zneužití nebo modifikace údajů	1	2	4															1											
Zneužití vnitřních prostředků, sabotáž	1										2			1	1	2	2	1	1			1			1				

Užívání software v rozporu s licenčními podmínkami	3							2	2									2													
Pochybení ze strany zaměstnanců a neschopnost jeho včasného odhalení	2	2	3		2	3						2									1	2					2			
Zneužití vyměnitelných paměťových médií	2	1	2																											
Odcizení nebo poškození aktiva	2	2	4	4	2	4	4	1	1	1	3	2	1	1	1	1	1	1	1	1				1	1	1				
Poškození, nebo selhání technického, nebo programového vybavení	4					2	3																				2	2		
Škodlivý kód (např. viry, spyware, trojské koně)	2					3	4																				4	3	3	
Nedostatky při poskytování služeb informačního systému	2																											2	3	
Přerušení dodávky komunikačních služeb nebo elektrické energie	3										3		1	1	1	2		2												4
Nedostatečná údržba	3												1	1	1	1		1	2	2			1	1						
Chyba údržby informačního systému	3							1	2	2																	2	1	1	
Kybernetický útok z vnější komunikační sítě	2					3	4											1									3	3	3	
Kybernetický útok z vnitřní sítě	1					2	3											1									2	2	2	
Cílený kybernetický útok (pomocí sociálního inženýrství, použití špionážních technik)	2	1	3	1	3	2	3											2										1		
Nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů	4	1	3	3	1	3	4	1	1	1																				
Nepřesné nebo nejednoznačné vymezení práv a povinností administrátorů	2					3	4																				3			
Nepřesné nebo nejednoznačné vymezení práv a povinností bezpečnostních rolí	2																				1	3								
Nevhodné nastavení přístupových oprávnění	3					1	3											1			1	3								
Nedostatečné postupy při identifikování a ošetřování bezpečnostních událostí a incidentů	3					3	4																							
Nedostatečné monitorování činnosti uživatelů	4					3	4	1	1			2			1						1	2								
Nedostatečné monitorování činnosti administrátorů	3					2	3	1	1	1																				
Nevhodná bezpečnostní architektura	2					2	3	1	1	1	1		1			1			1				1							
Nedostatečná míra nezávislé kontroly	3	1	2								1			1	1	1							1	1						

6.2.6 Výsledné riziko

Pravděpodobnost výskytu hrozby, dopad hrozeb a zranitelnost aktiv vůči hrozbám, představují, společně s ohodnocením aktiv, vstupní informace, potřebné pro výpočty analýzy rizik.

Výsledným rizikem je definována pravděpodobnost, s jakou hrozba zneužije zranitelnosti aktiva. Míra rizika je kalkulována pro každou kombinaci aktivum / hrozba.

Pro výpočet míry rizika se použije tento vzorec:

R = T * A * V,

kde „R“ je míra rizika, „T“ je pravděpodobnost hrozby, „A“ je hodnota aktiva a „V“ je zranitelnost. Výsledné hodnoty tohoto vzorce jsou vyjádřeny třemi kategoriemi rizik:

Tab. 12 Kategorie rizik, Mičulková 2018

Rozmezí možného rizika	Stupnice míry rizika
1 – 20	Nízká míra rizika
21 – 40	Střední míra rizika
41 – 64	Vysoká míra rizika

6.3 Hodnocení rizik

Rizika s nízkou hodnotou je obvykle možné přijmout, jelikož opatření ke snížení těchto rizik, by svými náklady mohla snadno přesáhnout možné škody, ke kterým rizika vedou. Tyto jevy vedou s malou pravděpodobností k nízkému dopadu na činnost a bezpečnost podniku. Pořizovací cena těchto aktiv může být v některých případně značně vysoká (kamery, switche aj.), ale náhrada je okamžitá a ztráty při výpadku budou minimální.

Výskytu rizik se střední hodnotou může mít již vliv na činnost podniku nebo jeho částí. Tyto rizika by se měla snižovat účinnými opatřeními na přijatelnou úroveň.

Vysoká rizika vedou k velmi vážným dopadům na celý podnik a je nutné se na ně zaměřit a efektivně je redukovat.

V případě, že některá rizika přesahují střední úroveň rizika a pro podnik je problematické je snižovat např. z důvodu vysokých nákladů, je nutné rozhodnout o tom, zda se budou i tato rizika akceptovat či nikoli.

Toto rozhodnutí spadá do kompetence top managementu podniku, který jako jediný může posoudit, zda tato rizika mohou významně poškodit dosahování cílů organizace. Pokud se

vedení rozhodne tato rizika akceptovat, bere tím na vědomí, že by v budoucnu mohly nastat situace, kdy se tato rizika uplatní.

Z provedené analýzy rizik vyplynulo, že podnik ohrožuje:

- 3 Vysokých rizik;
- 35 Středních rizik;
- 274 Nízkých rizik.

Následně je zpracována matice rizik, ze které je vidět, že největší riziko představuje nedostatečné bezpečnostní povědomí uživatelů a administrátorů, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů a nedostatečné monitorování činnosti uživatelů.

Těmito třemi riziky je potřeba se při návrhu opatření přednostně zabývat a navrhnout opatření pro jejich zvládání.

Tab. 13 Matice rizik, Mičulková 2018

	Popis aktiva	Listiny - standardní důvěrnost	Listiny - vysoká důvěrnost	Sklad důvěrný	Sklad standard	Elektronická data	Elektronická data-důvěrná	Provozní SW	Systémový SW	Operační systémy	Server	Čtečky/Av technika/média	UPS, EZS	Kamery	Tiskárny	Switche	Síťová infrastruktura	Pracovní stanice/notebooky	Datová kabeláž	Elektrické rozvody	Lidé - standardní důvěrnost	Lidé - vysoká důvěrnost	Budovy	Datové centrum	Kanceláře	Přírůční archiv	Elektronická pošta	Webové stránky	Připojení k internetu
	Hodnota aktiva (A)	3	3	3	3	3	3	3	4	4	4	3	3	2	2	4	4	3	3	3	3	3	3	4	3	3	3	3	3
Popis hrozby	**Pravděpodobnost hrozby (T)**																												
Zemětřesení	1	0	0	0	0	0	3	3	4	4	4	0	3	2	2	4	4	3	3	3	0	0	6	4	3	3	0	6	3
Povodně	1	3	6	3	3	0	0	3	4	4	8	3	3	6	2	8	4	3	6	6	0	0	6	8	3	3	0	0	3
Hurikán / Přívalový déšť	1	0	0	3	0	0	0	0	0	0	8	0	3	4	4	0	4	0	3	6	0	0	6	4	3	3	0	0	3
Blesk	2	0	0	0	0	0	0	6	8	8	16	6	12	12	8	16	8	12	6	6	6	6	6	8	6	0	0	0	6
Průmyslová akce	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16	0	0	0	0	0	0	0	0	0	0	0	6
Nedostatečná ochrana vnějšího perimetru / krádež	2	6	18	0	6	18	0	0	0	0	0	12	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0
Použití zbraní / bomby	1	3	6	3	3	0	0	0	0	4	4	0	3	2	2	4	4	3	3	3	6	9	3	4	3	3	0	0	0
Škoda způsobená průnikem neoprávněné osoby	3	18	36	18	9	27	0	0	0	0	0	0	0	0	0	0	0	18	0	0	0	0	0	0	0	9	0	0	0
Nedostatek zaměstnanců s potřebnou odbornou úrovní	3	0	0	0	0	18	27	9	12	0	0	0	0	0	0	0	0	0	0	0	27	36	0	0	0	0	0	0	0
Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	4	0	0	0	0	12	24	0	0	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	48	0	0
Provedení neoprávněných činností	2	6	12	6	6	6	12	6	8	8	8	6	6	4	4	8	8	6	6	6	6	12	6	8	6	6	6	6	6
Zneužití oprávnění ze strany uživatelů	3	27	36	36	18	18	36	0	0	0	0	18	0	0	0	0	0	18	0	0	18	27	0	0	0	0	27	0	18
Zneužití oprávnění ze strany administrátorů	2	0	0	0	0	12	18	0	0	0	0	0	0	8	0	0	0	12	0	0	6	18	0	16	0	0	18	0	0
Zneužití identity jiné fyzické osoby	3	18	27	0	0	18	27	0	0	0	0	0	0	0	0	0	0	18	0	0	0	0	0	0	0	0	0	0	0

Zneužití nebo modifikace údajů	1	6	12	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0
Zneužití vnitřních prostředků, sabotáž	1	0	0	0	0	0	0	0	0	0	8	0	0	2	2	8	8	3	3	0	0	3	0	0	3	0	0	0	0
Užívání software v rozporu s licenčními podmínkami	3	0	0	0	0	0	0	18	24	0	0	0	0	0	0	0	0	18	0	0	0	0	0	0	0	0	0	0	0
Pochybení ze strany zaměstnanců a neschopnost jeho včasného odhalení	2	12	18	0	12	18	0	0	0	0	0	12	0	0	0	0	0	0	0	0	6	12	0	0	0	0	12	0	0
Zneužití vyměnitelných paměťových médií	2	6	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Odcizení nebo poškození aktiva	2	12	24	24	12	24	24	6	8	8	24	12	6	4	4	8	8	6	6	6	0	0	0	8	6	6	0	0	0
Poškození, nebo selhání technického, nebo programového vybavení	4	0	0	0	0	24	36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	24	24	0
Škodlivý kód (např. viry, spyware, trojské koně)	2	0	0	0	0	18	24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	24	18	18
Nedostatky při poskytování služeb informačního systému	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	18
Přerušení dodávky komunikačních služeb nebo elektrické energie	3	0	0	0	0	0	0	0	0	0	36	0	9	6	6	24	0	18	0	0	0	0	0	0	0	0	0	0	36
Nedostatečná údržba	3	0	0	0	0	0	0	0	0	0	0	0	9	6	6	12	0	9	18	18	0	0	9	12	0	0	0	0	0
Chyba údržby informačního systému	3	0	0	0	0	0	0	9	24	24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	18	9	9
Kybernetický útok z vnější komunikační sítě	2	0	0	0	0	18	24	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	18	18	18
Kybernetický útok z vnitřní sítě	1	0	0	0	0	6	9	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	6	6	6
Cílený kybernetický útok (pomocí sociálního inženýrství, použití špionážních technik)	2	6	18	6	18	12	18	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	0	0	0	0	0	6	0
Nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů	4	12	36	36	12	36	48	12	16	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Nepřesné nebo nejednoznačné vymezení práv a povinností administrátorů	2	0	0	0	0	18	24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	18	0	0
Nepřesné nebo nejednoznačné vymezení práv a povinností bezpečnostních rolí	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	18	0	0	0	0	0	0	0
Nevhodné nastavení přístupových oprávnění	3	0	0	0	0	9	27	0	0	0	0	0	0	0	0	0	0	9	0	0	9	27	0	0	0	0	0	0	0
Nedostatečné postupy při identifikování a ošetřování bezpečnostních událostí a incidentů	3	0	0	0	0	27	36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Nedostatečné monitorování činnosti uživatelů	4	0	0	0	0	36	48	12	16	0	0	24	0	0	8	0	0	0	0	0	12	24	0	0	0	0	0	0	0
Nedostatečné monitorování činnosti administrátorů	3	0	0	0	0	18	27	9	12	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Nevhodná bezpečnostní architektura	2	0	0	0	0	12	18	6	8	8	8	0	6	0	0	8	0	0	6	0	0	0	6	0	0	0	0	0	0
Nedostatečná míra nezávislé kontroly	3	9	18	0	0	0	0	0	0	0	12	0	0	6	6	12	0	0	0	0	0	0	9	12	0	0	0	0	0

7 ZAVEDENÍ ISMS V PODNIKU

Řízení rizik je oblast řízení organizace zaměřující se na analýzu a snížení rizika pomocí různých metod technik pro prevenci rizik, které eliminují rizika. Zvládáním se rizika identifikovaná v analýze rizik snižují výběrem vhodných opatření tak, aby se zbytková rizika (rizika, která zbydou po implementaci vybraných opatření) snížila na přijatelnou úroveň.

7.1 Výběr opatření

Opatření pro snížení rizik v oblasti bezpečnosti informací jsou vybrána podle normy ČSN ISO/IEC 27001, příloha A. V této kapitole konkrétně popisuji jednotlivá opatření, které jsem vybrala na základě výsledků analýzy rizik. Návrhy řešení jednotlivých opatření vychází z normy ISO 27002, soubor nejlepších praktik při zavádění ISMS v organizaci a literatury [2].

7.1.1 Opatření podle normy ČSN ISO/IEC 27001

Tab. 14 Soubor opatření a stav v organizaci [2], upravila Mičulková 2018

		Stav	Počet hodin
A.5 Politiky bezpečnosti informací			
A.5.1 Směřování bezpečnosti informací vedením organizace			
A.5.1.1	Politiky pro bezpečnost informací	zavedeno	
A.5.1.2	Přezkoumání politik pro bezpečnost informací	zavést	20
A.6 Organizace bezpečnosti informací			
A.6.1 Interní organizace			
A.6.1.1	Role a odpovědnosti bezpečnosti informací	zavést	5
A.6.1.2	Princip oddělení povinností	později	
A.6.1.3	Kontakt s příslušnými orgány a autoritami		
A.6.1.4	Kontakt se zájmovými skupinami		
A.6.1.5	Bezpečnost informací v řízení projektů	později	
A.6.2 Mobilní zařízení a práce na dálku			
A.6.2.1	Politika mobilních zařízení	později	
A.6.2.2	Práce na dálku	zavedeno	
A.7 Bezpečnost lidských zdrojů			
A.7.1 Před vznikem pracovního vztahu			
A.7.1.1	Prověřování		
A.7.1.2	Podmínky pracovního vztahu	zavedeno	
A.7.2 Během pracovního vztahu			
A.7.2.1	Odpovědnosti vedení organizace	zavést	15
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	zavést	18
A.7.2.3	Disciplinární řízení	později	

A.7.3 Ukončení a změna pracovního vztahu			
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	zavedeno	
A.8 Řízení aktiv			
A.8.1 Odpovědnost za aktiva			
A.8.1.1	Seznam aktiv	zavedeno	
A.8.1.2	Vlastnictví aktiv	zavedeno	
A.8.1.3	Přípustné použití aktiv		
A.8.1.4	Navrácení aktiv	později	
A.8.2 Klasifikace informací			
A.8.2.1	Klasifikace informací	zavést	15
A.8.2.2	Označování informací	zavést	8
A.8.2.3	Manipulaci s aktivy	později	
A.8.3 Manipulace s médii			
A.8.3.1	Správa výměnných médií	později	
A.8.3.2	Likvidace médií	později	
A.8.3.3	Přeprava fyzických médií	později	
A.9 Řízení přístupu			
A.9.1 Požadavky organizace na řízení přístupu			
A.9.1.1	Politika řízení přístupu	zavést	10
A.9.1.2	Přístup k sítím a síťovým službám		
A.9.2 Řízení přístupu uživatelů			
A.9.2.1	Registrace a zrušení registrace uživatele	zavedeno	
A.9.2.2	Správa uživatelských přístupů	zavedeno	
A.9.2.3	Správa privilegovaných přístupových práv	zavedeno	
A.9.2.4	Správa tajných autentizačních informací uživatelů	zavedeno	
A.9.2.5	Přezkoumání přístupových práv uživatelů	zavést	5
A.9.2.6	Odebrání nebo úprava přístupových práv		
A.9.3 Odpovědnosti uživatelů			
A.9.3.1	Používání tajných autentizačních informací		
A.9.4 Řízení přístupu k systémům a aplikacím			
A.9.4.1	Omezení přístupu k informacím		
A.9.4.2	Bezpečné postupy přihlášení	zavést	6
A.9.4.3	Systém správy hesel	zavést	4
A.9.4.4	Použití privilegovaných programových nástrojů	zavedeno	
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	zavedeno	
A.10 Kryptografie			
A.10.1 Kryptografická opatření			
A.10.1.1	Politika pro použití kryptografických opatření	později	
A.10.1.2	Správa klíčů	později	
A.11 Fyzická bezpečnost a bezpečnost prostředí			
A.11.1 Bezpečné oblasti			
A.11.1.1	Fyzický bezpečnostní perimetr	zavedeno	
A.11.1.2	Fyzické kontroly vstupu	zavedeno	
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	zavedeno	
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	zavedeno	
A.11.1.5	Práce v bezpečných oblastech	zavedeno	
A.11.1.6	Oblasti pro nakládku a vykládku	zavedeno	

A.11.2 Zařízení			
A.11.2.1	Umístění zařízení a jeho ochrana	zavedeno	
A.11.2.2	Podpůrné služby	zavedeno	
A.11.2.3	Bezpečnost kabelových rozvodů	zavedeno	
A.11.2.4	Údržba zařízení	zavedeno	
A.11.2.5	Přemístění aktiv	zavedeno	
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	zavedeno	
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	zavedeno	
A.11.2.8	Uživatelská zařízení bez obsluhy	zavedeno	
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	zavedeno	
A.12 Bezpečnost provozu			
A.12.1 Provozní postupy a odpovědnosti			
A.12.1.1	Dokumentované provozní postupy	zavést	4
A.12.1.2	Řízení změn	později	
A.12.1.3	Řízení kapacit	později	
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu		
A.12.2 Ochrana proti malwaru			
A.12.2.1	Opatření proti malwaru	zavedeno	
A.12.3 Zálohování			
A.12.3.1	Zálohování informací	zavedeno	
A.12.4 Zaznamenávání formou logů a monitorování			
A.12.4.1	Zaznamenávání událostí formou logů	zavést	4
A.12.4.2	Ochrana logů	později	
A.12.4.3	Logy o činnosti administrátorů a operátorů	zavést	6
A.12.4.4	Synchronizace hodin	zavedeno	
A.12.5 Správa provozního softwaru			
A.12.5.1	Instalace softwaru na provozní systémy	zavedeno	
A.12.6 Řízení technických zranitelností			
A.12.6.1	Řízení technických zranitelností	zavedeno	
A.12.6.2	Omezení instalace softwaru	zavedeno	
A.12.7 Hlediska auditu informačních systémů			
A.12.7.1	Opatření k auditu informačních systémů	později	
A.13 Bezpečnost komunikací			
A.13.1 Správa bezpečnosti sítě			
A. 13.1.1	Opatření v sítích	zavedeno	
A.13.1.2	Bezpečnost síťových služeb	zavedeno	
A.13.1.3	Princip oddělení v sítích		
A.13.2 Přenos informací			
A.13.2.1	Politiky a postupy při přenosu informací	zavedeno	
A.13.2.2	Dohody o přenosu informací	později	
A.13.2.3	Elektronické předávání zpráv	později	
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	zavedeno	
A.14 Akvizice, vývoj a údržba systémů			
A.14.1 Bezpečnostní požadavky informačních systémů			
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	později	
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	zavedeno	
A.14.1.3	Ochrana transakcí aplikačních služeb	zavedeno	

A.14.2 Bezpečnost v procesech vývoje a podpory			
A.14.2.1	Politika bezpečného vývoje		
A.14.2.2	Postupy řízení změn systémů		
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy		
A.14.2.4	Omezení změn softwarových balíků	později	
A.14.2.5	Principy budování bezpečných systémů		
A.14.2.6	Prostředí bezpečného vývoje		
A.14.2.7	Outsourcovaný vývoj	později	
A.14.2.8	Testování bezpečnosti systémů	později	
A.14.2.9	Testování akceptace systémů	později	
A.14.3 Data pro testování			
A.14.3.1	Ochrana dat pro testování	později	
A.15 Dodavatelské vztahy			
A.15.1 Bezpečnost informací v dodavatelských vztazích			
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	zavedeno	
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	později	
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	později	
A.15.2 Řízení dodávek služeb dodavatelů			
A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	zavedeno	
A.15.2.2	Řízení změn ve službách dodavatelů		
A.16 Řízení incidentů bezpečnosti informací			
A.16.1 Řízení incidentů bezpečnosti informací a zlepšování			
A.16.1.1	Odpovědnosti a postupy	zavést	4
A.16.1.2	Hlášení událostí bezpečnosti informací	zavést	2
A.16.1.3	Hlášení slabých míst bezpečnosti informací	zavést	2
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	zavést	6
A.16.1.5	Reakce na incidenty bezpečnosti informací	zavést	2
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	zavést	2
A.16.1.7	Shromažďování důkazů	později	
A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací			
A.17.1 Kontinuita bezpečnosti informací			
A. 17.1.1	Plánování kontinuity bezpečnosti informací	později	
A.17.1.2	Implementace kontinuity bezpečnosti informací	později	
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	později	
A.17.2 Redundance			
A.17.2.1	Dostupnost vybavení pro zpracování informací	zavedeno	
A.18 Soulad s požadavky			
A.18.1 Soulad s právními a smluvními požadavky			
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	později	
A.18.1.2	Ochrana duševního vlastnictví	zavedeno	
A.18.1.3	Ochrana záznamů		
A.18.1.4	Soukromí a ochrana osobních údajů	zavedeno	
A.18.1.5	Regulace kryptografických opatření		

A.18.2 Přezkoumání bezpečnosti informací			
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	později	
A.18.2.2	Shoda s bezpečnostními politikami a normami	později	
A.18.2.3	Přezkoumání technické shody	později	
Celkový počet hodin potřebný k zavedení v 1. etapě			138

Soubor opatření obsahuje celkem 114 jednotlivých opatření rozdělených do 14 oblastí. Společnost má v současné době 44 opatření zavedených, 33 bude zavedeno později, 19 nezavedených a 18 firma nebude zavádět.

Zavádění opatření navrhuji provést ve několika etapách. V první etapě navrhuji zavést opatření označena v tabulce 14 jako „zavést“, která jsou důležitá pro zvládání a pokrytí největších rizik, která nejsou akceptována a jsou nízkonákladová z dostupných zdrojů podniku. V další etapě navrhuji zavádět opatření s označením „později“, které je uvedeno u bezpečnostních opatření pro zvládání rizik střední úrovně. Opatření „zavedeno“ jsou ta, která jsou již zavedena a nepotřebují žádným způsobem modifikovat. V dalších etapách budou zavedeny opatření pro snížení všech rizik všech hrozeb na akceptovatelnou úroveň.

7.2 Etapa 1. jednotlivá opatření

V této kapitole jsou popsána a tedy navrhuji k zavedení opatření, která je potřeba zavést přednostně v první etapě zavádění, aby byla pokryta největší rizika.

A.5 Politiky bezpečnosti informací

Cílem je určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organizace, příslušnými zákony a směrnicemi.

Společnost má vypracovánu komplexní formální bezpečnostní politiku, ale je potřeba ji deklarovat a získat podporu managementu společnosti k ochraně informací.

Přezkoumání politik pro bezpečnost informací (A.5.1.2)

Dokument „Bezpečnostní politika organizace“ je stěžejním dokumentem v rámci zavádění systému řízení bezpečnosti informací. Zaměstnanci by měli být s tímto dokumentem opakovaně seznamováni. Vytvořenou bezpečnostní politiku je potřeba udržovat a pravidelně aktualizovat na základě výsledku periodických bezpečnostních revizí. Dále je nutné bezpečnostní politiku velmi důsledně prosazovat (vypracovat poučení pro uživatele, opakovaně

školit a dalšími prostředky zvyšovat úroveň povědomí zaměstnanců o bezpečnosti informací, kontrolovat dodržování předpisů a využívat kárná opatření). Je vhodné vypracovat plán vývoje, přezkoumání a vyhodnocování politik s periodicitou dvakrát ročně. Za každou přezkoumanou politiku odpovídá vlastník. Revidované politiky budou schvalovány managementem.

Potřebné zdroje pro přijmutí opatření:

Časové: Přezkoumání a revize bezpečnostní politik: 20 hodin.

Za zavedení odpovídá: Bezpečnostní ředitel.

A.6 Organizace bezpečnosti informací

Jejím cílem je řídit bezpečnost informací ve společnosti zřízením bezpečnostního fóra vedeného managementem společnosti, které by schvalovalo politiku bezpečnosti, definovalo odpovědnosti v oblasti bezpečnosti informací a koordinovalo implementaci bezpečnosti. Zároveň je nutné zachovávat bezpečnost zařízení pro zpracování informací a bezpečnost informačních aktiv, které jsou přístupné třetím stranám, a to i v případech, kdy byla odpovědnost za zpracování informací přenesena na jinou organizaci

Společnost nemá zřízeno bezpečnostní fórum, není jednoznačně definovaná osoba zodpovědná za bezpečnost informací v organizaci. Během analýzy bylo zjištěno, že některé uzavřené smluvní vztahy mezi podnikem a jejími obchodními partnery nezohledňují dostatečné problematiku bezpečnosti informací nebo ji vůbec neřeší.

Role a odpovědnosti bezpečnosti informací (A.6.1.1)

Navrhuji zřídit bezpečnostní fórum a jednoznačně definovat odpovědnosti v oblasti bezpečnosti informací určeným pracovníkům. Dále doporučuji zhodnotit rizika, která vyplývají z přístupu třetích stran a zavést potřebná bezpečnostní opatření a požadavky, které budou zohledněny ve smlouvách s daným partnerem. A dále doplnit odpovědnosti podrobnějšími pokyny pro specifická pracoviště.

Potřebné zdroje pro přijmutí opatření:

Finanční: Žádné.

Časové: 5 hodin.

Za zavedení odpovídá: Bezpečnostní ředitel, obchodní ředitel.

A.7 Bezpečnost lidských zdrojů

Cílem je snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace. Zajistit, aby si zaměstnanci (případně dodavatelé, třetí strany) byli vědomi bezpečnostních hrozeb a problému s nimi spjatých a byli připraveni se podílet na dodržování bezpečnostní politiky v průběhu své běžné práce.

Odpovědnosti managementu organizace (A.7.2.1)

Společnost má vypracovánu formální bezpečnostní politiku, ale role a odpovědnosti v oblasti bezpečnosti informací nejsou adekvátně popsány. Noví uchazeči o zaměstnání nejsou systematicky prověřováni (z hlediska trestního rejstříku, z hlediska referencí). Zaměstnanci jsou částečně proškolováni nadřízenými pracovníky i v oblasti bezpečnosti informací, přesný rozsah a zaměření školení však není formálně upraveno. Nejsou definována pravidla pro předávání informací o nově příchozích či odcházejících zaměstnancích mezi oddělením IT a personálním oddělením. V důsledku toho může nastat situace, že v systému zůstávají aktivní uživatelská oprávnění i pro zaměstnance, kteří už ve společnosti nepracují. Není zaveden postup disciplinárního řízení. Nejsou formálně a dostatečně popsány pravidla pro uživatele IT systému (např. pravidla pro používání e-mailu, Internetu, mobilních prostředků apod.).

Navrhuji aktualizovat bezpečnostní politiku a definovat role a odpovědnosti v oblasti bezpečnosti informací. Zároveň doporučuji formálně popsat pravidla, která by uživatelé IT systému měli dodržovat (např. pravidla pro používání emailu, internetu apod.). U pracovních pozic vyžadujících přístup k citlivým informacím by společnost měla provést prověrky spolehlivosti. Noví zaměstnanci by měli absolvovat školení zaměřené na bezpečnost informací (prováděné kompetentní osobou – např. bezpečnostním ředitelem) v předem připraveném a schváleném rozsahu. Účast na školení a akceptace bezpečnostních požadavku by mela být formálně potvrzena v příloze k pracovní smlouvě. Doporučuji rozšířit standardizované postupy pro nástupní a výstupní procedury zaměstnanců i na oblast bezpečnosti informací (např. kde a jak hlásit nástup nového zaměstnance, kde a jak hlásit ukončení jeho pracovního poměru, jaké další kroky následují v obou zmiňovaných případech a kdo je za ně odpovědný). Dále doporučuji zavést formální proces disciplinárního řízení a definovat sankce, které pro zaměstnance vyplývají z porušení bezpečnostních ustanovení. Vedení organizace dává tímto závazkem najevo svou vůli zajistit podporu (včetně finančních zdrojů) prosazení bezpečnosti informací v podniku. To znamená, že i vedení je povinno se všemi platnými

pravidly řídit a jasně tak ukazovat celé organizaci, že bezpečnost informací je důležitou součástí firemní kultury.

Potřebné zdroje pro přijmutí opatření:

Časová náročnost formulace závazku vedení směrem k bezpečnosti informací: 15 hodin.

Za zavedení odpovídá: Bezpečnostní ředitel, top management.

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

Na základě tohoto opatření absolvuje každý zaměstnanec společnosti, který při své práci využívá firemní výpočetní techniku, školení o používání výpočetní techniky, firemního programového vybavení, informační bezpečnosti a bezpečnostních rizicích, která hrozí při používání výpočetní techniky. Navrhuji sestavit program školení pro zvyšování povědomí v oblasti bezpečnosti informací. Je důležité, aby zaměstnanci pochopili cíl bezpečnosti informací a možný dopad na organizaci. Školení musí probíhat minimálně jedenkrát ročně. Cílem tohoto opatření je prohlubování bezpečnostního povědomí formou školení, seminářů či jiných vzdělávacích aktivit.

Potřebné zdroje pro přijmutí opatření:

Časový fond na roční školení: 18 hodin.

Za zavedení odpovídá Bezpečnostní ředitel, Personální oddělení.

A.8 Řízení aktiv

Společnost vede dle zákona účetní evidenci aktiv, podrobnější evidenci HW, SW a síťových prvků vede neformálně oddělení IT. Nejsou jednoznačně definovaní vlastníci aktiv. Společnost nemá vypracovánu směrnici pro klasifikaci informací, která by informace klasifikovala dle jejich důležitosti a stupně utajení a která by určovala, jak mají být tyto informace označovány a jak má s nimi být nakládáno. Jistá forma klasifikace, která vychází z ústně dohodnutých pravidel, jak s kterými informacemi zacházet, existuje, není však známá všem zaměstnancům a nedefinuje přesně, které informace podléhají jakému stupni utajení.

Klasifikace informací (A.8.2.1)

Doporučuji nastavit a udržovat přiměřenou ochranu aktiv organizace. Udržovat přiměřenou ochranu aktiv společnosti prostřednictvím přesné evidence. Společnost by měla mít vypra-

covánu směrnici pro klasifikaci informací, kterou by se měli všichni zaměstnanci, kteří přicházejí při výkonu svých funkcí s informacemi do styku. Protože informace může v průběhu roku ztrácet na významu, je nutné na konci roku provést revizi těchto klasifikací. Informace stačí rozdělit na tři úrovně, a to veřejné, citlivé a utajované.

Potřebné zdroje pro přijmutí opatření:

Časové: 15 hodin.

Za zavedení odpovídá Bezpečnostní ředitel, top management.

Označování informací (A.8.2.2)

Pro každé jednotlivé aktivum by měl být definovaný vlastník aktiva, který bude za dané aktivum zodpovědný. Aktiva by měla být ohodnocena dle důležitosti, kterou pro organizaci má (aby mohla být přijata relevantní bezpečnostní opatření). Zároveň by u každého aktiva mělo být uvedeno jeho současné umístění. Podobně je potřeba také identifikovat a roztřídit všechna informační aktiva (např. smlouvy s klienty, dodavateli, nabídky, projektová dokumentace, účetní data apod.) dle stupně jejich potřebnosti, důležitosti a ochrany. Vytvořením směrnice pro klasifikaci informací zavést pravidla, jak informace označovat, třídit, značit, uchovávat a likvidovat. Označení by mělo odpovídat schématu pro klasifikaci.

Potřebné zdroje pro přijmutí opatření:

Časové: 8 hodin.

Za zavedení odpovídá Bezpečnostní ředitel, top management.

A.9 Řízení přístupu

Řídit přístup k informacím, předcházet neoprávněnému přístupu k operacím systémům počítačům, sítím, informačním systémům. Zajistit bezpečnost informací při použití mobilní výpočetní techniky a při využití prostředků pro práci na dálku.

Politika řízení přístupu (A.9.1.1)

Společnost nemá vypracovanou politiku řízení přístupu. Při nástupu nového pracovníka je jeho přímým nadřízeným specifikován SW, ke kterému má mít daný pracovník přístup. Nelze vyloučit existenci zaměstnanců s nesprávně vydefinovanými přístupovými oprávněními. Neprobíhá pravidelná revize přístupových oprávnění. Nejsou definována formální pravidla při ukončení pracovního poměru zaměstnance, rušení uživatelských účtu probíhá spíše

náhodné bázi. Není definována politika zachování bezpečnosti při práci na mobilních zařízeních. Někteří uživatele používají ke své práci notebooky, které obsahují hodnotná data. Tato data nejsou adekvátním způsobem zabezpečena (např. použitím šifrování dat). Proces změny přístupových oprávnění (např. zapomenuté heslo) není formálně upraven (zřejmě bez ověřování identity uživatele).

Navrhuji vypracovat politiku řízení přístupu. Žádost o vytvoření, změnu či zrušení přístupových oprávnění by mela být formalizovaným procesem. Doporučuji zavést přístup k systémům na základě využívání uživatelských rolí a profilu. Politika řízení přístupu by měla definovat přístupové role pro běžné kategorie činností. Přístupová práva by měla být vázána především na pracovní pozice (role), a ne na konkrétní fyzické osoby. Tento přístup podstatně zjednodušuje správu přístupových práv. Navrhuji zavést postupy pro ověřování uživatelů v případě potřeby změny hesla. Pro práci na mobilních zařízeních by měly být popsány pravidla zachování bezpečnosti.

Uživatel by měl mít jen přístupy a práva k informacím, které nezbytně potřebuje pro svoji pracovní činnost, nebo dočasný přístup nebo právo pro vykonání úkolu, který mu byl svěřen.

Potřebné zdroje pro přijmutí opatření:

Časové: Vytvoření směrnice definující přístupové role skupin uživatelů 10 hodin.

Za zavedení odpovídá: Bezpečnostní ředitel, správce IT.

Přezkoumávání přístupových práv uživatelů (A.9.2.5)

Přístupová práva uživatelů je potřeba přezkoumávat v pravidelných intervalech, případně při změně pracovní pozice, nebo ukončení pracovního poměru konkrétního zaměstnance. Veškeré změny je nutno evidovat.

Potřebné zdroje pro přijmutí opatření:

Časové: Přezkoumání a revize přístupových práv 5 hodin.

Za zavedení odpovídá: Bezpečnostní ředitel, správce IT.

Bezpečné postupy přihlášení (A 9.4.2)

Přístup k systémům a aplikacím musí být řízen postupy bezpečného přihlášení.

Přístup do systému a aplikací musí být umožněn pouze na základě jednoznačné identifikace a autorizace pracovníků a to včetně přístupů třetích stran.

Potřebné zdroje pro přijmutí opatření:

Časové: 6 hodin.

Za zavedení odpovídá: Bezpečnostní ředitel, správce IT.

Správa uživatelských hesel (A.9.4.3)

Upravuje pravidla pro přidělování a správu hesel k pracovním stanicím a informačnímu systému. Uživatelé by měli před prvním přihlášením obdržet jedinečné, náhodně vygenerované heslo (dlouhé minimálně 8 znaků, složité, a přitom snadno zapamatovatelné, mělo by obsahovat velká a malá písmena, čísla a speciální znaky), které jsou povinni ihned po přihlášení změnit a zvolit vlastní heslo. Zaměstnancům musí být předána bezpečným způsobem, ne pomocí elektronické pošty.

Potřebné zdroje pro přijmutí opatření:

Časové: 4 hodin.

Za zavedení odpovídá: Bezpečnostní ředitel, správce IT.

A.12 Bezpečnost provozu

Cílem těchto politik je zajištění správného a bezpečného provozování vybavení pro zpracování dat.

Dokumentace provozních postupů (A.12.1.1)

Provozní postupy musí být řádně dokumentovány a být k dispozici všem uživatelům. Musí být zpracovány dokumentované postupy pro ovládání počítače, zálohování, monitorování, údržba zařízení, zacházení s médii, správa počítačové místnosti, zacházení s emailem, archivace a bezpečnost práce.

Potřebné zdroje pro přijmutí opatření:

Časové: 4 hodin.

Za zavedení odpovídá: Správce IT.

Zaznamenávání událostí formou logů (A.12.4.1)

Musí být pořizovány a pravidelně přezkoumávány záznamy událostí formou logů zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.

Potřebné zdroje pro přijmutí opatření:

Finanční: HW pro uchovávání dat, logů 30 000,- Kč.

Časové: 4 hodin.

Za zavedení odpovídá: Bezpečnostní ředitel, správce IT.

Logy o činnosti administrátorů a operátorů (A.12.4.3)

Pořízené záznamy formou logů by neměli mít oprávnění ani správci systému měnit nebo mazat záznamy o svých vlastních aktivitách. Doporučuji realizovat toto opatření pomocí stávajících prostředků podporujících zaznamenávání činností formou logů.

Potřebné zdroje pro přijmutí opatření:

Časové: 6 hodin.

Za zavedení odpovídá: Bezpečnostní ředitel, správce IT.

A.16 Řízení incidentů bezpečnosti informací

Cílem je minimalizovat škody způsobené bezpečnostními incidenty a selháními, a sledovat je a učit se z nich. Bezpečnostním incidentem se rozumí událost, která přímo nebo nepřímo může vést k narušení bezpečnosti informací z pohledu dostupnosti, integrity a důvěrnosti.

Ve společnosti je vytvořen formální systém helpdesku, který umožňuje evidovat požadavky, bezpečnostní incidenty a zranitelnosti. Neexistuje však formální postup pro hlášení incidentu a zranitelností, který by určoval, co je bezpečnostní incident, co je zranitelnost a jak tyto problémy hlásit. Vyhodnocování incidentů probíhá jen okrajově a nepravidelně. Systémové logy nejsou systematicky procházeny.

Navrhuji zavést směrnici pro hlášení bezpečnostních incidentů a zranitelností, která bude specifikovat, co je bezpečnostní incident a co zranitelnost a jak tyto problémy hlásit. Zároveň doporučuji pravidelně vyhodnocovat bezpečnostní incidenty a systémové logy a dostatečné dlouhou dobu je archivovat pro potřeby důkazního řízení.

Odpovědnosti a postupy (A.16.1.1)

Je potřeba vypracovat a zavést směrnici s postupy pro plánování a přípravu reakce na bezpečnostní incidenty, pro monitorování, detekci a analýzu incidentů, pro zaznamenání a řízení incidentů formou logů, pro zacházení s forenzními důkazy.

Určit osobu, která bude přijímat hlášené incidenty, zaznamenávat a postupovat dle vypracované směrnice.

Potřebné zdroje pro přijmutí opatření:

Časové: 4 hodin.

Za zavedení odpovídá: Bezpečnostní ředitel.

Hlášení událostí bezpečnosti informací (A16.1.2)

Cílem je dosáhnutí rychlého hlášení událostí bezpečnosti informací ze strany všech zaměstnanců a partnerů. Určená osobu, která bude přijímat hlášené incidenty musí postupovat podle standardizovaných předpisů, aby nebyla ohrožena bezpečnost systému.

Potřebné zdroje pro přijmutí opatření:

Časové: 2 hodiny.

Za zavedení odpovídá: Bezpečnostní ředitel.

Hlášení slabých místech bezpečnosti informací (A.16.1.3)

Všichni zaměstnanci a partneři musí být proškoleni a musí jim být zdůrazněna povinnost hlásit všechny slabá místa bezpečnosti informací. Vytvořené kontaktní místo pro tyto informace by mělo zjednodušit a zrychlit podávání zpráv.

Potřebné zdroje pro přijmutí opatření:

Časové: 2 hodiny.

Za zavedení odpovídá: Bezpečnostní ředitel.

Posuzování a rozhodování o událostech bezpečností informací (A.16.1.4)

Bezpečnostní incidenty i domnělé musí být nejen hlášeny, ale pravidelně řešeny. Pokud bude vyhodnoceno, že se jedná o bezpečnostní incident musí se rozhodnout jaký má dopad na organizaci. Všechny výsledky řešení událostí se musí podrobně zaznamenat.

Potřebné zdroje pro přijmutí opatření:

Časové: 6 hodiny.

Za zavedení odpovídá: Bezpečnostní ředitel.

Reakce na incidenty bezpečnosti informací (A.16.1.5)

Doporučuji vypracovat postup, jak reagovat na incidenty bezpečnosti informací. Kontaktní místo, helpdesk musí postupovat podle tohoto dokumentu a zaznamenat důkazy bezprostředně po nahlášení incidentu, přesný postup co a jak zaznamenat musí byt nadefinován krok po kroku. Incident by měl být ihned vyřešen nebo se použije náhradní řešení a incident musí být vyřešen.

Potřebné zdroje pro přijmutí opatření:

Časové: 2 hodiny.

Za zavedení odpovídá: Bezpečnostní ředitel, správce IT.

Ponaučení z incidentů bezpečnosti informací (A.16.1.6)

Zajistit soulad všech postupů, oblastí a systémů s definovanými bezpečnostními politikami a směrnicemi. Z vyhodnocených incidentů použít řešení a analýzy. Tyto znalosti pomáhají k identifikaci opakujících se incidentů a incidentů s velkým dopadem. Události, které předcházely incidentům bezpečnosti informací a jsou zdokumentovány, mohou sloužit jako podklad pro proškolování zaměstnanců. Musí se posoudit zda je nutné upravit nebo zpracovat nové preventivní opatření a implementovat ho do směrnic.

Potřebné zdroje pro přijmutí opatření:

Časové: 2 hodiny.

Za zavedení odpovídá: Bezpečnostní ředitel, správce IT.

Doporučuji přijmout jednoho bezpečnostního/IT pracovníka, který bude vytvářet potřebné povědomí u zaměstnanců o závažnosti a významu činností v rámci bezpečnosti informací.

7.2.1 Zdroje a náklady na 1.etapu

V 1. etapě jsou zavedeny požadavky podle normy ČSN ISO/IEC 27001. Celkový součet hodin, který je potřeba pro zavedení ISMS je vyčíslen na 138 hodin. Dále je potřeba před zahájením sestavit realizační tým a zodpovědnou osobu za implementaci a všechny dostatečně proškolit. Na školení je stanoveno 15 hodin. Pro monitoring a přezkoumávání politik je počítáno s 20 hod/rok. Hodinová sazba byla stanovena 500,- Kč/hod bez DPH. Mzdové náklady na 1 nového pracovníka (30 000,- x 12 měsíců) tj. 360 000,- Kč.

Tab. 15 Sumarizace nákladů pro 1. etapu., Mičulková 2018

	Jednorázové náklady	**Každoroční náklady**
Zavedení opatření	69 000 Kč	29 000 Kč
Vstupní školení	7 500 Kč	
Nákup HW	30 000 Kč	
Nový pracovník		360 000 Kč

7.2.2 Časový plán zavedení opatření

Celkový čas na zavedení 1.etapy je rozvržen do třech měsíců.

Rozdělení všech opatření proběhne v časových etapách podle následujícího rozdělení:

Etapa 1 – září 2018 – listopad 2018 – opatření A.5 Politiky bezpečnosti informací, A.6 Organizace bezpečnosti informací, A.7 Bezpečnost lidských zdrojů, A.8 Řízení aktiv, A.9 Řízení přístupu, A.12 Bezpečnost provozu, A.16 Řízení incidentů bezpečnosti informací

Etapa 2 – prosinec 2018 – únor 2019 – opatření A.6 Organizace bezpečnosti informací, A.7 Bezpečnost lidských zdrojů, A.8 Řízení aktiv, A.10 Kryptografie, A.12 Bezpečnost provozu, A.13 Bezpečnost komunikací, A.14 Akvizice, vývoj a údržba systémů, A.15 Dodavatelské vztahy, A.16 Řízení incidentů bezpečnosti informací, A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací, A.18 Soulad s požadavky

Etapa 3 – březen 2019 – duben 2019 Průběžné školení, aktualizace směrnic, ostatní opatření, která nebyla z časových důvodů dosud přijata, prohlášení o aplikovatelnosti.

Tab. 16 Časový plán implementace opatření, Mičulková 2018

	Roky 2018-2019																																					
	Týden																																							
Etapa 1.	35.	36.	37.	38.	39.	40.	41.	42.	43.	44.	45.	46.	47.																										
Etapa 2.														48	49.	50.	51.	52.	1.	2.	3.	4.	5.	6.	7.	8.													
Etapa 3.																											9	10.	11.	12.	13.	14.	15.	16.	17.				

Jednotlivá opatření budou v podniku zaváděna dle etap a průběžně. Během 8 měsíců by měl proběhnout celý ISMS cyklus, včetně vyhodnocení slabých míst a návrhů na zlepšení.

Tab. 17 Opatření pro omezení rizika z hrozeb, Mičulková 2018

Poř.č.	Hrozba	Opatření
1	Zemětřesení	
2	Povodně	
3	Hurikán / Přívalový déšť	
4	Blesk	
5	Průmyslová akce	
6	Nedostatečná ochrana vnějšího perimetru / krádež	
7	Použití zbraní / bomby	
8	Škoda způsobená průnikem neoprávněné osoby	Řeší opatření A.9.1.1, A.9.4.2, A.9.4.3
9	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Řeší opatření A.7.2.1, A.6.1.1
10	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	Řeší opatření A.7.2.2
11	Provedení neoprávněných činností	Řeší opatření A.9.1.1
12	Zneužití oprávnění ze strany uživatelů	Řeší opatření A.9.1.1
13	Zneužití oprávnění ze strany administrátorů	Řeší opatření A.9.1.1
14	Zneužití identity jiné fyzické osoby	Řeší opatření A.9.1.1, A.9.4.2, A.9.4.3
15	Zneužití nebo modifikace údajů	
16	Zneužití vnitřních prostředků, sabotáž	
17	Užívání software v rozporu s licenčními podmínkami	Řeší opatření A.6.1.1, A.9.1.1
18	Pochybení ze strany zaměstnanců a neschopnost jeho včasného odhalení	
19	Zneužití vyměnitelných paměťových médií	
20	Odcizení nebo poškození aktiva	
21	Poškození, nebo selhání technického, nebo programového vybavení	
22	Škodlivý kód (např. viry, spyware, trojské koně)	Řeší opatření A.16.1.1 - A.16.1.6
23	Nedostatky při poskytování služeb informačního systému	
24	Přerušení dodávky komunikačních služeb nebo elektrické energie	
25	Nedostatečná údržba	
26	Chyba údržby informačního systému	
27	Kybernetický útok z vnější komunikační sítě	Řeší opatření A.12.4.1, A.16.1.5
28	Kybernetický útok z vnitřní sítě	Řeší opatření A.12.4.1, A.16.1.5
29	Cílený kybernetický útok (pomocí sociálního inženýrství, použití špionážních technik)	Řeší opatření A.12.4.1, A.16.1.5
30	Nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů	Řeší opatření A.6.1.1
31	Nepřesné nebo nejednoznačné vymezení práv a povinností administrátorů	Řeší opatření A.6.1.1
32	Nepřesné nebo nejednoznačné vymezení práv a povinností bezpečnostních rolí	Řeší opatření A.6.1.1
33	Nevhodné nastavení přístupových oprávnění	Řeší opatření A.6.1.1., A.9.1.1, A.9.2.5
34	Nedostatečné postupy při identifikování a ošetřování bezpečnostních událostí a incidentů	Řeší opatření A.16.1.1 - A.16.1.6
35	Nedostatečné monitorování činnosti uživatelů	Řeší opatření A.12.4.1
36	Nedostatečné monitorování činnosti administrátorů	Řeší opatření A.12.4.3

37	Nevhodná bezpečnostní architektura	
38	Nedostatečná míra nezávislé kontroly	Řeší opatření A.5.1.2

Z identifikovaných 38 hrozeb se po zavedení 1. etapy snížilo riziko z identifikovaných hrozeb na akceptovatelnou úroveň celkem v 20 případech.

ZÁVĚR

Cílem této práce bylo navrhnout optimalizaci procesů systému řízení bezpečnosti informací podle normy ČSN ISO/IEC 27001.

V teoretické části jsou popsány základní pojmy z oblasti bezpečnosti informací, zákony a normy související s touto oblastí a pospány přístupy, metody a postup analýzy rizik.

V další části je představena analyzovaná společnost, její cíle, politika a oblast managementu bezpečnosti informací.

V praktické části je na základě teoretických podkladů navrhnuta a popsána metodika zpracování analýzy rizik konkrétního výrobního podniku. Byla identifikována aktiva a hrozby a provedeno jejich ohodnocení. Dalším krokem bylo sestavení matice zranitelnosti a matice rizik.

Provedenou analýzou rizik byla vyhodnocena aktuální rizika, kterým je tato společnost vystavena a současně doporučeno zavádění navržených opatření za účelem snížení rizik a ochrany identifikovaných aktiv.

Realizace bezpečnostních opatření závisí především na možnostech a zdrojích, které je podnik schopen a ochoten poskytnout na řešení bezpečnosti. Zajištění bezpečnosti není hlavním posláním společnosti, ale je potřeba si uvědomit, že informace jsou nejdůležitějším nástrojem plnění úkolů ve firmě a tomu by měla také odpovídat pozornost a zdroje, které vedení na zajištění bezpečnosti svých informací poskytne.

Provedená analýza rizik a její závěry poskytují aktualizované informace k zajištění bezpečnosti svých informací. Doporučuji nezavádět všechna vybraná opatření najednou. Vhodné je nejprve zavést opatření uvedená v 1. etapě pro eliminaci zjištěných hrozeb a následně zavádět další opatření. Bezpečnost dat i ostatních firemních aktiv bude po zavedení opatření vysoká a opatření budou bránit útočníkům v získání důvěrných dat a zvýší se tím informační bezpečnost.

SEZNAM POUŽITÉ LITERATURY

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

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

[3] NENADÁL, Jaroslav. *Moderní management jakosti: principy, postupy, metody*. Praha: Management Press, 2008. ISBN 978-80-7261186-7.

[4] DRASTICH, Martin. *Systém managementu bezpečnosti informací*. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9.

[5] *ČSN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.* Praha: Český normalizační institut, 2014.

[6] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-05-7.

[7] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-19-4.

[8] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-67-5.

[9] *Slovník spisovné češtiny pro školu a veřejnost: Dodatkem Ministerstva školství, mládeže a tělovýchovy České republiky*. Vyd. 3., rev. Editor Vladimír MEJSTŘÍK. Praha: Academia, 2003. ISBN 978-80-20010-80-3.

[10] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.

[11] STRNÁD, O. *Systémový prístup k riadeniu informačnej bezpečnosti.* 1. vyd. Trnava (Slovensko): SP Synergia, 2008. 233 s. ISBN 978-80-89291-20-5.

[12] *ČSN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. Praha: Český normalizační institut, 2014.

[13] STAUDEK, J. Úvod do problematiky bezpečnosti IT. 3. [online]. FI MU Brno, verze podzim 2007. [cit. 2016-04-20]. URL: http://www.fi.muni.cz/usr/staudek/vyuka.

[14] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009. Knihovnicka.cz. ISBN 978-80-7399-731-1.

[15] ČERMÁK, Miroslav. *Clever and smart* [online]. 2012 [cit. 2018-03-24]. Informační bezpečnost: životní cyklus informace. Dostupné z WWW: <http://www.cleverand-smart.cz/informacni-bezpecnost-zivotni-cyklusinformace/>.

[16] ČESKO. Předpis č. 316/2014 Sb.: Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů ČR*. [Praha], 2014, ročník 2014, 127/2014.

[17] *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).* In: Brusel, 2016.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CL	Check list.
ČR	Česká republika.
ČSN	Česká technická norma.
ETA	Event Tree Analysis.
HAZOP	Hazard and Operability Study.
EU	Evropská unie.
HP	Hewlett-Packard.
HW	Hardware.
ICT	Informační a komunikační technologie.
IEC	Mezinárodní elektrotechnická komise.
IS	Informační systém.
ISMS	Information Security Management System.
ISO	International Organization for Standardization.
IT	Informační technologie.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost.
OS	Operační systém.
PDCA	Plan-do-check-act metoda.
RR	Relative Ranking.
SR	Safety Review.
SW	Software.
UPS	Uninterruptible Power Supply.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH