Analýzy rizik s ohledem na ISO 27 000

Radek Valenta

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

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

Jméno a příjmení:	**Radek Valenta**
Osobní číslo:	**A16054**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Analýzy rizik s ohledem na ISO 27 000**
Téma anglicky:	**Risk Analysis with Respect to ISO 27 000**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Vysvětlete základní pojmy, jako jsou hrozba a riziko.**
3. **Popište jednotlivé fáze a metody analýzy rizik.**
4. **Vysvětlete, co je systém řízení bezpečnosti informací a související standardy.**
5. **Proveďte analýzu rizik v konkrétní společnosti s ohledem na ISO 27 000.**
6. **Výsledky konzultujte s vedením firmy.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. In: 75/2014. 2014. Dostupné z: http://www.zakonyprolidi.cz/cs/2014-181.**
2. **HOFREITER, Ladislav, LOVEČEK, Tomáš, VEĽ AS, Andrej. Zásady a princípy analýzy rizík v oblasti fyzickej a objektovej bezpečnosti, Žilinská univerzita v Žiline, Fakulta špeciálneho inžinierstva, Žilina, 2006,.**
3. **SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. 483 s.Expert.**
4. **DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.**
5. **ČSN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 25 s.**
6. **ŠEFČÍK, Vladimír. Analýza rizik. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-696-8.**

Vedoucí bakalářské práce: **Ing. Lukáš Králík**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **20. prosince 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 20. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské 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 bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších 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/bakalářskou 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 bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Předmětem této bakalářské práce je vypracování analýzy rizik v konkrétní společnosti s ohledem na řadu norem ISO/IEC 27000. Teoretická část slouží pro objasnění problematiky analýzy rizik, představení pojmů a postupů při vypracování analýzy rizik. Následně poté objasněno co je to systém řízení bezpečnosti informací a jaké jsou jeho fáze. Praktická část se zabývá již samotnou analýzou rizik, která je vypracována v konkrétní reálné společnosti. Je představen postup samotné analýzy rizik, který na sebe postupně navazuje a jsou tak získány jednotlivé parametry pro výpočty daných rizik. Veškeré výpočty jsou prováděny v softwaru Microsoft Excel. Následně poté je věnován prostor pro konzultaci výsledků analýzy rizik s vedením společnosti a vyjmenováním opatření, které daná firma využívá pro snižování daných rizik. Závěr práce je doplněn o závěrečné doporučení tří možností, které by mohly vést ke zlepšení informační bezpečnosti v dané firmě.

Klíčová slova: analýza rizik, systém řízení bezpečnosti informací, informační bezpečnost, bezpečnost informací, hrozba, aktivum, riziko

ABSTRACT

This bachelor thesis focuses on elaborating a risk analysis of a particular company with respect to ISO/IEC 27000 standards. The theoretical part focuses on claryfiing the problematics of the risk analysis, its conception and the process of its elaborating. Henceforth, it is said what the information security management system and its phases are. The practical part focuses on the risk analysis itself that is elaborated in an actual, real company. The risk analysis process, by which individual parametres for calculations of the risks are secured, is set for individual calculations. All calculations are made in the Microsoft Excel software. Moreover, the thesis focus on discussion with company's headquarters about the outcomes of the risk analysis and also about provisions that the company uses for the risk reduction. The conclusion of the thesis is added by the recommendations of three possibilities that can lead to an improvement of security in the company.

Keywords: risk analysis, information security management system, information security, threat, asset, risk

Mé velké poděkování patří mému vedoucímu práce, panu Ing. Lukáši Králíkovi, za veškeré rady a konzultace, které mi během psaní mé bakalářské práce poskytl.

Dále pak bych chtěl poděkovat lidem ze společnosti, kteří mi poskytli možnost a prostor pro vypracování mé bakalářské práce.

V neposlední řadě děkuji mé rodině, která mi byla vždy na blízku po čas mého studia a vypracování bakalářské práce.

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

„Chcete-li vybudovat velký podnik, vybudujte nejdříve sebe.“

Tomáš Baťa

OBSAH

ÚVOD

Analýza rizik je v procesu řízení rizik naprosto neoddělitelnou součástí, která dává úspěšný předpoklad k tomu, aby řízení rizik mohlo probíhat co nejefektivněji. Analýza je vlastně dekompozice konkrétního celku na jednotlivé části, kde se zjišťují a identifikují tyto konkrétní části, vztahy mezi nimi, jejich uspořádání, kombinace, či jiné možnosti. Tato definice se zdá, ale poněkud příliš obecná, je totiž důležité si říct, co konkrétního je třeba analyzovat. Proto pokud dojde ke spojení dvou slov „analýza“ a „riziko“, vzniká slovní spojení analýza rizik. Analýza rizik je tedy identifikování několika dílčích částí, které s rizikem úzce souvisí a vymezení si vztahů mezi nimi. Těmito dílčími částmi, neboli pojmy, jsou zejména aktiva a hrozby. Tam kde dochází ke střetu aktiva a hrozby, vzniká riziko. Riziko lze tedy chápat jako míru ohrožení, že dojde k uplatnění dané hrozby na konkrétním aktivu. S tím poté dále souvisí další pojmy, které se v analýze rizik dále objevují, jako jsou například zranitelnost či protiopatření. Při spojení všech těchto pojmů dohromady dochází ke vzniku vztahů mezi těmito pojmy, které se přímo navzájem ovlivňují.

Analýza rizik se může uplatnit takřka ve všech oblastech a zaměřeních, jelikož metod a způsobů, jak lze analýzu rizik provádět je celá řada. Vypracováním takové analýzy rizik je možné získat základní přehled o daných hrozbách, konkrétních aktivech a nakonec i samotných rizicích. Výsledky, které se získají při provádění analýzy rizik, je možné využít při procesu tzv. snižování rizik.

Cílem této bakalářské práce je provést samotnou analýzu rizik v konkrétní společnosti s ohledem na řadu norem ISO/IEC 27000, jenž jsou základním předpokladem pro úspěšné řízení bezpečnosti informací ve firmě. Provedením analýzy rizik získá daná firmy podklady, které může využít při dalším postupu certifikace nebo může využít tyto podklady v rámci získávání nových potencionálních zákazníků, jenž zajímá jakým způsobem daná firma nakládá s bezpečností informací. Čtenář se tak seznámí s problematikou analýzy rizik, systémem řízení bezpečnosti informací či dalších souvisejících nařízeních, které vstupují do této problematiky.

I. TEORETICKÁ ČÁST

1 DEFINICE POJMŮ V ANALÝZE RIZIK

Pro správné pochopení analýzy rizik je nutné si nejprve představit pojmy, které jsou pro analýzu rizik klíčové. V této kapitole proto budou uvedeny a představeny pojmy analýzy rizik, kterými jsou aktivum, hrozba, zranitelnost, riziko a protiopatření. Znalost základní terminologie v oblasti analýzy rizik dává kladné předpoklady k tomu, že daná analýza rizik bude úspěšně realizována.

1.1 Aktivum

Prvním pojmem, který zde bude zmíněn, je aktivum (assets, v anglickém překladu). Aktivem se dá rozumět vše, co pro danou firmu či organizaci představuje nějakou hodnotu. Hodnota tohoto aktiva může být zmenšena působením hrozby. Z hlediska dělení se aktivum dělí na dva typy:

- Hmotná aktiva,
- Nehmotná aktiva. [1] [2] [3]

Do hmotných aktiv lze zařadit zejména nemovitosti, cenné papíry, peníze nebo například technické prostředky výpočetní techniky. U technických prostředků lze nalézt počítač, modemy, aktivní prvky počítačové sítě, kabelové rozvody, tiskárny a další jiné zařízení. Druhým typem aktiv jsou aktiva nehmotná, kde patří například:

- Pracovní postupy, Know-how.
- Data.
    - Datové soubory (vytvořené nebo převzaté).
- Softwarové vybavení.
    - Operační systémy, grafické programy, výpočetní aplikace apod.
- Služby.
    - Počítačové a komunikační služby. [1] [4]

Hodnota aktiva je jednou z hlavních vlastností aktiva. Tato hodnota je založena na objektivním vyjádření obecně vnímané ceny nebo může být založena na subjektivním ocenění důležitosti (kritičnosti) aktiva pro danou organizaci či například i samotnou kombinací obou uvedených přístupů. Hodnotu aktiva lze tedy brát jako relativní, neboť záleží na samotném úhlu pohledu při jeho hodnocení. [1] [2]

U hodnocení aktiv se bere ohled na následující hlediska:

- Celkové pořizovací náklady (či jiná hodnota aktiva).
- Význam aktiva a jeho důležitost pro existenci a chod organizace.
- Náklady na překonání případné újmy na aktivu.
- Rychlost odstranění újmy na aktivu.
- Ostatní hlediska (liší se případ od případu). [1]

1.2 Hrozba

Hrozba (threat, v anglickém překladu) je jeden z dalších pojmů, jenž velmi úzce souvisí s analýzou rizik. Hrozbu lze definovat jako událost, aktivitu, sílu nebo například osobu, která svým působením ohrožuje bezpečnost a může způsobit škodu určitému aktivu. Mezi hrozby lze zařadit například krádež zařízení, požár, přírodní katastrofa, získání přístupu k informacím neoprávněnou osobou či například chyba obsluhy. Vlastností hrozby je poté dopad hrozby, což může být definováno jako škoda, kterou způsobí hrozba při působení na aktivum. Dopad hrozby je možné odvodit od absolutní hodnoty ztrát, kde jsou zahrnuty náklady na znovuobnovení aktiva nebo náklady na odstranění následků vzniklých škod. [1] [2] [3]

Hrozby mohou nabývat rozdílných úrovní. Jedná se tak o vlastnost hrozby, kde úroveň se vyhodnocuje podle jednotlivých faktorů:

- Nebezpečnost.
- Přístup.
- Motivace.

Kde nebezpečnost je způsobilost hrozby páchat škodu na konkrétním aktivu. Druhým faktorem je přístup, který je definován jako pravděpodobnost, že hrozba se svou působností dostane k aktivu a získá tak němu přístup. Jeho další formou poté může být například i frekvence výskytu hrozby. Třetím faktorem je motivace, kterou lze chápat jako zájem o vyvolání hrozby vůči aktivu. [1] [2]

Hrozby se dále mohou dělit do několika kategorií:

- Přírodní a fyzické.
- Technické a technologické.

- Lidské.
    - Neúmyslné.
    - Úmyslné.
        - Zvenku systému.
        - Zevnitř systému. [4]

Do přírodních a fyzických hrozeb patří zejména živelné pohromy a nehody způsobené například poruchou dodávky elektrického proudu, vznik požáru, povodně, hurikánů, vichřice apod. Mezi technické a technologické hrozby patří hlavně poruchy nosičů dat, poruchy na sítích, poruchy způsobených daným programem (nedostatečné otestování programového vybavení, viry, trojské koně a jiné). [2] [4]

Specifickou hrozbou jsou poté hrozby lidské, které se dále dělí na úmyslné a neúmyslné. Neúmyslné hrozby většinou vznikají z důvodu neznalosti nebo zanedbání plnění povinností. Úmyslné hrozby jsou dále děleny podle dvojího charakteru, buď zvenku systému nebo zevnitř systému. Zvenku systému se tak může jednat o hackerské útoky, teroristické útoky či mezifiremní špionáže a další jiné. Zevnitř systému se může jednat o útoky například nespokojených zaměstnanců nebo například hostů a návštěvníků organizace a podobně. Většina hrozeb, které poškodí informační systém a informační komunikační technologie (dále jen IS/ICT) patří do kategorie neúmyslných hrozeb (více než 50 %). Podobnou situaci lze nalézt taky u hrozeb zevnitř organizace, kde podíl hrozeb je daleko větší než u hrozeb, které pochází z vnějšku organizace. Z hlediska statistiky až 98 % incidentů bývá způsobeno uvnitř organizace, kde nejčastějším důvodem může být neznalost pracovníku v oblasti bezpečnosti IS/ICT. [2] [4]

V oblasti informačních aktiv se tak lze setkat se základními hrozbami, kde patří neoprávněné, náhodné či úmyslné:

- Prozrazení.
    - Prozrazení interních informací dané organizace.
    - Vyzrazení dat neoprávněným uživatelem (náhodný nebo úmyslný způsob).
- Upravení.
    - Narušení integrity (zajištění správnosti a úplnosti informací, více v kapitole 4) dat neoprávněným uživatelem (náhodný nebo úmyslný způsob).

- Zničení.
    - Dochází k zničení dat systému neoprávněným uživatelem (náhodný nebo úmyslný způsob). [4]
- Bránění.
    - Bránění v dostupnosti dat, zdrojů či služeb IS oprávněným uživatelům. [4]

1.3 Riziko

Pojem riziko (risk, v anglickém překladu) představuje určitou míru ohrožení či míru nebezpečí daného aktiva, že dojde k uplatnění hrozby a vyvolání tak nežádoucích následků, které vedou ke vzniku škody. Riziko vzniká všude tam, kde dochází k vzájemnému působení hrozby a aktiva. [1] [2] [3]

Hrozby, které svým působením nepůsobí na žádné aktivum, by neměly být brány v úvahu při analýze rizik.

Obr. 1: Vznik rizika

Jsou-li zde aktiva, na které nepůsobí žádné hrozby, tak tyto aktiva nejsou dále předmětem analýzy rizik. U rizik se lze setkat s dalšími vlastnostmi či pojmy, jako jsou úroveň rizika, zbytkové riziko nebo referenční úroveň. Úroveň rizika bývá definována hodnotou daného aktiva, jeho zranitelností a samotnou úrovní hrozby. Snižování úrovně rizika lze dosáhnout pomocí daného protiopatření, kde náklady při návrhu protiopatření musí být přiměřené hodnotě chráněných aktiv (či hodnotě škod, které vzniknou dopadem hrozby). [1] [2]

Při analýze rizik se dále počítá i se zbytkovým rizikem, což je takové riziko, které díky své malé velikosti nepřesáhne danou referenční úroveň, a proto není pro daný subjekt dále podstatné a není proto třeba navrhovat další protiopatření na snižování tohoto rizika. Aby bylo možné oddělit zbytková rizika od ostatních podstatných rizik, musí zde existovat určitá referenční úroveň. Tato referenční úroveň je hranicí míry rizika, která stanovuje hodnotu velikosti rizika a rozhoduje o tom, či je dané riziko zbytkové (riziko menší než referenční úroveň) nebo není (riziko větší než referenční úroveň). Při stanovení referenční úrovně se musí brát v úvahu to, aby dopad hrozby byl co nejmenší a bylo možné jej zanedbat. [1] [2]

1.4 Zranitelnost

Dalším důležitým pojmem, který zde bude definován, je zranitelnost (vulnerability, v anglickém překladu). Zranitelnost si lze představit jako nedostatek, slabinu či stav daného aktiva, který může hrozba využít a ohrozit tak dané aktivum svým nežádoucím vlivem. Zranitelnost je tedy samotnou vlastností aktiva a udává, jak moc je aktivum citlivé na působení konkrétní hrozby. Vzniká všude tam, kde přichází aktivum ke kontaktu s hrozbou. Zranitelnost se dále dá dělit pomocí její úrovně, kde úroveň zranitelnosti daného aktiva se klasifikuje podle následujících okolností:

- Citlivost.
- Kritičnost.

Kde citlivost lze popsat jako náchylnost aktiva být poškozeno danou hrozbou a kritičnost je důležitost daného aktiva pro analyzovanou organizaci. [1] [2] [3]

Zranitelnost lze dále dělit na:

- Fyzickou.
    - Budovy či počítačové místnosti (oblast působnosti bezpečnosti organizace).
- Technických a programových prostředků.
    - Nejčastěji se projevují buď poruchou či chybou.
- Nosičů dat.
    - Může se jednat o selhání nosiče dat či jeho nečitelnost.
- Elektromagnetických zařízení.
    - Může se jednat o smazání obsahu nosiče dat, pokud se dostane do styku s intenzivním magnetickým polem.
- Komunikačních systémů a kabelových rozvodů.
    - Možnosti odposlechu či přerušení.
- Personální.
    - Úmyslné či neúmyslné chování osob. [4]

1.5 Protiopatření

Protiopatření nebo jen opatření (control, v anglickém překladu) je speciálně navrženo tak, aby snížilo působení hrozby či úplně eliminovalo hrozbu a zmírnilo tak zranitelnost nebo dopad dané hrozby. Protiopatřením tak může být například proces, postup, procedura,

technický prostředek či cokoliv jiného co by vedlo ke zmírnění hrozby a podobně. Při samotném návrhu daného protiopatření se klade důraz na předejití vzniku škody nebo usnadnění překonání následků vzniklé škody. Protiopatření má dále své další dělení z hlediska analýzy rizik. Prvním zmíněným je efektivita daného protiopatření a druhým zmíněným jsou náklady. Pojem efektivita udává, jak moc dané protiopatření je schopno snížit účinek hrozby. Efektivita bývá často využívána ve fázi zvládání rizik, kde je jako jeden z hlavních parametrů hodnocení vhodnosti použití daného protiopatření. Mezi náklady jsou nejčastěji započítávány náklady na pořízení daného protiopatření, jeho zavedení a následný provoz. Výběr samotného protiopatření tak bývá zohledněn právě na těchto dvou důležitých parametrech, kde se hledá nejúčinnější protiopatření a na jeho realizaci budou vynaloženy co nejmenší náklady. [1] [2] [3]

I zde u protiopatření dochází k dělení, kde je protiopatření děleno buď podle charakteru nebo podle sledovaného cíle. Dělení podle charakteru je následující:

- Administrativní.
    - Mezi tato protiopatření patří zejména směrnice pro práci s IS/ICT v organizaci a jiné.
- Fyzické.
    - Mezi tato protiopatření patří použití zámků, trezorů pro kopie dat, čipové karty pro přístup do tzv. režimových prostorů.
- Technické a technologické.
    - Mezi tato protiopatření patří například autorizace a autentizace přístupu uživatelů do IS/ICT, kde se nachází aktiva organizace (ochranou do systému se rozumí například využití přístupových hesel). [4]

Dělení podle sledovaného cíle je buď:

- Prevenční.
    - Cílem je minimalizovat rizika už předem (například automatické odhlášení uživatele při nečinnosti nebo automatické zavírání dveří a podobně).
- Detekční.
    - Cílem je odhalovat potencionální problémy a hrozby (například pravidelné vyhodnocování logovacích a auditních záznamů s možností identifikace bezpečnostních incidentů a jeho případným vyhlášením poplachu a podobně).

- Korekční.
    - Cílem je zajistit následnou minimalizaci dopadů, kdy daná hrozba již proběhla (například odstranění virů z napadených souborů). [4]

1.6 Kybernetické útoky

Kybernetické útoky patří k nejčastějším typům hrozeb, ke kterým dochází v síti Internet. V současné moderní době tak dochází k čím dál více útokům na počítače (hardware), software, data či samotné sítě. V oblasti kybernetických útoků tak může docházet k například k únikům informací, poškození či vymazání dat, bránění přístupu k informacím, aplikacím či systému nebo může dojít k zneužití informací neoprávněnou osobou. Kybernetických hrozeb je celá řada, a proto zde budou vyjmenovány pouze ty nejzákladnější. [5]

1.6.1 Hacking

Hacking lze definovat jako vniknutí do počítačového systému jiným způsobem, než je běžný standardní způsob. Dochází tak k obejití či prolomení bezpečnostního systému, kterým je dané zařízení vybaveno nebo chráněno. [5]

1.6.2 Phishing

Pojem phishing je způsob útoku, jehož cílem je získání informací o uživatelích (např. uživatelská jména, hesla, čísla kreditních karet, PIN a podobně). Jde o podvodný způsob jednání, který vyžaduje po uživateli, návštěvu podvodné stránky. [5]

1.6.3 Pharming

Pharming je poněkud složitější a více nebezpečnou formou výše zmíněného phishingu. Pharming je typem útoku, který se zaměřuje na DNS (Domain Name Server) server. Zde dochází k přeložení doménového jména na IP adresu. Útok začíná tehdy, kdy uživatel zadává adresu webového serveru do internetového prohlížeče, za účelem navštívení webové stránky. [5]

1.6.4 DDoS útok

DDoS útok, neboli Distributed Denial of Service (v překladu distribuované odepření služby), je takový typ útok, který provádí zahlcení koncového počítačového systému pomocí paketů z více počítačových systémů, které tyto pakety vysílají. Jelikož jsou tyto počítačové systémy

různě geograficky rozmístěny, je dost obtížné se proti tomuto útoku bránit nebo identifikovat útočníka. [5]

1.6.5 Spamming

Spamming je způsob útoku, kde dochází k zasílání nevyžádaných zpráv do elektronické pošty. Tyto zprávy jsou často reklamního typu, ale může se jednat i o zprávy obsahující viry a podobně. V oblasti informačních technologiích si pojem spam získal svůj význam jako „plané řeči“ či „kecy“. Spam tak dokáže zahltit celou elektronickou komunikaci a zcela tak znemožní i její funkci. [5]

1.6.6 Sniffing

Jde o typ útoku, který využívá ilegálního odposlechu dat pomocí tzv. snifferu. Tyto data jsou odposlouchávána v rámci počítačové sítě během komunikace mezi danou službou a počítačovým systémem. [5]

1.7 Informace

Informace jsou velmi důležitým aktivem a podstatné pro činnost všech druhů organizací. Jako ostatní typy aktiv i informace vyžadují adekvátní ochranu. Uchovávání těchto informací může probíhat ve třech formách:

- Digitální.
- Materiální.
- Nevyjádřená.

Digitální formou se rozumí to, že informace jsou uchovány v podobě datových souborů, které jsou uloženy na elektronických či jiných médií. Druhá forma je materiální, kde informace jsou zaznamenány na papíře. Poslední formou jsou nevyjádřené informace, které představují znalosti zaměstnanců. Přenos informací může probíhat různými způsoby, například elektronicky, verbální komunikací nebo pomocí kurýra. Většina informací je v organizacích závislá na informačních a komunikačních technologií, neboť tyto technologie výrazně napomáhají při tvorbě, zpracovávání, ukládání, přenosu či ochraně a zničení těchto informací. [6] [7]

Jako informační aktiva lze uvést několik příkladů:

- Databáze zákazníka.

- Databáze zaměstnanců organizace či uchazečů.
- Dokumentace, pracovní či technologické postupy, příručky.
- Materiály pro školení zaměstnanců.
- Personální informace.
- Obchodní plán.
- Finanční plán.
- Obchodní tajemství.
- Zálohy dat. [7]

2 ANALÝZA RIZIK

V oblasti snižování rizik je nejdůležitější jejich samotná analýza (Risk Analysis, v anglickém překladu). Analýza je prvním a základním krokem ke zvládání rizik v dané organizaci. Samotné hodnocení rizik není čistě jen technického charakteru, ale je zde využita kombinace dalších zaměření a disciplín, mezi které patří například přírodovědné zaměření, humanitní zaměření a samotné technické zaměření. Při rozhodovacích procesech se poté doplňují ještě další zaměření, které mohou být buďto ekonomické, psychologické nebo též i politické. Proces analýzy rizik je z velké části definován několika postupy. Mezi tyto postupy patří definování hrozeb, definování pravděpodobnosti a jejich uskutečnění a dopadu na aktivum čili stanovení rizika a jeho závažnosti. Na základě výsledků hodnocení rizik lze poté stanovit adekvátní kroky, které může vedení organizace aplikovat pro zvládání rizik a provést tak stanovená opatření, které by vedly k zamezení výskytu rizik. V analýze rizik je velmi důležité si také vytyčit danou úroveň, která oddělí jednotlivá rizika (stanovení zbytkového rizika). Nelze totiž provést úplné odstranění všech rizik, neboť tento proces by vedl k nepřiměřeným nákladům při realizaci daných protiopatření a současně by tak vedl k narušení funkčnosti dané organizace. Velmi důležitou částí při analýzy rizik je výběr její metody, jelikož existuje celá řada metod a postupů, kterými lze daná rizika ohodnotit. Výběr metody by se měl odvíjet vzhledem k situaci či danému cíli v organizaci, v němž je samotné hodnocení rizik uskutečněno. Jednotlivé metody analýz rizik se mohou lišit a každá metoda je jinak použitelná než ta druhá a mají své výhody a nevýhody v oblasti hodnocení rizik. [1] [2] [3] [8]

V oblasti analýzy rizik jsou zahrnuty následující kroky:

1. Stanovení hranice analýzy rizik.
2. Identifikace aktiv – vymezení posuzovaného subjektu a definice aktiv.
3. Stanovení hodnoty aktiv – stanovení hodnoty aktiva jejich významnosti pro organizaci, hodnocení dopadu jejich ztráty, změny či poškození na existenci či chod organizace.
4. Identifikace hrozeb a zranitelnosti – stanovení druhu události, které mohou negativně narušit hodnotu aktiva, určení slabých míst v organizaci, které mohou umožnit působení hrozeb.
5. Stanovení závažnosti hrozeb a míry zranitelnosti – určení míry výskytu hrozby a míry zranitelnosti organizace vůči konkrétní hrozbě. [1] [2] [3]

Dále pak hodnocení rizik představuje neustálé zvažování:

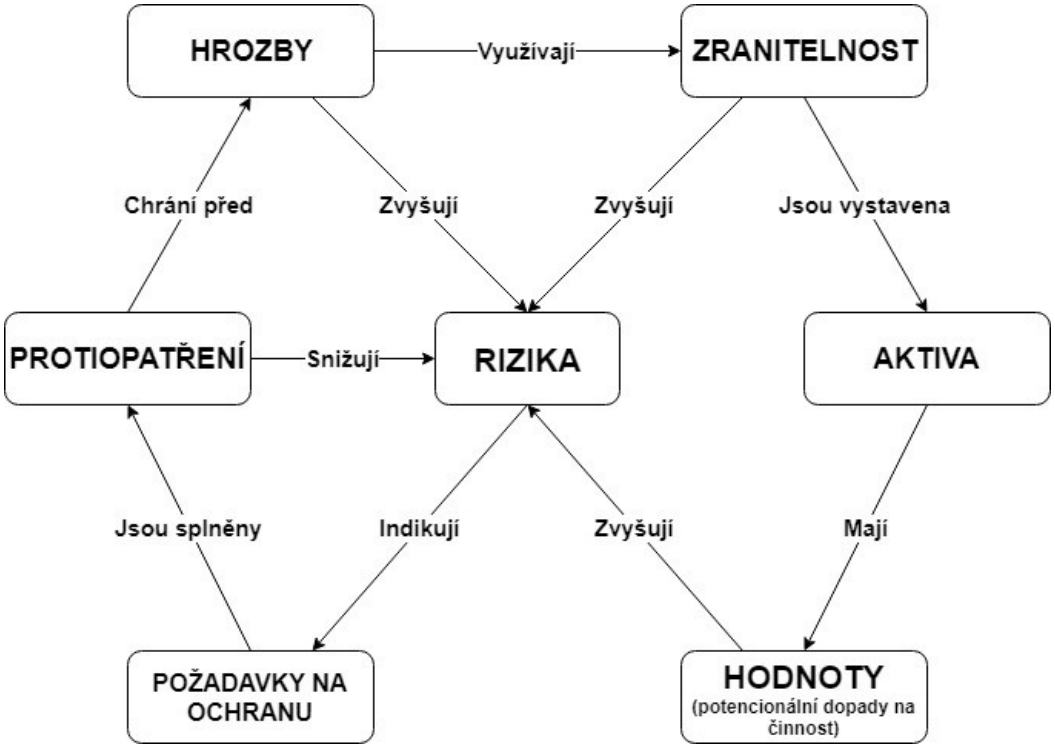
1. Narušení aktivit, která mohou být zapříčiněna uskutečněním hrozeb a je nutné vzít do úvahy jakékoliv potencionální důsledky.
2. Reálného výskytu takových rizik z pohledu převládajících hrozeb, zranitelnosti a aktuálně využitých protiopatření. [1]

2.1 Vztahy v oblasti analýzy rizik

Aby samotná analýza rizik mohla mít kladný výsledek je zapotřebí správně pochopit jednotlivé vztahy v analýze rizik a funkci jednotlivých pojmů, které byly definovány v kapitole 1. Existuje určitý mechanizmus uplatnění rizika, který funguje na následujícím principu:

- Zranitelnost je využita hrozbou, hrozba překonává protiopatření a negativně působí na aktivum či aktiva, kde následně způsobí škodu (dopad hrozby).
- Hodnota aktiva motivuje útočníka k aktivaci hrozby. Aktiva se vyznačují určitou zranitelností vůči působení hrozby.
- Protiopatření chrání dané aktivum před hrozbami. Detekuje hrozby a svou funkcí mírní nebo úplně zabraňuje jejich působení. Protiopatření může mít i odrazující účinek od aktivování hrozeb.
- Aktivum nebo protiopatření je vystaveno hrozbě, která si klade cíl získat přístup k aktivu. Hrozba musí být nejprve aktivována, aby mohla působit. Pro aktivaci jsou třeba určité předpoklady, které vedou k působení dané hrozby. [1] [2]

Další vztahy jsou přehledně definovány na obrázku 2, kde je zobrazeno riziko spolu s dalšími pojmy a pomocí šipek jsou vyobrazeny jednotlivé vztahy.



Obr. 2: Vztahy v oblasti analýzy rizik [1]

2.2 Postup analýzy rizik

Během analýzy rizik jsou provedeny konkrétní kroky, které vedou k získání potřebných informací a jsou pro analýzu stěžejní. Tyto kroky byly vyjmenovány v úvodu kapitoly 2 a v následujících kapitolách budou podrobněji vysvětleny a dle posloupnosti seřazeny.

2.2.1 Stanovení hranice analýzy rizik

Pod tímto krokem si lze představit to, že na začátku analýzy je vytyčena pomyslná čára, která odděluje aktiva. Pomocí stanovení hranice tak dochází k tomu, že aktiva jsou rozděleny buď to na aktiva, které jsou součástí analýzy a nebo na aktiva, které již nejsou součástí analýzy. Při samotném stanovení této hranice se vychází ze záměrů managementu a mají-li aktiva vztah k cílům managementu, tak poté budou tyto aktiva zařazeny do analýzy a budou se nacházet uvnitř hranice analýzy. [1] [2]

2.2.2 Identifikace aktiv

Dalším krokem analýzy, který následuje po stanovení hranice analýzy rizik je identifikace aktiv. Tento krok spočívá v provedení soupisu všech aktiv, které leží uvnitř hranice analýzy rizik. Při zařazování aktiva na soupis se uvádí název aktiva a umístění daného aktiva. [1]

2.2.3 Stanovení hodnoty a seskupení aktiv

Hodnotu aktiva lze stanovit na základě velikosti škody způsobené ztrátou aktiva či jeho zničením. Nejčastěji se stanovení hodnoty aktiva dá určit na základě dvou charakteristik. A to charakteristika nákladová, kde její součástí je pořizovací cena či reprodukční pořizovací cena. Druhou charakteristikou je charakteristika výnosová, kde si lze představit, že aktivum přináší organizaci významný přínos či zisk. Do této charakteristiky též patří i vlastnosti aktiv, kde vlastností může být to, že aktivum je k dosažení zisků využíváno nepřímo, například postavením na trhu, ochrannou známkou, či kvalifikací zaměstnanců a know-how firmy. Dále je pak důležité rozlišit to, či jde o aktivum jedinečné, nebo takové které lze jednoduše nahradit. V hodnotě aktiva je též i promítnuta závislost organizace na existenci a fungování tohoto aktiva. [1] [2]

Jelikož je poměrně velké množství aktiv, dochází k tomu, že se provede snížení počtu těchto aktiv a dojde k seskupení aktiv. Toto seskupení se provádí podle různých hledisek a okolností a to tak, že se vytvoří jednotlivé skupiny aktiv podobných vlastností. Aktiva se mohou seskupovat podle podobné kvality, účelu či například ceny. Po vytvoření skupiny pak poté každá skupina vystupuje jako jedno aktivum. [1] [2]

2.2.4 Identifikace hrozeb

Jestliže byla provedena samotná identifikace aktiv, stanovení jejich hodnot a seskupení, může být proveden další krok a tím je identifikace hrozeb. V tomto kroku se identifikují konkrétní hrozby, které by mohly ohrozit alespoň jedno aktivum organizace. Pro identifikaci hrozeb lze využít seznam hrozeb, který je sestaven dle literatury či například lze vycházet z vlastních zkušeností nebo dříve provedených analýz. Konkrétní hrozby se mohou lišit v závislosti na daném typu podnikání organizace či na statutu organizace. [1] [2]

2.2.5 Analýza hrozeb a zranitelností

Každá jednotlivá hrozba se hodnotí a určuje se její úroveň vůči každému aktivu či skupině aktiv. U aktiv, u kterých lze očekávat uplatnění konkrétní hrozby se určí úroveň hrozby vůči aktivu a určí se úroveň zranitelnosti aktiva vůči této hrozbě. Během stanovení úrovně hrozby se vychází ze tří hledisek, které byly výše vyjmenovány. Těmito hledisky jsou nebezpečnost, motivace a přístup. U zjištěných hrozeb se dále provádí určení výše dopadu na daném aktivum a výše škody, kterou daná hrozba může organizaci způsobit. Během stanovení úrovně zranitelnosti jsou zase brány v potaz hlediska jako je citlivost nebo kritičnost.

V neposlední řadě se bere ohled na realizovaná protiopatření při analýze hrozeb a zranitelností. Konkrétní protiopatření tak mohou snížit nejen úroveň hrozby, ale mohou se podílet též na snížení úrovně zranitelnosti. V samotném závěru je poté vytvořen seznam dvojic (hrozba a aktivum), kde je stanovena úroveň hrozby a zranitelnosti. [1] [4] [2]

2.2.6 Pravděpodobnost jevu

Specifickou vlastností je poté pravděpodobnost, která se doplňuje spolu s dalšími údaji ke konkrétnímu jevu a udává s jakou pravděpodobností může daný jev nastat. Aby bylo možné s touto vlastností dále počítat je nutné znát fakt, zdali je analyzovaný jev náhodný nebo či není náhodný. [1] [2]

2.2.7 Měření rizika

Aby bylo možné určit závažnost jakéhokoliv problému je nutné stanovit výši rizika. Tato hodnota se určí z hodnoty aktiva, úrovně dané hrozby a úrovně zranitelnosti aktiva. Analýza rizik pracuje s takovými veličinami, které není možné v mnoha ohledech naměřit. Velikost těchto veličin je tak z velké většiny odhadnuta specialistou, který analýzu rizik provádí a vše závisí na jeho získaných zkušenostech. Nejčastější vyjádření velikosti těchto veličin bývá typu „malý“, „střední“, „velký“, nebo například na základě stupnice od 1 až 10. V případě jednotlivce se poté měří riziko dle pravděpodobnosti nežádoucí odchylky od výsledku, který je očekáván jednotlivcem. Lze tedy říct to, že čím je vyšší pravděpodobnost, že k nežádoucí události dojde, tím vyšší je pravděpodobnost odchylky od kladného výsledku a tím vyšší bude i samotné riziko. [1] [2]

2.2.7.1 Výpočet úrovně rizika

Výše rizika se dá vypočítat různými způsoby. Jedním ze způsobu je ten, kde úroveň rizika se dá vypočítat jako součin závažnosti dopadu (D) a pravděpodobnosti výskytu (P) a vyděleným bezpečnostními opatřeními (B), viz vztah (1). Vyjádření dopadu a pravděpodobnosti, za účelem určení úrovně rizika, se mění dle typu rizika a účelu, pro který jsou výstupy posuzování rizika využity.

Vztah pro výpočet rizika pomocí prvního způsobu:

$$R = \frac{D \cdot P}{B} \tag{1}$$

Druhý způsob výpočtu je ten, kde úroveň rizika je vypočtena pomocí tří parametrů.

$$R = T \cdot A \cdot V \tag{2}$$

Kde parametr T je pravděpodobnost hrozby, parametr A je hodnota aktiva a parametr V je zranitelnost. [2] [9]

2.2.8 Zvládnutí rizika

Posledním krokem v analýze rizik je výběr vhodných bezpečnostních protiopatření pro úspěšné zvládnutí rizika. Při správném výběru bezpečnostních protiopatření je možné zjištěné hrozby eliminovat či případně snížit výši rizika u dané hrozby. Při výběru těchto protiopatření lze využít obecných doporučení z různých katalogů, norem či případně vlastních zkušeností. [1] [2] [4]

2.3 Metody analýzy rizik

V oblasti analýzy rizik existují dvě různé metody, pomocí kterých může být analýza vypracována. Jedná se o dvě následující metody:

- Kvalitativní metoda.
- Kvantitativní metoda.

Největším rozdílem mezi těmito dvěma metodami je ve způsobu vyjádření velikosti rizika. Pro lepší pochopení těchto metod jsou vypracovány následující podkapitoly, kde bude vysvětlen princip těchto metod. [1] [2]

2.3.1 Kvalitativní metoda

Prvním metodou, která zde bude definována je metoda kvalitativní. Tuto metodu lze popsat tak, že rizika jsou vyjádřena v určitém rozsahu. Tento rozsah může být podle tří kategorií:

- Bodové hodnocení.
- Slovní hodnocení.
- Hodnocení podle pravděpodobnosti.

V případě využití bodového hodnocení je nejčastěji využita bodová stupnice od 1 do 10. Slovní hodnocení bývá vyjádřeno pomocí slov, které mohou být typu „malý“, „střední“, „větší“ a podobně. Poslední možností, jak lze riziko vyjádřit je využití pravděpodobnosti (0; 1). Hlavní výhodou kvalitativní metody je její jednoduchost a rychlost provedení. Ovšem tato metoda je daleko více subjektivní než metoda kvantitativní. Větším problémem však může být to, že tato metoda je v oblasti zvládání rizik značně problematická, neboť vznikají

problémy při posuzování přijatelnosti finančních nákladů, které by vedly ke snížení či eliminaci dané hrozby. Chybí tak jednoznačné finanční vyjádření a tím se znesnadňuje kontrola efektivnosti nákladů. [1] [2]

2.3.1.1 Metoda Delphi

Jedná se o nejběžnější kvalitativní metodu analýzy rizik. Metoda účelových interview neboli metoda Delphi je založena na přímém kontaktu se specialisty hodnotící skupiny a účastníky hodnocené organizace, kteří jsou zároveň zastupiteli této organizace. Hlavní princip metody spočívá v tom, že je zde zahrnut seznam otázek, které jsou během pohovoru diskutovány. Seznam otázek je dělen na dvě části, kde první část je pevná, předem určená, a druhá část je variabilní, která záleží na konkrétním průběhu daného pohovoru a přístupu účastníka. [1]

Velkou výhodou této metody je to, že je zde podstatně menší časová náročnost nebo náročnost na spotřebu zdrojů. Metoda Delphi je prováděna opakovaně (2 až 3 opakování). Po každém opakování jsou výsledky statisticky zpracovány a jsou sděleny účastníkům. Ti pak poté musí proti těmto výsledkům zaujmout stanovisko a mohou tak buď korigovat či například zdůraznit svůj původní názor. [1]

2.3.2 Kvantitativní metoda

Druhou metodou analýzy rizik je metoda kvantitativní. Ta je oproti metodě kvalitativní značně rozdílná, protože ke svému výpočtu rizika využívá matematický výpočet. Výpočet bývá vypočten z frekvence výskytu dané hrozby a dopadu této hrozby. Vyjádření této metody bývá z pravidla ve finanční podobě (například tisíce Kč) a nejčastěji se toto riziko vyjadřuje ve formě roční předpokládané ztráty (v anglickém jazyce Annualized Loss Expectancy – ALE), které je vyjádření konkrétní finanční částkou. Ve srovnání s kvalitativní metodou je kvantitativní metoda daleko více přesnější, ale její provedení je daleko více časově náročnější a vyžaduje mnoho úsilí. Nicméně jejím výsledkem je finanční vyjádření rizika, které je daleko více výhodnější pro zvládání těchto rizik.

Kromě časové náročnosti této metody je další nevýhodou její samotný postup, neboť jde o vysoce formalizovaný postup, který může způsobit to, že nebudou postihnuta specifika posuzovaného objektu, které by mohli vést k jeho vysoké zranitelnosti. Důvodem této nevýhody bývá to, že samotný hodnotitel je zahlcen velmi rozsáhlým objemem dat. Mezi kvantitativní metody analýzy rizik patří například metoda CCTA Risk Analysis and

Management Methodology (CRAMM) či například metodika RISK, RiskPAC nebo RiskWatch. [1] [2]

2.3.2.1 Metoda CRAMM

Jde o kvantitativní metodu analýzy rizik, která našla své uplatnění v oblasti informačních systémů a bezpečnosti organizací. Metoda CRAMM vznikla na základě požadavků vlády Velké Británie (v roce 1985), avšak v současnosti je tato metoda využívána především jako prostředek pro vypracování analýzy rizik. Samotná analýza spočívá v ohodnocení systémových aktiv, jejich seskupení do skupin a určení hrozeb, které ovlivňují tyto aktiva, zjištění zranitelností systému a navržení bezpečnostních opatření. Využitím této metody je daná organizace připravena na získání certifikaci dle mezinárodní normy ISO/IEC 27001 (více v kapitole 5), po úspěšném provedení analýzy. Důležitým atributem, pro získání kvalitní analýzy, jsou výsledky, na kterých je metoda CRAMM nejvíce závislá. Výsledky jsou zde získány na základě strukturovaných rozhovorů mezi uživatelem a odborníkem, který analýzu provádí. Hlavní nevýhodou této metody je její vysoká cena, resp. vysoká cena za software, který metodu CRAMM využívá. Cena se pohybuje v řádech statisíců. [1] [10]

3 INTEGROVANÝ SYSTÉM ŘÍZENÍ

Integrovaný systém řízení, v anglickém překladu Integrated Management System (IMS), je systém, který se komplexně věnuje problematice řízení v organizaci a zajišťuje tak navazování vazeb mezi jednotlivými oblastmi řízení. Tento systém vznikal na základě prvotních autonomních systémů řízení a byly tak pro ně utvořeny normativy, které jsou v současné době používány. Vydavatelem těchto normativ je mezinárodní organizace pro normalizace International Organization for Standardization, která sídlí v Ženevě ve Švýcarsku. Normy, jež jsou vydávány touto organizací nesou zkratu ISO. Normy jsou současně vystaveny pravidelným revizím, které vedou k jejím pozdějším úpravám, aby mohla být zajištěna aktuálnost měnících se potřeb dané organizace. Během samotného zavádění systému řízení, kdy tento systém je zároveň v souladu s mezinárodními standardy, přináší normy procesní přístup k budování, zdokumentování, zavedení, provozování, monitorování, udržování a zvyšování účinnosti systému řízení dané organizace. V oblasti elektrotechniky, elektřiny, IS/ICT a dalších odvětví se samotnou přípravou a publikováním norem zabývá světová organizace International Electrotechnical Commission (IEC), která byla založena roku 1906 v Ženevě. Lze se tedy setkat s normami označenými jako ISO/IEC. [4]

Z hlediska využitelnosti jsou normy použitelné pro všechny typy organizací, bez ohledu na jejich velikost. Přijetí a zavedení norem je zcela dobrovolné, ale též i výhodné pro konkrétní organizaci. V případě norem je kladen největší důraz na:

- Chápání, očekávání požadavků a potřeb zainteresovaných stran (zákazník, vlastník, dodavatel, společnost, akcionáři, lidé uvnitř organizace).
- Stanovení potřebných zásad a cílů.
- Zavádění systémových protiopatření.
- Monitorování a hodnocení systému řízení z hlediska funkčnosti a účinnosti.
- Zlepšování, zdokonalování systému řízení dle konkrétního měřítka účinnosti systému a dosažení tak stálého úspěchu organizace. [4]

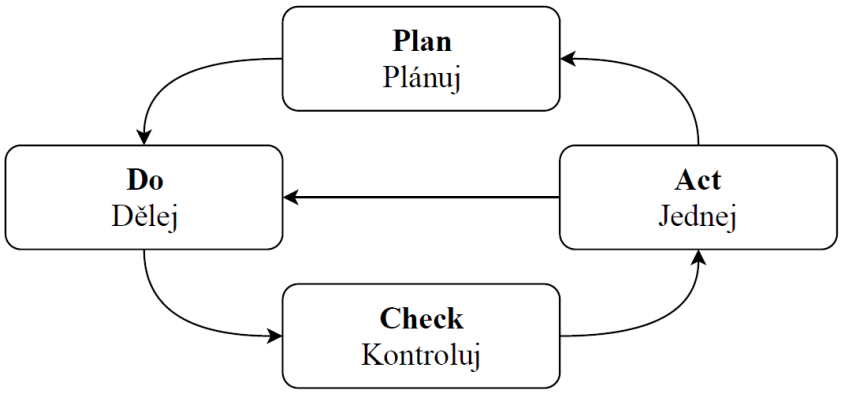
V České republice se normotvorbou nově zabývá Česká agentura pro standardizaci (ČAS), která byla založena Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ). Normy vydávané agenturou ČAS nesou označení ČSN. [4] [11]

Mezi hlavní vlastnost integrovaného systému řízení patří to, že je možné využívat podobné postupy a metody při řízení všech jeho komponentů. Příkladem mohou být metody a postupy

řízení rizik, řízení jejich dopadu na organizaci a chování dané organizace či například sledování účelnosti a účinnosti nebo provádění auditních postupů. Tyto postupy a metody, které jsou zde výše vyjmenovány, jsou součástí životního cyklu, který vychází ze starého manažersky osvědčeného konceptu řízení tzv. PDCA. Tento koncept je dále vysvětlen v následující podkapitole. [4]

3.1 Model PDCA

PDCA se skládá ze čtyř anglických slov plan, do, check, act (PDCA), které jsou za sebou systematicky zařazeny a vzájemně na sebe navazují. V českém překladu plánuj, dělej, kontroluj a jednej. Spolu navzájem tvoří životní cyklus kompletního integrovaného systému řízení a poskytuje tak i samotnou zpětnou vazbu. Tento koncept byl poprvé použit v práci Williama Edwardse Deminga, kde Deming definoval zásady vymezení konkrétního systému řízení, od jeho realizace až po snahu jeho neustálého zlepšování. V současné době je tak základem pro mezinárodní standardy v oblasti IMS a konkrétně oblasti řízení bezpečnosti informací. Samotné pojetí toho modelu je znázorněno na následujícím obrázku 3. [4]



Obr. 3: Cyklus modelu PDCA [4]

První fáze plánování (Plan) v sobě zahrnuje samotnou definici cílů komponentů integrovaného systému řízení, strategii při realizaci komponentů, ukazatele pro měření účinnosti a analýzu rizik. V druhé fázi (Do) jsou implementovány komponenty integrovaného systému řízení do systému řízení dané organizace. Ve třetí fází kontroly (Check) je provedeno nastavení počátečních hodnot ukazatelů. Je prováděno monitorování předem nadefinovaných hodnot, s hodnotami naměřenými, které jsou získány ukazateli a vzniká vyhodnocení výsledků. V závěrečné fázi (Act) jsou provedeny změny, získané na základě výsledků v předchozí fázi. Vzniká tak příprava na realizaci potřebných změn a v této fázi tak dochází ke získání systémové zpětné vazby. [4]

4 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Systém, který zde bude dále definován se nazývá systém řízení bezpečnosti informací, v anglickém překladu Information Security Management System (ISMS). ISMS je dokument celkového systému řízení organizace, který je založen na přístupu konkrétní organizace k rizikům činností. Zabývá se ustanovením, zaváděním, provozem, monitorováním, přezkoumáváním, údržbou a v neposlední řadě zlepšováním bezpečností informací. O systému řízení bezpečnosti informací pojednává mezinárodní standard norem ISO/IEC 27000, který specifikuje soubor postupů, požadavků, měření či jiných dalších směrnic, jež jsou s touto problematikou spjaté. Konkrétní části ISMS jsou součástí norem ISO/IEC 27001 a ISO/IEC 27002. Řada norem ISO/IEC 27000 je blíže popsaná v kapitole 5. [4] [12]

4.1 Bezpečnost informací

Hlavním a důležitým cílem bezpečnosti informací je zajištění zásad pro bezpečnou práci s informacemi všeho druhu. Tyto informace nemusí být vždy digitálního charakteru. U nedigitálních materiálů záleží především na tom, jakým způsobem jsou tyto materiály zpracovány, spravovány, archivovány, skartovány či transportovány na jiná místa. S bezpečností informací souvisí tři následující aspekty:

- Důvěrnost (Confidentiality).
  - Zajištění důvěrnosti znamená to, že informace jsou dostupné pouze oprávněným osobám.
- Integrita (Integrity).
  - Je pojem, který uvádí zajištění správnosti a úplnosti informací.
- Dostupnost (Availability).
  - Zajištění dostupnosti znamená to, že informace jsou přístupné oprávněným uživatelům v případě okamžité potřeby.

Aby mohla být zajištěna bezpečnost informací, je nutné implementovat vhodná bezpečnostní protiopatření, která by zajišťovala minimální dopad incidentů na bezpečnost informací. [4] [6]

4.2 Řízení přístupu

Velmi důležitým faktorem v oblasti bezpečnosti informací je řízení přístupu do informačních systémů a aplikací. Významnými prvky, které se podílejí na řízení přístupu, jsou přístupová práva a soubor pravidel, kterými se organizace řídí. Těmito prvky jsou:

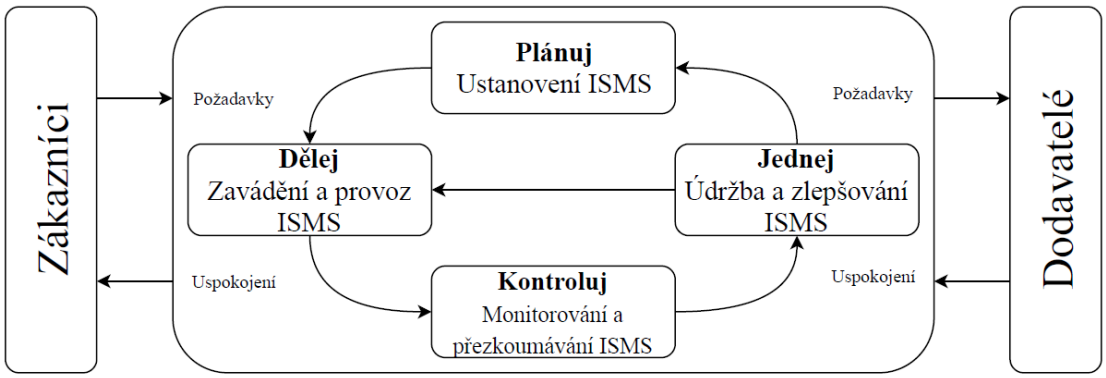
- Identifikace (Identification).
  - Jedná se o proces, pomocí něhož je umožněno rozeznání entity za pomocí využití výpočetní techniky uživatelských jmen.
- Autentizace (Authetication).
  - Jde o proces ověření identity, kde se ověřuje jeho pravost. Slovo autentický znamená pravý, původní.
- Autorizace (Authorization).
  - Je povolení k přístupu ke konkrétním zdrojům a činnostem, ke kterým chce daná entita přistupovat. S autorizací entity souvisí i samotná úspěšná autentifikace, která je předpokladem pro provedení autorizace. [4]

4.3 Fáze ISMS

Systém řízení bezpečnosti informací si zakládá na modelu PDCA (viz kapitola 3.1). Tento model je v oblasti ISMS rozdělen na čtyři fáze, které spolu tvoří životní cyklus. Mezi tyto základní čtyři fáze patří:

- Ustanovení ISMS.
- Zavádění a provoz ISMS.
- Monitorování a přezkoumávání ISMS.
- Údržba a zlepšování ISMS.

Vyobrazení fází ISMS je na obrázku 4, kde jsou jednotlivé fáze implementovány právě do modelu PDCA. Samotná fáze „Ustanovení ISMS“ je v následující podkapitole blíže rozepsána.



Obr. 4: Využití modelu PDCA v rámci řízení bezpečnosti informací [4]

4.3.1 Ustanovení ISMS

První krokem při tvorbě systému řízení bezpečnosti informací je provedeno samotné ustanovení tohoto systému. Během tohoto kroku tak dochází k tomu, že jsou upřesněny korektní formy řešení bezpečnosti informací a je provedeno odsouhlasení prohlášení o politice ISMS. Prohlášením o politice ISMS je myšleno to, že vedení podniku dalo závazek k podporování informační bezpečnosti. Výstup tohoto kroku by měl být zakončen souhlasem vedení se zavedením ISMS dle daných potřeb konkrétní organizace, které byly zjištěny při analýze rizik ISMS. Analýza rizik je jednou z nejzásadnějších částí fáze „Ustanovení ISMS“, neboť může mít zásadní dopady na funkci ISMS během celého životního cyklu. Ustanovení ISMS se tedy dělí na následující kroky, kterými jsou:

- Definování rozsahu, hranic a vazeb ISMS.
- Definování a odsouhlasení Prohlášení o politice ISMS.
- **Analýza a zvládání rizik.**
- Souhlas vedení organizace s navrhovanými zbytkovými riziky a se zavedením ISMS.
- Příprava Prohlášení o aplikovatelnosti. [4]

4.3.1.1 Analýza a zvládání rizik

Velkou úlohu v oblasti systému řízení bezpečnosti informací hraje i samotné řízení rizik a jejich analýza. Znalost všech konkrétních rizik, které mohou skutečně nastat, dává velkou váhu při výběru adekvátních bezpečnostních protiopatření, které jsou schopny zmenšit negativní dopad skutečných rizik. Organizace, jež se chtějí podílet na efektivním systému řízení bezpečnosti informací by měly brát značný ohled na oblast řízení rizik. Tato analýza

rizik představuje základní stavební kámen pro úspěšné řízení rizik a dále je rozdělena do následujících kroků:

- Identifikování aktiv ISMS a určení míry důvěrnosti, integrity a dostupnosti.
- Identifikování hrozeb ISMS.
- Stanovení výše dopadu a výše škody hrozby na daném aktivum.
- Určení pravděpodobnosti, že daná hrozba může nastat.
- Identifikace zranitelnosti.
- Stanovení výsledného rizika.
- Výběr vhodných bezpečnostních protiopatření.

Dle normy ISO/IEC 27001 by měl být postup řízení rizik patřičně zdokumentován a měla by být vypracována zpráva o hodnocení rizik. Obecný postup analýzy rizik je podrobněji popsán výše v kapitole 2. [4]

Při bližším pohledu na tuto problematiku si lze všimnout, že analýza rizik obecně vychází ze základního (obecného) postupu. Jednotlivé postupy různých analýz rizik si jsou velmi podobné, ale z pravidla se mohou měnit v závislosti na řešené problematice. Právě analýza rizik, která se provádí u ISMS v sobě zahrnuje ještě dodatečné určení důvěrnosti, integrity a dostupnosti daných aktiv.

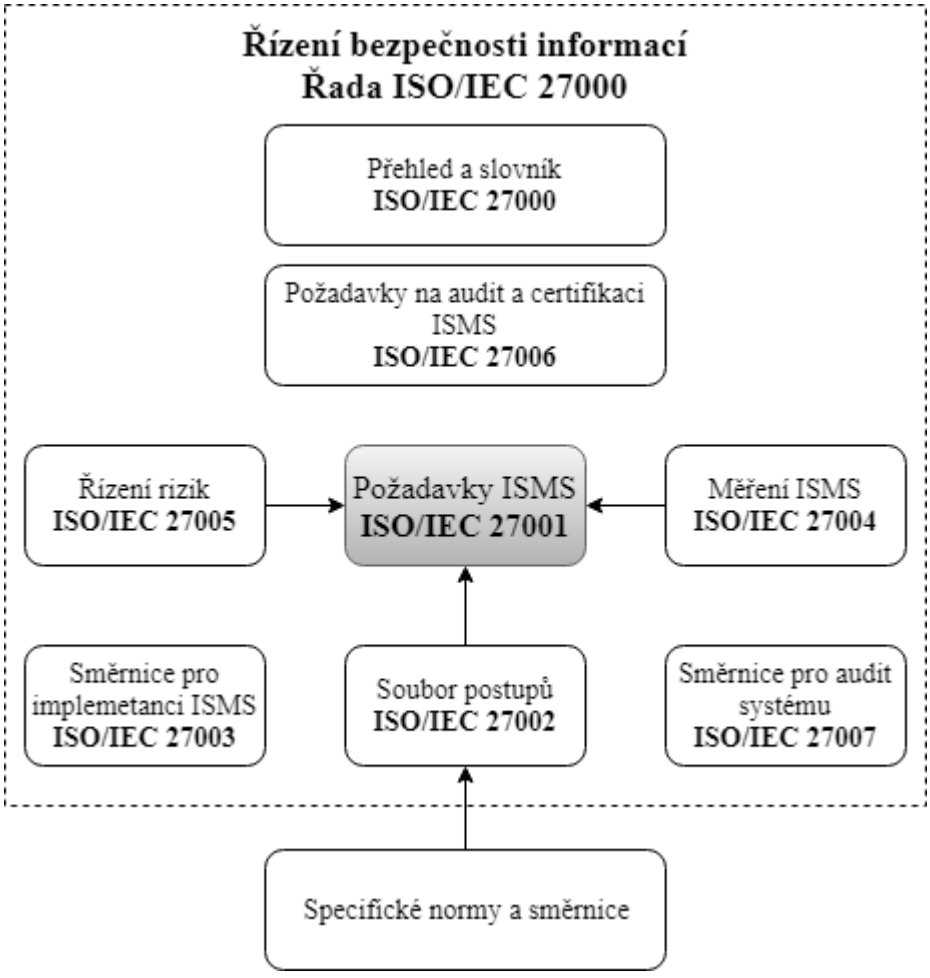
5 ŘADA NOREM ISO/IEC 27000

V roce 2005 byla představena nová řada norem organizací ISO. Řada norem dostala označení ISO 27000 a měla se tak věnovat problémům v oblasti řízení bezpečnosti informací. V současné době je řada norem ISO/IEC 27000 velmi obsáhlá a je doplněna dalšími informaci a doporučeními, které se týkají různých oblastí řízení bezpečnosti informací. Mezi nejzákladnější a nejdůležitější normy, které se podílejí na problematice ISMS, patří následující:

- ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník.
    - Jde o první normu z řady ISO/IEC 27000, která dává přehled o souvisejících termínech využívané v ISMS a definuje samotný systém řízení bezpečnosti informací. Organizaci či jednotlivce tak seznamuje se všemi normami, které se zabývají ISMS. V této normě jsou následně vysvětleny principy, kterými se ISMS řídí a vysvětluje podstatu a důležitost tohoto systému spolu s jeho přínosy. [6]
- ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.
    - Jedná se o mezinárodní normu, která svým obsahem ustanovuje požadavky na implementování, ustavení, udržování a neustálé zlepšování ISMS v dané organizaci. Součástí této normy jsou i požadavky pro posouzení a ošetření rizik bezpečnosti informací, které jsou uzpůsobeny konkrétním potřebám dané organizace. Veškeré požadavky obsažené v této normě jsou zcela použitelné pro všechny typy organizací nehledě na velikost těchto organizací či typ jejich podnikání. [13]
- ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací.
    - Následující normou z řady norem ISMS je norma s označením ISO/IEC 27002. Tato norma poskytuje pro organizaci či jednotlivce pokyny pro uplatnění a výběr ideálních opatření, které zajistí dostatečnou bezpečnost informací v konkrétní organizaci. Daná doporučení a pokyny, které jsou obsaženy v této normě, jsou v souladu s požadavky definovanými v normě ISO/IEC 27001. [14]

- ISO/IEC 27003 Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací.
    - Součástí normy ISO/IEC 27003 je soubor praktických pokynů k provedení úspěšné implementaci systému řízení bezpečnosti informací. Dále pak norma obsahuje dodatečné informace o ustanovení, provozu, monitorování, přezkumu, udržování, či například zlepšování systému řízení bezpečnosti informací dle požadavků, které jsou uvedeny v normě ISO/IEC 27001. [6]
- ISO/IEC 27004 Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření.
    - Aby systém řízení bezpečnosti informací byl dostatečně efektivní, je potřeba provádět jeho pravidelná měření. V této normě lze nalézt řadu doporučení pro použití a vývoj měření. Na základě těchto měření se tak posuzuje efektivnost ISMS či například efektivnost daných opatření, které jsou použity v systému řízení bezpečnosti informací. [6]
- ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.
    - Řízení rizik se systémem řízení bezpečnosti informací úzce souvisí, z toho důvodu existuje mezinárodní norma ISO/IEC 27005, kde lze nalézt směrnice pro řízení rizik bezpečnosti informací. [6]
- ISO/IEC 27006 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.
    - Specifické požadavky jsou nastaveny i pro samotné orgány, které se zabývají certifikací a auditem ISMS. Tato norma definuje pokyny a požadavky dle normy ISO/IEC 27001 a slouží jako podpora při akreditaci, kterou provádí certifikační orgány u certifikovaných organizací. Při splnění všech předpokladů získává organizace certifikát shody dle stanovených požadavků. [6]
- ISO/IEC 27007 Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací.
    - Je přehled pokynů, které slouží organizacím při provádění potřebných interních a externích auditů ISMS nebo při řízení programu auditu ISMS. [6]

Jak již bylo uvedeno výše, řada norem ISO/IEC 27000 je daleko obsáhlejší a z toho důvodu zde byly uvedeny jen ty nejzákladnější normy z této řady. Postupem času došlo k zařazování dalších norem, které doplňují důležité informace z různých oblastí řízení bezpečnosti informací. Uplatnění této řady norem je takřka neomezené a dá se pouze očekávat jeho rozšíření do dalších oblastí. Na obrázku 5 je zobrazen koncept této normy, na kterém si lze všimnout prvních osmi norem a vstupujících dalších specifických norem a směrnic z konkrétní oblasti bezpečnosti. Tyto specifické normy plní tu úlohu, že pomáhají při výběru optimálních bezpečnostních protiopatření v dané oblasti. [4] [6]



Obr. 5: Koncept řady norem ISO/IEC 27000 [4]

6 SOUVISEJÍCÍ NAŘÍZENÍ

V předchozí kapitole byla představena řada norem ISO/IEC 27000, jenž se problematikou řízení bezpečnosti informací zabývá. Jak již bylo uvedeno výše, normy jsou záležitostí zcela dobrovolnou a je jen na každé organizace, zdali přistoupí na přijetí některé z norem. Potom jsou zde ale i taková ustanovení a nařízení, kterými se organizace musí řídit zcela povinně, pokud se chce vyhnout případným trestům a pokutám, které s konkrétními nařízeními souvisí. Následující kapitola se proto bude věnovat dvěma tématům, kterými jsou:

- Obecné nařízení na ochranu osobních údajů.
- Zákon o kybernetické bezpečnosti.

6.1 Obecné nařízení na ochranu osobních údajů

Obecné nařízení na ochranu osobních údajů nebo lépe známější General Data Protection Regulation (GDPR) je soubor pravidel, který představuje ochranu osobních údajů v Evropské Unii (EU). GDPR se snaží co nejvíce hájit práva občanů Evropské Unie, proti neoprávněnému nakládání s jejich osobními údaji a daty. Nařízení se tedy týká všech, kteří se podílejí zpracování osobních údajů a dat občanů Evropské Unie, zejména společností a institucí, které podnikají na evropském trhu, ale nejsou součástí EU. GDRP se dále dotýká i samotných firem, institucí či jednotlivců, kteří pracují s osobními údaji zaměstnanců, zákazníků, nebo například klientů a dodavatelů ve všech daných odvětvích (například zdravotnictví, bankovní instituce, veřejná správa, internetové obchody a podobně). GDPR vešlo v platnost 25. května 2018 a nahradilo tak v České republice starou směrnici 95/46/ES. Koncem dubna, roku 2019, byl uveden nový zákon, který v sobě zahrnuje pravidla uvedené v GDPR a zároveň tak nahrazuje starý zákon č. 101/2000 Sb. o ochraně osobních údajů. Nový zákon nese označení zákon č. 110/2019 Sb. o zpracování osobních údajů. V současné době se v České republice regulací ochrany osobních údajů zabývá Úřad pro ochranu osobních údajů (ÚOOÚ). [15]

Hlavním důvodem pro zavedení GDPR bylo to, že předchozí legislativa z roku 1995 se jevila v dnešní době již jako zastaralá, neboť v té době ještě neexistovaly sociální sítě či různá cloudová uložiště a technologie nebyly tak rozvinuté jako jsou nyní. Jeden z dalších důvodů byl ten, že některé tajné služby mimo Evropskou Unii shromažďovaly osobní údaje o lidech, kteří žijí na území Evropské Unie [15]

6.1.1 Přínos GDPR

Jako obrovským přínosem je vymahatelnost práv v celé Evropské Unii a daleko lepší spolupráce dozorových orgánu v rámci EU. Občan Evropské Unie tak získává nová práva jako například:

- Právo vznesení námitky proti zpracování (zpracovatel nemůže údaje dále zpracovávat).
- Právo na přenositelnost osobních údajů (od jednoho zpracovatele k druhému).
- Právo na přístup k osobním údajům, které jsou o něm zpracovávány.
- Právo na výmaz a být zapomenut (vymazání osobních údajů, pokud zde není žádné právní stanovisko pro další zpracování těchto údajů).
- Právo na nápravu osobních údajů.
- Získání nových osobních údajů (email, IP adresa či cookies v zařízeních uživatele).
- Právo na informovanost o úniku osobních dat.

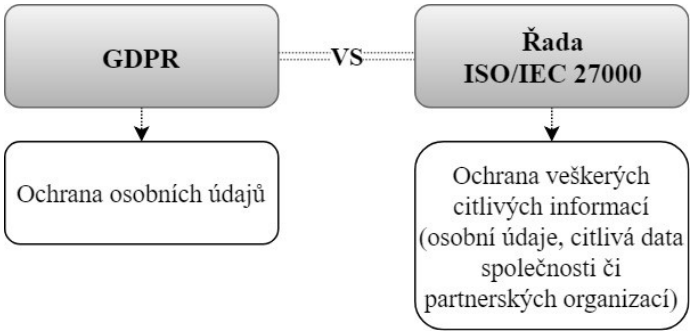
Nařízení GDPR tedy dopadá na všechny ty, kteří při svém podnikání pracují s osobními údaji. GDPR mimo jiné přináší i další nové pravidla, kde například musí zpracovatel dokumentovat platnost těchto informací, a že skutečně informace zpracovává jen k nezbytným účelům, po celou dobu jejich zpracování. Tímto tedy vzniká zcela logicky velká administrativní a časová náročnost. [15]

Nyní nově přibyla i nová povinnost, kde firmy či jiný zpracovatelé osobních dat by měly v případě narušení bezpečnosti údajů oznámit tuto skutečnost Úřadu pro ochranu osobních údajů, a to nejpozději do 72 hodin od zjištění incidentu. V dalším případě by zpracovatel měl informovat i tyto konkrétní osoby a subjekty, kterých se únik dat týkal. V případě neohlášení takového incidentu hrozí několika tisícové pokuty až do maximální výše 20 000 000 eur nebo 4 % z celkového ročního obratu společnosti (výši této pokuty může ovlivnit řada faktorů, jako například závažnost porušení, délka porušení či počet poškozených osob apod.). Tyto pokuty se vztahují i k samotnému porušení nebo například k nezavedení a nepřipravenosti společnosti k nařízení GDPR. [15]

6.1.2 GDPR a řada norem ISO/IEC 27000

Co se týče GDPR a řady norem ISO/IEC 27000 jedná se o dva odlišné nástroje, ale s velmi podobným cílem. Cílem řady norem ISO/IEC 27000 není se pouze zaměřit na ochranu osobních údajů, jako u GDPR, ale zaměřit se na veškeré citlivé údaje a bezpečnost informací,

kde mohou spadat například citlivá data o společnosti, či partnerských organizací a podobně. Organizace, které splňují systém ISMS mají z velké části již GDPR splněno. Řada norem ISO/IEC 27000 totiž klade velký důraz na důvěrnost, integritu a dostupnost informací a díky tomu tak napomáhá organizaci při zavádění GDPR právě na základě funkčního systému, který přesně popisuje, kdo data zpracovává, kde se tyto data nachází a jakým způsobem jsou dále zpracovány. Na základě tohoto jsou poté data snadno a lehce dohledatelná. [16] [17]



Obr. 6: GDPR vs. Řada norem ISO/IEC 27000

V dalším případě norma vyžaduje, při její implementaci, soulad s právními úpravami, kde patří současná legislativa EU a tím pádem i GDPR. Řada norem ISO/IEC 27000 dále specifikuje oznamovací povinnost organizace, pokud dojde k bezpečnostním událostem. Tuto oznamovací povinnost dále uvádí i samotné GDPR. Dle požadavků normy ISO/IEC 27001 musí být všichni zaměstnanci proškoleni a dále pak vzdělávání o povědomí bezpečnosti informací. Tento požadavek se týká i samotného GDPR, kde pověřenec pro ochranu osobních údajů musí dbát na zvýšení povědomí a odbornosti pracovníků, kteří jsou zapojeni do operací zpracování osobních údajů. [16] [17]

6.2 Zákon o kybernetické bezpečnosti

V lednu roku 2015 vešel v platnost zákon, který pojednává o problematice kybernetické bezpečnosti. Jedná se o zákon 181/2014 Sb. tedy zákon o kybernetické bezpečnosti. Hlavním cílem a účelem tohoto zákonu je:

- Stanovení základní úrovně bezpečnostních opatření.
- Zlepšení detekcí kybernetických bezpečnostních incidentů.
- Zavedení hlášení kybernetických bezpečnostních incidentů.
- Zavedení systému opatření při reakci na kybernetické bezpečnostní incidenty.
- Upravení činnosti dohledových pracovišť.
- Stanovení povinností orgánům a osobám v oblasti kybernetické bezpečnosti dle § 3.

Zákon mimo jiné popisuje základní pojmy jako je například kybernetická bezpečnostní událost či kybernetický bezpečnostní incident a dále pak uvádí povinnosti o hlášení kybernetického bezpečnostního incidentu buďto provozovateli národního CERT (Computer Emergency Response Team) nebo pak Národnímu bezpečnostnímu úřadu (NBÚ). Pokud k takovému závažnému bezpečnostnímu incidentu dojde může NBÚ provést reaktivní či ochranné opatření pro zabezpečení klíčové infrastruktury a mimo jiné i vyhlásit stav kybernetického nebezpečí. [18] [19]

Zákon o kybernetické bezpečnosti se dotýká zejména odvětví:

- Telekomunikační a internetové služby.
- Veřejná správa.
- Zdravotnictví.
- Doprava.
- Energetika.
- Poskytovatel finančních služeb.
- Provozovatel komunikačních a informačních systémů.

Firmy a organizace, kterých se zákon č. 181/2014 Sb. týká, tak musely implementovat systém řízení bezpečnosti informací. Pokud nedochází k naplnění bezpečnostních opatření uvedeném v zákoně, ukládá zákon přestupek, ve kterém může být uložena pokuta ve výši až 5 000 000Kč dle § 25 odst. 12 písm. a) zákona č. 181/2014 Sb. o kybernetické bezpečnosti. [18] [19]

II. PRAKTICKÁ ČÁST

7 ANALÝZA RIZIK VE VYBRANÉ SPOLEČNOSTI XY

V následující kapitole bude vypracována již samotná analýza rizik, jenž bude zaměřena na řadu norem ISO/IEC 27000. Pro účely provedení analýzy rizik byla zvolena česká společnost, která se zabývá výrobou elektrotechnických a elektronických zařízení pro nejrůznější průmyslové aplikace. Společnost se zaměřuje především na zahraniční trh, ale působí i na českém trhu. V současné době tato firma zaměstnává více než 200 zaměstnanců. V rámci zachování anonymity společnosti bude využíván fiktivní název společnosti XY a nebudou zde uvedena žádná jména osob, která se podílí na chodu samotné společnosti. Cílem této praktické části a bakalářské práce je:

- Vypracování analýzy rizik s ohledem na ISO/IEC 27000 ve společnosti XY, kterou může společnost využít v rámci:
  - Certifikace s normou ISO/IEC 27000.
  - Získávání nových obchodních nabídek u zákazníků, jenž zajímá, jakým způsobem společnost nakládá s bezpečností informací.
  - Budoucí (opakované) analýzy rizik.
- Provedení diskuze s vedením společnosti XY ohledně výsledků analýzy rizik a prevence těchto rizik.

Samotná společnost, jenž je předmětem této analýzy rizik, se nepodílí na žádných konkrétních službách, které jsou uvedeny v zákoně č. 181/2014 Sb. dle § 3. Na společnost se tedy nevztahují povinnosti v oblasti kybernetické bezpečnosti dle zákona č. 181/2014 Sb.

Pro provedení analýzy rizik bude využita kvalitativní metoda, jenž využívá bodové stupnice. Postup analýzy byl stanovený na několik kroků, které na sebe postupně navazují. Jednotlivé kroky analýzy (určení výskytu hrozeb, určení dopadu hrozeb, výpočet výše rizika) jsou převzaty z odborné literatury [9] (není-li uvedeno jinak) a poupraveny tak, aby vyhovovaly parametrům pro provádění analýzy v dané společnosti. Postup analýzy rizik je následující:

1. Identifikace a definice aktiv.
2. Identifikace hrozeb.
3. Stanovení hodnoty aktiv.
4. Určení výskytu hrozeb.
5. Určení dopadu hrozeb.
6. Výpočet výše rizika.

7.1 Identifikace a definice aktiv

V prvním kroku je provedena identifikace a definice aktiv, ve které jsou vyjmenovány a popsány konkrétní aktiva společnosti. V rámci identifikace je kladen důraz především na důležitost těchto aktiv, které pro firmu představují. Následně jsou definována tím způsobem, že je určen:

- Zdroj aktiva.
- Aktivum.
- Nosič aktiva.

Tab. 1: Postup pro identifikaci aktiv

Zdroj	Aktivum	Nosič aktiva
Server	Databáze zákazníků	Informační systém (Software)
Server	Technická data	

V tabulce 1 je uveden příklad, jakým způsobem bude provedena identifikace aktiv, kde je uvedeno konkrétní aktivum, zdroj aktiva a samotný nosič aktiva.

Zdrojem aktiva se rozumí to, kde jsou dané aktiva uloženy, a kde probíhá jejich práce s nimi. Nosičem aktiva je myšlen konkrétní software, systém či jiná aplikace, která může být instalována například na pracovní stanici uživatele. Tento software dále pak zprostředkovává data, která jsou uložena na konkrétním zdroji.

Seznam identifikovaných aktiv je následující:

- Obchodní informace.
- Obchodní kontakty.
- Informace o zaměstnancích.
- Informace o zákaznících.
- Technická data (výrobní postupy, dokumentace, know-how, apod.).
- Firemní předpisy.
- Firemní dokumenty.
- Záznamy o jednání.
- Informace o projektech.
- Strategická obchodní data.

- Evidence smluv.
- Evidence právních dokumentů.

Pro bližší uvedení společnosti jsou uvedeny následující informace. Samotná společnost, jenž je předmětem analýzy rizik, využívá ke svému podnikání a řízení firmy firemní server, ke kterému má přístup přes 150 počítačů, které se nachází především v kancelářích. Tyto počítače aktuálně běží na operačním systému Windows 10 nebo Windows 7. Pro účely vzdálené komunikace vlastní někteří zaměstnanci firmy i firemní notebook, pomocí něhož mohou na dálku komunikovat s firemním serverem a jeho aplikacemi. I samotné notebooky běží na operačním systému Windows 10. Další elektronická zařízení, kterými firma disponuje, jsou poté využity v rámci samotné výroby. Na firemním serveru běží většina důležitých aplikací a systémů, pomocí kterých firma funguje. Tyto aplikace slouží jednak pro plánování výroby, řízení samotné výroby či pro komunikaci zaměstnanců mezi sebou nebo se zákazníky a podobně. Případně jsou některé aplikace (nosiče aktiv) nainstalovány přímo na samotných počítačích či firemních noteboocích.

Pro zpracování a nakládání s daty jsou dále využity externí webové služby, které jsou využity v rámci řízení vztahů se zákazníky, zpracování údajů o zákaznících, evidenci právních dokumentů či například záznamů o jednání a podobně. Tyto externí webové služby jsou tedy jakýmsi zpřehledněním informací pro jejich lepší správu a nakládání s nimi. V rámci pohovorů s danou firmou byly během tohoto kroku zjištěny následující aktiva, ke kterým budou nyní přiřazeny konkrétní nosiče aktiv.

Tab. 2: Identifikace aktiv 1/2

Zdroj	Aktivum	Nosič aktiva
Server	Obchodní informace Obchodní kontakty Informace o zaměstnancích Informace o zákaznících Technická data	Informační systém
	Technická data	Nástavbový software pro výrobu
	Technická data	Nástavbový software pro plánování a řízení výroby (webové rozhraní)

Tab. 3: Identifikace aktiv 2/2

Zdroj	Aktivum	Nosič aktiva
Server	Firemní předpisy Firemní dokumenty	Software pro řízení dokumentace a správu managementu
	Informace o zaměstnancích	Docházkový software
	Informace o zaměstnancích	Software pro správu přístupového systému
	Technická data	FTP
	Obchodní informace Obchodní kontakty Technická data Informace o zaměstnancích Informace o projektech Informace o zákaznících	Software pro e-mailovou komunikaci
Externí webová služba (Cloud)	Obchodní informace Obchodní kontakty Záznamy o jednání Informace o zaměstnancích Informace o zákaznících Informace o projektech	Software pro řízení vztahů se zákazníky
	Strategická obchodní data Informace o zaměstnancích Informace o zákaznících	Software pro strategické plánování
	Evidence smluv Evidence právních dokumentů Informace o zaměstnancích Informace o zákaznících	Software pro správu právní agendy

Jak již bylo zmíněno výše, společnost v rámci svého podnikání využívá firemní server a externí webové služby, které jsou různého charakteru a každý software, služba nebo aplikace plní jiný účel. Z výše vyjmenovaných aktiv si lze všimnout toho, že převážná část se nachází

v informačním systému, v softwaru pro e-mailovou komunikaci či softwaru pro řízení vztahů se zákazníky. Tyto samotné nosiče aktiv se zatím jeví i jako největší nosiče informací ze všech výše uvedených. V informačním systému se nachází veškeré informace o zákaznících či zaměstnancích. Dále pak informační systém v sobě zahrnuje veškerá technická data, výrobní postupy, výrobní dokumentace a podobně. V případě přenosu technický dat a dalších dokumentací je využit přenos dat pomocí protokolu FTP (File Transport Protocol). [9]

Na informační systém dále pak navazuje nástavbový software pro samotnou výrobu, kde se sice jedná o informace převzaté z informačního systému, nicméně jde pouze o informace určené pro samotnou výrobu (technická data, výrobní postupy, dokumentace atd.). K těmto informacím mají přístup především samotní dělníci ve výrobě pomocí firemních elektronických zařízení.

Co se týče dalších nosičů aktiv, lze zde nalézt další software, který je využit pro řízení dokumentace v souladu s požadavky norem nebo samotnou správou managementu. Nachází se zde firemní předpisy, dokumenty a jiné náležitosti. V případě docházkového systému jde především o zdroj informací o zaměstnancích. Docházkový systém zaznamenává zaměstnance pomocí přístupových karet, kde vyhodnocuje příchody a odchody zaměstnanců či monitoruje jejich pohyb v rámci budovy. Docházkový systém dále doplňuje software pro správu přístupového systému, kde jsou nastaveny práva do jednotlivých částí budov. Opět i zde je možné objevit základní informace o zaměstnancích (např. jeho jméno, příjmení a osobní číslo, které mu bylo přiděleno při vstupu do pracovního poměru)

Zbývající nosiče aktiv jsou již externí webové služby, které slouží zejména pro zpřehlednění informací, jenž firma shromažďuje. Tyto informace mohou být jak obchodního charakteru, tak personálního charakteru nebo právního charakteru a podobně, viz poslední tabulka identifikace aktiv.

7.2 Identifikace hrozeb

Navazujícím krokem, po identifikaci a definici aktiv, je identifikace hrozeb. Po diskuzi s vedením společnosti byly zjištěny následující hrozby, které mohou ohrozit daná aktiva. Po identifikaci je možné poté provést v následujících krocích již samotné určení hodnoty aktiv, určení výskytu hrozeb a dopadu těchto hrozeb na výše uvedená aktiva.

V rámci identifikace hrozeb byly zjištěny následující hrozby:

- Ohrožení interní infrastruktury vyšší a cizí mocí. (zničení, poškození, nedostupnost dat)
    - Požár serveru.
    - Vytopení serveru.
    - Nedostupnost kvůli uzavření objektu státním orgánem (policie, hasiči a podobně).
    - Odstávka energie.
- Útok na stanici uživatele (pro odstavení stanice, pro krádež dat, pro přípravu na komplexní útok, pro útok na data na síti).
    - Útok na operační systém (využití zranitelnosti systému Windows bez interakce uživatele).
    - Útok na aplikace a software (využití zranitelnosti těchto aplikací bez interakce uživatele).
    - Využití uživatelské interakce (kliknutí na škodlivý odkaz, spuštění škodlivého kódu v příloze e-mailu atd.).
    - Zneužití přihlašovacích údajů.
- Útok na data a systémy na serveru (pro způsobení nedostupnosti služeb a dat, pro krádež dat).
    - Útok na operační systém (využití zranitelnosti systému Windows bez interakce uživatele).
    - Útok na aplikace a software (využití zranitelnosti těchto aplikací bez interakce uživatele).
    - Využití uživatelské interakce (kliknutí na škodlivý odkaz, spuštění škodlivého kódu v příloze e-mailu atd.).
    - Zneužití přihlašovacích údajů při přístupu přes interní síť.
    - Zneužití přihlašovacích údajů při přístupu z internetu.
- Útok na komponenty interní infrastruktury (router, switch, Wi-Fi, diskové pole atd.).
    - Zranitelnost firmware komponent bez interakce uživatele.
    - Zneužití přihlašovacích údajů.

- Útok na internetovou konektivitu (pro způsobení nedostupnosti služeb, pro odposlech komunikace).
    - Útok na router (využití zranitelnosti routeru bez interakce uživatele).
    - Zahlcení DDoS útokem.
- Útok na webové služby (pro způsobení nedostupnosti služeb, krádež dat, pro poškození dat).
    - Využití zranitelnosti serverů s webovými službami bez interakce uživatele.
    - Zneužití přihlašovacích údajů.
    - Zahlcení DDoS útokem.
- Útok uživatele na data (autorizovaný uživatel provede poškození dat).
    - Útok na e-maily.
    - Útok na sdílená data.
    - Útok na informační systémy.
- Krádež datových médií.
    - Krádež přístupových karet.
    - Využití zranitelnosti systému, bez interakce uživatele, ke změně přístupových práv.
- Vyzrazení informací z řad uživatelů.
    - Úmyslné vyzrazení informací (např. osoba ve zkušební pracovní době či nespokojený zaměstnanec)
    - Neúmyslné vyzrazení informací (např. špatně odeslaný e-mail a podobně)

Výše uvedené hrozby jsou uvedeny velmi obecně, neboť způsobů a možností, jak lze jednotlivé útoky provést je velká škála. Z toho důvodu je ke každému bodu uveden alespoň jeden příklad, jakým způsobem může být daný útok proveden.

7.3 Stanovení hodnoty aktiva

Po následné identifikaci aktiv a hrozeb je provedeno stanovení hodnoty aktiva, resp. nosičů aktiv. Stanovení hodnoty je prováděno proto, aby bylo zřejmé, které aktiva jsou z hlediska důležitosti a fungování nejvíce závažná pro danou firmu. Pro stanovení hodnot u konkrétního aktiva bude využit Common Vulnerability Scoring System (CVSS) verze 3. Při hodnocení bude brána v ohled pouze jen ta nejzávažnější hrozba, která může ohrozit dané aktivum a na základě vyhodnocení zranitelnosti konkrétního nosiče aktiva bude pomocí CVSS určena hodnota aktiv. [20]

Obr. 7: Logo CVSS [20]

Common Vulnerability Scoring System je volně dostupný standard pro posouzení zranitelnosti systému a chyb zabezpečení počítačového systému, který byl uvedený na trh v roce 2005, jako první verze. Systém CVSS poskytuje způsob, jak lze zachytit hlavní charakteristiky zranitelnosti dle několika metrik a umožňuje tak vytvořit numerické skóre odrážející závažnost dané zranitelnosti. Numerické skóre je poté převedeno do kvalitativní podoby, kde může nabývat následujících hodnot, viz tabulka. [20]

Tab. 4: Hodnocení dle CVSS [20]

Hodnocení dle CVSS	**Skóre**
Nulová hodnota	0,0
Nízká hodnota	0,1 – 3,9
Střední hodnota	4,0 – 6,9
Vysoká hodnota	7,0 – 8,9
Kritická hodnota	9,0 – 10

Z výše uvedené tabulky si lze všimnout hodnot, které CVSS vyhodnocuje na základě zvolených metrik. Tyto výsledné hodnoty mají tu výhodu, že se jedná o standardizované skóre zranitelnosti, které může být využito napříč všemi společnostmi po celém světě a správa těchto zranitelností tak zůstává stejná. V současné době je na trhu třetí verze, která byla uvedena v roce 2015 a ta se oproti předchozí verzi liší v několika metrikách, které výrazně vylepšují samotné hodnocení zranitelností. [20]

Obr. 8: CVSS Calculator (verze 3.0) [20]

Na obrázku si lze všimnout osmi základních metrik, pomocí kterých je provedeno určení dané zranitelnosti a získání tak hodnoty dané zranitelnosti. CVSS disponuje sadou několika dalších metrik pro upřesnění dané zranitelnosti, avšak pro účely analýzy rizik bude plně dostačovat využití těchto osmi základních. Tyto jednotlivé metriky budou nyní detailněji popsány.

Tab. 5: Metriky CVSS 1/4 [20]

Metrika	Možnost	Popis
Attack Vector (AV) Typ útoku	**Physical** Fyzický	Útočník potřebuje fyzický přístup k aktivu, aby s ním mohl poté dále nakládat a manipulovat.
	Local Lokální	Útočníkovi se stačí pouze přihlásit lokálně do daného systému nebo může využít interakci uživatele.
	Adjacent Přilehlý	Přístup k aktivu je útočníkovi umožněn na úrovni místní sítě.
	Network Síťový	Je nejzávažnější, neboť přístup k aktivu je na síťové úrovni. Tato možnost je zvolena tehdy, kdy je patrné, že k aktivu existuje přístup pomocí sítě (skrze internet).

Tab. 6: Metriky CVSS 2/4 [20]

Metrika	Možnost	Popis
Attack complexity (AC) Složitost útoku	**Low** Nízká	Složitost útoku je nízká, protože k realizaci útoku nemusí být splněno žádných podmínek pro získání přístupu k aktivu.
	High Vysoká	Útočník potřebuje investovat nějaké úsilí při přípravě nebo provedení útoku (např. útočník musí provést průzkum na zaměřený cíl, útočník musí provést přípravu prostředí pro pozdější využití útoku).
Privileges Required (PR) Požadované oprávnění	**None** Žádné	Útočník nemusí disponovat žádným účtem v systému a nemusí tak provádět žádnou autorizaci.
	Low Malé	Útočník má v systému některý z účtů s omezenými právy, které poskytují základní uživatelské funkce. Tyto funkce by mohly ovlivnit pouze nastavení a soubory, jenž vlastní sám uživatel.
	High Vysoké	Útočník musí mít v systému vyšší oprávnění (např. administrativní), aby mohl zneužít chyby v zabezpečení nad zranitelnou částí, která by mohla ovlivnit nastavení a soubory v celé svém rozsahu.
User Interaction (UI) Interakce uživatele	**None** Žádná	Zranitelná část může být využívána bez interakce jakéhokoliv uživatele. Není vyžadován žádný uživatelský přístup ze strany uživatele k provedení útoku.
	Required Požadovaná	Zranitelná část je využita ze strany interakce uživatele, tzn. že uživatel provede např. otevření škodlivého dokumentu či odkazu.

Tab. 7: Metriky CVSS 3/4 [20]

Metrika	Možnost	Popis
Scope (S) Rozsah útoku	**Unchanged** Nezměněný	Zranitelnost i dopad se týká stejných komponentů.
	Changed Změněný	Zranitelný komponent se liší od komponentu ovlivněného a zneužití zranitelnosti má tak dopad na jinou komponentu. (např. pokud dochází k útoku na server a dojde ke ztrátě dat uživatelů, je rozsah útok změněný, protože se netýká již pouze serveru, ale i dat uživatelů, aplikací běžících na serveru a podobně)
Confidentiality (C) Dopad na důvěrnost	**None** Žádný	Nedochází se k žádnému dopadu na důvěrnost, tedy žádnému úniku dat v rámci daného zranitelné části
	Low Malý	Dochází v malé ztrátě důvěrnosti. Útočník získal přístup k některým omezeným informacím, ale útočník nemá kontrolu nad získanými informacemi.
	High Velký	Nastává kompletní ztráta důvěrnosti, což vede k úniku veškerých citlivých informací a dat k útočníkovi.
Integrity (I) Dopad na integritu	**None** Žádný	Ve zranitelné části nedochází k žádné ztrátě integrity na datech a informacích.
	Low Malý	Modifikace dat je umožněna, ale je omezeno množství dat. Dochází tak k malé ztrátě integrity.
	High Velký	Dochází k úplné ztrátě integrity nebo k úplné ztrátě ochrany informací. Útočník je schopen modifikovat veškeré soubory a znehodnotit je tak.

Tab. 8: Metriky CVSS 4/4 [20]

Metrika	Možnost	Popis
Availability (A) Dopad na dostupnost	**None** Žádný	V rámci ovlivněného komponentu nedochází k žádnému dopadu na dostupnost dat.
	Low Malý	Data jsou částečně nebo plně dostupné, či například jsou plně k dispozici pouze po určitou dobu. Přístup k datům tedy není plně odepřen, ale existují částečná zamítnutí.
	High Velký	Přístup k datům je zcela odepřen a dochází k úplné ztrátě dostupnosti. Tato ztráta dostupnosti je buď udržovaná (útočník pokračuje nadále v útoku) nebo přetrvávající (stav omezení dostupnosti přetrvává i po dokončení útoku).

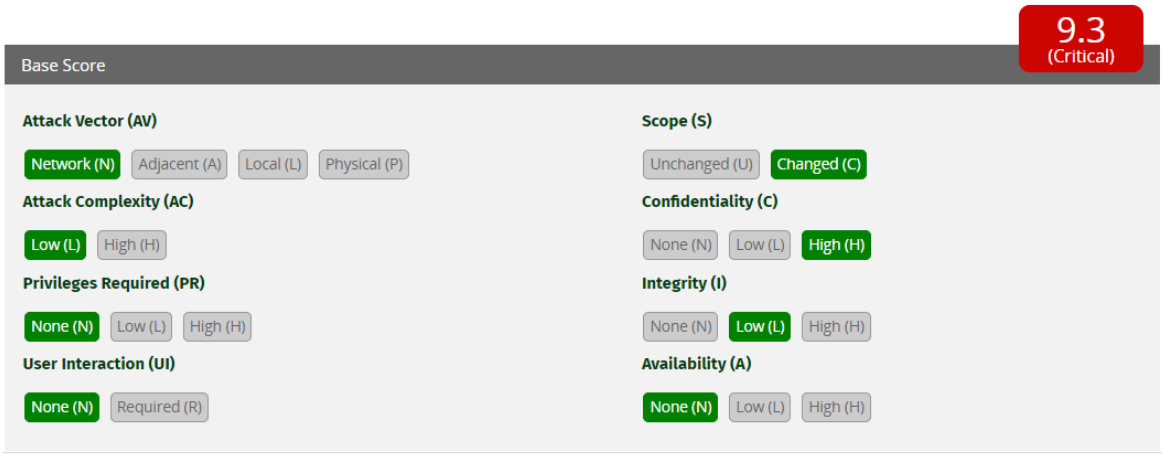
Výše uvedené tabulky popisují 8 základních metrik, pomocí kterých je získána standardizovaná hodnota zranitelnosti. Pomocí těchto metrik a uvedených možností, kterými disponují, se budou hodnotit identifikovaná aktiva, resp. nosiče aktiv.

Při stanovení hodnoty aktiva se posuzuje pouze ta nejzávažnější hrozba či událost, která by vedla k přístupu samotným aktivům. Nejprve bude představena tabulka s finálními hodnotami, jež byly u daných nosičů aktiv zjištěny a poté bude uveden jeden příklad, jakým způsobem byl veden postup.

Tab. 9: Stanovení hodnot aktiv

Zdroj	Nosič aktiva	Hodnota aktiv (A)
Server	Informační systém	8,5
	Nástavbový software pro výrobu	6
	Nástavbový software pro plánování a řízení výroby (webové rozhraní)	6
	Software pro řízení dokumentace a správu managementu	8,4
	Docházkový software	6,4
	Software pro správu přístupového systému	6,4
	FTP	5,3
	Software pro e-mailovou komunikaci	7,5
Externí webová služba (Cloud)	Software pro řízení vztahů se zákazníky	9,3
	Software pro strategické plánování	5,8
	Software pro správu právní agendy	8,6

Při pohledu do tabulky si lze všimnout toho, že nejvyšších hodnot nabývá především software pro řízení vztahu se zákazníky či software pro správu právní agendy a samotný informační systém. Přehlednější vyobrazení hodnot je na následujících stránkách.



Obr. 9: Hodnocení nosiče aktiva (Software pro řízení vztahů se zákazníky)

Pro názornou ukázku bude nyní rozebrán postup, který byl využit při určování hodnot dle CVSS kalkulátoru. Pro příklad bude použit nosič aktiva „Software pro řízení vztahů se zákazníky“, u kterého se hodnota zastavila na 9,3.

Nejzávažnější hrozba, jenž v tomto případě hrozí u tohoto typu nosiče aktiva, je především útok na webové služby v podobě zneužití přihlašovacích údajů, či jakýkoliv jiný způsob, který by mohl vést k získaní přístupu do účtů uživatelů společnosti.

Jelikož se jedná externí webovou službu musí být Attack Vector (typ útoku) zvolen Network (N), tedy síťový typ útoku, neboť útočník může k danému nosiči přistupovat z internetu. Následující metrikou je Attack Complexity (složitost útoku), kde je zvolena hodnota Low (L). Nízká hodnota je zvolena z toho důvodu, že útočník se může pokoušet o zadání hesla v určitém cyklu, kdy bude zkoušet různé varianty hesel a nemusí k tomu splňovat žádné další podmínky.

Následuje metrika Privileges Required (požadovaná oprávnění), u které je zvolena hodnota None (N), tedy hodnota žádná. Ta je zvolena z toho důvodu, protože útočník k provedení útoku nepotřebuje žádné požadované oprávnění. User Interaction (uživatelská interakce) je na hodnotě None (N), jelikož útok je možné provést bez jakékoliv interakce uživatele.

Poslední čtyři metriky jsou Scope (rozsah útoku) a dopady na důvěrnost, integritu a dostupnost. Rozsah útoku je ohodnocen jako Changed (C), tedy změněný. To z toho důvodu, neboť případná změna dat, odcizení dat nebo zničení těchto dat by mohlo ovlivnit další komponent. Při provedení úspěšného útoku je dopad na důvěrnost hodnocen jako High (H), jelikož útočník má v ten moment k dispozici veškeré obchodní informace, obchodní kontakty, informace o zaměstnancích, zákaznících či informace o proběhlých nebo

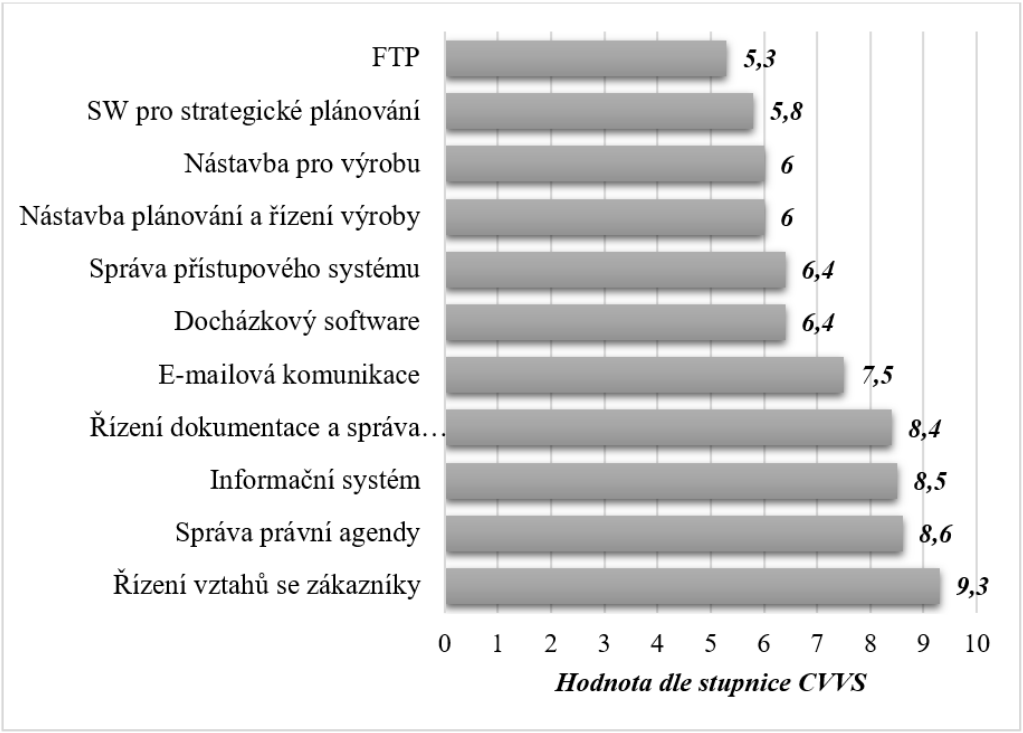
probíhajících jednání. Dopad na integritu je v tomto případě na hodnotě Low (L). Útočník může provádět modifikaci dat, ale nikoliv v úplné míře. Samotné hodnocení uzavírá metrika dopad na dostupnost, která je ohodnocena jako None (N). Útočník sice získá přístup k datům, avšak žádným způsobem neohrozí dostupnost těchto dat.

Obr. 10: Vector String

(Software pro řízení vztahů se zákazníky)

Po ohodnocení daného nosiče je získán Vector String, pomocí kterého je možné vrátit se zpět k původním zvoleným hodnotám, které byly při předchozím ohodnocení zvoleny. Tyto hodnoty se vkládají do políčka pro URL adresu v internetovém prohlížeči hned za adresu, která odkazuje na samotný kalkulátor. Před Vector String se ještě vkládá symbol # a následně poté je vložena hodnota Vector Stringu. Tvar tedy bude vypadat následujícím způsobem.

Obr. 11: Tvar adresy při zadávání Vector String



Obr. 12: Přehled hodnot aktiv u konkrétních nosičů aktiv

(od nejmenšího po největší)

Na výše uvedeném obrázku si lze povšimnout veškerých nosičů aktiv a jejich hodnot, které jsou v tomto případě seřazeny od nejmenšího po největší. Nejvýše ohodnoceným nosičem aktiv je v tomto případě „Software pro řízení vztahů se zákazníky“ (9,3), neboť tento software v sobě zpracovává velké množství obchodních informací, obchodních kontaktů, informací o zaměstnancích, zákaznících a dalších důležitých obchodních záležitostí.

Následuje software pro správu právní agendy, u kterého je vypočítaná hodnota 8,6. Tento software je především správcem veškerých smluv ať už se zákazníky, dodavateli, zaměstnanci nebo dalších právních dokumentů.

Hlavní třetici uzavírá samotný informační systém, který je z hlediska fungování naprosto nezbytný, neboť na něm běží kompletně celá výroba. Hodnota informačního systému nabývá hodnoty 8,5 dle CVSS kalkulátoru.

Tab. 10: Vector String nosičů aktiv 1/2

Nosič aktiva	**Vector String**
Informační Systém	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
Nástavbový software pro výrobu	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L
Nástavbový software pro plánování a řízení výroby (webové rozhraní)	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L
Software pro řízení dokumentace a správu managementu	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:L
Docházkový software	CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
Software pro správu přístupového systému	CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
FTP	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Software pro e-mailovou komunikaci	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Software pro řízení vztahů se zákazníky	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N

Tab. 11: Vector String nosičů aktiv 2/2

Nosič aktiva	Vector String
Software pro strategické plánování	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L
Software pro správu právní agendy	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Pro přehled zbývajícího hodnocení je v horní tabulce uveden Vector String u všech jednotlivých nosičů dat.

7.4 Určení výskytu hrozeb

Následujícím krokem při analýze rizik bude určení výskytu dané hrozby. Jak již bylo uvedeno výše, jedná o bodové hodnocení, které se pohybuje v rozmezí hodnot od 1 do 5.

Tab. 12: Hodnocení pro určení výskytu hrozeb

Hodnocení	Slovní vyjádření	Četnost výskytu
1	Nahodilá hrozba	Hrozba se může vyskytnout jen velmi málo (jednou za 5 let nebo četnost výskytu hrozby blíží k nule)
2	Nepravděpodobná hrozba	Hrozba se může vyskytnout jen velmi zřídka (jednou za 3 roky)
3	Pravděpodobná hrozba	Hrozba se může vyskytnout párkrát během jednoho roku (maximum 5)
4	Velmi pravděpodobná hrozba	Hrozba se může vyskytnout několikrát za rok či jednou do měsíce
5	Trvající hrozba	Hrozba se může vyskytovat opakovaně nebo několikrát do měsíce

Kde hodnota 1 je brána jako nejnižší hodnota a hodnota 5 je hodnotou maximální. V rámci doplnění tohoto kroku, je hodnocení doplněno o parametr „četnost výskytu“, který určuje, jak často se daná hrozba může vyskytnout.

Tab. 13: Určení výskytu hrozeb

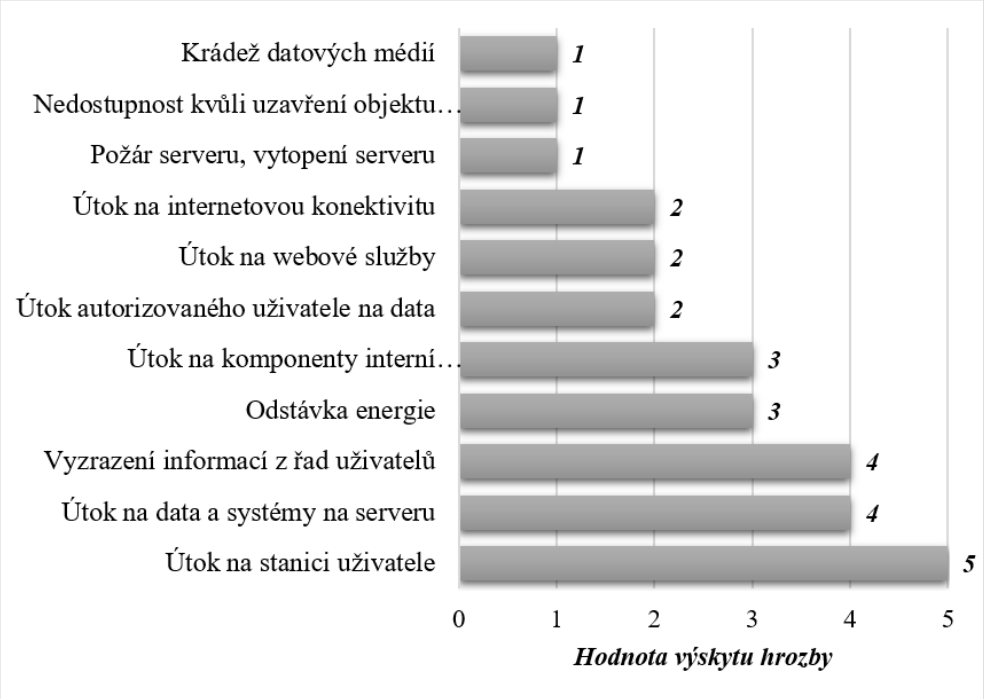
Určení výskytu hrozby (VH)		
Hrozba	**Hodnota**	**Slovní vyjádření**
Požár serveru, vytopení serveru	1	Nahodilá hrozba
Nedostupnost kvůli uzavření objektu státním orgánem	1	Nahodilá hrozba
Odstávka energie	3	Pravděpodobná hrozba
Útok na stanici uživatele	5	Trvající hrozba
Útok na data a systémy na serveru	4	Velmi pravděpodobná hrozba
Útok na komponenty interní infrastruktury	3	Pravděpodobná hrozba
Útok na internetovou konektivitu	2	Nepravděpodobná hrozba
Útok autorizovaného uživatele na data	2	Nepravděpodobná hrozba
Útok na webové služby	2	Nepravděpodobná hrozba
Krádež datových médií	1	Nahodilá hrozba
Vyzrazení informací z řad uživatelů	4	Velmi pravděpodobná hrozba

Při pohledu do tabulky je zjevné, že nejvyšší hodnotu „5“ obdržela hrozba „Útok na stanici uživatele“. Je to z toho důvodu, neboť samotná společnost se potýká s častými útoky na e-mailové schránky zaměstnanců. Nejčastěji se jedná o různé typy spamu či různých falešných odkazů vedoucích na škodlivé stránky a podobně. Jednou z příčin, takto častých útoků, může být to, že určitá skupina zaměstnanců má uveřejněné své e-mailové adresy

přímo na stránkách společnosti. Díky tomu tak mají potencionální útočníci možnost útočit na tyto e-mailové schránky, pomocí kterých se snaží proniknout ke stanici uživatele skrze e-mailovou schránku a získat tak přístup ke konkrétním informacím.

Co se týče například hrozby „Vyzrazení informací z řad uživatelů“ byla zvolena hodnota „4“. I když společnost zaměstnává více než 200 zaměstnanců, snaží se firma neustále rozvíjet a přijímat nové a kvalifikované zaměstnance. Při vzniku pracovního poměru u nového zaměstnance platí dle § 35 odst. 1 písm. a) zákona č. 262/2006 Sb. zákoník práce tříměsíční zkušební doba. Dochází tak k tomu, že někteří noví zaměstnanci ukončí pracovní poměr ve firmě již ve zkušební době a mohou tak informace, které získali při výkonu své práce v této společnosti, předávat dál. [21]

V případě hodnot „3“, tedy hrozeb pravděpodobných, se jedná hrozby typu „Útok na komponenty interní infrastruktury“ a „Odstávka energie“. K útokům na komponenty interní infrastruktury dochází během roku několikrát, nicméně četnost výskytu není vyšší jak hraniční hodnota 5. Nejčastěji se jedná o útoky přímo na samotný firemní router či dochází k útokům na bezdrátovou komunikaci (Wi-Fi). Odstávka energie je hrozba, která se zkrátka během roku může párkrát vyskytnout. Zejména se jedná o letní měsíce, kdy je zde vyšší šance odstávky energie.



Obr. 13: Přehled hrozeb a jejich výskytu

(od nejmenšího po největší)

Následující dvě hodnoty „2“ a „1“ jsou přiřazeny hrozbám, které svoji četnost výskytu mají velmi malou. Jde například o „Požár serveru, vytopení serveru“, „Nedostupnost kvůli uzavření objektu státním orgánem“, „Krádež datových médií“. U těchto hrozeb byla zvolena nejnižší možná hodnota, a to z toho důvodu, že samotná společnost se doposud s takovými hrozbami nesetkala. Hodnota „2“ byla zvolena tří zbývajících hrozeb „Útok autorizovaného uživatele na data“, „Útok na internetovou konektivitu“ a „Útok na webové služby“. Jelikož se společnost doposud s těmito hrozeb nesetkala, je zde daleko vyšší možnost výskytu než u předchozích hrozeb, které obdržely hodnocení 1.

7.5 Určení dopadu hrozeb

Posledním krokem, který se týká identifikovaných hrozeb je určení dopadu těchto hrozeb. Ten se může lišit z hlediska typů hrozby a z hlediska posuzovaného aktiva, zdali v případě uplatnění hrozby se jedná o fatální dopad pro danou společnost či nikoliv.

Tab. 14: Hodnocení pro určení dopadu hrozeb

Hodnocení	**Slovní vyjádření**
1	Hrozba nemá **žádný** dopad na organizaci
2	Hrozba má **zanedbatelný** dopad na organizaci
3	Hrozba může organizaci způsobit **menší finanční potíže**
4	Hrozba může způsobit **vážné** či **podstatné finanční ztráty**
5	Hrozba může způsobit organizaci **vážné finanční potíže** a **ohrožuje organizaci na existenci**

Pro hodnocení dopadu hrozeb bude i zde využito bodové ohodnocení, které bude nabývat stejných hodnot jako u předchozího kroku. Dle výše uvedené tabulky bude nyní provedeno hodnocení dopadu jednotlivých hrozeb u daných nosičů aktiv. Na základě diskuze s vedením firmy byly stanoveny následující dopady pro jednotlivé druhy hrozeb.

Tab. 15: Určení dopadu hrozeb 1/4

Dopad Hrozby (DH)	**Server**		
Hrozba	**Informační systém**	**Nástavbový SW pro výrobu**	**Nástavbový SW pro plánování a řízení výroby**
Požár serveru, vytopení serveru	4	3	2
Nedostupnost kvůli uzavření objektu státním orgánem	3	1	1
Odstávka energie	3	3	3
Útok na stanici uživatele	4	2	1
Útok na data a systémy na serveru	4	2	1
Útok na komponenty interní infrastruktury	4	2	1
Útok na internetovou konektivitu	2	3	1
Útok autorizovaného uživatele na data	4	3	4
Krádež datových médií	4	1	1
Vyzrazení informací z řad uživatelů	4	3	4

Tab. 16: Určení dopadu hrozeb 2/4

Dopad Hrozby (DH)	**Server**		
Hrozba	**SW pro řízení dokumentace a správu managementu**	**Docházkový software**	**SW pro správu přístupového systému**
Požár serveru, vytopení serveru	2	2	2
Nedostupnost kvůli uzavření objektu státním orgánem	1	1	1
Odstávka energie	2	1	1
Útok na stanici uživatele	2	2	2
Útok na data a systémy na serveru	2	2	2
Útok na komponenty interní infrastruktury	2	2	2
Útok na internetovou konektivitu	1	-	-
Útok autorizovaného uživatele na data	3	2	1
Krádež datových médií	2	2	1
Vyzrazení informací z řad uživatelů	3	2	1

Tab. 17: Určení dopadu hrozeb 3/4

Dopad Hrozby (DH)	**Server**	
Hrozba	**FTP**	**SW pro e-mailovou komunikaci**
Požár serveru, vytopení serveru	1	4
Nedostupnost kvůli uzavření objektu státním orgánem	1	2
Odstávka energie	2	3
Útok na stanici uživatele	2	4
Útok na data a systémy na serveru	2	4
Útok na komponenty interní infrastruktury	2	4
Útok na internetovou konektivitu	2	2
Útok autorizovaného uživatele na data	3	3
Krádež datových médií	2	4
Vyzrazení informací z řad uživatelů	3	3

Tab. 18: Určení dopadu hrozeb 4/4

Dopad Hrozby (DH)	**Externí webová služba (Cloud)**		
Hrozba	**SW pro řízení vztahů se zákazníky**	**SW pro strategické plánování**	**SW pro správu právní agendy**
Nedostupnost kvůli uzavření objektu státním orgánem	1	1	1
Útok na stanici uživatele	4	2	4
Útok na komponenty interní infrastruktury	4	2	4
Útok autorizovaného uživatele na data	4	2	4
Útok na webové služby	4	2	4
Vyzrazení informací z řad uživatelů	4	2	4

Výše uvedené tabulky dávají jednoznačný přehled o tom, jak moc velký dopad může mít konkrétní hrozba na dané nosiče aktiva, resp. aktiva samotné. Při pohledu do první tabulky se jeví „Informační systém“ jako nejvíce náchylný na důsledky daných hrozeb. Jak již bylo mnohokrát zmiňováno „Informační systém“ je nepostradatelným prostředkem (aplikací) pro samotné řízení firmy a chod samotný. Z toho důvodu je většina hrozeb, z hlediska dopadu, ohodnocena hodnotou „4“, tedy druhou nejvyšší ze stupnice. V dalším případě se poté jedná o „SW pro e-mailovou komunikaci“, kde i v jako předchozím případě je dopad hrozeb nejčastěji ohodnocen známkou „4“. Jelikož se jedná o hlavní způsob jednání se zákazníky a zaměstnanci v rámci firmy, je zcela patrné že dopad hrozeb u tohoto nosiče aktiva bude nabývat vyšších hodnot, jelikož pracuje s takovými informacemi, které by mohli být pro potencionálního útočníka velice lákavými.

Dále pak jsou zde tři externí webové služby, které daná firma využívá. Dle výše uvedeného hodnocení jsou „SW pro řízení vztahů se zákazníky“ a „SW pro správu právní agendy“ nejvíce ohroženými nosiči aktiv z hlediska externích webových služeb. Je to z toho důvodu,

neboť představují velmi důležitý zdroj obchodních a jiných informací. Při hodnocení dopadů hrozeb byly brány v potaz i již aplikované protiopatření, které daná firma využívá.

7.5.1 Výpočet výše rizika

Posledním krokem, po získání veškerých informací o hrozbách, aktivech a podobně, je vypočítána výše rizika. Tato výše rizika využívá jednoduchého vztahu za pomocí tří parametrů, jenž byly uvedeny výše, tedy hodnota aktiva, výskyt hrozby a dopad hrozby.

$$R = A \cdot VH \cdot DH \tag{3}$$

Kde: R je Riziko

A je Hodnota aktiva

VH je Výskyt hrozby

DH je Dopad hrozby

Po dosazení veškerých hodnot do vztahu je vypočítána hodnota rizika, která je poté dle tabulky vyhodnocena.

Pro příklad je uveden následující případ, kde je převzata hodnota 8,5 (Informační systém). Tato hodnota je dle stupnice CVSS posouzena jako hodnota vysoká. V případě hrozby „Požár serveru, vytopení serveru“ je výskyt hrozby ohodnocen hodnotou „1“. Jedná se tedy o hrozbu nahodilou. Posledním vstupujícím parametrem je dopad hrozby, kde konkrétní hrozba byla na stupnici od 1 do 5 ohodnocena hodnotou „4“, tedy „Hrozba může způsobit vážné či podstatné finanční ztráty“. Při získání všech hodnot proměnných jsou hodnoty dosazeny do vztahu (3):

$$R = 8{,}5 \cdot 1 \cdot 4$$

$$R = 34$$

Je vypočítaná výše rizika, která má hodnotu 34. Při pohledu do tabulky pro vyhodnocení výše rizika se jedná o riziko spadající do kategorie „bezvýznamné riziko“.

Tab. 19: Hodnocení výše rizika

Hodnocení	Slovní vyjádření
0–50	**Bezvýznamné** riziko pro organizaci (Není nutné provádět žádná protiopatření)
51–100	**Akceptovatelné** riziko pro organizaci (Riziko je z hlediska vypočtené hodnoty tolerovatelné a je doporučeno provádět monitorování)
101–150	**Mírné** riziko pro organizaci (Riziko je nutné monitorovat a je doporučeno provést požadovaná protiopatření)
151–200	**Nežádoucí** riziko pro organizaci (Z hlediska výše rizika je nutné provést zásadní protiopatření pro snížení rizika)
201–250	**Nepřijatelné** riziko pro organizaci (Protiopatření jsou zde naprosto nutná, neboť je ohrožen chod a existence organizace)

Nyní v samotném závěru analýzy rizik proběhne dosazení veškerých získaných hodnot, z předchozích kroků, do daného vztahu (3) a bude tak vypočítaná velikost daného rizika.

Tab. 20: Vypočítané hodnoty rizik 1/4

Riziko (R)	**Server**		
Hrozba	**Informační Systém**	**Nástavbový SW pro výrobu**	**Nástavbový SW pro plánování a řízení výroby**
Požár serveru, vytopení serveru	34	18	12
Nedostupnost kvůli uzavření objektu státním orgánem	25,5	6	6
Odstávka energie	76,5	54	54
Útok na stanici uživatele	170	60	30
Útok na data a systémy na serveru	136	48	24
Útok na komponenty interní infrastruktury	102	36	18
Útok na internetovou konektivitu	34	36	12
Útok autorizovaného uživatele na data	68	36	48
Krádež datových médií	34	6	6
Vyzrazení informací z řad uživatelů	136	72	96

Tab. 21: Vypočítané hodnoty rizik 2/4

Riziko (R)	**Server**		
Hrozba	**SW pro řízení dokumentace a správu managementu**	**Docházkový software**	**SW pro správu přístupového systému**
Požár serveru, vytopení serveru	16,8	12,8	12,8
Nedostupnost kvůli uzavření objektu státním orgánem	8,4	6,4	6,4
Odstávka energie	50,4	19,2	19,2
Útok na stanici uživatele	84	64	64
Útok na data a systémy na serveru	67,2	51,2	51,2
Útok na komponenty interní infrastruktury	50,4	38,4	38,4
Útok na internetovou konektivitu	16,8	-	-
Útok autorizovaného uživatele na data	50,4	25,6	12,8
Krádež datových médií	16,8	12,8	6,4
Vyzrazení informací z řad uživatelů	100,8	51,2	25,6

Tab. 22: Vypočítané hodnoty rizik 3/4

Riziko (R)	**Server**	
Hrozba	**FTP**	**SW pro e-mailovou komunikaci**
Požár serveru, vytopení serveru	5,3	30
Nedostupnost kvůli uzavření objektu státním orgánem	5,3	15
Odstávka energie	31,8	67,5
Útok na stanici uživatele	53	150
Útok na data a systémy na serveru	42,4	120
Útok na komponenty interní infrastruktury	31,8	90
Útok na internetovou konektivitu	21,2	30
Útok autorizovaného uživatele na data	31,8	45
Krádež datových médií	10,6	30
Vyzrazení informací z řad uživatelů	63,6	90

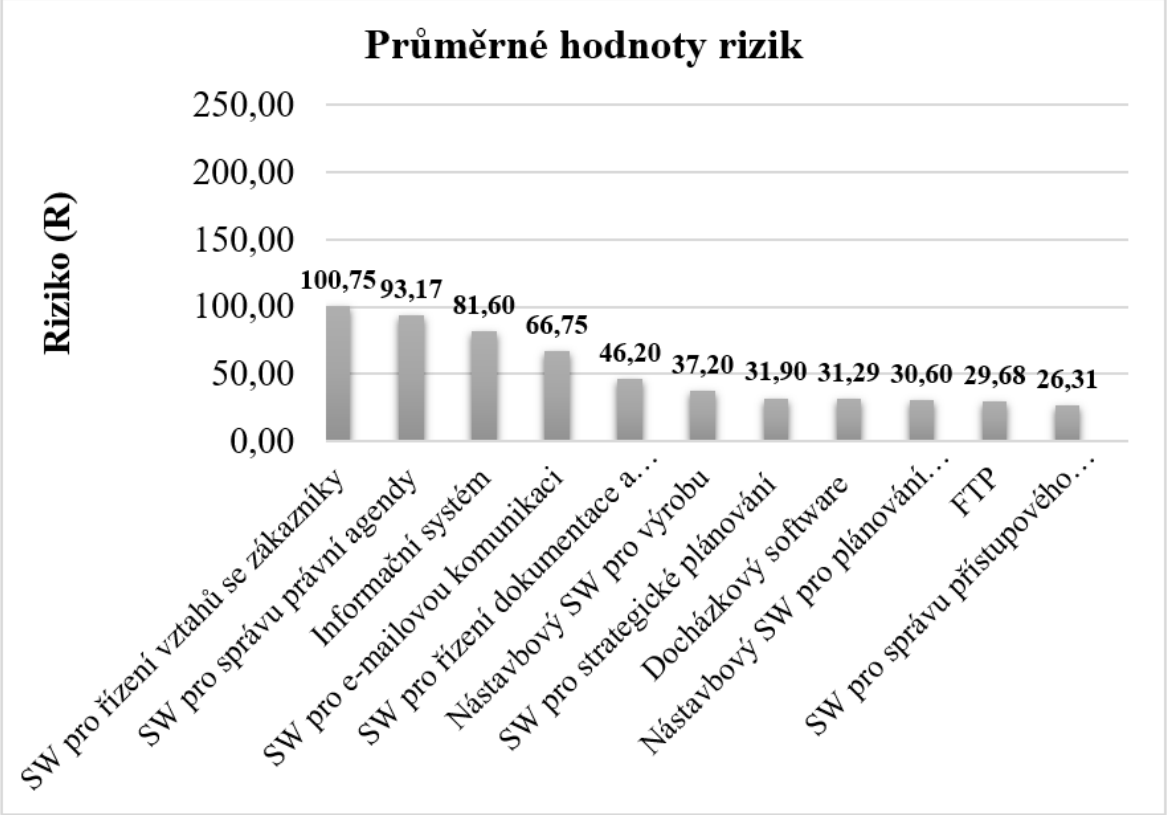
Tab. 23: Vypočítané hodnoty rizik 4/4

Riziko (R)	**Externí webová služba (Cloud)**		
Hrozba	**SW pro řízení vztahů se zákazníky**	**SW pro strategické plánování**	**SW pro správu právní agendy**
Nedostupnost kvůli uzavření objektu státním orgánem	9,3	5,8	8,6
Útok na stanici uživatele	186	58	172
Útok na komponenty interní infrastruktury	111,6	34,8	103,2
Útok autorizovaného uživatele na data	74,4	23,2	68,8
Útok na webové služby	74,4	23,2	68,8
Vyzrazení informací z řad uživatelů	148,8	46,4	137,6

Ve výše uvedených tabulkách jsou uvedeny hodnoty daných rizik pro konkrétní hrozbu a nosič aktiv, resp. aktivum. V příloze je poté uveden soubor, který byl vypracován v rámci analýzy rizik. Jedná se o přílohu 1, která byla vypracována v softwaru Microsoft Excel. Tento soubor v sobě zahrnuje podrobnější a lépe rozvržené informace o samotné analýze rizik. Samotný „excelovský“ soubor obsahuje čtyři listy, kde první list obsahuje vstupní parametry s hodnotami, které se mají vyplnit. Na druhém listu je poté umístěn již samotný přehled a zpracování analýzy rizik s výsledky rizik k daným aktivům a podobně. Třetí list zahrnuje v sobě zejména veškeré grafy a hodnoty, které vychází z předchozího listu, pro lepší znázornění. Poslední čtvrtý list obsahuje nápovědu pro hodnocení jednotlivých parametrů, jenž vstupují do vztahu (3).

8 KONZULTACE VÝSLEDKŮ S VEDENÍM FIRMY

Během probíhající analýzy rizik probíhaly s vedením firmy rozsáhlé diskuze o tom, jakým směrem by se dále měla daná společnost, z hlediska informační bezpečnosti, ubírat. Ze zjištěných výsledků, které se podařilo zjistit během této analýzy rizik, může daná firma věnovat pozornost právě těmto oblastem, u kterých byly zjištěny nejvyšší hodnoty daných rizik. Z následujícího obrázku je patrné, které nosiče aktiv zaznamenaly nejvyšší hodnoty rizik.



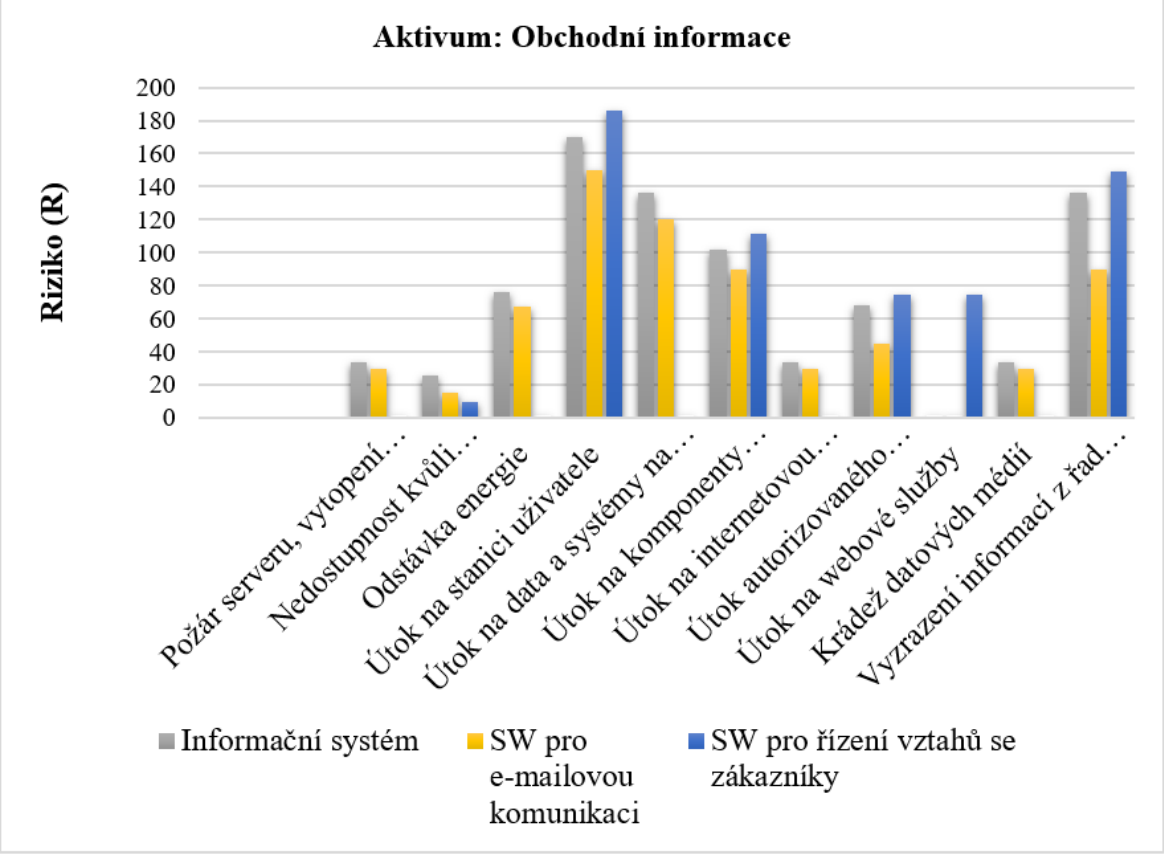
Obr. 14: Průměrné hodnoty rizik u daných nosičů aktiv

Ze zjištěných hodnot v rámci analýzy rizik se nejvyšší průměrné hodnoty rizik pohybují zejména u těchto nosičů aktiv:

- SW pro řízení vztahů se zákazníky **(100,75)**.
  - Obchodní informace.
  - Obchodní kontakty.
  - Záznamy z jednání.
  - Informace o zaměstnancích.
  - Informace o projektech.
  - Informace o zákaznících.

- SW pro správu právní agendy **(93,17)**.
    - Evidence smluv.
    - Evidence právních dokumentů.
    - Informace o zaměstnancích.
    - Informace o zákaznících.
- Informační systém **(81,60)**.
    - Obchodní informace.
    - Obchodní kontakty.
    - Informace o zaměstnancích.
    - Informace o zákaznících.
    - Technická data.

Ty v sobě zároveň nesou a zpracovávají daná aktiva, která jsou pod nimi uvedena. Lze si tak všimnout, že právě „SW pro řízení vztahů se zákazníky“ se jeví jako nejvíc náchylný na působení hrozeb a průměrná hodnota všech rizik se tak pohybuje na hodnotě 100,75.



Obr. 15: Výše rizik u jednotlivých hrozeb (Obchodní informace)

Při bližším pohledu na výše uvedený obrázek (úryvek z přílohy 1) si lze všimnout toho, že aktivum „Obchodní informace“ je nejvíce ohroženo hrozbou útoku na stanici uživatele. Konkrétně jde tedy o externí webovou službu (SW pro řízení vztahů se zákazníky), u níž byla vypočítána nejvyšší hodnota rizika.

Dle vyjádření vedení společnosti se samotná firma aktivně podílí na neustálém zlepšování informační bezpečnosti a školení svých zaměstnanců v rámci tohoto tématu. V budoucí době by se firma ráda podílela na zlepšení v několika oblastech a právě vypracovaná analýza rizik by měla firmě pomoci při:

- Zlepšování informační bezpečnosti.
- Budoucí získávání potencionálních zákazníků, které zajímá, jakým způsobem firma nakládá s informacemi.
- Využití analýzy rizik při certifikaci s normou ISO/IEC 27001.

S vyplývajících výsledků analýzy rizik se potvrdilo to, že dána firma má přehled o daných hrozbách, které firmu ohrožují a aktivně se snaží těmto hrozbám čelit a snižovat jejich výskyt. Během konzultací byly dále zjištěny následující opatření, kterými se společnost podílí na snižování výše uvedených rizik. Opatření jsou následující:

- AntiSpam.
    - Využití v rámci e-mailové komunikace.
- Antivirový program.
    - Využití v rámci zabezpečení firemních počítačů a notebooků.
- Bezpečnostní politika přílohy e-mailů.
    - Ochrana před otevřením příloh e-mailů.
- Školení zaměstnanců.
    - Aktivní školení zaměstnanců z informační bezpečnosti a bezpečnosti informací.
- Právní dokumenty.
    - Dohoda o mlčenlivosti mezi zaměstnavatelem a zaměstnancem.
- Pravidelná instalace aktualizací serverů a PC.
- Automatické uzamykaní stanic při nečinnosti Windows.
    - Uzamykání firemních počítačů po uplynutí stanovené doby, při nečinnosti Windows.
- Šifrování disků v noteboocích (BitLocker).

- Bezpečnostní politika hesel pro vstup do Windows (12 znaků + složitost).
- Omezení přístupu do Wi-Fi (IEEE 802.1x, MAC).
- Dvoufaktorová autentizace pro vzdálený přístup (Multi-factor authentication) pomocí mobilu či aplikace.
    - V případě vzdáleného přístupu pomocí notebooku, jsou zaměstnanci povinni využít dvoufaktorovou autentizaci skrze jejich osobní či firemní telefon.
- Pravidla na routeru pro externí přístupy z vybraných IP adres.
- Bezpečnostní politika nutnosti zabezpečení mobilu pomocí PIN v případě využívání firemního e-mailu.
    - V případě osobního telefonu musí mít daný zaměstnanec uzamčený telefon pomocí PINu, jinak není možné přistupovat k e-mailu skrze aplikaci v mobilu.
- Zabránění fyzického přístupu ke klíčovým prvkům interní infrastruktury (server, switche, disková pole, apod.).
    - Využití a nastavení práv pro přístupové karty zaměstnanců.
- Zálohování dat (metoda 3-2-1).
    - Tři kopie dat, na různých médiích.
- Bezpečnostní politika pro omezení spouštění spustitelného kódu z profilu uživatele.
- Omezení oprávnění uživatelů k prostředkům – Informační systém.
- Omezení oprávnění uživatelů k prostředkům – Sdílené složky.
- Omezení oprávnění uživatelů k prostředkům – Další systémy.

8.1 Závěrečné doporučení

Závěrečný bod se týká samotného zlepšení informační bezpečnosti. Na základě výsledků zjištěných v analýze rizik (uvedených v tomto dokumentu či v příloze 1) byl získán základní přehled o daných hrozbách a jejich rizicích. Aby bylo možné se aktivně podílet na snižování rizik a zlepšování tak informační bezpečnosti a bezpečnosti informací, je nutné provést závěrečné doporučení, které by mohlo vést ke zlepšení současného stavu. V rámci závěrečného doporučení jsou navrženy tři možnosti opatření:

- Využití SIEM technologií.
- Využití správce hesel LastPass a bezpečnostní politika hesel.
- Využití penetračního testování.

8.1.1 Využití SIEM technologií

Technologie Security information and event management (SIEM) je bezpečnostní software, jak již z názvu vypovídá, který se zabývá managementem bezpečnosti informací a událostí. Tyto technologie SIEM slouží zejména k monitorování, ukládání či k správě bezpečnostních událostí, které jsou sbírány z konkrétních zařízení uvnitř IT infrastruktury. Díky analytickým funkcím dokáže model SIEM provést identifikaci bezpečnostních hrozeb a zranitelností v daném IT prostředí. [22] [23] [24]

Modernější SIEM produkty dokáží zejména sbírat data a dále je poté doplňovat o informace a aktuálních bezpečnostních situacích ze všech koutů světa. Tyto informace poskytují zejména profesionální dohledové týmy, které se zabývají právě touto analýzou. **Výhody které se získají v případě využití aplikace SIEM systémů:**

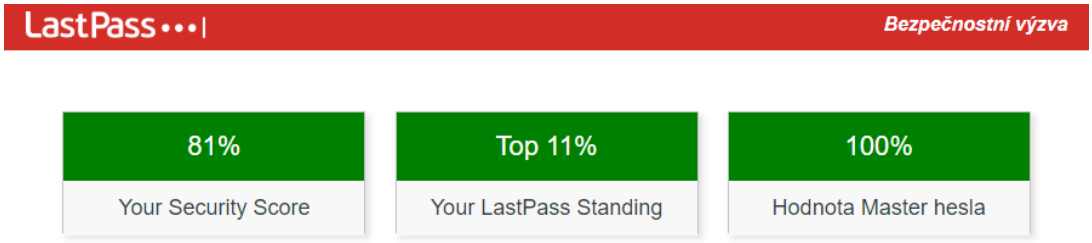
- Lepší a efektivnější správa firemní infrastruktury.
- Získávání informací a statistik o dané infrastruktuře.
- Lepší detekce hrozeb.
- Rychlejší detekce hrozeb.
- Efektivnější práce při řízení rizik.

Nabídka produktů SIEM:

- AlienVault OSSIM.
- McAfee ESM.
- LogRhytm.
- LOGmanager (SIEM). [22] [23] [24]

8.1.2 Využití správce hesel LastPass a bezpečnostní politika hesel

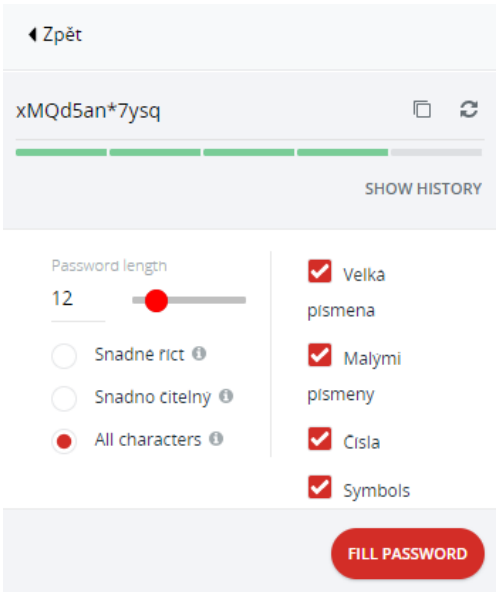
Jelikož daná společnost disponuje celou řadou aplikací a software, musí si zaměstnanci pamatovat každá jednotlivá hesla do různých typů aplikací. To vede k tomu, že hesla se buď zapomínají nebo často opakují a dochází tak k tomu, že jedno heslo může být použito u více aplikací či účtů. V rámci bezpečnosti politiky hesel má daná společnost stanovenou složitost hesla pouze pro operační systém Windows, nikoliv však již pro další aplikace.



Obr. 16: Správce hesel LastPass – bezpečnostní výzva [25]

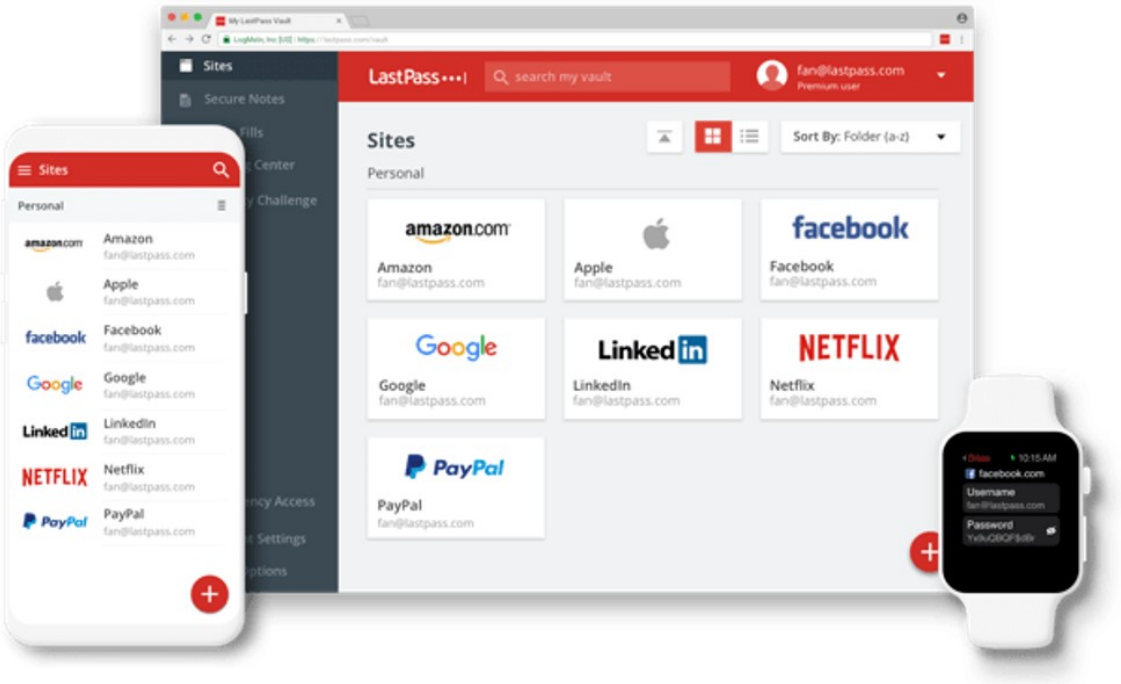
Jako možným prvkem ke zlepšení právě bezpečnostní politiky hesel je zavedení samotného správce hesel v podobě aplikace LastPass, která slouží k jejich ukládání a přístupu k těmto heslům z každého počítače či mobilního telefonu. [25]

Další velkou výhodou tohoto správce je to, že umožňuje provádět generování silných hesel, jejich následné ukládání v databázi uživatele či provádět analýzu bezpečnosti hesel. [25]



Obr. 17: Generování hesla (LastPass) [25]

V případě využití toho správce hesel si stačí pamatovat pouze jedno silné heslo k samotnému účtu LastPass a další hesla si pamatuje již samotná aplikace.



Obr. 18: Správce hesel LastPass [25]

Aplikace LastPass je zcela zdarma, nicméně pro firemní využití je doporučeno aplikování LastPass Teams či LastPass Enterprise, které zahrnují kompletní správu všech hesel u všech uživatelů. Cena této aplikace je:

- LastPass Teams.
  - 4 $ / měsíc.
  - 5–50 uživatelů.
- LastPass Enterprise.
  - 6 $ / měsíc.
  - 5+ uživatelů. [25]

Výhody které se získají v případě využití aplikace LastPass:

- Lepší správa hesel.
- Lepší bezpečnost hesel.
- Bezpečné sdílení hesel v rámci uživatelů.
- Přidání či odebrání uživatelů v rámci firmy.
- Zlepšení bezpečnosti ostatních aplikací. [25]

8.1.3 Využití penetračního testování

Jako další možností, které by vedlo ke zlepšení současného stavu informační bezpečnosti, je příležitost penetračního testování. Penetrační testování je metoda nebo způsob, jakým je možné otestovat bezpečnost počítačových systémů, zařízení či jiných aplikací a zjištění tak zranitelností daného systému. Penetrační testování většinou probíhá formou simulace útoků, buďto jako externí či jako interní penetrační test. Externí penetrační testování je prováděno zvenčí, kde se testuje především bezpečnost systému zvenčí, testy DoS a DDoS útoků a reakce na ně, nebo dále testování a prověřování bezdrátové komunikace Wi-Fi či testování propustnosti firewallů a dalších služeb. Interní útoky jsou prováděny zevnitř, kde je provedena identifikace systémů, invertizace systémů, kontrola služeb, sítě, síťových prvků a dalších jiných záležitostí. [26]

Výhody jenž se získají v případě využití penetračního testování:

- Vyhodnocení zranitelných částí systému.
- Souhrnná zpráva a úroveň zabezpečení daného systému a jeho aplikací.
- Testy z pohledu externího a interního útočníka.
- Hodnocení rizik z hlediska úrovně bezpečnosti PC sítě. [26]

ZÁVĚR

Tato bakalářská práce pojednává o problematice analýzy rizik a uplatnění analýzy rizik s řadou norem ISO/IEC 27000. V teoretické části byly představeny základní pojmy, které jsou nezbytným základem pro správné pochopení analýzy rizik a jejího postupu. Těmito základními pojmy jsou zejména aktivum, hrozba, riziko, zranitelnost, protiopatření a další doplňující informace. V další části práce je poté rozebrán obecný postup analýzy rizik, kde je vysvětleno jakým způsobem probíhá identifikace aktiv, stanovení hodnoty aktiv, identifikace hrozeb, zranitelností, určení míry dopadu či míry výskytu daných hrozeb a samotný výpočet rizik.

V navazujících kapitolách jsou poté čtenáři představeny dvě základní organizace, jenž se podílí na normotvorbě a úpravě norem ISO/IEC 27000 či dále je již uveden samotný systém řízení bezpečnosti informací spolu s jeho jednotlivými fázemi, které vychází z W. E. Demingova cyklu PDCA. Další kapitoly jsou poté věnovány jednak řadě norem ISO/IEC 27000 a dalším souvisejícím nařízením, kterými jsou GDPR a zákon o kybernetické bezpečnosti.

Praktická část je věnována již samotné analýze rizik, která probíhala v reálné firmě, avšak není zde uveden název samotné firmy či jména osob, které se podílely na konzultacích při zpracování této bakalářské práce. Cílem této práce bylo vytvořit analýzu rizik s ohledem na řadu norem ISO/IEC 27000, kterou by firma mohla využít v rámci certifikace s touto normou nebo v rámci získávání nových zákazníků, jenž zajímá jakým způsobem daná firma nakládá s bezpečností informací. Při analýze rizik byla představena metoda, kterou bude využita při provádění analýzy a byly rozebrány jednotlivé postupy, které na sebe navazují. Při vypracování této analýzy byl zvolen software Microsoft Excel, ve kterém probíhaly veškeré matematické a grafické výpočty pro lepší znázornění vypočítaných rizik. V závěru práce proběhla diskuze s vedením firmy ohledně výsledků analýzy či současného bezpečnostního stavu firmy a typů protiopatření, kterými se podílí na snižování rizik zjištěných v analýze rizik.

Jako poslední kapitola je závěrečné doporučení pro danou firmou, která v sobě zahrnuje tři možné varianty protiopatření, jenž může firma využít v rámci budoucího zlepšování informační bezpečnosti.

SEZNAM POUŽITÉ LITERATURY

[1] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 2., aktualiz. a rozš. vyd. Praha: Grada, c2006, 296 s. Expert. ISBN 80-247-1667-4.

[2] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012. 386 s. ISBN 9788087500194.

[3] ČERMÁK, Miroslav. Analýza rizik: Jemný úvod do analýzy rizik. Clever And Smart [online]. 2010 [cit. 2019-04-08]. Dostupné z: https://www.cleverand-smart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

[4] DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

[5] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016, 522 s. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cyber-crime.pdf

[6] ČSN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník. 4. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

[7] Informační aktiva. ManagementMania.com [online]. Wilmington (DE), 2017 [cit. 2019-04-03]. Dostupné z: https://managementmania.com/cs/informacni-aktiva

[8] KOUDELKA, Ctirad a Václav VRÁNA. Rizika a jejich analýza [online]. Ostrava, 2006 [cit. 2019-04-08]. Dostupné z: http://fei1.vsb.cz/kat420/vyuka/Magister-ske%20nav/prednasky/web/RIZIKA.pdf. Přednáškový materiál. Vysoká škola báňská – Technická univerzita Ostrava.

[9] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013, 377 s. ISBN 978-80-7204-872-4.

[10] YAZAR, Zeki. A qualitative risk analysis and management tool – CRAMM. SANS Institute [online]. 2002 [cit. 2019-04-08]. Dostupné z: https://pdfs.sema-ticschlar.org/3743/6a533bcbcd1bb42000383eae445840e5cefc.pdf

[11] Vznik České agentury pro standardizaci. Ústav pro technickou normalizaci, metrologii a státní zkušebnictví [online]. Praha, 2017 [cit. 2019-04-08]. Dostupné z: http://www.unmz.cz/test/vznik-ceske-agentury-pro-standardizaci

[12] NOVÁK, Luděk a Josef POŽÁR. ISMS (ISO 2700x): sborník příspěvků z bezpečnostního semináře Policejní akademie a evropského vedení AFCEA konaného dne 22. září 2011 na Policejní akademii České republiky v Praze. Praha: Policejní akademie České republiky, 2011. ISBN 978-80-7251-356-7.

[13] ČSN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 25 s.

[14] ČSN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 73 s.

[15] ŠKORNIČKOVÁ, Eva. Obecné nařízení o ochraně osobních údajů – prakticky. GDPR [online]. [cit. 2019-04-03]. Dostupné z: https://www.gdpr.cz/

[16] GDPR ve vztahu k ISO 27001. Quality Austria [online]. Praha [cit. 2019-04-08]. Dostupné z: https://www.qualityaustria.cz/gdpr-ve-vztahu-k-iso-27001

[17] Co přináší GDPR a jak je možné využít ISO 27001 a ZKB. Krucek CyberSecurity [online]. [cit. 2019-04-08]. Dostupné z: https://www.krucek.cz/cz/co-prinasi-gdpr-a-jak-je-mozne-vyuzit-iso-27001-a-zkb-87800/

[18] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti. Sbírka zákonů [online]. 2014 [cit. 2019-04-08]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[19] MATZNER, Jiří. Dopady zákona o kybernetické bezpečnosti. Systemonline.cz [online]. [cit. 2019-04-08]. Dostupné z: https://m.systemonline.cz/it-pravo/dopady-zakona-o-kyberneticke-bezpecnosti.htm

[20] FIRST: Common Vulnerability Scoring System [online]. FIRST [cit. 2019-04-08]. Dostupné z: https://www.first.org/cvss/

[21] Zákon č. 262/2006 Sb. zákoník práce. Sbírka zákonů [online]. [cit. 2019-04-08]. Dostupné z: https://www.zakonyprolidi.cz/cs/2006-262

[22] Systémy SIEM – kompletní správa IT infrastruktury. PCS.cz [online]. [cit. 2019-04-08]. Dostupné z: http://www.pcs.cz/divize-pcs/dataguard/aktuality/siem-security-information-and-event-management/

[23] BUDÍN, Emil. K čemu je SIEM?. SystemOnline [online]. 2014 [cit. 2019-04-08]. Dostupné z: https://www.systemonline.cz/it-security/k-cemu-je-siem.htm

[24] SIEM software (Security information and event management). ManagementMania.com [online]. 2018 [cit. 2019-04-08]. Dostupné z: https://managementmania.com/cs/siem-software-security-information-and-event-management

[25] LastPass [online]. 2019 [cit. 2019-04-08]. Dostupné z: https://www.lastpass.com/

[26] OULEHLA, Milan. Výukový materiál: Analýza rizik a penetrační testy: Bezpečnost informačních systémů. Fakulta aplikované informatiky, Univerzita Tomáše Bati ve Zlíně, 2019.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

A	Aktivum
ALE	Annualized Loss Expectancy (Roční předpokládaná ztráta)
CERT	Computer Emergency Response Team
CRAMM	CCTA Risk Analysis and Management Methodology
CVSS	Common Vulnerability Scoring System
ČAS	Česká agentura pro standardizaci
ČSN	Česká technická norma
DDoS	Distributed Denial of Service
DH	Dopad hrozby
FTP	File Transport Protocol
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IMS	Integrated Management System
IS	Information System
ISMS	Information Security Management System
ISO	International Organization for Standardization
NBÚ	Národní bezpečnostní úřad
PDCA	Plan Do Check Act
R	Riziko
SIEM	Security information and event management
ÚNMZ	Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví
ÚOOÚ	Úřad pro ochranu osobních údajů
VH	Výskyt hrozby

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ANALÝZA RIZIK ISO 27000

V příloze se nachází soubor s kompletní vypracovanou analýzou rizik pomocí software Microsoft Excel. Součástí tohoto souboru jsou čtyři listy, kde první list obsahuje vstupní parametry, jenž vstupují do analýzy rizik. Dále na druhém listě se nachází již základní přehled vypočítaných rizik a všemi identifikovanými aktivy. Na třetím listě lze nalézt veškeré grafy, které dávají přehled o daných hrozbách a rizicích v grafickém provedení. Čtvrtý list slouží jako nápověda s tabulkami pro ohodnocení vstupujících parametrů. Příloha je uložena na přiloženém CD.