Návrh systému řízení bezpečnosti informací vybraného subjektu

Bc. Jakub Jareš

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jakub Jareš**
Osobní číslo:	**L19601**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Studijní obor:	**Rizikové inženýrství**
Forma studia:	**Kombinovaná**
Téma práce:	**Návrh systému řízení bezpečnosti informací vybraného subjektu**

Zásady pro vypracování

1. Proveďte literární rešerši současného stavu systému řízení bezpečnosti informací.
2. Navrhněte metodický rámec práce a zvolte nástroje potřebné k provedení analýz a přípravných prací.
3. Analyzujte současný stav systému řízení bezpečnosti informací vybraného subjektu.
4. Navrhněte kroky ke zlepšení současného stavu systému řízení bezpečnosti informací vybraného subjektu.

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

Seznam doporučené literatury:

1. DOUCEK, Petr. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha: Professional Publishing, 2020. ISBN 978-80-88260-39-4.
2. HARKINS, Malcolm. *Managing Risk and Information Security: Protect to Enable.* New York: Apress, 2013. ISBN 978-14-30251-13-2.
3. KOLOUCH, Jan, Pavel BAŠTA a kol. *Cybersecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-31-7.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2020**
Termín odevzdání diplomové práce: **14. května 2021**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

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

V Uherském Hradišti dne 2. prosince 2020

Prohlašuji, že

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

Prohlašuji,

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

V Uherském Hradišti, dne: 3.8.2021

Jméno a příjmení studenta : Bc. Jakub Jareš

. . . . . .

podpis studenta

ABSTRAKT

Diplomová práce je zaměřena na proces nasazení systému řízení bezpečnosti informací ve vybraném ekonomickém subjektu v České republice. V teoretické části jsou shrnuty užívané standardy, legislativní požadavky, prostředky, metody a užívaná terminologie v oblasti informační a kybernetické bezpečnosti. Praktická část obsahuje popis realizace kroků ve vybrané organizaci, vytvoření metodik pro identifikaci a hodnocení aktiv, sestavení katalogu hrozeb, stanovení metodického rámce pro určení pravděpodobností a dopadů a analýzu rizik, pro kterou jsou definovány modely výpočtů, včetně zahrnutí předpokládaného vlivu ochranných opatření na zbytkové riziko. Na základě výstupů je navržena podoba a obsah základní bezpečnostní dokumentace nutné k zavedení systému řízení bezpečnosti informací do procesů organizace. Principy a metody definované v diplomové práci jsou přenositelné a lze je použít jako metodické vodítko k nasazení systému řízení informační bezpečnosti v dalších organizacích.

Klíčová slova: Analýza rizik, bezpečnost informací, , bezpečnostní politika, identifikace aktiv, ISMS, kybernetická bezpečnost, systém řízení

ABSTRACT

The diploma thesis is focused on the process of deploying an information security management system in a selected economic operator located in the Czech Republic. The theoretical part summarizes used standards, legislative requirements, means, methods and terminology used in the information and cyber security sphere. The practical part contains a description of the implementation steps in the selected organization, creating methodical scopes for identifying and evaluating assets, creating a threat catalog, methodologies for determining probabilities and impacts and risk analysis, where specific calculation models are defined, including the expected countermeasure impact at residual risk. Based on the results are proposed the form and content of the basic security documentation, which is necessary to implement an information security management system in the organization's processes. The principles and methods defined in the diploma thesis are portable and can be used as a methodological guide to the deployment of information security management system in other organizations.

Keywords: Assets identification, cybersecurity, information security, ISMS, management system, risk analysis, security policy

Rád bych poděkoval vedoucímu práce, Ing. Petrovi Svobodovi Ph.D. za cenné rady, postřehy, čas a pomoc, které mi věnoval v průběhu zpracování diplomové práce. Děkuji vybranému ekonomickému subjektu za spolupráci, významný dík také patří mé rodině a přátelům za podporu během celého mého studia.

OBSAH

ÚVOD

„Tyhle aféry každého jenom otravují. Já bych všechny ty internety a počítače zakázala.“(Pohlová, 1999)

Legendární prohlášení dvaasedmdesátileté důchodkyně v deníku Metro se vztahovalo k případu úniku dat společnosti Česká spořitelna, který měl na svědomí jeden ze správců počítačové sítě poškozené společnosti (iDnes.cz, 1999).

Pojem **Bezpečnost informací** je čím dál více skloňován nejen v soukromé sféře ochrany osobních údajů, či lokálně umístěných firemních dat, ale zejména v souvislosti s postupující digitalizací, přesuny dat do online kyberprostoru, potřebou jejich okamžité dostupnosti na jakémkoliv zařízení a platformě, od osobních počítačů a mobilních telefonů, přes projekty autonomních výrobních linek, chytrých domů, kanceláří, spotřebičů, až po nositelnou elektroniku, kterou z historických důvodů nazýváme hodinky.

V podstatě každý den v některém ze světových deníků můžeme nalézt zprávu o úniku dat nebo útoku hackerů, nejen v souvislostech s obchodními daty soukromých společností nebo sociálními sítěmi, čím dál častěji jsou zveřejňovány informace o působení škod ve státním sektoru nebo o zapojení státních skupin v roli aktérů takových útoků.

Lze předpokládat, že každá organizace má zájem na ochraně dat svých i zákaznických, avšak rychlost technologického vývoje a neustálé nasazování nových produktů do firemního prostředí klade zvyšující se nároky na znalost administrace těchto nástrojů i zodpovědnost samotných uživatelů, kdy míra růstu bezpečnostního povědomí a odpovídajících opatření nemusí být dostatečná.

CÍL PRÁCE A POUŽITÉ METODY

Cílem diplomové práce je návrh systému řízení bezpečnosti informací vybraného ekonomického subjektu v souladu s nejlepší praxí a platnou legislativou.

Dílčími cíli práce jsou kroky nutné k zavedení systémově řízené ochrany bezpečnosti informací, zejména:

- Zjištění současného stavu ochrany informací a technologií souvisejících s jejich vytvářením, zpracováním, uchováním a přenosem ve vybraném subjektu.
- Návrh postupů a metod identifikace a hodnocení informačních aktiv.
- Návrh a sestavení metodického rámce analýzy rizik.
- Návrh a realizace softwarové podpory pro analýzu rizik.
- Návrh bezpečnostní dokumentace nutné pro dosažení, udržování a zlepšování ochrany informací v organizaci.

Vzhledem k citlivosti informací a možnému bezpečnostnímu riziku při zveřejnění zjištěných skutečností byla s Vybraným subjektem uzavřena Dohoda o mlčenlivosti (NDA – Non-disclosure agreement). Z tohoto důvodu jsou veškerá data použitá v diplomové práci důsledně anonymizována. Přestože je skryt název organizace a konkrétní data i hodnocení aktiv jsou změněna, výstup dotazníkového šetření, postup jednotlivých kroků, použité metody a prostředky, způsoby hodnocení a vzorce výpočtů jsou zachovány.

Použité metody

Teoretická část obsahuje syntézu informací získaných rešeršní činností z literárních a legislativních zdrojů v oblasti managementu, bezpečnosti informací a kybernetické bezpečnosti. V praktické části je nejprve zpracován základní přehled o stavu řízení bezpečnosti informací ve vybraném subjektu zajištěný dotazníkovým šetřením, zaměřeným zejména na existenci a stav bezpečnostní dokumentace. Pro následné zpracování Orientační analýzy rizik byla zvolena Peltierova metoda FRAP, tedy sada řízených rozhovorů s týmem bezpečnosti informací vybraného subjektu. K těmto rozhovorům jsou, za účelem získání specifických informací, postupně přibíráni zástupci jednotlivých oddělení subjektu a v případě potřeby další odborníci se specializací. Pro fázi identifikace a ohodnocení aktiv jsou navrženy metodické pomůcky s vysvětlením hodnoticích kritérií. Pro vytvoření katalogu hrozeb, stanovení pravděpodobností a dopadů je plánováno použití brainstormingu. Pro výpočet rizika dle metodického rámce, navrženého v praktické části diplomové práce a schválené týmem vybraného subjektu, poslouží standardní

tabulkový procesor naplněný zjištěnými vstupními daty. Jeho součástí bude i výpočet vlivu ochranného opatření na hodnotu zbytkového rizika. Výstupem praktické části je komplexní soubor tabulkového procesoru ke zpracování analýzy rizik, doplněný návrhem bezpečnostní dokumentace.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST INFORMACÍ A JEJÍ POJETÍ V ČESKÉ REPUBLICE

„V ČR je v oblasti informačních a komunikačních technologií řada kvalitních odborníků. Problémem však zůstává skutečnost, že se bezpečnost řeší převážně v této oblasti. Zkušenosti ze zahraničí poukazují na potřebu vnímat informační bezpečnost v daleko širším kontextu. Nejen v oblasti firemních ICT a zabezpečení jejich systémů, ale v návaznosti a ve vztazích ke zbytku firmy, včetně jejich prostor, objektů a zaměstnanců. Informační bezpečnost se nevztahuje jen k ICT, ale prakticky ke všem procesům a byznysu každé firmy.“ (Drastich, 2011, s. 18)

Dále Drastich uvádí, že ve výsledcích průzkumu stavu informační bezpečnosti ČR z roku 2009, který byl proveden společnostmi Ernst and Young, DSM – Data Security Management a NBÚ na vzorku o rozsahu 1100 subjektů, je dvoutřetinový podíl společností, které mají implementovánu Bezpečnostní politiku a pouze 16% podíl organizací, které nikdy neprovedly analýzu IS (Drastich, 2011).

Zpráva o kybernetické bezpečnosti České republiky za rok 2020, vydaná Národním úřadem pro kybernetickou a informační bezpečnost, poukazuje, na základě výsledků vlastních průzkumů, na nedostatek odborníků a nízké rozpočty v této oblasti. Dále zmiňuje, že téměř všichni respondenti nemají obsazené všechny pozice v těchto oborech. Přitom úřad evidoval dvojnásobný nárůst nahlášených kybernetických incidentů oproti předchozímu roku. Mezi nejčastější patřily útoky typu spam, phishing a skenování perimetru sítí. Jako nejzávažnější pak jsou hodnoceny útoky útoky ransomware, DoS/DDoS a spear-phishing (cílený phishing) (nukib.cz, 2021).

Nedostatek zaměstnanců na klíčových pozicích informační a kybernetické bezpečnosti je dlouhodobý problém, který je zmiňován i ve zprávě o kybernetické bezpečnosti za rok 2019. Zde je uváděno, že 88 % dotázaných organizací potřebuje obsadit tyto pozice a polovina respondentů tuto oblast řeší formou outsourcingu (nukib.cz, 2020c).

Ve strategickém kontextu **Národní strategie kybernetické bezpečnosti pro období 2021 – 2025** je současná úroveň označena jako bezprecedentní a tento stav je připisován rozmachu digitalizace společnosti, kdy probíhající přesun tradičních bezpečnostních hrozeb do kyberprostoru otvírá nové, dříve neznámé, prostředí, jehož dynamiku umocňuje právě používání nových technologií. Zároveň je zdůrazňována závislost státu a společnosti na moderních technologiích, kdy úroveň této závislosti je vnímána jako kritická (nukib.cz, 2020a).

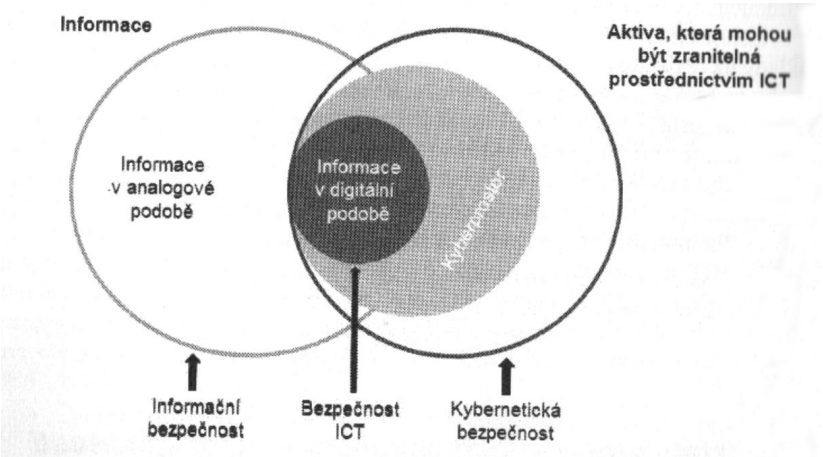
Je zde znatelný výrazný posun oproti strategii předchozího období 2015 – 2020, která popisuje kybernetickou bezpečnost jako negativní průvodní jev usnadnění komunikace a sdílení informací. Oproti aktuální strategii je zde zdůrazněno **nedostatečné zabezpečení malých a středních podniků**, kde je doporučováno seznámení s aktuálními

metodami ochrany dat a nejlepší praxí (nukib.cz, 2015).

Výroční zpráva NCOZ za rok 2020 v oddílu Sekce kybernetické kriminality uvádí 25% nárůst registrovaných skutků oproti roku 2019, přičemž tento vývoj považuje za odpovídající vzhledem k situaci ve vyspělých státech Evropy i celého světa. Zejména zdůrazňuje proběhlé útoky v oblasti zdravotnictví, které označuje jako vysoce profesionální z důvodu vícekrokového průběhu, kdy po kompromitaci jednoho koncového zařízení je škodlivý software schopen se rozšířit na ostatní systémy v počítačové síti. Pro budoucnost předpovídá zvýšený zájem zahraničních aktérů o systému kritické informační infrastruktury a významné informační systémy ČR. Jako nejčastější způsoby páchání trestné činnosti v kyberprostoru zpráva uvádí ransomware (šifrovací software), malware (obecně jakýkoliv škodlivý software), průnik do počítačových systémů prostřednictvím zranitelností s cílem odcizit citlivá data, útoky DDoS (přetížení za účelem odepření služeb), phishing (lákání uživatel podvrženým obsahem), spear phishing (cílené podvržení obsahu) a následné získání citlivých údajů, jako jsou například hesla, platební údaje, přihlašovací údaje, popřípadě jiná citlivá osobní často i intimní data, obvykle za účelem kompromitace osoby nebo finančního zisku (policie.cz, 2021).

1.1 Vztah bezpečnosti informací a kybernetické bezpečnosti

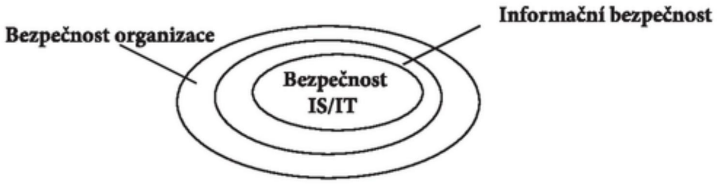
Doucek tvrdí, že informační bezpečnost má za úkol chránit důvěrnost, dostupnost a integritu informací, zatímco kybernetická bezpečnost cílí zejména na řešení kybernetických incidentů oproti pouhé ochraně důvěrnosti, dostupnosti a integrity informace (Doucek, Konečný a Novák, 2019).



Obrázek 1.1 Kyberbezpečnost v rámci informační bezpečnosti (Doucek, Konečný a Novák, 2019)

Požár pokládá informační bezpečnost za mladý obor, který je podřízen bezpečnosti organizace a má za úkol zabezpečení informací ve všech fázích jejich životního cyklu, tedy vzniku, zpracování, uložení, přenosu a likvidace za použití logických, fy-

zických,technických, programových a organizačních opatření, která mají působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot (Požár, 2010).



Obrázek 1.2 Podřízenost informační bezpečnosti k bezpečnosti organizace (Požár, 2010)

Kolouch uvádí, že v rámci bezpečnosti informací není důležité, zda informace existuje na papíře či v elektronické podobě v jakémkoliv systému a nastoluje otázku, zda se současná definice informační bezpečnosti vztahuje odpovídajícím způsobem ke kyberprostoru. Dále tvrdí, že informační bezpečnost ve vztahu k využívání výpočetních a komunikačních technologií by bylo vhodnější nazývat kybernetickou bezpečností (Kolouch et al., 2019).

„*Kybernetická bezpečnost jako poměrně mladý obor je pak součástí informační bezpečnosti (information security), jejímž cílem je, jak již název napovídá, právě ochrana informací zpracovávaných, uchovávaných a přenášených v jakékoli a po jakémkoli médiu. Tedy nikoliv jen v elektronické podobě mezi počítači, ale také v papírové podobě a tudíž sem patří například i ústní výměna informací mezi lidmi, kteří jsou rovněž součástí informačního systému.*“ (Šulc, 2018, s. 10)

V současné době některé firmy zavádí na tzv. bezpapírovou agendu, zároveň velké softwarové společnosti přechází k modelu poskytování programového vybavení jako služby (SaaS – Software as a Service), s čímž souvisí i přenos uživatelských dat do online datových úložišť (cloud), a tak jsou informace samotné ve firemním prostředí stále méně přítomné pouze v analogové formě a zároveň v digitální podobě pouze v uzavřeném prostředí firemní infrastruktury. Z uvedených důvodů tyto oblasti již natolik splývají, že je obtížné, ne-li nemožné, vymezit přesnou hranici, kde lze hovořit pouze o kybernetické bezpečnosti v rámci bezpečnosti informací.

1.2 Řízení bezpečnosti informací

Doucek považuje za nutné systém řízení bezpečnosti informací v organizacích zavést, v rámci účelnosti a účinnosti ochrany informací však doporučuje omezit rozsah na základě porozumění kontextu organizace a zainteresovaných stran, případně jasně stanovit hranici a rozhraní na subjekty, které řízení bezpečnosti informací podporují, ale nejsou zahrnuty v omezeném rozsahu (Doucek, Konečný a Novák, 2019).

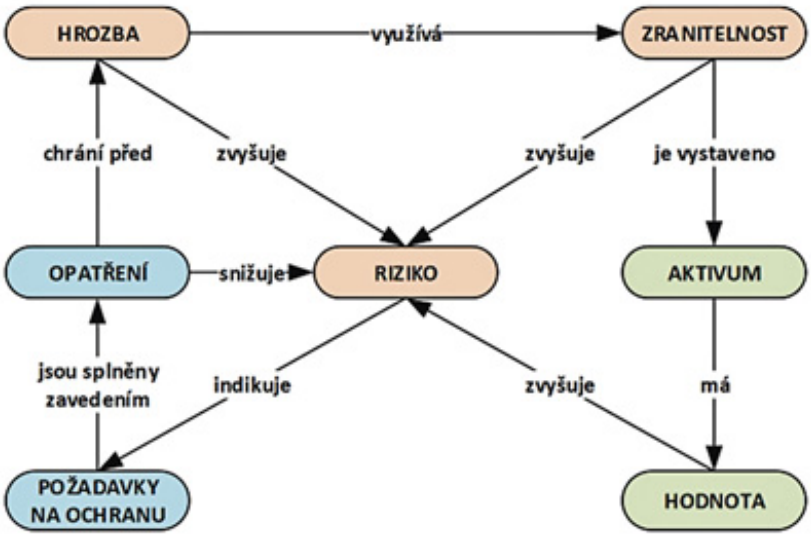
„Systém řízení bezpečnosti informací (Information Security Management System – ISMS) představuje soubor pravidel, jejichž cílem je zachovat důvěrnost, integritu a dostupnost informací aplikováním procesu řízení rizik a dát jistotu zainteresovaným stranám, že jsou rizika přiměřeně řízena. V rámci ISMS jsou chráněna aktiva, řízena rizika bezpečnosti informací a již zavedená opatření jsou kontrolována.“ (Kolouch et al., 2019, s. 253)

Peltier definuje informační bezpečnost jako prevenci před neautorizovaným a nechtěným použitím, změnou, zničením nebo vyzrazením informace nebo jejího zdroje, resp. zotavení po takové události, bez ohledu na to, zda se jedná o náhodný nebo úmyslný jev. Dále jako jemnější definici uvádí, že se jedná o ochranu informací a zdrojů z hlediska dostupnosti, celistvosti a důvěrnosti (Peltier, 2004).

„Systém řízení bezpečnosti informací – SŘBI (Information Security Management System – ISMS) – Část systému řízení, založená na přístupu k bezpečnostním rizikům, k ustavení, implementování, provozování, monitorování, přezkoumávání, spravování a zlepšování bezpečnosti informací.“ (Jirásek, Novák a Požár, 2015, s. 32)

2 UŽÍVANÉ STANDARDY A LEGISLATIVNÍ VÝCHODISKA

Z historického hlediska první normované doporučení vydala Mezinárodní organizace pro standardizaci v roce 1996 (český překlad vyšel až v roce 1999) normu ISO/IEC 1335-1 v podobě TR (Technical Report – technická zpráva), která shrnuje výtah z tehdejších doporučení založených na nejlepší praxi (best practise). Česká podoba z roku 1999 zejména definuje obecné pojetí a základní modely řízení bezpečnosti informačních technologií. Mimo jiné obsahuje i schéma vzájemných vztahů aktiv, hrozeb, opatření a rizik (Goll, 2019).



Obrázek 2.1 Přehledové schéma řízení rizik (Goll, 2019)

V ČR byly následně vydány normy ČSN ISO/IEC 1335-2:2000 a ČSN ISO/IEC 1335-3:2000, u kterých Goll zdůrazňuje zejména téma organizace bezpečnosti informačních technologií a její vztah k řízení informačních technologií a dále pak první zmínku o možnosti využití Demingova cyklu PDCA (Plan - Do - Check - Act). Norma ČSN ISO/IEC 1335-3:2000 obsahuje popisy technik řízení rizik, plánu bezpečnosti, monitoring, důraz na bezpečnostní povědomí, řízení incidentů a další prvky řízení bezpečnosti informačních technologií. Goll ji přirovnává k současné normě ČSN ISO/IEC 27002:2014 (Goll, 2019).

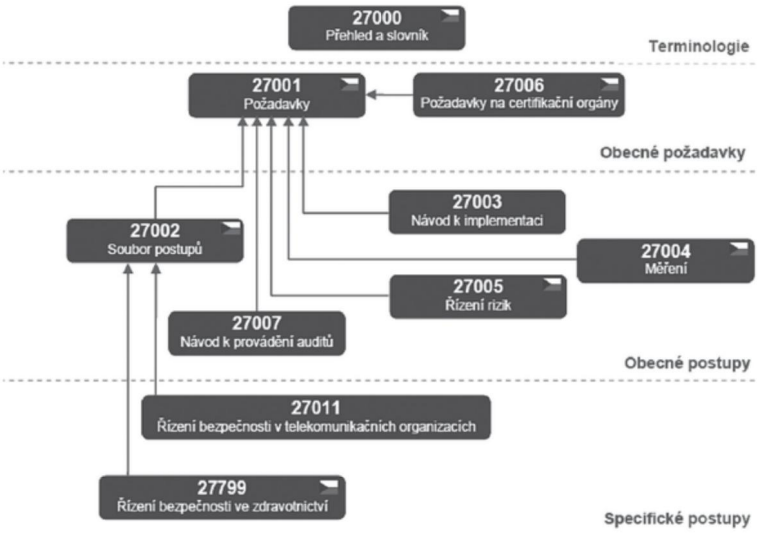
V roce 2000 byla vydána norma ISO/IEC 17799, která byla koncipována jako klíčová pro zavádění a zejména certifikaci systémů řízení bezpečnosti informací v organizacích a pokryla všechny oblastí získávání, zpracování a uchovávání informací v organizaci. Jejím základem byla britská národní norma UK BS 7799 a jedním z nejdůležitějších prvků je aplikace Demingova PDCA cyklu, který je zároveň součástí norem ISO/IEC 9000 a ISO/IEC 14000 (iso.cz, 2000).

2.1 Řada norem ISO/IEC 27000

Mezinárodní norma pro Systém řízení bezpečnosti informací (ISMS) univerzálně použitelná pro všechny typy i velikosti organizací. Expertní komise ISO věnující se vývoji norem systémů řízení bezpečnosti informací vytvořila v této sadě norem model, který reflektuje současný mezinárodní vývoj. Kterýkoliv subjekt by měl být, při použití vodítek a příkladů v této sadě norem, schopen definovat a nasadit systém řízení bezpečnosti informací tak, aby mohl být posouzen nezávislým auditem v oblasti bezpečnosti informací (Smejkal, Sokol a Kodl, 2019).

Podle Koloucha mezi základní normy informační bezpečnosti patří:

- ČSN ISO/IEC 27001:2014 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.
- ČSN ISO/IEC 27002:2014 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací (Kolouch et al., 2019).



Obrázek 2.2 Schéma využití norem ČSN ISO/IEC 27000 (Smejkal, Sokol a Kodl, 2019)

Smejkal dále zdůrazňuje normy

- ČSN ISO/IEC 27003:2018 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Pokyny.
- ČSN ISO/IEC 27004:2018 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Monitorování, měření, analýza a hodnocení.
- ČSN ISO/IEC 27005:2019 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Řízení bezpečnosti informací.

- ČSN ISO/IEC 27006:2016 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.
- ČSN ISO/IEC 27007:2018 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Směrnice pro audit systémů řízení bezpečnosti informací (Smejkal, Sokol a Kodl, 2019).

2.2 Zákon č. 2/1993 Sb.: Listina základních práv a svobod

V listině práv a svobod je zakotvena nedotknutelnost osob a jejich soukromí, právo na zachování důstojnosti, cti, dobré pověsti a ochrany jména. Je garantováno právo na ochranu před neoprávněným zasahováním do soukromí a právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Je zde uveden zákaz porušení listovního tajemství, tajemství jiných písemností a záznamů uchovávaných či zasílaných poštou nebo jiným způsobem, stejně jako zachování tajemství zpráv podávaných telefonem nebo jiným podobným zařízením (Zákon č. 2/1993 Sb.).

2.3 Zákon č. 89/2012 Sb.: Občanský zákoník

Občanský zákoník výslovně stanovuje povinnost smluvních stran dbát na ochranu před zneužitím nebo prozrazením důvěrných údajů nebo sdělení a zároveň právo vést o nich záznamy, i v případě, že smlouva nebude uzavřena (Zákon č. 89/2012 Sb.).

2.4 Zákon č. 480/2004 Sb.: o některých službách informační společnosti

Zákon upravuje odpovědnosti, práva a povinnosti osob poskytujících služby informační společnosti nebo šíří obchodní sdělení. Zákon definuje službnu informační spolenčosti jako jakoukoliv službu poskytnutou elektronickými prostředky, což zákon dále definuje jako službu odeslanou prostřednictvím sítě elektronické komunikace a vyzvednutou uživatelem z elektronického zařízení pro ukládání dat. Zákon také definuje elektronickou poštu jako textovou, hlasovou zvukovou nebo obrazovou zprávu poslanou veřejnou sítí elektronické komunikace, která může být uložena v síti nebo koncovém zařízení, dokud si ji uživatel nevyzvedne. Obchodní sdělení je popsáno jako jakákoliv forma sdělení, včetně reklamy a vybízení k návštěvě internetových stránek sloužících k přímé i nepřímé podpoře zboží, služeb nebo image podniku (Zákon č. 480/2004 Sb.).

2.5 Zákon č. 110/2019 Sb.: o zpracování osobních údajů

Zákon zapracovává Směrnici Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 a Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů. Definuje subjekt údajů jako fyzickou osobu, k níž se osobní údaje vztahují, omezuje nakládání s nimi pouze pro konkrétní potřeby a zavádí mimo jiné povinnost informovaného souhlasu o jejich zpracování (Zákon č. 110/2019 Sb.).

2.6 Zákon č. 412/2005 Sb.: o ochraně utajovaných informací a o bezpečnostní způsobilosti

Zákon upravuje zásady pro stanovení utajování informací, požadavky na jejich ochranu a řízení přístupu k nim, podmínky pro jejich výkon a s tím spojený výkon státní správy. Definuje utajovanou informaci jako informaci v jakékoliv podobě zaznamenanou na jakémkoliv nosiči a označenou v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné. Jako zájem republiky je uvedeno zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob. Zákon definuje čtyři stupně utajení v závislosti na míře poškození zájmů české republiky následovně:

- Přísně tajné – zneužití nebo vyzrazení může způsobil mimořádně vážnou újmu.
- Tajné – zneužití nebo vyzrazení může způsobil vážnou újmu.
- Důvěrné – zneužití nebo vyzrazení může způsobil prostou újmu.
- Vyhrazené – zneužití nebo vyzrazení může být nevýhodné pro zájmy ČR (Zákon č. 412/2005 Sb.).

2.7 Zákon č. 181/2014 Sb.: o kybernetické bezpečnosti

Zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. Zároveň se však nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi. Definuje kybernetický prostor jako digitální prostředí umožňující vznik, zpracování a výměnu informací, bezpečnost informací jako zajištění důvěrnosti, integrity a dostupnosti informací a dat, kritickou informační infrastrukturu, významné informační systémy, provozovatele a správce informačních a komunikačních systémů. Dále definuje orgány a osoby

povinné k zapracování bezpečnostních opatření, která rozděluje na organizační a technická, zavádí povinnost ohlášení kybernetických incidentů Úřadu pro kybernetickou a informační bezpečnost (Zákon č. 181/2014 Sb.).

2.8 Vyhláška č. 82/2018 Sb.: o kybernetické bezpečnosti

Prováděcí vyhláška k zákonu č. 181/2014 Sb. upravuje pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém, informační systém základní služby anebo informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb

- Obsah a strukturu bezpečnostní dokumentace.
- Obsah a rozsah bezpečnostních opatření.
- Typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incident.
- Náležitosti a způsob hlášení kybernetického bezpečnostního incidentu.
- Náležitosti oznámení o provedení reaktivního opatření a jeho výsledku.
- Vzor oznámení kontaktních údajů a jeho formu.
- Způsob likvidace dat, provozních údajů, informací a jejich kopií.

Dále vyhláška upřesňuje rozsah a náležitosti oblastí Organizačních a Technických opatření k zajištění kybernetické bezpečnosti, stanovuje povinnost mít sepsánu Bezpečnostní politiku a bezpečnostní dokumentaci, definuje kategorizaci kybernetických incidentů a formu jejich ohlašování. V přílohách Vyhlášky jsou pak uvedeny modelové příklady pro hodnocení aktiv, návrh metodiky výpočtu rizika, příklady hrozeb a zranitelností a návrh úrovní pro bezpečnou likvidaci dat (Vyhláška č. 82/2018 Sb.).

3 ZÁKLADNÍ POJMY SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

„*Praxe ukazuje, že zajištění bezpečnosti informací je ve skutečnosti spíše manažerský než technický problém. Pro efektivní řešení bezpečnosti – ať jde o řízení informační bezpečnosti, přípravu havarijních plánů nebo implementaci technologií – je klíčová existence procesů a struktur, stejně jako dostatek lidských a finančních zdrojů, které budou řešení bezpečnosti zajišťovat.*“ (Risk Analysis Consultants, 2021)

„*Sestavit v dnešní době slovník z oblastí spojených s informační a komunikační technologií (ICT) je úkol značně složitý a současně velmi naléhavý. Nesnadnost spočívá v tom, že se tento obor stále ještě velmi rychle rozvíjí, což se sebou nese terminologickou explozi, doprovázenou zákonitě mnohonásobně duplicitním pojmenováním stejných jevů, a to přímo v dominantním jazyku oboru, angličtině. Nutnost pokusit se kodifikovat vyjadřovací prostředky v tomto oboru pak vyplývá ze skutečnosti, že s ICT pracuje stále větší množství pracovníků i manažerů na různém stupni znalostí a dovedností, kteří nutně potřebují komunikovat pomocí pokud možno jednotné české slovní zásoby.*“ (Jirásek, Novák a Požár, 2015, s. 7)

Gogela tvrdí, že často i odborná veřejnost se nedokáže shodnout na významu a obsahu jednotlivých pojmů v oblasti informační bezpečnosti (Gogela, 2011).

Následující podkapitoly uvádí nejčastější definice základních pojmů v oblasti řízení bezpečnosti informací.

3.1 Aktivum

„*Cokoliv, co má hodnotu pro jednotlivce, organizaci nebo veřejnou správu.*“ (Jirásek, Novák a Požár, 2015, s. 17)

Kolouch dělí aktiva na hmotná (např. budova, počítačový systém, zboží) a nehmotná (např. informace, data, znalost) avšak dále uvádí např. dobré jméno či lidské znalosti a zkušenosti (Kolouch et al., 2019).

Vyhláška o kybernetické bezpečnosti aktiva dělí na primární (informace nebo služba) a podpůrná (technická aktiva, zaměstnance, dodavatele) (Vyhláška č. 82/2018 Sb.).

3.2 Hrozba vs. Zranitelnost

Hrozba

„*Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.*“ (Jirásek, Novák a Požár, 2015, s. 25)

Podle Koloucha lze hrozbu definovat jako jakýkoli jev, který je schopen narušit běžný nebo řádný stav a zasáhnout do práv jiných subjektů (Kolouch et al., 2019).

Vyhláška 82/2018 pak definuje hrozbu jako potenciální příčinu bezpečnostní události nebo incidentu, která může způsobit škodu (Vyhláška č. 82/2018 Sb.).

Zranitelnost

Slovník kybernetické bezpečnosti zranitelnost uvádí jako slabé místo aktiva, které může být využito hrozbou nebo hrozbami (Jirásek, Novák a Požár, 2015).

Kolouch také označuje zranitelnost jako slabé místo aktiva nebo softwaru, které může být využito hrozbou a dále je rozděluje na zranitelnosti známé a neznámé, kdy toto dělení je vztaženo zejména na softwarové zranitelnosti (Kolouch et al., 2019).

Vyhláška 82/2018 také definuje zranitelnost jako slabé místo aktiva nebo opatření, které může být využito hrozbou nebo hrozbami. V jejích přílohách jsou také uvedeny modelové příklady hrozeb a zranitelností i možných vazeb mezi nimi, ale tyto modely jsou pro pochopení vztahu **hrozba** × **zranitelnost** spíše matoucí (Vyhláška č. 82/2018 Sb.).

„Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby.“ (Smejkal a Rais, 2013, s. 98)

Podle Čermáka je třeba si nejprve identifikovat hrozby a zranitelnosti a na tomto základě je pak možné stanovit pravděpodobnost (Čermák, 2012).

3.3 Pravděpodobnost a dopad

Ve slovníku kybernetické bezpečnosti je pravděpodobnost uvedena stroze, pouze jako možnost, že se něco stane. Dopad je zde definován jako nepříznivá změna dosaženého stupně cílů nebo následky určitého činu nebo události (Jirásek, Novák a Požár, 2015).

Čermák tvrdí, že míru pravděpodobnosti u neúmyslných hrozeb lze definovat an základě historických dat, avšak pro hrozby úmyslné uvádí možnost přímé souvislosti s hodnotou aktiva a dalšími faktory, jako je např. velikost, významnost nebo obliba organizace. Dopad pak vztahuje k hodnotě aktiva, které může být zranitelnosti postiženo (Čermák, 2012).

Kolouch pojem pravděpodobnost používá pouze jako dílčí součást pojmu riziko, kde tvrdí, že událost nastane nebo nastat nemusí. Dále uvádí základní vzorec výpočtu rizika jako **Významnost** rizika = **Dopady** rizika × **Pravděpodobnost** výskytu rizika. Dopad pak považuje za negativní důsledek na ochranu důvěrnosti, dostupnosti nebo integrity aktiva a kontinuitu poskytování služeb (Kolouch et al., 2019).

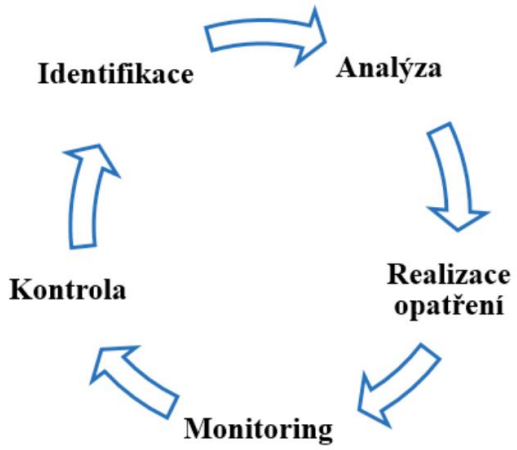
Vyhláška 82/2018 pak pravděpodobnost jako takovou vůbec nezmiňuje, je zahrnuta v definici rizika, jako možnost že určitá hrozba využije zranitelnosti aktiva a způsobí

škodu. Dopady vyhláška doporučuje hodnotit podle ohodnocení aktiv z hlediska důvěrnosti, dostupnosti a integrity (Vyhláška č. 82/2018 Sb.).

3.4 Analýza rizik

„Analýza rizik je značně obtížná a vyžaduje znalost aktiv, hrozeb a zejména je třeba mít v této oblasti již nějaké zkušenosti. Na základě analýzy rizik je možné stanovit opatření za účelem minimalizace nebo úplného odstranění rizik.“ (Kolouch et al., 2019, s. 71)

Dále uvádí, že za podpory dalších procesů je možné k analýze rizik přirovnat i udržování kybernetické bezpečnosti (Kolouch et al., 2019).



Obrázek 3.1 Analýza rizik podle Koloucha
(Kolouch et al., 2019)

Podle Kruliše je cílem analýzy rizik **identifikovat včas všechna významná potenciální rizika a jejich příčiny**. Její provádění je podmíněno vyčleněním potřebných časových i finančních zdrojů a je třeba v organizaci vytvořit vhodné procesní, metodické a kvalifikační předpoklady. Metody analýzy rizik lze podle Kruliše rozdělit na

- **Kvantitativní** – používá přesné údaje, je náročná na zpracování a čas, používá se zejména pro finanční nebo technickou bezpečnost.
- **Kvalitativní** – používá pojmy jako nízká, střední apod. slouží často k porovnávání alternativ produktů, technologií, je rychlá.
- **Smíšené** (semikvantitativní) – definuje číselnou kategorizaci na základě obecných pojmů, dovoluje tak matematické výpočty i nad mlhavými odhady (Kruliš, 2011).

Slovník kybernetické bezpečnosti analýzu rizik uvádí pouze jako proces pochopení rizika a určení jeho úrovně (Jirásek, Novák a Požár, 2015).

Přestože v jiných oborech existuje celá řada pokročilých metod k analýze a ošetření rizik, v oblasti bezpečnosti informací, potažmo kybernetické bezpečnosti, se nejčastěji používá součin pravděpodobnosti aktivace hrozby a míra jejího dopadu na aktivum. Je to zřejmě dáno snadností její aplikace, rychlý a přehledný operativní výstup pro všechny zúčastněné strany.

3.5 Matice rizik

Matice rizik přehledným způsobem zobrazuje kategorizaci míry rizika při použití nejjednoduššího vzorce výpočtu R = P × D. Na uvedeném obrázku „/“Likelihood odpovídá pravděpodobnosti (P) a „Severity“ dopadu (D). Kategorie „Accept“ představuje zanedbatelná rizika, kategorie „Allow“ mírná rizika, kategorie „Mitigate“ závažná rizika, která je třeba snížit a kategorie „Avoid“ kritická rizika, která je nutné neprodleně ošetřit nebo se jim vyhnout (stakeholdermap.com, 2019).

Obrázek 3.2 Matice rizik (stakeholdermap.com, 2019)

3.6 Traffic Ligh Protocol

Fórum FIRST (Forum of Incident Response and Security Teams), které od roku 1990 sdružuje týmy pro řešení incidentů, definovalo snadný protokol pro rychle identifikovatelné označování důvěrnosti informací a možnosti jejich sdílení. Protokol je postaven na čtyřech značkách odvozených od semaforů pro řízení pozemní dopravy. Odtud je ostatně odvozen i jeho název. Kromě označování míry důvěrnosti informace jej lze použít ekvivalentně i pro rozsahy pravděpodobností, dopadů rizik a dalších měřitelných veličin v analýze rizika.

Užívaná označení TLP:

- **WHITE** — bez omezení, pro veřejnost (zanedbatelné riziko).

- **GREEN** — omezeno na organizaci a partnery s vyloučením veřejných kanálů (mírné riziko).
- **AMBER** — omezeno na organizaci a partnery podle pravidla "potřeba vědět"(závažné riziko).
- **RED** — omezeno výhradně na účastníky (kritické riziko) (first.org, 2016).

3.7 Opatření ke snížení rizika

Pro kvalitativní analýzu rizika Čermák uvádí vzorec R=AxTxV (R=riziko, A=hodnota aktiva, T=hrozba, V=zranitelnost), který následně upravuje pro výpočet zbytkového rizika na RR=AxTxV/C, kde RR je zbytkové riziko (residual risk) a C je opatření (countermeasure) (Čermák, 2010).

Obrázek 3.3 Nákladový model pro realizaci opatření (Doucek et al., 2019)

3.8 Bezpečnostní politika

„Pro účinné vynucení bezpečnostních opatření organizační a technické povahy je nutné, aby veškeré požadavky byly dokumentovány. Určité bezpečnostní standardy jsou často formulovány v bezpečnostní politice, standardech a příručkách. Ačkoliv je mezi těmito dokumenty podstatný rozdíl, jsou velice často zaměňovány. Dokumenty, ve kterých jsou bezpečnostní zásady formulovány, jsou pouze určitým předpokladem k dosažení požadované úrovně bezpečnosti.“ (Šulc, 2018, s. 98)

Dále Šulc dělí bezpečnostní dokumentaci na:

- **Bezpečnostní politiku** (Proč?)– strategický dokument, který definuje účel, cíl, vůli a záměr vedení společnosti v oblasti bezpečnosti.

- **Standard** (Co?) – taktický dokument s obecnými požadavky jako povolené služby, úroveň logování, politika hesel.
- **Procedura** (Jak?) – provozní dokument s popisem konkrétních činností nebo opatření (Šulc, 2018).

Smejkal shodně považuje bezpečnostní politiku za vrcholovou úroveň dokumentace stanovující přístup organizace k řízení cílů bezpečnosti informací, na nižších úrovních pak dílčí dokumenty se specifickými tématy, které by měly být strukturovány pro potřeby cílových skupin v organizaci nebo pokrývat specifická témata (Smejkal, Sokol a Kodl, 2019).

Vyhláška 82/2018 stanovuje povinnost mít bezpečnostní politiku a vést bezpečnostní dokumentaci, povinnost tuto dokumentaci přezkoumávat a udržovat ji aktuální. Příloha 5 vyhlášky pak popisuje doporučenou strukturu a obsah bezpečnostní dokumentace (Vyhláška č. 82/2018 Sb.).

3.9 Triáda C, I, A

Šulc tvrdí, že cílem bezpečnosti informací je zajištění důvěrnosti, dostupnosti a integrity informací.

- Důvěrnost (Confidentiality – C): zajištění, že informace jsou zpřístupněny pouze těm, kteří jsou k tomu oprávněni.
- Integrita (Integrity – I): zajištění správnosti a úplnosti informace (ochrana proti nežádoucím změnám).
- Dostupnost (Availability – A): zajištění, že informace je dostupná v okamžiku potřeby oprávněného uživatele (Šulc, 2018).

Kolouch tuto triádu považuje za nejpoužívanější, avšak pro udržení adekvátní úrovně kybernetické ochrany v současné době nedostačující a požaduje začlenění dalších principů jako Posession/Control (držení či kontrola), Authenticity (autentičnost) a Utility (užitečnost) (Kolouch et al., 2019).

3.10 Cyklus PDCA

Systematický čtyřkrokový proces postupného zlepšování kvality produktů, procesů nebo služeb je připisován Williamu Demingovi a jeho mentorovi Walteru Shewhartovi, proto je také znám jako Demingův nebo Shewhartův cyklus. Jeho název PDCA je akronym jednotlivých fází Plan, Do, Check, Act. Později Deming nahradil fázi Check fází Study,

proto je také možné se setkat s pojmenováním PDSA. Tuto změnu zdůvodňuje nutností prostudovat aktuální výsledky a snahu o zlepšení, zatímco Check (kontrola) spíše sleduje úspěch či neúspěch plánovaných akcí (deming.org, 2021).

Cyklus PDCA byl začleněn do normy ČSN ISO/IEC27001 následujícím způsobem:

- Plánuj (Plan – P): ustavení ISMS, definice cílů, procesů a postupů v souladu s celkovou politikou a cíli organizace.
- Dělej (Do – D): zavádění a provozování ISMS, opatření, procesů a postupů.
- Kontroluj (Check – C): monitorování a přezkoumávání ISMS, měření výkonu vůči cílům a praktickým zkušenostem.
- Jednej (Act – A): udržování a zlepšování ISMS, přijetí opatření k nápravě a opatření založená na výsledcích auditu tak, aby bylo zajištěno neustálé zlepšování (Smejkal, Sokol a Kodl, 2019).

Kolouch považuje PDCA cyklus za jeden ze základních manažerských principů pro postupné zlepšování kvality díky opakování jeho čtyř základních činností, přičemž považuje za vhodnou modifikaci pro oblast kybernetické bezpečnosti variantu OPDCA, kdy je původní model rozšířen o fázi pozorování (Observe – O), která by měla předcházet fázi plánování (Kolouch et al., 2019).

3.11 Princip KISS

Princip KISS vznikl v USA v šedesátých letech dvacátého století, jedná se o akronym ze slov Keep It Simple Stupid, připisovaný Clarenci Leonardovi 'Kelly' Johnsonovi, který jej měl použít při vývoji letounů Lockheed U-2 Dragon Lady a SR-71 Blackbird. Jde o požadavek udržet systém tak jednoduchý, jak je možné, pro zajištění jeho nejlepší funkcionality (marketbussinesnews.com, 2021).

Z hlediska řízení bezpečnosti informací aplikace tohoto principu může pozitivně ovlivňovat všechny úrovně řízení bezpečnosti informací.

4 DÍLČÍ ZÁVĚR

Pro nasazení, udržení a zlepšování systému řízení bezpečnosti informací v organizaci je nutné stanovit hranice oblasti ochrany informací, identifikovat hlavní informační aktiva firmy a jejich umístění v rámci aktiv podpůrných, která umožňují vytváření, zpracování, uložení a distribuci informací jak v rámci vnitrofiremní komunikace, tak při jejich sdělování mimo organizaci.

Je třeba správně identifikovat průchod informace firemními procesy z důvodu správného přiřazení vlastníků/garantů informačních aktiv a zjistit způsob, podobu, místo a prostředky k jejich vytváření, zpracování, uložení a přenosu. Teprve na tomto základě je možné definovat požadavky na ochranu jejich důvěrnosti, dostupnosti, integrity, popřípadě dalších atributů jako je např. účelnost nebo autenticita. Přestože literární i legislativní zdroje uvažují různé atributy ohrožení informací, plná shoda panuje v definici ochrany důvěrnosti, dostupnosti a integrity informací a dat. Při uvažování vlivu této trojice na ostatní procesy ve firmě lze hledisko důvěrnosti mimo jiné považovat za určující pro míru distribuce informací, dostupnost jako důležitý ukazatel pro bussiness continuity a požadavky na integritu lze chápat i jako vyjádření důvěryhodnosti při komunikaci organizace s okolím. Např. u dokumentu opatřeného kvalifikovaným digitálním podpisem lze snadno ověřit, že k příjemci dorazil beze změn a je skutečně od odesilatele.

V okamžiku, kdy je známo množství a forma aktiv, je možné sestavit katalog známých hrozeb a zranitelností, které jsou relevantní pro zjištěná aktiva, a stanovit pravděpodobnosti jejich aktivace. V oblasti definic hrozeb a zranitelností lze nalézt různá vysvětlení těchto pojmů, avšak vždy je třeba uvažovati souvislost s příslušným aktivem, neboť pro aktivum bez zranitelnosti není hrozba relevantní a naopak u zranitelného aktiva bez známé hrozby nelze stanovit pravděpodobnost. Zranitelnost tedy je možné definovat i jako citlivost aktiva vůči hrozbě.

Následujícím krokem je stanovení očekávaných dopadů, kdy už není otázkou zda, případně kdy, nežádoucí situace nastane, ale jde o vyjádření obvykle finanční hodnoty, případně úrovně omezení ekonomické činnosti, které budou následkem takové události.

Oblast ochrany informací a kybernetické bezpečnosti je velmi dynamickým oborem, kdy neustále jsou v hardwaru i softwaru nalézány nové, dříve neznámé, zranitelnosti a lidští útočníci, automatizované systémy i sítě z již napadených strojů v podstatě nepřetržitě útočí na počítače i uživatele po celém světě. Zřejmě i z tohoto důvodu nejsou při analýze rizik bezpečnosti informací používány sofistikovanější metody, které známe z jiných bezpečnostních oborů. Větší váhu zde má totiž rychlost analýzy a snadná přenositelnost výsledku, který lze rychle prezentovat odpovědným osobám a rolím v organizaci.

Pro zmírnění rizika lze při návrhu opatření uvažovat jeho vliv na pravděpodobnost aktivace hrozby nebo snížení míry dopadu na aktivum, či chod organizace. Je však třeba vyhodnotit zejména cenu, náročnost implementace a možnost negativního vlivu na ostatní aktiva, procesy a činnosti ve firmě.

Řízení bezpečnosti informací nesmí být jednorázovou aktivitou typu nastav a zapomeň, jedná se o nikdy nekončící proces analýz, vyhodnocování, návrhů, implementace a sledování změn po celou dobu trvání organizace.

II. PRAKTICKÁ ČÁST

5 ZJIŠTĚNÍ STAVU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ V SUBJEKTU

„*Svět není, co býval ještě minulý týden*“ (Doctorow, 2011, s. 98)

K efektivnímu řízení bezpečnosti informací je nezbytné mít zpracovánu odpovídající dokumentaci, která vymezuje zejména záměr a cíle organizace v oblasti ochrany informací a technologií souvisejících s jejich vytvářením, zpracováním, přenosem a ukládáním. Dílčí prvky této dokumentace by pak měly definovat rozsah oblasti ochrany informací, popis technologií a jejich vzájemných vztahů, prvky ochrany určené k dodržování a plány činností při nežádoucích jevech a událostech. Kromě existence takové dokumentace je však třeba se i zaměřit na její stav, podobu a míru akceptace v rámci organizace. I v případě, že dokumentace neexistuje nebo je v nevyhovující podobě a rozsahu, skutečný stav ochrany informací v organizaci nutně nemusí být špatný, především díky využívání obecně známých principů ochrany informací a zařazování technik nejlepší praxe, což ale vyžaduje samostatnost a aktivitu jednotlivců a podporu vedoucích pracovníků napříč organizací.

5.1 Popis subjektu a základní informace

Vybraný ekonomický subjekt měl za poslední ekonomické období dvacet šest kmenových zaměstnanců, roční obrat menší než 10 milionů EUR a není vlastněn jinými subjekty. Podle definice malých a středních podniků, který je přílohou nařízení evropské komise č. 651/2014 se tedy jedná o **nezávislý malý podnik** (API, 2018). Hlavní činností firmy je dodávka staveb na klíč, včetně projekce, výroby stavebních součástí, stavebních a montážních prací a výroby nábytku. Strukturu vedení má definovánu jako liniově-štábní, kromě sídla má navíc jednu provozovnu v jiném kraji. Jsou zde, mimo obvyklých oddělení jako ekonomické, provozní, nákup, výroba, marketing a prodej, specifická pracoviště projekce, logistiky a podpory staveb, která jsou obsluhována kmenovými zaměstnanci, do oddělení výroby a na realizaci staveb jsou pak najímáni externisté prostřednictvím pracovních agentur a subdodavatelé z řad OSVČ nebo malých firem v místech realizace staveb.

5.2 Povinnosti subjektu dle legislativy

Zkoumaný subjekt není zařazen mezi prvky kritické infrastruktury, neprovozuje významné informační a komunikační systémy ani nedodává základní služby z hlediska zákona č. 181/2014 Sb.: o kybernetické bezpečnosti. Organizace nezpracovává utajované informace a nejsou na ni kladeny požadavky ve smyslu zákona č. 412/2005 Sb.: o ochraně utajovaných informací a bezpečnostní způsobilosti.

Subjekt zpracovává osobní údaje zaměstnanců, klientů, partnerů a je provozovatelem

služby informační společnosti vzhledem k poskytování reklamních a jiných materiálů elektronickou cestou, je tedy povinnou osobou ve smyslu zákonů č. 89/2012 Sb.: Občanský zákoník, č. 480//2004 Sb.: o některých službách informační společnosti, č. 110/2019 Sb.: o zpracování osobních údajů.

Organizace nemá v současné době partnery, kteří by vyžadovali certifikaci dle norem ČSN ISO/IEC 27001 a 27002, ani v krátkodobém výhledu nemá zájem o takovou certifikaci usilovat.

Z uvedených důvodů postačí pro systém řízení bezpečnosti informací vycházet zejména z vyhlášky č. 82/2018 Sb.: o kybernetické bezpečnosti a metodických materiálů Národního úřadu pro kybernetickou a informační bezpečnost.

5.3 Dotazníkové šetření

Pro zjištění existence a stavu bezpečnostní dokumentace a zároveň reálného stavu ochrany informací v subjektu byl vytvořen vstupní dotazník se pětistupňovým hodnocením podle následujících kritérií:

0 – nejsou podklady, v praxi není vykonáváno nebo nelze zjistit.

1 – nejsou podklady, ale v praxi je vykonáváno na základě doporučení.

2 – existuje koncept, ale není oficiálně zavedeno.

3 – dokumentace byla schválena, ale není vynucována.

4 – dokumentace je pravidelně revidována a jsou používány nástroje k jejímu naplnění.

S takto nastavenou hodnoticí stupnicí byli seznámeni jednatel subjektu, office manager a zástupce externího subdodavatele správy IS/IT a byl jim předložen dotazník s následující sadou otázek:

1. Existuje dokument, který vyjadřuje záměry a cíle organizace v oblasti ochrany informací? (Bezpečnostní politika)
2. Existují dokumenty, které by popisovaly např. politiku hesel, schvalování softwaru a běžících služeb, povinnosti uživatelů počítačů nebo chytrých telefonů? (Bezpečnostní standardy)
3. Existují dokumenty, které by popisovaly např. reakci na podezření z napadení počítače, způsoby obnovy dat, zajištění nápravy při selhání serverů? (Bezpečnostní procedury)

4. Existují dokumenty, které popisují způsoby zařazení uživatelů do skupin, např. v závislosti na jejich pracovním zařazení?
5. Existují požadavky na subdodavatele za účelem ochrany např. osobních dat klientů?
6. Existuje plán školení uživatelů v oblasti bezpečnosti informací?
7. Existují pravidla pro ochranu budov a pohyb osob v areálu?
8. Existují pravidla řízení přístupu uživatelů k informacím? (např. všichni všechno, jen pro oddělení apod.)
9. Existují požadavky na automatické uzamčení zařízení při nečinnosti?
10. Je omezeno/řízeno použití vlastních prostředků pro pracovní účely? (BYOD)
11. Je omezeno/řízeno použití firemních prostředků pro soukromé účely? (COPE)
12. Existuje plán zálohování?
13. Existuje plán řízení změn v IS/IT? (Nákup a obnova HW,SW)

5.4 Zpracování výstupu dotazníku a zhodnocení současného stavu

Oslovení hodnotitelé v rámci téže pracovní schůzky nejprve prodiskutovali jednotlivé otázky a následně vyplnili jeden exemplář dotazníku hromadně, neboť byli názorově ve shodě, vyjma hodnocení otázek č. 5 – řízení subdodavatelů a č. 7 – ochrana perimetru, kdy externí správce IS/IT nedisponoval dostatečnou znalostí vnitřních předpisů organizace, proto byla použita hodnota uvedená jednatelem a office managerem subjektu.

Z hodnocení výrazně vystupuje řízení ochrany budov a pohybu osob, to je však zapříčiněno ochranou majetku a strojů a řízením BOZP. V ostatních aspektech subjekt doposud spoléhal na řešení ochrany informací ad-hoc, tedy podle aktuálních potřeb a událostí, bez vyšší konceptuality a centrálního řízení. Pravděpodobně je to způsobeno růstem subjektu v minulých letech, kdy se z mikropodniku rodinného typu stala malá společnost s množstvím subdodavatelů a externích agenturních zaměstnanců. Celkově lze stav hodnotit jako neuspokojivý (ačkoliv je zde patrná snaha o zajištění bezpečnosti informací, zejména u zaměstnanců s vyšší mírou informační gramotnosti) vzhledem k tomu, že zde doposud nebyly vyčleněny finanční a personální zdroje pro centrální řízení, které musí jednoznačně definovat organizace, nikoliv subdodavatel správy IS/IT. Výstupní hodnocení tedy vypadá následovně:

Tabulka 5.1 Výstup dotazníku (vlastní zpracování)

1.	Bezpečnostní politika	1
2.	Bezpečnostní procedury	2
3.	Bezpečnostní standardy	1
4.	Řízení uživatelů	2
5.	Řízení subdodavatelů	3
6.	Školení bezpečnosti informací	1
7.	Ochrana perimetru	4 (v rámci ochrany majetku)
8.	Řízení přístupu k informacím	2
9.	uzamčení při nečinnosti	1
10.	BYOD	0
11.	COPE	0
12.	Plán zálohování	2
13.	Řízení změn IS/IT	1
Suma		20/52

5.5 Dostupné softwarové nástroje pro analýzu rizika

Subjekt nemá zakoupenu licenci na žádný softwarový produkt, který by umožňoval analýzu rizik nebo poskytoval nástroje k jejich řízení. Licenční politika specializovaného nástroje RISKAN společnosti T-SOFT a.s., používaného na Univerzitě Tomáše Bati, zase nedovoluje jeho použití pro komerční účely v privátním sektoru, navíc výstupy z tohoto nástroje pro tabulkový procesor sice umožňují upravovat hodnotu aktiv, pravděpodobnosti a dopadu, ale nelze již změnit seznam aktiv, katalog hrozeb ani pravděpodobnostní a dopadová kritéria. Z těchto důvodů byla pro organizaci vytvořena nová metodika, zohledňující potřeby organizace pro zavedení systému řízení bezpečnosti informací, založená na zpracování dat ve standardním tabulkovém procesoru.

6 ORIENTAČNÍ ANALÝZA RIZIK

V oblasti řízení bezpečnosti informací ve vybraném subjektu doposud nebyla provedena analýza rizik, která by pomohla určit, kde jsou v rámci systémů pro vytváření, zpracování, přenos a ukládání informací zranitelná místa, s jakou pravděpodobností hrozí nebezpečí pro tyto systémy a data v nich uložená, ani jaký by mohla mít dopad aktivace hrozeb na společnost. V oblasti reálného zabezpečení jsou sice aplikovány vybrané metody ochrany dat, ale pravidla jsou určována převážně „per os“ (lat. ústně) a nejsou stanoveny postihy za jejich porušování. Veškeré změny jsou tak realizovány pouze na základě přesvědčení a známé praxe v okolí firmy nebo ze strany externího správce IS/IT.

Orientační (nebo také vstupní) analýza rizik si klade za cíl sestavit přehled aktiv, rozdělit je na primární a podpůrná, zjistit od vlastníků aktiv jejich ohodnocení, za přispění správce IS/IT sestavit katalog relevantních hrozeb, pravděpodobností takových situací a za součinnosti vedení firmy a ekonomického oddělení stanovit kategorie dopadů, které by při aktivaci hrozeb mohly nastat.

6.1 Sestavení metodiky získání informací

Pro získání vstupních dat analýzy rizik byla zvolena Peltierova metoda FRAP (Facilitated Risk Analysis Process), kdy zpracovatelský tým vedený facilitátorem během řízených rozhovorů se zástupci jednotlivých oddělení a technického personálu, který má na starosti běh informačních systémů, analyzuje vztahy informací a jejich důležitosti s požadavky na jejich uložení a ochranu z hlediska důvěrnosti, dostupnosti a integrity.

Metoda FRAP obvykle probíhá ve čtyřech fázích:

1. Iniciační schůzka vedení společnosti, zpracovatelského týmu a facilitátora.
2. Schůzky zpracovatelského týmu se zástupci jednotlivých oddělení.
3. Analýza a vytvoření zprávy facilitátorem.
4. Prezentace závěrů a doporučení vedení společnosti zpracovatelským týmem (Peltier, 2000).

Na iniciační schůzce byl potvrzen záměr subjektu provést analýzu rizik a zároveň byl ustaven tým bezpečnosti informací v obsazení Manažer informační bezpečnosti a Architekt informační bezpečnosti, kdy do role manažera byl jmenován Office manager a do role architekta interní správce účtů informačních systémů. Nesplňují sice kompletní požadavky na tyto role z hlediska doporučení vyhlášky 82/2018, ale jejich pracovní zařazení a náplň činností jsou v rámci kmenových zaměstnanců nejblíže požadovaným

rolím, navíc patří mezi ty jedince, kteří se nad bezpečností informací v organizaci zamýšlí a proaktivně se o ni zasazují. Vytvoření nových pracovních pozic pro tyto role a vypsání výběrového řízení na jejich obsazení v současné době není v možnostech subjektu, zároveň však tyto role nelze outsourcovat, proto je takové rozhodnutí dočasně akceptovatelné. Pozice Auditora informační bezpečnosti není pro analýzu rizik nezbytná a je možné ji v případě potřeby zajistit externě. Tým pro provedení analýzy rizik tak tvoří manažer, architekt, externí správce IS/IT a facilitátor, kterým byl zvolen autor diplomové práce.

6.1.1 Identifikace a hodnocení aktiv

Pro účely identifikace a ohodnocení byla aktiva rozdělena na:

- **Hlavní:** – informace a data, která mají pro organizaci hodnotu a jejichž poškození, ztráta, či nedostupnost by znamenaly škodu, např:
  - smlouvy,
  - faktury,
  - osobní údaje klientů, zaměstnanců, dodavatelů,
  - strategická data a plánování,
  - technologická znalost,
  - výrobní a stavební plány,
  - dokumentace staveb a další...
- **Podpůrná:** – zařízení a služby, které umožňují vytváření, zpracování, ukládání a přenos hlavních aktiv, např:
  - servery,
  - informační a ekonomické systémy,
  - e-mail,
  - notebooky, tablety a mobilní telefony,
  - služby instant messagingu,
  - papír, archiv písemností a další...

Zároveň byly k primárním aktivům sestaveny podpůrné vodící materiály k hodnocení vlastníků aktiv z hlediska požadavků na jejich důvěrnost, dostupnost a integritu. Všechny hodnotící škály jsou celočíselné v rozpětí 1–4, což jednak dovoluje přehledné obarvení pomocí traffic light protokolu a zároveň nedovolí hodnotiteli uchýlit se k volbě

tzv. střední cesty, jak by tomu mohlo být u stupnice s lichým počtem prvků. Také byla pro hodnocení stanovena preference vyšší hodnoty při stavu nejistoty ve volbě odpovídající kategorie.

Vedoucí jednotlivých oddělení organizace byli v rámci následných pracovních schůzek dotazováni na hlavní aktiva, bylo jim vysvětleno, že jako vlastníci/tvůrci těchto aktiv jsou zodpovědní za určení požadované míry důvěrnosti, dostupnosti a integrity těchto aktiv a jsou spoluzodpovědní za jednoznačné určení jejich umístění v rámci podpůrných aktiv. Zároveň vlastníci byli dotázáni na podobu primárních aktiv, zda se jedná o **dokument** (samostatný soubor), **data** (např. vyplnění v IS a zápis do databáze) nebo **papírový dokument**. Pro hodnocení triády C, I, A byly vytvořeny a odsouhlaseny následující hodnotící kritéria.

Tabulka 6.1 Metodické vodítko k hodnocení důvěrnosti (first.org, 2016 - upraveno)

Hodnota	Označení	Popis
1	veřejná	kdokoliv i mimo organizaci se může dostat k informaci bez omezení
2	interní	kdokoliv v organizaci má přístup k informaci, partneři a subdodavatelé pouze důvěrnou cestou (email, SMS a pod.)
3	důvěrná	k informacím je omezený přístup, např. v rámci oddělení nebo pracovního týmu
4	vyhrazené	k informacím má přístup jen omezený počet vyjmenovaných jednotlivců

Tabulka 6.2 Metodické vodítko k hodnocení dostupnosti (vlastní zpracování)

Hodnota	Označení	Popis
1	týden	informace nechybí nebo se dá snadno opatřit jinde
2	den	požadavky lze krátkodobě odložit aniž by to způsobilo potíže
3	4 hodiny	informace musí být zpracována v rámci jedné směny
4	okamžitě	nedostupnost informace může způsobit okamžitou škodu

Zároveň v průběhu vyhodnocování byly pro každé podpůrné aktivum zaznamenány vždy nejvyšší dosažené hodnoty atributů C, I, A, pro určení míry požadované ochrany podpůrného aktiva a také sumy dosažených hodnot těchto atributů pro další zpracování.

Tabulka 6.3 Metodické vodítko k hodnocení integrity (vlastní zpracování)

Hodnota	Označení	Popis
1	lze zjistit pohledem	informaci lze opravit nebo má nízkou důležitost
2	oznámení o změně	stačí vědět, že se informace změnila, případně kdo změnu provedl
3	zamezení změn	informaci je třeba chránit např. zápisem nové verze s číslem nebo datem
4	ověření nezměnitelnosti	proti změnám ověřit kontrolním součtem nebo digitálním podpisem

6.1.2 Sestavení katalogu hrozeb a určení pravděpodobností

Po dokončení identifikace a klasifikace hlavních a podpůrných aktiv byl týmem formou brainstormingu sestaven katalog hrozeb za použití seznamů modelových hrozeb z vyhlášky o kybernetické bezpečnosti 82/2018, internetových zdrojů a vlastních zkušeností, který byl následně redukován na hrozby relevantní pro podpůrná aktiva organizace. Výstupem diskuze o hrozbách a zranitelnostech bylo rozhodnutí definovat zranitelnost jako citlivost aktiva vůči působení hrozby, tedy průsečík na osách **Hrozba** × **Podpůrné aktivum**. Místo prostého označení zranitelnosti byla v rámci urychlení postupu v tomtéž kroku určena míra pravděpodobnosti aktivace pomocí následující metodiky, která jako vstupní údaje používá veřejně dostupné zdroje o četnostech útoků, vyhodnocení serverových logů, tiskové zprávy Núkib, informace z odborných webových stránek i známé události z okolí subjektu.

Tabulka 6.4 Metodické vodítko k hodnocení pravděpodobnosti (vlastní zpracování)

Hodnota	Označení	Popis
1	nízká	1/10 let, téměř se nevyskytuje
2	střední	1/rok, hrozí např. při dokončení stavby/projektu
3	vysoká	4-10/rok
4	kritická	trvalé ohrožení (např. APT, zaměstnanci apod.)

6.1.3 Stanovení dopadů

Po určení zranitelností a odhadu pravděpodobnosti jejich aktivace bylo pro definici dopadových kritérií nutné přizvat vedení firmy a zástupce ekonomického oddělení, neboť je v jejich kompetenci řízení finančních toků a zodpovědnost za chod firmy.

Při stanovení dopadu je třeba si uvědomit, že ne vždy se jedná čistě o finanční, či jednoznačně vyčíslitelnou škodu např. o pokutu při porušení povinností ochrany osobních údajů, nemusí se jednat o pouhý nákup a reinstalace serverů či notebooků, ale také může nastat situace, že bude nutné zajistit obnovu struktury a dat informačního

systému. Proto byla v dopadech kromě finančních nákladů/ztráty započtena i doba, po kterou by uživatelé neměli přístup k hlavním nebo podpůrným aktivům a jak moc by to ovlivnilo chod firmy.

Tabulka 6.5 Metodické vodítko k hodnocení dopadu (vlastní zpracování)

Hodnota	Slovní označení	Popis
1	zanedbatelný	do 10 tis. / zastaví jednotlivce
2	významný	do 50 tis. / zastaví tým nebo oddělení
3	závažný	do 500 tis. / zastaví více týmů nebo oddělení
4	kritický	nad 500 tis. / zastaví všechny / likvidační

6.2 Sestavení metodiky výpočtu rizika

Harkins popisuje výpočet rizika jako „*Impact of Asset* × *Probability of Threat* × *Vulnerability exposure* = *Total Risk Points*“ (dopad na aktivum × pravděpodobnost hrozby × vystavení zranitelnosti = celkové riziko) (Harkins, 2013).

Nejběžnější a nejpoužívanější vzorec pro výpočet rizika v oblasti ISMS z českých zdrojů je

$$\mathbf{R} = \mathbf{P} \times \mathbf{D}$$

kdy **R** znamená výsledné riziko, **P** pravděpodobnost aktivace hrozby a **D** dopad na aktivum.

Požadavkem vyhlášky o kybernetické bezpečnosti je vyjádření rizika vzhledem k atributům důvěrnosti, dostupnosti a integrity aktiva, avšak není definován způsob takového výpočtu. Protože však v rámci identifikace hlavních aktiv a jejich umístění na podpůrných aktivech byly od vlastníků zjištěny požadované úrovně těchto atributů, bylo možné je do výpočtu zahrnout a rozšířit jej o příslušná váhová kritéria.

Nový vzorec výpočtu tedy zahrnuje vážený průměr triády C, I, A jako podíl nejvyšších dosažených hodnot jednotlivých atributů v rámci podpůrného aktiva násobených sumou příslušných atributů za všechna aktiva a sumy všech atributů.

$$\mathbf{R} = \mathbf{P} \times \mathbf{D} \times \frac{\sum_c \times max_c + \sum_i \times max_i + \sum_a \times max_a}{\sum_{(cia)}}$$

Výpočet zahrnuje jak hodnotu podpůrného aktiva vzhledem k možnému ohrožení důvěrnosti, dostupnosti a integrity, tak jeho podíl v rámci všech podpůrných aktiv organizace.

6.3 Vliv opatření a metodika výpočtu zbytkového rizika

Při návrhu opatření na zmírnění rizika je zvažován jeho vliv zejména na pravděpodobnost a dopad, zároveň však je třeba vyhodnotit i cenu takového opatření a jeho relevanci. Není ekonomicky smysluplné snížit dopad negativní události např. o dvacet tisíc zavedením opatření v ceně stovek tisíc korun.

Základní vzorec pro výpočet vlivu opatření na výsledné riziko modifikovaný podle Čermáka (Čermák, 2010).

$$\mathbf{R} = \frac{\mathbf{P} \times \mathbf{D}}{\mathbf{O}}$$

Při aplikaci vlivu opatření do rozšířeného modelu byl uvažován vliv opatření na pravděpodobnost i na dopad. Přestože v rámci brainstormingu realizačního týmu analýzy rizik nebylo nalezeno opatření, které by mělo vliv na oba parametry zároveň, neznamená to, že takové opatření neexistuje nebo v budoucnu nebude existovat. Vzhledem k možnému synergickému efektu takového opatření byl výpočet určen jako součin vlivu na pravděpodobnost (O_P) a dopad (O_D). Výsledný vzorec je tedy

$$\mathbf{R} = \frac{\mathbf{P} \times \mathbf{D} \times \frac{\sum_c \times max_c + \sum_i \times max_i + \sum_a \times max_a}{\sum_{(cia)}}}{O_P \times O_D}$$

který lze zjednodušeně vyjádřit také jako

$$\mathbf{R} = \mathbf{P} \times \mathbf{D} \times \frac{\sum_c \times max_c + \sum_i \times max_i + \sum_a \times max_a}{\sum_{(cia)} \times O_P \times O_D}$$

Tabulka 6.6 Metodické vodítko k hodnocení vlivu ochranného opatření (vlastní zpracování)

Hodnota	Slovní označení	Popis
1	zanedbatelný	opatření nemá vliv na hrozbu/dopad
2	znatelný	opatření má měřitelný vliv
3	významný	opatření má velký vliv na hrozbu nebo významně snižuje dopad
4	eliminační	opatření eliminuje hrozbu nebo sníží dopad na minimum

6.4 Vlastní excelový soubor

Takovouto analýzu rizik by měl tým bezpečnosti informací provádět periodicky (ideálně jednou za rok) za účelem ověření, zda se v organizaci nezměnil počet aktiv a jejich využívání, dále pak před každou plánovanou změnou v prostředí IS/IT nebo před změnami

v organizační struktuře společnosti. Vzhledem k těmto povinnostem byl vznesen požadavek subjektu na zapracování zjištěných dat a vzorců pro výpočet rizika do souboru standardního tabulkového procesoru, který tým informační bezpečnosti bude moci použít při dalších analýzách. Struktura souboru a popisy jednotlivých funkcionalit jsou v následujících podkapitolách.

6.4.1 List A – Aktiva

Na listu Aktiva jsou ve sloupci A položkově v řádcích uvedena hlavní aktiva, seskupená podle jednotlivých oddělení a sumarizovaná podle typu (např. personalistika, projektová dokumentace), ve sloupci pak B případný upřesňující popis o jaká data se jedná (např. smlouvy+mzdové výměry, výkres/situační zpráva). Sloupec C obsahuje informaci o jakou podobu aktiva se jedná, zda o dokument, data (v IS, databázi) či papír, ve sloupci D je pak uveden vlastník aktiva. Sloupce F, G a H obsahují hodnocení aktiva vlastníkem z hlediska požadavků na ochranu důvěrnosti, dostupnosti a integrity v celočíselné škále 1-4. Je zde pro jednotlivé hodnoty použito podmíněné formátování pro obarvení v souladu s TLP. Ve sloupcích J-Z jsou pak na řádku 5 uvedena jednotlivá podpůrná aktiva společnosti, kdy umístění hlavního aktiva na podpůrném je vyjádřeno písmenem „x“ na příslušném průsečíku. Podpůrná aktiva jsou barevně rozlišena na ta, která má subjekt pod vlastní správou, včetně administrátorských přístupů, a pronajaté služby, kde je konfigurace jen na vyžádání nebo není možná. V náhledu zpracování jsou použita vybraná aktiva oddělení projekce, hodnoty důvěrnosti, dostupnosti a integrity a umístění na podpůrných aktivech byly náhodně změněny.

Tabulka 6.7 List A (vlastní zpracování)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	**Aktivum**	Popis aktiva	**typ**	**Vlastník**		**Dův**	**Dos**	**Int**		**Kde leží**																
2					Suma Dův	23			Max Dův	4	3	3	4	4	4	3	3	3	4	3	4	0	3	4	0	4
3					Suma Dos		17		Max Dos	2	4	4	2	4	4	3	4	3	4	4	2	0	4	4	0	4
4					Suma Int			24	Max Int	4	4	4	4	4	4	4	4	4	4	4	4	0	4	4	0	4
5	*Název aktiva*	*Smlouva, Podklady, Faktura, Výkres*	*Data, Dokument, Papír, Ústní informace*	*Manažer, Vedoucí, Autor*						InfOS	Windows server	Priv. Cloud	Project management	mail	lokální disky	výměnná média	Papír	archiv	telefon	instant messaging	Tabule	Sítě evidence	Zálohovací server	geo záloha	data u IT	privátní úložiště
6																										
7	**Projekce**																									
8	projektová dokumentace pro st. Řízení	výkres, zpráva	dokument, papír	Vedoucí projekce		3	2	4			x	x		x	x	x	x	x	x	x			x	x		x
9	přílohy pro SOD	výkres	dokument, papír	Vedoucí projekce		3	3	4			x	x		x	x	x	x	x	x	x			x			x
10	projekt k realizaci	výkres	dokument, papír	Vedoucí projekce		3	4	3			x	x		x	x		x		x	x			x	x		x
11	subdodávky pro projekci	objednávka, sdělení podkladů	dokument	Vedoucí projekce		4	2	4		x			x	x	x				x		x				x	
12	vyhodnocení dodavatelů		dokument	Vedoucí projekce		4	2	3						x	x										x	x
13	Koordinace procesů jednotlivých projektů		data	Vedoucí projekce		3	2	3					x				x				x					
14	předprojektová příprava	náčrt, vizuální představa	dokument, papír	Vedoucí projekce		3	2	3			x	x	x	x	x		x		x				x			x
15																										

Pro další použití byla definována následující speciální pole:

F2 obsahuje sumu hodnocení požadované důvěrnosti hlavních aktiv, G3 sumu hodnocení požadované dostupnosti hlavních aktiv a H4 sumu hodnocení požadované integrity hlavních aktiv.

Vzorová funkce pro získání hodnoty pro pole F2 je

```
=SUM(F6:F100)
```

Pole J2-Z4 obsahují nejvyšší získané ohodnocení důvěrnosti, dostupnosti a integrity pro příslušná podpůrná aktiva na základě umístění aktiv hlavních a jejich hodnocení vlastníky. Platné maximum bylo vyhledáno pomocí funkce MAXIFS.

Vzorová funkce pro získání hodnoty pro pole J2 je

```
=MAXIFS($F$6:$F$100;J$6:J$100;"x")
```

6.4.2 Listy P a D – Pravděpodobnost a Dopad

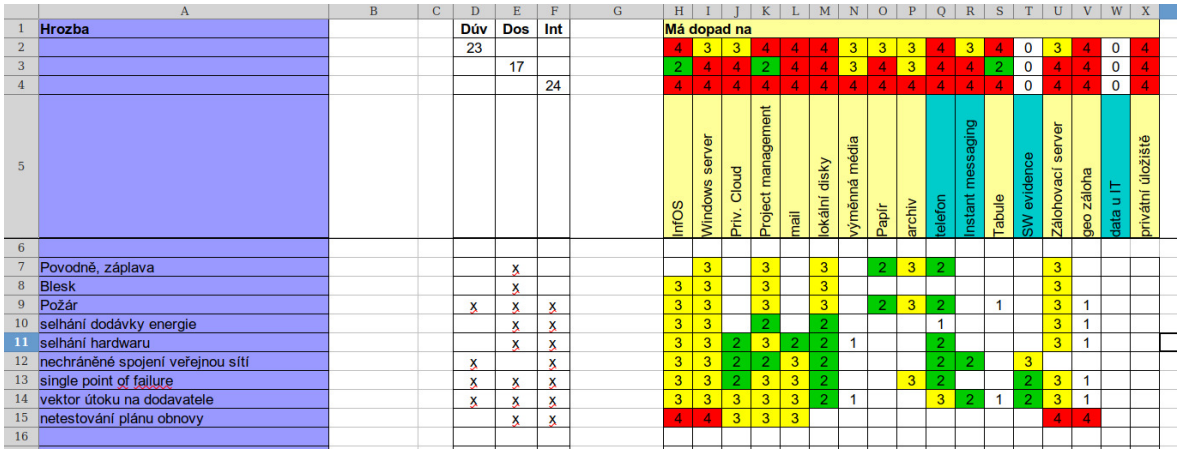
Na listu Pravděpodobnost jsou ve sloupci A položkově řazeny relevantní hrozby, sloupec B slouží pro poznámky nebo upřesnění. Ve sloupcích D, E a F je pak písmenem „x“ vyznačeno, zda se jedná o hrozbu pro důvěrnost, dostupnost nebo integritu dat umístěných na podpůrném aktivu. Ve sloupcích H-X je pak do průsečíků Hrozba × podpůrné aktivum zaznamenána úroveň pravděpodobnosti takové zranitelnosti. Pole H2-X5 obsahují nejvyšší dosažené hodnoty důvěrnosti, dostupnosti a integrity příslušných aktiv převzaté z listu Aktiva, protože čím významnější data jsou uložena na podpůrném aktivu, tím může být atraktivnějším cílem pro případného útočníka. Pro zadané hodnoty pravděpodobností je použito podmíněné formátování pro obarvení v souladu s TLP. V náhledu zpracování jsou uvedeny náhodně vybrané hrozby, vyjádření zranitelnosti a hodnot pravděpodobnosti jsou náhodná.

Tabulka 6.8 List P (vlastní zpracování)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	**Hrozba**	Popis hrozby		**Dův**	**Dos**	**Int**		**Ohrožuje**																
2				23				4	3	3	4	4	4	3	3	3	4	3	4	0	3	4	0	4
3					17			2	4	4	2	4	4	3	4	3	4	4	2	0	4	4	0	4
4						24		4	4	4	4	4	4	4	4	4	4	4	4	0	4	4	0	4
5								InfOS	Windows server	Priv. Cloud	Project management	mail	lokální disky	výměnná média	Papír	archiv	telefon	Instant messaging	Tabule	SW evidence	Zálohovací server	geo záloha	data u IT	privátní úložiště
6																								
7	Povodně, záplava				x			2			2		2		2	2	3				2			
8	Blesk				x			2	2		2		2								2			
9	Požár			x	x	x		1	1		1		1		1	1	1		1		1	1		
10	selhání dodávky energie				x	x		2	2		2		1				1				2	1		
11	selhání hardwaru				x	x		1	1	1	1	1	2	1			2				1	1		
12	nechráněné spojení veřejnou sítí			x		x		3	3	3	3	3	3				3	3		3				
13	single point of failure			x	x	x		4	4	4	4	4	2			3	2			4	4	3		
14	vektor útoku na dodavatele			x	x	x		4	4	4	4	4	4	4			4	4	4	4	4	4		
15	netestování plánu obnovy				x	x		4	4	4	4	4									4	4		
16																								

List Dopad popsanou strukturu kompletně kopíruje, slouží však pro stanovení míry dopadu. V náhledu zpracování jsou přejaty vybrané hrozby z listu Pravděpodobnost, hodnoty dopadů jsou náhodné.

Tabulka 6.9 List D (vlastní zpracování)

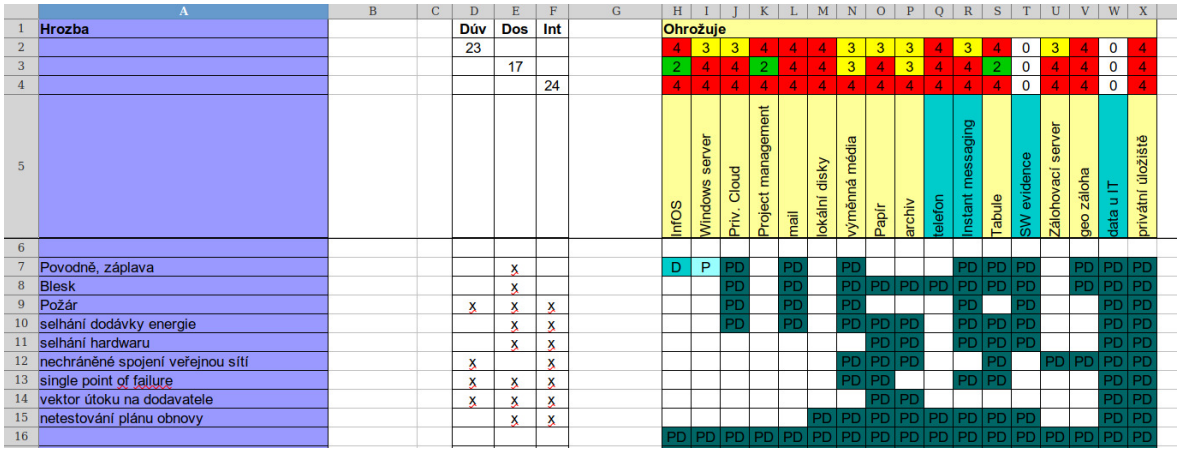


	A	D	E	F	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	**Hrozba**	**Dův**	**Dos**	**Int**	**Má dopad na**																
2		23			4	3	3	4	4	4	3	3	3	4	3	4	0	3	4	0	4
3			17		2	4	4	2	4	4	3	4	3	4	4	2	0	4	4	0	4
4				24	4	4	4	4	4	4	4	4	4	4	4	4	0	4	4	0	4
5					InfOS	Windows server	Priv. Cloud	Project management	mail	lokální disky	výměnná média	Papír	archiv	telefon	Instant messaging	Tabule	SW evidence	Zálohovací server	geo záloha	data u IT	privátní úložiště
6																					
7	Povodně, záplava		x			3		3		3		2	3	2				3			
8	Blesk		x		3	3		3		3								3			
9	Požár	x	x	x	3	3		3		3		2	3	2		1		3	1		
10	selhání dodávky energie		x	x	3	3		2		2				1				3	1		
11	selhání hardwaru		x	x	3	3	2	3	2	2	1			2				3	1		
12	nechráněné spojení veřejnou sítí	x		x	3	3	2	2	3	2				2	2		3				
13	single point of failure	x	x	x	3	3	2	3	3	2			3	2			2	3	1		
14	vektor útoku na dodavatele	x	x	x	3	3	3	3	3	2	1			3	2	1	2	3	1		
15	netestování plánu obnovy		x	x	4	4	3	3	3									4	4		
16																					

6.4.3 List C – Kontrola

List Kontrola slouží k ověření, zda byly vyplněny shodné průsečíky zranitelností pro pravděpodobnost a dopad a zároveň, zda jsou ve správném rozsahu hodnot. Kontrola je prováděna rekurzivním použitím funkcí IF a AND. Pokud jsou obě položky vyplněny, je v kontrole zobrazeno prázdné pole. Chybějící pravděpodobnost je označena písmenem „P“, chybějící dopad písmenem „D“. Pokud není na příslušných listech v odpovídajícím poli žádná hodnota, je to chápáno tak, že hrozba nemá na aktivum vliv a je vypsáno „PD“. Všechny varianty jsou pro snazší detekci barevně rozlišeny.V náhledu zpracování jsou přejaty vybrané hrozby z listu Pravděpodobnost, záměrně je zde na chybějících hodnotách na listech Pravděpodobnost a Dopad předvedena funkce kontroly.

Tabulka 6.10 List C (vlastní zpracování)



	A	D	E	F	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	**Hrozba**	**Dův**	**Dos**	**Int**	**Ohrožuje**																
2		23			4	3	3	4	4	4	3	3	3	4	3	4	0	3	4	0	4
3			17		2	4	4	2	4	4	3	4	3	4	4	2	0	4	4	0	4
4				24	4	4	4	4	4	4	4	4	4	4	4	4	0	4	4	0	4
5					InfOS	Windows server	Priv. Cloud	Project management	mail	lokální disky	výměnná média	Papír	archiv	telefon	Instant messaging	Tabule	SW evidence	Zálohovací server	geo záloha	data u IT	privátní úložiště
6																					
7	Povodně, záplava		x		D	P	PD		PD		PD				PD	PD	PD		PD	PD	PD
8	Blesk		x				PD		PD		PD	PD	PD	PD	PD	PD	PD		PD	PD	PD
9	Požár	x	x	x			PD		PD		PD				PD		PD			PD	PD
10	selhání dodávky energie		x	x			PD		PD		PD	PD	PD		PD	PD	PD			PD	PD
11	selhání hardwaru		x	x								PD	PD		PD	PD	PD			PD	PD
12	nechráněné spojení veřejnou sítí	x		x							PD	PD	PD			PD		PD	PD	PD	PD
13	single point of failure	x	x	x							PD	PD			PD	PD				PD	PD
14	vektor útoku na dodavatele	x	x	x								PD	PD							PD	PD
15	netestování plánu obnovy		x	x						PD	PD	PD	PD	PD	PD	PD	PD			PD	PD
16					PD	PD	PD	PD	PD	PD	PD	PD	PD	PD	PD	PD	PD	PD	PD	PD	PD

Vzorová funkce pro provedení kontroly v poli H7

```
=IF(
    AND(
        $D.H7>=1;
        $D.H7<=4
    );
    (
    IF(
        AND(
            $P.H7>=1;
            $P.H7<=4
        );
        "";
        "P"
    ));
    IF(
        AND(
            $P.H7>=1;
            $P.H7<=4
        );
        "D";
        "PD"
    )
 )
```

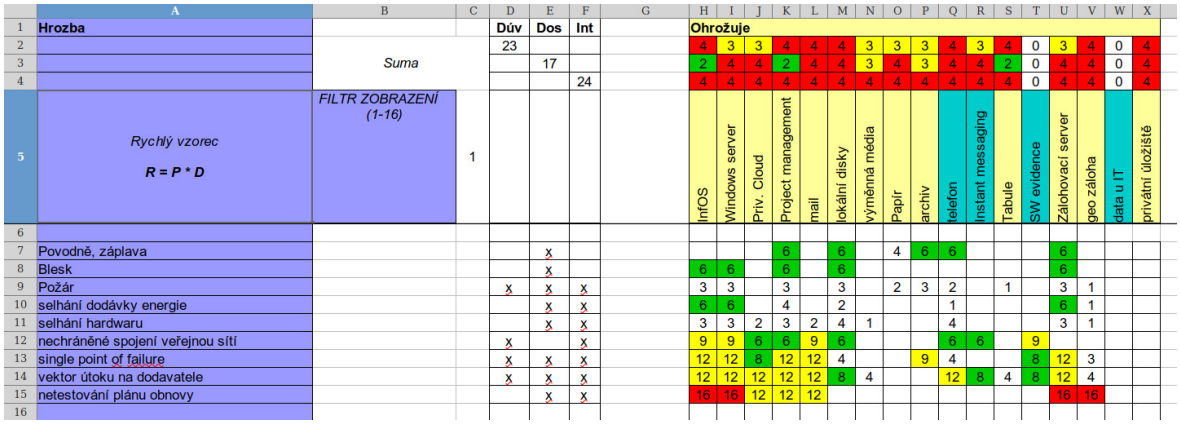
6.4.4 List R_PD – Základní výpočet rizika

Na listu Rizika_PD je v polích, kde je na předchozích listech definována Pravděpodobnost a Dopad výsledek vzorce R = P × D. Obarvení podle TLP je pak realizováno rovnoměrně v rozsazích

- **1-4** – zanedbatelné riziko
- **5-8** – mírné riziko
- **9-12** – závažné riziko
- **13-16** – kritické riziko

Pro lepší možnosti vyhodnocování informací bylo doplněno pole „Filtr zobrazení“, který lze zároveň použít k nastavení limitní hranice akceptovatelného rizika. K funkci je použita hodnota pole **C5**, kdy zadáním čísla v rozsahu 1-16 je definována spodní hranice pro zobrazení jednotlivých výsledků, zároveň toto pole je také obarveno podle TLP. Když se zpracovatel například rozhodne, že kategorie zanedbatelných rizik nemá být zobrazena, docílí toho zadáním hodnoty 5 do pole C5. V náhledu zpracování jsou přejaty vybrané hrozby z listu Pravděpodobnost.

Tabulka 6.11 List R_PD (vlastní zpracování)



	Hrozba			Dúv	Dos	Int	Ohrožuje															
2		Suma		23			4	3	3	4	4	4	3	3	3	4	3	4	0	3	4	0	4
3					17		2	4	4	2	4	4	3	4	3	4	4	2	0	4	4	0	4
4						24	4	4	4	4	4	4	4	4	4	4	4	4	0	4	4	0	4
5	Rychlý vzorec R = P * D	FILTR ZOBRAZENÍ (1-16)	1				InfOS	Windows server	Priv. Cloud	Project management	mail	lokální disky	výměnná média	Papír	archiv	telefon	Instant messaging	Tabule	SW evidence	Zálohovací server	geo záloha	data u IT	privátní úložiště
6																							
7	Povodně, záplava				x					6		6		4	6	6				6			
8	Blesk				x		6	6		6		6								6			
9	Požár			x	x	x	3	3		3		3		2	3	2		1		3	1		
10	selhání dodávky energie				x	x	6	6		4		2				1				6	1		
11	selhání hardwaru				x	x	3	3	2	3	2	4	1			4				3	1		
12	nechráněné spojení veřejnou sítí			x		x	9	9	6	6	9	6				6	6		9				
13	single point of failure			x	x	x	12	12	8	12	12	4			9	4			8	12	3		
14	vektor útoku na dodavatele			x	x	x	12	12	12	12	12	8	4			12	8	4	8	12	4		
15	netestování plánu obnovy				x	x	16	16	12	12	12									16	16		
16																							

Vzorová funkce pro provedení základního výpočtu v poli H7 a kontrolu hodnoty proti filtru zobrazení.

```
=IF(
    ($P.H7*$D.H7
    )<$C$5;
    "";
    ($P.H7*$D.H7)
 )
```

6.4.5 List R_PDV – Rozšířený výpočet rizika

Na listu Rizika_PDV je v polích, kde je na předchozích listech definována Pravděpodobnost a Dopad výsledek vzorce

$$\mathbf{R} = \mathbf{P} \times \mathbf{D} \times \frac{\sum_c \times max_c + \sum_i \times max_i + \sum_a \times max_a}{\sum_{(cia)}}$$

kde pro výpočet pole H7 je jako max_c použita hodnota H2, pro max_a hodnota H3 a max_i hodnota H4. Pro $\sum_c$ je pak použita hodnota pole D2, pro $\sum_a$ E3 a $\sum_i$ F4.

Protože už je v tomto kroku počítán vážený průměr důvěrnosti, dostupnosti a integrity aktiva, a poměrné rozdělení možných hodnot rizika na čtvrtiny nemusí být pro organizaci výhodné, je kategorizace rizik a obarvení podle TLP nastaveno dynamicky. Podmíněné formátování je načítáno z hodnot v polích Z8-Z11, které vyjadřují vždy spodní hranici dané kategorie. Ve výchozím stavu je rozdělení upraveno na stejné části, ale kdykoliv může být podle požadavku organizace změněno na spodní hranici kterékoliv kategorie a dynamické obarvení se pak automaticky změní příslušným způsobem. Při započtení vah jednotlivých kritérií výsledek přestává být celočíselný, proto je výpočet horní hranice podmíněného formátování nastaven jako spodní hranice následující kategorie mínus jedna miliardtina. Zároveň pro zachování přehlednosti je ve formátu buněk nastaveno zaokrouhlení na celá čísla. Rozsah dynamického obarvení podle TLP je pak definován vztahy

- **1-(Z7–1/8^{9})** – zanedbatelné riziko
- **Z7-(Z8–1/9^{9})** – mírné riziko
- **Z8-(Z9–1/10^{9})** – závažné riziko
- **Z9-Z10** – kritické riziko

Také na tomto listu je použita funkce Filtr zobrazení, používá však rozsah 1-64 a je dynamicky formátována TLP podle stejného rozdělení. V náhledu zpracování jsou přejaty vybrané hrozby z listu Pravděpodobnost.

Tabulka 6.12 List R_PDV (vlastní zpracování)

	A	B	C	D	E	F	G
1	**Hrozba**			**Dův**	**Dos**	**Int**	
2				23			
3		*Suma*			17		
4						24	
5		*FILTR ZOBRAZENÍ (1-64)*	5				Koeficient
6							
7	Povodně, záplava				x	x	
8	Blesk				x		
9	Požár			x	x	x	
10	selhání dodávky energie				x	x	
11	selhání hardwaru				x	x	
12	nechráněné spojení veřejnou sítí			x		x	
13	single point of failure			x	x	x	
14	vektor útoku na dodavatele			x	x	x	
15	netestování plánu obnovy				x	x	
16							

	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	**Ohrožuje**																
2	4	3	3	4	4	4	3	3	3	4	3	4	0	3	4	0	4
3	2	4	4	2	4	4	3	4	3	4	4	2	0	4	4	0	4
4	4	4	4	4	4	4	4	4	4	4	4	4	0	4	4	0	4
5	InfOS	Windows server	Priv. Cloud	Project management	mail	lokální disky	výměnná média	Papír	archiv	telefon	Instant messaging	Tabule	SW evidence	Zálohovací server	geo záloha	data u IT	privátní úložiště
6																	
7				12		15		10	14	15				15			
8		6				6								6			
9	10	11		10		12		7	10	8				11			
10	12	15		8		5								15			
11	6	8	5	6	5	10				10				8			
12	26	23	15	18	26	18				18	15						
13	42	44	29	42	48	16			30	16				44	12		
14	42	44	44	42	48	32	14			48	29	14		44	16		
15	33	41	31	24	31									41	41		
16																	

	Z	AA
5	**Spodní hranice (lze předefinovat)**	**Význam**
6	1	**zanedbatelné riziko**
7	16	**mírné riziko**
8	32	**závažné riziko**
9	48	**kritické riziko**
10	64	**maximální hodnota**

Vzorová funkce pro provedení rozšířeného výpočtu v poli H7 a kontrolu hodnoty proti filtru zobrazení.

```
=IF(
     (
       (
         (
           IF(
               $D7="x";
               (H$2*$D$2);
               0
             )
         )+(
              IF(
                  $E7="x";
                  (H$3*$E$3);
                  0
                )
           )+(
               IF(
                   $F7="x";
                   (H$4*$F$4);
                   0
                 )
             )
       )/SUM(
              $D$2;
              $E$3;
              $F$4
```

```
            )*(
                $P.H7*$D.H7
              )
    )<$C$5;
    "";
    (
      (
        IF(
            $D7="x";
            (H$2*$D$2);
            0
          )
      )+(
          IF(
              $E7="x";
              (H$3*$E$3);
              0
            )
        )+(
            IF(
                $F7="x";
                (H$4*$F$4);
                0
              )
          )
    )/SUM(
            $D$2;
            $E$3;
            $F$4
            )*(
                $P.H7*$D.H7
              )
)
```

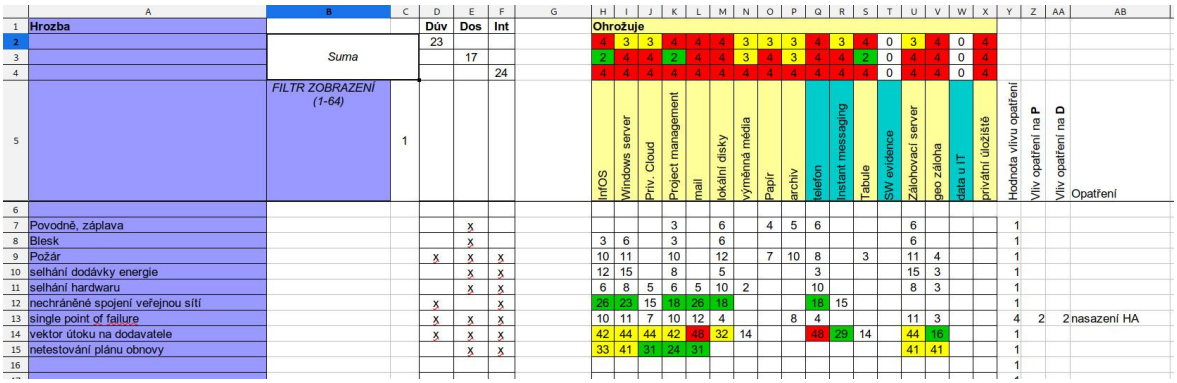
6.4.6 List 0 – Vliv opatření

List Opatření kopíruje strukturu a základ vzorce z listu Rizika_PDV, přidává sloupce Y, Z, AA a AB, kde Y je součin Z a AA, Z je vliv opatření na Pravděpodobnost, AA vliv opatření na Dopad a AB je pro popis vlivu zkoumaného opatření. V náhledu zpracování jsou přejaty vybrané hrozby z listu Pravděpodobnost, jako příklad pro výpočet je uvedeno „nasazení HA“ (High Avalability – systémy s vysokou dostupností) s vlivem o hodnotě 2 na Pravděpodobnost i Dopad.

Vzorec pro výpočet zbytkového rizika je pak

$$\mathbf{R} = \frac{\mathbf{P} \times \mathbf{D} \times \frac{\sum_c \times max_c + \sum_i \times max_i + \sum_a \times max_a}{\sum_{(cia)}}}{O_P \times O_D}$$

Tabulka 6.13 List O (vlastní zpracování)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB
1	**Hrozba**			**Dův**	**Dos**	**Int**		**Ohrožuje**																				
2		Suma		23				4	3	3	4	4	4	3	3	3	4	3	4	0	3	4	0	4				
3					17			2	4	4	2	4	4	3	4	3	4	4	2	0	4	4	0	4				
4						24		4	4	4	4	4	4	4	4	4	4	4	4	0	4	4	0	4				
5		FILTR ZOBRAZENÍ (1-64)	1					InfOS	Windows server	Priv. Cloud	Project management	mail	lokální disky	výměnná média	Papír	archiv	telefon	Instant messaging	Tabule	SW evidence	Zálohovací server	geo záloha	data u IT	privátní úložiště	Hodnota vlivu opatření	Vliv opatření na **P**	Vliv opatření na **D**	Opatření
6																												
7	Povodně, záplava				x						3		6		4	5	6				6				1			
8	Blesk				x			3	6		3		6								6				1			
9	Požár			x	x	x		10	11		10		12		7	10	8		3		11	4			1			
10	selhání dodávky energie				x	x		12	15		8		5				3				15	3			1			
11	selhání hardwaru				x	x		6	8	5	6	5	10	2			10				8	3			1			
12	nechráněné spojení veřejnou sítí			x		x		26	23	15	18	26	18				18	15							1			
13	single point of failure			x	x	x		10	11	7	10	12	4			8	4				11	3			4	2	2	nasazení HA
14	vektor útoku na dodavatele			x	x	x		42	44	44	42	48	32	14			48	29	14		44	16			1			
15	netestování plánu obnovy				x	x		33	41	31	24	31									41	41			1			
16																									1			

Vzorová funkce pro provedení rozšířeného výpočtu v poli H7 a kontrolu hodnoty proti filtru zobrazení.

```
=IF(
      (
        (
          (
            IF(
                $D7="x";
                (H$2*$D$2);
                0
              )
          )+(
              IF(
                  $E7="x";
                  (H$3*$E$3);
                  0
                )
            )+(
                IF(
                    $F7="x";
                    (H$4*$F$4);
                    0
                  )
              )
        )/SUM(
                $D$2;
                $E$3;
                $F$4
            )*(
                 $P.H7*$D.H7/$Y7
              )
      )<$C$5;
      "";
      (
        (
          IF(
              $D7="x";
              (H$2*$D$2);
              0
            )
        )+(
            IF(
                $E7="x";
                (H$3*$E$3);
```

```
                0
            )
        )+(
            IF(
                $F7="x";
                (H$4*$F$4);
                0
            )
        )
    )/SUM(
            $D$2;
            $E$3;
            $F$4
        )*(
            $P.H7*$D.H7/$Y7
        )
)
```

6.4.7 List Hodnocení rizik

List Hodnocení rizik obsahuje základní zobrazení matic rizika a rozsahy hodnocení výsledků pro základní výpočet P × D i pro výpočet rozšířený o váhy aktiv.

Tabulka 6.14 List Hodnocení rizik (vlastní zpracování)

1											
2			Základní výpočet								
3				D						Vypočtené riziko	
4			1	2	3	4				Rozsah	Význam
5	P	1	1	2	3	4				1-4,99	zanedbatelné riziko
6		2	2	4	6	8				5-8,99	mírné riziko
7		3	3	6	9	12				9-12,99	závažné riziko
8		4	4	8	12	16				13-16	kritické riziko
9											
10											
11											
12											
13											
14			Rozšířený výpočet								
15				V						Vypočtené riziko	
16	7		1	2	3	4				Rozsah	Význam
17	P*D	4	4	8	12	16				1-15,99	zanedbatelné riziko
18		6	6	12	18	24				16-31,99	mírné riziko
19		12	12	24	36	48				32-47,99	závažné riziko
20		16	16	32	48	64				48-64	kritické riziko
21											

7 PROHLÁŠENÍ O APLIKOVATELNOSTI

Po ukončení analýzy rizik byla vedení subjektu předložena zpráva, která obsahuje manažerské shrnutí, popis průběhu projektu a prohlášení o aplikovatelnosti.

7.1 Manažerské shrnutí

Během orientační analýzy rizik, která ve společnosti [redacted] probíhala v období říjen 2020 – duben 2021, byla identifikována informační aktiva firmy, způsoby jejich vytváření, zpracování, ukládání a přenosu. Následně byl vytvořen katalog hrozeb, stanoveny pravděpodobnosti jejich aktivace a dopady, které by tyto nežádoucí události mohly mít. Ve finální fázi pak byl definován způsob výpočtu výsledných rizik a modifikován pro možnosti započtení vlivu ochranných opatření a vyjádření zbytkového rizika. Ustanovený tým řízení bezpečnosti informací se podílel na definici jednotlivých metrik a je podrobně seznámen s metodikou analýzy rizik tak, aby její periodické opakování zvládl bez nutnosti externí spolupráce. Výstupem projektu, kromě zápisů z jednotlivých pracovních schůzek, je: tato zpráva obsahující Prohlášení o aplikovatelnosti a sešit tabulkového procesoru obsahující metodické pomůcky, seznam aktiv a jejich vazeb, katalog hrozeb a výpočty rizik, včetně zahrnutí vlivu ochranných opatření.

7.2 Popis průběhu projektu

Období prováděných činností: říjen 2020 – duben 2021 (viz zápisy)

Projektové etapy:

- identifikace aktiv,
- klasifikace pravděpodobností,
- analýza dopadů,
- základní výpočet rizika,
- výpočet rizika rozšířený o váhová kritéria,
- nastavení výpočtu zbytkového rizika při aplikaci nápravných opatření.

Aktéři: jednatel společnosti, Manažer IB, Architekt IB, správce IS/IT (ext.), konzultant (ext.), hlavní ekonom, vedoucí oddělení (uvedeni v zápisech)

Fáze Identifikace aktiv

Po ustavení týmu bezpečnosti informací v obsazení Manažer IB a Architekt IB (role Auditora IB v současné době není vyžadována, lze později i outsourcovat) byli, během

plánovaných setkání, vytěženi vedoucí jednotlivých oddělení společnosti, seznámeni s rolemi vlastníků primárních informačních aktiv, zodpovědných za stanovení úrovně hodnotících kritérií (důvěrnost, dostupnost, integrita) a vyžadování konkrétních podpůrných aktiv k jejich vytváření, ukládání, zpracování a přenosu.

Fáze Sestavení katalogu hrozeb

Následně byl za asistence externího správce IS/IT sestaven katalog relevantních hrozeb pro podpůrná aktiva a stanoveny pravděpodobnosti jejich působení proti podpůrným aktivům.

Fáze Stanovení dopadů

Na stanovení dopadů pro případy aktivace hrozeb se kromě Týmu IB podílel jednatel firmy a hlavní ekonom.

Výpočet rizika

Ve výstupním sešitu tabulkového procesoru jsou prezentovány tři způsoby výpočtu rizika.

- Základní výpočet P∗D (součin pravděpodobnosti a dopadu s rozsahem 1–16).
- Rozšířený výpočet P*D*W (součin pravděpodobnosti a dopadu s váženým průměrem hodnot Důvěrnost, Dostupnost, Integrita).
- Zahrnutí vlivu ochranných opatření (podíl „Rozšířeného výpočtu“ se součinem vlivu na pravděpodobnost a/nebo dopad).

Návrhy opatření

Během analýzy rizik, zejména ve fázích Sestavení katalogu hrozeb a Stanovení dopadů, byla týmem diskutována možná opatření ke snížení pravděpodobnosti či dopadu, avšak bez komplexního pojetí by se převážně jednalo o nahodilé úkony bez měřitelného vlivu na celkovou bezpečnost informací v organizaci. Jako žádoucí byl vyhodnocen požadavek na šifrování všech médií, která opouštějí areál společnosti a stanovení základních pravidel zabezpečení vlastních zařízení, pokud je zaměstnanci povoleno jejich užití pro pracovní účely.

7.3 Prohlášení o aplikovatelnosti

Tým Informační bezpečnosti ve složení Manažer IB, Architekt IB, správce IS/IT (ext.) na základě provedení orientační analýzy rizik, prohlašuje, že bezpečnost informací ve společnosti [redacted] je možné řídit za předpokladu sestavení Bezpečnostní politiky. Bezpečnostní politika je dokument, kterým společnost prohlašuje, že na řízení bezpečnosti informací má zájem a dále dokument obsahuje jednotlivé kategorie stanovující definice aktiv, identifikace hrozeb, způsoby aplikace ochranných opatření, politiky

třídění dokumentů, politiky hesel, způsoby revizí, požadavky na audit a další souhrnné informace nezbytné k efektivnímu řízení informační bezpečnosti. Obsah každé z uvedených sekcí je pak podrobně rozveden v příslušných přílohách Bezpečnostní politiky, které lze upravovat podle aktuálních potřeb.

8 NÁVRH BEZPEČNOSTNÍ DOKUMENTACE PRO SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ V SUBJEKTU

Pro úspěšné zavedení systému řízení bezpečnosti informací ve vybraném subjektu je třeba vytvořit a odsouhlasit základní bezpečnostní dokumentaci, zejména bezpečnostní politiky, technických opatření a organizačních opatření. Pro jejich návrh byl využit metodický materiál Národního úřadu pro kybernetickou a informační bezpečnost Minimální bezpečnostní standard v 1.0 (podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti) (nukib.cz, 2020b).

8.1 Návrh Bezpečnostní politiky

Identifikační údaje

Název organizace: Společnost [redacted] IČ: [redacted] se sídlem [redacted]
Typ organizace: nezávislý malý podnik

Bezpečnostní politika

Aktuální verze: 0.99a
Počátek platnosti: bude oznámeno
Konec platnosti: do odvolání
Schválil:
Datum schválení:

Prohlášení

Společnost [redacted] IČ: [redacted] se sídlem [redacted] si je vědoma velké důležitosti zabezpečení informací, které vytváří, zpracovává a ukládá na firemních zařízeních a systémech. Zejména osobních informací o klientech, partnerech a subdodavatelích, dále pak informací plynoucích z obchodního styku a dokumentace projektů, které pro své klienty vytváří. Jako svůj základní úkol v této oblasti považuje zajištění důvěrnosti, integrity a dostupnosti takových dat.

Závaznost

Bezpečnostní politika je závazným interním předpisem a její dodržování je vyžadováno interními i externími pracovníky bez vlivu na funkci nebo zařazení. Je vztažena i na subdodavatele, včetně smluvních partnerů pro správu IS/IT.

Rozsah

Rozsah systému řízení bezpečnosti informací je definován na zařízení a informační systémy, které má ve vlastní správě, v zajistitelné míře i na systémy, které nakupuje jako službu. Zároveň se společnost zavazuje revidovat pravidla používání systémů, které nemůže mít pod svojí plnou kontrolou a v případě rozporu s pravidly firemní politiky

je nebude nadále používat.

Seznam dílčích politik

Dílčí politiky slouží k naplňování firemních cílů v oblasti bezpečnosti informací. Jsou definovány v následujících přílohách bezpečnostní politiky:

- Organizační standardy – dokument OrSta.pdf.
- Technické standardy – dokument TeSta.pdf.

8.2 Návrh dokumentu Organizační standardy (OrSta.pdf) – příloha č. 1 Bezpečnostní politiky

Identifikační údaje

Název organizace: Společnost [redacted] IČ: [redacted] se sídlem [redacted]

Organizační standardy

Aktuální verze: 0.99a

Počátek platnosti: bude oznámeno

Konec platnosti: do odvolání

Schválil:

Datum schválení:

Dokument OrSta.pdf je dílčí součástí Bezpečnostní politiky a slouží k definici organizačních pravidel pro splnění stanovených cílů v oblasti ochrany bezpečnosti informací.

Kap.1 – Určení bezpečnostních rolí v organizaci

Roli manažera informační bezpečnosti zastává [redacted], kancelář č. 3 budova A. Součástí jeho povinností je mimo jiné zajištění informovanosti o schválených principech, pravidlech a úkonech požadovaných v rámci zajištění IB, provádění kontroly dodržování stanovených pravidel a řízení komunikace mezi vlastníky aktiv a technickým personálem, který zajišťuje provoz systémů schválených k vytváření, zpracování, distribuci a ukládání informací.

Roli architekta informační bezpečnosti zastává [redacted], kancelář č. 7 budova A. Součástí jeho povinností je mimo jiné zajištění včasnosti provedení analýz nezbytných pro vyřazení stávajících systémů nebo zavedení nových technologií pro vytváření, zpracování, distribuci a ukládání informací. Je také kontaktní osobou pro konzultace požadavků na změny v informačních systémech a řízení uživatelů.

Kap.2 – Řízení aktiv

Organizace definuje informace jako hlavní aktiva firmy, systémy sloužící k jejich vytváření zpracování, ukládání a distribuci jako aktiva podpůrná. Vlastníkem hlavního aktiva je vedoucí oddělení, kde tato data vznikají a je zodpovědný za správnou definici

požadavků na zajištění jejich důvěrnosti, dostupnosti a integrity. Hodnocení je prováděno celočíselným vyjádřením ve škále 1-4 podle následujících metodik:

Metodické vodítko k hodnocení důvěrnosti informace

1 veřejná - kdokoliv i mimo organizaci se může dostat k informaci bez omezení

2 interní - kdokoliv v organizaci má přístup k informaci, partneři a subdodavatelé pouze důvěrnou cestou (email, SMS a pod.)

3 důvěrná - k informacím je omezený přístup, např. v rámci oddělení nebo pracovního týmu

4 vyhrazená - k informacím má přístup jen omezený počet vyjmenovaných jednotlivců

Metodické vodítko k hodnocení dostupnosti informace

1 týden - informace nechybí nebo se dá snadno opatřit jinde

2 den - požadavky lze krátkodobě odložit aniž by to způsobilo potíže

3 4 hodiny - informace musí být zpracována v rámci jedné směny

4 okamžitě - nedostupnost informace může způsobit okamžitou škodu

Metodické vodítko k hodnocení integrity informace

1 lze zjistit pohledem - informaci lze opravit nebo má nízkou důležitost

2 oznámení o změně - stačí vědět, že se informace změnila, případně kdo změnu provedl

3 zamezení změn - informaci je třeba chránit např. zápisem nové verze s číslem nebo datem

4 ověření nezměnitelnosti - proti změnám ověřit kontrolním součtem nebo digitálním podpisem

Kap. 3 – Řízení dodavatelů

Organizace vyžaduje od svých dodavatelů a jejich zaměstnanců odpovídající přístup k ochraně předaných osobních údajů svých zaměstnanců, partnerů a zákazníků, kdy toto předávání je řízeno tzv. potřebou vědět. Tento požadavek musí být nedílnou součástí všech smluv, kde dochází k předání osobních údajů, stejně tak musí být označeny

jako „důvěrné“ všechny další papírové i elektronické dokumenty, které jsou pro zajištění subdodávky nutné a zároveň obsahují citlivé informace. Toto nařízení se vztahuje i na smluvní partnery pro správu IS/IT.

Kap. 4 – Řízení změn

Před provedením změn v infrastruktuře podpůrných aktiv, například zavedení nového systému nebo vyřazení stávající služby, je nutné provést dílčí analýzu rizik se zaměřením na ovlivnění pravděpodobnosti a dopadu hrozeb na aktiva společnosti. Tomu předchází revize katalogu hrozeb příslušným způsobem. Na základě výsledku dílčí analýzy rizik tým kybernetické bezpečnosti rozhodne zda, jakým způsobem a v jakém časovém horizontu je možné změnu provést. Veškeré změny je nutné dokumentovat a následně upravit katalog aktiv společnosti.

Kap. 5 – Řízení kontinuity činností

Pro zajištění obnovení činnosti po nežádoucí události (např. úspěšný kybernetický útok, živelná pohroma, havárie) je třeba vypracovat a udržovat aktuální plány pro udržení kontinuity provozu a plány obnovy informačních systémů a jejich dat. Tyto plány musí obsahovat práva a povinnosti aktérů (administrátoři, správci, vedoucí pracovníci), popis činností a postupy pro řízení průběhu mimořádné události (včetně možných scénářů), minimální standardy možnosti používání podpůrných aktiv, hierarchický postup obnovy systémů, stanovení času pro obnovení a stanovení minimálních objemů dat pro obnovení. Přednost při obnově provozu nebo dat mají podpůrná aktiva s vyšším hodnocením požadavku na dostupnost na základě analýzy rizik.

Kap. 6 – Zavádění ochranných opatření

Nejde-li o situaci, která nesnese odklad, všechna navrhovaná opatření musí projít dílčí analýzou rizik, která stanoví úroveň vlivu opatření na pravděpodobnost či dopad. Po jejím provedení bude vyhodnocen poměr ceny opatření k očekávané úspoře nechtěných výdajů. Pokud podíl ceny opatření k možnému dopadu přesáhne 1/4, je pro jeho schválení nutný informovaný souhlas jednatele společnosti.

Kap. 7 – Řízení lidských zdrojů

Všichni kmenoví zaměstnanci i externí agenturní zaměstnanci musí být seznámeni se zástupci bezpečnostních rolí ve společnosti. Všichni zaměstnanci budou nejpozději při předání přístupových údajů k aktivům společnosti seznámeni se základy kybernetické bezpečnosti a bezpečnostními politikami a následně pravidelně proškolováni nejméně jednou ročně. Společnost je oprávněna přiměřeným způsobem ověřovat dodržování bezpečnostních standardů a jejich porušení sankcionovat. Zaměstnanci zastávající bezpečnostní role mají nárok na absolvování odborných školení, souvisejících s výkonem jejich rolí, nad rámec běžných školení kybernetické bezpečnosti.

Kap. 8 – Nastavení PDCA cyklu

Dodržování cyklu Plan, Do, Check, Act je nezbytné pro udržení odpovídající míry a rozvoje řízení bezpečnosti informací. Tým bezpečnosti informací nejméně jednou ročně provede analýzu rizik informačních aktiv organizace, dále pak pokaždé při požadavku na změnu, zavedení nových nebo vyřazení stávajících hlavních nebo podpůrných aktiv.

Po provedení analýzy rizik navrhne bezpečnostní opatření ke snížení pravděpodobnosti hrozby nebo dopadu na aktiva a posoudí jeho vliv v poměru k ceně a udržitelnosti takového opatření. Při odsouhlasení opatření vypracuje časový plán jeho nasazení a stanoví odpovědnosti a povinnosti dotčených osob. Nejpozději v rámci následující analýzy rizik vhodnými prostředky ověří účinnost nasazeného opatření a vyhodnocení předloží vedení organizace.

Kap. 9 – Audit systému řízení bezpečnosti informací

Audit systému řízení bezpečnosti informací má za cíl nezávislé objektivní posouzení správnosti, přiměřenosti a účinnosti systému a příslušných opatření v rámci organizace. Lze jej provést jako interní (vyžaduje obsazení role autora informační bezpečnosti) nebo externě nezávislým hodnotitelem.

Očekávané přínosy auditu jsou identifikace dosud nepopsaných hrozeb, zjištění nedostatků řízení bezpečnosti informací a prováděných opatření, ověření správnosti dopadových kritérií, prioritizace zjištěných rizik, pohled na systém bez předchozího zatížení tzv. profesní slepotou.

Požadavky na auditora budou při zadání požadavku na audit upřesněny, nejméně však v souladu s Vyhláškou 82/2018 Sb., případně dalších souvisejících předpisů.

8.3 Návrh dokumentu Technické standardy (TeSta.pdf) – příloha č. 2 Bezpečnostní politiky

Identifikační údaje

Název organizace: Společnost [redacted] IČ: [redacted] se sídlem [redacted]

Technické standardy

Aktuální verze: 0.99a

Počátek platnosti: bude oznámeno

Konec platnosti: do odvolání

Schválil:

Datum schválení:

Dokument TeSta.pdf je dílčí součástí Bezpečnostní politiky a slouží k definici technických prostředků, postupů a metod pro splnění stanovených cílů v oblasti ochrany bezpečnosti informací.

Kap. 1 – Fyzická bezpečnost

Fyzická bezpečnost je primárně řešena interními směrnicemi pro ochranu majetku a BOZP. Zjistí-li zaměstnanec jakékoliv podezřelé aktivity ve vztahu k podpůrným aktivům společnosti, neprodleně informuje nadřízeného a osoby zastávající bezpečnostní role. Zvýšenou pozornost je také třeba věnovat ochraně zařízení, se kterými zaměstnanec opouští areál společnosti.

Kap. 2 – Ochrana před škodlivým kódem

Všechna podpůrná aktiva společnosti musí být chráněna proti působení nežádoucího software. Instalace neschválených softwarových aplikací není na firemních zařízeních povolena. Jedná-li se o vlastní zařízení použité pro pracovní účely, je v pravomoci osob zastávajících bezpečnostní role namátková kontrola instalace a funkčnosti příslušné ochrany na zařízení zaměstnance.

Kap. 3 – Řízení přístupů

Cílem řízení přístupů je přidělování přihlašovacích údajů a oprávnění ke službám dané tzv. potřebou vědět. Požadavky na zakládání/blokaci/rušení uživatelských účtů, e-mailových schránek, členství ve skupinách a přístup k počítačové sítí příslušným administrátorům zadává pouze jednatel a Office manager. Jiné požadavky musí být zamítnuty a o takové události jsou informováni zaměstnanci plnící bezpečnostní role.

Přístup k bezdrátové síti je pro kmenové zaměstnance a externí agenturní zaměstnance určen jednoznačným identifikátorem. Pro ostatní je umožněn pouze přístup k síti pro hosty. Přístup k ethernetovému spojení je udělován pouze individuálně, přičemž jakékoliv zjištění pokusu o připojení k této síti (včetně návštěv) musí být neprodleně hlášeno nadřízenému pracovníkovi a zaměstnancům plnícím bezpečnostní role.

Používání vlastních zařízení není zakázáno, za podmínky zabezpečení biometrickým ověřováním a šifrováním všech úložišť daného zařízení.

Požadavky řízení přístupu k podpůrným aktivům na základě hodnocení důvěrnosti hlavních aktiv, ke kterým poskytují přístup:

- Veřejné – aktivum nevyžaduje pro oprávněné uživatele přihlášení.
- Interní – aktivum musí být schopno ověřit oprávněného uživatele (např. jméno+heslo, certifikát, Active Directory), přístup k datům je povolen pouze validním/aktivním účtům.
- Důvěrné – aktivum musí mít možnost ověření oprávněného uživatele a jeho členství v uživatelských skupinách, přístupová oprávněné musí být řízena na základě nejméně skupinových oprávnění.

- Vyhrazené – aktivum musí mít možnost ověření oprávněného uživatele, přístupová oprávnění musí být možné řídit pro jednotlivé uživatele zvlášť.

Kap. 4 – Kryptografické prostředky

Všechna zařízení, která zaměstnanec používá k vytváření, zpracování, distribuci nebo ukládání informací, musí být chráněna heslem, biometrickým ověřením, je-li k dispozici a šifrováním úložišť, dále musí být nastavena funkce automatického uzamčení při nečinnosti delší než 5 minut pro počítač a 1 minutu pro mobilní zařízení.

Všechna přenosná média (např. USB flashdisky, paměťové karty) musí být, dovoluje-li to používané zařízení, šifrovány nejméně na úrovni algoritmů

- AES s minimální délkou klíče 128 bitů.
- Twofish s minimální délkou klíče 128 bitů.
- Serpent s minimální délkou klíče 128 bitů.

Obsah pevných disků notebooků, počítačů a serverů pak musí být šifrován způsobem odpovídajícím použitému operačnímu systému, např. BitLocker (MS Windows), LUKS/dm-crypt (GNU/Linux), APFS (Apple OSX). Klíče pro obnovení ukládá správce IS/IT na bezpečné místo.

Kap. 5 – Politika hesel

Každý uživatel má povinnost používat hesla o minimální délce 12 znaků, pro účty administrátorů a správců minimálně o délce 16 znaků, při použití vždy nejméně jednoho zástupce ze skupin znaků (a-Z), (0-9), (,.-?:_!()[]@#%&*/).

Pro služby, které umožňují vícefaktorovou autorizaci je stanovena povinnost použít nejméně dva faktory.

Ukládání hesel je zakázáno v prosté textové podobě, pro jejich uložení lze použít aplikace správce hesel nebo hardwarové peněženky, pouze po konzultaci se zaměstnanci plnícími bezpečnostní role nebo správcem IS/IT. Pro přístupové údaje do takových aplikací a zařízení je minimální délka hesla 16 znaků, při použití vždy nejméně jednoho zástupce ze skupin znaků (a-Z), (0-9), (,.-?:_!()[]@#%&*/).

Kap. 6 – Zálohování a obnova dat

Pro všechna podpůrná aktiva firmy, vyjma mobilních telefonů a osobních počítačů je stanovena povinnost zálohování v maximálním časovém okně 4 hodiny, při použití inkrementálních záloh pak povinnost plné zálohy nejméně jednou týdně.

Veškeré zálohování probíhá v režimu 3-2-1, tedy vždy tři kopie dat, nejméně na dvou zařízeních, z toho nejméně jedno na geograficky vzdáleném umístění.

Mobilní telefony a data na osobních počítačích jsou uživatelé povinni zálohovat na firemní datové úložiště ve vhodném čase v závislosti na hodnocení dostupnosti stanoveném vlastníky hlavních informačních aktiv, neméně však dvakrát za směnu.

Na základě hodnocení dostupnosti stanoveném vlastníky hlavních informačních aktiv jsou sestaveny plány obnovy dat při výpadku nebo havárii podpůrných aktiv, včetně popisu možných scénářů, odpovědností a součinnostmi v samostatném dokumentu Plán_obnovy.pdf.

Kap. 7 – Likvidace dat

Po ukončení platnosti dat nebo zákonné lhůty hlavních informačních aktiv a při ukončení životního cyklu podpůrných aktiv je provedena příslušná forma likvidace dat v závislosti na hodnocení důvěrnosti aktiva podle následujících parametrů:

1 veřejná - prosté smazání dat, papírové dokumenty do tříděného odpadu

2 interní - přepis dat nulami, pro papírové dokumenty skartace přímým řezem s maximální šířkou 6mm

3 důvěrná - přepis dat náhodným obsahem, pro papírové dokumenty skartace přímým řezem s maximální šířkou 2mm nebo křížovým řezem s maximálním rozměrem 4*80mm

4 vyhrazená - několikanásobný přepis dat náhodným obsahem nebo fyzická likvidace, pro papírové dokumenty skartace pouze křížovým řezem s maximálním rozměrem 2*15mm

ZÁVĚR

Správa informací a jejich ochrana je jeden z důležitých cílů kterékoliv organizace. Rychlost rozvoje informačních a komunikačních technologií současnosti a rostoucí složitost systémů a zařízení užívaných k vytváření, zpracování, uchovávání a distribuci informací a dat tak klade neustále se zvyšující nároky nejen na správce takových technologií, ale také na uživatele a zejména na management firem, jehož povinností je zajistit u zaměstnanců, partnerů i klientů dostatečné povědomí o ochraně citlivých informací a osobních údajů a tuto ochranu také odpovídajícím způsobem zajistit a podporovat.

Diplomová práce v teoretické části zpracovává přehled používaných norem, legislativních požadavků, klíčové terminologie, metod a postupů používaných v oblasti informační a kybernetické bezpečnosti. V praktické části jsou pak použity metody a postupy nejvhodnější pro aplikaci v prostředí vybraného ekonomického subjektu a navrženy nové způsoby výpočtu, které zahrnují hodnoty klíčových atributů informačních aktiv do analýzy rizik a vliv ochranných opatření na zbytkové riziko. Tyto postupy byly následně transformovány do podoby univerzálně použitelného souboru tabulkového procesoru, který vybranému subjektu v budoucnu umožní opakování analýzy rizik v rámci řízení bezpečnosti informací.

Pro zpracování návrhu zavedení systému řízení bezpečnosti ve vybraném subjektu bylo nutné nejprve zjistit současný stav ochrany informací v organizaci, sestavit tým informační bezpečnosti a v součinnosti s ním definovat metodický rámec postupů orientační analýzy rizik, která poskytne rámcový přehled aktiv firmy, seznam hrozeb, které na tyto aktiva mohou cílit, pravděpodobnost nežádoucích událostí a definovat dopad, jaký by takové události měly na chod organizace. Výstupem orientační analýzy rizik ve vybraném subjekt bylo Prohlášení o aplikovatelnosti, které potvrzuje možnost řízení bezpečnosti informací za podmínky existence odpovídající dokumentace.

Pro budoucí zavedení systému řízení bezpečnosti informací byl navržen rámec a základní podoba nezbytné bezpečnostní dokumentace v rozsahu návrhu Bezpečnostní politiky, Organizačních a Technických standardů podle metodického pokynu Minimální bezpečnostní standard v 1.0 (podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti) vydaného Národním úřadem pro kybernetickou a informační bezpečnost. Na základě výstupů praktické části, lze usoudit, že cíle diplomové práce byly úspěšně naplněny.

Přílohou diplomové práce je archiv AR.zip, v němž je vložen demonstrační soubor AR.xlsx, který obsahuje vzorová data a kompletní vzorce použité během analýzy rizik ve vybraném subjektu a je určen jako podpůrný metodický materiál pro aplikaci těchto postupů v jiných organizacích.

SEZNAM POUŽITÉ LITERATURY

API. *Definice malých a středních podniků* [online]. 2018. [cit. 2021-03-06]. Dostupné z: https://www.agentura-api.org/wp-content/uploads/2018/10/definice-malych-a-strednich-podniku-2014.pdf.

Čermák, Miroslav. *Analýza rizik: hodnocení aktiv, hrozeb a zranitelností* [online]. 2012. [cit. 2021-07-10]. Dostupné z: https://www.cleverandsmart.cz/analyza-rizik-hodnoceni-aktiv-hrozeb-a-zranitelnosti/.

Čermák, Miroslav. *Vyhodnocení rizik: kvantifikace opatření* [online]. 2010. [cit. 2021-07-10]. Dostupné z: https://www.cleverandsmart.cz/vyhodnoceni-rizik-kvantifikace-opatreni/.

deming.org. *PDSA Cycle* [online]. 2021. [cit. 2021-07-31]. Dostupné z: https://deming.org/explore/pdsa/.

Doctorow, Cory. *Malý bratr.* Triton, 2011. ISBN 978-80-7387-455-1.

Doucek, Petr, Martin Konečný, Luděk Novák. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Professional Publishing s.r.o., 2019. ISBN 978-80-88260-39-4.

Drastich, Martin. *Systém managementu bezpečnosti informací.* Grada, 2011. ISBN 978-80-247-4251-9.

first.org. *TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0* [online]. 2016. [cit. 2021-07-10]. Dostupné z: https://www.first.org/tlp/docs/tlp-v1.pdf.

Gogela, Robert. *Standardy a definice pojmů bezpečnosti informací* [online]. 2011. [cit. 2021-07-03]. Dostupné z: https://www.cybersecurity.cz/data/Gogela.pdf.

Goll, Jan. *Z norem řízení bezpečnosti informací se postupně vytrácí řada užitečných věcí* [online]. 2019. [cit. 2021-07-03]. Dostupné z: https://m.systemonline.cz/sprava-it/normy-rizeni-bezpecnosti-informaci.htm.

Harkins, Malcolm. *Managing Risks and Information Security: Protect to Enable.* Apress, 2013. ISBN 978-14-30251-13-2.

iDnes.cz. *Zloději dat ze spořitelny hrozí až pět let vězení* [online]. 1999. [cit. 2021-03-06]. Dostupné z: https://www.idnes.cz/zpravy/domaci/zlodeji-dat-ze-sporitelny-hrozi-az-pet-let-vezeni.A_990915_100307_domaci_itu.

iso.cz. *Norma ČSN ISO/IEC 17799:2000* [online]. 2000. [cit. 2021-07-04]. Dostupné z: http://www.iso.cz/iso17799.html.

JIRÁSEK, Petr, Luděk NOVÁK, Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti*. Policejní akademie ČR, 2015. Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf. ISBN 978-80-7251-436-6.

KOLOUCH, Jan et al. *CyberSecurity*. CZ.NIC, 2019. ISBN 978-80-88168-31-7.

KRULIŠ, Jiří. *Jak vítězit nad riziky*. Linde Praha a.s., 2011. ISBN 978-80-7201-835-2.

MARKETBUSSINESNEWS.COM. *KISS principle – definition and meaning* [online]. 2021. [cit. 2021-07-11]. Dostupné z: https://marketbusinessnews.com/financial-glossary/kiss-principle/.

NUKIB.CZ. *Národní strategie kybernetické bezpečnosti pro 2021 – 2025* [online]. 2015. [cit. 2021-03-06]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2015-2020.pdf.

NUKIB.CZ. *Národní strategie kybernetické bezpečnosti pro 2021 – 2025* [online]. 2020a. [cit. 2021-03-06]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf.

NUKIB.CZ. *Minimální bezpečnostní standard v 1.0* [online]. 2020b. [cit. 2021-07-14]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf.

NUKIB.CZ. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019* [online]. 2020c. [cit. 2021-07-30]. Dostupné z: https://nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf.

NUKIB.CZ. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* [online]. 2021. [cit. 2021-07-30]. Dostupné z: https://nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf.

PELTIER, Thomas R. *Facilitated Risk Analysis Process (FRAP)* [online]. CRC Press, 2000. [cit. 2021-06-20]. Dostupné z: http://ittoday.info/AIMS/DSM/85-01-21.pdf.

PELTIER, Thomas R. *Information Security Policies and Procedures*. CRC Press, 2004. ISBN 978-0-8493-1958-7.

POHLOVÁ, Věra. *Deník METRO*. MAFRA, 1999.

POLICIE.CZ. *Výroční zpráva NCOZ 2020* [online]. 2021. [cit. 2021-07-03]. Dostupné z: https://www.policie.cz/soubor/vyrocni-zprava-ncoz-2020.aspx.

Požár, Josef. *Manžerská informatika.* Aleš Čeněk s.r.o., 2010. ISBN 978-80-7380-276-9.

Risk Analysis Consultants, s.r.o. *ISM – ŘÍZENÍ BEZPEČNOSTI INFORMACÍ* [online]. 2021. [cit. 2021-07-03]. Dostupné z: https://www.rac.cz/cs/rizeni-bezpecnosti-informaci/.

Smejkal, Vladimír, Karel Rais. *Řízení rizik ve firmách a jiných organizacích (4. vyd.).* Grada, 2013. ISBN 978-80-247-4644-9.

Smejkal, Vladimír, Tomáš Sokol, Jindřich Kodl. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Aleš Čeněk s.r.o., 2019. ISBN 978-80-7380-765-8.

stakeholdermap.com. *Risk Assessment Matrix* [online]. 2019. [cit. 2021-07-11]. Dostupné z: https://www.stakeholdermap.com/risk/risk-assessment-matrix-4x4.html.

Šulc, Vladimír. *Kybernetická bezpečnost.* Aleš Čeněk s.r.o., 2018. ISBN 978-80-7380-737-5.

Vyhláška č. 82/2018 Sb.: o kybernetické bezpečnosti [online]. 2018. [cit. 2021-06-12]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82.

Zákon č. 110/2019 Sb.: o zpracování osobních údajů [online]. 2019. [cit. 2021-06-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110.

Zákon č. 181/2014 Sb.: o kybernetické bezpečnosti [online]. 2014. [cit. 2021-06-12]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181.

Zákon č. 2/1993 Sb.: Listina základních práv a svobod [online]. 2019. [cit. 2021-06-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-127.

Zákon č. 412/2005 Sb.: o ochraně utajovaných informací a o bezpečnostní způsobilosti [online]. 2005. [cit. 2021-06-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412.

Zákon č. 480/2004 Sb.: o některých službách informační společnosti [online]. 2004. [cit. 2021-07-31]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-480.

Zákon č. 89/2012 Sb.: občanský zákoník [online]. 2012. [cit. 2021-06-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
APFS	Apple File System
AR	Analýza rizik
BOZP	Bezpečnost a ochrana zdraví při práci
BYOD	Bring Your Own Device
COPE	Corporate Owned, Personally Enabled
ČR	Česká republika
ČSN	Československá státní norma
DDoS	Distributed Denial of Services
DoS	Denial of Services
DSM	Data Security Manament
FIRST	Forum of Incident Response and Security Teams
FRAP	Facilitated Risk Analysis Process
GNU	GNU's Not Unix (svobodný operační systém)
HW	Hardware
IB	Informační bezpečnost
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IS	Informační systém
ISMS	Information Security Management System
ISO	Intrenational Organization for Standardization
IT	Informační technologie
KISS	Keep It Simple Stupid
LUKS	Linux Unified Key Setup
NBÚ	Národní bezpečnostní úřad
NCOZ	Národní centrála proti organizovanému zločinu
NDA	Non Disclosure Agreement
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OPDCA	Observe Plan Do Check Act cyklus
PDCA	Plan Do Check Act cyklus
PDSA	Plan Do Check Study Act cyklus
SaaS	Software as a Service
SŘBI	Systém řízení bezpečnosti informací
SW	Software
TLP	Traffic Light Protocol
TR	Technical Report

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

P I. AR.zip

PŘÍLOHA P I. AR.ZIP

CD–R médium v příloze diplomové práce obsahuje text práce ve formátu *PDF* a archiv AR.zip, v němž je vložen demonstrační soubor AR.xlsx, který obsahuje ukázková náhodná data a kompletní sadu vzorců použitých při analýze rizik ve vybraném subjektu.