Bezpečnostní politika informačního systému obchodně výrobního podniku

Bc. Michal Košut

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. Michal Košut**
Osobní číslo:	**L19604**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Studijní obor:	**Rizikové inženýrství**
Forma studia:	**Kombinovaná**
Téma práce:	**Bezpečnostní politika informačního systému obchodně výrobního podniku**

Zásady pro vypracování

1. Zpracujte literární rešerši současného stavu předmětné oblasti.
2. Posuďte rizika související s bezpečnostní politikou informačního systému obchodně výrobního podniku.
3. Navrhněte klasifikaci informací vybraného obchodně výrobního podniku z hlediska důvěrnosti.
4. Zpracujte bezpečnostní politiku informačního systému vybraného obchodně výrobního podniku.

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

Seznam doporučené literatury:

1. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity.* Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.
2. ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.
3. SCHOU, Corea a Seven HERNANDEZ. *Information assurance handbook.* New York: McGraw-Hill Education, 2015. ISBN 978-0-07-182165-0.
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

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- 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;
- 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;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- 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 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 obsahově totožné.

V Uherském Hradišti, dne: 7.5.2021

Jméno a příjmení studenta: Bc. Michal Košut

…….
podpis studenta

ABSTRAKT

Diplomová práce teoreticky popisuje problematiku bezpečnostní politiky v podnicích. Bezpečnostní politika je nedílnou součástí fungování podniku, především z hlediska zabezpečení aktiv, citlivých údajů a informací. Teoretická část práce definuje principy, pojmy, analýzy a zákony související s bezpečnostní politikou. Následně je obsah směřován na bezpečnostní politiku informačního systému, tedy na kyberprostor, který představuje významnou oblast pro podnik, ale bohužel i pro útoky vně podniku. V praktické části je pracováno s konkrétním podnikem, kde je zmíněn nejprve obecný popis, následují definice základních odvětví podniku, definice a popis informačního systému. Následují klíčové kapitoly, ve kterých se kvantifikují hrozby a vyhodnocuje zranitelnost aktiv podniku. Na tato slabá místa je nutné reagovat a hrozby minimalizovat, k tomu jsou použity opatření a způsoby popsané v kapitole „Opatření pro snížení míry rizika“. Celkově pak práci lze použít v praxi na jiný podnik jakožto návod, jak kvantifikovat aktiva, zjistit a určit jejich zranitelnost, hrozby podniku a kritické oblasti zabezpečit lépe použitím vhodných opatření.

Klíčová slova: aktiva, bezpečnost, bezpečnostní politika, data, hrozby, informace, informační systém, uživatel.

ABSTRACT

The diploma thesis theoretically describes the issue of security policy in companies. Security policy is an integral part of the company's operations, especially in terms of securing assets, sensitive data and information. The theoretical part of the thesis defines the principles, concepts, analyzes and laws related to security policy. Subsequently, the content is directed to the security policy of the information system, that is to cyberspace, which is an important area for a company, but unfortunately also for attacks outside a company. The practical part is already dealing with a specific company, where the general description is mentioned first, followed by definitions of the basic branches of the company, definitions and description of the information system. The following are key chapters in which threats are quantified and the vulnerability of the company's assets is evaluated. These weaknesses need to be addressed and threats minimized, using the measures and techniques described in the chapter "Risk mitigation measures". Overall, the work can be used in practice for another company as a guide on how to quantify assets, identify and identify their vulnerabilities and threats to the company and secure critical areas better using appropriate masures.

Keywords: actives, data, information, nformation system, security, security policy, threats.

Rád bych poděkoval Ing. Petrovi Svobodovi, Ph.D., za odborné vedení, poskytnutí cenných rad, informací, pomoci a času v průběhu zpracování bakalářské práce. Dále bych rád poděkoval rodině za podporu během mého celého studia, především manželce a dceři.

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

OBSAH

ÚVOD

Současné pojetí IT technologií a jejich vývoj postupuje mílovými kroky a s tím i zkušenosti a dovednosti profesionálních uživatelů. Součástí všech technologií a systémů jsou informace a data, která je nutné mít na správném místě, ve správný čas, požadované kvalitě. Pokud by tomu tak nebylo mohou být následky pro daný podnik likvidační. Můžeme konstatovat, že téměř každé zabezpečení je možné prolomit, rozklíčovat. Na druhé straně jsou podniky a společnosti, které disponují jak fyzickým majetkem – hmotnými aktivy, tak majetkem nehmotným, ale přesto nesmírně cenným, například výrobní data a postupy, know how, údaje o zaměstnancích a podobně, které musí chránit. V zájmu každého podniku, tedy i našeho, je především řádná péče a bezpečnost informací a dat kolujících v systémech.

Úkolem každého podniku je mít bezpečnostní úroveň na co nejvyšším stupni za co nejnižší náklady a maximálně minimalizovat možnost odcizení, zničení nebo neoprávněného přístupu k datům. Pro diplomovou práci byl vybrán konkrétní podnik, ve které jsem zaměstnán a zabývám se otázkou bezpečnosti a napadnutelných, či nedostatečně zabezpečených míst. Práci je možno s ohledem na výběr správných metod použít i na jiný podnik jako návod, jak postupovat při kvantifikaci podnikových údajů, analýzy hrozeb a nedostatečně zabezpečených oblastí podniku, až po návrh na zlepšení podnikové bezpečnosti. K tomu je možné dospět tak, že budou navržena vylepšení, která rizika minimalizují či úplně eliminují.

Diplomová práce nejprve o tématu pojednává teoreticky, popsány a vysvětleny jsou zejména oblasti bezpečnostní politiky v podniku z obecného hlediska, informační systém včetně nároků na zabezpečení, proces tvorby bezpečnostní politiky informačního systému, kde je vysvětleno, jakým způsobem je možné analyzovat rizika podniku.

Praktická část představuje konkrétní údaje o velikosti podniku. V analýze rizik jsou pomocí řízených pohovorů, Brainstormingu, identifikována a klasifikována aktiva, hrozby, zranitelnost a v matici rizik je vyhodnoceno celkové riziko. Analýza je první potřebný krok k tomu, abychom mohli navrhnout patřičná opatření pro snížení míry rizika, která jsou výstupem práce.

CÍL PRÁCE A POUŽITÉ METODY

Hlavním cílem a myšlenkou diplomové práce bude návrh opatření pro zvýšení úrovně zabezpečení informačního systému vybraného subjektu. Použitím vhodných metod bude kladen zřetel a důraz na nalezení slabých míst a možných hrozeb z hlediska bezpečnosti informačního systému podniku a následně navrhnout opatření pro snížení zjištěných rizikových faktorů. V úvodu praktické části bude podnik představen včetně jeho částí, personálního rozdělení, definice aktiv hmotných a nehmotných. K tomu, abychom byli schopni určit slabá místa podniku, bude třeba nejprve tyto oblasti charakterizovat, použitím vhodných metod bude provedena analýza bezpečnostně rizikových míst a následně návrh řešení, jejichž úkolem a zároveň jedním z dílčích cílů práce, bude minimalizace bezpečnostních rizik.

Dílčí cíle práce

Jednotlivé dílčí cíle bezpečnostní politiky informačního systému obchodně výrobního podniku:

- Zpracování literární rešerše současného stavu předmětné oblasti.
- Posouzení rizik souvisejících s bezpečnostní politikou informačního systému vybraného obchodně výrobního podniku.
- Návrh klasifikace informací vybraného obchodně výrobního podniku z hlediska důvěrnosti.
- Zpracování zjednodušeného návrhu bezpečnostní politiky informačního systému vybraného obchodně výrobního podniku.

V teoretické části budou popsány teoretické možnosti a souvislosti spjaté s bezpečnostní politikou informačního systému podniku. V historii podniku došlo již minimálně dvakrát k bezpečnostnímu incidentu, a to vždy formou Ransomware.

Zvolené metody zpracování

Současná technologicky vyspělá doba nabízí nepřeberné množství bezpečnostních mechanických a elektronických prvků, které slouží k zabezpečení objektů. K odhalení možných hrozeb a rizik byly použity následující metody:

Uvedené metody jsou použity především v praktické části kapitoly č.5 diplomové práce.

- **Syntéza** – metodu syntézy jsem aplikoval při sdružení mnoha informací do jednoho bloku, např. při vyhledání informací v odborné literatuře a následném zpracování do souvislosti. Jde o proces, myšlenkový pochod, kdy se jednotlivé části – myšlenky, skládají do jednoho celku. Opačný postup, tedy z jednoho celku vyvodit menší části používá proces zvaný analýza. (Syntéza, c 2011-2016)
- **Abdukce** – je proces, ve kterém se posuzují předpoklady, které vyústily v pravdivý závěr. Slovo totiž pochází z latinského jazyka a přeložit jej můžeme jako „odvození". Abdukce představuje inverzní vztah k dedukci. Hlavním přínosem abdukce je schopnost generovat nové myšlenky. (Žák Krzyžanková, 2019)
- **Dedukce** – myšlenkový postup, který vyvozuje nové a logicky jisté závěry pomocí již známých a ověřených skutečností, tvrzení a faktů. Hlavním výsledkem dedukce jsou nové závěry a predikce, které jsou jisté, nejen pravděpodobné. Používá se tam, kde je třeba zkoumat různé zákonitosti a ověření obecně známých hypotéz. Dedukce je také nezbytnou součástí oblastí jako logika a matematika, které jsou též nazývány „deduktivní věda". (Dedukce, 2011-2016)
- **Pozorováním** – aplikace metody pozorováním byla provedena napříč všemi informačními systémy a jejich zabezpečením. Jde o souvislou činnost, která nemusí vždy vyžadovat zásah, ale pozvolnou kontrolu, zdali například navržená opatření fungují, nebo je třeba navrhnout kvalitnější řešení. Proces pozorování také slouží k odhalení rizikových oblastí, a to zejména dojde-li během pozorování ke zhoršení situace.
- **Komparace –** v našem případě ji považujeme za metodu, která pracuje s propracovanou teorií. Řídíme se základními pravidly, kterými rozumíme definici objektu komparace, určení cílů komparace a stanovení kritérií pro naši analýzu objektů, které jsme si vybrali, a nakonec vytyčení vztahu samotné komparace vzhledem k časové ose.
- **Analýza rizik** – konkrétně využitím řízeného rozhovoru, Brainstormingu, matice rizik.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ POLITIKA OBECNĚ

Bezpečnostní politika představuje soubor nástrojů, postupů a metod, které mají za cíl ochranu a zabezpečení citlivých údajů společnosti. Každý podnik spravuje vlastní bezpečnostní politiku na nejvyšší možné úrovni. Zejména je nutné, aby bezpečnostní politika chránila prvky, které představují pro podnik hodnotu – hmotná i nehmotná aktiva. Důležitou součástí při tvorbě bezpečnostní politiky podniku je identifikace rizik a jejich ohodnocení – resp. jaký vliv na bezpečnost podniku může mít jejich ohrožení (Schou a Hernandez, 2015).

1.1 Definice základních pojmů bezpečnostní politiky

Aktiva jsou veškeré zpracovávané informace, hardware (dále jen „HW“), software (dále jen „SW“), dokumentace, majetek či činnosti, mající pro podnik určitou hodnotu, která může být snížena nebo znehodnocena působením negativních vlivů. Čas vynaložený na náhradu poškozených či odcizených aktiv může hrát pro podnik významnou existenční roli (Smejkal a Rais, 2013).

Analýza rizik vyjadřuje míru pravděpodobnosti, s jakou bude konkrétní aktivum zničeno, či poškozeno, objeví-li se působení hrozby. Tato hrozba většinou působí na oslabenou stránku aktiva. V zájmu podniku a jeho bezpečnostní politiky je tuto pravděpodobnost minimalizovat, čímž se zvyšuje míra zabezpečení aktiv podniku.

Audit je systematický, nezávislý a dokumentovaný proces pro získání informací, důkazů a jejich objektivní hodnocení s cílem stanovit rozsah, v němž jsou předem stanovena kritéria. Audit by měl představovat skutečnou podobu bezpečnostních opatření v technickém, personálním, fyzickém a organizačním sektoru podniku. Výstupem auditu je zpráva, na základě, které se provede nové zabezpečení aktiv. Cílem auditu je zjištění bezpečnostní úrovně v podniku, zjištění nedostatků a rizikových oblastí, navýšení bezpečnostní úrovně, sestavení účinnějšího řešení bezpečnosti společně s finančními náklady.

Autentizace je proces ověření identity. Tento pojem úzce souvisí s identifikací a autorizací. Proces autentizace je zjednodušeně zadání přihlašovacích údajů do systému, k čemuž potřebujeme vědět heslo. Systém si takto ověří, že je daný uživatel oprávněn k přihlášení. Způsob autentizace může být i jinou formou, například otiskem prstu, oční sítnicí, případně i složitější možností autentizace – kombinace více faktorů např. heslo + otisk prstu (Ondrák, Sedlák a Mazálek, 2013).

Autorizace poskytuje osobě **souhlas** k dané činnosti. Autorizovaná osoba je v podstatě osoba mající právo konkrétní činnost vykonat. Může se jednat o souhlas, oprávnění k přístupu do různých objektů podniku, přístup k informacím, produktům či výrobním postupům podniku.

Bezpečnostní opatření jsou praxe, postupy nebo mechanismy snižující riziko poškození, narušení či odcizení aktiv podniku. Cílem bezpečnostní politiky podniku je mít opatření na co nejvyšší úrovni a minimalizovat tak rizika spojená s bezpečností aktiv.

Bezpečnost informačního systému značí rezistenci Informačního systému (dále jen „IS“ proti narušení důvěrnosti, integrity a dostupnosti informací. Vzhledem k tomu, že se jedná o velmi využívaný sektor v rámci kyberprostoru, setkáváme se s různými prvky ochrany IS, jako např. antivirová ochrana, nutnost zálohování a archivace, kontrola bezpečnosti systému a vypracování krizového plánu (Ondrák, Sedlák a Mazálek, 2013).

Dostupnost znamená poskytnout na požádání autorizované osoby potřebné informace v požadovaném čase. Informace musí být úplné a správné. V případě, že dostupnost není zachována, mohou nastat dopady pro organizaci v pěti úrovních: žádný dopad, zanedbatelný dopad, potíž či peněžní ztráta, vážná potíž či peněžní ztráta, existenční potíž (Ondrák, Sedlák a Mazálek, 2013).

Důvěrnost je vlastnost, že informace není poskytnuta neautorizovaným žadatelům. V opačném případě hovoříme o **porušení důvěrnosti**. Která může nastat v momentě, kdy jsou neautorizované osobě poskytnuty důvěrné informace (Ondrák, Sedlák a Mazálek, 2013).

Integrita dat představuje správnost a úplnost informací. Ke změně či ztrátě některých informací nemusí dojít cíleně, nýbrž náhodou a nechtěně. Tato změna nebo ztráta může mít zásadní dopad na organizaci v závislosti na rychlost odhalení. Společným jmenovatelem pojmů integrita, dostupnost a důvěrnost je pojem **bezpečnost dat** (Ondrák, Sedlák a Mazálek, 2013).

Informace je definovaná jako sdělení, které snižuje míru neurčitosti na straně adresáta. V podniku se nejčastěji setkáváme se dvěma typy informací – elektronická nebo tištěná. Tato data by měla být snadno čitelná, pochopitelná a využitelná subjektem, kterému jsou určena. Podniky vyžadují kvalitní, pravdivé a aktuální informace. Informace v organizaci jsou chráněny a uchovávány v informačním systému (Ondrák, Sedlák a Mazálek, 2013). Za informaci je považován i jazykový projev, ve kterém jsou konstatována fakta (Požár, 2010).

Informační Systém je funkční celek technických prostředků, programů a lidí zabezpečující cílevědomé a systematické shromažďování, zpracování, přenos, uchování a zpřístupnění dat. Informační systém se používá na všech úrovních podniku.

Přerušení můžeme charakterizovat jako výpadek dostupnosti informací. Přerušení může mít významný vliv na fungování podniku a na jeho ochranu. V zájmu každého podniku je minimalizovat dobu, či úplně eliminovat možnost přerušení.

Hrozba je pojem, který bývá často používám v souvislosti s pojmem "riziko". Jde o negativní situaci, aktivitu, stav, kdy cílem uměle vyvolaným, případně náhodným, je poškození, zničení nebo ztráta aktiva. Může se jednat například o přírodní vlivy, společenské jevy, ekonomickou situaci, případně záměrné chování jednotlivce (Hrozba-Threat, © 2011-2016).

Riziko je v návaznosti na předchozí pojem charakterizováno jako jev, událost, proces, nebo činnost, která podléhá určité míře pravděpodobnosti, že nastane. Riziko představuje dva základní parametry. **Míru neurčitosti**, což značí pravděpodobnost, že se daná situace vyskytne, kterou se snažíme minimalizovat a velikost nebezpečí, tedy jak nebezpečná situace podniku hrozí v případě, že hrozba nastane (Koudelka a Vrána, 2006).

Uživatel je jakýkoliv zaměstnanec nebo partner společnosti, který má oprávnění k přístupu k jakémukoli zdroji elektronických informací společnosti.

Citlivé informace jsou veškeré informace podniku, které nejsou veřejně známé a obsahují hmotné a nehmotné informace ve všech formách, jako jsou informace, které jsou pozorovány nebo ústně doručeny, v elektronické podobě, písemně nebo v jiné hmotné formě. Citlivé informace mohou mimo jiné zahrnovat zdrojový kód, návrhy a plány produktů, výsledky beta a srovnávacích testů, přihlášky patentů, výrobní metody, plány produktů, seznamy a informace o zákaznících, seznamy a informace o vyhlídkách, propagační plány, informace o konkurenci, jména, platy, dovednosti, pozice pracovníků, náklady na produkty a ceny a informace o zaměstnancích a seznamy včetně organizačních schémat.

Informační aktivum mohou být informace nebo data v jakékoli formě, včetně fyzické, elektronické, optické a magnetické, vytvořená nebo použitá při podnikání. Informační aktiva jsou důležitou součástí pro sestavování finančních plánů a efektivní řízení nákladů na ochranu aktiv.

Zranitelnost je nedostatek, slabina analyzovaného bezpečnostního systému, která může být zneužita hrozbou k poškození či zničení hodnoty aktiv nebo uplatnění nežádoucího

vlivu. Zranitelnost se vyskytuje tam, kde dochází k interakci mezi hrozbou a aktivem (Mlýnek, c2007).

Útok je cílený jev, jehož hlavním cílem je poškození, zničení, nebo krádež. V souvislosti s podnikem a informačním prostředím hovoříme o kyberútoku. Ty mají na svědomí tzv. hackeři, kteří jsou díky svým vysoce nadprůměrným dovednostem schopni najít slabinu a do systému tak proniknout.

Nebezpečí lze definovat jako pravděpodobnou možnost, že v budoucnosti nastane situace, při které podniku vzniknou škody, neštěstí nebo jiné nežádoucí a ztrátové jevy, jež mohou mít finanční, materiálové, nebo například věrohodné následky. Dále se pojem nebezpečí může používat pro současný stav, nebo podmínky v danou chvíli, ve které se některé oblasti podniku nacházejí – tato situace musí být urgentně řešena a zjednána náprava (Definice nebezpečí, 2020).

Řízení aktiv je soustavná činnost, kdy hlavním cílem je volba takových aktiv, kdy se při minimálním riziku snažíme maximalizovat zisk. Např. servisní služební vůz je třeba využívat tak, aby podniku generoval co možná nejvyšší přidanou hodnotu.

Odpovědnost osoby v podniku může být chápana jako stav, kdy osoba, zaměstnanec, ručí za určitý výsledek nebo stav. Například odpovědnost svářeče je, že konkrétní výrobek a jeho sváry budou kvalitní a v souladu s výrobními požadavky. Odpovědnost top managementu je úspěšné řízení podniku. Odpovědnost může být *retrospektivní*, tedy zpětná (např. odpovědnost právní), nebo prospektivní, což poukazuje na budoucnost (např. počet výrobků bude vyroben).

Role představuje souhrn činností politiky prováděný zaměstnancem podniku plynoucích z bezpečnostní politiky. Role je definice rozsahu činností, které má uživatel povoleny v rámci informačního systému. Například role uživatel má omezenější práva a možnosti než role administrátor, který má všechna práva.

Identifikace spočívá v prokázání totožnosti a jiných unikátních údajů o osobě, které jsou následně porovnány a na základě výsledku je pak osoba oprávněna k dalším úkonům (Gála, Pour a Šedivá, 2015).

Incident značí událost, která vede k ohrožení bezpečnosti. Jde o událost, kdy je narušena bezpečnost informací v informačních systémech, nebo narušení bezpečnosti služeb. Za incident můžeme také považovat pokus o narušení bezpečnostní politiky, případně o pokus překonání bezpečnostních opatření (Gála, Pour a Šedivá, 2015).

1.2 Princip bezpečnostní politiky

Bezpečnostní politiku si můžeme chápat jako dokument, který však není jasně definovaný ani specifikovaný, co se obsahu a rozsahu týče. Dokument může být několikastránkový, ale i značně obsáhlý. (Schou a Hernandez, 2015) Bezpečnostní politika podniku rozlišuje zejména tři hlavní sub-oblasti:

- Bezpečnost informační.
- Bezpečnost technická.
- Bezpečnost personální a osobní (Schou a Hernandez, 2015).

Každá z výše uvedených oblastí by měla být zabezpečena nejlépe, a to tak, aby byla minimalizována šance na napadení z vnějšího či vnitřního prostoru.

1.2.1 Bezpečnost informační

Cílem informační bezpečnosti je především identifikace, pochopení a kontrola hrozeb za pomoci použití podnikových informací a informačních systémů. Informační bezpečnost se zabývá životním cyklem informací zejména v oblastech důvěryhodnosti, integrity, dostupnosti, nepopíratelnosti, ověřování (Schou a Hernandez, 2015).

Následující dva elementy jsou zásadní z hlediska informační bezpečnosti. Informační bezpečnost zahrnuje všechny informace v organizaci, které mohou být zpracovány, ukládány, vysílány, případně šířeny za použití médií. Informační bezpečnost, ochrana informací a ochrana v kyberprostoru jsou podmnožinami bezpečnostní politiky. (Schou a Hernandez, 2015)

1.2.2 Ochrana informací

Kapitolu ochrana informací lze nejlépe pozorovat jako podskupinu bezpečnostní politiky. Často bývá definována v podmínkách o ochraně důvěrnosti a integrity informací prostřednictvím prostředků, jako jsou politika, standardy, fyzická kontrola, technická kontrola, monitoring, klasifikace a kategorizace informací.

Stejně jako informační bezpečnost, tak i ochrana informací zahrnuje všechny informace, které mohou být zpracovány, uchovány, vysílány, nebo šířeny prostřednictvím médií. Tím pádem listinné informace, na externím zařízení, v paměti zaměstnance, nebo na internetovém úložišti jsou považovány jako „v rozsahu“ (Schou a Hernandez, 2015).

1.2.3 Kyberochrana

Nejprve je vhodné vysvětlit, co si pod pojmem kyberprostor můžeme představit. Zkráceně lze kyberprostor popsat jako virtuální počítačový svět, který vnímáme v celosvětovém, globálním měřítku. Kyberprostor je tvořen velkým množstvím počítačových sítí, které komunikují pomocí protokolu TCP/IP a díky kterému je možné si vyměňovat data.

Vzhledem k tomu, že každý systém je obtížněji či snáze napadnutelný, jedná se o velmi citlivou část ochrany podniku. Pojem kyberprostor a kyberochrana je novým pojmem, kterému předcházel pojem „počítačová bezpečnost“. Známějšími pojmy jsou hackování (hacker) a crackování. Oba tyto pojmy souvisí s bezpečností v kyberprostoru.

Velmi nadaní počítačoví experti (hackeři) dokážou odhalit chyby různých systémů, webů, platebních bran atd. Za pomocí svých excelentních dovedností pak páchají trestné činy. Hackeři mají často lepší schopnosti a znalosti, než tvůrci a programátoři zmíněných systémů, webu, platebních bran atd. Kyberochrana se primárně zaměřuje na ochranu počítačových sítí a elektronických informačních systémů.

2 INFORMAČNÍ SYSTÉM

Umožňuje časovou a prostorovou komunikaci a transformaci informací pro řádnější využití, nežli byly v původním stavu. Současně můžeme říct, že dochází mezi lidmi, technologickými prostředky a informačními zdroji k účelovému uspořádání vztahů a informačních kanálů. Informační systém viz. obr. 1, se může skládat ze spousty podsystémů, které jsou vzájemně propojeny a dochází zde k získávání, zpracování, distribuci, změně, ukládání a přenosu informací mezi jednotlivými účastníky. Mezi základní funkce informačního systému řadíme:

- Pořizování.
- Sběr.
- Přenos.
- Zpracování.
- Distribuce.
- Prezentace.
- Ochrana (Požár, 2010).

Z hlediska provozu informačního systému (dále jen "IS") je nezanedbatelnou částí příprava a školení pracovníků k získání potřebných návyků. V tomto významu je možné uživatele přistupující do IS rozdělit na:

- Specialisty IS.
  - Analytik.
  - Programátor.
  - Správce sítě.
  - Správce databázové základny.
  - Technik pro údržbu hardware (dále jen "HW").
- Uživatele IS.
  - Neuživatelé.
  - Nepřímí uživatelé.
  - Aktivní uživatelé (Požár, 2010).

2.1 Informační technologie

Informační technologie dělíme na technické prostředky a programové vybavení. Pod pojmem technické prostředky si může vybavit veškerý hardware, jako jsou např. osobní

počítače, telekomunikační zařízení. Programové vybavení znamená všechen využívaný software. Obě kategorie lze dále členit na menší celky.

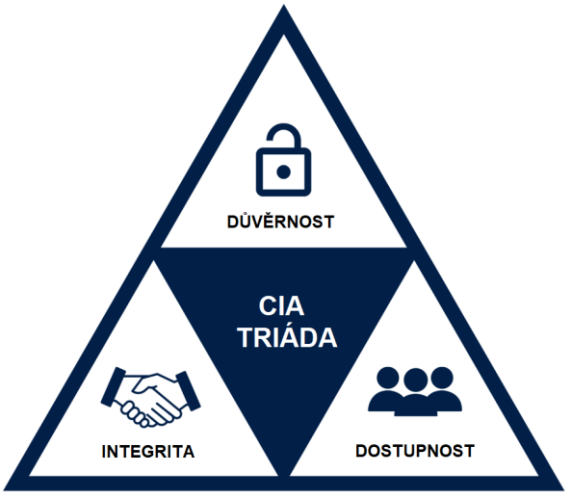
Obrázek 1 – Informační systém (Informační systém jako ideální nástroj pro řízení zakázek stavebních firem, © 2001-2020)

Základní software je soubor programů s různou specializací jako jsou např. operační systémy osobních počítačů (dále jen "PC") a serverů, podpůrné programy a speciální služební programy. Mezi základní operační systémy patří MS Windows. (Gála, Pour a Toman, 2006) Operační systémy můžeme rozdělit:

- Pracovní stanice.
  - Windows.
  - Linux.
  - Mac OS.
- Serverové.
  - Windows server 2012.
  - Mac OS server.
  - Red Hat Linux.
- Pro mobilní zařízení.
  - IOS.
  - Symbian.
  - Android.
- Speciální (Gála, Pour a Toman, 2006).

2.2 Triáda CIA

Cílem informační bezpečnosti podniku je udržovat níže vyobrazenou triádu, která sestává ze tří hlavních částí. Důvěrnosti, integrity a dostupnosti, viz. obr. 2.



Obrázek 2 – Triáda CIA (Brathwaite, 2021 - upraveno)

Důvěrnost znamená skutečnost, že k informacím musí mít přístup pouze uživatelé s příslušným oprávněním. Dojde-li k tomu, že společnost data poskytne neoprávněným osobám, hovoříme o narušení důvěrnosti informací. Abychom si důvěrnost zachovali, je třeba dodržet některé z následujících kroků: šifrování, silná hesla, více faktorová ověření osoby, správa identity a přístupu, správné technické kontroly, fyzické zámky na dveřích – trezory a podobné typy zabezpečení informací (Confidentiality, Integrity, & Availability, ©2020, Tuma, 2008).

Integrita představuje ochranu dat před možnou změnou či narušením, neoprávněnými osobami. Pokud je integrita dodržena, hovoříme o důvěryhodnosti a přesnosti informací. Pokud ale dojde ke změně či poškození informací osobou uvnitř, nebo vně podniku, hovoříme o narušení integrity informací. V organizaci musí existovat prostředky a nástroje, díky kterým je dohledatelné, zda byly informace upraveny a případně kým, kterým účtem. K zajištění používáme nástroje: hashování (změna podoby textu do speciální formy), zálohování, nebo řízení přístupu uživatelů (What is the CIA Triad?, 1999 - 2020).

Dostupnost informací je nutná záležitost v době, kdy oprávnění uživatelé potřebují mít danou informaci k dispozici. Příkladem může být televizní vysílací společnost, která požaduje od svých partnerských společností přístup více než 99,5 %, čímž garantují, že my jako diváci budeme mít přístup k těmto službám (filmům a kanálům) s téměř maximální

jistotou a bez problémů (Kolouch a Bašta, 2019, Brathwaite, 2021). Dostupnost je nejlépe zajištěna důslednou údržbou veškerého hardware, okamžitým provedením oprav zařízení v případě potřeby a udržováním správně fungujícího prostředí operačního systémů, kde je cílem minimalizovat softwarové konflikty. Důležité je udržovat informace o všech nezbytných upgradech systému aktuální (What is the CIA Triad, 1999–2020).

2.3 Bezpečnostní hrozby

V systému se mohou nacházet slabá místa, která jsou hrozbou pro IS a příčinou vzniku incidentu. Značná majorita, tedy více než padesát procent hrozeb, patří do kategorie neúmyslných. Do hranice základních hrozeb náleží náhodné, neoprávněné nebo úmyslné, kterými jsou např. prozrazení tajných informací, upravení nebo zničení informací či bránění dostupnosti IS autorizovaným osobám. K charakteristickým útokům patří odposlech, vyhledávání hesel či modifikace dat. Z těchto důvodů je nutné přijmout bezpečnostní opatření, kterým je věnována následující kapitola (Gála, Pour a Šedivá, 2015).

Každý informační systém je vystaven potencionálním hrozbám, kterým musí odolávat. Hrozby můžeme klasifikovat následujícím způsobem:

- Přírodní.
- Technické.
- Technologické.
- Lidské.
    - Úmyslné.
        - Vnitřní.
        - Vnější.
    - Neúmyslné.

Většina hrozeb je situována na třídy neúmyslných, ale mezi základní hrozby patří taktéž nekompetentní, náhodné či úmyslné:

- Prozrazení.
- Upravení.
- Zničení.
- Bránění (Smejkal, Sokol, Kodl, 2019).

Mezi nejčastější útoky můžeme zařadit:

- Odposlech.
- Modifikaci dat.
- Odmítnutí.
- Popření (Smejkal, Sokol, Kodl, 2019).

Agresoři útočící na IS při svých pokusech o prolomení obrany IS používají různých speciálních programových kódů, jejichž posláním je poškodit zařízení, data, programy, zdroje a zcizit informace a data. Níže je uveden výčet škodlivých zdrojů:

- Viry.
- Trojské koně.
- Červi (Smejkal, Sokol, Kodl, 2019).

Výše uvedené škodlivé zdroje mohou způsobit nežádoucí jevy:

- Poplašné zprávy.
- Spyware.
- A další (Smejkal, Sokol, Kodl, 2019).

2.4 Bezpečnostní protiopatření

Uvědomíme-li si, že neexistuje universální celistvé řešení opatření vůči útokům a hrozbám, musí být vždy konkrétní řešení orientováno vůči konkrétnímu riziku. Protiopatření můžeme rozdělit na:

- Preventivní – jejím smyslem je minimalizovat příčiny vzniku incidentů.
- Dynamická – smyslem je minimalizovat dopady případných incidentů.
- Následná – minimalizace případných dopadů proběhlých incidentů (Gála, Pour a Šedivá, 2015).

Při výběru opatření je nutné posuzovat jeho účinnost, náklady a celkový přínos neboli jakým způsobem protiopatření sníží případné hrozby nebo rizika. Náklady, které budou vynaloženy na redukci rizika musí být úměrné hodnotě chráněných aktiv (Čermák, 2009, s. 113.).

- Odstrašení útoku.
- Zadržení útoku.
- Detekci útoku.
- Reakci na útok.
- Obnově po útoku (Čermák, 2009, s. 111).

2.5 Legislativní dokumenty a normy

Bezpečnostní politika obecně musí dodržovat zásady a normy stanovené v zákonech a ustanoveních. V následující kapitole je přehled několika základních norem a směrnic, které definují požadavky a nařízení, jež musí být dodrženy.

2.5.1 Zákony

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti (Maisner, 2015). V zákoně č. 181 z roku 2014 sbírky jsou vymezena práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetiky. Setkáváme se s pojmy kyberprostor – digitální prostředí, kde vznikají, mění se a předávají se informace, kde hlavním nástrojem jsou sítě a služby elektronických komunikací. Zákon zabezpečuje informace z hlediska důvěrnosti, integrity a dostupnosti informací (Zákon 181/2014 Sb., 2014).

Zákon č. 110/2019 Sb., o zpracování osobních údajů. Původní zákon 101/2000 Sb., vešel v platnost 4. dubna roku 2000. Zákon se vztahuje na osobní údaje, které jsou dále používány státními orgány, orgány územní samosprávy, jinými orgány veřejné moci, fyzickými a právnickými osobami. Důležitým faktorem je, že používání osobních údajů musí podléhat striktnímu dodržování a musí být s údaji nakládáno pouze pro konkrétní potřeby, nikoliv pro osobní potřebu (Zákon o ochraně osobních údajů 101/2000 Sb., 2014).

Zákon č. 480/2004 Sb., o některých službách informační společnosti. Zákon platný od 29. července roku 2004. Zjednodušeně lze zákon definovat jako odpovědnost, práva a povinnosti osob, které poskytují služby informační společnosti a šíří obchodní sdělení, kdy poskytovatelem takové služby je fyzická nebo právnická osoba, která službu informační společnosti využívá zejména za účelem vyhledávání či zpřístupňování informací. Obchodním sdělením rozumíme například reklamu, nabídku k návštěvě webových stránek, přímou či nepřímou podporu zboží a služeb nebo zlepšení image společnosti (480/2004 Sb. Zákon o některých službách informační společnosti, 2021).

Zákon č.89/2012., občanský zákoník. V Občanském zákoníku se setkáváme s definicí odpovědnosti a práva a povinnosti osob, které poskytují služby informační společnosti a šíří obchodní sdělení. Účelem tohoto zákona se rozumí jakákoliv informační služba poskytovaná elektronickými prostředky a textová, obrazová, či hlasová zpráva. Poskytovatelem služby je

každá fyzická nebo právnická osoba, a to za účelem vyhledávání či zpřístupňování informací (480/2004 Sb. Zákon o některých službách informační společnosti, 2021).

Zákon č. 40/2009 Sb., trestní zákoník. V trestním zákoníku nalezneme tři části – část obecnou, zvláštní a přechodná a závěrečná ustanovení. V jeho obsahu, v části obecné nalezneme ustanovení trestných činů a vymezení trestní odpovědnosti, jaké tresty jsou za dané trestné činy ukládány, jaká známe ochranná opatření a základní používané pojmy. Dále v zákoně nalezneme samotnou kvalifikaci trestných činů (40/2009 Sb. Trestní zákoník, 2021).

Zákon č. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve kterém se zejména pojednává o zásadách, které musí být dodržovány při stanovování informací klasifikovaných jako utajované. Dále podmínky a přístup k nim a ostatní nároky na ochranu. Zákon nadále upravuje zásady ke stanovení citlivých činností a stanovuje podmínky, které jsou nutné k jejich výkonu, s čímž je spojený výkon státní správy (Zákon č. 412/2005 Sb., 2021).

Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti. Jedná se o vyhlášku z roku 2018, která upravuje obsah a strukturu bezpečnostní dokumentace, dále obsah a rozsah bezpečnostních opatření, rozeznává typy, kategorie a hodnocení bezpečnostních incidentů v oblasti kybernetiky, dále upravuje vzor oznámení kontaktních údajů a jejich formu. Poslední položkou je způsob, jak likvidovat data, provozní údaje, informace a kopie (82/2018 Sb. Vyhláška o bezpečnostních opatřeních, 2021).

2.5.2 Normy

ČSN ISO/IEC 27000:2014 „Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník“. Jedná se o normu v české verzi, která je převzata z verze evropské normy EN ISO/IEC 27000:2017. Tato mezinárodní norma poskytuje přehled systémů řízení bezpečnosti informací a termíny a definice běžně používané v rodině standardů Information Security Management System – Systém managementu bezpečnosti informací (dále jen „ISMS.“) Tato mezinárodní norma je použitelné pro všechny typy a velikosti organizací např. komerční podniky, vládní agentury, neziskové organizace (EN ISO/IEC 27000:2017, 2013).

ČSN ISO/IEC 27001:2014 „Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky“ norma specifikuje požadavky na

ustanovení, implementování, udržování a neustálé zlepšování ISMS. Součástí normy jsou i požadavky na posouzení a ošetření rizik bezpečnosti informací, které jsou přizpůsobené potřebám organizace. Norma prosazuje přijetí procesního přístupu k řešení ISMS a zavádí Demingův model PDCA. Neméně podstatná je příloha „A“ této normy. Příloha obsahuje soupis cílů a jednotlivých opatření, které jsou propojeny s opatřeními v normě ISO/IEC 27002:2014. Požadavky této normy je možné aplikovat ve všech organizacích bez ohledu na jejich typ, velikost a povahu (ČSN ISO/IEC 27001, © 2006).

ČSN ISO/IEC 27002:2014 „Soubor postupů pro opatření bezpečnosti informací“ – norma je určena pro organizace jako doporučení pro výběr opatření v rámci ISMS. Jde o soubor postupů pro řízení bezpečnosti informací. Předchůdcem této normy byla ISO/IEC 17799:2005. Součástí je detailní rozbor vhodných opatření. Tato norma je také určena pro použití při vyvíjení směrnic pro řízení bezpečnosti informací se zaměřením na průmysl. Norma přihlíží na konkrétní prostředí rizik pro bezpečnost informací. Bezpečnostní opatření podporující dosahování cílů, kdy odpovědnost za ně je možné přiřadit odpovědným osobám dle jejich funkcí (Drastich, 2011).

ČSN ISO/IEC 27003:2011 „Směrnice pro implementaci systému řízení bezpečnosti informací“ – norma zprostředkovává doporučení pro ustanovení a implementaci ISMS v souladu s požadavky normy ISO/IEC 27000. Normu je možné použít pro všechny typy organizací. Obsahem normy je vysvětlení návrhu a implementace ISMS za pomocí popisu zahájení, definování a plánování projektu implementace ISMS. Norma obsahuje popis implementace ISMS v pěti krocích:

- Souhlas vedení organizace se zahájením ISMS.
- Definice rozsahu, hranic a politik ISMS.
- Analýza požadavků bezpečnosti informací.
- Provedení hodnocení rizik a plánování zvládání rizik.
- Návrh ISMS (Drastich, 2011).

3 PROCES TVORBY BEZPEČNOSTNÍ POLITIKY INFORMAČNÍHO SYSTÉMU

Bezpečnostní politika informačního systému představuje dokument, ve kterém je jasně definováno, jak má být informační systém provozován, aby se minimalizovala či eliminovala rizika spojená s citlivými údaji podniku. Bezpečnostní politika informačního systému musí splňovat několik základních kritérií:

- Nesmí obsahovat konkrétní typy informací (typy HW / SW, složky, údaje o parametrech, atd).
- Dokument plní normy a požadavky legislativy, zejména v oblastech o ochraně osobních údajů.
- Měl by být jasný, stručný a k tomu úměrně dlouhý.
- Dokument bezpečnostní politiky informačního systému musí být schválen kompetentní osobou organizace.

Dokument by měl být sestaven v následujícím pořadí:

- Úvodní ustanovení.
- Personální bezpečnost.
- Počítačová bezpečnost.
- Kryptografická ochrana.
- Fyzická bezpečnost.
- Administrativní bezpečnost.
- Řízení a plánování kontinuity.
- Další bezpečnostní dokumentace (Zásady tvorby bezpečnostní dokumentace informačních systémů určených k nakládání s utajovanými informacemi, 2017).

3.1 Soupis aktiv informačního systému

K tomu, abychom mohli aktiva chránit, musíme je nejprve identifikovat a analyzovat. Jeden člověk nedokáže určit veškerá aktiva systému, proto je nutné, aby se na identifikaci podílelo několik kompetentních osob a každý zveřejnil výčet aktiv dle svého sektoru. Důležité je při identifikaci aktiv, aby nebylo žádné aktivum opomenuto, což by následně mělo za následek, že není chráněno.

Za aktivum lze považovat vše, co má pro jeho vlastníka nějakou hodnotu. Kybernetická bezpečnost rozděluje aktiva na:

- Informační.
- Technická.
- Podpůrná.

3.1.1 Informační aktiva

Informační aktivum představuje ucelené svazky informací, které jsou pro podnik hodnotné. Stejně jako hmotné aktivum (výrobní stroj, budova, služební automobil), tak i informační aktivum má pro podnik významnou hodnotu. Jedná se o aktiva, na která si nemůžeme sáhnout, jsou to například databáze dodavatelů, výrobní dokumentace, manuály a návody, finanční a obchodní plány, zálohování potřebných dat, informace o zaměstnancích, a podobně. Níže je uvedeno několik příkladných definic, které určují informační aktiva:

- Stejně jako hmotné aktivum má informační aktivum pro podnik významnou hodnotu.
- Informační aktivum je samostatná součást figurující v aktivech podniku.
- Hodnota aktiva je pro podnik známá a dokážeme ji určit.
- Ztráta, poškození či odcizení informačního aktiva je vyčíslitelná.
- Informační aktivum představuje hodnotu podniku, postavení na trhu, konkurenceschopnost.
- Informační aktivum bývá zpravidla tajné, chráněné a přístupné pouze oprávněným osobám (Informační aktiva, © 2011-2016).

3.1.2 Technická aktiva

Můžeme nazvat vše, co je dotčeno technickým vybavením, tedy hardware, programové vybavení, komunikační systém a stavby, ve kterých je zařízení instalováno. Jde tedy například o IT vybavení podniku, které často spravují externí společnosti. Mnohdy bývá v režii jiné společnosti, která se stará o dodání, servis, opravy a výměnu staršího vybavení za nové. Mezi technická aktiva řadíme také softwarové vybavení informačního systému (Kybernetická bezpečnost, 2020).

3.1.3 Podpůrná aktiva

Podpůrná aktiva jsou nadřazenou skupinou technických aktiv, do které mj. spadají pracovníci podniku a pracovníci třetích stran, kteří se spolupodílí na provozu a správě informačního a komunikačního systému.

Cílem podpůrných aktiv je zajišťovat fungování, a především dostupnost aktiv primárních. Každé primární aktivum je závislé na podpůrném aktivu (Metodika pro identifikaci a hodnocení aktiv a rizik, 2020).

3.2 Klasifikace informací

Data a informace, které se v podniku vyskytují a užívají mají pro tento podnik různou důležitost i význam. Informace mohou mít následují formu:

- Elektronickou.
- Tištěnou.
- Faxovou.
- Ústní.

Pro přiměřenou ochranu informací je důležité zavedení klasifikace informací. Data a informace podniku je potřebné chránit z hlediska:

- Důvěrnosti.
- Integrity.
- Dostupnosti.

Aby bylo možné zabezpečit data komplexně, je nevyhnutelná jednotná klasifikace informací. Prvotní je klasifikace z hlediska důvěrnosti, protože obsah sdělení informace je jejím nejdůležitějším znakem. Z hlediska integrity a dostupnosti je to opačně a lze říci, že tato klasifikace má spíše technický význam (Mlýnek, c2007). Můžeme říct, že v komerční sféře je zažita následující klasifikace informací:

- Chráněné – neoprávněné nakládání s informacemi by mohlo zapříčinit značné poškození či zničení organizace (např. únik uživatelských hesel, dokumentace, aj.).

  Interní neoprávněné nakládání s informacemi by mohlo přivodit postižení organizace.

- Citlivé – neoprávněné nakládání s informacemi by mohlo mít negativní dopad na podnik.
  Veřejné – neoprávněné nakládání s informacemi nezpůsobí žádnou škodu a nebude mít žádný dopad na podnik.

Mohou existovat i jiné klasifikace, které jsou v rámci společnosti přijaty na základě uvážení pověřených osob nebo zákonných předpisů a norem.

Jsou-li klasifikace dodržovány a respektovány, je předpoklad, že výrazným způsobem sníží dopady případných kybernetických útoků. Pro klasifikaci informací lze také použít Traffic light protocol (Dále jen „TLP“) který je uveden níže (Klasifikace informací v korporátním prostředí, 2018).

Traffic Light Protocol

Na základě potřeby sdílet informace a data citlivé povahy vznikl počátkem roku 2000 protokol TLP, jehož úkolem je zrychlit výměnu informací mezi zúčastněnými stranami a současně vymezit pravidla, jak s předávanými informacemi zacházet. Předávající vždy každou informaci barevně označí a ta příjemci stanoví, jakým způsobem je možné s informací zacházet (Kolouch a Bašta, 2019).

3.3 Analýza rizik

Analýza rizik představuje nutnou součást informačního systému, jejímž úkolem je zvládnutí různých rizikových situací, zejména takových, které by mohly ohrozit lidské zdraví a životní prostředí. Analýza rizik je široký pojem, který zahrnuje a kombinuje technické, přírodovědecké a humanitní oblasti. Hodnocení rizik může být využito i v procesech rozhodování, v tento moment se dále připojují aspekty z oblasti ekonomiky, psychologie, ale i politiky. Hodnocení rizik nabízí poznatky, které lze využít jak ve fázi předcházení nežádoucích událostí, při přípravě na jejich odstranění (pokud by nastala), tak i při samotném zásahu. Veškeré poznatky, které o riziku získáme, se dále používají během tvorby bezpečnostní politiky, stanovování priorit činností, posouzení možností, vymezení zdrojů a podobně. To se děje na úrovních podnikových, regionálních i národních. Díky tomu, že poznáváme několik způsobů a postupů, jak můžeme rizika hodnotit, je velmi důležité zvolit správnou metodu, vhodný přístup vzhledem k dané situaci, cíli a kontextu, v němž se hodnocení provádí. Každý přístup i metoda analýzy rizik má výhody, ale i nedostatky.

Zvolení správného přístupu a metody je závislé na účelu prováděné analýzy dat, jenž jsou k dispozici, výši finančních rezerv a mnohdy i na sociálně politické úrovni.

Často při analýze rizik bývá zásadním problémem nedostatek poskytnutých dat a informací. Například se může jednat o údaje o poruše zařízení, lidského faktoru a charakteristik následků po selhání.

Vzhledem k tomu, že hodnocení rizik představuje základní zdroj informací pro dosažení rozhodnutí, je nutné brát v potaz všechna omezení použitých metod. Analýza rizik je soubor několika kroků počínaje definováním účelu analýzy, identifikací nebezpečí, sběrem nutných informací, posuzováním následků a pravděpodobnosti vzniku až po analýzu míry závažnosti. Prioritní podmínkou je dostatečně kvalitní transparentnost jednotlivých kroků (Vymazal, Míka a Misák, 2015).

Dlouhou dobu se hodnocení rizik provádělo neformálně. Postupem času ale vyšlo najevo, že analýza rizik je nezbytnou součástí pro předcházení a systematickou práci v oblasti zajištění úspěchu. Každá analýza rizik sestává z několika částí, které jsou stejné pro všechny způsoby a také pro to, jak se rozvíjí. Patří mezi ně zejména:

- Identifikace nebezpečí.
- Stanovení rizika (posouzení pravděpodobnosti a následku možné škody pro každou nebezpečnou situaci nebo zdroj nebezpečí).
- Rozhodnutí, zda je riziko přijatelné.

Analýza rizik vycházející z metody participativního přístupu (tedy na spolupráci mezi jednotlivými pracovníky) pomáhá zaměstnancům i vedení podniku pochopit a souhlasit s konáním firmy, kdy:

- Vedení i zaměstnanci společně vnímají závažnosti rizik.
- Je nutný pro fungování podniku.
- Musí být úspěšný v oblasti předcházení nehod.
- Sestavuje vhodná opatření z hlediska bezpečnosti.
- Klade důraz na neustálé vylepšování a navyšování bezpečnostní úrovně práce.
- Cílem je snižování finančních ztrát a škod, které jsou důsledkem nastalých nehod (Vymazal, Míka a Misák, 2015).

3.3.1 Základní kroky hodnocení rizik

- **Klasifikace pracovních činností –** nejprve je nutné vytvořit list pracovních činností, které se v podniku provádějí, a to včetně jejich charakteristiky. Obsaženy by měly být i takové činnosti, které nejsou vykonávány denně, ale i v delším časovém sledu.
- **Identifikace nebezpečí –** jde o vytvoření veškerých možných zdrojů, ze kterých plyne riziko, a to z jejich nebezpečných vlastností. Identifikuje se nebezpečí vysoké, střední i nízké. Posuzování nebezpečí provádíme pro veškeré fáze provozu – tedy mimo standardní provoz také odstávky, údržbu a podobně.
- **Stanovení rizik – jde** o odhad rizika, které je spojeno s nebezpečím. Na základě odhadu je nutné stanovit bezpečnostní opatření. Takové opatření musí být účinné, minimalizovat možnost selhání a následků.
- **Rozhodnutí o přijatelnosti rizika –** posuzujeme, zdali bezpečnostní opatření, které bylo nebo bude vytvořeno, je dostatečné. Je nutné zajistit a udržet nebezpečí na co minimální úrovni a v momentě rozhodnutí o přijatelnosti se rozhoduje, zdali je míra nebezpečí přijatelná. Pokud ne, je třeba vypracovat opatření lépe.
- **Příprava nápravných opatření ke snížení rizika** (je-li nutné) **-** tento bod je nutný pouze v případě, bylo-li v předcházejícím kroku zjištěno, že některá z opatření nejsou dostačující a riziko nebezpečí je příliš vysoké. V tento moment se hledá alternativa, jak riziko snížit, tak, aby byla míra nebezpečí rizika přijatelná.
- **Posouzení, zda plán nápravných opatření je odpovídající** – zpětné zhodnocení a kontrola kvality opatření, jejichž cílem je minimalizovat míru nebezpečí. Pokud je stále riziko příliš vysoké, vracíme se o krok zpět do návrhu a přípravy na snížení opatření rizik (Základní kroky analýzy a hodnocení rizik, 2020).

Posuzování rizik lze provádět na několika kvantitativních úrovních. Některé metody vyjadřují rizika komplexně, ale to není nutné u všech podniků. Za nutnost je toto považováno například u podniků z oblastí chemických, jaderných atd. U podniků z ostatních oblastí si vystačíme s jednoduššími metodami. Poznáváme několik úrovní:

- Bezvýznamné, zanedbatelné riziko.
- Akceptovatelné, méně významné riziko.
- Nežádoucí riziko.
- Významné riziko.
- Nepřijatelné riziko.

Bezvýznamné, zanedbatelné riziko – nepotřebujeme zvláštní opatření ani v momentě, kdy se nejedná o riziko nulové, tedy absolutní bezpečnost. Na této úrovní je vhodné na riziko poukázat a brát jej v potaz.

Akceptovatelné, méně významné riziko – již je potřeba prodiskutovat možná řešení nebo provést návrhy na zlepšení. Pokud byl pokus o provedení neúspěšný, je nutné zvážit náklady a proces opakovat. Jedná se o proškolení obsluhy, dozor a podobně.

Nežádoucí riziko – na této úrovni zatím není nutnost opatření tak vysoká jako u následujících významných rizik, přesto je nutné již realizovat bezpečnostní opatření podle plánu, který schválilo a realizovalo vedení podniku. Finanční prostředky musí být vyhrazeny v konkrétním časovém úseku. Pracuje se na snížení rizika na akceptovatelnou, ideálně na bezvýznamnou úroveň.

Významné riziko – již se dostáváme na předposlední úroveň, ve které je nutné reagovat urychleně a míru rizika minimalizovat. K tomu se používá postup bezpečnostních opatření, je nutné čerpat finanční a materiálové zdroje. Často se rizikem musí podnik zabývat v horizontu maximálně několika dnů. (Koudelka a Vrána, 2006)

Nepřijatelné riziko – hovoříme o nejvyšší možné úrovni rizika, kdy jsou podniky nuceny vzhledem k nejvyšší možné míře nebezpečí pozastavovat svůj provoz a řešení rizikové situace se stává prioritou všech kompetentních osob. Je nutné vyhradit potřebné finanční zdroje. Fungování podniku je zastaveno do té doby, dokud míra rizika není snížena na nižší úroveň. Tato situace může mít pro podnik fatální následky (Koudelka a Vrána, 2006). Rizika informačního systému by měla být řízena dle modelu PDCA, viz obr. 3.

- Plánuj – analýzy prostředí, zdrojů, rizik, kontrola návrhů atd.
- Dělej – plán zavedení opatření, dokumentace opatření, kontrola a oprava zavedení opatření.
- Kontroluj – plán, provedení, vyhodnocení kontrol.
- Jednej – vyhodnocení výsledků kontrol, ověření vhodnosti opatření a jejich úpravy (Čermák, 2009, s. 128).

Obrázek 3 – PDCA (How to do PDCA step by step, 2019)

3.3.2 Řízený rozhovor

Představuje metodu analýzy rizik, která spočívá v diskusi kompetentních osob, kde cílem je sběr informací o vybraném subjektu. Výstupem řízeného rozhovoru by měl být soubor dat, názorů a poznatků, které slouží k identifikaci a minimalizaci rizik podniku. Podstatou je předání informací osob mezi sebou, neboť jedna osoba nemá přehled o míře rizika ve všech odvětvích podniku.

Nejčastěji jsou účastníky řízeného rozhovoru zástupci jednotlivých sektorů podniku, například: vedoucí výrobní haly, ředitel servisního střediska, ředitel obchodního oddělení, vedoucí nákupu, vedoucí expedice, účetní, vedoucí společnosti zajišťující informační technologie, vedoucí softwarového vývoje a vedoucí hardwarového vývoje – konstrukce.

3.3.3 Brainstorming

Podstata brainstormingu spočívá v zaměření se a hledání řešení jednoho konkrétního problému. Metoda je prováděna ve skupině lidí, jejichž nápady se zpočátku mohou zdát nevhodné, odvážné či nereálné. Doporučuje se používat papír, či jiný způsob zapisování si nápadů, metod a doporučení. Nejprve skupina osob navrhne myšlenku, případně řešení problematiky, tyto podněty jsou bez komentáře zapsány. Následně se všechny nápady přesunou do fáze hodnocení. Na základě ohodnocení se potom skupina shodne na společném výsledku, který uspěje. Tato metoda je použita v diplomové práci v ohodnocení informačních, technických a podpůrných aktiv. Názory a ohodnocení aktiv byly následně

zprůměrovány a tím bylo dosaženo finální hodnoty, se kterou se v práci dále pracuje (Jak využít brainstorming v obchodu a managementu, 2021).

3.3.4 Kontrolní seznam (Check list)

Check list představuje způsob analýzy, kdy se používá již existující kontrolní seznam. Jedná se o jednoduchý způsob, kdy se podávají dotazy na chyby a nesrovnalosti například výrobního procesu. Díky tomu je možné pracovat na vylepšeních bezpečnostních opatření. Pokud se vytváří nový seznam, osoba k tomu používá informace, které čerpá z předpisů a norem.

Pokud kontrolní seznam vytváří specializovaná osoba nebo tým osob, je výsledkem jeho vyšší kvalita. Jeho výhodou je možnost kombinace s dalšími metodami, například What-If metoda (Co se stane, pokud…). Výhodou metody Check list je možnost použití v libovolné fázi procesu (Bernatík, 2016).

3.3.5 Matice rizik

Matice rizik je další z metod vyhodnocování míry rizika bezpečnosti podniku. Používá se v jednoduché tabulkové formě, kdy na horizontální ose značíme pravděpodobnost, že riziko nastane. Na vertikální ose potom hodnotíme význam neboli závažnost, pokud riziko nastane. Tyto dvě hodnoty jsou následně násobeny, čímž dostaneme součin dvou čísel – pravděpodobnost krát závažnost. Výsledné číslo poté kategorizujeme do předem stanoveného žebříčku. V závislosti na škále žebříčku se pak rizikem buď zabýváme, nebo jej vyhodnotíme jak nízko-rizikové a není třeba mu věnovat speciální pozornost. Na obr. 4 lze vidět názorný příklad matice rizik.

Obrázek 4 – Matice rizik (Matice významnosti rizik, 2020)

II. PRAKTICKÁ ČÁST

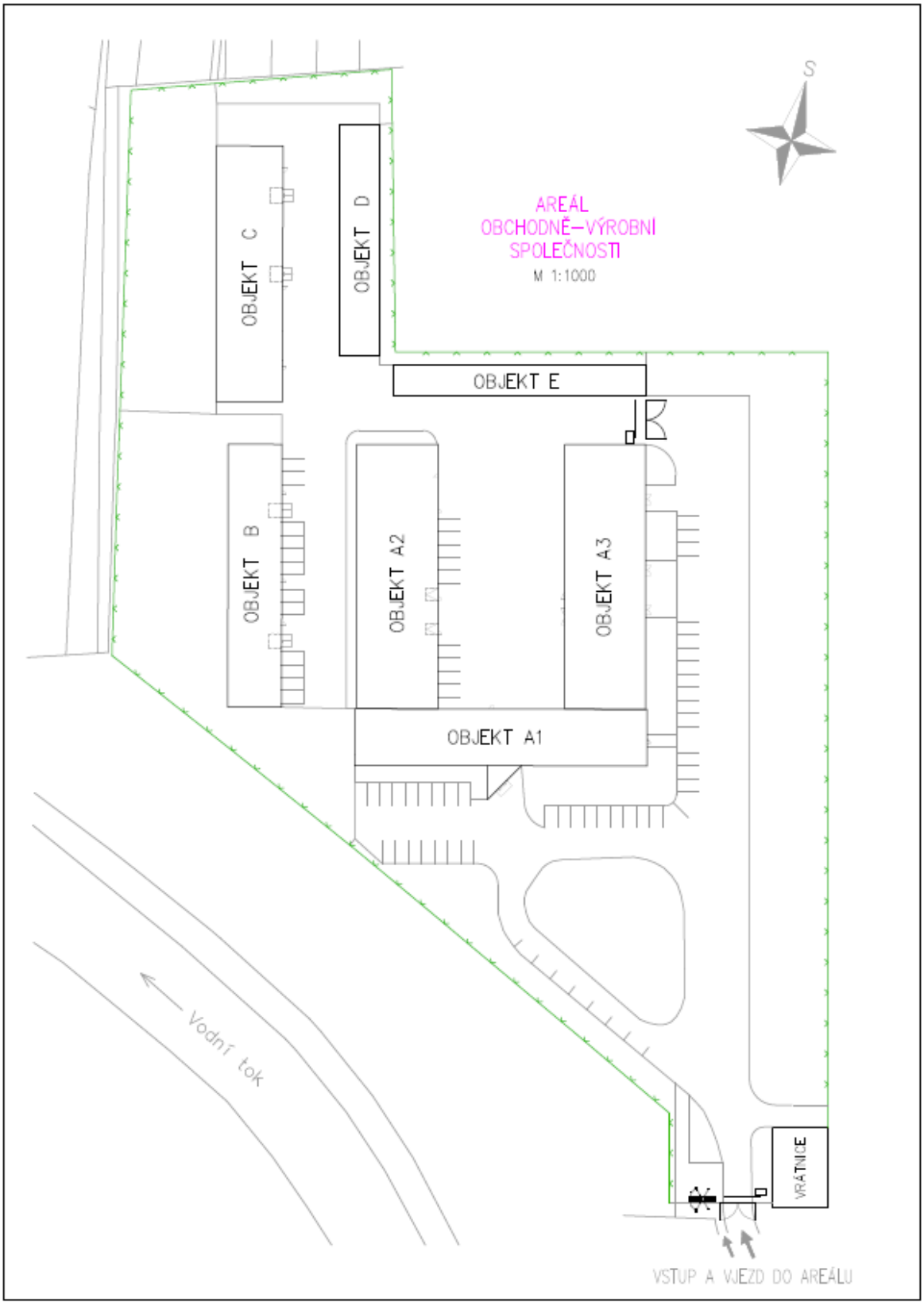
4 POPIS POSUZOVANÉHO OBCHODNĚ VÝROBNÍHO PODNIKU

V diplomové práci je posuzován reálný podnik. Bohužel nejvyšší management společnosti se neztotožnil se zveřejněním lokalizace a jména podniku, především proto, že by mohlo dojít ke zmínění citlivých informací nebo Know-how, proto bude o podniku pojednáváno obecně a anonymně. Jedná se o společnost, která vyrábí a prodává kvalitní výrobky a služby. Produkty společnosti jsou nabízeny na tuzemském trhu pracovníky obchodního oddělení přímo koncovým zákazníkům a na trhu zahraničním jsou prodávány pracovníky zahraničního obchodu, přes obchodní zástupce v jednotlivých zemích celého světa. Provoz podniku je rozdělen mezi následující střediska:

- Výroba.
- Obchod – CZ.
- Obchod – zahraniční.
- Vývoj HW.
- Vývoj SW.
- Servis.
- Ekonomický úsek.
- Nákup.
- Management.

Podnik zaměstnává celkem 180 pracovníků. Z toho jsou 3 členové představenstva, tedy vyššího managementu, 6 ředitelů středisek středního managementu, 9 mistrů výroby a 8 vedoucích pracovníků menších skupin, tedy nižšího managementu.

Zbývající zaměstnanci jsou pracovníci ve výrobních prostorech, technici, pracovnice účtárny, uklízečky atd. Areál podniku sestává ze sedmi budov označenými písmeny římské abecedy, který je zobrazen na obr. 5.



Obrázek 5 – Areál obchodně výrobního podniku (interní zdroj podniku)

4.1 Identifikace aktiv informačního systému

Mezi aktiva řadíme všechno, co má pro podnik hodnotu a mělo by být příslušným způsobem chráněno. Účelem a úkolem aktiv je přinášet podniku finanční zisky. Aktiva představují majetek jak hmotný, tak nehmotný. Při vyhodnocení aktiv bylo využito metod řízeného rozhovoru a Brainstormingu.

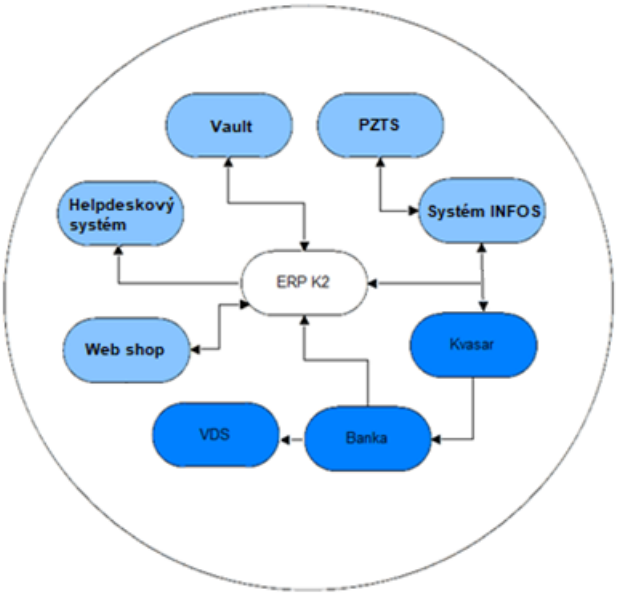
4.1.1 Podnikový informační systém

Informační systémy jsou důležitou součástí bezpečného chodu podniku. Stejně tak předmětný podnik, který se zabývá vývojem, projekcí, výrobou, prodejem a následným servisem svých produktů používá podnikový informační systém. V podniku probíhá velké množství procesů a je nutné odpovídajícím způsobem zpracovávat a shromažďovat potřebné množství dat a informací. Podnik zakoupil několik systémů, které jsou propojeny do podnikového IS. Na obr. 6 jsou znázorněny vazby jednotlivých systémů a informačních toků. Ceny systémů jsou uvedeny v tab. 3

Jádro informačního systému je tvořeno ERP systémem K2, který je mimo systém video dohledový systém (dále je „VDS“) propojený s dalšími systémy. Jednotlivé moduly a funkce ERP systému K2 jsou následující:

- Vault – je nástroj pro evidenci, označení a uchování dokumentace produktů společnosti ve formátu dwg.
- Web shop – internetový prodej produktů přes webové stránky podniku.
- Poplachový zabezpečovací a tísňový systém (dále jen „PZTS“) je propojený s přístupovým systémem (dále jen „ACS“) a propojení slouží pouze k zastřežení a odstřežení systému, kdy po přiložení ID karty ke čtečce ACS a validním vyhodnocení systém zasílá signál PZTS.
- Kvasar – personální systém propojený s Infosem, kde jsou importována a exportována matriční data zaměstnanců v pravidelných intervalech,
- Banka – aplikace k provádění standardních plateb, propojený s ERP K2 a se systémem Kvasar pro zasílání mzdy zaměstnancům.
- Helpdeskový systém – eviduje a uchovává požadavky zákazníků, propojení je jednosměrné, kdy helpdeskový systém čerpá skladové položky produktů z ERP systému.

- Infos – je systém, který obsahuje přístupový systém, docházkový systém a stravovací systém, kdy vše pracuje na jedné společné databázi MS SQL. Infos je obousměrně propojený se systémem ERP K2.
- Video dohledový systém (Dále jen „VDS“) – není nijak propojený na další systémy.



Obrázek 6 – Informační systém podniku (vlastní zpracování)

4.1.2 Informační aktiva

Z hlediska plnění cílů podniku představuje Dataware citlivá primární data, která mají význačnou hodnotu a případné škody na nich mohou způsobit paralýzu celého podniku. Hovoříme zejména o informacích a datech uložených na sdílených discích podnikového intranetu a databázi jednotlivých modulů IS. K vyjádření významu citlivosti informací byla použita klasifikace dle důvěrnosti následujících kategorií:

- D – důvěrné, koeficient klasifikace 4. v tabulce 1 zvýrazněno červeně
- O – omezený přístup, koeficient klasifikace 3.
- I – interní, koeficient klasifikace 2.
- V – veřejné, koeficient klasifikace 1.

Tabulka 1 – Informační aktiva (vlastní zpracování)

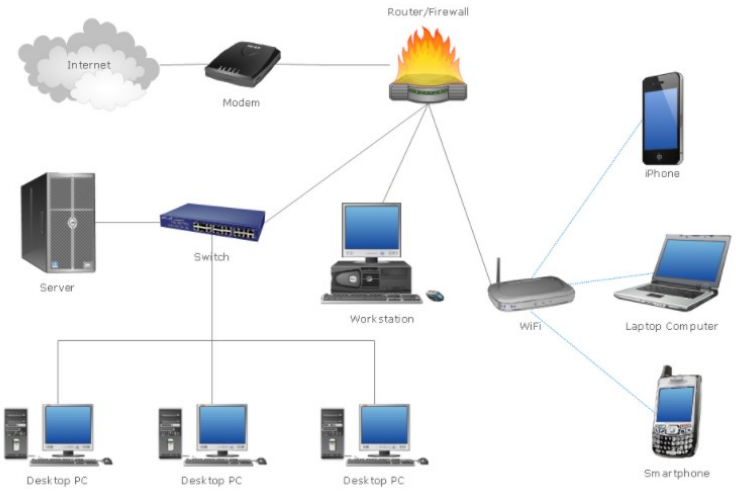
Číslo	Aktivum	Klasifikace	Číslo	Aktivum	Klasifikace
1	Účetnictví		6	Logistika	
1.1	DPH	O	6.1	Stavy skladů	D
1.2	Silniční daň	O	6.2	Vyhodnocení skladu	O
1.3	Interní doklady	D	6.3	Převodky	O
1.4	Základní nastavení účetnictví	O	6.4	Příjemky	O
1.5	Účetní deník	D	6.5	Výdejky	O
1.6	Položky účetního deníku	O	6.6	Inventury	O
1.7	Likvidace a účtování	O	6.8	Zásilkové služby	I
1.8	Hlavní kniha	D	6.9	Doprava	I
1.9	Ekonomické analýzy	D	7	Výroba	
1.10	Ostatní funkce	O	7.1	Technologická příprava výroby	D
1.11	Kontroly zaúčtování	O	7.2	Průvodky	O
1.12	Přecenění k rozvahovému dni	O	7.3	Výrobní příkazy	O
1.13	Servisní funkce	O	7.4	Řízení výroby	D
1.14	Účetní závěrka	D	7.5	Vyhodnocení výroby	I
1.15	Nezaúčtované doklady	O	7.6	Vyhledávání sériového čísla	I
1.16	účetní sestavy	I	8	Projekty	
2	Marketing		8.1	Základní nastavení	I
2.1	Nabídka/Poptávka	O	8.2	Projekty	D
2.2	Partneři	O	8.3	Výkazy práce	O
2.3	Kontaktní osoby	O	9	Celnice	
2.4	Aktivity	O	9.1	Základní data	I
2.5	Příležitosti	O	9.2	JCD - Dovoz	O
2.6	Kampaně	V	9.3	JCD - Vývoz	O
2.7	Vyhodnocení marketingu	I	9.4	JCD - Zjednodušený příjem	O
2.8	Správa a nastavení	O	9.5	JCD - Zjednodušený výdej	O
3	Prodej		9.7	JCD - Tranzit	I
3.1	Základní data	O	9.8	Celní sazebník	V
3.2	Kontakty	D	10	Banka	
3.3	Zakázky	D	10.1	Banka	D
3.4	Položky prodeje	I	10.2	Položky platebních dokladů	D
3.5	Objednávky přijaté	D	10.3	Saldokonto	O
3.6	Rezervační listy	I	10.4	Upomínky	O
3.7	Výdejky	O	10.5	Opravné daňové doklady	O
3.8	Dodací listy vydané	O	10.6	Skonto	O
3.9	Faktury vydané	D	10.7	Platební kalendář	D
3.10	Zálohy přijaté	O	10.8	EET	O
3.11	Ostatní pohledávky	O	10.9	VP Banka	O
3.12	Vyhodnocení prodeje	I	11	Majetek	
3.13	Kupónové slevy	O	11.1	Kniha majetku	D
3.14	Funkce	I	11.2	Propojení s prvotními doklady	O
4	Nákup		11.3	Hospodářský rok	D
4.1	Poptávky	I	11.4	Prostorová procesní evidence	O
4.2	Kontakty	D	12	Mzdy	
4.3	Objednávky vydané	I	12.1	Personální údaje	D
4.4	Položky nákupu	O	12.2	Pracovní vztahy	D
4.5	Potvrzení dodání	I	12.3	Mzdové údaje	D
4.6	Příjemky	O	12.4	Srážky z mezd	D
4.7	Faktury přijaté	D	12.5	Mzdové výpočty	D
4.8	Zálohy poskytnuté	O	12.6	Kvalifikace	O
4.9	Ostatní závazky	O	12.7	Závazky z mezd	D
4.10	Vyhodnocení nákupu	I	12.8	Organizační struktura	O
5	Reklamace		13	Internetový obchod	
5.1	Servisní zakázky	O	13.1	Kniha pro internetový obchod	O
5.2	Servisní listy	O	13.2	Související knihy	O
5.3	Vyhodnocení servisu	O	13.3	Správa a nastavení	O
5.4	Přehledy	I	13.4	Kupónové slevy	I

Údaje v tab. 1 vychází z ohodnocení odpovědnými vedoucími osobami podniku. V příloze je uvedena obsáhlá tabulka se zhruba 110 položkami. Celkem šest odpovědných osob hlasovalo v rozmezí hodnot 1-4 nezávisle na sobě. Hodnoty jednotlivých ptracovníků byly následně zprůměrovány a tak byla konkrétním aktivům přiřazena hodnota v podobě daného písmena. Uveďme si příklad ohodnocení prvního aktiva:

V tabulce pod identifikátorem 1.1 nalezneme položku DPH, kterou hodnotilo šest osob v tomto pořadí: 4, 2, 3, 3, 4, 3. Sečtením čísel a podílem počtem osob jsme dospěli k průměrné hodnotě 3 po zaokrouhlení. Hodnota 3 odpovída v klasifikaci aktiv písmenu O, tedy aktiva s omezeným přístupem. Kompletní tabulka hodnocení jednotlivých zainteresovaných pracovníků se nachází v příloze diplomové práce.

4.1.3 Technická aktiva

Základ programového vybavení tvoří ERP systém K2 obsahující 13 modulů. Jednotlivé moduly jsou znázorněny v tab. 1. Tyto moduly nejsou instalovány na koncových stanicích, ale na serveru a komunikace probíhá pomocí klientských stanic. Všechny koncové stanice mají nainstalován operační systém (dále jen „OS“) Win 10, aplikace kancelářského balíčku Office 365 licenci E3, Adobe Acrobat Reader DC, Skype for Business a případné další licencované programy jako např. AutoCad, Vault, CRM nebo aplikace vyvinuté podnikem. Pro práci v prostředí internetu jsou podporovány pouze prohlížeče Microsoft EDGE nebo Mozilla Firefox. Podniková síť je tvořena strukturovanou kabeláží (dále jen „SK“) cat. 5E s topologií hvězda viz. Obr. 8.



Obrázek 7 – Schéma sítě (Computer network system design diagram, © 1993–2020)

Součástí SK jsou i jednotlivé datové rozvaděče Rack, routery, switche, Acess pointy pro WIFI, IP kamery, přístupový, docházkový a stravovací sytém. Přípojné body pro uživatele jsou vyvedeny v parapetních žlabech. Pro uživatele jsou na serveru dostupné sdílené disky, ale i osobní adresář pro ukládání pracovních souborů.

Uživatelé disponují pracovními stanicemi značky Hewlett-Packard (dále jen „HP“) a jednotlivá střediska využívají sdílených tiskáren se skenery. Pro interní podnikové hovory slouží telefonní ústředna Siemens s kompatibilními aparáty. Areál podniku tvoří sedm budov vzájemně propojených kabelovými kanály. Kompletní soupis technických aktiv podniku je uveden v tab. 3. V prvním sloupci je identifikační číslo a v druhém sloupci je uveden název komponenty. Následují třetí a čtvrtý sloupec, kde jsou údaje o pořizovací ceně aktiva a jeho chráněné hodnotě. Pořizovací hodnota je daná, proto nepodléhá nutnému hodnocení odpovědných osob. Způsob hodnocení chráněné hodnoty aktiva je uveden v tab. 2. Byly využity čtyři rozmezí pořizovací ceny, kde každému rozmezí je přiřazeno písmeno. Zmíněných šest odpovědných osob nezávisle na sobě ohodnotilo chráněné hodnoty. Výsledky hlasování jsou zprůměrovány a chráněná hodnota je přiřazena jednotlivé komponentě. Kompletní tabulka s výsledky hodnocení odpovědných osob je uvedeno v příloze. Pro vyjádření hodnoty kritičnosti technických aktiv bylo využito kombinace parametrů:

- Pořizovací cena aktiva.
- Výše možné škody při poškození nebo zničení aktiva.

Tabulka 2 – Hodnota aktiv (vlastní zpracování)

Pořizovací cena		Chráněná hodnota	
1	<10.000 Kč	A	<10.000 Kč
2	10.000 - 100.000 Kč	B	10.000 - 100.000 Kč
3	100.000 - 500.000 Kč	C	100.000 - 500.000 Kč
4	> 500.000 Kč	D	> 500.000 Kč

Technická aktiva jsou zobrazena v tab.3, do kterých spadají licencované programy nezbytné k fungování společnosti, hardwarové a síťové prostředky, PZTS, video dohledový systém a výčet objektů podniku.

V případě, že by vznikla škoda, její výše může přesáhnout hodnotu aktiva, například nefunkční PZTS vs. napadení koncové stanice nebo NTB vs. ztráta citlivých informací či know-how.

Tabulka 3 – Technická aktiva (interní zdroj podniku, vlastní zpracování)

Číslo	Komponenty	Klasifikace		Číslo	Komponenty	Klasifikace	
		Pořizovací cena	Chráněná hodnota			Pořizovací cena	Chráněná hodnota
1.	Software a aplikace			4.	Poplachový zabezpečovací a tísňový systém		
1.1	ERP systém K2	4	D	4.1	Ústředna PZTS	3	D
1.2	Operační systém Win 10	2	D	4.2	Kabelové rozvody PZTS	3	D
1.3	Office365	2	C	4.3	Detektory	2	D
1.4	Eset Endpoint Antivirus	3	D	4.4	Ovládací zařízení	1	C
1.5	CRM Databox	3	C	4.5	Signalizační zařízení	2	D
1.6	Helpdeskový systém Apollo	3	C	5.	Video dohledový systém		
1.7	Web shop	3	D	5.1	Záznamové zařízení	3	D
1.8	Firemní aplikace	4	D	5.2	Kabelové rozvody	2	B
1.9	Adobe Acrobat	2	C	5.3	IP Kamery	3	C
1.10	Auto CAD	2	D	6.	Objekty		
1.11	Vault	4	D	6.1	Administrativní budova A1		
2.	Komunikační infrastruktura			6.1.1	Zasedací místnosti	3	C
2.1	Serverovna	4	D	6.1.2	Jídelna	2	B
2.2	Datový rozvaděč RACK	2	B	6.1.3	Kanceláře	3	D
2.3	Kabelové rozvody	3	C	6.1.4	Archiv	2	D
3.	Síťové prostředky			6.1.5	Serverovna	4	D
3.1	Server	4	D	6.1.6	Parkoviště	3	C
3.2	Diskové pole	3	D	6.2	Výrobní hala A2		
3.3	Router	1	C	6.2.1	Sklad EV	4	D
3.4	Switch	2	B	6.2.2	Expedice	3	C
3.5	Access point	1	D	6.2.3	Klimatická komora	3	C
3.6	Tiskárny	2	B	6.2.4	Vývoj HW	2	C
3.7	Přístupový systém	4	D	6.7	Skladovací hala A3	4	D
3.8	Docházkový systém	3	D	6.8	Výrobní hala B	4	D
3.9	Stravovací systém	2	D	6.9	Výrobní hala C	4	D
3.10	Přenosné PC	2	D	6.10	Sklad D	4	D
3.11	Mobilní telefony	2	D	6.11	Sklad E	4	D
3.12	Telefonní ústředna	3	C	6.11	Parkoviště mezi halami	3	C

4.1.4 Podpůrná aktiva

Fungování HW a SW se neobejde bez Peopleware, do kterého můžeme zařadit jednotlivé uživatele, skupiny nebo projektové týmy. Peopleware stanovuje uplatnění lidských zdrojů v rozsahu provozu IS a je zaměřen na pracovníky zejména z hlediska jejich povinností vůči IS. Kritičnost lidského elementu v soupisu aktiv byla ohodnocena dle požadované úrovně odborné způsobilosti:

- 1 – základní.
- 2 – střední.
- 3 – vyšší.
- 4 – nejvyšší, v tabulce 4 zvýrazněno červeně

Vyhodnocení podpůrných aktiv je zobrazeno v tab. 4.

Tabulka 4 – Podpůrná aktiva (vlastní zpracování)

Číslo	Aktivum	Klasifikace
1	**Kmenoví zaměstnanci**	
1.1	Top management	4
1.2	Manažer IT	4
1.3	Manažer bezpečnosti informací	4
1.4	Střední management	3
1.5	Mistři výroby	2
1.6	Dělníci	1
2	**Externí pracovníci**	
2.1	Správce IS	4
2.2	Správce IT	4
2.3	Provider	2
2.4	Daňový poradce	1
2.5	Právní kancelář	1
2.6	Revizní technici	1
2.7	Pracovníci státní správy	1

Stejným postupem jako u informačních a technických aktiv probíhalo ohodnocení podpůrných aktiv, kdy šest odpovědných osob provedlo hodnocení. Jejichž výsledky byly zprůměrovány a aktiva byla ohodnocena příslušnou hodnotou číselné stupnice. Jednotlivé výsledky hlasování jsou uvedeny v příloze diplomové práce.

4.1.5 Určení vlastníků aktiv

Cílem identifikace a ohodnocení aktiv je zabezpečit jejich přiměřenou ochranu. Důležitá informační aktiva jsou evidována v rámci Bezpečnostní politiky informačního systému (Dále jen „BPIS“), je stanovena odpovědnost za jejich správu a je určen jejich garant. Za evidenci aktiva odpovídá jeho garant. Garantem aktiva je zpravidla vedoucí zaměstnanec, který nese za aktivum odpovědnost. Pro všechna důležitá aktiva musí garanti určovat přiměřená bezpečnostních opatření.

Správcem aktiva je zaměstnanec pověřený správou aktiva v rámci svých pracovních povinností. Uživatelem aktiva je pracovník, jenž aktivum používá ke své práci a je povinen dodržovat bezpečnostní opatření pro zacházení s aktivem stanovená garantem.

4.1.6 Identifikace hrozeb

Hrozby pro informační systém byly posouzeny na základě negativního dopadu na aktiva dle důvěrnosti, dostupnosti a integrity aktiv, které jsou uvedeny v jednotlivých sloupcích viz. tab. 5, a jsou označeny následujícím způsobem:

- Důvěrnost – Confidence (CN).
- Dostupnost – Availability (AVL).
- Integrita – Integrity (INT).

Hrozby mohou vzniknout úmyslně či neúmyslně nebo taktéž může být jejich původ přírodního charakteru. V tabulce jsou uvedené jevy označeny následně:

- Úmyslné – Deliberately (DLB).
- Neúmyslné – Accidentaly (ACC).
- Přírodní – Enviromental (ENV).

Tabulka 5 - Identifikace hrozeb (Čermák, 2009 - upraveno autorem)

Číslo	Hrozba		CNF	INT	AVL	DLB	ACC	ENV
1.	Lidé	Hacker, špion, konkurence	x	x	x	x	x	
2.		Zaměstnanec	x	x	x	x	x	
3.		Neproškolený uživatel				x	x	
4.		Externí pracovník dodavatele				x	x	
5.		Správce systému				x	x	
6.		Návštěva				x	x	
7.	Fyzické poškození	Požár		x	x	x	x	x
8.		Povodeň			x			x
9.		Orkán			x			x
10.		Zemětřesení			x			x
11.		Výbuch		x	x	x	x	x
12.		Prach koroze			x			x
13.		Zatopení (porucha ústředního topení nebo vodoinstalace)		x	x	x	x	x
14.		Porucha klimatizace			x	x	x	
15.	Služby	Dodávka el. Energie			x	x	x	x
16.		Výpadek konektivity IS		x	x	x		
17.		Dodávky materiálu			x	x	x	
18.	Informace	Odposlech	x			x		
19.		Přerušení	x			x	x	
20.		Nesprávné ověření identity uživatele	x	x	x	x	x	
21.		Změna dat				x	x	
22.		Kopírování				x		
23.		Změna při přenosu				x		
24.		Vymazání				x	x	
25.	Selhání lidského faktoru	Krádež	x	x	x	x		
26.		Neadekvátní servisní činnost				x	x	
27.		Nedostatek zaměstnanců s potřebnou odbornou úrovní					x	
28.	HW	Porucha	x	x	x		x	
29.		Odcizení	x	x	x	x		
30.		Poškození	x	x	x	x		
31.	SW	Kopírování				x	x	
32.		Viry	x	x	x	x	x	
33.		Úmyslné vymazání				x		
34.		Neúmyslné vymazání					x	
35.		Kyberterorismus	x	x	x	x		
36.		Porucha zálohování		x	x	x	x	
37.		Použití neautorizovaného SW		x	x	x		

4.2 Kvantifikace hrozeb

Následujícím krokem po identifikaci hrozeb je stanovení pravděpodobnosti výskytu hrozby, kdy bude stanovena hrozba vždy pro tandem hrozba/aktivum. Pro kvantifikaci hrozeb neexistuje žádný algoritmus. Je tedy založena pouze na úsudku hodnotitelů. Pro vyhodnocení hrozeb bylo použito stupnice uvedené v tab.6

Tabulka 6 – Pravděpodobnost hrozby (vlastní zpracování)

Míra pravděpodobnosti výskytu hrozby	Číselná hodnota
Nízká pravděpodobnost	1
Střední pravděpodobnost	2
Vysoká pravděpodobnost	3
Kritická pravděpodobnost	4

Hodnota hrozby je uvedena v následující tabulce č. 7. K hodnocení bylo využito stupnice, kde kvantifikace hrozeb vychází z posouzení jednotlivých hodnotitelů, kteří ohodnocení provedli na základě svých zkušeností, vědomostí a subjektivních pocitů. K jednotlivým položkám byla přidělena hodnota hrozby.

Tabulka 7 – Hodnota hrozby (vlastní zpracování)

Číslo	Hrozba		Hodnota hrozby	Číslo	Hrozba		Hodnota hrozby
1.	Lidé	Hacker, špion, konkurence	1	20.	Informace	Nesprávné ověření identity uživatele	3
2.		Zaměstnanec	3	21.		Změna dat	3
3.		Neproškolený uživatel	2	22.		Kopírování	3
4.		Externí pracovník dodavatele	3	23.		Změna při přenosu	2
5.		Správce systému	3	24.		Vymazání	2
6.		Návštěva	2	25.	Selhání lidského faktoru	Krádež	2
7.	Fyzické poškození	Požár	2	26.		Neadekvátní servisní činnost	2
8.		Povodeň	1	27.		Nedostatek zaměstnanců s potřebnou odbornou úrovní	2
9.		Orkán	1	28.	HW	Porucha	4
10.		Zemětřesení	1	29.		Odcizení	4
11.		Výbuch	2	30.		Poškození	2
12.		Prach koroze	2	31.	SW	Kopírování	3
13.		Zatopení (porucha ústředního topení nebo vodoinstalace)	2	32.		Viry	3
14.		Porucha klimatizace	3	33.		Úmyslné vymazání	2
15.	Služby	Dodávka el. Energie	4	34.		Neúmyslné vymazání	1
16.		Výpadek konektivity IS	3	35.		Kyberterorismus	3
17.		Dodávky materiálu	2	36.		Porucha zálohování	4
18.	Informace	Odposlech	3	37.		Použití neautorizovaného SW	4
19.		Přerušení	3				

4.3 Vyhodnocení zranitelnosti aktiv

Každé aktivum disponuje zranitelností, která umožňuje uplatnění hrozby. Zranitelnost aktiv je vyjádřena na základě citlivosti, kdy je aktivum náchylné ke způsobení rizika hrozbou a kritičnosti, což je význam aktiva pro IS a respektive pro celý podnik. Mezi nejzranitelnější patří aktiva technická, jejichž napadením může dojít k výrazným škodám. Dále informační aktiva zařazená do kategorie důvěrné a podpůrná aktiva, u nichž je vyžadován nejvyšší stupeň odborné kvalifikace. Tato aktiva budou dále posuzována dle zranitelnosti hrozeb uvedených v následující kapitole.

Vyhodnocení zranitelnosti

Dalším krokem v analýze rizik je posouzení zranitelnosti jednotlivých aktiv uvedených v tab. 9, do které byly doplněny hodnoty aktiv a pravděpodobnost hrozeb.

Tabulka 8 – Míra zranitelnosti (vlastní zpracování)

Míra zranitelnosti aktiva	Číselná hodnota
Nízká zranitelnost	1
Střední zranitelnost	2
Vysoká zranitelnost	3
Kritická zranitelnost	4

K vyhodnocení zranitelnosti byla použita metoda řízeného rozhovoru a brainstormingu. Vzhledem k tomu, že se jedná o metodu „sjednoceného názoru“ a následně hodnot uvedených jednotlivými vedoucími podniku, není v tomto případě nutné posuzovat jednotlivé hrozby číselnou hodnotou a tu následně průměrovat, jako je tomu například u technických, informačních a podpůrných aktiv. Nicméně i v tomto hodnocení byl použit rozsah stupnice hodnocení od 1 do 4, který je uveden v tabulce č. 8.

Tabulka 9 – Vyhodnocení zranitelnosti (vlastní zpracování)

	Aktiva	Doklady účetnictví	Faktury vydané prodeje	Objednávky prodeje	Faktury přijaté nákupu	Stavy skladů logistiky	Technologie a řízení výroby	Bankovní doklady	Mzdové údaje	ERP systém K2	Antivir Eset	OS Win 10	Autocad / Vault	Firemní aplikace	Serverovna	Aktivní síťové prvky	Prvky PZTS	Záznamové zařízení VDS	Jednotlivé stavební objekty podni	Management společnosti	Manager IT a bezpečnosti informa	Externí správce IS	Externí správce IT
Hodnota aktiv		4	4	4	4	4	4	4	4	4	3	2	3	4	4	3	3	3	4	4	4	4	4
Hrozby	**Hodnota hrozby**																						
Lidé																							
Hacker, špion, konkurence	1	2	2	2	2	3	1	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3
Zaměstnanec	3	4	3	3	4	3	3	4	4	4	3	3	3	3	3	4	4	4	2	4	4	4	4
Neproškolený uživatel	3	4	4	4	3	4	4	3	3	4	3	4	3	3	3	4	4	4	3	3	3	4	4
Externí pracovník dodavatele	3	2	2	2	2	2	2	2	2	3	3	3	3	2	3	3	2	2	1	2	2	3	3
Správce systému	3	2	2	2	1	2	2	2	2	2	2	2	2	1	2	3	2	2	1	2	2	2	2
Návštěva	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Fyzické poškození																							
Požár	2	1	1	1	1	2	3	1	1	1	1	1	2	1	3	3	1	1	3	1	1	1	1
Povodeň	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	3	1	1	3	1	1	1	1
Orkán	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	3	1	1	3	1	1	1	1
Zemětřesení	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	3	1	1	3	1	1	1	1
Výbuch	2	1	1	1	1	1	3	1	1	2	1	1	1	1	3	3	3	2	3	1	1	1	1
Prach koroze	2	1	1	1	1	3	1	1	1	1	1	1	1	1	1	3	1	1	3	1	1	1	1
Zatopení (porucha ústředního topení nebo vodoinstalace)	2	1	1	1	1	3	1	1	1	1	1	1	1	1	1	3	1	1	3	1	1	1	1
Porucha klimatizace	3	1	1	1	1	2	1	1	1	1	1	1	1	1	2	4	1	1	2	1	1	1	1
Služby																							
Dodávka el. Energie	4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1
Výpadek konektivity IS	3	2	2	2	2	2	2	2	1	2	1	1	1	2	2	2	2	2	2	2	2	2	2
Dodávky	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Informace																							
Odposlech	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	2	2
Přerušení	3	2	2	2	1	1	1	1	2	2	1	1	1	1	3	3	2	2	1	1	1	1	1
Krádež identity uživatele	3	4	4	4	4	3	2	4	4	3	2	2	2	4	4	4	3	3	2	4	4	3	3
Změna dat	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
Kopírování	3	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Změna při přenosu	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Vymazání	2	1	1	1	1	1	1	1	1	1	3	1	2	2	1	1	1	1	1	1	1	1	1
Selhání lidského faktoru																							
Krádež	2	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Neadekvátní servisní činnost	2	2	1	1	2	2	2	1	1	3	1	1	1	2	1	1	1	1	2	1	1	1	1
Nedostatek zaměstnanců s potřebnou odbornou úrovní	2	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	3	3	1	1	1	1	1
HW																							
Porucha	4	1	1	1	1	1	2	1	1	2	2	1	2	1	2	1	2	2	1	1	1	1	1
Odcizení	4	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1
Poškození	2	1	1	2	1	1	2	1	1	1	1	1	1	1	3	3	3	3	3	1	1	1	1
SW																							
Kopírování	3	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
Viry	3	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1
Úmyslné vymazání	2	1	1	1	2	2	2	1	2	1	3	1	1	1	1	1	1	1	1	1	1	1	1
Neúmyslné vymazání	1	2	2	3	2	2	3	1	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2
Kyberterorismus	3	2	2	2	2	2	3	2	3	2	2	4	2	2	2	2	2	2	2	3	3	2	2
Porucha zálohování	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	3	4	3	4	4	3	3
Použití neautorizovaného SW	4	2	2	3	2	2	3	2	3	2	2	3	4	2	2	2	3	3	1	2	2	3	3

4.4 Vyhodnocení rizik - Matice

Kapitola vyhodnocení rizik obsahuje rozsáhlou tabulku, která je barevně rozlišena do čtyřech možných variant, a to na základě výsledné hodnoty rizika, která vznikla vztahem R = A x H x Z, kdy:

- R = Výsledná hodnota rizika.
- A = Hodnota aktiva.
- H = Pravděpodobnost výskytu hrozby.
- Z = Zranitelnost aktiva.

Na základě výsledné hodnoty R byla riziku přidělena barva, která charakterizuje úroveň rizika, viz tab. 10. V ideálním případě bychom v podniku chtěli mít bílé a zelené výsledky, nicméně v našem případě se setkáváme se žlutou i červenou barvou, což nám značí, že riziko je příliš vysoké a ohrožující podnik. Je tedy nutné reagovat a pomocí návrhu vhodných opatření a řešení, která minimalizují úroveň rizika.

Tabulka 10 – Úroveň rizika (vlastní zpracování)

Stanovení úrovně rizika	Rozsah hodnot
Nízké riziko	1–3
Střední riziko	3–10
Vysoké riziko	11–30
Nepřijatelné kritické riziko	≥ 31

Pro vyhodnocení matice rizik byl uplatněn tabulkový editor Excel a za pomoci aplikace vzorců jednotlivých buněk a současného nastavení podmíněného formátování pro barevné rozlišení vyjádřené hodnoty ke kterému jsme dospěli k tab. 11 „Vyhodnocení rizik“.

Tabulka 11 – Vyhodnocení rizik – část 1 (vlastní zpracování)

	Aktiva	Doklady účetnictví	Faktury vydané prodeje	Objednávky prodeje	Faktury přijaté nákupu	Stavy skladů logistiky	Technologie a řízení výroby	Bankovní doklady	Mzdové údaje	ERP systém K2	Antivir Eset	OS Win 10	Autocad / Vault	Firemní aplikace	Serverovna	Aktivní síťové prvky	Prvky PZTS	Záznamové zařízení VDS	Jednotlivé stavební objekty podniku	Management společnosti	Manager IT a bezpečnosti informací	Externí správce IS	Externí správce IT
Hodnota aktiv		4	4	4	4	4	4	4	4	4	3	2	3	4	4	3	3	3	4	4	4	4	4
Hrozby	**Hodnota hrozby**																						
Lidé																							
Hacker, špion, konkurence	1	8	8	8	8	12	4	12	12	12	9	6	9	12	12	9	9	9	8	12	12	12	12
Zaměstnanec	3	48	36	36	48	36	36	48	48	48	27	18	27	36	36	36	36	36	24	48	48	48	48
Neproškolený uživatel	3	48	48	48	36	48	48	36	36	48	27	24	27	36	36	36	36	36	36	36	36	48	48
Externí pracovník dodavatele	3	24	24	24	24	24	24	24	24	36	27	18	27	24	36	27	18	18	12	24	24	36	36
Správce systému	3	24	24	24	12	24	24	24	24	24	18	12	18	12	24	27	18	18	12	24	24	24	24
Návštěva	2	8	8	8	8	8	8	8	8	8	6	4	6	8	8	6	6	6	8	8	8	8	8
Fyzické poškození																							
Požár	2	8	8	8	8	16	24	8	8	8	6	4	12	8	24	18	6	6	24	8	8	8	8
Povodeň	1	4	4	4	4	12	4	4	4	4	3	2	3	4	4	9	3	3	12	4	4	4	4
Orkán	1	4	4	4	4	12	4	4	4	4	3	2	3	4	4	9	3	3	12	4	4	4	4
Zemětřesení	1	4	4	4	4	12	4	4	4	4	3	2	3	4	4	9	3	3	12	4	4	4	4
Výbuch	2	8	8	8	8	8	24	8	8	16	6	4	6	8	24	18	18	12	24	8	8	8	8
Prach koroze	2	8	8	8	8	24	8	8	8	8	6	4	6	8	8	18	6	6	24	8	8	8	8
Zatopení (porucha ústředního topení nebo vodoinstalace)	2	8	8	8	8	24	8	8	8	8	6	4	6	8	8	18	6	6	24	8	8	8	8
Porucha klimatizace	3	12	12	12	12	24	12	12	12	12	9	6	9	12	24	36	9	9	24	12	12	12	12
Služby																							
Dodávka el. Energie	4	16	16	16	16	16	16	16	16	16	12	8	12	16	16	12	12	12	32	16	16	16	16
Výpadek konektivity IS	3	24	24	24	24	24	24	24	12	24	9	6	9	24	24	18	18	18	24	24	24	24	24
Dodávky	2	8	8	8	8	8	8	8	8	8	6	4	6	8	8	6	6	6	8	8	8	8	8

Tabulka 12 – Vyhodnocení rizik – část 2 (vlastní zpracování)

	Aktiva	Doklady účetnictví	Faktury vydané prodeje	Objednávky prodeje	Faktury přijaté nákupu	Stavy skladů logistiky	Technologie a řízení výroby	Bankovní doklady	Mzdové údaje	ERP systém K2	Antivir Eset	OS Win 10	Autocad / Vault	Firemní aplikace	Serverovna	Aktivní síťové prvky	Prvky PZTS	Záznamové zařízení VDS	Jednotlivé stavební objekty podniku	Management společnosti	Manager IT a bezpečnosti informací	Externí správce IS	Externí správce IT
Hodnota aktiv		4	4	4	4	4	4	4	4	4	3	2	3	4	4	3	3	3	4	4	4	4	4
Hrozby	**Hodnota hrozby**																						
Informace																							
Odposlech	3	24	24	24	24	24	24	24	24	24	18	12	18	24	24	18	18	18	24	12	12	24	24
Přerušení	3	24	24	24	12	12	12	12	24	24	9	6	9	12	36	27	18	18	12	12	12	12	12
Krádež identity uživatele	4	48	48	48	48	36	24	48	48	36	18	12	18	48	48	36	27	27	24	48	48	36	36
Změna dat	3	24	24	24	24	24	24	24	24	24	18	12	18	24	24	18	18	18	24	24	24	24	24
Kopírování	3	24	24	24	24	12	12	12	12	12	9	6	9	12	12	9	9	9	12	12	12	12	12
Změna při přenosu	2	8	8	8	8	8	8	8	8	8	6	4	6	8	8	6	6	6	8	8	8	8	8
Vymazání	2	8	8	8	8	8	8	8	8	8	18	4	12	16	8	6	6	6	8	8	8	8	8
Selhání lidského faktoru																							
Krádež	2	8	8	8	8	8	16	8	8	8	6	4	6	8	8	6	6	6	8	8	8	8	8
Neadekvátní servisní činnost	2	16	8	8	16	16	16	8	8	24	6	4	6	16	8	6	6	6	16	8	8	8	8
Nedostatek zaměstnanců s potřebnou odbornou úrovní,	2	8	8	8	8	16	16	8	8	8	6	4	6	8	8	6	18	18	8	8	8	8	8
HW																							
Porucha	4	16	16	16	16	16	32	16	16	32	24	8	24	16	32	12	24	24	16	16	16	16	16
Odcizení	4	16	16	16	16	16	16	16	16	16	12	16	12	16	16	12	12	12	16	16	16	16	16
Poškození	2	8	8	16	8	8	16	8	8	8	6	4	6	8	24	18	18	18	24	8	8	8	8
SW																							
Kopírování	3	12	12	12	12	12	12	12	12	12	9	6	18	12	12	9	9	9	12	12	12	12	12
Viry	3	12	12	12	12	12	12	12	12	12	9	12	9	12	12	9	9	9	12	12	12	12	12
Úmyslné vymazání	2	8	8	8	16	16	16	8	16	8	18	4	6	8	8	6	6	6	8	8	8	8	8
Neúmyslné vymazání	1	8	8	12	8	8	12	4	8	8	9	4	6	8	8	6	6	6	8	8	8	8	8
Kyberterorismus	3	24	24	24	24	24	36	24	36	24	18	24	18	24	24	18	18	18	24	36	36	24	24
Porucha zálohování	3	36	36	36	36	36	36	36	36	36	27	18	27	36	36	36	27	36	36	48	48	36	36
Použití neautorizovaného SW	4	32	32	48	32	32	48	32	48	32	24	24	48	32	32	24	36	36	16	32	32	48	48

5 OPATŘENÍ PRO SNÍŽENÍ MÍRY RIZIKA

Po analýze bezpečnostních rizik je nezbytné vysoce rizikové oblasti minimalizovat. K tomu je nutné navrhnout a realizovat příslušná opatření. Jako první způsob aplikujeme pravidelné školení zaměstnanců, kteří budou v návaznosti na pracovní pozice v podniku rozděleni do čtyř skupin, dle kterých se bude odvíjet rozsah školení.

Druhou metodou pro zkvalitnění bezpečnostní infrastruktury a minimalizaci bezpečnostních rizik je pravidelné zálohování dat. Celkem budou probíhat tři zálohovací cykly, každá záloha má vlastní čas spuštění a dobu udržitelnosti zálohovaných dat a informací. Třetí metodou, která významně přispěje ke zvýšení bezpečnostních kvalit podniku, je správa hesel k čemuž bude využit software KEEPASS. Tímto se minimalizuje možnost zneužití hesla v cizí prospěch a přístup neoprávněné osoby k firemním datům. V pořadí čtvrtým opatřením, je návrh na aktivaci TPM čipu a nástroje BitLocker, dále návrh klasifikace informací v prostředí podniku a zjednodušený návrh bezpečnostní politiky informačního systému pro potřeby uživatelů podniku.

5.1 Školení zaměstnanců

Ke zlepšení a zvýšení kvalifikace zaměstnanců budou probíhat pravidelná školení, vedená elektronickou formou, vždy ve stejné posloupnosti – nejprve proběhne školení, jehož délka závisí na typu konkrétního školení. Následuje ověření, zdali osoba školení absolvovala úspěšně. Při neúspěšném výsledku, je třeba ověření znalostí ze školení absolvovat opakovaně.

Pro zjednodušení školení proběhlo sdružení několika uživatelů do skupin viz. tab. 13, a to v závislosti na pracovní pozici, kteří jsou v tabulce níže uvedení jako uživatel 1-4. Rozdělení uživatelů do skupin je následující:

- 1 - Management.
- 2 - Pokročilí uživatelé.
- 3 - Externí pracovníci.
- 4 - Výroba.

Každá skupina má odlišný postup a rozsah školení. Školení se bude týkat čtyřech základních oblastí:

- **Aplikace**, ve které se nachází například podoblast Office365, ERP, HelpDesk a poplachový zabezpečovací a tísňový systém.

- **Bezpečnost zaměstnanců**, ve které jsou části školení např. bezpečnost a ochrana zdraví zaměstnanců při práci, GDPR a klasifikace informací.
- **Bezpečnost v síti**, jež obsahuje užitečné a potřebné informace z hlediska přenosných médií, sdílených disků a práce s nimi, jak svůj počítač chránit před škodlivými programy, jaké existují standardy při správě hesel a správné zálohování dat.
- **Řízení přístupu a VDS** je poslední, čtvrtou skupinou, která obsahuje i stejnojmenné podoblasti – řízení přístupu a VDS.

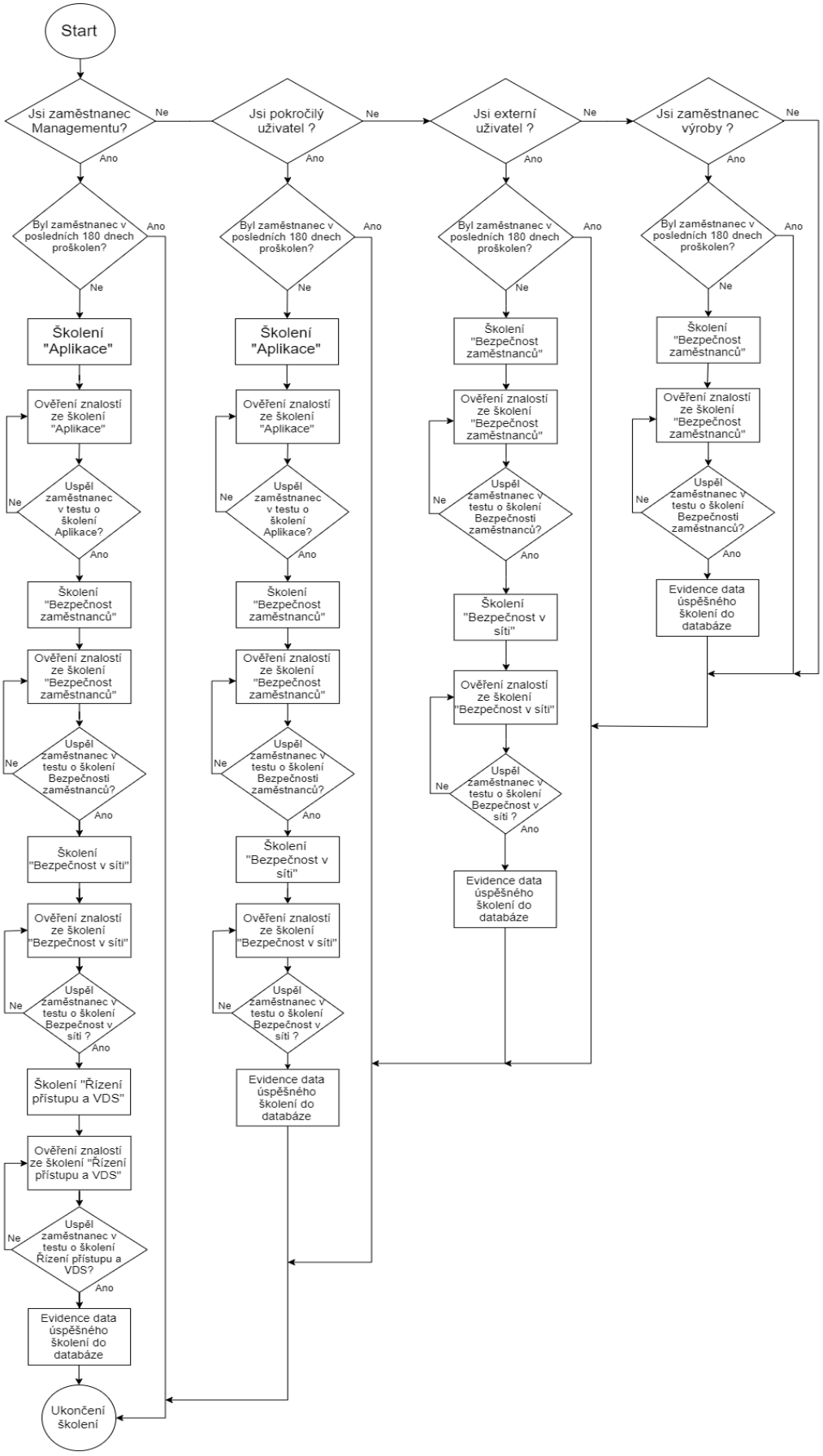
Tabulka 13 – Rozdělení uživatelů do skupin (vlastní zpracování)

Školení zaměstnanců	**Uživatel**												
	1			**2**		**3**		**4**					
	Management	Manager IT	Manager bezpečnosti	Externí pracovníci	Externí správci	Výroba strojní	Výroba elektro	Mistři výroby	Servis	Obchod	Ekonom. Odd.	Vývoj HW	Vývoj SW
Office 365	●	●	●					●	●	●	●	●	●
ERP	●	●	●					●	●	●	●	●	●
Helpdesk	●	●	●					●	●	●	●	●	●
PZTS	●	●	●	●	●	●	●	●	●	●	●	●	●
Klasifikace informací	●	●	●	●	●	●	●	●	●	●	●	●	●
GDPR	●	●	●	●	●	●	●	●	●	●	●	●	●
BOZP	●	●	●	●	●	●	●	●	●	●	●	●	●
Využívání přenosných medii	●	●	●	●	●			●	●	●	●	●	●
NDA	●	●	●	●	●			●	●	●	●	●	●
Zálohování dat	●	●	●	●	●			●	●	●	●	●	●
Standardy správy hesel	●	●	●	●	●			●	●	●	●	●	●
Ochrana před škodlivým software	●	●	●	●	●			●	●	●	●	●	●
Sdílené disky	●	●	●	●	●			●	●	●	●	●	●
Využívání internetu	●	●	●	●	●			●	●	●	●	●	●
Řízení přístupu	●	●	●										
VDS	●	●	●										

Pro přehlednost byl vytvořen vývojový diagram viz. obr. 8, který znázorňuje postup při školení. Nejprve je nutno ověřit, jestli zaměstnanec spadá do skupiny management, pokročilý uživatel, externista, nebo pracovník výroby. Následně proběhne ověření, zda byl zaměstnanec proškolen v průběhu posledních 180 dnů. Pokud ano, školení není nutné a je ukončeno. Pokud školení neproběhlo, nebo později než před 180 dny, musí zaměstnanec příslušné oblasti školení absolvovat.

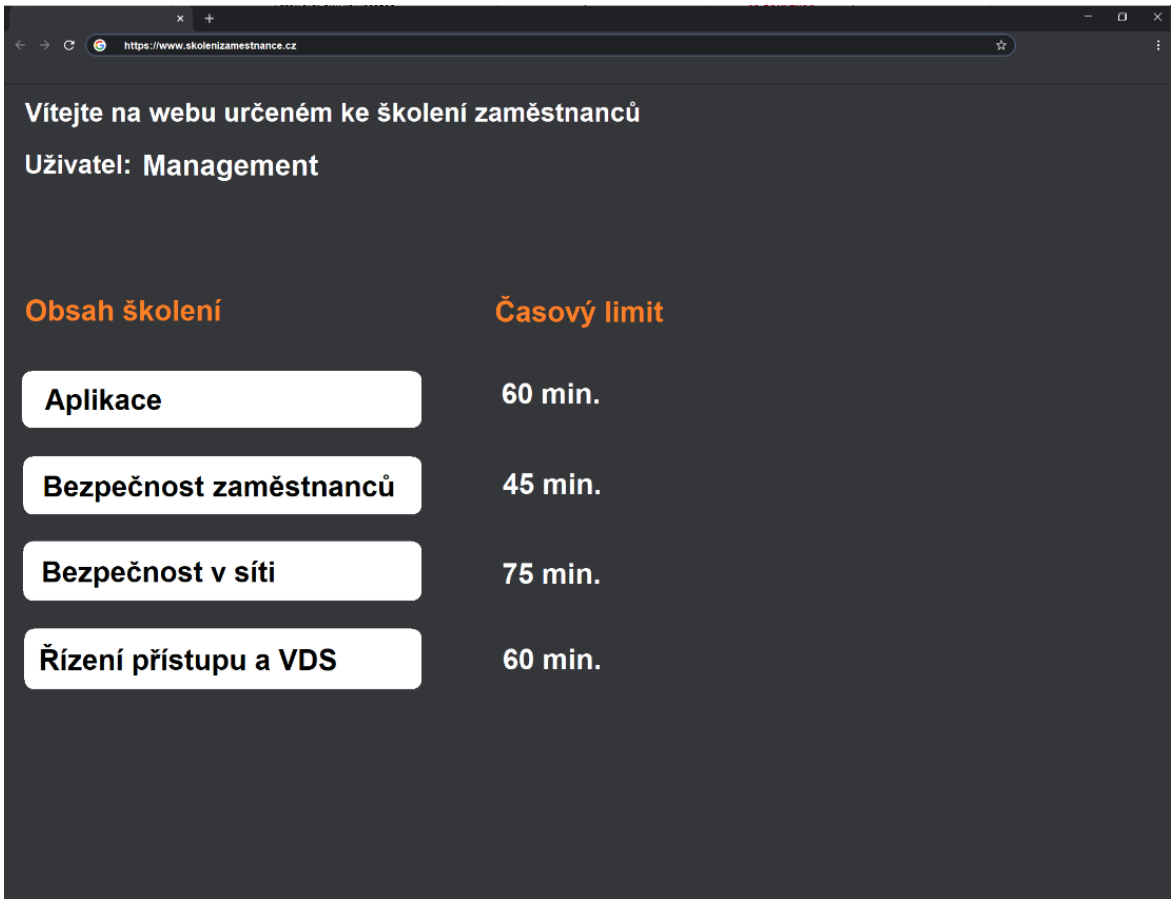
Jedná-li se o zaměstnance managementu, musí být osoba proškolena ve všech čtyřech zmíněných oblastech – aplikace, bezpečnost zaměstnanců, bezpečnost v síti a řízení přístupu a VDS. Po jednotlivém školení následuje ověření znalostí, což si můžeme představit jako test ve škole. Následná podmínka ověřuje, jestli osoba test úspěšně zvládla. Pokud ano, pokračujeme na následující oblast školení, pokud ne, musí se o zvládnutí testu podstoupit znovu. Ve stejném duchu se pokračuje s následujícími oblastmi. Jakmile osoba úspěšně složila test znalostí ze školení, údaj o úspěšném absolvování školení se zaznamená do databáze a začne se plynout lhůta 180 dní, po kterou je školení platné.

Ostatní oblasti uživatelů, tedy pokročilí, externisté a zaměstnanci výroby absolvují naprosto stejný postup, který je uvedený výše, pouze s tím rozdílem, že oblastí školení je méně. U pokročilých uživatelů to jsou oblasti Aplikace, Bezpečnost zaměstnanců a Bezpečnost v síti. U externích zaměstnanců podniku je nutné absolvovat školení v oblastech Bezpečnost zaměstnanců a Bezpečnost v síti. Poslední skupinou uživatelů jsou pracovníci ve výrobních prostorách, kteří musí jednou za půl roku absolvovat školení Bezpečnost zaměstnanců. Vývojový diagram znázorňující postup při školení uživatelů se nachází na následující straně.



Obrázek 8 – Vývojový diagram školení uživatelů (vlastní zpracování)

Po zvládnutí posledního ověření znalostí se do databáze školení zapíše datum, čas, evidenční číslo zaměstnance, jméno, příjmení a oblasti školení dané osoby. Na obr. 9 je uveden návrh webové stránky, tedy část fyzického datového modelu, kde zaměstnanec zjistí, které školení je nutné absolvovat a jeho časovou náročnost. Po přihlášení na webu www.podnik.cz/skolenizamestnance se zobrazí role uživatele, do které je přihlášen. Kliknutím na oblast Aplikace se odstartuje školicí proces v časovém limitu, který je uveden na obrázku níže. Automaticky se poté oblasti školení přepínají v závislosti na zvládnutí požadovaného testu při úspěšnosti minimálně 70 %, což je hranice určena managementem společnosti.



Obrázek 9 – Webová stránka – Školení zaměstnanců (vlastní zpracování)

5.2 Zálohování dat

Zálohování dat společnosti je velmi důležitou funkcí, která zajišťuje opětovný přístup k daným datům v případě výpadku. Nemožnost přístupu k datům z důvodu poškození či ztráty může mít pro podnik fatální následky v závislosti na druhu dat. V diagramu viz. obr.10 je graficky znázorněn logický proces zálohování dat v závislosti na jejich typu a časovém intervalu. Jednotlivá data, která podléhají zálohování byla rozdělena do třech základních

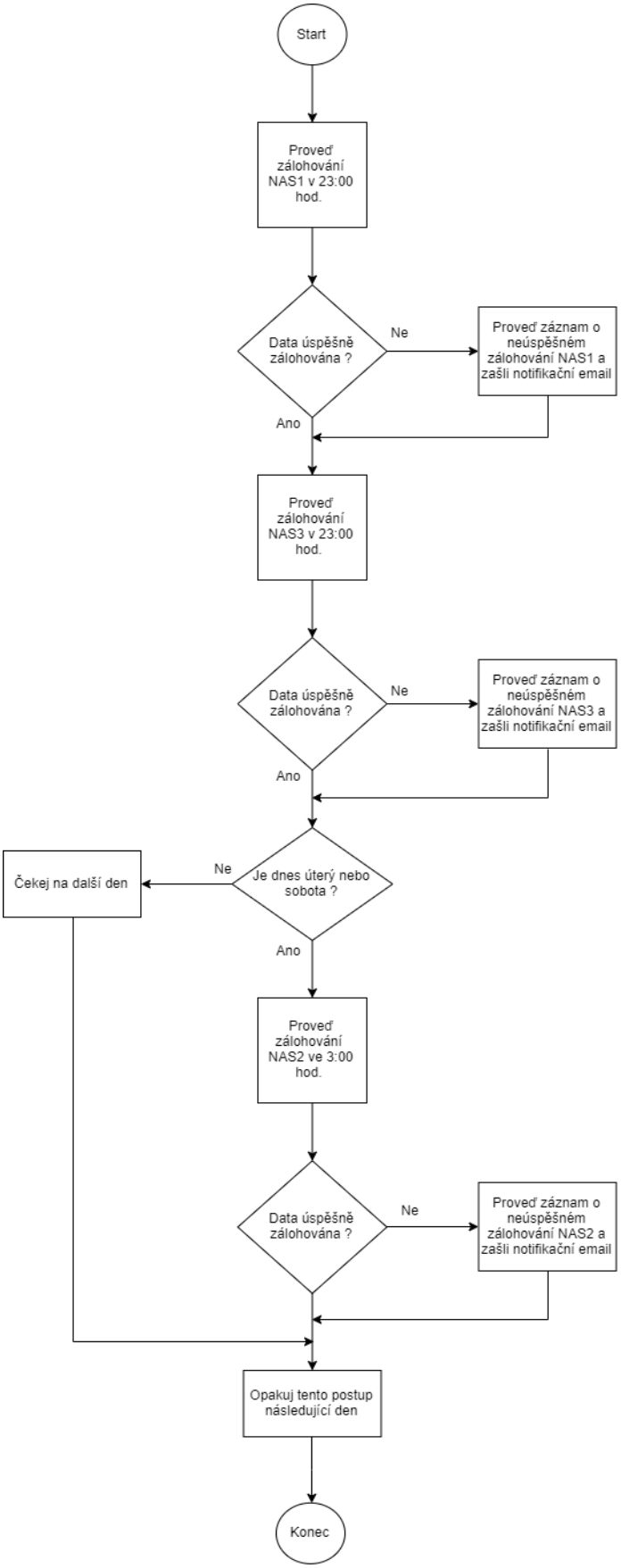
skupin: DATA1, DATA2 a DATA3, a to také z důvodu, že každé uložiště NAS bude umístěno v jiné budově, tak aby při vzniku mimořádné události např. v administrativní budově, neztratil podnik všechna data. Rozmístěním NAS do tří budov je zajištěno, že vždy budou k dispozici zálohovaná data. V podniku budou data zálohována ve třech různých časových intervalech:

- **NAS1**, denní zálohování v 18 hod., udržitelnost zálohy 20 dnů
- **NAS2**, zálohování úterý a sobota, vždy ve 3 hod., udržitelnost zálohy 3 dny
- **NAS3**, denní zálohování ve 23 hod., udržitelnost zálohy 180 dnů

Dvě zálohování pojmenovaná NAS1 a NAS3 jsou prováděna denně, záloha NAS2 se provádí dvakrát týdně. V tab. 14 je přehledně znázorněno, která data jsou kdy zálohována, včetně informace o časové udržitelnosti zálohy.

Tabulka 14 – Rozdělení zálohování (vlastní zpracování)

	NAS1	NAS2	NAS3
DATA1	•	•	•
DATA2	•	•	
DATA3	•		•



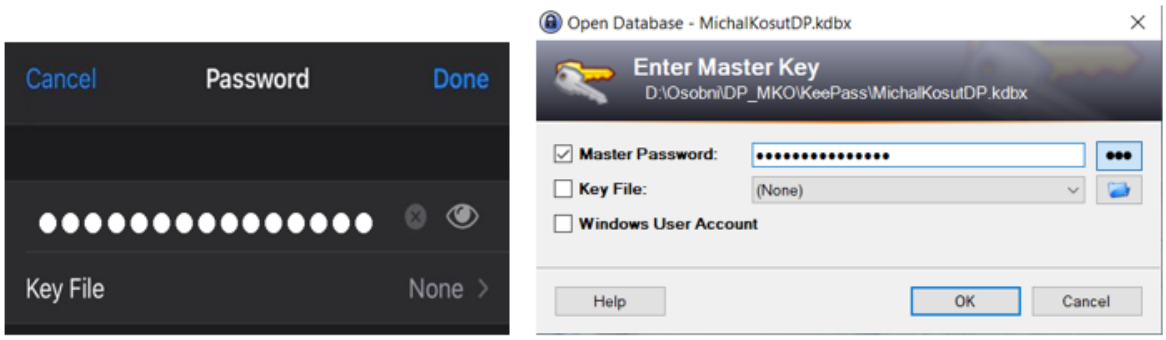
Obrázek 10 – Vývojový diagram – Zálohování (vlastní zpracování)

5.3 Zabezpečení hesel aplikací KeePass

K minimalizaci nabourání se neoprávněné osoby do účtu uživatele podniku pomocí odcizení nebo zkopírování hesla (např. emailové schránky, internetu, firemní sítě atd.) bude použita aplikace KeePass. Vzhledem k podrobnému zkoumání a porovnávání podobných aplikací, kde hlavní roli sehrály faktory jako: dostupnost, přehlednost, funkcionalita, uživatelské rozhraní, ovladatelnost a podobně, byla ze skupiny čtyř různých aplikací vybrána aplikace KeePass. Princip fungování je velmi jednoduchý. Vzhledem k dnešní povaze internetu a aplikací, kdy lidé mají mnoho přihlašovacích údajů a hesel do různých míst, byla vybrána aplikace, která ulehčuje práci s hesly a minimalizuje možnost jejich zapomenutí. Ocenitelnou funkcí softwaru je možnost generovat náhodné heslo dle zadaných bezpečnostních kritérií. Jak KeePass Touch funguje? Tato kapitola znázorňuje nejprve grafické rozhraní v mobilní aplikaci a následně v operačním systému Windows. Software je volně ke stažení jako mobilní aplikace na Google Play a AppStore, pro operační systém Windows na odkazu: https://keepass.info/

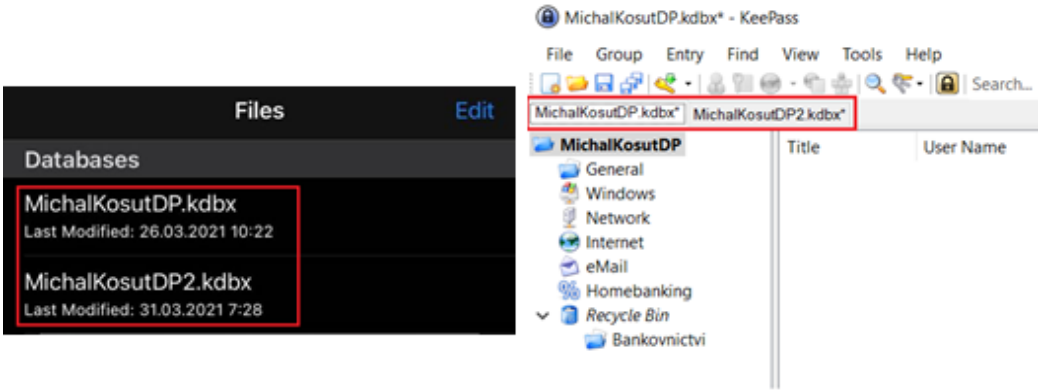
Obrázek 11 – Loga aplikace KeePass (vlastní zpracování)

Prvním krokem po spuštění aplikace je zadání prvotního, silného hesla, které musí obsahovat velká a malá písmena, číslice a znaky. Požadovaná délka je minimálně 10 znaků, avšak může být i více. Obr. 12 znázorňuje první krok – přihlášení do aplikace.



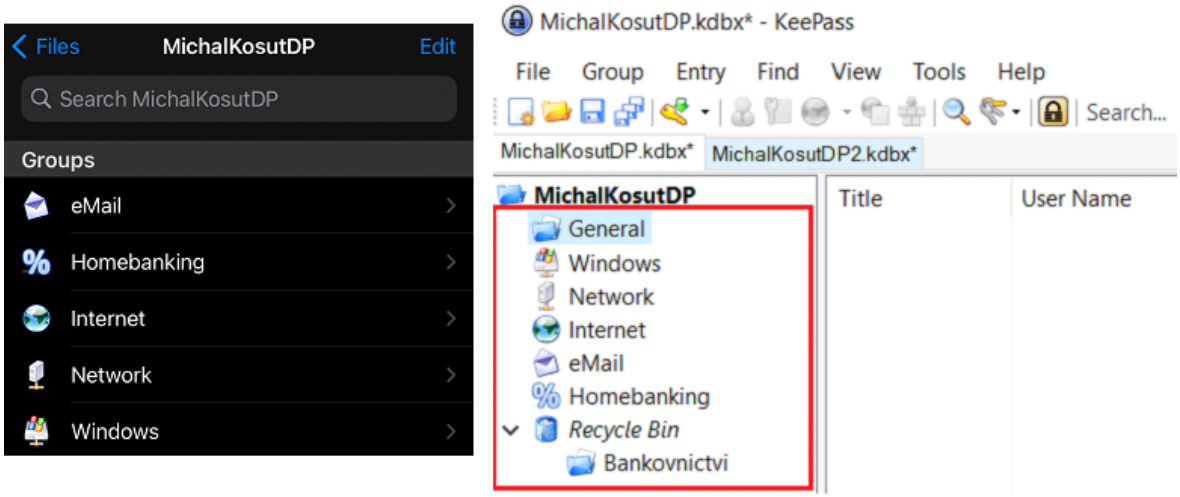
Obrázek 12 – Přihlášení do aplikace (vlastní zpracování)

Po zadání prvotního hesla se nám zobrazí dostupné databáze. Pro případ diplomové práce si autor vybral a nazval dvě databáze MichalKosutDP a MichalKosutDP2. Na obr. 13, je uvedeno grafické zpracování v mobilní aplikaci a programu pro operační software Windows



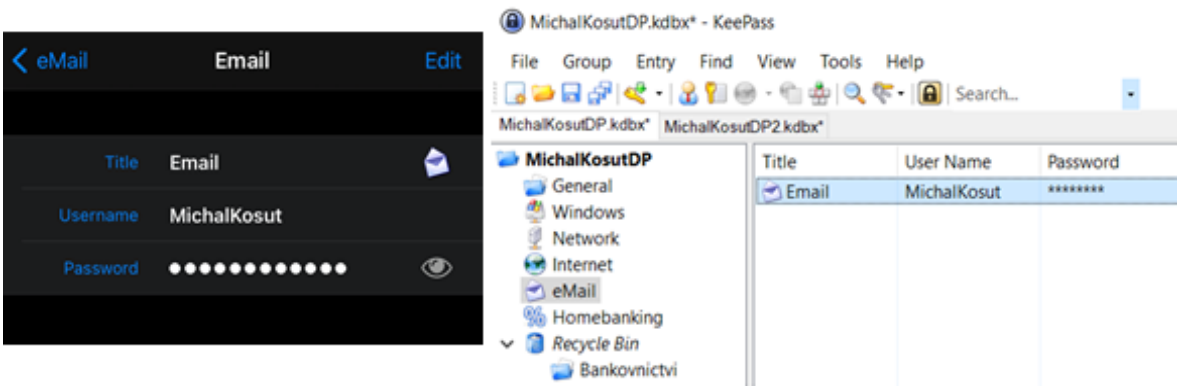
Obrázek 13 – Databáze v aplikaci KeePass (vlastní zpracování)

Po přihlášení do své databáze viz. obr. 14, se osoba dostane do prostředí, ve kterém si může nastavit různé oblasti a místa, do kterých se přihlašuje, například internetové bankovnictví, heslo k počítači, heslo do firemní sítě, heslo k emailové poště atd.



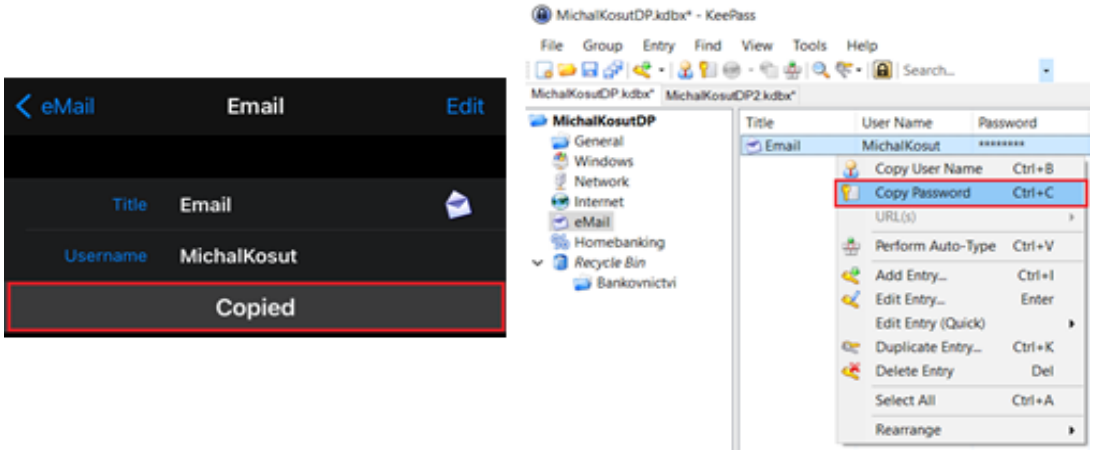
Obrázek 14 – Prostředí aplikace KeePass (vlastní zpracování)

Výhodou a hlavním přínosem aplikace je tento moment, kdy můžeme mít několik různých hesel do několika různých oblastí, ale stačí nám pamatovat si pouze jedno – počáteční velmi kvalitní a silné heslo pro přístup do aplikace KeePass. Pokud klikneme na první položku „eMail“, zobrazí se nám informační údaje s heslem ve skryté podobě, pokud je nutné si heslo připomenout, klikneme na ikonu vedle hesla a heslo se zobrazí, viz. obr. 15.



Obrázek 15 – Přihlášení do aplikace (vlastní zpracování)

V momentě, kdy klikneme na bílé tečky, je heslo zkopírováno do schránky. Následně se přesuneme do emailového klienta, kde zkratkou CTRL+V heslo vložíme. Druhou, pomalejší variantou je přepisování jednotlivých znaků daného hesla. V programu KeePass v operačním systému Windows se heslo zkopíruje kliknutím pravým tlačítkem myši a vybráním položky „Kopírovat“ viz. obr. 16.



Obrázek 16 – Práce s heslem (vlastní zpracování)

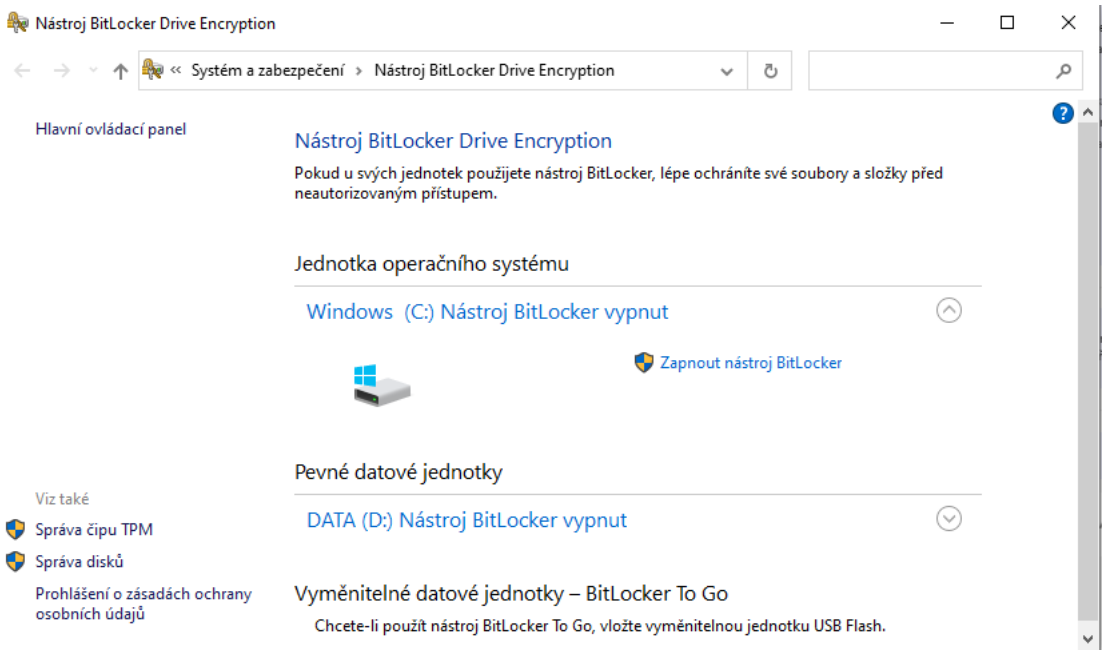
Dle výše uvedeného postupu je možné aplikaci KeePass používat pro všechny oblasti, které jsme si v mobilní aplikaci a Windows vytvořili. Hlavním přínosem aplikace je eliminace hrozby ztráty či zapomenutí hesla a také minimalizace možnosti přístupu neoprávněné osoby. Management podniku rozhodl, že všichni uživatelé disponující pracovními PC stanicemi musí tento formát aplikace používat povinně na firemní úrovni. Používání aplikace na osobní úrovni pro přístup k osobním entitám nebude po zaměstnancích z hlediska podniku vyžadováno.

5.4 Zabezpečení pomocí TPM čipu a nástroje BitLocker

Vzhledem k možné ztrátě firemního notebooku, či vysokému riziku jeho odcizení a získání tak firemních citlivých dat nebo osobních údajů, bylo managementem společnosti nařízeno všem uživatelům disponující firemním notebookem, aktivace čipu TPM a nástroje BitLocker, viz. obr. 17.

Pokud by došlo ke ztrátě přenosného PC, musela by tato skutečnost být v souvislosti s nařízením GDPR ohlášena na Úřad pro ochranu osobních údajů, což by znamenalo významné komplikace. Aktivací TPM čipu můžeme charakterizovat jako kvalitní a přínosnou záležitost. Software totiž šifruje úložiště v notebooku – tzv. harddisk (pevný disk), na kterém jsou uložena veškerá data. Operační systém Windows nabízí BitLocker zdarma v rámci systému. Zkratka TPM představuje anglická slova Trusted Platform Module, volně přeloženo jako „Modul ověřené platformy“ a v praxi jde o modul, resp. čip, který generuje a ukládá kryptografické klíče. BitLocker používá TPM k ochraně klíčů, které jsou používány k zašifrování pevných disků a také poskytuje ověřování integrity.

Samotný BitLocker je technologie, která šifruje disky – jak již bylo zmíněno, na operačních systémech Windows je zdarma. Dokáže šifrovat kompletní systémové i nesystémové oddíly, ale i přenosná úložiště jako například externí harddisky, USB flash disky a podobně (BitLocker – Šifrování systémových disků, 2021)



Obrázek 17 – Aktivace BitLockeru (BitLocker – Šifrování systémových disků, 2021)

5.5 Návrh klasifikace informací v prostředí podniku

Počátečním úkolem klasifikace informací je zajištění ochrany informací, které musí být klasifikovány dle jejich důležitosti pro zabezpečení chodu podniku. V podniku bude všem informacím, přiřazen stupeň důvěrnosti dle protokolu TLP, uvedeném v teoretické části práce bodě 3.2. Za správnou klasifikaci aktiv je plně odpovědný vlastník aktiva, což může být autor, původce či zhotovitel informace. Důležitost ochrany a stupeň klasifikace exaktně stanovuje pravidla pro zacházení a nakládání s informacemi podniku. Z důvodu nutnosti chránit informace byla stanovena pravidla upřesňující zacházení s informacemi v počítačích, sítích, serverech, systémech, aplikacích, emailech a poštovní komunikaci. Tato pravidla se vztahují na všechny zaměstnance podniku, dodavatele, konzultanty a pracovníky na dohodu o provedení práce. Existují dva možné způsoby klasifikace informací. První varianta je uvedena níže v tab. 15, kdy jednotlivé dokumenty jsou označovány dle TLP. Druhou variantou je, že je stanovena klasifikace informací, ale dokumenty nejsou označovány, a to z toho důvodu, že pokud by neoprávněná osoba přišla do styku s chráněným dokumentem, který je takto označen, tato osoba se začne o dokument intenzivně zajímat a může ho odcizit. Pokud by dokument nebyl barevně označen, neoprávněná osoba na první pohled nezjistí, že se jedná o chráněný dokument a nebude si jej všímat. Management podniku se bude muset rozhodnout, kterou variantu využije.

Všechny informace musí být rozděleny do následujících čtyř kategorií citlivosti:

- Chráněné – vztahuje se na nejcitlivější obchodní informace, které jsou určeny k použití pouze v rámci podniku. Vyzrazení chráněné informace by mohlo mít vážný a nepříznivý dopad na podnik, jeho zákazníky, obchodní partnery a dodavatele.
- Citlivé – vztahuje se na méně citlivé obchodní informace, které jsou určeny k použití pouze v rámci podniku. Vyzrazení citlivé informace by mohlo nepříznivě ovlivnit podnik, jeho zákazníky, obchodní partnery a dodavatele.
- Interní – vztahuje se na informace, které nepatří do dvou výše uvedených skupin, přesto jejich vyzrazení může způsobit méně závažné ovlivnění podniku, jeho zákazníků, obchodních partnerů a dodavatelů
- Veřejné – jsou informace určené pro veřejné zveřejnění, kdy jejich šíření nepředstavuje žádnou újmu.

Tabulka 15 – TLP (Traffic light protocol, 2021, upraveno autorem)

Úroveň	**Veřejné**	**Interní**	**Citlivé**	**Chráněné**
Barva	**Bílá**	**Zelená**	**Žlutá**	**Červená**
Kdy použít	Informace neobsahují žádné předvídatelné riziko zneužití v rámci platných pravidel a postupů	Pro zvýšení informovanosti všech zúčastněných organizací	V případě, kdy informace vyžadují efektivní reakci dalších jednotlivců a přináší jisté riziko pro podnik, pověst a v případě sdílení mino podnik	V případě, kdy by mohlo dojít k dopadům na podnik, jeho pověst nebo zneužití
Možnosti sdílení	V souladu se stanovenými pravidly je možná distribuce bez omezení	Je možné sdílet se zákazníky a partnery, nikoliv však veřejně dostupnými kanály	Sdílení je možné v rámci podniku a zákazníky, kteří potřebují informace znát	Pouze v rámci jednotlivců konkrétní výměny či schůzky, pouze verbálně nebo osobně
Uložení dokumentů tisk / elektronicky	Standardně na určených místech / na disku osobního PC a flash disku.	V uzamčené kanceláři a dodržení pravidla čistého stolu / na souborovém serveru v určených složkách nebo disku osobního PC.	Musí být uloženy v uzamykatelných nábytkových skříňkách / na souborovém serveru v určených složkách.	Musí být uloženy v trezoru nebo místnosti pro dané účely s řízeným přístupem / je umožněno ve složkách k tomu určených. Tyto složky mají v názvu znak $, např. \\a-03\zaloha$, kdy je tato složka pro uživatele bez oprávnění neviditelná.
Kopírování tisk / elektronicky	Bez omezení pro pracovní účely.	Pouze pro pracovní účely / pouze v rámci souborového serveru a disku osobního PC.	Pouze pro pracovní účely / pouze v rámci souborového serveru.	Může pouze autorizovaná osoba pro seznámení se s dokumentem. Dokument nesmí být při kopírování ponechán bez dohledu / zakázáno
Distribuce tisk / elektronicky	V zalepené obálce / bez omezení.	V zalepené obálce doporučeně, klasifikace je uvedena uvnitř dokumentu / pouze v rámci podniku mezi zaměstnanci a současně označení v předmětu zprávy	V zalepené obálce doporučeně, klasifikace je uvedena uvnitř dokumentu / pouze osobám určeným pro seznámení se s dokumentem, označení v předmětu zprávy	Pouze seznamu osob určených pro seznámení se s dokumentem, klasifikace je uvedena uvnitř dokumentu.
Zveřejnění	Neomezené zveřejnění	Omezené zveřejnění jen v organizaci účastníků	Omezené zveřejnění	Pouze pro dané účastníky, nezveřejňovat
Příklad	VOP, tiskové zprávy, inzeráty, reklamní letáky.	Školící materiály pro zaměstnance, SoD, účetní sestavy, marketingové zprávy atd.	Mzdové údaje, bankovní zprávy, zásady IT, interní audity, pracovní smlouvy, údaje o zákaznících, slevy atd.	Výrobní dokumentace, technologické postupy, ekonomické analýzy, strategické plány podniku, dokumenty o fúzi atd.

6 ZJEDNODUŠENÝ NÁVRH BEZPEČNOSTNÍ POLITIKY INFORMAČNÍHO SYSTÉMU PRO POTŘEBY UŽIVATELŮ

Účelem tohoto dokumentu je zjednodušený úvod do problematiky BPIS a pokyny pro její dodržování určený pro potřeby uživatelů podniku.

V dnešní hektické době jsou moderní technologie natolik nedílně spojené s naším životem, až lze snadno zapomenout, že jejich používáním se vystavujeme riziku. Proto je ochrana IS a veškerého jeho obsahu právě tak zásadní jako uzamčení dveří, když odcházíte z domova. Chceme zaměstnancům tímto pomoci při osvojení bezpečnosti IS a způsobů, jimiž uchovávají svá zařízení, informace a data v bezpečí.

IT bezpečnost, známá také jako kybernetická bezpečnost, znamená proces a techniky, které se podílejí na ochraně citlivých dat, výpočetních systémů, sítí a aplikačního softwaru před kybernetickými útoky. Kybernetický útok je obecný termín, který může označovat:

- Neoprávněnou manipulaci se systémy a daty v nich uloženými.
- Zneužití zdrojů.
- Získání neoprávněného přístupu do určitého systémů a přístupu k citlivým údajům.
- Narušitelské zastavení normálního chodu podnikových činností a souvisejících procesů.
- Použití útoků Ransomwaru k zašifrování dat a k vymáhání finančních prostředků od poškozených.

Na úvod je třeba se seznámit všechny pracovníky a uživatele systému se škálou existujících hrozeb:

- **Viry a malware** – škodlivý software, vyvinutý tak, aby poškodil váš počítač.
- **Ransomware** – druh škodlivého softwaru, který dokáže zašifrovat vaše soubory a vymáhat od vás „výkupné“ (ransom) čili peníze za obnovení přístupu k vašim informacím.
- **Phishing** – forma internetového podvodu, při němž obdržíte e-mail předstírající, že jeho původcem je poskytovatel IT služeb nebo jiný důvěryhodný zdroj. Zpráva v e-mailu od vás může požadovat, abyste „ověřili“ nebo „potvrdili“ údaje ke svému účtu tím, že se přihlásíte k podvodným webovým stránkám.
- **E-mailový spam** – někdy také označovaný jako reklamní pošta, ale přesněji jde o nevyžádané e-maily. Většina spamů má komerční povahu, mohou ale také

obsahovat odkazy vedoucí na phishingové stránky nebo na webové stránky hostující malware.

Vedení podniku považuje za důležité, aby všichni uživatelé IS sami přispěli k udržování bezpečného stavu podnikové sítě a IS tím, že budou dbát na svou informovanost a na efektivní využívání nástrojů, které jsou k dispozici.

6.1 Zabezpečení technických prvků

V kapitole zabezpečení technických prvků hovoříme zejména o fyzických zařízeních (hardware) technického směru i softwaru, například následující podkapitola počítačová síť, nebo přístupy uživatelů a GDPR.

6.1.1 Počítačová síť

V podniku jsou instalovány dvě fyzicky oddělené sítě, které jsou realizovány strukturovanou kabeláží CAT5e. Jednotlivé budovy jsou propojeny optickým kabelem stejně jako připojení k internetu.

První je počítačová síť a druhou síť využívá přístupový, docházkový, stravovací a kamerový systém, který je ve správě určeného technika servisu. V podniku jsou dále zprovozněny čtyři wifi sítě. Veřejně přístupná WIFI pod názvem VISITOR je přístupná bez hesla, avšak omezená datovým tokem a rozsahem dostupnosti pouze v lokalitě 1.NP administrativní budovy. Veřejně přístupná WIFI pod názvem VISITOR 2 je přístupná pouze s validním heslem a je určená pro VIP klienty a akcionáře podniku, kteří nemají přístup do sítě přes doménový účet. Podniková šifrovaná WIFI síť pod názvem ABC-ADMIN s dosahem po administrativní budově. Za správnost nastavení odpovídá Manager IT a externí správce IT. Podniková šifrovaná WIFI síť se skrytým názvem – Výroba s pokrytím na Hale B, je určena pro testování a vývoj produktů společnosti střediskem vývoje HW-T. Nevyužité zásuvky strukturované kabeláže jsou neaktivní, což zamezí náhodnému zneužití sítě LAN.

6.1.2 Server, Serverovna

Server je zařízení, na kterém funguje operační systém určený pro síťové prostředí. Server je umístěn ve druhém podlaží administrativní budovy. Jedná se o samostatnou místnost, do které je umožněn přístup pouze manager IT a externímu správci IT v doprovodu managera IT. V serverovně jsou instalovány dvě klimatizační jednotky, a to pro případnou poruchu jedné z nich. Jsou zde současně umístěny řídící jednotky ACS, ústředna PZTS a telefonní ústředna.

6.1.3 Kancelářská technika

Jedná se především o pevné koncové desktopové počítačové stanice vč. monitorů, za které je odpovědný zaměstnanec, jemuž bylo příslušné zařízení přiděleno.

6.1.4 Přenosná technika

Zabezpečení a bezpečnost veškeré přenosné techniky notepadů, laptopů, mobilních telefonů apod. je odpovědností zaměstnance, jemuž bylo příslušné zařízení přiděleno.

6.1.5 Sdílené disky

Sdílené disky jsou umístěny v serverovně a jsou uživatelům dostupné pod názvy: Disk Podnik\01-W slouží jako File Server, tedy disk pro uložení podnikových dokumentů jako jsou např. informace o jednotlivých produktech, manuály, POS, schémata, Firmware, technologické postupy, výrobní dokumentace a další interní dokumenty. Disk Podnik\01-O\ je určen pro individuální potřebu uživatelů, kde si ukládají rozpracované úkoly atd.

Firemní informace společnosti smějí být uchovávány výhradně na úložištích IT služeb, které jsou buď zabezpečovány útvarem IT nebo na které tento útvar přesměrovává, tedy např. u služeb podniku OneDrive, SharePoint nebo na sdílených firemních diskových jednotkách.

Je striktně zakázáno ukládat firemní informace u jiných služeb poskytujících úložiště souborů na internetu, jako jsou například (aniž je tento výčet úplný) Dropbox, Google Drive, iCloud a osobní nefiremní služba OneDrive.

6.1.6 Paměťová média

Uživatelé v podniku mohou používat pouze přenosné disky taktéž nazývané flash disky vydané manažerem IT, na kterých je nastaveno šifrování. Tyto disky je zakázáno připojovat k cizím zařízením. Před použitím musí být vždy zkontrolovány antivirovým programem.

6.1.7 Ochrana před poškozením a odcizením

Každý zaměstnanec je povinen uplatňovat odpovídající a doporučené metody zabezpečení daného zařízení a zajistit tak, aby svěřený majetek byl neustále uchováván v bezpečí a tím bylo chráněno zabezpečení majetku.

6.2 Personální Bezpečnostní politika

Podstatné je určení rolí pro minimalizaci rizik vyplývající z hrozeb všech interních tak externích uživatelů přistupujících do IS.

6.2.1 Role

Definování jednotlivých rolí podniku je následující:

- Top management
- Ředitelé středisek
- Manager bezpečnosti
- Manager IT
- Uživatelé IS
- Externí správci systému

6.2.2 Zabezpečení přístupu uživatele

Každému zaměstnanci musí být přiděleny jednoznačné identifikační údaje pro přístup. Není dovoleno používat anonymní nebo skupinovou identifikaci, není povoleno, aby některé pracoviště mělo obecné přihlašovací údaje pro všechny zaměstnance. Každý zaměstnanec musí mít své vlastní identifikační a přihlašovací údaje.

- Všichni zaměstnanci musí mít pro přístup zvoleno heslo, které se řídí standardem pro správu hesel.
- Uživatelé s privilegovaným povolením pro vzdálený přístup musí při použití vzdáleného přístupu dodržovat uvedené povinnosti uvedené standardy správy hesel.

6.2.3 Vznik a ukončení pracovního poměru

Při vzniku pracovního poměru musí být nadřízeným pracovníkem, ředitelem střediska, vyplněn formulář Průvodce nového zaměstnance uloženého na intranetu podniku. Uživatelé IS musí být před udělením přístupu do IS prokazatelně seznámeni a proškoleni s celkovou BPIS. Školení musí být zaměřeno na bezpečnostní pravidla, zásady a navazující bezpečnostní dokumentaci. Evidence záznamů provedených školení zaměstnanců jsou uložena na personálním oddělení, evidence záznamů provedených školení pracovníků třetích stran je uložena u managera bezpečnosti.

Při ukončení pracovního poměru je pracovník povinen nejpozději v den ukončení pracovního poměru předat veškeré dokumenty, písemnosti, data, informace a pracovní prostředky řediteli střediska. O předání bude vždy provedený záznam na formuláři uloženém na intranetu podniku, kde je stanoveno, komu a co pracovník předává. Za zrušení uživatelských oprávnění v IS je odpovědný ředitel střediska, který informuje dotčené interní i externí pracovníky, čímž jsou dané osobě odebrána přístupová oprávnění.

6.2.4 Standardy správy hesel

Uživatelé jsou povinni své heslo nikomu nesdělit, neprozradit a udržovat v tajnosti. Heslo je nutné měnit minimálně jednou ročně, heslo nesmí být použito stejné nebo jeho verzováním, kdy by byla změněna např. pouze číslice. Je zakázáno hesla zaznamenávat na monitorech, telefonech, PC stanicích, kancelářském vybavení atd. Pokud je heslo zapomenuto, manager IT zajistí přidělení nového hesla. Uživatelská hesla se při zadávání nesmí zobrazovat jako prostý text.

Uživatelské účty musí být uzamčeny po třech neúspěšných pokusech o přihlášení. Jakmile má uživatel uzamčen svůj účet, pro odemknutí účtu kontaktuje Managera IT.

Uživatelé přistupující do IS se vždy identifikují uživatelským jménem a heslem, které musí splňovat min. tři ze čtyř parametrů a administrátoři přistupující do IS se vždy identifikují uživatelským jménem a heslem, které musí splňovat čtyři ze čtyř následujících parametrů:

- Počet znaků min. 8.
- Min. jednu číslici (0 až 9).
- Speciální znak (*, +, -, /, @, #, %).
- Malé písmeno (a až z).
- Velké písmeno (A až Z).

Jako hesla je zakázáno používat jména rodinných příslušníků či jména uživatelů. Pokud uživatel heslo obnovuje musí se nové heslo lišit min čtyřmi znaky od předchozího hesla.

6.2.5 Ochrana osobních údajů

Vedení podniku si nadmíru uvědomuje důležitost ochrany osobních údajů, které shromažďuje nebo uchovává u zaměstnanců, zákazníků, dodavatelů a dalších osob, s nimiž komunikuje prostřednictvím služeb, které podnik poskytuje.

Všichni zaměstnanci musí být minimálně 1 x ročně školeni v oblasti GDPR a ochrany osobních údajů. Je zakázáno uchovávat údaje o:

- Sexuální orientaci.
- Duševním a fyzickém zdraví.
- Náboženství.
- Politické příslušnosti.

V rámci programu GDPR budou smluvní vztahy pravidelně aktualizovány tak, aby bylo dosaženo dodržování nových povinností stanovených příslušnými zákony a vyhláškami upravující vztah mezi správci údajů a zpracovateli údajů. Tím bude zajištěno dodržování smluvních ustanovení na straně podniku i zákazníků.

6.3 Řízení komunikací a provozu

Zabezpečení objektů, předmětů, subjektů zajištující komunikaci řeší politika řízení komunikací a provozu. Vztahuje se na servery, koncové stanice, mobilní zařízení vybavené poštovním klientem Outlook a internetovým prohlížečem a dalšími prostředky v podnikové síti.

6.3.1 Ochrana pře škodlivým software

Ochrana před škodlivým SW je zabezpečována na úrovni firewallu. Ochrana před škodlivým kódem na úrovni rozhraní vnitřní a vnější sítě je založena na antivirovém nástroji, firewallu a IDSPS. Aktualizace serverů a pracovních stanic bude pomocí služeb nástrojů automatizovaná dle předpisů výrobců a budou nastaveny komunikační kanály emailem na administrátory uvedených služeb. Logování systému činností a událostí u vybraných informačních a komunikačních technologiích (dále jen “ICT“) aktiv bude prováděno např. nástrojem LOG manager.

6.3.2 Evidence aktiv a správa licencí SW produktů

Pro účinnou správu aktiv je nevyhnutelné udržovat aktuální přehled aktiv a instalovaného SW. Manager IT k tomuto účelu může využit některý z dostupných SW nástrojů. Administrátor systému nastavuje omezení uživatelských práv koncových uživatelů systému tak, aby nebylo umožněno uživatelům svévolně instalovat SW.

6.3.3 Vyřazení a likvidace nosičů dat

Data uložená na pevných discích pracovních stanic jsou na konci svého životního cyklu vymazána a předána k jejich fyzické a ekologické likvidaci smluvnímu partnerovi. Listinné nosiče informací jsou vyřazovány a likvidovány skartací nebo smluvním partnerem.

6.3.4 Datová schránka

Přístup do datové schránky má pouze pověřený zaměstnanec, tedy konkrétně pracovnice sekretariátu, která přijaté zprávy dále přeposílá pomocí emailu odpovědným osobám. Uživatele je nutné pravidelně školit, jakým způsobem je možné se zprávami z datové schránky pracovat a jakým způsobem je možné zprávy odesílat.

6.3.5 Fyzická pošta

Za evidenci fyzické pošty je odpovědný pověřený pracovník obchodního oddělení, který vede evidenci pošty a odpovídá za následující:

- Zápis přijaté pošty do deníku vč. informací o odesílateli, a základních údajů o zásilce.
- Zápis do deníku pošty odesílaných zásilek vč. informací o adresátovi a základních informací o zásilce.
- Odesílání poštovních zásilek.
- Zajištění přepravy rozměrných zásilek.
- Řešení celních doložek pro zásilky zasílané do zahraničí.
- Předání packing listu zákazníkům.

6.4 Provozní bezpečnostní politika

6.4.1 Politika zálohování

Zálohování dat je jeden z nejdůležitějších procesů, který nesmí být opomenut. V případě zničení, poškození nebo ztráty dat budou tyto obnoveny ze záložních disků. Bohužel se stává, že při obnovení dat dochází ke ztrátám uložených dat, která byla vytvořena od posledního provedené zálohy, proto je důležité, aby uživatelé svá data zálohovali pravidelně na konci pracovního dne. Data uložená na sdílených discích a serverech budou zálohovaná pravidelně každý den ve 23:00 hod.

6.4.2 Havarijní plán

Účelem havarijního plánu je poskytnout podporu řídícím pracovníkům formou typových plánů a podpůrných informací. Řídící pracovníci musí mít kopii tohoto pokynu uloženou na pevném disku své pracovní stanice, a to pro případ vyhlášení kritického stavu a nedostupnosti služeb ICT, kdy v počáteční komunikace mezi řídícími pracovníky a dalšími uživateli bude možná pouze telefonním spojením nebo formou SMS. Při vyhlášení krizového stavu je nutné zaznamenat následující informace:

- Datum a čas vzniku krizového stavu.
- Rozsah krizového stavu.
- Časový odhad obnovy.
- Datum a čas posledních datových záloh.

Na základě výše uvedených informací rozhodne krizový štáb o dalším postupu a informuje všechny vedoucí pracovníky a následně všechny zaměstnance o vzniku krizového stavu a dalším postupu. Krizový štáb svolává ředitel společnosti.

6.4.3 Řízení kontinuity činností

Záměrem plánu řízení kontinuity činností po narušení IS a ICT je překlenout krizový stav, který může nastat neočekávaně, a to i přes veškerá implementovaná opatření, přechodem na nouzový stav a současně obnova služeb ICT a dosažení normální stavu chodu podniku.

Rozeznáváme dva základní stavy:

- Normální stav – funkčnost všech služeb není omezena neplánovaným narušením či nedostupností.
- Krizový stav – je takový stav, kdy došlo k nepředvídané události, která dlouhodobě a zásadním způsobem ovlivňuje a omezuje činnosti podniku.

Základním požadavkem na systém řízení kontinuity činností je dokumentace systému, stanovení pravidel, stanovení organizační struktury, vytvoření realizačních týmů, stanovení jednotlivých kroků a postupů pro zvládnutí krizového stavu a aktualizace a proces zlepšování funkčnosti.

Návodem pro vyhlášení krizového stavu je rozhodující rozsah nedostupnosti služeb ICT a IS v daném časovém horizontu, kdy současně odhad času na obnovu jejich dostupnosti přesahuje 1 pracovní den. Na plán řízení kontinuity činností přímo navazuje plán obnovy.

6.4.4 Plán obnovy

Stanovuje postupy obnovy ICT a IS prostředků pro obnovení chodu narušených služeb v podniku. Za vytvoření, pravidelné aktualizace a uložení těchto plánů je odpovědný manager IT. Tyto plány spadají do klasifikace „Citlivé“ s omezením okruhu pracovníků, kteří jsou s dokumenty seznamováni. Pro plán obnovy musí být vytvořeny následující plány:

- Plán reakce na krizové situace.
- Plán nástupnictví – popis odpovědnosti v případě kdy zaměstnanci nemohou plnit své povinnosti.
- Datová studie – popis dat uložených v systému a jejich důvěrnost.
- Kritičnost služeb – plán obnovy v krátkodobém i dlouhodobém výhledu.
- Plán zálohování – která data jsou nebo nejsou zálohována, kde jsou zálohy uloženy, jak často je zálohování prováděno.
- Plán obnovy dat – popis obnovy dat ze zálohy.
- Plán výměny HW – popis HW nutného k výměně, uvedení pořadí výměny.

Po vytvoření plánu obnovy je důležité tyto plány otestovat v praxi a zjistit, zdali jsou proveditelně, případně zajistit nápravu. Testování musí probíhat minimálně v intervalu 1 x ročně.

6.4.5 Hlášení incidentů

Všichni zaměstnanci, pracovníci a dodavatelé jsou povinni jakýkoli bezpečnostní incident nebo jen jeho podezření hlásit emailem a adresu IT @podnik.cz, nebo telefonicky managerovi IT. V případě nedostupnosti managera IT hlásí pracovníci incident svému přímému nadřízenému.

V případě že se jedná o incident týkající se osobních údajů, jsou tyto incidenty hlášeny pověřenci OÚ na emailovou adresu GDPR@podnik.cz. Postup pro zvládání bezpečnostních incidentů:

- Reakce – přijetí opatření eliminaci a likvidaci následků,
- Analýza opatření, tak aby se incident nevyskytl na jiném místě, přezkoumání incidentu, určení příčin.
- Provedení nápravných opatření.
- Přezkum účinnosti.
- Návrh na změny a zlepšení.

6.5 Monitoring a přezkoumání

V kapitole monitoring a přezkoumání klademe důraz na kontrolu a dohled nad nastavenými opatřeními tak, aby bylo dosaženo stanovených priorit. Lze tedy hovořit o nastavení podmínek a opatření, které je následně nutné dodržovat a jejich dodržování kontrolovat.

6.5.1 Monitorování

Postup monitorování stavu plnění BPIS, záznam a vyhodnocení sledovaných parametrů je nevyhnutelný pro zajištění úrovně účinnosti přijatých opatření a jejich porovnání s požadovanými hodnotami. Pro zjišťování a měření účinnosti byla stanovena následující kritéria:

- Zajištění dostupnosti služeb.
- Zabránění úniku citlivých informací.
- Zajištění integrity dat.
- Zajištění klasifikace informací.
- Předejití nebo včasné zachycení kybernetických útoků.

Pro kritéria byly stanoveny následující parametry:

- Dostupnost IS v minimální hodnotě 99 % ve standardní pracovní době 8:00 – 16:00 v rámci jednoho měsíce s výjimkou předem naplánovaných a ohlášených odstávek systému.
- Bez úniku Chráněních, Interních a Citlivých informací
- Bez kybernetických útoků.
- Zajištění obnovy služeb do 24 hodin od zjištění nefunkčnosti IS.

Monitorování plnění BPIS, její analýzu a vyhodnocování provádí manažer bezpečnosti podniku, který je současně odpovědný za roční vyhodnocení a měření účinnosti BPIS. Výsledky vyhodnocení jsou prezentovány nejvyššímu managementu podniku.

6.5.2 Hodnocení a přezkoumání

Zprávu o hodnocení a přezkoumání BPIS připravuje a předkládá vedení společnosti manager bezpečnosti v koordinaci s řediteli středisek. Ve zprávě vedení podniku ukládá odpovědným pracovníkům splnění navržených opatření s jasně definovaným termínem splnění úkolu Záměrem provádění přezkoumání je prověření aktuálního stavu BPIS.

ZÁVĚR

V rámci informačních systémů podniku je nakládáno s informacemi a daty, které představují značnou hodnotu a v případě poškození, změny nebo ztráty mohou být následky fatální z hlediska fungování a existence podniku.

Diplomová práce se zabývá otázkou bezpečnostní politiky informačního systému reálného obchodně výrobního podniku. Aktiva představují pro každý podnik podstatnou hodnotu, kterou je nutné chránit na maximální možné úrovni ve vztahu nákladů na opatření versus hodnota aktiva.

V první části byla věnována pozornost bezpečnostní politice, informačnímu systému, s ním související legislativě a normám, definici aktiv a metodám analýzy rizik. V praktické části byl nastíněn pohled na reálný podnik. Na základě řízených rozhovorů a brainstormingu s vybranými pracovníky managementu proběhlo hodnocení aktiv, identifikace a hodnocení hrozeb, vyhodnocení zranitelnosti aktiva a následně vyhodnocení pomocí matice rizik. Výstupem práce je charakteristika aktiv, hrozeb a rizik. Následně byla navržena vhodná opatření pro snížení míry rizika s úmyslem zvýšení bezpečnostní úrovně analýzou zjištěných rizikových aktiv.

Hlavním cílem diplomové práce byl návrh opatření pro zvýšení úrovně zabezpečení informačního systému vybraného subjektu. Použitím vhodných metod analýzy rizik byla odhalena nedostatečně zabezpečená místa v podniku, kterým byla věnována pozornost ke zvýšení bezpečnostní úrovně navrženými opatřeními. Konkrétně se jedná o zpracování návrhu školení uživatelů systému, návrh zálohování firemních dat a informací, zabezpečení přístupových hesel aplikací, zvýšení úrovně zabezpečení zneužití citlivých informací přenosných médií, návrh klasifikace informací dle TLP a zjednodušený návrh BPIS pro potřeby uživatelů podniku. V práci byl posuzován konkrétní podnik, nicméně práci lze využít jako vodítko k podobnému účelu pro jiný podnik.

Vzhledem k tomu, že se vedení podniku rozhodlo získat certifikaci ISO 27001, můžeme diplomovou práci považovat za vhodný základ pro získání certifikace. Na základě výstupu praktické části se lze domnívat, že cíl práce byl splněný.

SEZNAM POUŽITÉ LITERATURY

40/2009 Sb. Trestní zákoník: Zákon trestní zákoník, 2021. *Zakonyprolidi.cz* [online]. Zlín: © AION CS [cit. 2021-04-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

Aktiva [online], © 2020. Horní Počernice: acsoffice [cit. 2020-11-25]. Dostupné z: https://acsoffice.cz/kyberneticka-bezpecnost/aktiva/

BERNATÍK, Aleš, 2016. Analýza nebezpečí a rizik. In: *Fbi.vsb* [online]. Ostrava: VŠB – TU Ostrava [cit. 2020-12-31]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/cs/.content/galerie-souboru/U3V/studijni-materialy/U3V_Analyza_nebezpeci_a_rizik.pdf

BitLocker – šifrování systémových disků, 2021. *Samuraj-cz.* [online]. Praha: samuraj [cit. 2021-4-23]. Dostupné z: https://www.samuraj-cz.com/clanek/bitlocker-sifrovani-systemovych-disku/

Computer network system design diagram, © 1993–2020. *Conceptdraw* [online]. San Jose: CS Odessa [cit. 2020-12-29]. Dostupné z: https://www.conceptdraw.com/How-To-Guide/picture/Computer-network-system-design-diagram.png

Confidentiality, Integrity, & Availability: Basics of Information Security, ©2020. *Smarteyetechnology.com* [online]. Peachtree Corners: Smart eye technology [cit. 2020-12-31]. Dostupné z: https://smarteyetechnology.com/confidentiality-integrity-availability-basics-of-information-security/

ČERMÁK, Miroslav, 2009. *Řízení informačních rizik v praxi*. Brno: Tribun EU. Knihovnicka.cz. ISBN 978-80-7399731-1.

ČSN ISO/IEC 27001, © 2006. *Csnonlinefirmy* [online]. Praha: © Český normalizační institut, 2006 [cit. 2020-12-31]. Dostupné z: http://csnonlinefirmy.unmz.cz/html_nahledy/36/76533/76533_nahled.htm

Dedukce, c2011-2016. ManagementMania.com [online]. Wilmington: MANAGEMENTMANIA [cit. 2021-04-13]. Dostupné z: https://managementmania.com/cs/dedukce

Definice nebezpečí, 2020. *Judikaty* [online]. Snina: EUROGENIUS GROUP [cit. 2020-12-31]. Dostupné z: https://www.judikaty.info/cz/vrchni-a-krajske-soudy-cr/definice-nebezpeci/

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

GÁLA, Libor, Jan POUR a Prokop TOMAN, 2006. *Podniková informatika*. Praha: Grada Publishing. ISBN 80-247-1278-4.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ, 2015. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi*. 3., aktualizované vydání. Praha: Grada Publishing. Management v informační společnosti. ISBN 978-80-247-5457-4.

HANÁČEK, Petr a Jan STAUDEK. *Bezpečnost informačních systémů: Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií* [online]. [cit. 2020-11-25].

How to do PDCA step by step, 2019. *Https://www.siteware.co/* [online]. Belo Horizonte: Siteware [cit. 2020-12-29]. Dostupné z: https://www.siteware.co/en/methodologies/how-to-do-pdca-step-by-step/

Hrozba (Threat), © 2011-2016. *ManagementMania.com* [online]. Wilmington: MANAGEMENTMANIA [cit. 2020-11-25]. Dostupné z: https://managementmania.com/cs/hrozba-threat

Informační aktiva [online], © 2011-2016. Wilmington: managementmania [cit. 2020-12-31]. Dostupné z: https://managementmania.com/cs/informacni-aktiva

Informační systém jako ideální nástroj pro řízení zakázek stavebních firem, © 2001-2020. *Tzbinfo* [online]. Praha 6: Topinfo [cit. 2020-12-29]. Dostupné z: https://elektro.tzb-info.cz/informacni-a-telekomunikacni-technologie/15870-informacni-system-jako-idealni-nastroj-pro-rizeni-zakazek-stavebnich-firem

Information Security, © 2020. *Quickbase* [online]. Salt Lake City: Quick Base [cit. 2020-12-31]. Dostupné z: https://www.quickbase.com/articles/information-security-a-closer-look

Jak využít brainstorming v obchodu a managementu, 2021. Businessanimals.cz [online]. Praha 1: Business Animals [cit. 2021-04-13]. Dostupné z: https://www.businessanimals.cz/brainstorming/

Klasifikace informací v korporátním prostředí, 2018. *Aec* [online]. Praha 8: AEC [cit. 2020-12-31]. Dostupné z: https://www.aec.cz/cz/ztisku/matej-kacic-klasifikace-informaci-v-korporatnim-prostredi-dsm-2018.pdf

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN ISBN978-80-88168-34-8.

KOUDELKA, Ctirad a Václav VRÁNA, 2006. *Rizika a jejich analýza* [online]. Ostrava: VŠB – TU Ostrava [cit. 2020-12-31]. Dostupné z: https://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf

Kybernetická bezpečnost [online], 2020. Praha: Asociace za lepší ICT řešení [cit. 2020-12-31]. Dostupné z: https://lepsi-reseni.cz/ochrana-osobnich-udaju-gdpr/kyberneticka-bezpecnost-i-uvod/

MAISNER, Martin, 2015. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.

Metodika pro identifikaci a hodnocení aktiv a rizik, 2020. *Mestokladno* [online]. T-Soft [cit. 2020-12-31]. Dostupné z: https://mestokladno.cz/assets/File.ashx?id_org=6506&id_dokumenty=1474792

MLÝNEK, Jaroslav, c2007. *Zabezpečení obchodních informací*. Brno: Computer Press. ISBN 978-80-251-1511-4.

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

PATTYNOVÁ, Jana, 2018. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě: komentář*. Praha: Leges. Komentátor. ISBN 978-80-7502-288-2.

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

SCHOU, Corey a Steven HERNANDEZ, [2015]. *Information assurance handbook: effective computer security and risk management strategies*. New York: McGraw-Hill Education. ISBN 0071821651.

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

Syntéza, c 2011-2016. ManagementMania.com [online]. Wilmington: MANAGEMENTMANIA [cit. 2021-04-13]. Dostupné z: https://managementmania.com/cs/synteza

TICHÝ, Milík, 2006. *Ovládání rizika: analýza a management*. V Praze: C.H. Beck. Beckova edice ekonomie. ISBN 80-7179-415-5.

Traffic light protocol, 2021[online]. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY [cit. 2020-12-29]. Dostupné z: https://www.cisa.gov/tlp

TUMA, Jiří, 2008. Úvod do klasických a moderních metod šifrování. *Úvod do klasických a moderních metod šifrování* [online]. Praha [cit. 2021-04-02]. Dostupné z: https://www2.karlin.mff.cuni.cz/~tuma/ciphers08/sifry5.ppt

Vyhláška č. 82/2018 Sb.: Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), 2020. *Zakonyprolidi* [online]. Zlín: AION CS [cit. 2020-12-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

VYMAZAL, Tomáš, Otakar Jiří MÍKA a Petr MISÁK, 2015. *Analýza, posouzení a ošetření rizik technických systémů* [online]. Brno: VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ [cit. 2020-12-31]. Dostupné z: http://www.szk.fce.vutbr.cz/vyuka/OP2/RI%202015.pdf

What is the CIA Triad?, 1999 - 2020. *Whatls* [online]. Atlanta: TechTarget [cit. 2020-12-31]. Dostupné z: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Základní kroky analýzy a hodnocení rizik, 2020. *Guard7* [online]. Pardubice: Guard [cit. 2020-12-31]. Dostupné z: https://www.guard7.cz/lexikon/zakladni-kroky-analyzy-a-hodnoceni-rizik

Zákon 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů, 2014. *Zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů* [online]. Praha: Národní bezpečnostní úřad [cit. 2021-04-02]. Dostupné z: https://www.nbu.cz/download/pravni-predpisy/181_2014.pdf

Zákon č. 412/2005 Sb.: Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti, 2021. *Zakonyprolidi.cz* [online]. Zlín: © AION CS [cit. 2021-04-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

Zákon č. 480/2004 Sb.: Zákon o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), 2020. *Zakonyprolidi* [online]. Zlín: © AION CS [cit. 2020-12-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-480?text=480%2F2004

Zákon č. 89/2012 Sb.: Zákon občanský zákoník, 2020. *Zakonyprolidi* [online]. Zlín: © AION CS [cit. 2020-12-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89?text=89%2F2012

Zákon o ochraně osobních údajů 101/2000 Sb., 2014. *Http://zakony.centrum.cz/zakon-o-ochrane-osobnich-udaju/cast-1* [online]. Praha 8: Ekonomia [cit. 2021-04-02]. Dostupné z: http://zakony.centrum.cz/zakon-o-ochrane-osobnich-udaju/cast-1

Zásady tvorby bezpečnostní dokumentace informačních systémů určených k nakládání s utajovanými informacemi, 2017. *NBU* [online]. Praha: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2020-12-31]. Dostupné z: https://www.nbu.cz/download/bezpecnost-informacnich-systemu/DokumentaceIS-vzor.pdf

ŽÁK KRZYŽANKOVÁ, Katarzyna, 2019. K roli abdukce v právním myšlení aneb jak poznatky o abdukci mohou zvýšit pro-systémovost interpretace a aplikace práva. AUC IURIDICA [online]. 65(4), 69-88 [cit. 2021-04-13]. ISSN 2336-6478. Dostupné z: doi:10.14712/23366478.2019.40

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACC	Accidental threat – náhodná hrozba
AVL	Availability – dostupnost
BOZP	Bezpečnost a ochrana zdraví při práci
BPIS	Bezpečnostní politika informačního systému
CNF	Confidentiality – důvěrnost
DLB	Deliberate threat – úmyslná hrozba
ENV	Environmental threat – přírodní hrozba
ERP	Enterprise resource planning – Podnikový informační systém
GDPR	General Data Protection Regulation
HW	Hardware
ICT	Informační a telekomunikační technologie
IDPS	Intrusion Detection and Prevention Systems
INT	Integrita
IS	Informační systém
ISMS	Information Security Management System – Systém řízení bezpečnosti informací
ISO/IEC	International Organization for Standardization, International Electrotechnical Commissio – Mezinárodní elektrotechnické komise
IT	Informační technologie
LAN	Local Area Network
NAS	Network Attached Storage – úložné zařízení
NTB	Notebook, laptop
OS	Operační systém
PDCA	Plan, Do, Check, Act – plánuj, dělej, kontroluj, jednej.
POS	Prohlášení o shodě
PZTS	Polachové zabezpečovací a tísňové systémy

SMS	Short message service
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TLP	Trafic light protocol
VDS	Video dohledový systém
VOP	Veřejné obchodní podmínky
WIFI	Wireless fidelity – bezdrátová síť

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: KVANTIFIKACE AKTIV A HROZBY ODPOVĚDNÝMI OSOBAMI

V příloze diplomové práce naleznete tabulky, které byly vytvořeny na základě hlasování vedoucích osob podniku. Tabulky představují subjektivní pohled na ohodnocení aktiv.

Tabulka „Informační aktiva“ je z třech tabulek nejrozsáhlejší. Nachází se zde oblasti účetnictví, marketing, nákup, prodej apod. Celkem šest osob z top managementu bylo vybráno, aby posoudilo jednotlivá aktiva z hlediska míry jejich ohrožení. Hodnoty jsou v rozmezí 1-4, přičemž k výsledné hodnotě jsme došli nastavením součtu hodnot a vydělení počtem hodnotitelů – aritmetický průměr.

Technická aktiva, jak z názvu vyplývá, zahrnují technické vybavení společnosti. Rozeznáváme hmotná i nehmotná aktiva, která představují pro společnost významnou hodnotu a jejich poškození, ztráta či odcizení by mohlo mít na podnik negativní dopad. Stejní hodnotitelé ohodnotili míru hrozby v případě jednotlivých aktiv. Všechny tyto výsledky s hodnotami 3 a 4 jsou v praktické části diplomové práce předmětem pro návrh na minimalizaci hrozeb.

Podpůrná aktiva jsou v tabulce rozčleněna do dvou skupin a sice personálních. První skupina je pojmenována kmenoví zaměstnanci, do které spadají osoby působící v top managementu, manažeři, výrobní mistři a dělníci. Druhou skupinou jsou externí pracovníci, z nichž pouze první dvě položky správce IS a správce IT představují nejvyšší hodnotu 4. Výše uvedené tabulky v příloze 1 jsou zásadní pro následný rozbor a návrh řešení minimalizace bezpečnostních rizik v podniku. Poslední tabulka č. 21 „Ohodnocení hrozeb podniku“ znázorňuje jednotlivé hodnoty osob managementu podniku, které byly zprůměrovány a na základě výsledné hodnoty červeně vyznačeny ty nejrizikovější.

Tabulka 16 – Hodnocení informačních aktiv – část 1 (vlastní zpracování)

Číslo	Aktivum	Klasifikace	Generální ředitel	Provozní ředitel	Výrobní ředitel	Ředitel střediska podpory	Ředitel vývoje hardwaru	Ředitel vývoje softwaru	**Výsledná hodnota**
1	Účetnictví								
1.1	DPH	O	4	2	3	3	4	3	**3**
1.2	Silniční daň	O	3	4	3	2	2	3	**3**
1.3	Interní doklady	D	4	4	4	4	3	4	**4**
1.4	Základní nastavení účetnictví	O	2	4	2	3	3	3	**3**
1.5	Účetní deník	D	4	2	4	4	4	4	**4**
1.6	Položky účetního deníku	O	3	3	2	4	3	4	**3**
1.7	Likvidace a účtování	O	3	4	3	2	2	4	**3**
1.8	Hlavní kniha	D	4	2	4	3	4	4	**4**
1.9	Ekonomické analýzy	D	4	4	4	3	4	4	**4**
1.1	Ostatní funkce	O	3	2	4	4	2	4	**3**
1.11	Kontroly zaúčtování	O	3	4	3	2	2	3	**3**
1.12	Přecenění k rozvahovému dni	O	3	3	2	4	3	3	**3**
1.13	Servisní funkce	O	2	4	2	4	3	4	**3**
1.14	Účetní závěrka	D	4	4	4	4	4	4	**4**
1.15	Nezaúčtované doklady	O	4	4	2	4	2	3	**3**
1.16	účetní sestavy	I	2	1	2	3	2	1	**2**
2	Marketing								
2.1	Nabídka/Poptávka	O	3	3	2	4	3	3	**3**
2.2	Partneři	O	3	4	3	2	2	3	**3**
2.3	Kontaktní osoby	O	2	3	4	2	3	3	**3**
2.4	Aktivity	O	3	2	3	3	4	3	**3**
2.5	Příležitosti	O	4	4	2	2	3	4	**3**
2.6	Kampaně	V	1	2	1	1	2	1	**1**
2.7	Vyhodnocení marketingu	I	3	1	2	3	2	2	**2**
2.8	Správa a nastavení	O	3	4	3	4	3	2	**3**
3	Prodej								
3.1	Základní data	O	3	3	2	4	3	3	**3**
3.2	Kontakty	D	4	4	3	4	3	4	**4**
3.3	Zakázky	D	3	4	4	3	4	4	**4**
3.4	Položky prodeje	I	2	1	2	2	3	2	**2**
3.5	Objednávky přijaté	D	4	3	4	4	3	4	**4**
3.6	Rezervační listy	I	2	1	2	2	3	3	**2**
3.7	Výdejky	O	4	3	3	4	2	2	**3**
3.8	Dodací listy vydané	O	3	4	3	2	2	3	**3**
3.9	Faktury vydané	D	4	3	4	4	3	4	**4**
3.1	Zálohy přijaté	O	3	3	2	4	3	3	**3**
3.11	Ostatní pohledávky	O	2	3	3	4	3	4	**3**
3.12	Vyhodnocení prodeje	I	2	3	1	2	3	2	**2**
3.13	Kupónové slevy	O	3	4	3	2	2	3	**3**
3.14	Funkce	I	2	2	2	3	2	3	**2**

Tabulka 17 – Hodnocení informačních aktiv – část 2 (vlastní zpracování)

Číslo	Aktivum	Klasifikace	Generální ředitel	Provozní ředitel	Výrobní ředitel	Ředitel střediska podpory	Ředitel vývoje hardwaru	Ředitel vývoje softwaru	**Výsledná hodnota**
4	Nákup								
4.1	Poptávky	I	3	2	2	1	2	1	**2**
4.2	Kontakty	D	3	4	4	3	4	4	**4**
4.3	Objednávky vydané	I	2	1	2	3	1	2	**2**
4.4	Položky nákupu	O	3	3	3	3	2	3	**3**
4.5	Potvrzení dodání	I	1	2	3	3	1	3	**2**
4.6	Příjemky	O	3	2	4	3	2	4	**3**
4.7	Faktury přijaté	D	3	3	4	4	4	4	**4**
4.8	Zálohy poskytnuté	O	3	2	3	3	4	3	**3**
4.9	Ostatní závazky	O	4	3	3	4	3	2	**3**
4.1	Vyhodnocení nákupu	I	2	3	2	2	1	1	**2**
5	Reklamace								
5.1	Servisní zakázky	O	3	3	2	3	3	3	**3**
5.2	Servisní listy	O	3	2	3	4	3	2	**3**
5.3	Vyhodnocení servisu	O	2	4	3	4	3	2	**3**
5.4	Přehledy	I	2	2	3	1	1	2	**2**
6	Logistika								
6.1	Stavy skladů	D	4	3	4	3	4	4	**4**
6.2	Vyhodnocení skladu	O	3	2	3	4	3	4	**3**
6.3	Převodky	O	3	2	2	3	3	3	**3**
6.4	Příjemky	O	3	3	4	3	2	3	**3**
6.5	Výdejky	O	3	2	4	4	2	2	**3**
6.6	Inventury	O	3	2	3	2	4	3	**3**
6.8	Zásilkové služby	I	2	1	2	2	3	1	**2**
6.9	Doprava	I	1	3	2	2	1	3	**2**
7	Výroba								
7.1	Technologická příprava výroby	D	3	4	4	3	4	3	**4**
7.2	Průvodky	O	3	2	3	3	2	3	**3**
7.3	Výrobní příkazy	O	4	3	4	4	2	3	**3**
7.4	Řízení výroby	D	3	4	4	4	4	2	**4**
7.5	Vyhodnocení výroby	I	3	1	1	2	2	2	**2**
7.6	Vyhledávání sériového čísla	I	2	2	3	2	2	3	**2**
8	Projekty								
8.1	Základní nastavení	I	2	2	3	2	3	1	**2**
8.2	Projekty	D	4	4	3	4	4	3	**4**
8.3	Výkazy práce	O	2	3	4	3	2	3	**3**
9	Celnice								
9.1	Základní data	I	2	2	3	1	2	2	**2**
9.2	JCD - Dovoz	O	3	4	2	3	3	2	**3**
9.3	JCD - Vývoz	O	4	4	2	3	3	2	**3**
9.4	JCD - Zjednodušený příjem	O	3	3	4	3	2	3	**3**
9.5	JCD - Zjednodušený výdej	O	3	4	4	3	3	2	**3**
9.7	JCD - Tranzit	I	3	2	1	2	1	2	**2**
9.8	Celní sazebník	V	1	1	1	2	2	1	**1**

Tabulka 18 – Hodnocení informačních aktiv – část 3 (vlastní zpracování)

Číslo	Aktivum	Klasifikace	Generální ředitel	Provozní ředitel	Výrobní ředitel	Ředitel střediska podpory	Ředitel vývoje hardwaru	Ředitel vývoje softwaru	**Výsledná hodnota**
10	Banka								
10.1	Banka	D	4	4	4	3	4	4	**4**
10.2	Položky platebních dokladů	D	4	3	3	4	4	4	**4**
10.3	Saldokonto	O	3	2	3	3	4	3	**3**
10.4	Upomínky	O	2	2	3	3	2	3	**3**
10.5	Opravné daňové doklady	O	3	2	3	3	2	3	**3**
10.6	Skonto	O	2	4	3	4	3	4	**3**
10.7	Platební kalendář	D	4	3	4	4	3	3	**4**
10.8	EET	O	3	2	3	4	3	2	**3**
10.9	VP Banka	O	3	2	3	4	3	3	**3**
11	Majetek								
11.1	Kniha majetku	D	4	4	4	3	3	3	**4**
11.2	Propojení s prvotními doklady	O	3	2	3	3	2	4	**3**
11.3	Hospodářský rok	D	3	4	2	4	4	4	**4**
11.4	Prostorová procesní evidence	O	3	3	4	3	2	3	**3**
12	Mzdy								
12.1	Personální údaje	D	4	4	4	3	4	4	**4**
12.2	Pracovní vztahy	D	4	3	2	4	4	4	**4**
12.3	Mzdové údaje	D	4	4	4	4	4	4	**4**
12.4	Srážky z mezd	D	3	4	4	3	4	4	**4**
12.5	Mzdové výpočty	D	4	2	4	4	3	4	**4**
12.6	Kvalifikace	O	3	2	3	3	2	3	**3**
12.7	Závazky z mezd	D	4	3	4	4	4	3	**4**
12.8	Organizační struktura	O	2	3	2	3	3	2	**3**
13	Internetový obchod								
13.1	Kniha pro internetový obchod	O	3	3	3	2	3	2	**3**
13.2	Související knihy	O	2	3	3	4	3	4	**3**
13.3	Správa a nastavení	O	2	4	4	2	4	3	**3**
13.4	Kupónové slevy	I	3	1	2	1	2	2	**2**

Tabulka 19 - Hodnocení technických aktiv – část 1 (vlastní zpracování)

Číslo	Komponenty	Pořizovací cena	Chráněná hodnota	Generální ředitel	Provozní ředitel	Výrobní ředitel	Ředitel střediska	Ředitel vývoje HW	Ředitel vývoje SW	**Výsledná hodnota**
1	Software a aplikace									
1.1	ERP systém K2	3	D	4	3	4	4	3	4	**4**
1.2	Operační systém Win 10	2	D	3	4	4	3	4	4	**4**
1.3	Office365	2	C	3	2	4	3	3	2	**3**
1.4	Eset Endpoint Antivirus	3	D	4	4	3	2	4	4	**4**
1.5	CRM Databox	3	C	3	2	3	3	4	4	**3**
1.6	Helpdeskový systém Apollo	3	C	4	3	4	2	2	3	**3**
1.7	Web shop	3	D	4	3	4	4	4	4	**4**
1.8	Firemní aplikace	4	D	4	4	3	4	3	4	**4**
1.9	Adobe Acrobat	2	C	3	3	2	3	4	3	**3**
1.1	AutoCad	2	D	4	4	4	3	4	3	**4**
1.11	Vault	4	D	4	4	4	3	3	4	**4**
2	Komunikační infrastruktura									
2.1	Serverovna	4	D	4	3	4	4	3	3	**4**
2.2	Datový rozvaděč RACK	2	B	2	2	3	2	1	2	**2**
2.3	Kabelové rozvody	3	C	3	4	3	3	4	3	**3**
3	Síťové prostředky									
3.1	Server	4	D	4	4	3	4	3	4	**4**
3.2	Diskové pole	3	D	4	3	4	4	2	4	**4**
3.3	Router	1	C	3	2	3	3	4	2	**3**
3.4	Switch	2	B	2	3	2	2	1	3	**2**
3.5	Acces point	1	D	4	4	3	4	4	2	**4**
3.6	Tiskárny	2	B	3	2	2	1	3	2	**2**
3.7	Přístupový systém	4	D	4	4	4	3	4	2	**4**
3.8	Docházkový systém	3	D	4	3	3	4	4	3	**4**
3.9	Stravovací systém	2	D	4	3	3	3	4	4	**4**
3.1	Penosné PC	2	D	4	3	4	4	4	4	**4**
3.11	Mobilní telefony	2	D	3	4	4	4	4	3	**4**
3.12	Telefonní ústředna	3	C	3	2	3	2	3	3	**3**

Tabulka 20 – Hodnocení technických aktiv – část 2 (vlastní zpracování)

Číslo	Komponenty	Pořizovací cena	Chráněná hodnota	Generální ředitel	Provozní ředitel	Výrobní ředitel	Ředitel střediska	Ředitel vývoje HW	Ředitel vývoje SW	**Výsledná hodnota**
4	Poplachový a zabezpečovací systém									
4.1	Ústřadna PZTS	3	D	4	4	4	3	4	3	**4**
4.2	Kabelové rozvody PZTS	3	D	4	4	4	3	4	4	**4**
4.3	Detektory	2	D	4	3	4	4	4	3	**4**
4.4	Ovládací zařízení	1	C	3	2	3	3	4	3	**3**
4.5	Signalizační zařízení	2	D	4	4	4	2	3	4	**4**
5	Kamerový systém									
5.1	Záznamové zařízení	3	D	4	4	4	3	4	2	**4**
5.2	Kabelové rozvody	2	B	2	3	2	2	3	2	**2**
5.3	IP Kamery	3	C	3	4	3	3	2	3	**3**
6	Objekty									
6.1.1	Zasedací místnosti	3	C	3	2	3	3	4	2	**3**
6.1.2	Jídelna	2	B	3	2	2	3	2	2	**2**
6.1.3	Kanceláře	3	D	4	3	4	4	4	3	**4**
6.1.4	Archiv	2	D	4	3	4	4	3	3	**4**
6.1.5	Serverovna	4	D	4	4	3	4	3	4	**4**
6.1.6	Parkoviště	3	C	3	3	2	3	2	3	**3**
6.2.1	Sklad EV	4	D	4	3	4	4	3	4	**4**
6.2.2	Expedice	3	C	2	4	3	3	3	2	**3**
6.2.3	Klimatická komora	3	C	3	2	2	3	2	3	**3**
6.2.4	Vývoj HW	2	C	3	3	3	2	2	3	**3**
6.7	Skladovací hala A3	4	D	4	3	4	4	4	3	**4**
6.8	Výrobní hala B	4	D	4	4	4	4	4	4	**4**
6.9	Výrobní hala C	4	D	4	3	4	3	4	4	**4**
6.1	Sklad D	4	D	3	3	4	4	3	4	**4**
6.11	Sklad E	4	D	3	4	4	3	4	3	**4**
6.11	Parkoviště mezi halami	3	C	2	3	2	3	2	3	**3**

Tabulka 21 – Hodnocení podpůrných aktiv (vlastní zpracování)

Číslo	**Aktivum**	**Klasifikace**	Generální ředitel	Provozní ředitel	Výrobní ředitel	Ředitel střediska	Ředitel vývoje HW	Ředitel vývoje SW	**Výsledná hodnota**
1	**Kmenoví zaměstnanci**								
1.1	Top management	4	4	3	4	4	3	4	**4**
1.2	Manažer IT	4	3	4	4	3	4	4	**4**
1.3	Manažer bezpečnosti informací	4	4	3	4	4	4	3	**4**
1.4	Střední management	3	4	3	3	2	3	2	**3**
1.5	Mistři výroby	2	2	1	3	2	2	2	**2**
1.6	Dělníci	1	1	1	1	2	1	2	**1**
2	**Externí pracovníci**								
2.1	Správce IS	4	4	4	3	4	3	4	**4**
2.2	Správce IT	4	4	4	3	3	4	4	**4**
2.3	Provider	2	2	3	2	2	2	2	**2**
2.4	Daňový poradce	1	1	1	2	1	1	2	**1**
2.5	Právní kancelář	1	1	2	1	1	1	1	**1**
2.6	Revizní technici	1	2	1	1	1	1	1	**1**
2.7	Pracovníci státní správy	1	1	1	2	2	1	1	**1**

Tabulka 22 – Hodnocení hrozby (vlastní zpracování)

Číslo	Hrozba		Generální ředitel	Provozní ředitel	Výrobní ředitel	Ředitel střediska podpory	Ředitel vývoje hardwaru	Ředitel vývoje softwaru	Výsledná hodnota
1.	Lidé	Hacker, špion, konkurence	1	2	2	1	1	2	**1**
2.		Zaměstnanec	2	3	3	3	2	3	**3**
3.		Neproškolený uživatel	2	3	3	3	2	3	**3**
4.		Externí pracovník dodavatele	3	2	2	4	3	3	**3**
5.		Správce systému	3	2	3	3	2	3	**3**
6.		Návštěva	1	2	1	2	2	2	**2**
7.	Fyzické poškození	Požár	2	3	1	2	3	2	**2**
8.		Povodeň	1	2	1	1	2	1	**1**
9.		Orkán	1	1	2	1	1	1	**1**
10.		Zemětřesení	1	1	1	1	1	1	**1**
11.		Výbuch	1	2	2	2	1	2	**2**
12.		Prach koroze	2	2	1	2	2	3	**2**
13.		Zatopení (porucha ústředního topení nebo vodoinstalace)	2	1	2	3	2	2	**2**
14.		Porucha klimatizace	2	3	2	3	3	2	**3**
15.	Služby	Dodávka el. Energie	2	4	4	4	2	4	**4**
16.		Výpadek konektivity IS	4	3	3	2	4	4	**3**
17.		Dodávky materiálu	3	2	2	4	2	2	**2**
18.	Informace	Odposlech	2	1	2	2	3	3	**3**
19.		Přerušení	2	3	3	2	3	2	**3**
20.		Nesprávné ověření identity uživatele	3	4	3	2	3	3	**3**
21.		Změna dat	3	3	2	3	3	3	**3**
22.		Kopírování	2	2	3	3	3	4	**3**
23.		Změna při přenosu	2	2	3	2	2	2	**2**
24.		Vymazání	3	2	2	2	2	2	**2**
25.	Selhání lidského faktoru	Krádež	2	2	2	1	3	2	**2**
26.		Neadekvátní servisní činnost	2	3	1	2	2	2	**2**
27.		Nedostatek zaměstnanců s potřebnou odbornou úrovní	3	2	2	2	2	2	**2**
28.	HW	Porucha	4	4	2	4	4	3	**4**
29.		Odcizení	4	4	4	3	4	4	**4**
30.		Poškození	2	3	2	2	3	2	**2**
31.	SW	Kopírování	2	3	2	3	3	3	**3**
32.		Viry	3	3	4	2	3	3	**3**
33.		Úmyslné vymazání	2	3	2	2	3	2	**2**
34.		Neúmyslné vymazání	1	2	1	1	1	1	**1**
35.		Kyberterorismus	3	3	3	2	3	3	**3**
36.		Porucha zálohování	3	4	3	4	4	3	**4**
37.		Použití neautorizovaného SW	4	3	4	4	4	4	**4**