VYSOKÁ ŠKOLA POLYTECHNICKÁ JIHLAVA

Aplikovaná informatika

Řízení informačních a kybernetických rizik v průmyslovém podniku

Bakalářská práce

Autor práce: Karel Svoboda

Vedoucí práce: Ing. Roman Černický

Jihlava 2024

Vysoká škola polytechnická Jihlava

Tolstého 16, 586 01 Jihlava

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Autor práce:	**Karel Svoboda**
Studijní program:	Aplikovaná informatika
Obor:	Aplikovaná informatika
Garant studijního programu:	Ing. Lenka Kuklišová Pavelková, Ph.D.
Název práce:	**Řízení informačních a kybernetických rizik v průmyslovém podniku**
Vedoucí práce:	Ing. Roman Černický
Konzultant práce:	Mgr. Antonín Přibyl
Cíl práce:	Cílem práce je popsat proces řízení informačních a kybernetických rizik v průmyslovém podniku v České republice a porovnat ji s úrovní řízení rizik v Evropské unii. Teoretická část popíše legislativní podklady pro řízení rizik a organizace upravující oblast kybernetické bezpečnosti v České republice. Dále bude práce obsahovat postup při provádění analýzy a řízení informačních a kybernetických rizik. Cílem praktické části je vytvořit a implementovat proces řízení informačních a kybernetických rizik pro fiktivní průmyslový podnik.

Abstrakt

Bakalářská práce se zabývá řízením informačních a kybernetických rizik v průmyslovém podniku. V teoretické části se zaměřuje na popis legislativního rámce, který stanovuje pravomoci a povinnosti v oblasti IKB. Teoretická část dále obsahuje vymezení základních pojmů v oblasti IKB a jejich uplatnění, definici a popis podniku v České republice a přístup Evropské unie k IKB a řízení rizik. Praktická část definuje podnik, který spadá do regulace dle připravovaného zákona o kybernetické bezpečnosti, a poskytuje praktický návod na provedení analýzy rizik v daném podniku. Po provedené analýze rizik hodnotí práce stav IKB v podniku a prezentuje možná nápravná opatření pro zajištění adekvátní úrovně IKB.

Klíčová slova

Analýza rizik; kybernetická bezpečnost; primární aktivum; podpůrné aktivum; Systém řízení bezpečnosti informací; hardening;

Abstract

The bachelor's thesis deals with the management of information and cyber risks in an industrial enterprise. In the theoretical part, the thesis focuses on the description of the legislative framework, which establishes the rights and obligations in the field of information and cyber security. The theoretical part also contains the definition of basic concepts in the field of information and cyber security and their application, the definition and description of a business in the Czech Republic and the approach of the European Union to information and cyber security. The practical part defines the businesses that fall under the regulation of the upcoming Cyber Security Act and provides practical guidance for conducting a risk analysis in a given business. After the risk analysis, the work evaluates the state of information and cyber security in the company and presents possible corrective measures to ensure an adequate level of information and cyber security.

Keywords

Risk analysis; cyber security; primary asset; supporting asset; Information security management system; hardening;

Prohlašuji, že předložená bakalářská práce je původní a zpracoval/a jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil/a autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v platném znění, dále též „**AZ**“).

Byl/a jsem seznámen/a s tím, že na mou bakalářskou práci se plně vztahuje **AZ**, zejména § 60 (školní dílo).

Podle § 47b zákona o vysokých školách souhlasím se zveřejněním své práce podle směrnice prorektora pro studium č. 2/2020, a to bez ohledu na výsledek obhajoby.

Beru na vědomí, že VŠPJ má právo na uzavření licenční smlouvy o užití mé bakalářské práce a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

Jsem si vědom/a toho, že užít své bakalářské práce či poskytnout licenci k jejímu využití mohu jen se souhlasem VŠPJ, která má právo ode mě požadovat přiměřený příspěvek na úhradu nákladů, vynaložených vysokou školou na vytvoření díla (až do jejich skutečné výše), z výdělku dosaženého v souvislosti s užitím díla či poskytnutím licence.

V Jihlavě dne 3. června 2024

Podpis studenta/ky

Poděkování

Chci poděkovat mému vedoucímu práce za čas a trpělivost, kterou se mnou při psaní práce měl a všem, především rodině, kteří mě při psaní podporovali.

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

BOZP	Bezpečnost a ochrana zdraví při práci
C2M2	Cybersecurity capability maturity model
CERT	Computer emergency response team
CIA	Model důvěrnosti, integrity a dostupnosti
CIS	Center for internet security
CSIRT	Computer Security Incident Response Team
ČR	Česká republika
ČSN	Česká státní norma
ČSU	Český statistický úřad
DMS	Data management system
EC	European commission
ECM	Enterprise content management
ENISA	European Network and Information Security Agency
ERP	Enterprise resource planning
EU	Evropská Unie
FP	Fyzické prostory
GPS	Global Positioning Systém
GWh	Gigawathodina
HA	High availability
HMI	Human-machine interface
HR	Human resources
HW	Hardware
ICS	Industrial control systems
IDS	Intrusion detection system
IKB	Informační a kybernetická bezpečnost
IoT	Internet věcí
IPS	Intrusion prevention system
IS	Informační systém

ISMS	Information Security Management Systém
ISO	Mezinárodní organizace pro normalizaci
IT	Information technology
ITSRM^2	IT security risk management methodology
MIL	Maturity indicator level
MSP	Malé a střední podniky
MTU	Master terminal unit
MW	Megawatt
MWh	Megawathodina
NB	Notebook
NIS	Network and Information Security
NTP	Network Time Protocol
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OOP	Opatření obecné povahy
OrS	Organizační struktura
OSN	Organizace spojených národů
OT	Operational technology
PC	Osobní počítač
PDCA	Demingův cyklus (Plan, Do, Check, Act)
PLC	Programmable logic controller
RM	Risk management
SCADA	Supervisory Control and Data Acquisition
SIEM	Security and information and event management
SW	Software
TLP	Traffic light protocol
UPS	Uninterruptible power supply
VŠPJ	Vysoká škola polytechnická Jihlava
ZoKB	Zákon o kybernetické bezpečnosti
ZoUI	Zákon o ochraně utajovaných informací

Úvod

Cílem práce je popsat proces řízení informačních a kybernetických rizik ve fiktivním průmyslovém podniku v České republice. Teoretická část popíše legislativní podklady pro řízení rizik a organizace upravující oblast kybernetické bezpečnosti v České republice a EU. Dále bude práce obsahovat postup při provádění analýzy a řízení informačních a kybernetických rizik. Cílem praktické části je vytvořit a implementovat proces řízení informačních a kybernetických rizik pro fiktivní průmyslový podnik.

Důvodem ke zpracování tématu je autorovo zaměstnání a chystané změny v oblasti informační a kybernetické bezpečnosti (IKB) související s přijetím směrnice EU – tzv. NIS 2. Zavedením směrnice do českého právního rámce vznikne povinnost zohlednit IKB do pracovních činností několika tisícům českých firem. Přínos práce tak bude v přehledu legislativních požadavků, které již platí a které budou v blízké době platit, ale především v aplikaci IKB a řízení rizik pro fiktivní podnik tak, aby mohla být tato bakalářská práce využita jako vzor i pro skutečnou firmu, které se zavedení normy NIS 2 týká.

1 Teoretická část

Cílem teoretické části je vysvětlit základní pojmy v oblasti IKB, vymezit legislativní rámec pro IKB v České republice, popsat legislativu vymezující IKB v Evropské unii. Dále popsat metody pro určení úrovně IKB v organizaci a řízení rizik v organizaci, které budou využity v praktické části práce.

1.1 Pojmy v informační a kybernetické bezpečnosti

Kapitola slouží jako základní slovník pojmů použitých v této práci.

Bezpečnostní hrozba – potenciální nežádoucí událost, která může mít za následek poškození systému a aktiv. (MVČR, 2019)

Bezpečnostní opatření – souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru. Bezpečnostní opatření lze rozdělit na organizační a technická opatření. (Zákon č. 181/2014 Sb., 2014)

Bezpečnostní událost – Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. (Zákon č. 181/2014 Sb., 2014)

Bezpečnostní incident – Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události. (Zákon č. 181/2014 Sb., 2014)

CIA – model důvěrnost, integrita, dostupnost. Jednotlivé položky jsou vysvětleny v rámci této kapitoly. Model se může upravovat dle preferencí firmy, např. AIC.

Hardening – soubor pravidel a nastavení pro zajištění co nejlepší úrovně bezpečnosti IT, ICS za účelem snížení rizik. (CIS benchmarks, 2024)

Hodnocení aktiv – hodnocení aktiv dle čtyřstupňové stupnice dle důvěrnosti, dostupnosti a integrity. Stupně jsou Nízké, Střední, Vysoké, Kritické. (Vyhláška č. 82/2018 Sb., 2018)

ICS – programovatelné systémy sloužící k ovládání průmyslového technologického procesu v reálném čase. ICS systémy se skládají z ovládacího SW a HW jako jsou senzory, manipulátory, síťové prvky atd. (NÚKIB, 2024)

Řízení rizik – činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik. (Vyhláška č. 82/2018 Sb., 2018)

Významná změna – změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko. (Vyhláška č. 82/2018 Sb., 2018)

Zranitelnost – potenciálně slabá místa systému, aktiv nebo dalších prvků v organizaci, která mohou být zneužita hrozbou nebo hrozbami. (Vyhláška č. 82/2018 Sb., 2018)

Center for internet security (CIS) – komunitní nezisková organizace poskytující postupy, návody a příručky pro zabezpečení IT systémů. Poskytuje i hardenované verze operačních systémů pro využití v oblasti IT. (CIS benchmarks, 2024)

Aktiva – jako aktivum lze označit cokoliv, co má pro daný subjekt určitou hodnotu a subjekt má zájem o jeho ochranu. Aktiva lze dle vyhlášky o KB rozdělit na primární a podpůrná aktiva. (NÚKIB, 2024)

Primární aktivum – informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém. (Vyhláška č. 82/2018 Sb., 2018)

Podpůrné aktivum – technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému. (Vyhláška č. 82/2018 Sb., 2018)

Analýza rizik – součást procesu řízení rizik. Analýza spočívá v identifikaci a ohodnocení rizik u vybraného subjektu. (ISO 27000, 2020)

Bezpečnostní klasifikace – ohodnocení systému na definované stupnici a jeho zařazení do klasifikační třídy.

Organizační opatření – soubor opatření dle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb. Dle vyhlášky se dělí na Systém řízení bezpečnosti informací, řízení aktiv, řízení rizik, organizační bezpečnost, bezpečnostní role, řízení dodavatelů, bezpečnost lidských zdrojů, řízení provozu a komunikací atd. (Vyhláška č. 82/2018 Sb., 2018)

Prohlášení o aplikovatelnosti – přehled bezpečnostních opatření požadovaných vyhláškou o kybernetické bezpečnosti č. 82/2018 Sb. Přehled obsahuje opatření, která nebyla aplikována včetně odůvodnění a která byla aplikována včetně způsobu plnění. (Vyhláška č. 82/2018 Sb., 2018)

Důvěrnost – kritérium hodnocení aktiva, v angličtině známé jako confidentiality z modelu CIA. Kritérium určuje, komu je aktivum přístupné a jak je důležité před neautorizovaným přístupem (platí pro vytváření, zpracování i přenos aktiva). Úroveň může být čtyřstupňová (nízká, střední, vysoká, kritická). (Metodika NÚKIB, 2021)

Dostupnost – kritérium hodnocení aktiva, v angličtině známé jako availability z modelu CIA. Kritérium určuje dobu, po kterou se bez daného aktiva subjekt obejde (aktivum není dostupné) a jaké mu hrozí ztráty při jeho nedostupnosti. Úroveň může být čtyřstupňová (nízká, střední, vysoká, kritická). (ISVS, 2023)

Integrita – kritérium hodnocení aktiva, v angličtině známé jako integrity z modelu CIA. Kritérium definuje přesnost/neměnnost aktiva. Na základě úrovně (nízká, střední, vysoká, kritická) je stanovena ochrana aktiva, aby nedošlo k narušení integrity, změně nebo zničení aktiva. (ISVS, 2023)

Riziko – možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu. (Vyhláška č. 82/2018 Sb., 2018)

Hrozba – potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu. (Vyhláška č. 82/2018 Sb., 2018)

Technické aktivum – technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na informační a komunikační systém. (Vyhláška č. 82/2018 Sb., 2018)

Významná změna – změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko. (Vyhláška č. 82/2018 Sb., 2018)

Významný dodavatel – provozovatel informačního nebo komunikačního systému a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému. (Vyhláška č. 82/2018 Sb., 2018)

SCADA – systém, který získává data z prvků umístěných v technologii. Je také označován jako Dispečerské řízení a sběr dat. Prvky umístěné v technologii jsou připojené do remote terminal unit (RTU) a odtud jsou přenášeny do master terminal unit (MTU) a databázového serveru (MySQL, Oracle SQLite atd.) a zobrazovány na terminálech HMI. (NÚKIB, 2024)

1.2 Podnik

Podnikání v České republice upravuje zejména zákon č. 89/2012 Sb. Občanský zákoník a zákon č. 90/2012 Sb. Zákon o obchodních společnostech a družstvech (zákon o obchodních korporacích). Občanský zákoník rozlišuje jako podnikající subjekt fyzické a právnické osoby. Povinnosti z hlediska IKB se v současnosti týkají především úzce vymezených právnických osob a organizací. Do budoucna po implementaci směrnice NIS2 do české legislativy se okruh organizací značně rozšíří. Podnik, který nyní podléhá směrnici NIS, resp. zákonu o kybernetické bezpečnosti (ZoKB), bude s největší pravděpodobností do budoucna regulován i směrnicí NIS2. (Zákon č. 89/2012 Sb., Zákon č. 90/2012 Sb., 2012) Aby byl podnik regulován dle směrnice NIS2, musí podle článku č. 2 zmíněné směrnice splňovat následující podmínky:

- organizace poskytuje alespoň jednu službu uvedenou v přílohách směrnice a zároveň
- je středním nebo velkým podnikem, tedy zaměstnává 50 a více zaměstnanců, nebo dosahuje ročního obratu nebo bilanční sumy roční rozvahy alespoň 10 milionů eur (zhruba 250 milionů korun). (Směrnice NIS2, 2022)

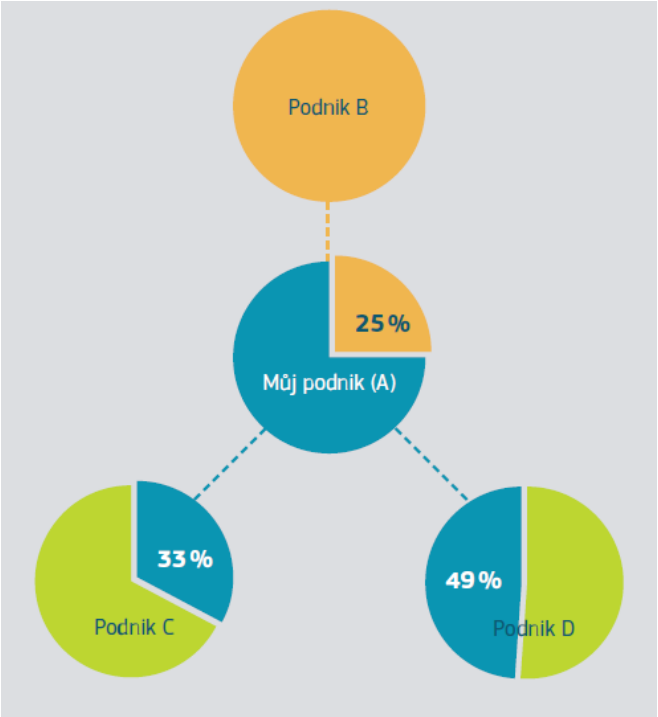
Pro účely této práce je uvažována tzv. soukromá organizace neboli právnická osoba. Za veřejnou organizaci lze považovat mimo jiné státní instituce a úřady.

Jako pomůcku pro definici a určení velikosti firmy lze využít doporučení Evropské komise 2003/361/EC a Uživatelskou příručku k definici malých a středních podniků. Evropská unie považuje za podnik „každý subjekt vykonávající hospodářskou činnost, bez ohledu na jeho právní formu“. (Uživatelská příručka k definici MSP, 2019) Podle uvedené definice tak za podnik lze považovat i fyzickou osobu. Do budoucna tak bude záležet na implementaci směrnice NIS2 do nového ZoKB.

Uživatelská příručka rozděluje proces identifikace malých a středních podniků (MSP) do čtyř kroků. První spočívá v určení, zda je subjekt podnikem. Druhý krok vyjmenovává kritéria, která je třeba ověřit a stanovuje hodnoty kritérií. Jsou podobná již zmíněným v začátku této kapitoly.

- Počet zaměstnanců menší než 250 osob
- Roční obrat nepřesahuje 50 milionů EUR

- Bilanční suma roční rozvahy nepřesahuje 43 milionů EUR



Obr. 1: Partnerský podnik

(Uživatelská příručka MSP, 2019)

Aby podnik spadal do kategorie MSP, musí splňovat první kritérium a zároveň druhé nebo třetí. Střední podnik tak má od 50 do 250 zaměstnanců a obrat do 50 milionů EUR nebo bilanční sumu roční rozvahy do 43 milionů EUR. Pokud by měl podnik méně zaměstnanců, jednalo by se buď o malý podnik nebo mikropodnik. Analogicky, pokud by měl podnik více než 250 zaměstnanců, jednalo by se o velký podnik. Třetí krok příručky popisuje kritéria z druhého kroku. Vyjmenovává osoby, které se započítávají do počtu zaměstnanců a v jakém měřítku (dle úvazku v podniku), vysvětluje určení ročního obratu a bilanční sumy roční rozvahy. Poslední krok ještě definuje nezávislý, partnerský a propojený podnik a výpočet hodnot podle stanovených kritérií. To, zda je podnik nezávislý, partnerský nebo propojený má zásadní vliv na výpočet hodnot.

Na obrázku uvedeném výše se jedná o tzv. partnerský podnik. Pří zjišťování počtu zaměstnanců, ročního obratu a bilanční sumy roční rozvahy je nutné zahrnout i podíly ostatních podniků, tj. 100 % podniku A, 25 % podniku B, 33 % podniku C a 49 % podniku D.

Pro účely práce tak platí, že je uvažováno se středním nebo velkým podnikem, který splňuje požadavky na finanční ukazatele a požadavky NIS2.

Dále je uvažováno s podnikem, jehož oblast podnikání je zaměřeno průmyslově (výroba, distribuce, koordinace dopravy atd.). Na základě toho může být podnik se svým použitým IT a ICS lokalizován na jednom konkrétním místě nebo na rozsáhlém území. Vzhledem k údržbě systémů může být používán vzdálený přístup k určitým částem systému. Základním požadavkem však u průmyslového podniku zůstává, kromě bezpečnosti samotného výrobního/provozního procesu a ochrany personálu, dostupnost ICS systémů, která musí být nepřetržitá (24/7, celý rok). Dalším předpokladem je real-time dostupnost údajů ze systému (v rámci milisekund). To se může týkat například podniků s chemickou výrobou, elektráren atd., kdy je nutné mít okamžitý přehled o stavu technologie. U průmyslových podniků je tak prioritní zájem na

dostupnosti systémů, následně až na integritě a důvěrnosti (úprava modelu CIA na AIC nebo ACI). U ICS systémů jsou značné rozdíly oproti běžným IT systémům, mají rozdílnou délku životního cyklu, použitou kabeláž a rozhraní, požadavky na poruchovost atd. Větší specifikace podniku bude provedena v praktické kapitole.

1.3 Legislativa

Účelem kapitoly Legislativa je popsat právní rámec týkající se informační a kybernetické bezpečnosti. Vzhledem k problematice s licenčními ujednáními a publikováním zde nebude uveden popis ISO norem, ze kterých je v rámci práce v praktické části čerpáno. Jedná se především o normy pro systém řízení bezpečnosti informací ISMS řady 27 000.

1.3.1 Zákon o kybernetické bezpečnosti

Základním legislativním pilířem je zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti (ZoKB). Aktuální znění má 37 paragrafů a dělí se na šest hlav. Na začátku je důležité podotknout, že vzhledem k implementaci směrnice EU Network and information security 2 (NIS2), právě probíhá příprava nového ZoKB, který by snad měl vejít v platnost na začátku roku 2025. (Zákon č. 181/2014 Sb., 2014)

Hlava I obsahuje vymezení pojmů, které jsou popsány výše v kapitole 1.1. Důležitý je § 3, který definuje orgány a osoby povinné v oblasti kybernetické bezpečnosti. Povinnosti se následujících orgánů a osob:

- *poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),*
- *orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),*
- *správce a provozovatel informačního systému kritické informační infrastruktury,*
- *správce a provozovatel komunikačního systému kritické informační infrastruktury,*
- *správce a provozovatel významného informačního systému,*
- *správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),*
- *provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a*
- *poskytovatel digitální služby.* (Zákon č. 181/2014 Sb., 2014)

Zákon v § 3a pamatuje i na situaci, kdy výše uvedený správce nebo provozovatel nemá sídlo v ČR ani v EU a nemá svého zástupce v EU.

Hlava II se týká systému zajištění kybernetické bezpečnosti a definuje opatření, kterými se musí osoby a orgány povinné dle § 3 řídit. Zároveň jsou povinnosti roztříděny dle jednotlivých písmen § 3. Pokud je průmyslový podnik zařazen do písm. c) § 3, má např. povinnost „zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury…“. (Zákon č. 181/2014 Sb., 2014) V § 5 je bezpečnostní opatření rozděleno na organizační a technická opatření. Některé pojmy jsou podrobně vysvětleny v kapitole 1. 1. výše. Větší detaily, jako je obsah bezpečnostních

opatření, struktura bezpečnostní dokumentace atd. stanovuje prováděcí právní předpis. Definice kybernetické bezpečnostní události a incidentu je popsáno v § 7.

Pro orgány a osoby z § 3 je důležité hlásit kybernetické bezpečnostní incidenty dle § 8. Incidenty se hlásí bezodkladně po jejich detekci buď přímo Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB) nebo provozovateli národního CERT (computer emergency response team) dle rozdělení v § 3.

Hlášené kybernetické bezpečnostní incidenty NÚKIB eviduje dle § 9. Evidence incidentů obsahuje informace o systému, kde se incident objevil, informace o zdroji incidentu, postup při jeho řešení, výsledek řešení atd. Zveřejňování informací o incidentech je omezeno a anonymizováno, aby nemohl být z poskytnutých informací určen dotčený orgán nebo osoba, která incident ohlásila.

Opatření, která může NÚKIB dle ZoKB použít jsou tři:

- Varování
- Reaktivní opatření
- Ochranné opatření

Při uplatnění opatření jsou využity kontaktní údaje osob dle § 3. Požadavky týkající se kontaktních údajů jsou uveden v § 16. Osoby podle ZoKB jsou myšleny jak právnické, tak podnikající fyzické osoby. Osoby i orgány jsou povinné hlásit změny v kontaktních údajích.

Národního CERTu, provozovatele národního CERTu a vládního CERTu se týká § 17, 18 a 20. Národní CERT plní i roli týmu CSIRT (Computer Security Incident Response Team) v rámci EU.

Stav kybernetického nebezpečí je popsán v hlavě III § 21. Jedná se o ekvivalent krizových stavů dle zákona č. 240/2000 Sb. Krizový zákon. Vyhlašuje se maximálně na dobu 7 dnů, prodloužit ji může ředitel NÚKIB maximálně na dobu 30 dnů. V průběhu vyhlášeného stavu kybernetického nebezpečí informuje ředitel NÚKIB o postupech řešení a aktuálním stavu hrozeb. NÚKIB je oprávněn vydávat rozhodnutí a opatření obecné povahy (OOP) pokud je vyhlášen stav kybernetického nebezpečí nebo nouzový stav. (Zákon č. 181/2014 Sb., 2014)

Hlava IV je výkon státní správy a v § 21 a 22 popisuje NÚKIB, jeho povinnosti, pravomoci, sídlo atd. Další paragrafy se týkají provozovatelů základní služby a informačního systému základní služby a zpracování osobních údajů.

Kontroly, nápravná opatření a přestupky jsou obsahem hlavy V. NÚKIB je zodpovědný za výkon kontrol v oblasti kybernetické bezpečnosti. Kontroluje osoby a orgány stanovené dle § 3, jak plní povinnosti, které jim byly přiděleny dle ZoKB. NÚKIB může uložit nápravná opatření při zjištění nedostatků z kontrol. NÚKIB podléhá kontrole poslanecké sněmovny, konkrétně Stálé komisi pro kontrolu činnosti NÚKIB. § 25 obsahuje výčet přestupků a sankce za jejich nesplnění. Hlava VI obsahuje závěrečná ustanovení.

1.3.2 Vyhláška o kybernetické bezpečnosti

Prováděcím právním předpisem k ZoKB je vyhláška č. 82/2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. (Vyhláška č. 82/2018 Sb., 2018)

Vyhláška se dělí na pět částí, první obsahuje úvodní ustanovení včetně vymezení pojmů.

Druhá část se týká bezpečnostních opatření a jejich rozdělení na organizační opatření a technická opatření. Detailněji popisuje zákonné požadavky. Stanovuje povinnosti v rámci organizačních opatření – v systému řízení bezpečnosti informací, řízení aktiv a rizik, organizační bezpečnost, bezpečnosti role, řízení dodavatelů atd. Obdobně jsou požadavky stanoveny v rámci technických opatření – fyzická bezpečnost, bezpečnost komunikačních sítí, správa a ověřování identit, ochrana před škodlivým kódem atd. (Vyhláška č. 82/2018 Sb., 2018)

V třetí části vyhlášky je kategorizace kybernetického bezpečnostního incidentu. Podle kategorie incidentu (I – méně významný, III velmi významný) se odvíjí hlášení na NÚKIB nebo CERT a forma hlášení. Čtvrtá část vyhlášky upřesňuje zákonné požadavky na Reaktivní opatření a kontaktní údaje. Pátá část jsou závěrečná ustanovení. (Vyhláška č. 82/2018 Sb., 2018)

Důležité jsou u vyhlášky přílohy. První příloha se týká hodnocení aktiv a obsahuje stupnice pro hodnocení důvěrnosti, dostupnosti a integrity. Ve druhé příloze je návod na hodnocení rizik a stupnice hodnocení hrozeb, zranitelností a rizik. Jedná se o obecnější návody, které by si měla každá osoba nebo orgán přizpůsobit svým podmínkám. Příloha č. 3 obsahuje vybrané kategorie z katalogu hrozeb a zranitelností. Příloha č. 4 udává povinnosti v oblasti likvidace dat. Likvidací dat lze rozumět jejich odstranění, přepsání a fyzickou likvidací nosiče informace. Příloha č. 5 obsahuje návod, jak si stanovit bezpečnostní politiku a bezpečnostní dokumentaci. Body v příloze jsou podobné postupu dle ČSN ISO 27001. Stanovení výboru pro kybernetickou bezpečnost, manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a další funkce nezbytné pro efektivní výkon IKB jsou uveden v příloze č. 6. Příloha č. 7 dává návrh smlouvy uzavírané s dodavateli pro nastavení řízení dodavatelů. Poslední příloha č. 8 obsahuje formulář pro hlášení kontaktních údajů. Ten slouží, buď k prvotnímu hlášení osoby nebo orgánu, která byla zařazena dle § 3 ZoKB jako povinná osoba, nebo k hlášení změn. (Vyhláška č. 82/2018 Sb., 2018)

1.3.3 Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti

V § 1 ZoKB písm. 3 uvádí *„Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.“* Proto je zde stručně uveden zákon č. 412/2005 Sb. O ochraně utajovaných informací a o bezpečnostní způsobilosti (ZoUI). Některé osoby a orgány nakládají s utajovanými informacemi, a proto k tomu musí mít přizpůsobeny nejen systémy a sítě, ale i například fyzickou ochranu. Zákon klasifikuje informace stupněm utajení. Stupně jsou čtyři:

- Vyhrazené
- Důvěrné
- Tajné
- Přísně tajné (Zákon č. 412/2005 Sb., 2005)

Ochrana utajovaných informací má podobné atributy jako ze ZoKB. Konkrétně je ochrana zajišťována personální bezpečností, průmyslovou bezpečností, administrativní bezpečností, fyzickou bezpečností, bezpečností informačních nebo komunikačních systému a kryptografickou ochranou. Jednotlivé způsoby ochrany a jak je naplňovat jsou v ZoUI popsány. Komunikační systém, který nespadá pod ZoKB, ale pod ZoUI je popsán v § 35. Komunikační systém musí mít

schválený projekt bezpečnosti od NÚKIB, aby mohl být provozován. NÚKIB má v rámci zákona více stanovených úkolů, například certifikuje stínící komory před únikem kompromitujícího vyzařování. (Zákon č. 412/2005 Sb., 2005)

1.3.4 Legislativa Evropské unie a IKB

Agentura, která se zabývá kyberbezpečností v rámci Evropské unie se nazývá ENISA (European Network and Information Security Agency) se sídlem v Aténách. Účelem agentury je zajišťovat kybernetickou politiku EU a spolupracovat se členskými státy, orgány EU a připravovat je na možné kybernetické hrozby. Agentura byla založena v roce 2004. Agentura vydává publikace týkající se IKB, ochrany kritické infrastruktury, řízení rizik, kybernetického krizového řízení atd. (ENISA, 2023)

Pro regulaci organizací v oblasti IKB vydala EU direktivu EU 2016/1148 direktivu NIS. Ta byla transponována do ZoKB, který byl popsán v kapitole výše. V roce 2023 vešla v platnost, pro všechny členské státy, směrnice NIS2, která značně rozšiřuje okruh povinných subjektů. NIS2 zavádí například povinnost vytvořit národní strategii pro kybernetickou bezpečnost a kybernetické bezpečnostní politiky pro určité oblasti. Jedná se o bezpečnost dodavatelského řetězce, koordinované zveřejňování informací o zranitelnostech, incident reporting atd. Dále směrnice požaduje hlubší spolupráci s členskými státy při řešení kybernetických událostí, kybernetickém krizovém řízení, při vymáhání povinností. Součástí jsou i sankce za neplnění povinností při zařazení do tzv. základních subjektů a důležitých subjektů. (Směrnice NIS, 2016; směrnice NIS2, 2022)

Směrnice jako taková není závazná pro členské státy. Závazné je jí implementovat do právního řádu členského státu. Termín pro převedení směrnice do české legislativy je dva roky po jejím vydání. V současnosti probíhá schvalování zákona. Schvalování však provází obsáhlé připomínkování organizací, ministerstev a hospodářské komory a jak bylo zmíněno výše, předpoklad vydání zákona je začátek roku 2025.

1.4 Metody zjištění úrovně informační a kybernetické bezpečnosti

Firmy, které už nějakým způsobem museli IKB řešit, mají alespoň základní přehled o stavu kyberbezpečnosti ve svém prostředí. Firmy, které s IKB teprve začínají si před samotným řízením rizik musí stanovit kontext organizace, stanovit rozsah systému managementu informační a kybernetické bezpečnosti. Existuje mnoho metod, které lze využit. Vzhledem k autorově zkušenostem a omezením této práce byla vybrána metoda C2M2 – Cybersecurity Capability Maturity Model, ENISA risk toolbox. V praktické části budou použity i kroky a metody z řízení rizik dle modelu ISMS a řady ISO norem 27 000 a 31 000. V teoretické části nebudou ISO normy kvůli omezením s publikováním popsány.

1.4.1 Cybersecurity Capability Maturity Model

Účelem C2M2 modelu je identifikovat stav IKB ve společnosti. Model lze použít pro IKB v rámci IT systémů, ale i ICS (někdy také označované jako OT) systémů. Pojmy IT/ICS/OT jsou vysvětleny v kapitole 1.1. Model umožňuje posílit organizaci problematické oblasti IKB, vyhodnotit schopnosti IKB, sdílet znalosti postupy a reference s ostatními organizacemi, stanovit priority

akcí a investic za účelem vylepšení IKB. Model C2M2 je prováděn metodou sebehodnocení, na které se podílí hodnotící tým sestavený dle příručky C2M2. Model je k dispozici zdarma. Model lze vyplňovat buď ve webovém prohlížeči nebo ve formuláři PDF. Proces lze v průběhu vyplňování ukládat ve formátu .json a po vyplnění exportovat do pdf. (C2M2, 2023)

Model rozděluje problematiku IKB do deseti tzv. domén. Jedná se o:

- Aktiva (Asset)
- Hrozby a zranitelnosti (Threat)
- Rizika (Risk)
- Přístup (Access)
- Povědomí (Situation)
- Odezva (Response)
- Třetí strany (Third-parties)
- Řízení pracovní síly (Workforce)
- Architektura (Architecture)
- Program IKB (Program)

Doména Aktiva se týkají aktiv organizace včetně HW, SW a informačních aktiv (dle zařazení organizace do kritické infrastruktury). Doména Hrozby a zranitelnosti zkoumá organizaci, zda má plány, postupy a prostředky pro detekci, identifikaci, analýzu, správu a reakci na hrozby a zranitelnosti. Doména Rizika zkoumá připravenost organizace na řízení rizik, identifikaci, analýzu a reakci na rizika, které se organizace týkají. Jsou brány v potaz i dceřiné společnosti, společná infrastruktura a zainteresované strany. Doména přístup řeší log management společnosti včetně fyzických přístupů k aktivům společnosti. Doména Povědomí se týká sbírání informací z provozovaných systémů, SIEM, hlášení a alarmů. Doména Odezva se dotazuje, zda organizace má zpracovány plány, postupy a technologie pro mitigaci, reakci, analýzu a zotavení z bezpečnostních událostí a incidentů. Doména Třetí strany se zabývá kontrolou rizik, které vznikají ze strany dodavatelů a třetích stran. Doména Řízení pracovní síly zjišťuje stav kultury kybernetické bezpečnosti v organizaci, způsobilost personálu a jeho školení. Doména Architektura spočívá v nastavení architektury kybernetické bezpečnosti organizace, vrstvení sítě, výběr technologie, ovládacích prvků, systém změn atd. Poslední doména Program zkoumá stav strategického plánování a sponzorování aktivit IKB v organizaci. (C2M2, 2023)

V každé doméně je pět podoblastí, které obsahují otázky na danou podoblast. Odpověď lze vybrat ze čtyř možností – neimplementováno, částečně implementováno, značně implementováno a plně implementováno.

Na základě odpovědí jsou jednotlivé oblasti zahrnuty do tzv. MIL, které jsou rozděleny do úrovně 0 až 3. Úroveň 0 znamená, že činnosti nejsou v dané oblasti vůbec prováděny, v úrovni jedna jsou prováděny počáteční činnosti, ale většinou ad hoc. V úrovni 2 je k postupům vytvořena dokumentace a k procesu jsou přiděleny adekvátní zdroje. Nejvyšší úroveň znamená, že činnosti jsou řízeny organizačními politikami nebo organizačními příkazy, jsou přiděleny zodpovědnosti, pravomoci a povinnosti, personál má dostatečné znalosti a zkušenosti. Efektivnost procesu je hodnocena a ověřována. (C2M2, 2023)

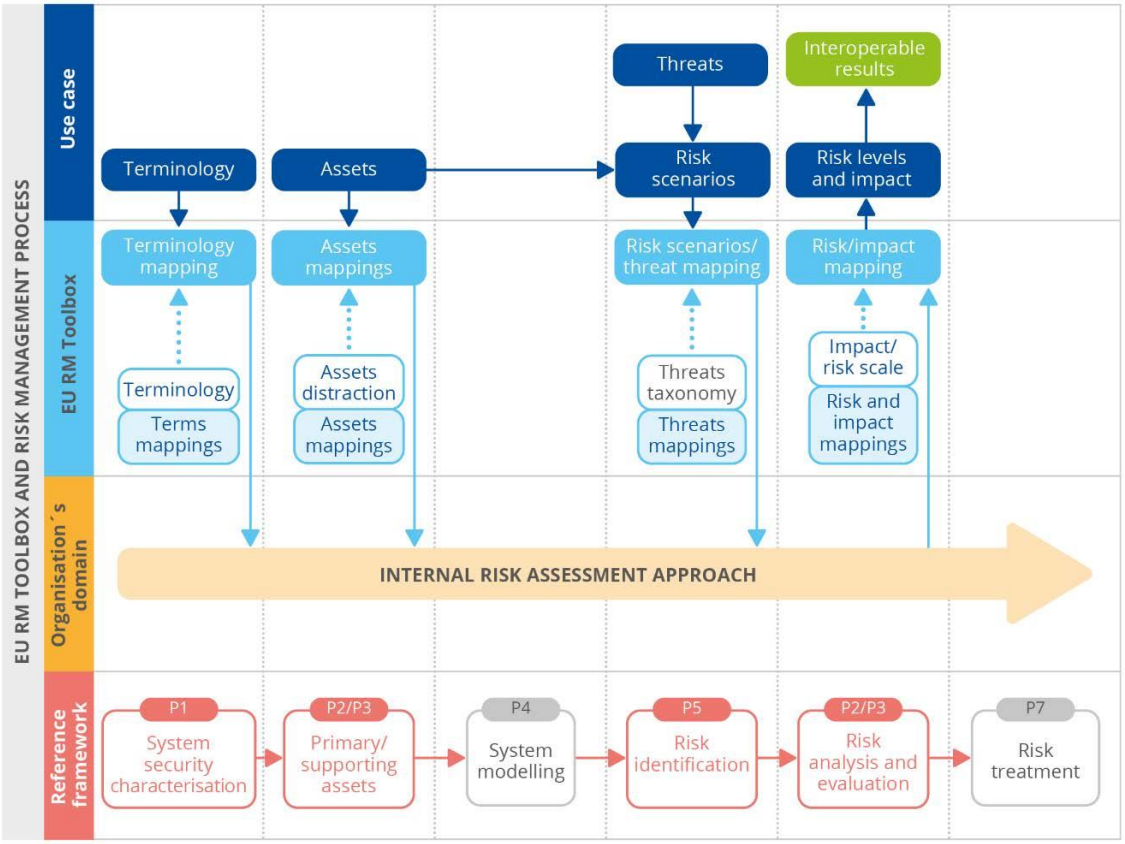
V práci je použitý model verze 2.1 z června 2022. Model C2M2 bude použit v praktické části na fiktivní podnik a bude provedeno zhodnocení úrovně IKB.

1.4.2 ENISA Risk toolbox

Risk toolbox lze přeložit jako sadu nástrojů na řízení rizik. Sada nástrojů spadá pod rámec řízení rizik EU (EU Risk management framework). Hlavní účel sady nástrojů je integrace řízení rizik do organizace a porovnatelnost sady s ostatními metodami pro řízení rizik. Po integraci do podniku neslouží pouze pro sledování aktiv, hrozeb a rizik, ale i k reportování příslušným úřadům nebo zainteresovaným stranám nejen v rámci ČR, ale porovnání a reportování je možné i v rámci EU.

Pro využití v práci bylo čerpáno z dokumentu Interoperable EU Risk Management Toolbox. Dokument se skládá z pěti sekcí a osmi příloh.

- Sekce 1 – Úvod
- Sekce 2 – Interoperabilní sada nástrojů EU RM
- Sekce 3 – Metoda použití
- Sekce 4 – Vývoj sady nástrojů
- Sekce 5 – Závěry
- Příloha I – terminologie
- Příloha II – Aktiva
- Příloha III – Hrozby
- Příloha IV – Úrovně dopadu
- Příloha V – Úrovně rizik
- Příloha VI – Interoperabilní příklady výpočtu rizik
- Příloha VII – Knihovny sady nástrojů
- Příloha VIII – Příklady použití



Obr. 2: Umístění sady nástrojů v procesu řízení rizik

(Interoperable EU Risk management Toolbox, 2023)

Obrázek č. 2 zobrazuje, jak je sada nástrojů EU RM zasazena do prostředí organizace. Z obrázku je patrné, že v organizaci již řízení rizik nějakým způsobem probíhá. Sada nástrojů tak nutně nemusí nahrazovat již zaběhlé procesy pro řízení rizik, ale poskytuje informace pro chápání aktiv, rizik a rizikových scénářů zúčastněným stranám v organizaci i mimo ni. Sadu nástrojů lze použít v organizaci i samostatně, neboť poskytuje dostatečné informace a podklady pro identifikaci aktiv (assets), rizikové scénáře, případy užití, úrovně rizika a dopady. Výsledky hodnocení rizik jsou převedeny na matici rizik, která poskytuje relevantní informace srovnatelné s jinými metodikami pro řízení rizik. Jak již bylo zmíněno, sada nástrojů spadá pod rámec interoperabilního managementu rizik a metodiky ITSRM[2]. (Risk management framework, 2022)

Při zavádění sady nástrojů do organizace by měla organizace definovat a provést následující:

- Vytvořit dohodu o prováděných činnostech během zavádění procesu řízení rizik v organizaci. Při využití metodiky a sady nástrojů existuje definovaný slovník a soubor podmínek, které umožňují popis a pochopení činností při řízení rizik. V kombinaci s další metodikou pro řízení rizik tak nevzniknou duplicitní nebo nejasné činnosti.
- Definovat rozsah v organizaci, kde bude řízení rizik aplikováno. Sada nástrojů umožňuje vymezit a klasifikovat aktiva v definovaném rozsahu organizace. Jakmile organizace identifikuje a klasifikuje aktiva, přiřadí je k možným rizikovým scénářům.
- K hrozbám nebo skupinám hrozeb přiřadit rizikové scénáře. U jednotlivých rizikových scénářů je pak následně použita taxonomie hrozeb, které poskytuje sada nástrojů. Po

provedení těchto kroků je organizace schopná vyhodnotit úroveň rizik a reagovat na získané výsledky.

- Získané výsledky promítnout do rizikové stupnice. Získané výsledky jsou normalizovány, aby mohly být porovnány v rámci organizace a ostatních subjektů. Sada nástrojů poskytuje společnou referenční stupnici k hodnocení rizik. (Risk management framework, 2022)

Sadu nástrojů lze rozdělit na složky, které slouží jako funkční část v oblasti řízení rizik a složky, které jsou tzv. knowledge base neboli znalostní základna pro hodnocení rizik. Složky jsou vzájemně provázané, protože znalostní báze slouží jako zdroj informací pro funkční komponenty, které provádějí řízení rizik. Znalostní základnu lze rozdělit dle Sady nástrojů (Risk management framework, 2022) následovně:

- Terminologie
- Klasifikace aktiv
- Taxonomie hrozeb
- Dopad rizika/stupnice rizika

I přes velikost znalostní báze se nadále předpokládá její rozšiřování v závislosti na nové hrozby nebo hrozby specifické pro dané prostředí (ICS systémy). Sada nástrojů mapuje terminologii a umožňuje srovnání s jinými metodami řízení rizik. Mapování je uloženo ve formě knihoven a komponent pro znalostní bázi.

Terminologie

Účelem části terminologie je porozumět pojmům souvisejícím s řízením rizik napříč použitými metodami. Příloha 1 sady nástrojů obsahuje základní a běžně používané pojmy z metodik a rámců analýzy rizik. Obsahuje i jejich vysvětlení a interpretaci v sadě nástrojů. Sada nástrojů plně implementovala pojmy v ISTRM^2 a ISO 27005.

Klasifikace aktiv

Aktiva se rozdělují, jak už bylo uvedeno výše v základních pojmech, na primární a podpůrná. Jejich identifikace je klíčová při analýze rizik a odhadu dopadu, které organizace utrpí v případě bezpečnostního incidentu. Primární aktiva jsou hlavní procesy a funkce organizace včetně poskytování služeb třetím stranám. Do primárních aktiv jsou zahrnuty i informace, které slouží ke konkrétním hlavním procesům a funkcím organizace. Podpůrná aktiva se skládají z:

- Hardware, zařízení, vybavení síťová zařízení, internet věcí (IoT), ICS systémy, PLC atd.
- Software – firmware, operační systémy, aplikace, procesy spojené s podporou a vývojem softwaru a hardwaru, poskytování služeb, informací a dat.
- Fyzické prostory – skutečné umístění aktiv, jako jsou budovy, místnosti, serverovny atd.
- Organizační struktura – dokumentační podklady organizace jako jsou metodiky, postupy, podpůrné služby (informační a komunikační technologie, sítě, cloud atd.).
- Lidské zdroje – zaměstnanci, dodavatelé atd. (Risk management framework, 2022)

Taxonomie hrozeb

Kategorie hrozeb v sadě nástrojů je v souladu s pokyny ISRM[2] a ISO 27005. Kategorie hrozeb jsou následující:

- Naturogenní hrozby
- Antropogenní hrozby
- Chyby a neúmyslné selhání
- Úmyslné poškozování
- Hrozby spojené se službami (myšleno cloudové služby a služby třetích stran)

Jakmile subjekt identifikuje všechny své hrozby, zařadí je do výše uvedené kategorie. Hrozba je navázána i na konkrétní aktiva, která může ohrozit a důsledky, které u daného aktiva ohrozí (dostupnost, důvěrnost nebo integritu). Sada nástrojů bere v úvahu i původ hrozby, ten může být úmyslný, neúmyslný nebo přírodní). (Risk management framework, 2022)

Dopad rizika/stupnice rizika

Po rozdělení aktiv a identifikaci všech hrozeb je nutné pospat nebo ještě lépe vyčíslit pravděpodobnost výskytu a dopadu hrozby na aktiva firmy. Tím získáme výsledné riziko.

Všeobecně se uznává rozdělení na tři typy hodnocení rizik:

- Kvalitativní
- Semi-kvantitativní
- Kvantitativní

Kvalitativní metoda používá slovní ohodnocení a jsou nutné znalosti procesu ke stanovení rizika. Kvantitativní hodnocení používá číselné ohodnocení na definované stupnici a vyžaduje dostatek definovaných dat, aby bylo možné provést hodnocení. Semi-kvantitativní metoda je kombinací kvalitativní a kvantitativní, výsledek může mít jak slovní, tak číselné vyhodnocení rizika. (Risk management framework, 2022)

Vztah lze dle Sady nástrojů (2023) shrnout do všeobecně uznávané jednoduché rovnice:

Riziko = pravděpodobnost výskytu hrozby x dopad hrozby

Z uvedeného vztahu vyplývá, že existuje pravděpodobnost, s jakou se může konkrétní zranitelnost/hrozba vyskytovat v čase a zasáhnout aktiva subjektu. V praxi se lze setkat ještě s rovnicí, která je doplněná o zranitelnost. (Risk management framework, 2022)

Stanovit interval pravděpodobnosti výskytu je klíčový ve správném výpočtu rizika. Interval se může u různých metod řízení rizik lišit a subjekt provádějící řízení rizik si ho musí zvolit, aby reflektoval co nejreálněji možnost výskytu. Stupnice mohou být v intervalu od denního výskytu až po jednou za století. Sada nástrojů využívá pětistupňový model pravděpodobnosti výskytu hrozby, který je následující:

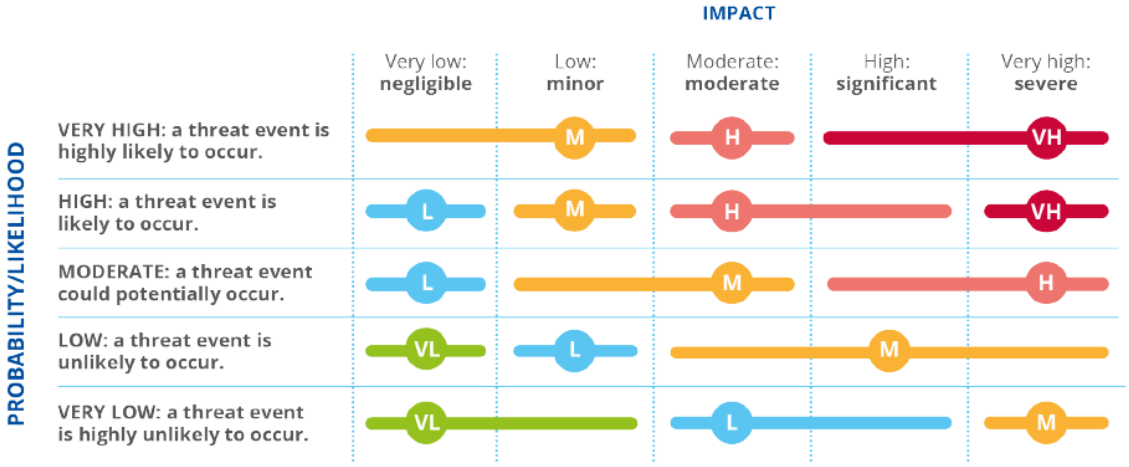
- Velmi vysoká
- Vysoká
- Střední
- Nízká
- Velmi nízká

Druhá součást rovnice je velikost dopadu na subjekt. Dopad lze chápat jako velikost poškození, které vzniklo jako důsledek úmyslných ale i neúmyslných akcí, které ovlivní dostupnost, důvěrnost nebo integritu. (Risk management framework, 2022) Stupnice dopadu se, obdobně jako u pravděpodobnosti výskytu, liší podle použité metody a subjekt provádějící analýzu rizik ho musí vhodně nastavit. Sada nástrojů i u dopadu na subjekt využívá pětistupňový model:

- Velmi vysoký
- Vysoký
- Střední
- Nízký
- Zanedbatelný

Určení dopadu na aktiva subjektu je klíčové pro určení výsledné úrovně rizika a je vhodné ho určit co nejdříve po identifikaci aktiv, tj. co se stane, pokud jsou identifikovaná aktiva nějakým způsobem nedostupná (narušení dostupnosti, důvěrnosti nebo integrity). (Risk management framework, 2022)

Vypočítané riziko záleží na použité metodě a definované stupnici, ale obecně lze říci, že každá metoda stanovuje pásma rizik, která jsou přijatelná/zanedbatelná, rizika, která je třeba pravidelně revidovat a sledovat a rizika, na která je nutné co nejdříve reagovat. Zde popisovaná metoda definuje pět úrovní rizik, úrovně se odvíjejí od nastavených stupnic dopadu a pravděpodobnosti (viz následující obrázek.



Obr. 3: Výsledná matice rizik

(Interoperable EU Risk management Toolbox, 2023)

Obrázek výše zobrazuje matici rizik, kdy vlevo je pravděpodobnost působení hrozby a nahoře dopad. Průnik pravděpodobnosti a dopadu zobrazuje úroveň rizika od velmi nízké (VL), nízké (L), střední (M), vysoké (H) až po velmi vysokou (VH). Po rozčlenění rizik do příslušných pásem jsou organizací přijata opatření pro snížení, eliminaci (pokud je to možné) případně přenesení velmi vysokého a vysokého rizika. U středního rizika lze přijmout náhradní opatření nebo ho pravidelně revidovat. U nízkých a velmi nízkých rizik je vhodné jednou za rok zkontrolovat, zda se pořád nacházejí v pásmu, které není pro organizaci problémové. Důležité je určit tzv. vlastníka rizika, osobu v organizaci, která je zodpovědná za riziko. (Risk management framework, 2022)

Sada nástrojů obsahuje čtyři připravené soubory, které obsahují výše uvedené body nutné pro řízení rizik (terminologie, klasifikace aktiv, taxonomie hrozeb a dopad rizika). Jsou ve formátu Microsoft Excel a v praktické části práce budou upraveny pro použití na fiktivní podnik. (Risk management framework, 2022)

2 Praktická část

V praktické části budou využity základní pojmy a legislativní požadavky pro definování fiktivního podniku. Metody C2M2 a ENISA risk toolbox popsané v teoretické části budou aplikovány na fiktivní podnik, aby odhalily slabá místa v IKB.

2.1 Definice fiktivního podniku

Kapitola definuje konkrétní parametry fiktivního podniku, které budou využity v dalších částech práce pro určení úrovně rizik a stavu IKB.

Parametry byly zvoleny tak, aby subjekt spadal do kategorie středních podniků. Je to z důvodu, aby bylo možné co nejreálněji odhadnout aktiva, hrozby a dopady pro subjekt firmy. U velkého podniku by bylo problematické vydefinovat aktiva, především HW (síťově prvky, PLC a celkově architekturu), SW (počet a ceny licencí) atd. Je nutné zmínit, že v rámci implementace NIS2 je sice velikost subjektu základním určujícím prvkem, ale u některých specifikovaných služeb nebude hrát roli a subjekty budou poskytovatelé regulované služby.

U poskytované služby byl použit návrh vyhlášky o regulovaných službách, který se připravuje v rámci implementace NIS2. Práce bere fiktivní podnik jako povinnou osobu tzv. poskytovatele regulované služby a nezohledňuje subjekty, které budou nahrazeny novým zákonem (provozovatelé základní služby, KII atd.). Podnik bude spadat do režimu vyšších povinností, protože jsou specifikovány ve vyhlášce č. 82/2018 Sb., která bude aktualizována. Pro subjekty v režimu nižších povinností bude vytvořen samostatný prováděcí právní předpis. Podnik se zabývá výrobou elektřiny dle regulované služby 2.1 II. tj. je středním podnikem a disponuje výrobnou s celkovým instalovaným elektrickým výkonem nejméně 100 MW. Výrobna je provozována v nepřetržitém směnovém provozu, administrativní část podniku funguje v pracovní dny v obvyklé pracovní době. Výrobna i administrativní část se nachází v jednom areálu. Pro účely a rozsah práce není nutné blíže specifikovat technologii výrobny.

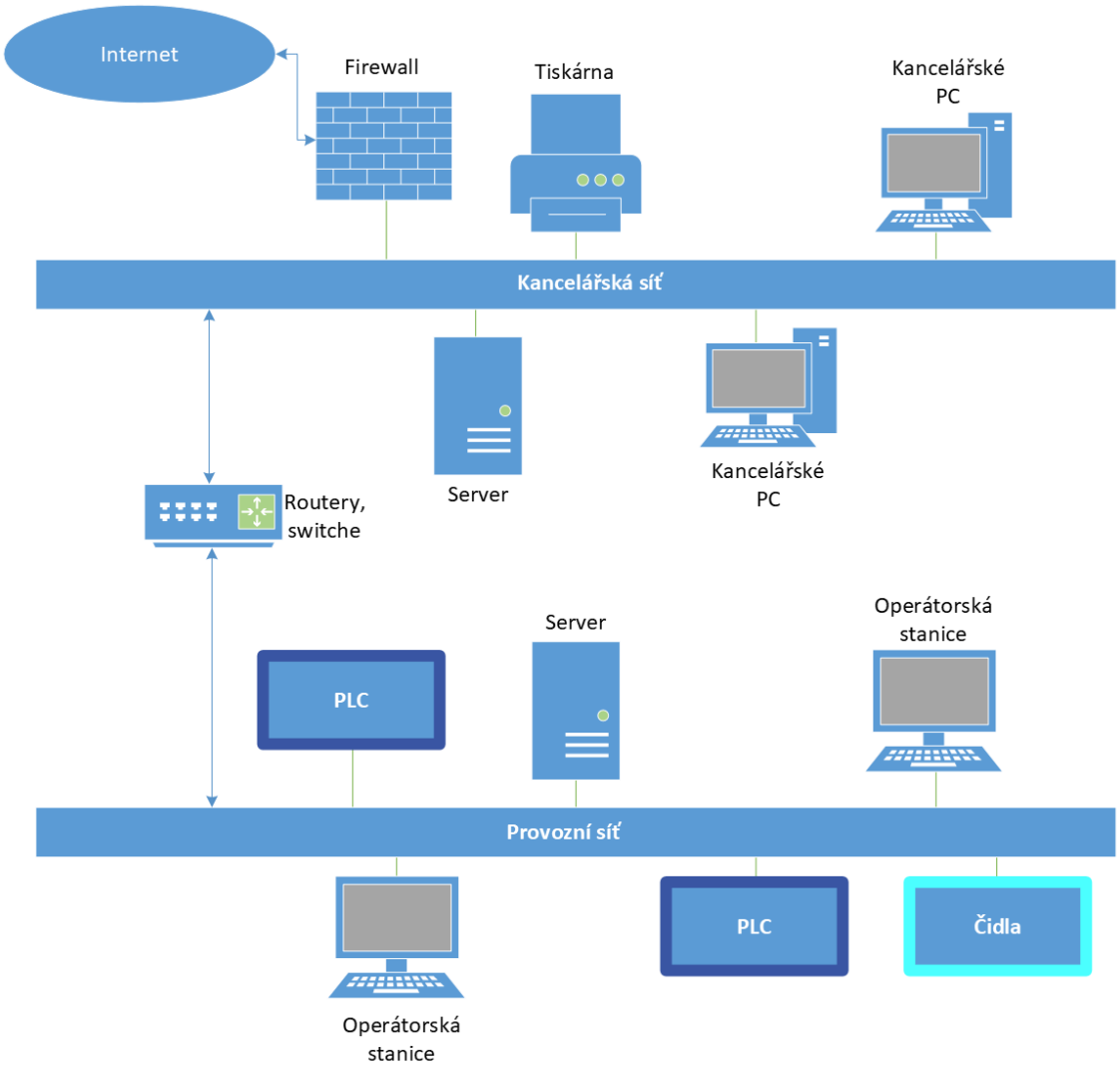
V následující tabulce jsou shrnuty parametry podniku.

Tabulka č. 1: Parametry fiktivního podniku

Fiktivní podnik	
Počet zaměstnanců	200
Poskytovaná služba	2.1 Výroba elektřiny
Roční obrat	≤50 milionů EUR
Výkon výrobny el. Energie	≥100 MW

Zdroj: vlastní zpracování

Síť podniku je v podstatě plochá bez velké segmentace. Zjednodušený diagram podnikové a provozní sítě lze vidět na obrázku č. 4.



Obr. 4: Zjednodušené schéma sítě v definovaném podniku
(Vlastní, 2024)

Kancelářská síť je od internetu oddělena pomocí firewallu. Kancelářská síť se skládá z uživatelských stanic (kancelářská PC a NB), periférií (tiskárny, skenery atd.), serverů (poštovní, webový, ukládání provozních údajů atd.) a je určena pro administrativní chod podniku (ekonomika, účetnictví, management, hodnocení provozu atd.), zároveň slouží i jako diagnostická síť, kde se shromažďují informace z provozní technologie, chodí chybové hlášky a alarmy a je možné se z kancelářské sítě připojovat do provozní sítě. Provozní síť je propojená s kancelářskou sítí pomocí routerů a switchů (na obrázku jeden, ve skutečnosti by jich bylo samozřejmě víc).

Pod provozní sítí (ICS) si lze zjednodušeně představit výrobnu elektrické energie. Čidla sbírají údaje z technologie (tlaky, teploty atd.), PLC slouží pro řízení technologie v provozním pásmu, pro odstavování technologie a další řízení provozu. V provozní síti jsou dále umístěny servery pro ukládání provozních údajů do archivu včetně operátorských stanic, servery pro zálohování, servery pro časovou synchronizaci (GPS, NTP protokol), tiskárny pro tisk provozních údajů, řídící

panely na dozorně (HMI). V obou sítích je nasazeno pouze běžné logování v rámci operačního systému. Sledování prostředků a SIEM není v sítích implementován.

Je uvažováno, že se kybernetická bezpečnost podniku řešila spíše okrajově, i přesto, že má podnik vlastní IT oddělení. Hotovosti pro oblasti IT/ICS jsou řešeny dodavatelsky. Pro implementaci nových legislativních požadavků se uvažuje o rozšíření IT oddělení a zajišťování hotovostí vlastními prostředky.

Výrobna je provozována nepřetržitě s plánovanými odstávkami. Plánovaná odstávka je jednou za rok a trvá přibližně 45 dní. U systémů ICS je uplatňován důraz především na dostupnost, aby byly funkční 24/7. Jakýkoliv výpadek, který má vliv na provozuschopnost výrobny, se podepíše na hospodaření firmy. Denní a roční výroba elektřiny lze vypočítat jako:

$$Denní\ výroba = (výkon\ jednotky * 24)$$

$$Denní\ výroba = 2400\ MWh$$

$$Celková\ roční\ výroba = počet\ dní\ v\ provozu * (výkon\ jednotky * 24)$$

$$Celková\ roční\ výroba = (365 - 45) * (100 * 24)$$

$$Celková\ roční\ výroba = 768\ 000\ MWh = 768\ GWh$$

Pokud by došlo k odstavení výrobní jednotky, je denní ztráta na výrobě 2 400 MWh. Dle serveru kurzy.cz byla v roce 2023 průměrná cena za megawatthodinu 3326,5 Kč. Denní výpadek výroby tak může představovat ztrátu ve výši 7 983 600 Kč, hodinový výpadek výroby může představovat ztrátu 332 650 Kč. (Kurzy.cz, 2024)

2.2 Analýza rizik

Cílem kapitoly je identifikovat a vymezit primární a podpůrná aktiva organizace. Následně z kategorie hrozeb specifikovat katalog hrozeb, který by mohl zastavit provoz nebo ohrozit fungování společnosti. Ze získaných údajů bude provedena analýza rizik. Pro evidenci aktiv, hrozeb a dopadů se využije podkladů ze sady nástrojů ENISA Risk Toolbox, které budou upraveny.

2.2.1 Identifikace aktiv

Primárním aktivem ve fiktivním podniku je proces výroby a prodej elektrické energie, protože se jedná o hlavní proces, resp. obchodní činnost firmy.

Podpůrná aktiva lze rozdělit dle návodu sady nástrojů v teoretické části. Pro lepší orientaci a z hlediska bezpečnosti je vhodnější rozdělit firmu na výrobní a administrativní část, tj. na část IT a ICS, i přesto, že spolu samozřejmě souvisí. Detailní identifikace aktiv je časově náročný proces. Alternativním přístupem k identifikaci aktiv je určení scénářů událostí. Identifikace aktiv přes události umožňuje identifikovat kritická rizika nicméně nevede ke kompletní identifikaci aktiv a rizik s nižší úrovní, může tak vést k opomenutí některých částí systémů s dopadem do dostupnosti, důvěrnosti nebo integrity.

Podnik by měl ke každému aktivu vytvořit jedinečný identifikátor, který bude indikovat i zařazení do oblasti. Aktivum by mělo být dále zařazeno do oblasti (výrobní systémy, bezpečnostní systémy, administrativní systémy atd.). Název aktiva by měl odpovídat co nejblíže popisované

skutečnosti (například firewall Fortigate, router Cisco, software Eset atd.). Každé aktivum by mělo mít vlastníka, tj. osobu zodpovědnou za funkčnost, servis a dostupnost. Volitelně lze doplnit i vazbu na ostatní aktiva například hardware Fortigate a software Fortinet. Na základě bezpečnostní klasifikace každého aktiva by mělo být doplněno jeho hodnocení dle modelu CIA. Příklad, jak by mohla vypadat evidence aktiv ve fiktivním podniku je v příloze č. 1 soubor 02 – Aktiva. Rozdělení aktiv je na HW (výrobní, administrativní část), SW (výrobní, administrativní část), Fyzické prostory (výrobní, administrativní část), lidské zdroje, organizační struktura. (Risk management framework, 2022)

Hardware výrobní části

Firma by měla vycházet z technologického provedení výrobny a na základě rozdělení technologických systémů identifikovat specifický HW nutný k jejich provozu. Například HW klíčový pro:

- Řízení technologie výroby elektrické energie (zdroj)
- Řízení chladících systémů
- Řízení a monitorování elektrických zařízení (transformátory, turbogenerátory atd.)
- Sledování vedení a distribučního zařízení (pokud spadá pod výrobnu)

U HW výrobní části byl zvolen identifikátor HW_V_X, kdy X je pořadové číslo identifikátoru. Oblasti HW je rozdělená na výrobní systém a bezpečnostní systém. Více detailů je v příloze č. 1 soubor 02 – Aktiva, list HW_V. Seznam obsahuje PLC jednotky, převodníky, routery, switche a další HW spadající pod konkrétní systém. V seznamu nejsou uvedena aktiva spadající pod zabezpečovací systémy (kamery, alarmy atd.). Pokud by firma taková aktiva měla, je vhodnější je zpracovat samostatně. Pokud by taková aktiva spadala pod zákon o utajovaných informací, je samostatné zpracování analýzy rizik nutností. (Risk management framework, 2022)

Hardware administrativní část

HW v administrativní části podniku lze rozdělit standardně dle použití.

- Pracovní stanice, které používají zaměstnanci k práci v kanceláři. To může zahrnovat stolní počítače, notebooky, pracovní stanice a další zařízení.
- Servery, které poskytují služby a ukládají data pro zaměstnance a provoz firmy. Servery mohou zahrnovat e-mailové servery, servery pro správu souborů, databázové servery atd.
- Tiskárny a skenery – fyzická zařízení pro tisk, kopírování a skenování dokumentů.
- Síťová zařízení – hardware pro komunikaci a připojení počítačů a dalších zařízení k síti (switche, routery, externí síťové karty, wifi směrovače atd.)
- Zálohovací hardware pro zálohování a archivaci dat pro ochranu před ztrátou nebo poškozením. To může zahrnovat externí disky, pásky, cloudové úložiště atd.
- Bezpečnostní hardware pro ochranu dat a síťové bezpečnosti firmy. To může zahrnovat firewally, jump servery, datové diody a další.

Více detailů je v příloze č. 1 soubor 02 – Aktiva, list HW_A.

Software výrobní část

I pro software výrobní části by se měla firma držet systémového rozdělení výrobny a u každého systému určit SW nutný pro provoz. U specifických provozů, jako je i uvažovaná fiktivní firma, se

budou řídící systémy s největší pravděpodobností skládat ze SW vytvořeného na míru. Může se tak jednat o SW pro výrobní systém, chladící systém, diagnostický systém, SW pro programování PLC jednotek, SCADA systémů atd. Standardní SW by mohl být v databázových systémech, které ukládají data z provozu. (Risk management framework, 2022)

Návrh SW pro výrobní část je uveden v příloze č. 1 soubor 02 – Aktiva, list SW_V.

Software administrativní část

SW v administrativní části budou standardní balíky, které mohou být individuálně upraveny pro potřeby firmy. Shrnout je lze do následujících skupin:

- Kancelářský SW pro práci s dokumenty, tabulkami, prezentacemi, e-maily a dalšími kancelářskými úlohami.
- Účetní SW ke správě účetnictví, fakturace, platby, sledování nákladů a příjmů a dalších finančních operací.
- Databázový SW k ukládání dat o zákaznících, dodavatelích, majetku, materiálu, transakcích a dalších informacích nutných k ukládání.
- ERP SW k řízení podnikových procesů.
- ECM (DMS) SW pro správu dokumentů a jejich obsahu.
- SW pro řízení lidských zdrojů, pokud už není součástí předešlých položek.

Návrh SW pro administrativní část je uveden v příloze č. 1 soubor 02 – Aktiva, list SW_A.

Fyzické prostory výrobní část

Fyzické prostory lze rozdělit na stavební části výrobny a pak provést rozpad na jednotlivé místnosti. Dostatečný rozpad je důležitý z následující identifikace hrozeb, které mohou ovlivnit aktiva firmy (zaplavení objektu, odcizení aktiv atd.).

Je vhodné provázat aktiva z fyzických prostor s aktivy HW (sloupec Vazba v seznamu aktiv). Firma má pak přehled, kde konkrétně se nachází její aktiva. (Risk management framework, 2022)

Návrh evidence fyzických prostor pro výrobní část je uvedena v příloze č. 1 soubor 02 – Aktiva, list FP_V.

Fyzické prostory administrativní část

Provázanost je vhodné provést i v administrativní části podniku. Je předpoklad, že u uvažované firmy bude evidence administrativní části jednodušší a nebude tak rozsáhlá. Nemusí to být však pravidlem, zvlášť pokud má firma více administrativních budov, které nejsou umístěny ve stejném areálu.

Návrh evidence fyzických prostor pro administrativní část je uvedena v příloze č. 1 soubor 02 – Aktiva, list FP_A.

Lidské zdroje

Lidské zdroje jsou společné pro administrativní i výrobní část záměrně. Je totiž možné, že někteří zaměstnanci mohou vykonávat práce v obou oblastech, případně v jedné oblasti fungovat jako rezerva. Zaměstnance lze funkčně rozdělit následovně:

- Provozní směnový personál
- Technický personál určený pro údržbu výrobny
- Personál zodpovědný za administrativní činnosti
- Vedoucí pracovníci zodpovědní za provozní a administrativní činnosti
- Bezpečnostní pracovníci (ostraha, BOZP atd.)
- Dodavatelé

Z hlediska IKB lze zaměstnance rozdělit jednodušeji podle jejich přístupu k systémům. Lze využít i autorizační koncept, pokud ho má firma zpracovaný. Obecně lze rozdělit skupiny podle přístupů na:

- Běžný uživatel
- Administrátor
- Dodavatel/servis

Návrh lidských zdrojů je uveden v příloze č. 1 soubor 02 – Aktiva, list HR.

Organizační struktura

Organizační struktura není úplně přesný název kvůli šíři, kterou pokrývá. Oblast by se mohla jmenovat informační aktiva, protože do oblasti nespadá pouze interní dokumentace, jako jsou metodiky, pracovní postupy atd., ale lze sem zahrnout:

- Licence a povolení pro provoz výrobny
- Údaje o provozu a výkonnosti výrobny
- Klíčoví dodavatelé
- Služby a systémy zajišťované dodavatelsky
- Smlouvy s dodavateli elektřiny a spotřebiteli
- Pojistné smlouvy
- Kapitál pro investice
- Rezervy pro mimořádné situace a pro obnovu

Návrh aktiv spadajících do organizační struktury je v příloze č. 1 soubor 02 – Aktiva, list OrS.

Zpracování aktiv bylo v rámci práce provedeno do jednoho souboru. Z hlediska reálné složitosti provozu a pro zachování přehlednosti by bylo nutné každý systém zpracovat do samostatného souboru. (Risk management framework, 2022)

2.2.2 Identifikace hrozeb

Katalog hrozeb vychází ze sady nástrojů ENISA Risk Toolbox. Firma upraví katalog hrozeb dle podmínek pro výrobní a administrativní část, aby reflektoval skutečné hrozby vzhledem ke geografickému umístění aktiv, jejich připojení a dostupnosti. To lze v rámci firmy provést několika způsoby. Rychlým způsobem je například brainstorming. Hrozby by měly být zařazeny do kategorie zmíněné v teoretické části, jaký prvek modelu CIA hrozba ovlivňuje, jakého je

původu a která aktiva svým působením ohrožuje. I u hrozeb je vhodné mít identifikátory pro lepší přehlednost a možnost provázání s ostatními položkami.

Specifický katalog hrozeb pro uvažovaný fiktivní podnik je v příloze č. 1 soubor 03 – Hrozby, list Katalog hrozeb. Katalog obsahuje vyspecifikované hrozby relevantní pro fiktivní podnik. Pokud má firma k dispozici přístup k ISO normám, vhodný katalog hrozeb a zranitelností, ze kterého lze vybírat, je v přílohách normy ISO 27 005. Ve specifickém katalogu hrozeb má hrozba přiřazený identifikátor ve formátu H_Původ hrozbyX, kde X znamená pořadové číslo a původ hrozby je dle kategorie hrozby. Kvůli rozsahu práce byly jako kategorie hrozeb zvoleny kategorie Naturogenní (N) a Antropogenní (A). Pod ně tak lze umístit i hrozby z dalších kategorií definovaných v teoretické části. Výsledný identifikátor tak může vypadat H_N1, H_A1 atd. (ISO 27005, 2018)

2.2.3 Identifikace rizik a jejich úrovně

Pro účely práce byl zvolen následující model čtyřstupňové úrovně pravděpodobnosti a dopadu:

Tabulka č. 2: Úrovně pravděpodobnosti

Pravděpodobnost	Výskyt
4 - velmi vysoká	méně než za 1/2 roku
3 - vysoká	1x za 1/2 roku
2 - střední	1 x za 2 roky
1 - nízká	1x za 5 let

Zdroj: vlastní zpracování

Tabulka č. 3: Úrovně dopadu

Dopad	Velikost dopadu
4 - Kritický	Kritický, neschopnost vykonávat svoji činnost, ohrožení zdraví, osob a majetku – škody více než 51 milionů Kč
3 - Vážný	Významné dopady do činnosti firmy, vážné následky pro bezpečnost a majetek – škody 6–50 milionů Kč
2 - Významný	Zhoršení výkonu podniku, bez dopadu na bezpečnost a majetek – škody 1–5 milionů Kč
1 - Zanedbatelný	Bez následků na provoz nebo výkon podniku – škody do 1 milionu Kč

Zdroj: vlastní zpracování

Z výše definované rovnice a nastavených modelů pravděpodobnosti a dopadu byla určena následující matice rizik a stupnice rizika:

Tabulka č. 4: Matice rizik

Matice rizik		Dopad			
		Zanedbatelný	Významný	Vážný	Kritický
Pravděpodobnost	Velmi Vysoká	Nízké	Střední	Kritické	Kritické
	Vysoká	Nízké	Střední	Střední	Kritické
	Střední	Nízké	Nízké	Střední	Střední
	Nízká	Nízké	Nízké	Nízké	Nízké

Zdroj: vlastní zpracování

Tabulka č. 5: Úrovně rizika

Stupnice rizika	Výsledné riziko
12–16	Kritické
6–11	Střední
1–5	Nízké

Zdroj: vlastní zpracování

Pro identifikaci rizik včetně určení následků lze využít různé metody, již zmiňovaný brainstorming, dále například analýzu příčin a následků, analýzu způsobů a důsledků poruch, kontrolní seznamy, sebehodnocení atd. Výsledné riziko vychází z pravděpodobnosti výskytu a dopadu, nabývá hodnoty od 1 do 16 a na základě stupnice je riziko zařazeno do jedné ze tří kategorií (viz tabulka č. 5).

Identifikovaná rizika jsou zapsána ve formě evidence rizik a opatření pro jejich zmírnění v příloze č. 1 soubor 04 – Evidence rizik a opatření. Každé riziko má následující parametry:

- unikátní identifikátor (pro lepší rozlišení a identifikaci je ve formátu rok vzniku_X, kde X je pořadové číslo rizika, např. 2024_1),
- popis rizika,
- způsob a následky rizika,
- vlastník rizika,
- nápravná opatření,
- vlastník opatření,
- zbytkové riziko.

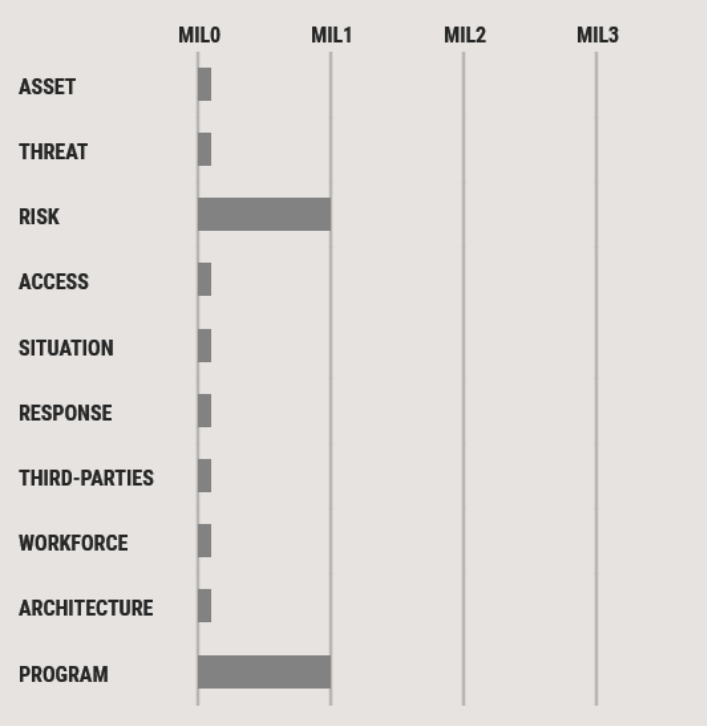
Každé riziko v evidenci rizik na základě zadané pravděpodobnosti a dopadu automaticky ohodnoceno a zvýrazněno dle tabulky č. 5. Kritická rizika je nutné řešit okamžitě, protože mají vliv na provoz a existenci podniku. Střední riziko je nutné řešit v dlouhodobějším horizontu a nízké riziko lze buď sledovat nebo provést opatření takové, které dává ekonomicky smysl.

2.3 Analýza dle C2M2

V rámci kapitoly bude provedena analýza úrovně informační a kybernetické bezpečnosti v rámci podniku metodou C2M2, která byla vyvinuta americkým ministerstvem energetiky. Sebehodnotící metoda pomáhá podniku určit rizikové oblasti IKB v rámci domén, které se pak v rámci analýzy rizik identifikují na konkrétní rizika a v případě nutnosti (střední a kritické riziko) se pro ně přijímají nápravná opatření.

V rámci analýzy bylo vyplněno 356 otázek, ze kterých byl vygenerován report, který lze interaktivně prohlížet ve webovém prohlížeči nebo provést export do pdf. Exportovaný report ve formátu pdf je uveden v příloze č. 2. (C2M2, 2023)

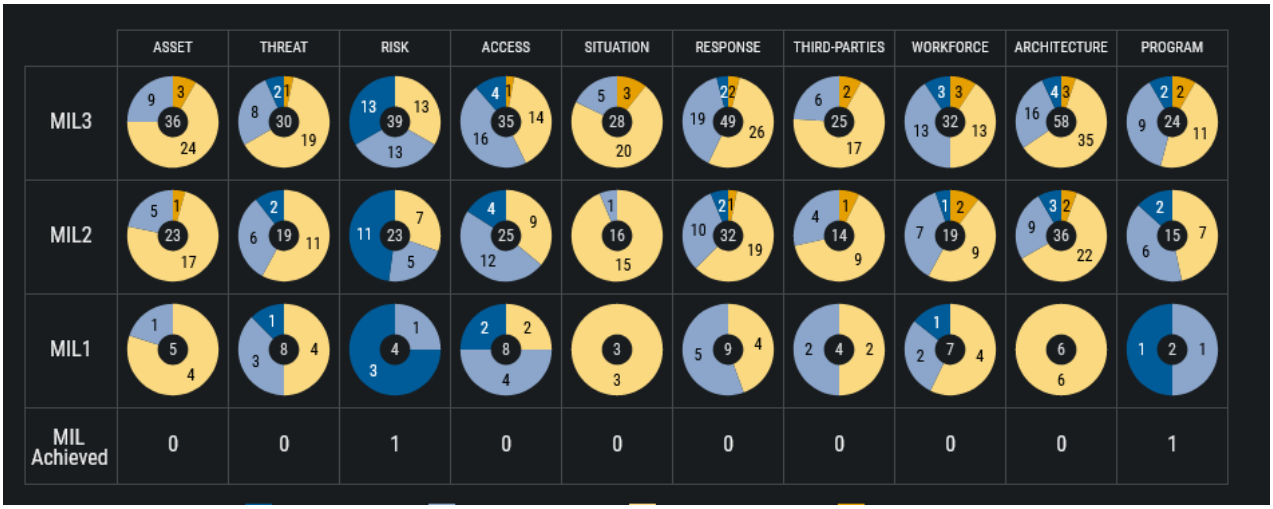
Na následujícím obrázku je zobrazen souhrn domén s úrovněmi, které podnik naplňuje.



Obr. 5: Dosažené úrovně IKB v rámci domén

(C2M2 model, 2024)

Na přehledu lze vidět, že v podniku jsou domény naplňovány na základní úrovni (MIL-0). Vyšší úroveň (MIL-1) dosahuje doména Riziko a Program IKB.



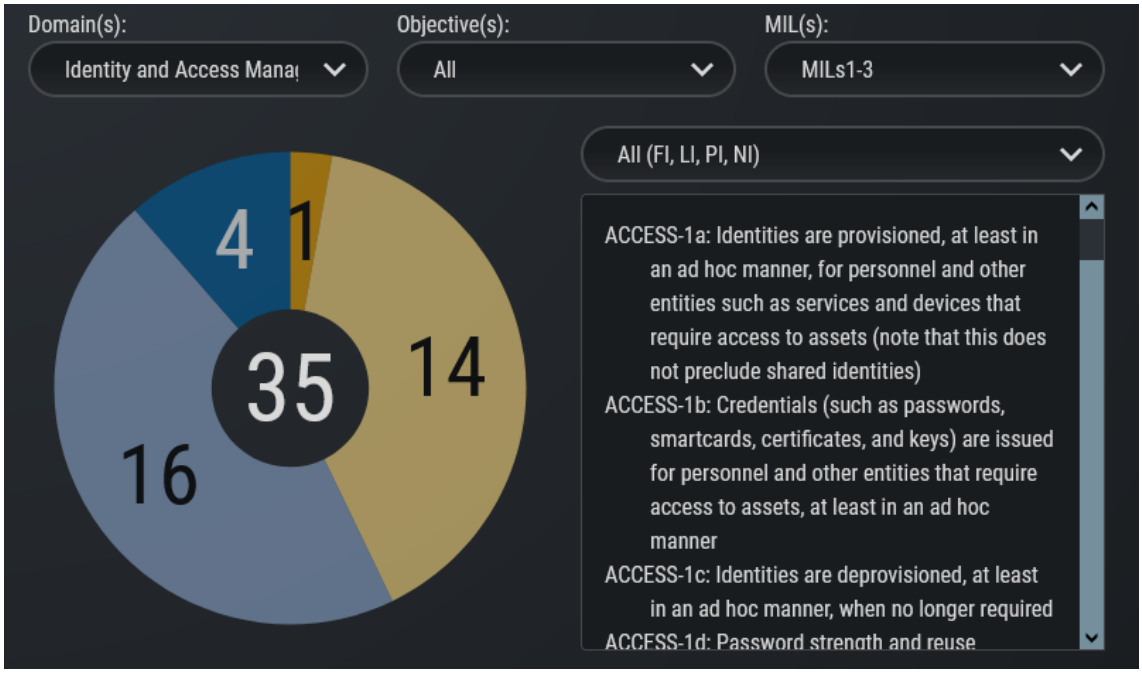
Obr. 6: Přehled domén a jejich plnění

(C2M2 model, 2024)

Na obrázku č. 6 lze vidět plnění jednotlivých úrovních. Oranžová barva označuje neimplementované položky, žlutá barva částečně implementované, ve větší míře indikuje světle modrá a tmavě modrá představuje plně implementovanou položku.

Interaktivní formulář umožňuje filtrování dat po kliknutí na jednotlivé koláčové grafy. Lze tak identifikovat konkrétní problematické oblasti.

Například doména Přístup (logování, fyzické přístupy) je částečně plněna 14 požadavky, ve větší míře naplňuje 16 požadavků, jeden požadavek je neimplementován a 4 jsou plně implementovány.

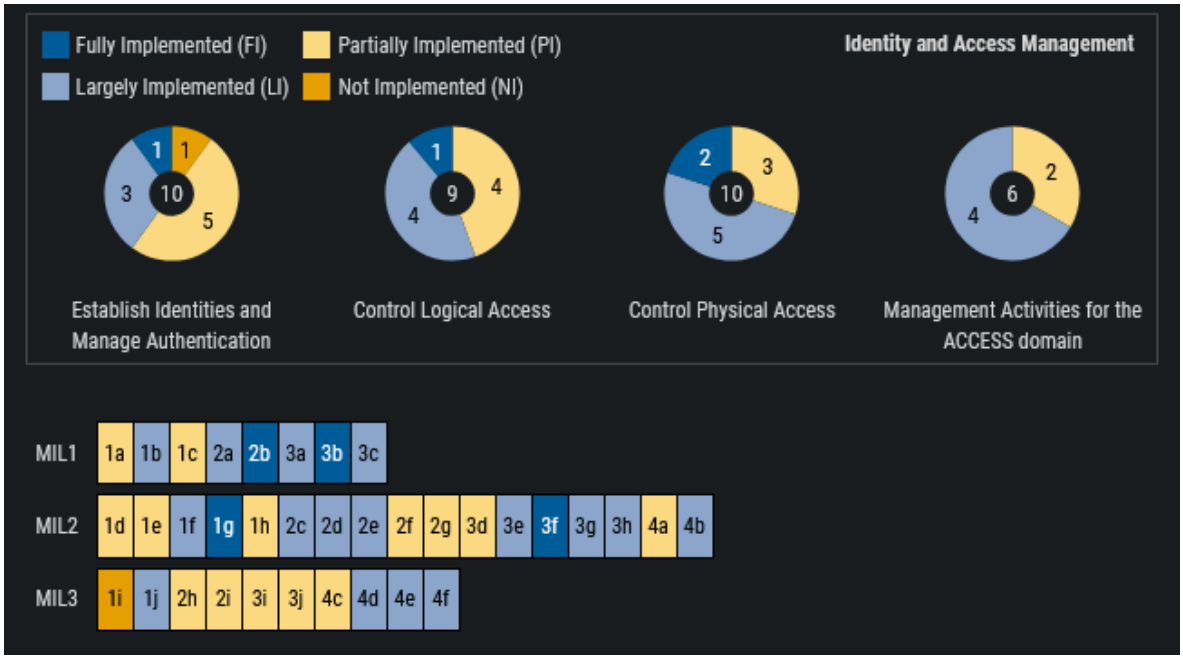


Obr. 7: Přehled plnění domény Přístup

(C2M2 model, 2024)

Dále report zobrazuje už konkrétní požadavky a úroveň jejich naplnění v rámci domény.

Na následujícím obrázku je opět doména Přístup a velikost plnění jednotlivých podoblastí.



Obr. 8: Naplnění podoblastí z domény Přístup

(C2M2 model, 2024)

V další části už je v reportu vidět konkrétní úroveň i s textovým zdůvodněním, které tam hodnotící tým uvedl pro pochopení a zapamatování zadané úrovně.

Například kritérium Access-2i je částečně implementováno, protože neprobíhá logování nestandardních fyzických přístupů, ale pouze základní vstupy v administrativní části podniku. Je nutné nastavit rozšířené logování. To představuje riziko, že případný útočník nebude odhalen. Podobá neshoda je v doméně Povědomí (Situation-2g), která není implementovaná vůbec. Jedná se o detailnější monitorování činností u aktiv vyšší důležitosti. To představuje také riziko, že nebudou odhaleny činnosti, které mohou vést k ohrožení nebo zničení aktiva.

Plně implementovaný požadavek je například v oblasti Hrozby a zranitelnosti konkrétně Threat-2e, který stanovuje, že má mít podnik vytvořený seznam hrozeb s definovanými vlastnostmi. Seznam hrozeb byl zpracován v předchozí kapitole, a proto lze požadavek označit jako plně implementovaný.

Metoda C2M2 ukazuje problematická místa v podniku a vhodně doplňuje metodu analýzy rizik. Výhodou metody je zapojení více zaměstnanců včetně managementu a využití jejich znalostí, aby nedošlo k opomenutí problémových oblastí. Velkou výhodou, jak už bylo uvedeno, je možnost porovnání vyplněných verzí a zobrazení, k jakému došlo posunu od poslední provedené kontroly metodou C2M2. (C2M2, 2023)

2.4 Stav informační a kybernetické bezpečnosti v podniku

Jakmile je provedena analýza rizik v rámci administrativní a výrobní části podniku a metody C2M2, vyplynou ohodnocená rizika na třístupňové škále. Níže je uveden možný přehled kritických rizik, středních rizik a nízkých rizik ve fiktivním podniku. Výpis rizik je uveden v příloze č. 1 soubor 04 – Evidence rizik a opatření.

Kritická rizika:

- Personální nedostatečnost útvaru IT
- Phishingový útok
- Selhání síťového zařízení
- Výpadek systému fyzického zabezpečení
- Ztráta dat z důvodu ransomware útoku

Střední rizika:

- Porucha výrobního systému
- Porucha bezpečnostního systému
- Selhání PLC zařízení
- Plochá síť v administrativní části
- Neoprávněný přístup do systémů ve výrobní části
- Neaktualizovaný software v administrativní části
- Fyzické poškození datového centra požárem
- Zneužití mobilních zařízení
- Neaktualizované zálohy
- Chyba v síťové komunikaci
- Únik citlivých dat z uživatelských PC
- Zavlečení malwaru do administrativní části
- Nesprávná klasifikace citlivých informací
- Nevyřešená ochrana osobních údajů (kamerové systémy)
- Nespolehlivý dodavatel

Nízká rizika:

- Nedodržení bezpečnostních postupů
- Ztráta dat z důvodu hardwarového selhání
- Plochá síť ve výrobní části
- Neoprávněný přístup do systému v administrativní části
- Selhání záložního napájení lidskou chybou
- Chyba v konfiguraci systému ve výrobní části
- Neaktualizovaný software ve výrobní části
- Selhání záložního systému
- Neoprávněné změny v konfiguraci systémů
- Porušení licenčních podmínek software
- Únik informací ze starých datových nosičů
- Neoddělené role v síti, neuplatnění principů nejmenších oprávnění
- Neoprávněné použití USB zařízení

- Chyba v softwarové aplikaci

Kritických rizik, která vyžadují neodkladné řešení by mělo být co nejméně (v případě fiktivního podniku je jich celkem pět). Ostatní rizika mají na řešení delší časový rámec.

2.5 Návrhy nápravných opatření

Navržená evidence rizik pro fiktivní podnik neobsahuje sloupec s termínem zavedení nápravného opatření. Je to z důvodu, že rizika mají více vlastníků opatření a mohou být zmírňována organizačními a technickými opatřeními zároveň. Konkrétní úkoly včetně termínů splnění je lepší nechat na vlastnících opatření a jejich útvarech.

Evidenci rizik a opatření je žádoucí pravidelně aktualizovat i vzhledem k PDCA cyklu v podniku alespoň jednou za rok. Podnik k tomu může vytvořit pracovní skupinu složenou z vlastníků opatření a na základě pravidelných jednání sledovat stav plnění jednotlivých opatření. Cílový stav je po implementaci opatření snížit riziko na nízkou (přijatelnou) úroveň. Pokud to z nějakého důvodu nelze (moc velké finanční náklady, moc složité technologické řešení atd.), je třeba vytvořit na takové riziko výjimku se zdůvodněním.

První kritické riziko se týká nedostatku personálu v útvaru IT. Než podnik přejde k náboru nových zaměstnanců, měl by si analyzovat současný stav útvaru. Kolik pracovníků potřebuje pro zajištění IT a ICS v rámci podniku, jaké je současné vytížení pracovníků a kde lze najít prostor ke zlepšení. Vzhledem k dalším rizikům je třeba aktualizovat kvalifikační katalog a identifikovat dovednosti, které bude podnik vyžadovat po nových zaměstnancích útvaru IT. Následně lze přejít k náboru nových zaměstnanců, případně IT/ICS služby outsourcovat. V případě, že firma nakládá s citlivými údaji, případně utajovanými informacemi, není outsourcing vhodnou metodou, protože jsou nutné další kvalifikační požadavky a bezpečnostní prověrky jak na vlastní zaměstnance, tak na externího dodavatele. Detailnější způsob hledání, náboru, motivace, outsourcingu zaměstnanců, spoluprací se školami atd. není předmětem této práce. Dalším způsobem je možné automatizovat procesy, které jsou prováděny manuálně (automatické zálohování, monitoring atd.), aby byla snížena vytíženost pracovníků útvaru IT.

Druhé kritické riziko je phishingový útok, protože ve firmě nejsou nasazena dostatečná technická a organizační opatření.

Technická opatření pro zmírnění phishingového útoku

- Implementace antiphishingového softwaru – nasazení antiphishingových řešení, která mohou detekovat a blokovat phishingové e-maily a škodlivé odkazy
- Firewall a IDS/IPS – nastavení firewallu a systémů pro detekci a prevenci průniků (IDS/IPS) pro monitorování síťového provozu a blokování phishingových útoků
- Dvoufaktorová autentizace (2FA) – zavedení dvoufaktorové autentizace pro přístup k firemním systémům, což snižuje riziko neoprávněného přístupu i v případě kompromitace hesla
- Omezení přístupu – omezení přístupu k citlivým datům a systémům na základě role a potřeby zaměstnanců
- Šifrování – použití šifrování pro citlivá data jak při přenosu, tak při uložení

Organizační opatření pro zmírnění phishingového útoku:

- Pravidelné školení zaměstnanců – školení zaměstnanců o identifikaci phishingových útoků, včetně ukázek reálných phishingových e-mailů
- Testování zaměstnanců – provádění pravidelných interních phishingových kampaní, které simulují útoky, a následná analýza výsledků pro zlepšení školení
- Zavedení bezpečnostních politik – stanovení bezpečnostních politik, které definují postupy pro identifikaci a hlášení phishingových útoků
- Oznámení incidentů – vytvoření způsobu, jak zaměstnanci mohou hlásit podezřelé e-maily nebo phishingové pokusy IT oddělení
- Kontrola přístupu – zavedení pravidel a kvalifikačních požadavků pro přístup k citlivým informacím a systémům, včetně pravidel pro správu hesel
- Bezpečnostní kultura – podpora bezpečnostní kultury v organizaci, kde je bezpečnost vnímána jako společná odpovědnost všech zaměstnanců
- Aktivní monitorování – monitorování e-mailové komunikace a síťového provozu pro včasné odhalení phishingových aktivit
- Incident response team – vytvoření týmu pro reakci na incidenty, který je připraven rychle reagovat na phishingové útoky a minimalizovat škody, ideálně pracujícím v režimu 24/7 a zajišťován zaměstnanci společnosti
- Zálohování dat – pravidelné zálohování dat, aby bylo možné rychle obnovit data v případě úspěšného phishingového útoku

Třetí kritické riziko je selhání síťového zařízení, jak v administrativní, tak výrobní části podniku. Je důležité rozlišovat IT a ICS část podniku, protože na obě jsou v rámci modelu CIA kladeny jiné požadavky. Opatření lze shrnout do následujících bodů:

Technická opatření pro zmírnění selhání síťového zařízení

- Redundantní síťová architektura – implementace redundantních cest a zařízení, jako jsou záložní routery, switche a firewally, aby se zabránilo výpadkům v případě selhání jednoho zařízení
- Využití clusterů (high availability konfigurace) – použití HA konfigurací pro klíčové síťové prvky, které zajistí, že pokud jedno zařízení selže, další okamžitě převezme jeho funkci.
- Zálohování konfigurací – pravidelné off-line zálohy konfigurací síťových zařízení, aby bylo možné rychle obnovit provoz v případě selhání
- Pravidelná kontrola a údržba – Plánovaná údržbová okna pro kontrolu fyzického stavu zařízení a kontrolu logů
- Aktualizace softwaru – pravidelné aktualizace firmwaru a softwaru na síťových zařízeních, aby byly chráněny před známými zranitelnostmi a chybami
- Monitorování sítě – použití nástrojů pro monitorování sítě (např. Zabbix), které poskytují nepřetržitý přehled o stavu síťových zařízení a upozorní na anomálie
- Segmentace sítě – oddělení IT a ICS sítě, stejně jako segmentace v rámci každé z nich, aby se minimalizovalo riziko šíření selhání nebo útoku
- Firewall a IDS/IPS – použití firewallů a systémů pro detekci a prevenci průniků (IDS/IPS) pro ochranu proti kybernetickým útokům, které mohou způsobit selhání zařízení

Organizační opatření pro zmírnění selhání síťového zařízení

- Školení personálu – pravidelné školení personálu o správném používání a údržbě síťových zařízení, stejně jako o aktuálních bezpečnostních hrozbách
- Zavedení bezpečnostních politik – viz předchozí riziko
- Kontrola prostředí – zajištění optimálních podmínek v serverovnách a síťových centrech, včetně kontroly teploty, vlhkosti a napájení
- Ochrana před fyzickým poškozením – zajištění fyzické bezpečnosti síťových zařízení pomocí uzamykatelných racků, kamerového systému, bezpečnostní službě a kontroly přístupů
- Dokumentace síťové infrastruktury – udržování aktuální dokumentace, včetně topologie sítě, konfigurací zařízení a kontaktů na dodavatele
- Plány obnovy – vypracování a pravidelná aktualizace plánů obnovy po havárii (Disaster Recovery Plans) a plánů kontinuity provozu (Business Continuity Plans)
- Kyber cvičení – pravidelné testování redundance a failover mechanismů, aby byla zajištěna jejich funkčnost v případě potřeby, provádění simulovaných výpadků a dalších cvičení, aby se zaměstnanci mohli lépe připravit na reálné situace

Čtvrté kritické riziko je výpadek systému fyzického zabezpečení (fyzické ochrany). Pokud by došlo skutečně k výpadku fyzického zabezpečení podniku, znamenalo by to kritické důsledky pro firmu. Ať už by se jednalo o možnost vniknutí útočníků do administrativní nebo výrobní části podniku, odnětí výrobní licence nebo finanční sankce od dozorných orgánů, které mají podnik v gesci. Níže jsou uvedena možná řešení snížení kritického rizika:

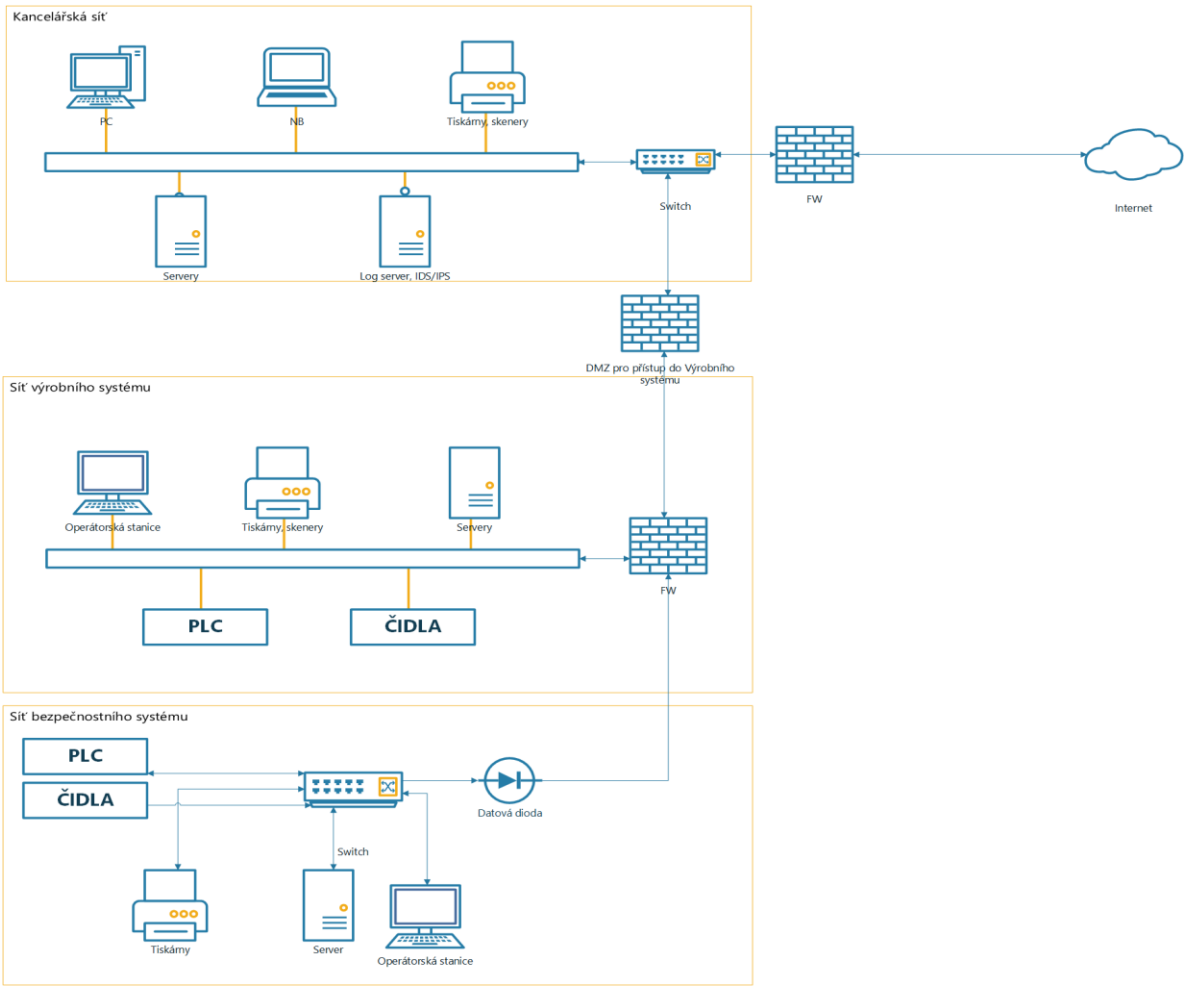
- Redundantní systém – použití redundantních systémů, sítí a zařízení pro kritické komponenty fyzického zabezpečení (UPS, kamery, servery atd.)
- Zálohování dat – viz předchozí rizika
- Pravidelná údržba –harmonogram pro kontrolu a údržbu fyzických zabezpečovacích systémů (kamery, fyzické zábrany atd.)
- Aktualizace softwaru a firmwaru – viz předchozí rizika
- Aktivní monitorování – viz předchozí rizika
- Proaktivní detekce chyb – implementace systémů pro detekci anomálií a prediktivní analýzu
- Ostrovní režim systému fyzického zabezpečení – oddělení od ostatních sítí, tak, aby k němu nebylo možné připojení z jiné sítě
- Školení personálu – pravidelné školení personálu, který spravuje fyzické zabezpečovací systémy, o správném používání a údržbě těchto systémů, stejně jako o aktuálních bezpečnostních hrozbách
- Zavedení bezpečnostních politik – viz předchozí riziko
- Dokumentace infrastruktury – udržování aktuální dokumentace fyzického zabezpečovacího systému, včetně topologie, konfigurací a kontaktů na dodavatele. Vzhledem k důležitosti podniku se může jednat o dokument spadající pod zákon o utajovaných informací a pro přístup k němu bude vyžadován příslušný stupeň oprávnění
- Plány obnovy – viz předchozí riziko
- Kyber cvičení – viz předchozí riziko

- Zvýšení počtu zaměstnanců – vyšší počet personálu fyzické ochrany v klíčových místech firmy

Poslední kritické riziko je ztráta dat z důvodu ramsomware útoku. Stejně jako u předchozích rizik je nutné uplatnit komplexní přístup a využít technická a organizační opatření, která mohou být následující:

- Zálohování dat – viz předchozí riziko
- Testování záloh – Pravidelně testovat zálohy a procesy obnovy, aby bylo zajištěno, že data mohou být v případě útoku obnovena
- Školení personálu – viz předchozí riziko
- Testování personálu – viz předchozí riziko, obdobně jako u testovací phishingové kampaně
- Aktualizace softwaru – viz předchozí riziko
- Správa zranitelností – provádění pravidelných skenů zranitelností a řešení identifikovaných problémů
- Hardening zařízení – mít nastavený hardening zařízení (PC, servery atd.) dle všeobecně uznávaných metodik (např. CIS) nebo využít hardenovaných obrazů od CIS (Linux, Win server, Windows Desktop atd.)
- Antivirový a antimalware software – použití aktualizovaného antivirového a antimalwarového softwaru na všech koncových zařízeních
- Kontrola přístupu – použití přístupových politik, včetně vícefaktorové autentizace (MFA) pro přístup k citlivým systémům a datům
- Segmentace sítě – viz předchozí riziko
- Monitorování sítě – viz předchozí riziko
- Implementace SIEM – implementace systémů pro správu bezpečnostních informací a událostí, které umožňují sledovat a analyzovat bezpečnostní události v reálném čase
- Webová filtrace – implementace webového filtrování, které blokuje přístup na známé škodlivé webové stránky a kontroluje stažený obsah
- Plán reakce na incidenty – viz předchozí riziko a incident response team
- Kyber cvičení – viz předchozí riziko
- Bezpečnostní audity – spolupráce s bezpečnostními odborníky a konzultanty, provádění pravidelných auditů a hodnocení bezpečnosti
- Sdílení informací – účast v bezpečnostních komunitách a sdílení informací o aktuálních hrozbách a bezpečnostních opatřeních včetně informací od státních organizací

Jak by mohla vypadat segmentovaná síť ve fiktivním podniku zobrazuje zjednodušeně obrázek č. 9. V podniku byla vytvořena síť pro bezpečnostní systém, která veškerá data odesílá přes datovou diodu a není možné se do něj přihlašovat vzdáleně. Uživatelsky je to zhoršení komfortu, nicméně z hlediska bezpečnosti je to nezbytný krok ke snížení rizika kompromitace systému. Síť výrobního systému už vzdálené připojení umožňuje, ale pouze přes demilitarizovanou zónu. V reálném podniku a síti by bylo schéma značně složitější, ale pro porovnání s plochou sítí z obrázku č. 4 je to pro potřeby práce dostačující.



Obr. 9: Segmentovaná síť ve fiktivním podniku

(Vlastní, 2024)

Princip řešení dalších rizik s hodnotou střední by byl podobný. Mitigace středního rizika nevyžaduje takovou urgenci a pro řešení by mohlo stačit (neplatí samozřejmě obecně) implementovat pouze organizační opatření, u nízkých rizik postačí jejich sledování. Proto zde již nejsou další způsoby řešení rizik se střední a nízkou hodnotou uvedena.

Závěr

V teoretické části práce bylo cílem představit základní pojmy v oblasti IKB, aby byly pochopitelné a srozumitelné v dalších částech práce. Dále teoretická část obsahovala vymezení podnikání a podniku jako takového v České republice. Kapitola legislativa popsala právní rámec v České republice, který upravuje oblasti IKB. Obsahovala i právní rámec v Evropské unii. Poslední kapitola teoretické části obsahovala metody použité v praktické části. Jednalo se o C2M2 metodu pro určení úrovně IKB v organizaci, metodu Risk toolbox tzv. sadu nástrojů od evropské agentury ENISA. Práce využívala i podklady z ISO norem řady 27 000 a 31 000.

V praktické části byl definován fiktivní podnik včetně použitých sítí uvnitř podniku, na který byly použity metody definované v teoretické části práce. Jako problematická se ukázala definice podniku. Bylo nutné definovat podnik tak, aby byl podnik fiktivní, ale zároveň dostatečně reálný. Dalším problémem se ukázala aplikace metod, protože bylo nutné vhodně kombinovat metody s podnikem, aby byly výsledky rozumně aplikovatelné. V rámci řízení rizik byl vytvořen terminologický slovník pro účely analýzy, byla vytvořena evidence aktiv v administrativní i výrobní části podniku a katalog hrozeb. Z uvedených byla vytvořena evidence rizik a opatření. Evidence obsahuje možná rizika s odpovídající hodnotou a opatřeními na jejich snížení.

Vytvořené dokumenty lze po adekvátní úpravě použít i v reálném podniku pro řízení informačních a kybernetických aktiv. Lze tak konstatovat vzhledem k naplnění definovaných dílčích úkolů, že práce splnila svůj cíl.

Seznam použité literatury

CIS. *CIS Benchmarks*. Online. CIS. 2024. Dostupné z: https://www.cisecurity.org/cis-benchmarks. [cit. 2024-05-05].

Cybersecurity Capability Maturity Model (C2M2). Online. 2023. Dostupné z: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2. [cit. 2023-12-30].

ENISA. Online. 2023. Dostupné z: https://www.enisa.europa.eu/about-enisa. [cit. 2023-12-30].

European Union Agency for Cybersecurity, Lambrinoudakis, C., Gritzalis, S., Xenakis, C. et al., *Interoperable EU risk management framework – Methodology for and assessment of interoperability among risk management frameworks and methodologies*, European Union Agency for Cybersecurity, 2022, https://data.europa.eu/doi/10.2824/07253

EUROPEAN UNION. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. In: . 2016.

EUROPEAN UNION. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). In: . 2022.

INTEROPERABLE EU RISK MANAGEMENT FRAMEWORK. Online. Second. European Union Agency for Cybersecurity, 2022. ISBN 978-92-9204-553-1. Dostupné z: https://doi.org/10.2824/07253. [cit. 2023-12-31].

ISO. ISO 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Edition 3.

ISO. ISO 27002:2022, Information security, cybersecurity and privacy protection — Information security controls. Edition 3.

ISO. ISO 31000:2018, Management rizik - Principy a směrnice. Edition 2.

ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISVS. *Analýza bezpečnosti: Jak hodnotit aktiva?* Online. ISVS. 2023. Dostupné z: https://www.isvs.cz/3-analyza-bezpecnosti-jak-hodnotit-aktiva/. [cit. 2024-05-05].

KURZYCZ. *Elektřina 2023 v CZK - cena elektřiny v roce 2023, minima, maxima, průměr. 1 MWh - měna CZK*. Online. Kurzy.cz. 2024. Dostupné z: https://www.kurzy.cz/komodity/cena-elektriny-graf-vyvoje-ceny/2023-czk-1MWh. [cit. 2024-05-05].

METODIKA PRO IDENTIFIKACI A HODNOCENÍ AKTIV A HODNOCENÍ RIZIK. Online. 4. NÚKIB, 2021.

MINISTERSTVO VNITRA ČR. *Bezpečnostní hrozby*. Online. Ministerstvo vnitra ČR. 2019. Dostupné z: https://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3d%3d. [cit. 2024-04-10].

NÚKIB. *Základní terminologie průmyslových řídicích systémů*. Online. NÚKIB. 2024. Dostupné z: https://osveta.nukib.gov.cz/course/view.php?id=112. [cit. 2024-05-05].

Uživatelská příručka k definici malých a středních podniků. Online. Úřad pro publikace Evropské unie, 2019. ISBN 978-92-79-69931-3. Dostupné z: https://doi.org/10.2873/117802. [cit. 2023-12-30].

Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti): Vyhláška č. 82/2018 Sb. In: . 2018.

Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti): Zákon č. 181/2014 Sb. In: . 2014.

Zákon o obchodních společnostech a družstvech (zákon o obchodních korporacích): Zákon č. 90/2012 Sb. In: . 2012.

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

Přílohy

Příloha č. 1:

01 – Terminologie

01 - Terminologie.xlsx

02 – Aktiva

02 - Aktiva.xlsx

03 – Hrozby

03 - Hrozby.xlsx

04 – Evidence rizik a opatření

04 - Evidence rizik a opatreni.xlsx

Příloha č. 2:

C2M2 zdrojový soubor

C2M2 - Zdrojovy soubor

C2M2 Report

C2M2 - Report