VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
FACULTY OF MECHANICAL ENGINEERING

ÚSTAV VÝROBNÍCH STROJŮ, SYSTÉMŮ A ROBOTIKY
INSTITUTE OF PRODUCTION MACHINES, SYSTEMS AND ROBOTICS

KYBERBEZPEČNOST V PRŮMYSLU
CYBERSECURITY IN THE ENGINEERING INDUSTRY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Kristýna Jemelíková

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Karla Maradová

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA STROJNÍHO INŽENÝRSTVÍ

Zadaní diplomové práce

Ústav:	Ústav výrobních strojů, systémů a robotiky
Studentka:	**Bc. Kristýna Jemelíková**
Studijní program:	Strojní inženýrství
Studijní obor:	Kvalita, spolehlivost a bezpečnost
Vedoucí práce:	**Ing. Karla Maradová**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Kyberbezpečnost v průmyslu

Stručná charakteristika problematiky úkolu:

Cílem práce je provést rešerše, jak vyhodnotit kyberbezpečnost dle platné legislativy ZoKB 181/2014 Sb. v průmyslu a vypracování hodnocení informačních rizik ve firmě.

Cíle diplomové práce:

Popis současného stavu a trendů v oblasti informační bezpečnosti.
Analýza současných legislativních požadavků ČR a EU.
Rešerše požadavků platných norem.
Systémový rozbor řešené problematiky.
Vypracování hodnocení informačních rizik ve firmě.
Vlastní závěry a/nebo doporučení pro další rozvoj řešené problematiky.

Seznam doporučené literatury:

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 9788072048724.

Zákon 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů.

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

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně, dne

L. S.

doc. Ing. Petr Blecha, Ph.D. ředitel ústavu	doc. Ing. Jaroslav Katolický, Ph.D. děkan fakulty

ABSTRAKT

Diplomová práce se zabývá řízením kybernetické bezpečnosti ve výrobním podniku. Teoretická část obsahuje pojmy a poznatky z kybernetické bezpečnosti a rozebírá současné požadavky legislativy a normy řady ISO/IEC 27000. V praktické části jsou navržena opatření ke zvýšení kybernetické bezpečnosti a bezpečnosti informací na základě teoretické části a analýzy současného stavu ve vybrané společnosti.

ABSTRACT

The master's thesis deals with the management of cyber security in a manufacturing company. The theoretical part contains concepts and knowledge of cyber security and discusses the current requirements of legislation and standards of the ISO/IEC 27000 series. In practical part are proposed measures to increase cyber security and information security based on the theoretical background and analysis of current state in the selected company.

KLÍČOVÁ SLOVA

systém řízení bezpečnosti informací ISMS, bezpečnost informací, kybernetická bezpečnost, normy řady ISO/IEC 27000, analýza rizik, bezpečnostní opatření

KEYWORDS

information security management system ISMS, information security, cyber security, standards of ISO/IEC 27000, risk analysis, security measures

BIBLIOGRAFICKÁ CITACE

JEMELÍKOVÁ, Kristýna. *Kyberbezpečnost v průmyslu* [online]. Brno, 2022 [cit. 2021-08-08]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/137006. Diplomová práce. Vysoké učení technické v Brně, Fakulta strojního inženýrství, Ústav výrobních strojů, systémů a robotiky. Vedoucí práce Karla Maradová.

PODĚKOVÁNÍ

Na tomto místě bych ráda poděkovala Ing. Karle Maradové za cenné připomínky a odborné rady při vedení práce. Dále bych chtěla poděkovat panu Janu Havlíkovi ze společnosti FERMAT. za poskytnuté konzultace pro realizaci praktické části této práce. V neposlední řadě bych chtěla vyjádřit poděkování svým blízkým, kteří mi byli oporou po celou dobu mého studia.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že tato práce je mým původním dílem, zpracoval jsem ji samostatně pod vedením Ing. Karly Maradové a s použitím literatury uvedené v seznamu.

V Brně dne 12.8.2021 ……

Kristýna Jemelíková

OBSAH

1 ÚVOD 15

2 TEORETICKÝ ÚVOD 17

2.1 Přehled pojmů 17

2.2 Legislativní požadavky a technické normy 24

2.2.1 Požadavky harmonizačních právních předpisů EU a ČR 24

2.2.2 Technické normy 25

2.2.3 Zákon o kybernetické bezpečnosti (ZoKB) 26

2.2.4 Vyhláška o kybernetické bezpečnosti (VoKB) 27

2.2.5 Normy řady ISO/IEC 27k 28

2.2.6 GDPR 34

2.2.7 Instituce 35

2.3 Systém řízení bezpečnosti informací 35

2.3.1 Ustanovení ISMS 37

2.3.2 Zavádění a provoz ISMS 39

2.3.3 Monitorování a přezkoumání ISMS 42

2.3.4 Údržba a zlepšování ISMS 42

2.4 Analýza a řízení rizik dle ISO/IEC 27005 43

2.4.1 Stanovení kontextu 45

2.4.2 Hodnocení rizik 45

2.4.3 Ošetření rizik 47

2.4.4 Akceptace rizik 48

2.4.5 Komunikace a projednávání rizik 48

2.4.6 Monitorování a přezkoumání rizik 48

3 ANALÝZA SOUČASNÉHO STAVU 49

3.1 Současný stav bezpečnosti informací v ČR 49

3.2 Popis společnosti 51

3.3 Analýza rizik 51

3.3.1 Identifikace a ohodnocení aktiv 51

3.3.2 Identifikace a ohodnocení hrozeb 52

3.3.3 Výpočet míry rizika 55

3.3.4 Vyhodnocení současného stavu 57

4 VLASTNÍ NÁVRH ŘEŠENÍ 59

4.1 Výběr opatření 59

4.1.1 A.5 Politiky bezpečnosti informací 61

4.1.2 A.6 Organizace bezpečnosti informací 62

4.1.3 A.7 Bezpečnost lidských zdrojů 63

4.1.4 A.8 Řízení aktiv 64

4.1.5 A.9 Řízení přístupu 66

4.1.6 A.11 Fyzická bezpečnost a bezpečnost prostředí 68

4.1.7 A.12 Bezpečnost provozu 69

4.1.8 A.13 Bezpečnost komunikací 71

4.1.9 A.14 Akvizice, vývoj a údržba systému 72

4.1.10 A.18 Soulad s požadavky 73

4.2 Soubor opatření 73

4.3 Zhodnocení opatření 75

5 ZÁVĚR 77

6 SEZNAM POUŽITÝCH ZDROJŮ 79
7 SEZNAM ZKRATEK 81
8 SEZNAM OBRÁZKŮ 83
9 SEZNAM TABULEK 85
10 SEZNAM PŘÍLOH 87

1 ÚVOD

Se vzestupem informační společnosti, urychlením komunikace a rozvojem služeb je spojena závislost na informačních technologiích. Informace a data jsou v dnešní době velmi cennou komoditou a je potřeba jim poskytnout náležitou ochranu, protože útoky proti informačním technologiím jsou stále častější a mají značný dopad na veřejný i soukromý sektor.

Tato diplomová práce se zabývá rozborem současného stavu a trendů kybernetické bezpečnosti a rozebírá aktuální situaci v konkrétní společnosti z oblasti strojírenské výroby.

V teoretické části práce jsou vyjmenovány základní pojmy, související harmonizované právní předpisy EU a ČR, normy a postupy pro zavedení a provozování systému řízení bezpečnosti informací. Nejvýznamnějším harmonizovaným právním předpisem v je ČR zákon o kybernetické bezpečnosti, resp. vyhláška o kybernetické bezpečnosti. Dále jsou popsány vybrané normy, především z řady ISO/IEC 27k, a systém řízení bezpečnosti informací ISMS, který slouží pro zajištění odpovídající úrovně kybernetické bezpečnosti a bezpečnosti informací uvnitř organizace.

Praktická část nejprve uvádí celkový pohled na aktuální stav kybernetické bezpečnosti v ČR jak o něm referuje Národní úřad pro kybernetickou a informační bezpečnost ve své zprávě za rok 2020. Dále je provedena analýza současného stavu a jsou navržena opatření ke zlepšení kybernetické bezpečnosti a bezpečnosti informací v brněnské pobočce společnosti FERMAT, resp. v celé společnosti. Analýza současného stavu i návrh opatření se zabývá informacemi a daty bez ohledu na to, zda jsou ve fyzické nebo elektronické formě.

2 TEORETICKÝ ÚVOD

Teoretická část práce obsahuje východiska pro analýzu současného stavu a tvorbu vlastního návrhu řešení. Kapitola vysvětluje pojmy, metody a postupy použité v ostatních částech práce.

2.1 Přehled pojmů

Informační systém (Information system)

Funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky. [1]

Informační a komunikační technologie (Information and communication technologies)

Veškerá technika, která se zabývá zpracováním a přenosem informací, tj. zejména výpočetní a komunikační technika a její programové vybavení. [1]

Data, údaje (Data)

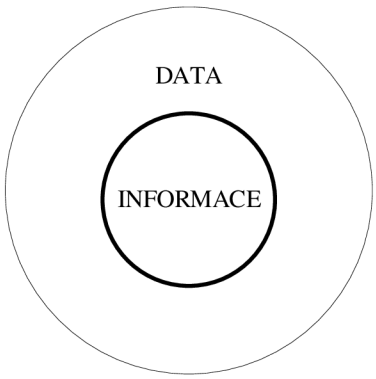
Data jsou jakákoliv fakta získána např. měřením, pozorováním, výpočtem apod.

Počítačová data jsou potom jakékoli vyjádření faktů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem. [2]

Informace (Information)

Údaje, které byly zpracovány do podoby užitečné a pochopitelné pro příjemce. Informace jsou aktivem podstatným pro fungování organizace a vyžadují odpovídající ochranu.

Každá informace je údajem, ale jakákoli uložená data se nemusejí stát informací. Schematicky jsou data množina a informace její podmnožinou, viz. obrázek 1. [3]



Obr. 1 Vztah dat a informací dle Kolouch [4]

Kyberprostor (Cyberspace)

„Digitální prostření umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.“ [5]

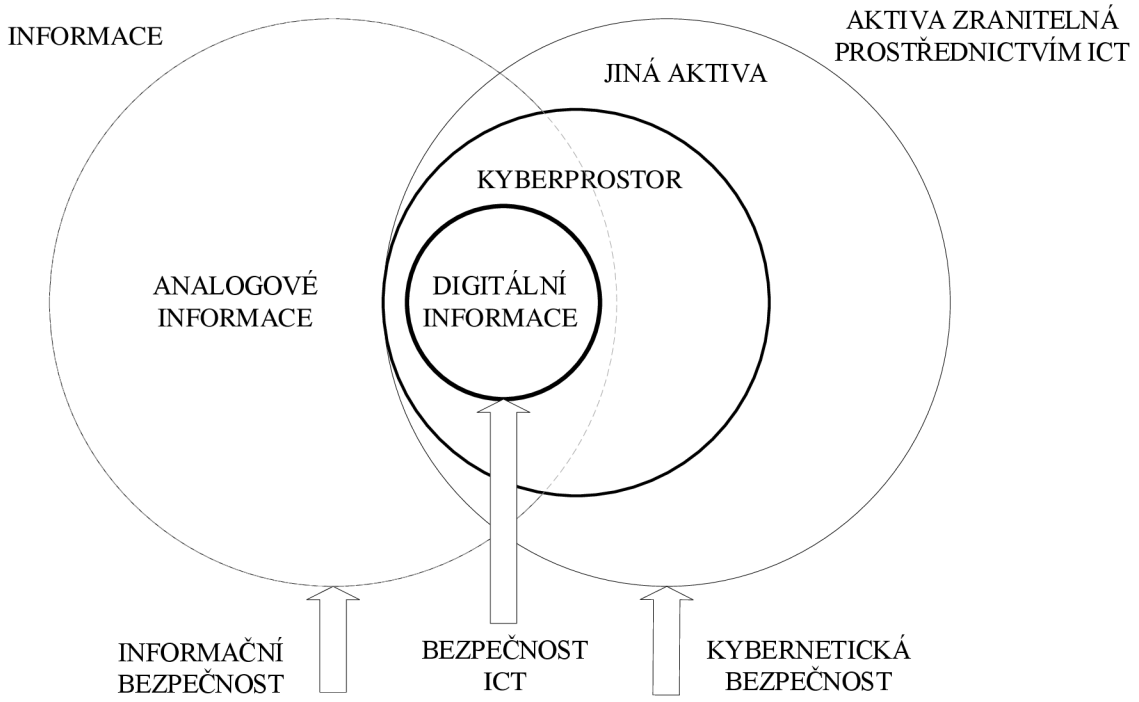
Bezpečnost informací (Information security)

„Zachování důvěrnosti, integrity a dostupnosti informací.“ [6]

Kybernetická bezpečnost (Cyber security)

„Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“ [1]

Bezpečnost informací se zabývá ochranou důvěrnosti, dostupnosti a integrity informací. Nezohledňuje při tom, zda se jedná o elektronickou, listinou nebo jinou formu nosiče informace. Předmětem zájmu kybernetické bezpečnosti je především řešení kybernetických incidentů. Na obrázku 2 je tento vztah znázorněn graficky. V rámci podniku nelze zanedbávat celkové nakládání s daty a informacemi, protože incident v oblasti bezpečnosti informací může způsobit incident kybernetické bezpečnosti.



Obr. 2 Vztah informační a kybernetické bezpečnosti dle Doucek [7]

Důvěrnost (Confidentiality)

Vlastnost, která udává, že k informacím, datům a ICT mají přístup pouze autorizované osoby, entity nebo procesy. Nežádoucí zpřístupnění informací znamená narušení důvěrnosti nebo únik. [4]

Dle vyhlášky o kybernetické bezpečnosti povinná osoba stanoví hodnocení a evidenci aktiv z hlediska důvěrnosti, alespoň v následujícím rozsahu [8]:

Úroveň nízká

- Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.
- V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP: WHITE
- Není vyžadována žádná ochrana.

Úroveň střední

- Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.
- V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: GREEN nebo TLP: AMBER.
- Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.

Úroveň vysoká

- Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje).
- V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: AMBER.
- Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků.

Úroveň kritická

- Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).
- V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: RED nebo TLP: AMBER.
- Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.

Integrita (Integrity)

Vlastnost, že pouze oprávněná osoba může zasáhnout do informací, dat, počítačových systémů a jejich nastavení. Nežádoucí modifikace, která nemusí být ihned patrná a odhalená, znamená narušení integrity. [4]

Dle vyhlášky o kybernetické bezpečnosti povinná osoba stanoví hodnocení a evidenci aktiv z hlediska integrity, alespoň v následujícím rozsahu [8]:

Úroveň nízká

- Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.
- Není vyžadována žádná ochrana.

Úroveň střední

- Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.

- Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis).

Úroveň vysoká

- Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.
- Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.

Úroveň kritická

- Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.
- Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

Dostupnost (Availability)

Vlastnost, díky které, jsou v případě potřeby spolehlivě zpřístupněny informace, data nebo počítačové systémy. Zničení části informací znamená narušení dostupnosti. [4]

Dle vyhlášky o kybernetické bezpečnosti povinná osoba stanoví hodnocení a evidenci aktiv z hlediska dostupnosti, alespoň v následujícím rozsahu [8]:

Úroveň nízká

- Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
- Pro ochranu dostupnosti je postačující pravidelné zálohování.

Úroveň střední

- Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.
- Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.

Úroveň vysoká

- Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.
- Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.

Úroveň kritická

- Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.
- Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Aktivum (Asset)

„Cokoliv, co má hodnotu pro jednotlivce, organizaci nebo veřejnou správu.“ [1]

Podpůrným aktivem jsou technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo zabezpečení informačního a komunikačního systému.

Primárním aktivem jsou informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém [8].

Hrozba (Threat)

Potenciální příčina bezpečnostního incidentu, která může způsobit škodu. Kybernetická hrozba je hrozba v kybernetickém prostoru. [1]

Rozdělení kybernetických hrozeb [7]:

- Lidské
    - úmyslné – externí (hackeři, mezifiremní špionáž), interní (zaměstnanci nebo hosté organizace)
    - neúmyslné – z neznalosti nebo zanedbání povinností
- Technické a technologické – chyba hardwaru nebo softwaru
- Přírodní a fyzické – přírodní pohromy a nehody (požár, vichřice apod.)

Základní hrozbou na informační aktiva je neoprávněné, náhodné nebo úmyslné prozrazení neveřejných informací organizace, jejich upravení, zničení nebo zabránění přístupu oprávněných uživatelům. [7]

Zranitelnost (Vulnerability)

„Slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.“ [8]

Opatření (Control)

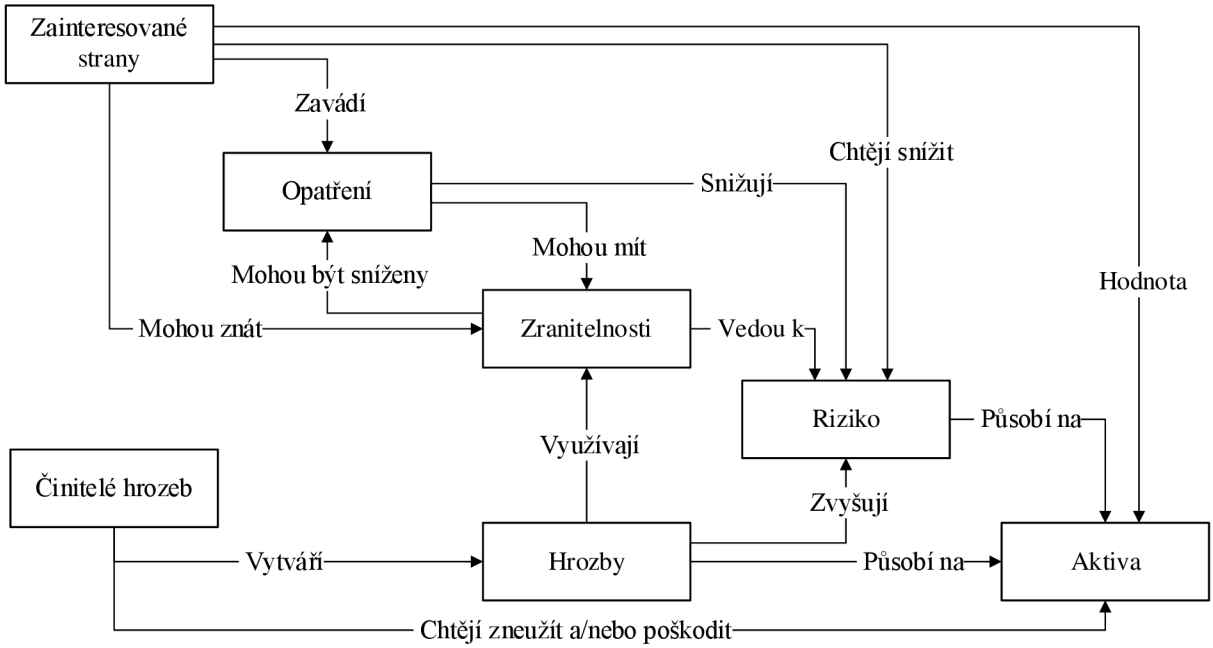
Prostředky ke snížení rizika, včetně politik, strategií, postupů, směrnic, obvyklých postupů nebo organizačních struktur, které mohou být administrativní, technické, řídící nebo právní povahy. [1]

Riziko (Risk)

Možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu. Akceptovatelné riziko je přijatelné pro orgán nebo osobu, které jsou povinny zavést bezpečnostní opatření dle zákona, a není nutné jej minimalizovat dalšími opatřeními. Kybernetické riziko je riziko způsobené kybernetickou hrozbou. [8]

Hodnocení významu rizika zohledňuje pravděpodobnost výskytu rizika a jeho dopady. Pro stanovení opatření k minimalizaci nebo odstranění rizika je vhodné přihlédnout i k povaze rizika či hrozby, zranitelnosti aktiva a jestli může dojít k bezpečnostní události nebo incidentu.

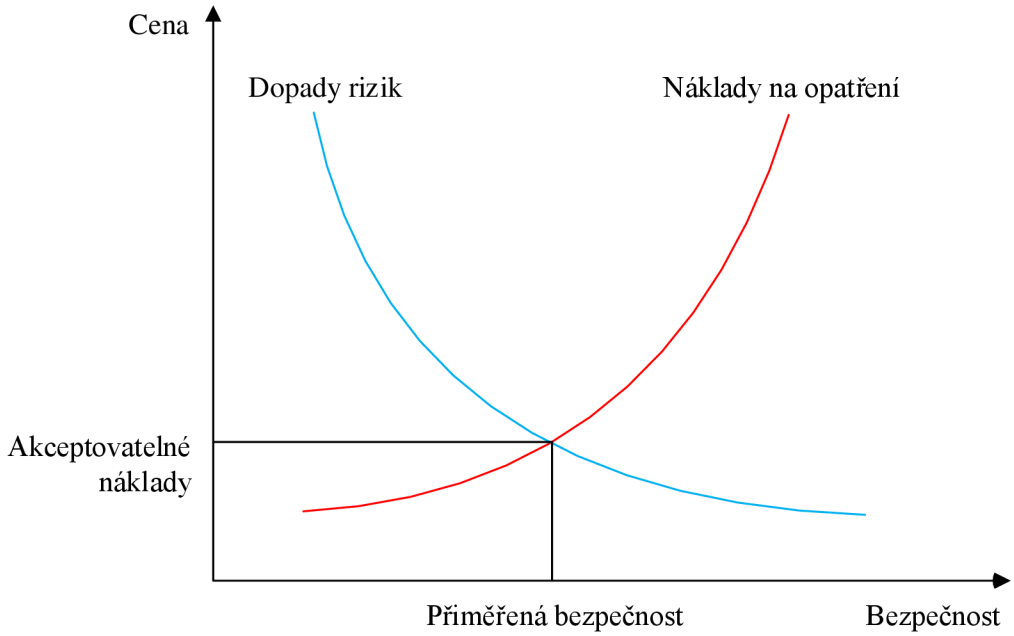
Vztahy mezi pojmy aktivum, hrozba, zranitelnost, opatření a riziko jsou znázorněny na obrázku 3.



Obr. 3 Vztahy mezi pojmy bezpečnosti informací dle ČSN ISO/IEC 27032:2013 [9]

Přiměřená bezpečnost

Velikost úsilí a investic do bezpečnosti musí odpovídat hodnotě aktiv a míře rizik, které mohou vzniknout. Přiměřenou bezpečnost stanovuje bezpečnostní politika organizace. Graf přiměřené bezpečnosti za akceptovatelné náklady je vyobrazen na obrázku 4. [10]



Obr. 4 Přiměřená bezpečnost za akceptovatelné náklady dle Ondrák [10]

Systém řízení bezpečnosti informací (Information security management system ISMS)

Součást systému řízení, která je založená na přístupu k bezpečnostním rizikům, ustavení, implementování, provozování, monitorování, přezkoumávání, spravování a zlepšování bezpečnosti informací. [1]

Kybernetická bezpečnostní událost (Security event)

„Událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity elektronických komunikací.“ [5]

Pokud nastane kybernetická bezpečností událost, nemuselo tím dojít i k narušení bezpečnosti, ale hrozba reálně existovala.

Kybernetický bezpečnostní incident (Security incident)

„Narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“ [5]

K narušení důvěrnosti, integrity nebo dostupnosti aktiv může dojít úmyslným nebo neúmyslným jednáním nebo zásahem vyšší moci. Vyhláška o kybernetické bezpečnosti udává pro potřeby hlášení a zvládání incidentů následující kategorie [8]:

Kategorie III

- Velmi významný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv.
- Řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.

Kategorie II

- Významný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv.
- Řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

Kategorie I

- Méně významný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv.
- Řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

Kybernetický útok (Cyber attack)

Útok na informační a komunikační infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků. Na rozdíl od kybernetického bezpečnostního incidentu se jedná o zcela záměrnou činnost. [1]

2.2 Legislativní požadavky a technické normy

Regulace informačních a komunikačních technologií definováním základních požadavků a norem je složitá. Dynamičnost oboru vyžaduje flexibilitu legislativy, aby bylo možné efektivně reagovat na nové hrozby. Zároveň v kyberprostoru nejsou definovány přesné hranice a legislativa musí mít mezinárodní návaznost.

2.2.1 Požadavky harmonizačních právních předpisů EU a ČR

Na bezpečnost informací v kybernetickém prostoru se obecně vztahuje mnoho předpisů, např. Ústava České republiky, Trestní zákoník nebo Listina základních práv a svobod. Dále jsou v úředním věstníku zveřejňovány všechny právní předpisy (nařízení) EU a směrnice EU, které se týkají všech členských států obecně a toto zveřejnění je podmínkou jejich platnosti. Rozsah předpisů je rozdílný pro orgány státní správy, pro podniky, které jsou součástí kritické infrastruktury (dle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury) a pro běžné průmyslové podniky. Tato práce je zaměřena na analýzu kybernetické bezpečnosti běžného průmyslového podniku a relevantní předpisy jsou následující:

- Směrnice Evropského parlamentu a Rady (EU) 2018/1972, kterou se stanoví evropský kodex pro elektronické komunikace, zveřejněno v Úředním věstníku Evropské unie, L 321, 17. prosince 2018
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS), zveřejněno v Úředním věstníku Evropské unie, L 194, 19. července 2016
- Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích), zveřejněno v Úředním věstníku Evropské unie, L 201, 31. července 2002
- Směrnice Evropského parlamentu a Rady 2013/40/EU o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV, zveřejněno v Úředním věstníku Evropské unie, L 218, 14. srpna 2013
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), zveřejněno v Úředním věstníku Evropské unie, L 119, 4. května 2016
- Rozhodnutí Rady 92/242/EHS o bezpečnosti informačních systémů, zveřejněno v Úředním věstníku Evropských společenství, L 123, 8. května 1992

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Zákon č. 110/2019 Sb., o zpracování osobních údajů
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

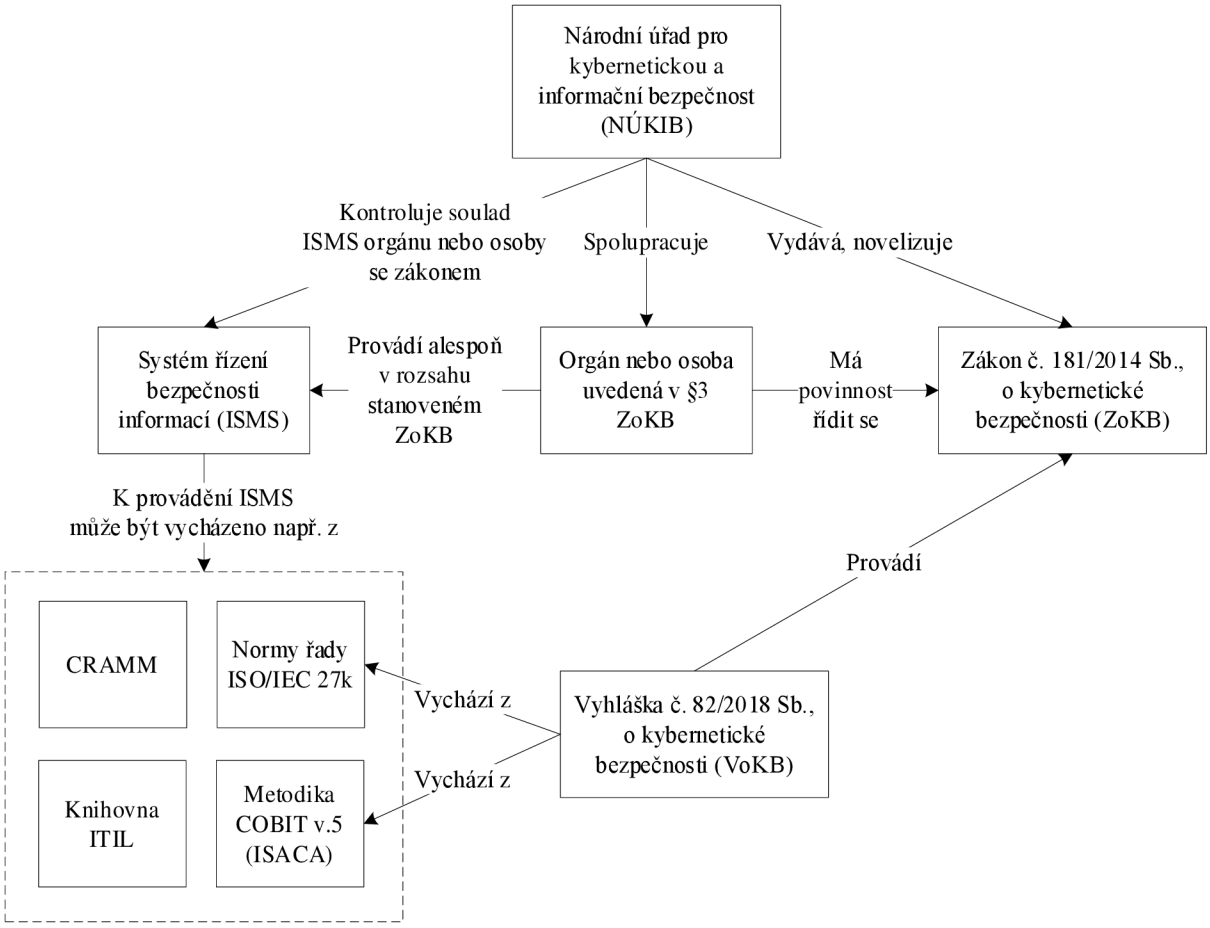
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

2.2.2 Technické normy

- ČSN ISO/IEC 27000:2020 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník
- ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky
- ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací
- ČSN ISO/IEC 27003:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny
- ČSN ISO/IEC 27004:2018 Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení
- ČSN ISO/IEC 27005:2019 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací
- ČSN ISO/IEC 27006:2021 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací
- ČSN ISO/IEC 27007:2020 Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací
- ISO/IEC 27013 Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ČSN ISO/IEC 27031:2016 Informační technologie – Bezpečnostní techniky – Směrnice pro připravenost informačních a komunikačních technologií pro kontinuitu činnosti organizace
- ČSN ISO/IEC 27032:2013 Informační technologie – Bezpečnostní techniky – Směrnice pro kybernetickou bezpečnost
- ČSN ISO/IEC 27033 Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – část 1 až 6
- ČSN ISO/IEC 27035 Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací – část 1 až 3
- ISO/IEC 27036 Information technology – Security techniques – Information security for supplier relationships – part 1 to 4
- ČSN EN ISO/IEC 27040:2015 Informační technologie – Bezpečnostní techniky – Zabezpečení úložišť dat
- ISO/IEC TS 27100:2020 Information technology – Cybersecurity – Overview and concepts

- ISO/IEC TR 27103:2018 Information technology – Security techniques – Cybersecurity and ISO and IEC Standards
- ISO/IEC TS 27110:2021 Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines
- ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
- ISO/TR 14121-2:2012 Safety of machinery – Risk assessment – Part 2: Practical guidance and examples of methods

Pro účely této práce je podrobněji rozebrán Zákon o kybernetické bezpečnosti, Vyhláška o kybernetické bezpečnosti, a především normy řady ISO/IEC 27k z oblasti bezpečnosti informací. Provázanost těchto dokumentů znázorňuje obrázek 5.



Obr. 5 Výřez z blokového schématu k ZoKB dle NÚKIB [11]

2.2.3 Zákon o kybernetické bezpečnosti (ZoKB)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) vstoupil v platnost 29. srpna 2014 s účinností od 1. ledna 2015. Zákon upravuje práva a povinnosti osob, pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zpracovává příslušné předpisy Evropské unie (jedná se o transpozici směrnice Evropského parlamentu a Rady 2016/1148 – směrnice NIS) a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. Tento zákon se nevztahuje

na informační nebo komunikační systémy, které nakládají s utajovanými informacemi. Cílem zákona je stanovení základní úrovně kybernetické bezpečnosti a vytvoření systému opatření, pro předcházení výskytu kybernetických bezpečnostních incidentů. Zákon §21a zřizuje správní úřad pro oblast kybernetické bezpečnosti: Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). [5]

Dle §3 ZoKB jsou orgány a osoby, kterým je uložena povinnosti v oblasti kybernetické bezpečnosti následující [5]:

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b)
b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d)
c) správce a provozovatel informačního systému kritické informační infrastruktury
d) správce a provozovatel komunikačního systému kritické informační infrastruktury
e) správce a provozovatel významného informačního systému
f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d)
g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f)
h) poskytovatel digitální služby

Změna a rozšíření působnosti ZoKB

V současné době probíhá projednávání novelizace směrnice 2016/1148 o opatřeních k dosažení vysoké společné úrovně kybernetické bezpečnosti v Unii, tzv. „NIS 2“. Z pohledu této práce je zásadní, že po implementaci nových předpisů do české legislativy bude podstatně rozšířen okruh povinných osob vůči ZoKB. Běžný strojírenský podnik v současnosti nespadá pod ZoKB, ale v návrhu směrnice jsou mezi důležité subjekty zařazeni mimo jiné i výrobci strojních zařízení.

2.2.4 Vyhláška o kybernetické bezpečnosti (VoKB)

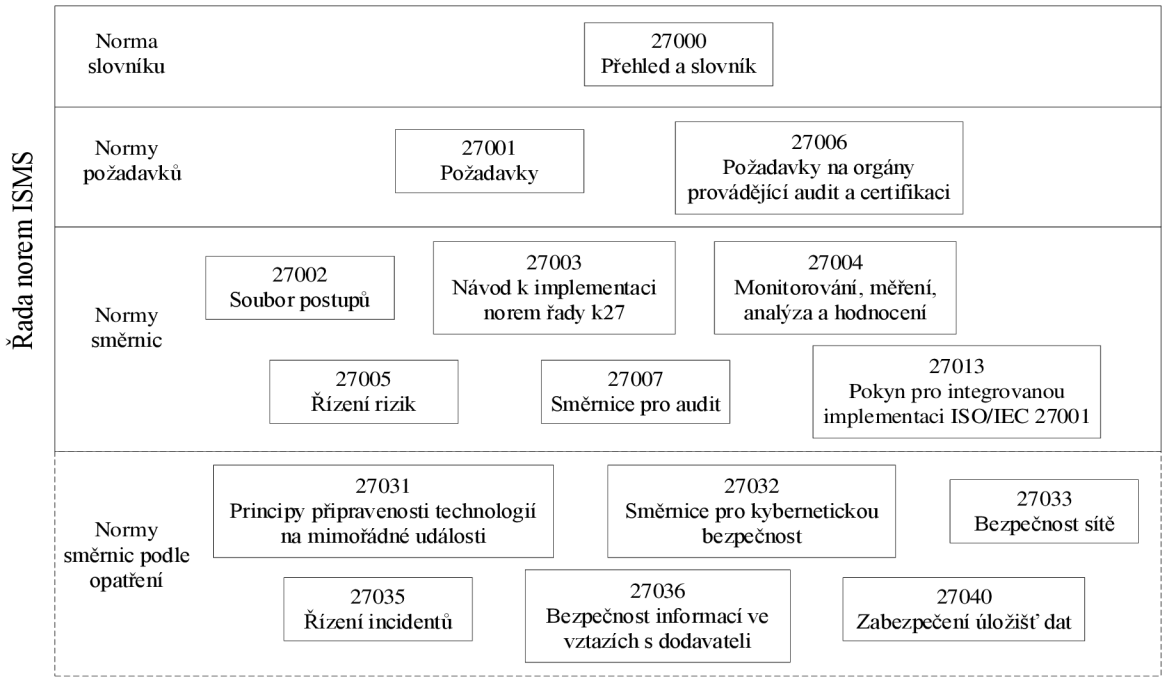
Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) vstoupila v platnost 28. května 2018. Tato vyhláška zapracovává směrnici NIS (směrnice Evropského parlamentu a Rady 2016/1148) a pro informační systémy kritické informační infrastruktury, komunikační systémy kritické informační infrastruktury, významné informační systémy, informační systémy základní služby anebo informační systémy nebo sítě elektronických komunikací, které využívá poskytovatel digitálních služeb, upravuje [8]:

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

Ve vyhlášce jsou podrobněji rozebrána obecná opatření ze ZoKB. Přílohy se zabývají hodnocením rizik a aktiv, vybranými kategoriemi zranitelností a hrozeb, povinnostmi správce ICT při likvidaci dat a jejich nosičů atd.

2.2.5 Normy řady ISO/IEC 27k

Rodina norem ISMS se skládá ze vzájemně souvisících norem, ať již zveřejněných, nebo v procesu vývoje. Součástí jsou normy popisující požadavky na ISMS, požadavky certifikačního orgánu na organizace. Dále normy s podrobnými pokyny nebo interpretací pro všechny procesy, normy pro ISMS jednotlivých odvětví a normy, které se zabývají posuzováním shody ve vůči ISMS. Vztahy mezi vybranými normami řady 27k jsou znázorněny na obrázku 6. Tyto normy jsou vybrány s ohledem zaměření diplomové práce na běžný průmyslový podnik. V současné době probíhá revize norem ISO/IEC 27001 a 27002, které byly vydány v roce 2013. [6]



Obr. 6 Vztahy mezi vybranými normami řady 27k dle ISO/IEC 27000:2020 [6]

Popis vybraných částí normy

ČSN ISO/IEC 27000:2020 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

Tato mezinárodní norma poskytuje přehled systémů řízení bezpečnosti informací, které tvoří předmět rodiny norem ISMS a definuje související termíny. Termíny a definice uvedené v této normě se týkají obecně použitých termínů a definic v rodině norem ISMS. Rodina norem má pomoci organizacím všech typů a velikostí zavést a provozovat systém ISMS. [10]

ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

Norma specifikuje požadavky na ustavení, implementování, udržování a neustálé zlepšování ISMS v rámci organizace. Uvedené požadavky jsou obecného charakteru aplikovatelné

a přizpůsobitelné všem organizacím bez ohledu na typ, velikost a povahu činnosti. Podle této normy probíhá certifikace ISMS a vynechání požadavků je pro certifikaci nepřijatelné. Norma zavádí model PDCA (Plan-Do-Check-Act) jako nástroj k implementaci a zdokonalování efektivnosti ISMS v organizaci. Tento model bude podrobněji rozebrán v kapitole 2.3. [12]

ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

Norma je sbírkou nejlepších bezpečnostních praktik a postupů z oblasti bezpečnosti informací a může být využita jako kontrolní seznam. Obsahuje 14 hlavních oddílů, které definují 35 cílů pro ochranu informačních aktiv proti narušení jejich důvěrnosti, dostupnosti a integrity. Všechna kontrolní opatření nejsou aplikovatelná univerzálně a mohou se objevit požadavky na přizpůsobení podle aktuálních potřeb organizace. Norma popisuje 114 základních opatření pro zajištění bezpečnosti informací, které se dále dělí na specifická opatření. [13]
Hlavní oddíly normy [7]:

- *Politiky bezpečnosti informací* – definice základních pravidel bezpečnosti informací
- *Organizace bezpečnosti informací* – upřesnění struktury pro řízení bezpečnosti informací v organizaci, zajištění bezpečnosti informací v rámci projektového řízení
- *Bezpečnost lidských zdrojů* – vymezení povinností a zajištění povědomí o ochraně informací u všech pracovníků
- *Řízení aktiv* – udržování přehledu o aktivech organizace a stanovení odpovědnosti za udržování jejich ochrany
- *Řízení přístupu* – pravidla pro přidělování a monitorování přístupu k prvkům informačních a komunikačních systémů
- *Kryptografie* – zajištění bezpečnosti prostřednictvím kryptografických nástrojů a řízení kryptografických klíčů
- *Fyzická bezpečnost a bezpečnost prostředí* – definice pravidel pro přístup osob do klíčových prostor organizace a ochrana prvků ICT
- *Bezpečnost provozu* – zajištění spolehlivého a bezpečného chodu produkčních informačních a komunikačních systémů organizace
- *Bezpečnost komunikací* – zajištění spolehlivého a bezpečného chodu produkčních informačních a komunikačních systémů organizace
- *Akvizice, vývoj a údržba systému* – prosazení principů bezpečnosti informací při rozvoji prvků ICT
- *Vztahy s dodavateli* – pravidla a opatření spojená s řízením bezpečnosti informací ve vztahu k externím subjektům
- *Řízení incidentů bezpečnosti informací* – pravidla a postupy pro řešení bezpečnostních incidentů včetně zajištění důkazů
- *Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací* – postupy prevence minimalizace škod plynoucích pro organizaci z havárií, živelních pohrom nebo jiných mimořádných událostí
- *Soulad s požadavky* – organizace dokládá splnění požadavků legislativy, smluvních a jiných závazků

Cílem normy není implementovat veškerá uvedená opatření. Volba a implementace vhodných opatření zůstává na rozhodnutí příslušné organizace na základě hodnocení rizik. V případě

procesu certifikace dle ČSN ISO/IEC 27001:2014 může být takový přístup vyhodnocen jako nedostatečný a je třeba zavést významnější opatření.

ČSN ISO/IEC 27003:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny

Norma obsahuje pokyny k požadavkům a poskytuje doporučení k implementaci ostatních norem série k27 a je určena k využití ve všech typech organizací, které mají v úmyslu zavést ISMS dle ČSN ISO/IEC 27001:2014. Jsou zdůrazněny následující fáze [13]:

- Pochopení potřeb organizace a nutnosti politiky bezpečnosti informací
- Posouzení rizik organizace v oblasti bezpečnosti informací
- Implementace a provozování procesů, kontrol a dalších opatření pro ošetření rizik v oblasti bezpečnosti informací
- Monitorování a přezkoumávání výkonnosti a efektivnosti ISMS
- Snaha o neustálé zlepšování

ČSN ISO/IEC 27004:2018 Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení

Norma poskytuje doporučení pro vývoj a používání metrik pro hodnocení výkonnosti a efektivnosti zavedeného ISMS na základě ČSN ISO/IEC 27001:2014. Výsledky mohou podporovat rozhodnutí při správě, managementu, provozní efektivity a neustálého zlepšování ISMS [13].

ČSN ISO/IEC 27005:2019 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

Norma poskytuje pokyny pro řízení rizik bezpečnosti informací v rámci organizace, ale neobsahuje specifikace nebo doporučení konkrétní metody řízení rizik.
Činnosti řízení rizik definované normou [14]:

- Stanovení kontextu řízení rizik – vymezení základních kritérií pro řízení bezpečnosti informací, definice rozsahu a hranic a stanovení organizační struktury pro řízení rizik.
- Hodnocení rizik – identifikace, analýza a ocenění rizik
- Zvládání rizik – výběr protiopatření k redukci, podstoupení, vyvarování se nebo přenosu rizik a definice plánu zvládání rizik.
- Akceptace rizik – učinění a formální zaznamenání rozhodnutí akceptace rizika a odpovědností za tato rozhodnutí
- Komunikace rizik – výměna a sdílení informací o rizicích
- Monitorování a přezkoumávání rizik – monitorování a přezkoumávání rizik a přiměřená reakce na významné změny

ČSN ISO/IEC 27006:2021 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

Norma specifikuje požadavky a poskytuje pokyny pro orgány provádějící audit a certifikaci ISMS. Vychází z normy ČSN EN ISO/IEC 17021–1:2016, která nastavuje kritéria pro organizace zabývající se auditem případně certifikací systému řízení organizace a doplňuje je odkazy na normu ČSN ISO/IEC 27001:2014.

ČSN ISO/IEC 27007:2020 Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací

Norma obsahuje doporučení pro řízení programu auditu ISMS, provádění auditů a odbornou způsobilost auditorů ISMS. Vychází z normy ČSN EN ISO/IEC 19011:2019 (směrnice pro auditování systémů managementu).

ISO/IEC 27013:2015 Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000–1

Norma obsahuje pokyny pro integrovanou implementaci ISO/IEC 27001:2013 a ISO/IEC 20000–1:2019 (specifikace řízení služeb IT převzatá z ITIL).

ČSN ISO/IEC 27031:2016 Informační technologie – Bezpečnostní techniky – Směrnice pro připravenost informačních a komunikačních technologií pro kontinuitu činnosti organizace

Norma se zabývá předpoklady pro zajištění kontinuity fungování ICT v organizaci, řízení bezpečnostních incidentů a následné opětovné zprovoznění služeb.

ČSN ISO/IEC 27032:2013 Informační technologie – Bezpečnostní techniky – Směrnice pro kybernetickou bezpečnost

Norma poskytuje doporučení pro efektivní sdílení informací a koordinaci řízení incidentů mezi organizacemi, uživateli, vládami a poskytovateli služeb. Norma se zaměřuje na klíčové hrozby týkající se kyberprostoru, sociální inženýrství, malware, odcizení identity, řízení rizik v kyberprostoru v rámci organizací a poskytování bezpečných a zabezpečených služeb poskytovateli služeb [14].

ČSN ISO/IEC 27033 Informační technologie – Bezpečnostní techniky – Bezpečnost sítě

Norma se zabývá síťovou bezpečností. Obsahuje celkem 6 částí [14]:

- ČSN ISO/IEC 27033–1:2016 Část 1: Přehled a pojmy – celkový přehled síťové bezpečnosti
- ČSN ISO/IEC 27033–2:2015 Část 2: Směrnice pro návrh a implementaci bezpečnosti sítě – návod k návrhu a implementaci síťové bezpečnosti v organizaci
- ČSN ISO/IEC 27033–3:2015 Část 3: Referenční síťové scénáře – Hrozby, techniky návrhu a otázky řízení – referenční scénáře pro řízení bezpečnosti, hrozeb, návrhů opatření a kontrol.
- ČSN ISO/IEC 27033–4:2016 Část 4: Zabezpečení komunikace mezi sítěmi s využitím bezpečnostních bran – návod pro zabezpečení komunikace mezi sítěmi prostřednictvím síťových bran, firewallů atp.
- ČSN ISO/IEC 27033–5:2016 Část 5: Zabezpečení komunikace mezi sítěmi s použitím virtuálních privátních sítí (VPN) – doporučení pro nezbytná technická opatření k zajištění síťové bezpečnosti prostřednictvím připojení přes virtuální privátní sítě (VPN).
- ČSN ISO/IEC 27033–6:2016 Část 6: Zabezpečení přístupu k bezdrátové IP síti – definuje specifická rizika, metody návrhu a opatření pro zabezpečení bezdrátových a rádiových sítí.

ČSN ISO/IEC 27035 Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací (ISO/IEC 27035 Information technology – Information security incident management)

Norma se zabývá řízením incidentů bezpečnosti informací. Věnuje se postupům včasné detekce incidentů, jejich hlášení, vyhodnocení závažnosti a následné reakce. Dává doporučení pro identifikaci existujících zranitelností, posouzení jejich závažnosti a přijetí odpovídajících opatření. Obsahuje celkem 3 části [14]:

- ČSN ISO/IEC 27035–1:2018 Část 1: Principy řízení incidentů – popisuje proces řízení incidentů bezpečnosti informací, který se skládá z pěti fází.
- ČSN ISO/IEC 27035–2:2018 Část 2: Směrnice pro plánování a přípravu odezvy na incidenty – doporučení, pro přípravu organizace k odpovídající reakci na bezpečnostní incidenty.
- ISO/IEC 27035–3:2020 Part 3: Guidelines for ICT incident response operations – doporučení pro řešení bezpečnostních incidentů.

ISO/IEC 27036 Information technology – Security techniques – Information security for supplier relationships

Norma se zabývá bezpečností informací ve vztazích s dodavateli. Zahrnuje například outsourcing IT, cloudové služby, bezpečnostní služby, úklidové služby, dodavatelské služby, údržba zařízení, služby ohledně konzultací a odborného poradenství atd. Obsahuje celkem 4 části [14]:

- ISO/IEC 27036–1:2014 Part 1: Overview and concepts – vymezení termínů a pojmů v souvislosti s bezpečnosti informací dodavatelských vztahů.
- ISO/IEC 27036–2:2014 Part 2: Requirements – základní požadavky na bezpečnost informací dodavatelských vztahů.
- ISO/IEC 27036–3:2013 Part 3: Guidelines for information and communication technology supply chain security – návod pro zákazníka i dodavatele ICT k řízení rizik bezpečnosti informací (např. malware, padělané produkty) v dodavatelském řetězci.
- ISO/IEC 27036–4:2016 Part 4: Guidelines for security of cloud services – doporučení bezpečnosti informací pro dodavatele a zákazníky cloudových služeb.

ČSN EN ISO/IEC 27040:2017 Informační technologie – Bezpečnostní techniky – Zabezpečení úložišť dat

Norma poskytuje doporučení pro bezpečné ukládání dat.

ISO/IEC TS 27100:2020 Information technology – Cybersecurity – Overview and concepts

Norma poskytuje přehled o kybernetické bezpečnosti a porovná kybernetickou bezpečnost a bezpečnost informací.

ISO/IEC TR 27103:2018 Information technology – Security techniques – Cybersecurity and ISO and IEC Standards

Norma obsahuje pokyny pro využití stávajících standardů ISO a IEC v oblasti kybernetické bezpečnosti.

ISO/IEC TS 27110:2021 Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines

Norma specifikuje pokyny pro vývoj v oblasti kybernetické bezpečnosti. Norma je vhodná pro všechny typy organizací bez ohledu na jejich velikost.

ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

Norma se zabývá řízením informací o soukromí, např. pro zajištění shody s požadavky GDPR Pomáhá organizacím ustavit, udržovat a neustále zlepšovat systém řízení informací o soukromí (PIMS) rozšířením stávajícího ISMS dle ISO/IEC 27001:2013 a ISO/IEC 27002:2013. Norma je vhodná pro všechny typy organizací bez ohledu na jejich velikost.

Porovnání ZoKB (resp. VoKB) s normou ISO/IEC 27001

Norma ČSN ISO/IEC 27001:2014 je univerzální a způsob implementace záleží na příslušné organizaci. Při certifikaci se ověřuje aplikace doporučení ve dvou krocích. Nejprve se zjišťuje soulad dokumentace s normou, následně soulad dokumentace reálnou aplikací v organizaci. ZoKB je závazným předpisem, který udává minimální úroveň ochrany aktiv a má přednost před ČSN ISO/IEC 27001:2014. Proto je nezbytné strukturu dokumentace přizpůsobit zákonu a až poté plnit požadavky normy. Důvodem pro neoznačení normy ČSN ISO/IEC 27001:2014 jako závazné, jsou možné problémy vycházející z volnosti normy, nejednoznačnosti doporučení a z autorských práv a nutnosti pořízení řady norem. Proto si NÚKIB ponechal možnost rychlejší reakce na změny a vliv na metodického vedení při implementaci opatření. V tabulce 1 je uvedeno porovnání přílohy A normy ČSN ISO/IEC 27001:2014 a vyhlášky č.82/2018 Sb. (VoKB). [15]

Tab. 1 Srovnání normy ČSN ISO/IEC 27001:2014 a vyhlášky č.82/2018 Sb. dle Goll [15].

ČSN ISO/IEC 27001:2014 - Příloha A	**Vyhláška č.82/2018 Sb.**
	§03 - Systém řízení bezpečnosti informací
A.5 - Politiky bezpečnosti informací	§30 - Bezpečnostní politika a dokumentace
A.6 - Organizace bezpečnosti informací	§06 - Organizační bezpečnost
A.6.1.1 - Role a odpovědnosti bezpečnosti informací	§07 - Bezpečnostní role
A.15 - Dodavatelské vztahy	§08 - Řízení dodavatelů
A.8 - Řízení aktiv	§04 - Řízení aktiv
	§05 - Řízení rizik
A.7 - Bezpečnost lidských zdrojů	§09 - Bezpečnost lidských zdrojů
A.9 - Řízení přístupu	§12 - Řízení přístupu
	§19 - Správa a ověřování identit
	§20 - Řízení přístupových oprávnění
A.11 - Fyzická bezpečnost a bezpečnost prostředí	§17 - Fyzická bezpečnost
A.12 - Bezpečnost provozu	§10 - Řízení provozu a komunikací
A.13 - Bezpečnost komunikací	§18 - Bezpečnost komunikačních sítí

A.12.2 - Ochrana proti malwaru	§21 - Ochrana před škodlivým kódem
A.10 - Kryptografie	§26 - Kryptografické prostředky
A.14 - Akvizice, vývoj a údržba systémů	§13 - Akvizice, vývoj a údržba
A.14.1 - Bezpečnostní požadavky ICT systémů	§25 - Aplikační bezpečnost
A.14.2 - Bezpečnost v procesech vývoje a podpory	§11 - Řízení změn
A.12.4 - Zaznamenávání formou logů a monitorování	§22 - Zaznamenávání událostí ICT systémů, jeho uživatelů a administrátorů
A.16 - Řízení incidentů bezpečnosti informací	§14 - Zvládání kybernetických bezpečnostních událostí a incidentů
	§23 - Detekce kybernetických bezpečnostních událostí
	§24 - Sběr a vyhodnocování kybernetických bezpečnostních událostí
A.17 - Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	§15 - Řízení kontinuity činností
A.17.2.1 - Dostupnost vybavení pro zpracování informací	§27 - Zajišťování úrovně dostupnosti informací
A.12.7 - Hlediska auditu informačních systémů	§16 - Audit kybernetické bezpečnosti
A.18 - Soulad s požadavky	
	§28 - Průmyslové, řídicí a obdobné specifické systémy
	§29 - Digitální služby

2.2.6 GDPR

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), známé jako GDPR. Toto nařízení v České republice upravuje zákon č. 110/2019 Sb., o zpracování osobních údajů. Nařízení se vztahuje na všechny subjekty, které zpracovávají nebo shromažďují osobní údaje občanů EU, včetně společností a institucí mimo území EU, které působí na evropském trhu. Mezi hlavní cíle patří stanovení komplexní ochrany fyzických osob před neoprávněným nakládáním s jejich daty a osobními údaji, vymezení oprávněných zájmů správců a zpracovatelů, vytvoření systému vymahatelnosti práva s mechanismem sankcí. Nařízení posiluje možnosti fyzických osob na kontrolu nad vlastními osobními údaji prostřednictvím práva na přístup k osobním údajům, práva na přenositelnost osobních údajů mezi poskytovateli služeb a právem být zapomenut. [16]

Ochrana osobních údajů se protíná s oblastí kybernetické bezpečnosti a bezpečnosti informací, ale je pouze jedním z cílů. Za osobní údaje se vztahem ke kybernetické bezpečnosti a bezpečnosti informací lze dle Koloucha [4] považovat např. identifikační číslo, lokalizační údaje, síťové identifikátory (IP adresa, identifikátory cookies), osobní a pracovní e-mail, fotografie, ověřovací identifikační údaje atd.

2.2.7 Instituce

Následující instituce byly zřízeny za účelem dohledu nad legislativou. Jejich úkolem je informační, kontrolní a řídící činnost v oblasti bezpečností informací.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

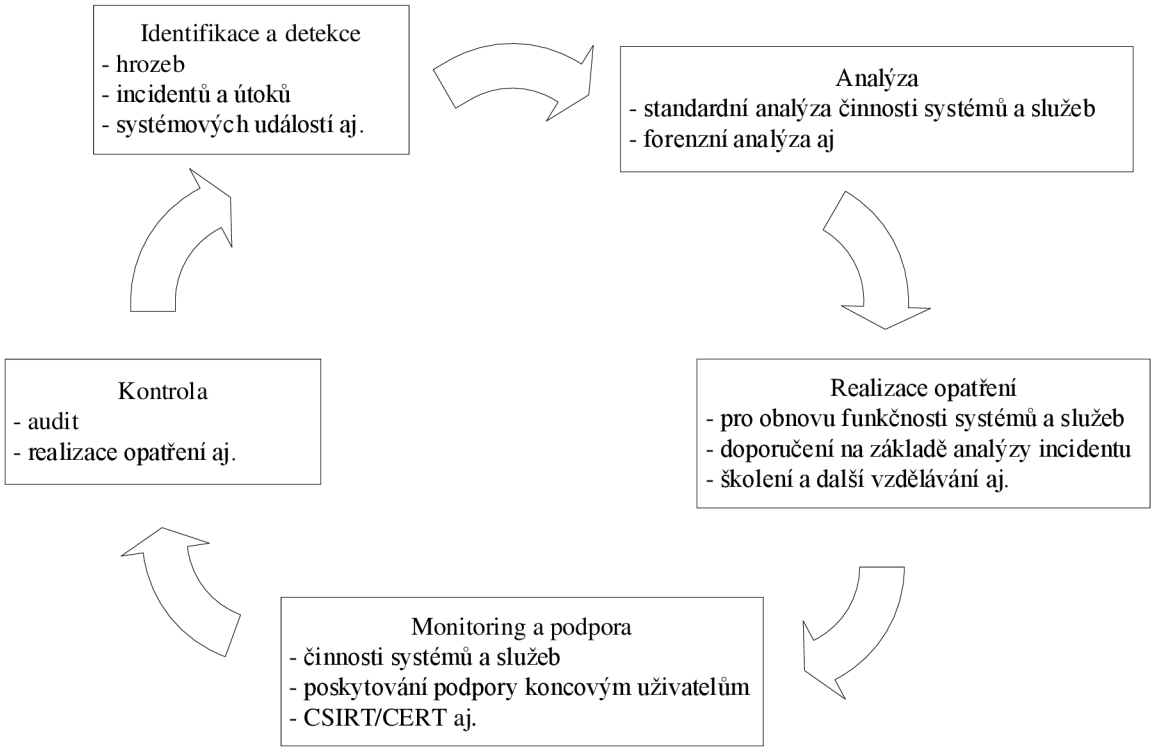
NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo. Úřad vznikl 1. srpna 2017 na základě zákona 205/2017 Sb., kterým byla vyčleněna problematika kybernetické bezpečnosti a bezpečnosti informací z působnosti Národního bezpečnostního úřadu (NBÚ). Výkonnou sekcí NÚKIB je Národní centrum kybernetické bezpečnosti (NCKB). NCKB zajišťuje např. činnost Vládního CERT, výzkum, vývoj a vzdělávací činnost v oblasti kybernetické bezpečnosti, vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímaní příslušných opatření, řešení kybernetických bezpečnostních incidentů, spolupráci na zajištění bezpečnosti kybernetického prostoru s národními i mezinárodními organizacemi atd. [17]

Bezpečnostní týmy

Bezpečnostní týmy typu CERT (Computer Emergency Response Team) nebo CSIRT (Computer Security Incident Response Team) se zabývají efektivní reakcí a prevencí bezpečnostních incidentů v souvislosti s počítačovými sítěmi. Pojem CERT je chráněnou značkou, proto se v praxi používá spíše pojem CSIRT. Bezpečnostní tým by měl být zapojen do světové bezpečnostní komunity a sdílet s ní informace. Na základě vymezené oblasti působnosti je možné příslušný tým kontaktovat při řešení kybernetických bezpečnostních incidentů. Z pohledu ZoKB je v České republice definován Vládní CERT a Národní CERT, další týmy jsou často spojeny s akademickou půdou např. CESNET, CZNIC, CSIRT-VUT, CSIRT-MU atd. Národní CERT (CSIRT.CZ) je provozován sdružením CZ.NIC podle veřejnoprávní smlouvy s NÚKIB a v oblasti kybernetické bezpečnosti poskytuje proaktivní služby a řešení bezpečnostních incidentů. Vládní CERT (GovCERT.CZ) je provozován ze strany NÚKIB a do jeho kompetencí patří sítě státní správy, samosprávy a kritické infrastruktury ČR. [7]

2.3 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací (ISMS) má za cíl udržet důvěrnost, integritu a dostupnost informací. Použití tohoto souboru pravidel dává jistotu směrem k zainteresovaným stranám, že jsou rizika přiměřeným způsobem řízena. ISMS je možné použít na celou organizaci nebo informační systém případně pouze na část organizace nebo informačního systému. Vytvoření a udržování ISMS je nekončící proces, viz. obrázek 7. [4]



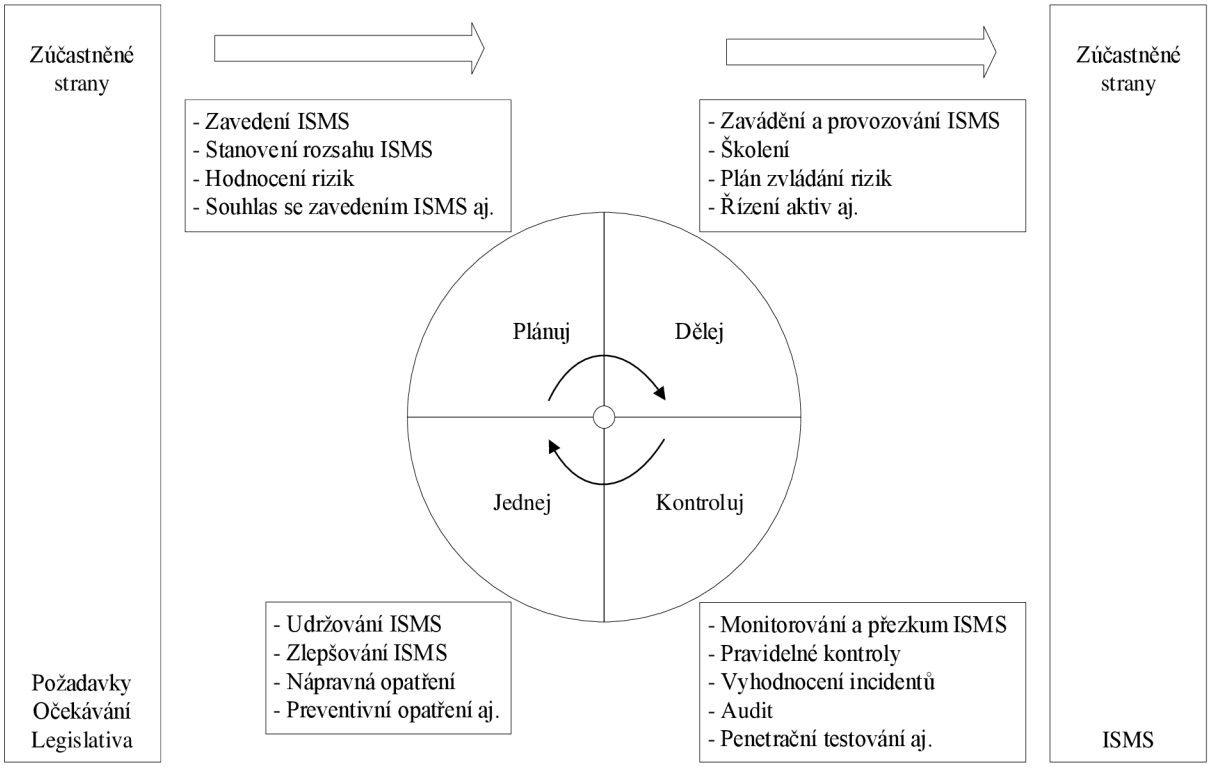
Obr. 7 Životní cyklus kybernetické bezpečnosti dle Kolouch [4]

ISMS v sobě zahrnuje organizační strukturu, politiky, plánování, odpovědnosti jednotlivých uživatelů, různé mechanismy, postupy, procesy a zdroje v rámci celého životního cyklu kybernetické bezpečnosti. Systém řízení je založen na PDCA cyklu neboli Demingově cyklu. PDCA cyklus je metoda postupného zlepšování výrobků, služeb nebo procesů. Součástí modelu PDCA je dokumentace každé etapy. Provádí se v něm čtyři základní činnosti, které se neustále opakují:

- Plánuj (**P**lan) – záměr zlepšení
- Dělej (**D**o) – realizace plánu
- Kontroluj (**C**heck) – ověření, zda se povedla realizace oproti původnímu plánu
- Jednej (**A**ct) – úpravy záměru a případná implementace zlepšení do praxe

Model PDCA aplikovaný na procesy ISMS (obr. 8) [4]:

- Ustanovení ISMS (plánuj) - ustavení politiky ISMS, cílů, procesů a postupů souvisejících s řízením rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace
- Zavádění a provoz ISMS (dělej) - zavedení a využívání politiky ISMS, opatření, procesů a postupů
- Monitorování a přezkoumání ISMS (kontroluj) - posouzení, kde je to možné i měření výkonu procesu vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání
- Údržba a zlepšování ISMS (jednej) - provedení nápravných a preventivních opatření, na základě výsledků interního auditu ISMS a přezkoumání ISMS ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS



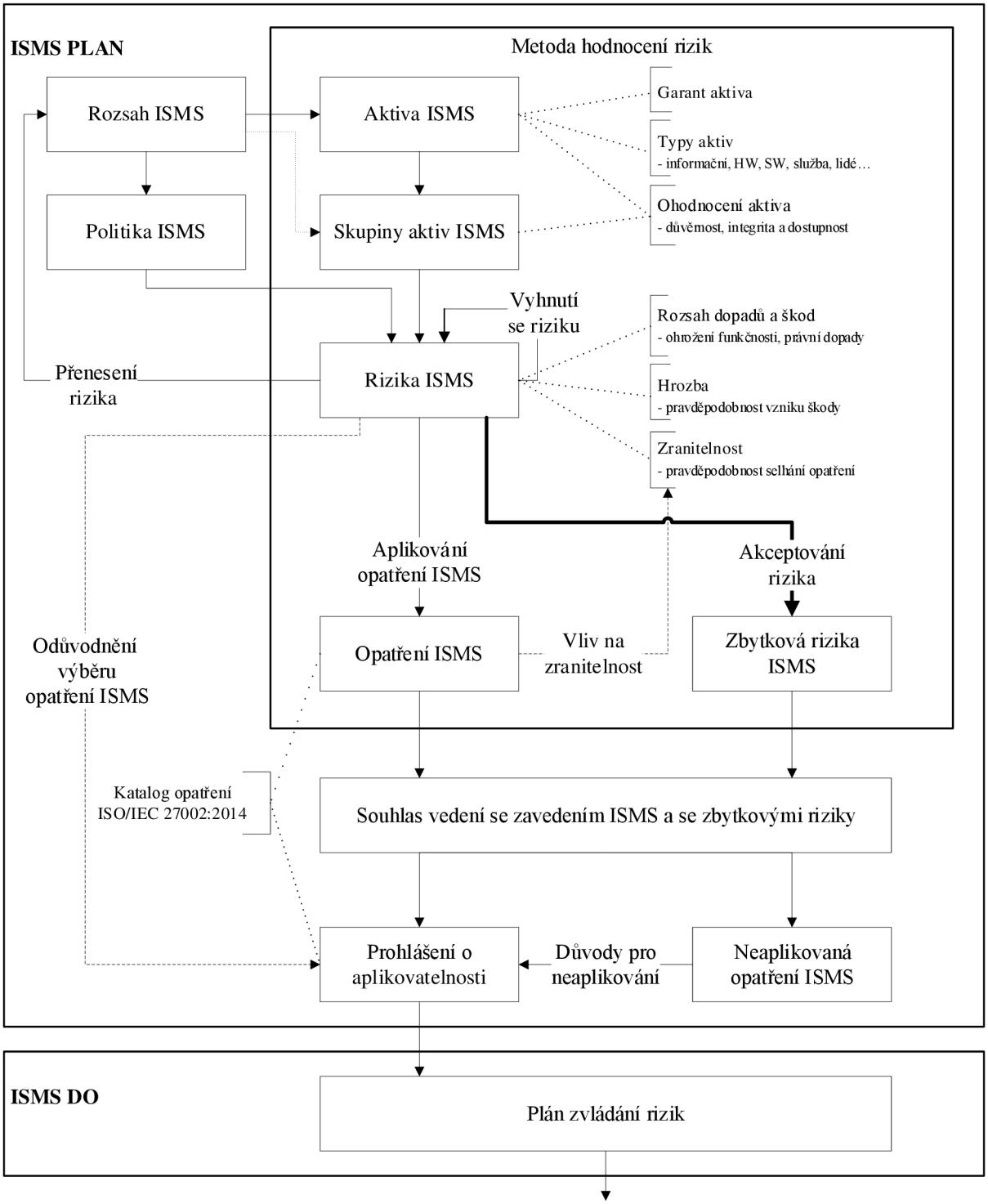
Obr. 8 PDCA model aplikovaný na procesy ISMS dle Kolouch [4]

2.3.1 Ustanovení ISMS

Budován ISMS začíná etapou ustanovení, ve které se definuje rozsah ISMS. Dále obsahuje odsouhlasení Prohlášení o politice ISMS a analýzu rizik s výběrem vhodných bezpečnostních opatření. Tato etapa by měla být ukončena souhlasem vedení se zavedením ISMS podle potřeb organizace, protože má zásadní vliv na fungování ISMS během jeho celého životního cyklu. Činnosti ve fázi ustavení ISMS [7]:

- definování rozsahu, hranic a vazeb ISMS
- definování a odsouhlasení Prohlášení o politice ISMS
- analýza a zvládání rizik
    - definování přístupu organizace k hodnocení rizik
    - identifikování rizika včetně určení aktiv a jejich vlastníků
    - analýza a vyhodnocení rizik
    - identifikace a ohodnocení variant pro zvládání rizik
    - výběr cílů opatření a jednotlivých opatření pro zvládání rizik
    - souhlas vedení organizace s navrhovanými zbytkovými riziky a se zavedením ISMS
- příprava Prohlášení o aplikovatelnosti

Na obrázku 9 je zobrazen postup činností a základní souvislosti v rámci etapy ustanovení ISMS.



Obr. 9 Budování ISMS dle Smejkal [13]

Rozsah ISMS

Rozsah a hranice ISMS jsou určeny po zvážení kontextu organizace, potřeb a očekávání zainteresovaných stran. ISMS lze aplikovat na celou organizaci nebo její jasně definovanou část. Výhodou soustředění činnosti na dílčí část je možnost věnování většího úsilí do zvolené oblasti. [7]

Politika ISMS

Politika ISMS (též Politika kybernetické bezpečnosti a bezpečnosti informací) je dokument vytvořený na základě specifických potřeb organizace. Úkolem tohoto dokumentu je upřesnit cíle a základní směr ISMS při zohlednění požadavků organizace. Politika ISMS by měla vytvořit vazby pro budování a údržbu ISMS v organizaci, stanovit kritéria popisu a hodnocení rizik. [7]

Analýza a zvládání rizik

Řízení rizik je klíčovým nástrojem ISMS. Znalost skutečných rizik rozhoduje o výběru bezpečnostního opatření ke snížení negativních dopadů těchto rizik. Podrobněji je problematika analýzy rizik rozebrána na základě normy ČSN ISO/IEC 27005:2019 v kapitole 2.4. [7]

Souhlas vedení se zavedením ISMS a se zbytkovými riziky

Vedení by mělo odsouhlasit návrh opatření ke snížení bezpečnostních rizik a vyjádřit se k přijatelnosti existujících zbytkových rizik. [7]

Prohlášení o aplikovatelnosti

Dokument, který popisuje cíle opatření a jednotlivá bezpečnostní opatření relevantní a aplikovatelná na ISMS organizace. Jedná se o povinný dokument pro organizace usilující o shodu vlastního ISMS s normou ČSN ISO/IEC 27001:2014. [7]

2.3.2 Zavádění a provoz ISMS

Etapa zavádění a provoz ISMS se soustředí na zavedení všech bezpečnostních opatření připravených během plánování ISMS. Důležité je prosadit připravené plány v souladu se zadáním, stanovenými termíny a očekávanými výsledky. V Příručce bezpečnosti informací by měla být dokumentová všechna bezpečnostní opatření a mělo by dojít k vysvětlení bezpečnostních principů všem uživatelům a manažerům.
Činnosti ve fázi zavádění a provoz ISMS [7]:

- formulování dokumentu Plán zvládání rizik a započít s jeho zaváděním
- zavedení plánovaných bezpečnostních opatření a zformulování Příručky bezpečnosti informací, která upřesní pravidla a postupy aplikovaných opatření v definovaných oblastech bezpečnosti informací (viz. ČSN ISO/IEC 27002:2014)
- definování programu budování bezpečnostního povědomí a provedení přípravy a zaškolení všech uživatelů, manažerů a odborných pracovníků z úseku informatiky
- upřesnění způsobů měření účinnosti bezpečnostních opatření a sledování stanovených ukazatelů
- zavedení postupů a dalších opatření pro rychlou detekci a reakci na bezpečnostní incidenty
- řízení zdrojů, dokumentů a záznamů ISMS

Plán zvládání rizik

Dokument, který popisuje všechny činnosti spojené s provozováním a rozvojem ISMS. Součástí je určení osobní odpovědnosti za provádění jednotlivých činností. Plán je sestaven na základě podkladů získaných při ustavení ISMS a při pravidelném přehodnocování ISMS vedením společnosti. [7]

Příručka bezpečnosti informací

Příručka bezpečnosti informací je souhrnem platných bezpečnostních principů, pravidel, zásad a odpovědností. Při tvorbě bezpečnostní dokumentace je třeba rozlišit úroveň dokumentů s ohledem na cílovou skupinu manažerů, uživatelů, operátorů, správců apod. Pro každou cílovou skupinu je vhodné vytvořit vlastní dokument s potřebnou mírou podrobností, tak aby byl snadno pochopitelný a srozumitelný. [7]

Prohlubování bezpečnostního povědomí

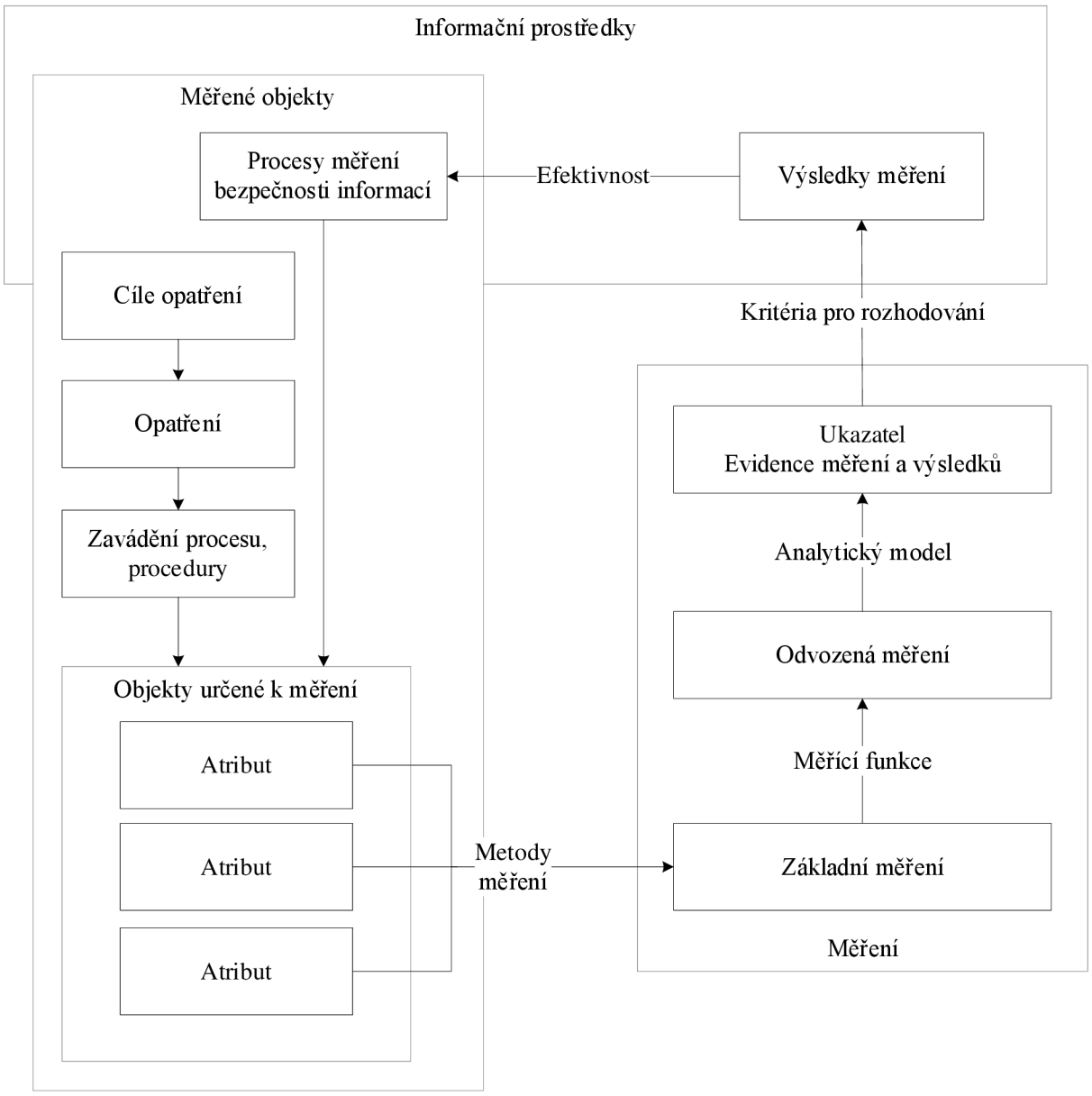
Lidský faktor je nejslabším článkem bezpečnosti informací. Prohlubování bezpečnostního povědomí při prosazování ISMS napomáhá promítnutí všech definovaných pravidel a postupů do chování všech odpovědných pracovníků a uživatelů. Při srozumitelném vysvětlování bezpečnostních principů a pravidel jsou pracovníci schopni reagovat i na situace, které dokumentace nepostihuje. Vlivem rozvoje ISMS a obměny pracovníků jde o nekončící proces, který vyžaduje dlouhodobé a systematické úsilí. [7]

Měření účinnosti ISMS

Pro zjištění efektivnosti systému řízení je třeba měřit účinnost aplikovaných bezpečnostních opatření pomocí pravidelného sledování definovaných údajů o jeho skutečném fungování. Koncept měření účinnosti ISMS v organizaci je potřebné mít už v okamžiku návrhu celého ISMS, protože součástí fáze ustavení ISMS jsou kroky podstatné pro měření efektivnosti a její vyhodnocování. Musí být nastaveny vhodné metody měření, které pomocí ukazatelů podporují rozhodovací proces v ISMS. Použití konkrétního systému ukazatelů a nastavení výchozích hodnot závisí na organizaci a na možnostech zajištění sběru dat. Ukazatele měření bezpečnosti informací lze rozdělit do skupin podle předmětu měření:

- finanční
- personální
- technické – ukazatele provozu IS/ICT

Řízení účinnosti bezpečnosti informací je zásadní podpůrný proces a nedílnou součástí životního cyklu. Celková skladba a doporučení pro nasazení jednotlivých ukazatelů záleží na ISMS v dané organizaci. Postup, jakým je měřena bezpečnost informací v organizaci je na obrázku 10. [7]



Obr. 10 Model měření bezpečnosti informací v organizace dle Doucek [7]

Řízení zdrojů, dokumentů a záznamů ISMS

Z činností řízených v rámci ISMS jsou shromažďovány podklady pro účely monitorování. Pro kontrolu funkčnosti ISMS je podstatné vytvořit definovaná pravidla pro tvorbu, schvalování, distribuci a aktualizaci dokumentace řízení bezpečnosti. Řízení dokumentovaných informací řeší celý životní cyklus, včetně vytváření záznamů o manipulaci s dokumenty (identifikace osoby, čas a místo realizace činnosti) a nakládání s neplatnými dokumenty. [7]

2.3.3 Monitorování a přezkoumání ISMS

Etapa monitorování a přezkoumání ISMS má za úkol zajištění účinné zpětné vazby. Pro splnění tohoto požadavku by proto mělo dojít k prověření všech aplikovaných bezpečnostních opatření a jejich vlivu na ISMS. Základem je přímá kontrola odpovědných osob ze strany jejich nadřízených případně bezpečnostním manažerem. Nezávislý pohled na fungování organizace je zajištěn pomocí interních auditů. Celkově je úkolem připravit dostatek podkladů o skutečném fungování ISMS pro přezkoumání ze strany vedení organizace.
Činnosti ve fázi monitorování a přezkoumání ISMS [7]:

- monitorování a ověření účinnosti prosazení bezpečnostních opatření
- provedení interních auditů ISMS s pokrytím celého ISMS
- připravení zprávy o stavu ISMS a na základě výsledků vedení organizace vyhodnotí ISMS (součástí je revize zbytkových a akceptovaných rizik)

Provádění kontrol

Pravidelné kontroly ze strany všech osob, které mají za fungování ISMS odpovědnost, jsou pro ISMS nezbytnou základní zpětnou vazbou. Součástí kontrol musí být schopnost včasné detekce chyb a pokusů o narušení bezpečnosti, schopnost sledování bezpečnostních událostí a včasná detekce bezpečnostních incidentů. Součástí kontrolních činností je i vyhodnocení měření účinnosti ISMS a aplikovaných opatření. Tyto podněty jsou promítnuty do aktualizace příslušných dokumentů a plánů ISMS. [7]

Interní audity ISMS

Provádění interních auditů zajišťuje potřebný nezávislý pohled na fungování ISMS. Zaměření auditů by mělo být rovnoměrně rozloženo na celý rozsah ISMS s ohledem na jeho cíle, priority a rizikové oblasti. Auditem je třeba prověřit jak dodržování procesních pravidel, tak fungování jednotlivých bezpečnostních opatření zavedených pro potřeby ISMS. [7]

Přezkoumání ISMS vedením organizace

Na základě podnětů a připomínek z monitorování ISMS by mělo pravidelně docházet k přezkoumání ISMS vedením organizace. K přezkoumání by mělo docházet alespoň jednou ročně, u nově zavedených ISMS častěji. [7]

2.3.4 Údržba a zlepšování ISMS

Poslední etapa zavádění ISMS se zabývá údržbou a zlepšováním. V této fázi dochází ke shromáždění podnětů pro zlepšení ISMS a pro nápravu všech neshod, které se objevují.
Činnosti ve fázi údržby a zlepšování ISMS [7]:

- provádění opatření pro nápravu a odstranění nedostatků
- zavádění zlepšení ISMS (především na základě přehodnocení vedením)

Neshody a nápravná opatření

Při zjištění jakéhokoliv nesouladu s požadavky ISMS, musí být provedeno nápravné opatření. Nápravné opatření vhodně reaguje na projevenou neshodu. Proaktivní řešení naopak spočívá v zavedení preventivního opatření v situaci, kdy se neshoda ještě neprojevila. Při odstraňování nedostatků je nutné analyzovat souvislosti a opatření realizovat tak, aby se omezily možnosti jejich opakování. Všechny postupy musí být dokumentovány. Po zavedení opatření je důležité přezkoumat, zda opatření skutečně zajistila očekávanou změnu efektivity ISMS. [7]

Neustálé zlepšování

Navrhnout dokonalý systém řízení je nereálné, proto je nezbytné do systému začlenit účinnou zpětnou vazbu. Ta musí odhalovat nedostatky a jejich příčiny a vhodně na ně reagovat. Podněty na případné nedostatky by měly pocházet od osob na všech úrovních, ale měly by být pečlivě zváženy dopady a rizika pro organizaci. Pro rozvoj ISMS je důležitá motivace pracovníků na účasti při všech činnostech spojených s ISMS. [7]

2.4 Analýza a řízení rizik dle ISO/IEC 27005

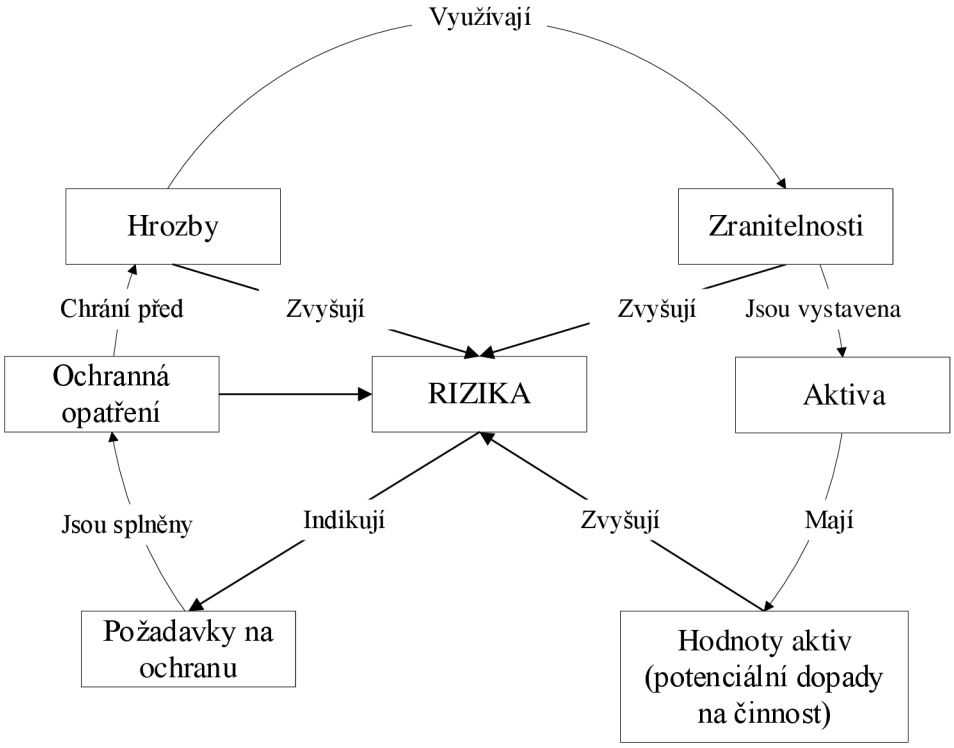
Systematický přístup k řízení rizik je nezbytný pro identifikaci potřeb organizace a pro zavedení a provozování účinného ISMS. Model na obrázku 11 znázorňuje vztahy při analýze a řízení rizik. Prvky řízení rizik uplatněné v jednotlivých fázích ISMS [18]:

Ustavení ISMS
- Stanovení kontextu
- Posouzení rizik
- Příprava plánu ošetření rizik
- Akceptace rizik

Zavádění a provoz ISMS
- Implementace plánu ošetření rizik

Monitorování a přezkoumání ISMS
- Kontinuální monitorování a přezkoumání rizik

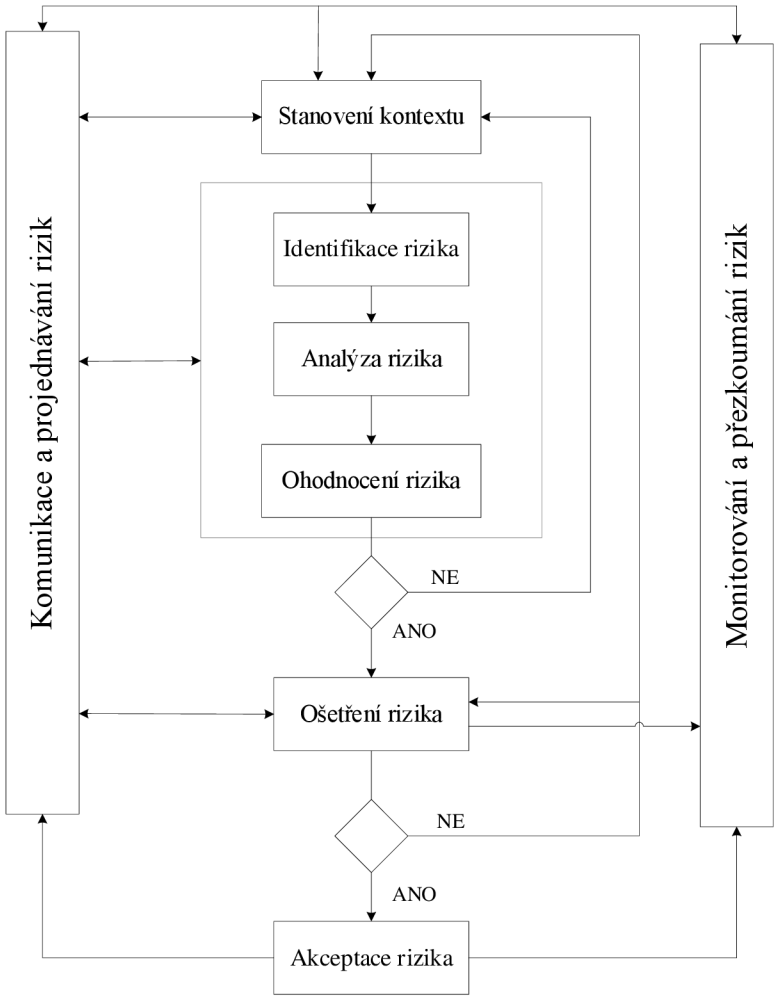
Údržba a zlepšování ISMS
- Udržování a zlepšování procesu řízení rizik bezpečnosti informací



Obr. 11 Vztahy při řízení rizik dle Smejkal [13]

Aplikace procesu řízení rizik naplňuje požadavek normy ČSN ISO/IEC 27001:2014, aby byla opatření implementovaná na základě rizik. Jak uvádí obrázek 12, proces řízení rizik bezpečnosti informací je proces iterativní. Kontext pro realizaci posouzení rizik je stanoven jako první. Následuje hodnocení rizik, při kterém je potřeba shromáždit dostatek informací, aby bylo možné přistoupit k ošetření rizik. V případě, že nejsou získané informace dostatečné, je provedena další iterace posouzení rizik s revidovaným kontextem nebo na omezených částech celkového rozsahu. Činnost akceptace rizik musí zajistit explicitní přijetí vedením organizace, zejména v případě, kdy byla implementace opatření vynechána nebo odložena. [18]

Tento lze aplikovat na celou organizaci, její část, na informační systém nebo plánované aspekty opatření. V průběhu je důležité zapojit a informovat zainteresované strany o identifikovaných rizicích a přijatých opatřeních a vést dokumentaci. [18]



Obr. 12 Ilustrace procesu řízení rizik bezpečnosti informací dle ISO/IEC 27005:2019 [18]

2.4.1 Stanovení kontextu

Ze všech dostupných relevantních informací organizace stanoví interní a externí rámec pro řízení rizik bezpečnosti informací, který zahrnuje nastavení nezbytných základních kritérií, definuje rozsah a mezní hodnoty a stanoví vhodnou organizační strukturu pro řízení rizik bezpečnosti informací. Účelem může být podpora řízení ISMS, právní shoda a důkaz povinné péče, příprava plánu kontinuity činností, příprava řešení incidentů a popis požadavků na bezpečnost informací u produktu, služby nebo bezpečnostního mechanismu. [18]

2.4.2 Hodnocení rizik

Smyslem posouzení rizik je rizika identifikovat, kvantitativně nebo kvalitativně popsat a stanovit priority ve vztahu ke kritériím hodnocení a cílům organizace. Posouzení rizik stanovuje hodnotu informačních aktiv, identifikuje možné hrozby a zranitelnosti, identifikuje stávající opatření a jejich dopad, určí priority odvozených rizik a roztřídí je podle kritérií hodnocení rizik uvedených při stanovení kontextu. Kroky posouzení rizik [18]:

- Identifikace rizik
- Analýza rizik
- Hodnocení rizik

Identifikace rizik

Identifikace a ocenění aktiv

Nejen hardware a software, ale vše, co má pro organizaci hodnotu je aktivem a vyžaduje ochranu. Bezpečnostní incident může ovlivnit i více aktiv nebo naopak jen část aktiva a jeho dopad záleží na úspěšnosti incidentu. Úroveň podrobnosti pro identifikaci aktiv ovlivňuje množství informací pro posouzení rizik. Je potřeba zvolit vhodnou úroveň a případně ji v další iteraci posouzení rizik zpřesnit. Při identifikaci a oceňování aktiv je možné redukovat jejich množství pomocí seskupení. Smyslem je vytvoření skupiny podobných vlastností (např. cena, kvalita, účel apod.), která je dále považována za jediné aktivum. Seznam identifikovaných aktiv obsahuje i vlastníka aktiva, což je přímo pověřená osoba odpovědná za příslušné aktivum, která zná i jeho hodnotu. [13]

K vyjádření významu aktiv pro činnost organizace je identifikovaným aktivům přiřazena hodnota na základě stanovených kritérií. Hodnota může být určena finančním ohodnocením nebo podle negativních dopadů plynoucích ze ztráty důvěrnosti, dostupnosti, integrity, individuální odpovědnosti, autenticity a spolehlivosti. Rozsah a způsob ohodnocení aktiv je na organizaci, ale Ondrák [10] doporučuje pro lepší orientaci v rozsáhlých záznamech barevné odlišení jednotlivých stupňů.

Identifikace hrozeb

Hrozba má potencionál poškodit aktiva (např. informace, procesy a systémy) a tím i celou organizaci. Hrozby mohou být náhodné nebo záměrné s přírodním nebo lidským původem a vznikem uvnitř nebo vně organizace. Všechny druhy hrozeb a jejich zdroje by měly být identifikovány. Identifikace probíhá ve dvou krocích, nejprve jsou hrozby identifikovány obecně a podle typu (např. neoprávněné akce, fyzické poškození, technické selhání atd.) a následně ve vhodných případech jednotlivé hrozby v rámci identifikované v rámci obecných tříd. Posouzení hrozeb se provádí z pohledu ztráty dostupnosti, důvěrnosti, integrity, individuální odpovědnosti, autentičnosti a spolehlivosti aktiv. Identifikace zranitelností odhalí slabá místa, která mohou být využita zdrojem hrozby a způsobit škodu na aktivech. [10]

Identifikace existujících opatření

Identifikace stávajících opatření slouží k předcházení zbytečné práci nebo nákladům (např. zdvojení opatření) a k provedení kontroly funkčnosti opatření. Pokud opatření nefunguje podle očekávání, může zapříčinit zranitelnost aktiva, proto je vhodné učinit rozhodnutí o ponechání, odstranění nebo nahrazení takového opatření. Pro identifikaci stávajících opatření slouží přezkoumání dokumentů s informacemi o opatřeních, provedení kontrol s odpovědnými osobami, fyzické přezkoumání a porovnání s dokumentací a přezkoumání výsledků auditu. [18]

Analýza rizik

Analýza rizik se provádí v různých stupních podrobnosti v závislosti na kritičnosti aktiv, rozsahu známých zranitelností a předchozích incidentů v organizaci. Odhadnuté riziko je kombinací pravděpodobnosti, že dojde k incidentu a jeho následků. Analýza rizik může být kvalitativní nebo kvantitativní, případně kombinaci obou metodik. V praxi se často metodiky kombinují. Pro určení obecné úrovně rizik a k odhalení významných rizik je použita kvalitativní analýza, která podle potřeby upřesnit rizika může být následně doplněna o specifičtější nebo kvantitativní analýzu. Důvodem jsou obvykle nižší náklady na provedení kvalitativní analýzy. [18]

Kvalitativní analýza rizik používá určitý rozsah (např. malé, střední a velké) k popisu závažnosti následků a pravděpodobnosti výskytu. Konkrétní úroveň je určena kvalifikovaným odhadem, proto je tato metoda subjektivní, ale rychlá, snadno pochopitelná a přizpůsobitelná daným okolnostem. Kvalitativní analýzu je vhodné použít jako počáteční prověřovací činnost k identifikaci rizik nebo při nedostatečné kvantitě a kvalitě údajů pro kvantitativní analýzu. [18]

Kvantitativní analýza rizik používá rozsah s číselnými hodnotami pro ocenění následků pravděpodobnosti vzniku události. Kvalita analýzy závisí na přesnosti a úplnosti údajů a platnosti použitých modelů. Metoda využívá historických dat o incidentech a tím je propojena s cíli bezpečnosti informací a zájmy organizace. Kvantitativní analýza je náročnější než kvalitativní a pokud není k dispozici dostatek dat o nových rizicích a slabých místech může dojít k mylnému zdání užitečnosti a přesnosti posouzení rizik. [18]

Hodnocení rizik

Výstupem analýzy rizik je seznam rizik s přidělenými úrovněmi hodnoty a kritéria hodnocení rizika. Tento výstup by měl být konzistentní s kritérii hodnocení rizik definovaných při stanovení kontextu. Podle výstupů z hodnocení rizik je třeba přijmout rozhodnutí, které činnosti mají být provedeny a priority pro ošetření rizik zohledňující odhadnutou úroveň. [18]

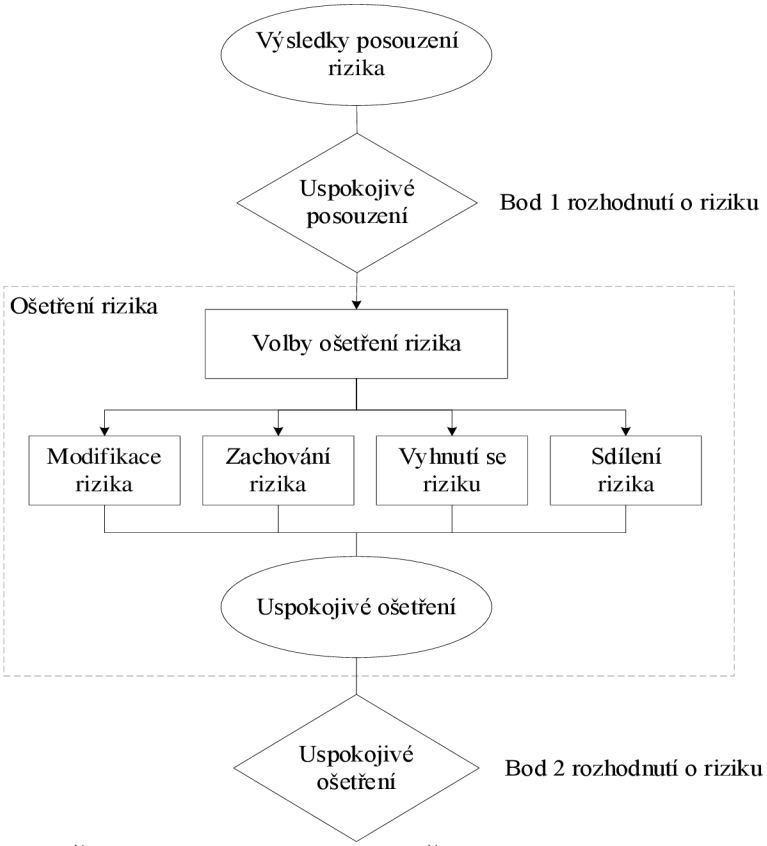
2.4.3 Ošetření rizik

Na základě seznamu rizik preferovaných podle hodnocení rizik jsou podle kritérií pro akceptaci rizik a legislativních požadavků zvolena opatření k minimalizaci případných rizik. Na obrázku 13 jsou znázorněny činnosti ošetřování rizika v rámci procesu řízení rizik bezpečnosti informací. [18]

Volby ošetření rizika [18]:

- Modifikace rizika – úroveň rizika by měla být regulována zavedením, odstraněním nebo změnou opatření, aby bylo zbytkové riziko přehodnoceno jako akceptovatelné.
- Zachování rizika – pokud úroveň rizika splňuje kritéria akceptace rizika, není zapotřebí přijímat další opatření a riziko lze zachovat.
- Vyhnutí se riziku – organizace může přijmout rozhodnutí o celkovém vyhnutí se riziku vyjmutím z plánované nebo existující činnosti nebo změnou podmínek provozu činnosti, pokud jsou identifikovaná rizika považována za příliš vysoká nebo náklady na ošetření rizik převyšují přínosy.
- Sdílení rizika – sdílení rizik zahrnuje rozhodnutí sdílet určitá rizika s externími stranami, přičemž mohou vznikat nová rizika nebo se měnit existující rizika, a proto může být nutné další ošetření rizik. Odpovědnost zvládat riziko je možné sdílet, ale není možné sdílet nevýhodu dopadu.

Konkrétní ošetření rizika je voleno podle výsledku z posouzení rizika, očekávaných nákladů na zavedení a očekávaných výhod. Prioritu má volba, která za relativně nízké náklady zajistí velké snížení rizika. Vzájemně se jednotlivé volby nevylučují, a naopak jejich kombinace může přinést výhody. Některá ošetření rizika mohou řešit víc než jedno riziko. Cílem ošetření rizik je snížení nepříznivých následků rizik na nejnižší míru dosažitelnou za přiměřených podmínek. [18]



Obr. 13 Činnosti ošetření rizika dle ČSN ISO/IEC 27005:2019 [18]

2.4.4 Akceptace rizik

Plány na ošetření rizik popisují, jak mají být posouzená rizika ošetřena, aby byla splněna kritéria akceptace. Odpovědné osoby přezkoumávají a schvalují navržené plány ošetření rizik a výsledná zbytková rizika a zaznamenávají podmínky schválení. V některých případech úroveň zbytkového rizika nevyhovuje kritériím akceptace rizik, protože uplatňovaná kritéria neberou v úvahu převládající okolnosti (např. nákladnost na ošetření rizik). To naznačuje nepřiměřenost kritérií akceptace rizik a potřebu jejich revidování. Pokud nakonec dojde k akceptaci takového rizika je potřeba aby se odpovědná osoba vyjádřila k rizikům a ospravedlnila rozhodnutí potlačit obvyklá akceptační kritéria. [18]

2.4.5 Komunikace a projednávání rizik

Účinná komunikace a výměna informací o rizicích mezi zúčastněnými stranami může mít zásadní vliv na rozhodnutí, které mají být přijata. Obousměrná komunikace usnadňuje porozumění podkladům, zlepšuje vnímání rizika a přínosů zúčastněnými stranami. Organizace by měla vytvořit plány komunikace pro běžný provoz i pro nepředvídatelné události. [18]

2.4.6 Monitorování a přezkoumání rizik

Rizika se neustále mění. Hodnotu aktiv, dopady, hrozby, zranitelnosti a pravděpodobnosti výskytu je třeba monitorovat a tím včas identifikovat jakékoliv změny v rámci organizace a udržovat přehled o úplném stavu rizik. Proces řízení rizik by měl být monitorován, přezkoumáván a zlepšován podle potřeby, aby celkový rámec zůstal relevantní a přiměřený okolnostem. [18]

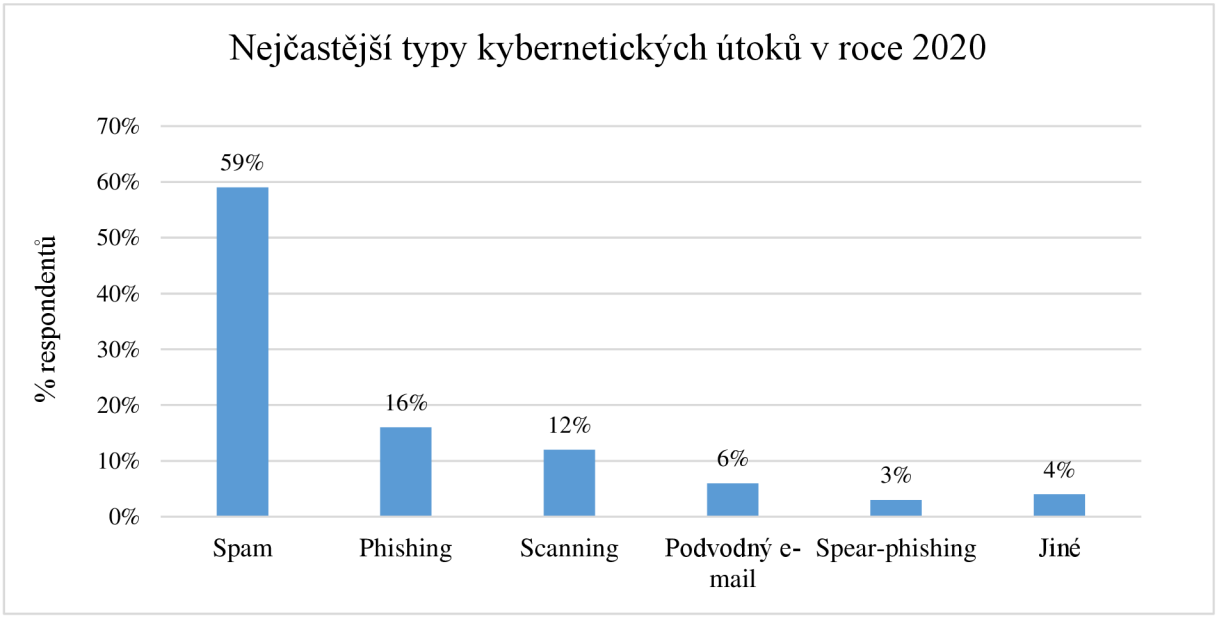
3 ANALÝZA SOUČASNÉHO STAVU

V této kapitole je uveden aktuální celkový stav bezpečnosti informací v ČR a na základě metodiky stanovené normou ČSN ISO/IEC 27005:2019 je popsána analýza rizik ISMS v brněnské pobočce společnosti FERMAT CZ S.R.O.

3.1 Současný stav bezpečnosti informací v ČR

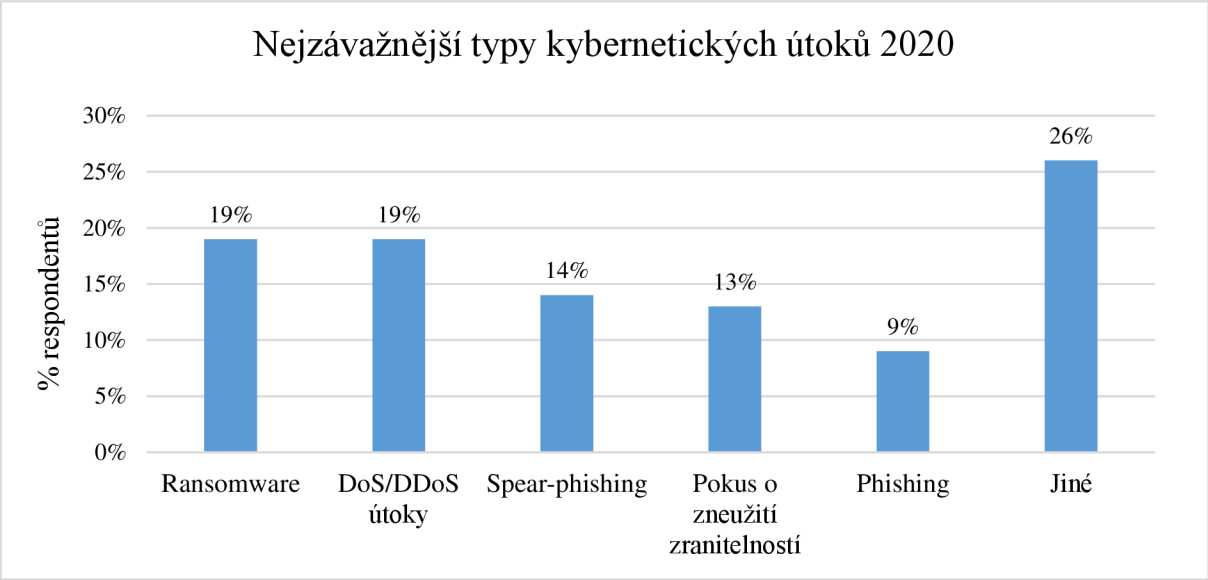
Přehled o celkovém aktuálním stavu kybernetické bezpečnosti v ČR nejlépe ilustruje Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020 vydaná NÚKIB. Zpráva NÚKIB čerpala z dotazníku rozeslaného subjektům regulovaným ZoKB i některým klíčovým institucím a organizacím, které nejsou regulovány ZoKB. Dotazník vyplnilo celkem 222 subjektů, z toho 63 institucí z veřejného sektoru, 24 finančních institucí, 77 zdravotnických zařízení, 14 organizací poskytujících digitální služby, 12 subjektů z energetického sektoru, 12 subjektů z průmyslu a 20 vzdělávacích institucí. [19]

Jako nejčastější typ útoků respondenti v dotaznících uváděli spam, phishing a skenování vnějších sítí organizací a naopak pokusy např. o skenování vnitřní sítě nebo o nelegální těžbu kryptoměn se vyskytly jen zřídka, viz. obrázek 14. [19]



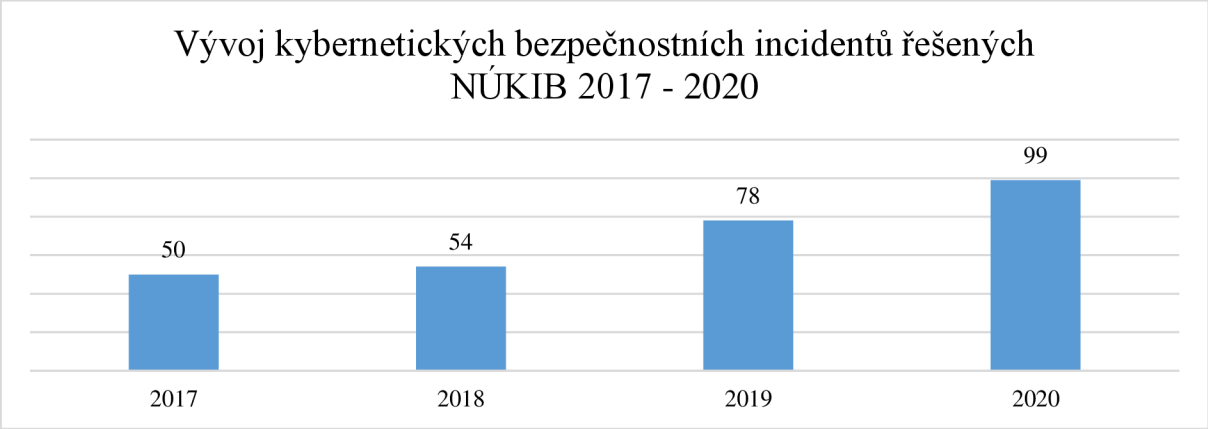
Obr. 14 Nejčastější typy kybernetických útoků v roce 2020 dle NÚKIB [19]

Nejzávažnějšími útoky byly z pohledu respondentů ransomware, DoS/DDoS útoky, spear-phishingové e-maily a pokusy o zneužití zranitelností (Obr. 15). Nadpoloviční část respondentů zaznamenala pokus o kybernetický útok, ale u téměř tří čtvrtin však tato událost nevedla ke kybernetickému bezpečnostnímu incidentu. [19]



Obr. 15 Nejzávažnější typy kybernetických útoků 2020 dle NÚKIB [19]

Celkově obdržel v roce 2020 NÚKIB 468 hlášení o kybernetických bezpečnostních incidentech, z tohoto počtu řešil pouze 99 incidentů. Zbývající ohlášené incidenty řešila jiná instituce nebo nebyl zásah ze strany NÚKIB potřebný, ovšem řada subjektů tyto incidenty vůbec nenahlašuje. Obrázek 16 ukazuje vzrůstající trend v počtu incidentů řešených NÚKIB od roku 2017. Počty nahlášených kybernetických incidentů jsou, ale jen zlomkem z celkového počtu kybernetických událostí, ke kterým denně dochází. [19]



Obr. 16 Vývoj kybernetických bezpečnostních incidentů řešených NÚKIB 2017–2020 [19]

Přehled o počtu kybernetických incidentů řešených NÚKIB v roce 2020 [19]:

- 37 škodlivý kód (např. virus, červ, trojský kůň, spywer)
- 26 narušení dostupnosti (např. vlivem DoS/DDoS útoku nebo sabotáží)
- 16 průnik (např. úspěšná kompromitace aplikace nebo uživatelského účtu)
- 7 podvod/phishing (např. e-mail se škodlivou přílohou nebo odkazem)
- 7 pokus o průnik (např. pokus o zneužití zranitelnosti, kompromitace aktiva)
- 3 sběr informací (např. skenování, sociální inženýrství)
- 1 urážlivý obsah (např. spam, kyberšikana, nevhodný obsah)
- 2 incident způsobený administrativní nebo technickou chybou

Zpráva uvádí následující velmi významné incidenty z roku 2020 [19]:

„Nejvýznamnějším a nejzávažnějším incidentem řešeným NÚKIB bylo zašifrování systémů Fakultní nemocnice Brno ransomwarem, k němuž došlo v březnu 2020. Incident vyústil ve významné omezení provozu nemocnice na třech lokalitách a způsobil škody v řádu stovek milionů korun.“

„Ve stejném měsíci se obětí ransomwaru stala Psychiatrická nemocnice Kosmonosy. V tomto případě došlo k ochromení zejména její administrativní infrastruktury, ale nebyla ohrožena schopnost poskytování péče pacientům, ani nedošlo k zasažení systémů, na kterých závisejí lidské životy.“

„Třetím velmi významným incidentem se v roce 2020 stala kompromitace několika desítek e-mailových účtů strategické státní instituce, ke které došlo v důsledku úspěšné spear-phishingové kampaně. Kromě narušení důvěrnosti obsahu schránek kompromitace vyústila v nedostupnost e-mailových služeb na jeden až dva dny.“

3.2 Popis společnosti

Společnost FERMAT byla založena v roce 1990 a stal se předním výrobcem nejsilnějších a přesných horizontálních vyvrtávacích, frézovacích strojů a válcových brusek, nabízející obráběcí stroje na všech hlavních trzích po celém světě. Dnes má FERMAT více než 470 zaměstnanců na třech kontinentech a ročně produkuje více než 100 strojů. Hlavní výrobní a montážní zařízení FERMAT je v Brně a v Lipníku nad Bečvou. Brněnská pobočka je rozmístěna ve třech budovách a má 100 administrativních pracovníků a 130 pracovníků výroby. [20]

3.3 Analýza rizik

Ve spolupráci se zástupcem organizace jsou identifikována nejdůležitější aktiva a hrozby. Hodnota aktiv, resp. pravděpodobnost hrozby je přidělena na základě tabulky 2, resp. tabulky 4 v kombinaci s dotazováním zaměstnance společnosti. Rizika jsou vyhodnocena prostřednictvím kvalitativní tří faktorové metody dle Ondrák. [10]

3.3.1 Identifikace a ohodnocení aktiv

Hodnocení aktiv v tabulce 3 vychází především z míry závažnosti možných dopadů při porušení důvěrnosti, dostupnosti nebo integrity vybraného aktiva. Čím více by úspěšný útok na dané aktivum ovlivnil společnost, tím vyšší hodnota mu náleží. Aktiva jsou hodnocena na stupnici 1 až 5, viz. tabulka 2.

Tab. 2 Stupnice pro hodnocení aktiv

Nevýznamné	1
Nízký význam	2
Střední význam	3
Vysoký význam	4
Kritické aktivum	5

Význam jednotlivých stupňů:

- Nevýznamné – poškození aktiva nemá vliv na společnost
- Nízký význam – poškození aktiva má zanedbatelný dopad na společnost
- Střední význam – poškození aktiva znamená potíže nebo finanční ztráty společnosti
- Vysoký význam – poškození aktiva znamená vážné potíže nebo značné finanční ztráty společnosti
- Kritické aktivum – poškození aktiva znamená existenční potíže společnosti

Tab. 3 Seznam a ohodnocení identifikovaných aktiv

Aktivum	Hodnota (A)
Technické vybavení	
Servery	4
NAS	4
PC a notebooky	3
Mobilní zařízení (mobilní telefony a tablety)	3
Tiskárny	2
Síťová infrastruktura	3
Programové vybavení	
Podnikový ERP systém	5
Systém pro podporu prodeje	4
Konstrukční SW	3
Operační systém	2
Kancelářské balíky	2
Antivirus	2
Data	
Výrobní dokumentace	5
Účetnictví	4
Údaje o zaměstnancích	4
Smluvní dokumentace	3
Zálohy dat	4
Služby	
Připojení k internetu	3
Webové stránky	1
Vzdálený přístup	2
Elektronická pošta	3
Nemovitý majetek	
Budovy	4

3.3.2 Identifikace a ohodnocení hrozeb

Hrozby mohou poškodit aktiva společnosti a ovlivnit činnost podniku. Hrozby v tabulce 5 jsou vybrány ze seznamu uvedených v normě ČSN ISO/IEC 27005:2019. K ohodnocení pravděpodobnosti výskytu hrozby se využije stupnice 1 až 5, viz. tabulka 4. Hrozby mají různý původ. Norma ČSN ISO/IEC 27005:2019 definuje následující zdroje hrozeb:

- A – náhodný (accindental) – lidské činnosti, které mohou náhodně poškodit informační aktiva
- D – úmyslný (deliberate) – úmyslné činnosti zaměřené na informační aktiva
- E – environmentální (enviromental) – incidenty, které nejsou založeny na lidské činnosti

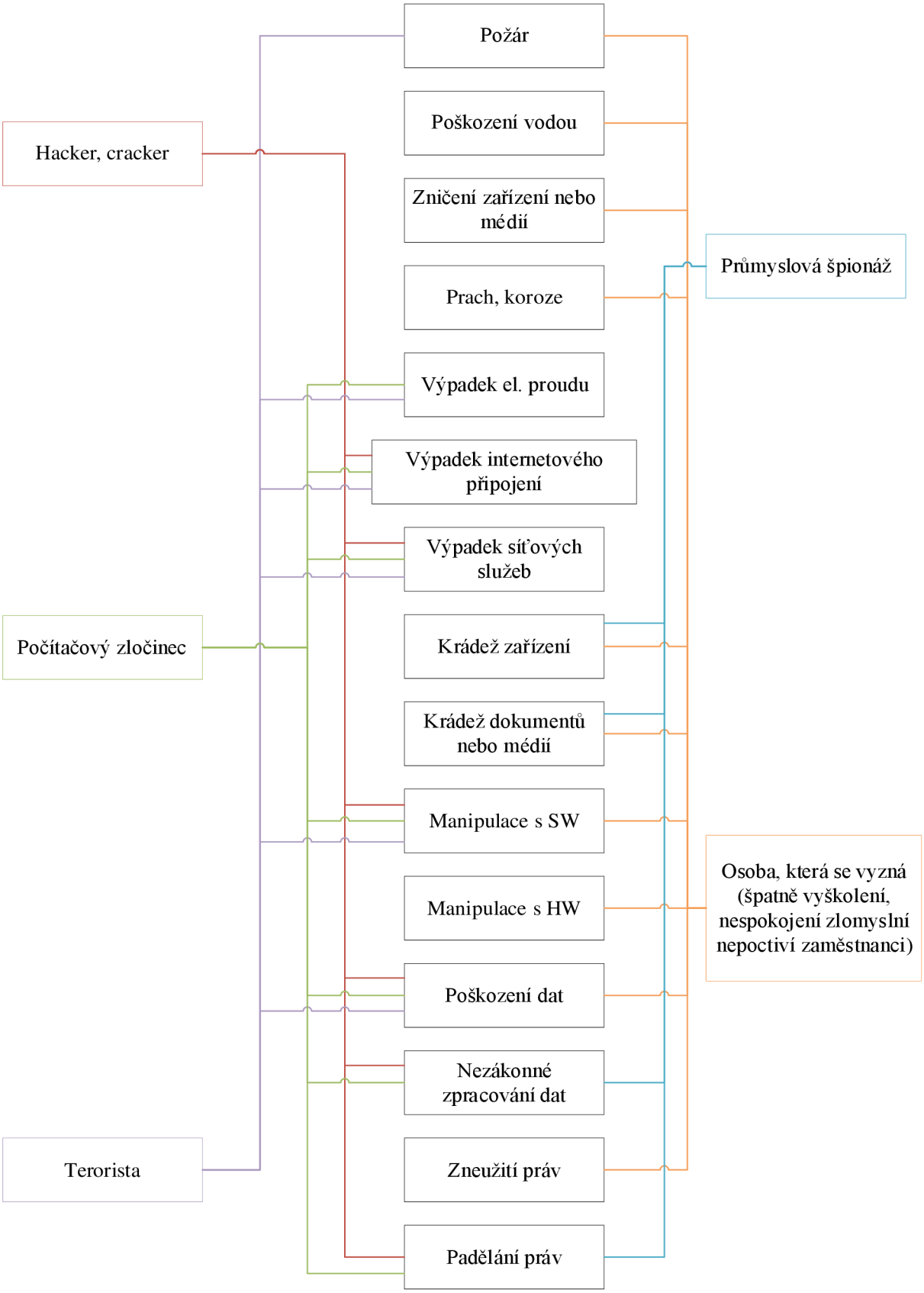
Tab. 4 Stupnice pro hodnocení pravděpodobnosti výskytu hrozby

Velmi nepravděpodobný	1
Málo pravděpodobný	2
Středně pravděpodobný	3
Velmi pravděpodobný	4
Téměř jistý	5

Tab. 5 Seznam a ohodnocení identifikovaných hrozeb

Hrozba	Pravděpodobnost (T)	Zdroj
Fyzické a přírodní události		
Požár	1	A, D, E
Poškození vodou	1	A, D, E
Zničení zařízení nebo médií	2	A, D, E
Prach, koroze	2	A, D, E
Meteorologické jevy	1	E
Ztráta základních služeb		
Výpadek el. proudu	3	A, D, E
Výpadek internetového připojení	3	A, D
Výpadek síťových služeb	4	A, D
Ohrožení informací		
Krádež zařízení	2	D
Krádež dokumentů nebo médií	3	D
Manipulace s SW	2	A, D
Manipulace s HW	2	D
Špionáž nebo škodlivý kód	4	D
Technické selhání		
Selhání SH	2	A
Selhání HW	2	A
Neoprávněné činnosti		
Poškození dat	3	D
Nezákonné zpracování dat	2	D
Ohrožení funkcí		
Zneužití práv	3	A, D
Padělání práv	3	D
Chyba při použití	4	A

Na obrázku 17 jsou možné lidské zdroje pro identifikované hrozby s úmyslným zdrojem.



Obr. 17 Lidské zdroje úmyslných hrozeb

3.3.3 Výpočet míry rizika

Matice zranitelnosti

Hodnoty zranitelnosti v matici zranitelnosti (Tab. 6) vycházejí ze vzájemného vztahu mezi identifikovaným aktivem a hrozbou. Hodnota na stupnici 1 až 5 udává pravděpodobnost, s jakou může hrozba poškodit dané aktivum.

Tab. 6 Výběr z matice zranitelnosti

Zranitelnost (V)	Hrozba	Zničení zařízení/médií	Prach, koroze	Meteorologické jevy	Výpadek el. proudu	Výpadek internetu	Výpadek síťových služeb	Krádež zařízení	Krádež dokumentů	Manipulace s SW	Manipulace s HW	Špionáž nebo škodlivý kód	Selhání SW	Selhání HW	Poškození dat	Nezákonné zpracování dat	Zneužití práv	Padělání práv	Chyba při použití
Aktivum	T / A	2	2	1	3	3	4	2	3	2	2	4	2	2	3	2	3	3	4
Servery	4	3	2	3	2	2	2	4		2	3	4	2	3	4	3	3	4	3
Zálohovací NAS	4	3	2	3	2	2	2	4		2	3	4	2	3	4	3	3	4	3
PC a notebooky	3	3	3	2	2	2	2	3		3	3	4	3	3	3	2	3	3	3
Mobilní zařízení	3	3	2	2				3		2		3	2		2	2	3	3	3
Síťová infrastruktura	3	4	1	3	3		3	1		2			3						
Podnikový ERP	5						3		4	4		5	4		4	4	4	4	3
Systém pro podporu prodeje	4						3		3	4		5	4		3	3	2	2	2
Konstrukční SW	3									2		4	4				2		2
Operační systém	2									2		4	4				3	3	3
Výrobní dokumentace	5	1		1					5			4			3	3	4	4	
Účetnictví	4	1		1					3			4			3	3	3	3	
Údaje o zaměstnancích	4	1		1					5			4			3	3	4	4	
Smlouvy	3	1		1					5			4			3	3	3	3	
Zálohy dat	4	2	2	3	1	2	2		5	3	3	5	2	3	3	3	3	3	4
Připojení k internetu	3				2	3					2	3		2					
Vzdálený přístup	2				3	3	3				3			3	3	2	4	4	3
El. pošta	3											4				2	3	3	2

Matice rizik

Matice rizik udává pro každou kombinaci aktiva a hrozby vypočítanou míru rizika podle vzorce $R = T \times A \times V$, kde R je míra rizika, A hodnota aktiva, T pravděpodobnost vzniku hrozby a V zranitelnost aktiva. Hranice rizika jsou stanoveny dle tabulky 7. [10]

Tab. 7 Ohodnocení míry rizika

Bezvýznamné riziko	0 až 10
Akceptovatelné riziko	10 až 20
Mírné riziko	20 až 30
Nežádoucí riziko	30 až 60
Nepřijatelné riziko	60 a více

Tab. 8 Výběr z matice rizik

Riziko (R)	Hrozba	Zničení zařízení/médií	Prach, koroze	Meteorologické jevy	Výpadek el. proudu	Výpadek internetu	Výpadek síťových služeb	Krádež zařízení	Krádež dokumentů	Manipulace s SW	Manipulace s HW	Špionáž nebo škodlivý kód	Selhání SW	Selhání HW	Poškození dat	Nezákonné zpracování dat	Zneužití práv	Padělání práv	Chyba při použití
Aktivum	A \ T	2	2	1	3	3	4	2	3	2	2	4	2	2	3	2	3	3	4
Servery	4	24	16	12	24	24	32	32	0	16	24	64	16	24	48	24	36	48	48
Zálohovací NAS	4	24	16	12	24	24	32	32	0	16	24	64	16	24	48	24	36	48	48
PC a notebooky	3	18	18	6	18	18	24	18	0	18	18	48	18	18	27	12	27	27	36
Mobilní zařízení	3	18	12	6	0	0	0	18	0	12	0	36	12	0	18	12	27	27	36
Síťová infrastruktura	3	24	6	9	27	0	36	6	0	12	0	0	18	0	0	0	0	0	0
Podnikový ERP	5	0	0	0	0	0	60	0	60	40	0	100	40	0	60	40	60	60	60
Systém pro podporu prodeje	4	0	0	0	0	0	48	0	36	32	0	80	32	0	36	24	24	24	32
Konstrukční SW	3	0	0	0	0	0	0	0	0	12	0	48	24	0	0	0	18	0	24
Operační systém	2	0	0	0	0	0	0	0	0	8	0	32	16	0	0	0	18	18	24
Výrobní dokumentace	5	10	0	5	0	0	0	0	75	0	0	80	0	0	45	30	60	60	0
Účetnictví	4	8	0	4	0	0	0	0	36	0	0	64	0	0	36	24	36	36	0
Údaje o zaměstnancích	4	8	0	4	0	0	0	0	60	0	0	64	0	0	36	24	48	48	0
Smlouvy	3	6	0	3	0	0	0	0	45	0	0	48	0	0	27	18	27	27	0
Zálohy dat	4	16	16	12	12	24	32	0	60	24	24	80	16	24	36	24	36	36	64
Připojení k internetu	3	0	0	0	18	27	0	0	0	0	12	36	0	12	0	0	0	0	0
Vzdálený přístup	2	0	0	0	18	18	24	0	0	0	12	0	0	12	18	8	24	24	24
El. pošta	3	0	0	0	0	0	0	0	0	0	0	48	0	0	0	12	27	27	24

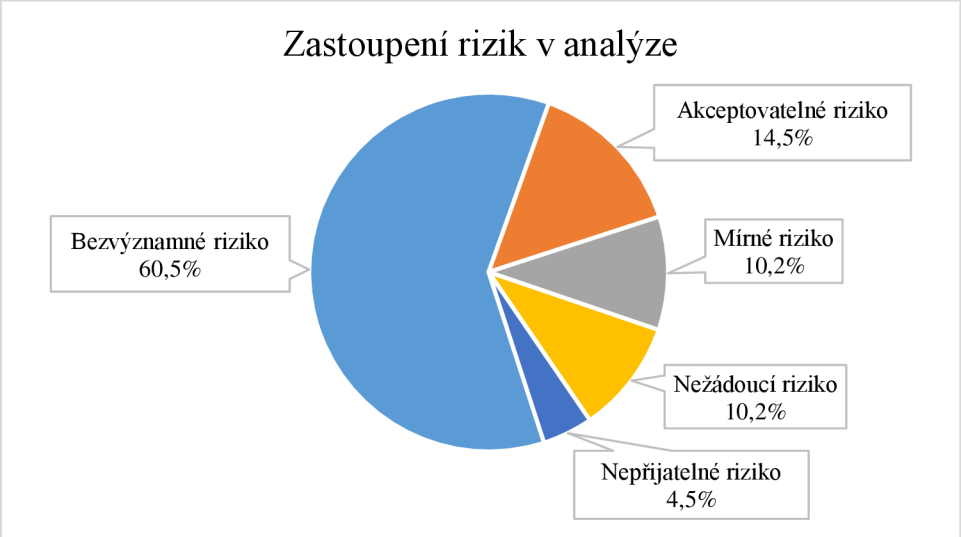
3.3.4 Vyhodnocení současného stavu

Společnost v současné době nemá vypracované komplexní řešení ISMS a základní bezpečnosti informací řeší pomocí externích služeb a smluvních opatření. Do budoucna bude pravděpodobně komplexní řešení problematiky nezbytné, vzhledem k započaté aktualizaci směrnice NIS z roku 2016. V návrhu směrnice NIS 2 je v současné době výrobce strojních zařízení uveden jako „důležitý subjekt“. Rozsah povinností při řešení ISMS pro společnosti typu FERMAT bude zřejmý až po schválení příslušné legislativy.

Analýza rizik ukazuje výskyt:

- 266x bezvýznamné riziko
- 64x akceptovatelné riziko
- 45x mírné riziko
- 45x nežádoucí riziko
- 20x nepřijatelné riziko

Procentuální zastoupení jednotlivých rizik v analýze rizik je na obrázku 18.



Obr. 18 Zastoupení rizik v analýze [zdroj: vlastní]

Nejvíce ohrožená aktiva jsou interní systémy a data. Jejich poškození nebo zneužití, by mělo zásadní dopad na existenci společnosti. Zásadní slabinu představuje škodlivý software a neoprávněný přístup. Část opatření je již zavedena např. v reakci na proběhlé incidenty. V rámci prvotní analýzy je možné akceptovat bezvýznamná a akceptovatelná rizika a zaměřit se především na zabezpečení a ochranu dat.

SWOT analýza

SWOT analýza v kontextu bezpečnosti informací zachycuje silné a slabé stránky současného stavu ISMS a interní i externí příležitosti a hrozby.

Silné stránky

- Pravidelné zálohování
- Vícenásobné zálohování
- Komunikace ve společnosti
- Zajištění bezpečné komunikace s vnější sítí

Slabé stránky

- Přezkoumávání účinnosti jednotlivých opatření
- Chybí pravidelné školení s ohledem na bezpečnost informací
- Není stanovena komplexní politika ISMS
- Absence řízení přístupu, zejména mobilních zařízení do sítě

Příležitosti

- Zavedení a rozvoj ISMS ve společnosti
- Změna právních předpisů (směrnice NIS 2)
- Poučení z předchozích událostí
- Zlepšení fyzického zabezpečení objektu
- Stanovení cílů bezpečnosti informací a jejich ukazatele
- Program Digitální Evropa
- Požadavky na bezpečnost informací začlenit do součástí smluv s dodavateli

Hrozby

- Chyby uživatelů vlivem nedostatečného školení v oblasti bezpečnosti informací
- Ztráta dat
- Zanedbání v oblasti bezpečnosti informací
- Neaktualizovaný SW
- Zanedbání v reakci na bezpečnostní události a incidenty
- Nedostatek lidských zdrojů pro řízení ISMS
- Zneužití přístupu třetích stran k vybavení pro zpracování informací

4 VLASTNÍ NÁVRH ŘEŠENÍ

Náplní této kapitoly je soubor vybraných opatření ke zvládání identifikovaných bezpečnostních hrozeb s ohledem na určenou míru rizika u aktiv společnosti. Norma ČSN ISO/IEC 27000:2020 uvádí pojem bezpečnost informací a nerozlišuje kybernetickou bezpečnost (viz. pojmy v kapitole 2.1 této práce). Navržená opatření jsou vybrána z přílohy A normy ČSN ISO/IEC 27001:2014 a normy ČSN ISO/IEC 27002:2014, proto jsou zaměřena na bezpečnost informací bez ohledu na nosič.

4.1 Výběr opatření

Podle výsledků analýzy současného stavu v kapitole 3 byla vybrána bezpečnostní opatření z přílohy A normy ČSN ISO/IEC 27001:2014 a normy ČSN ISO/IEC 27002:2014. V tabulce 9 jsou k identifikovaným hrozbám přiřazena opatření, která mají být zavedena nebo revidována pro zvýšení bezpečnosti a v tabulce 10 je seznam aplikovaných opatření.

Tab. 9 Vybraná opatření pro řešení identifikovaných hrozeb

Hrozba	Opatření
Požár	A.11.1.4
Poškození vodou	A.11.1.4; A.11.2.1
Zničení zařízení nebo médií	A.8.3.1; A.11.1.1; A.11.1.2; A.11.1.3; A.11.1.4; A.11.2.1; A.11.2.4
Prach, koroze	A.11.2.4
Meteorologické jevy	A.11.1.4; A.11.2.1
Výpadek el. proudu	A.11.2.2
Výpadek internetového připojení	A.11.2.2
Výpadek síťových služeb	A.11.2.2; A.13.1.2
Krádež zařízení	A.6.2.1; A.6.2.2; A.7.1.2; A.9.2; A.11.1.1; A.11.1.2; A.11.1.3; A.11.2.1
Krádež dokumentů nebo médií	A.6.2.1; A.6.2.2; A.7.1.2; A.8.1.3; A.8.3.1; A.9.1.1; A.9.2; A.9.3.1; A.9.4.1; A.9.4.2; A.11.1.1; A.11.1.3; A.11.2.8; A.11.2.9; A.12.2.1; A.12.3.1; A.13.2.1; A.13.2.3
Manipulace s SW	A.7.1.2; A.9.1.1; A.9.1.2; A.9.2; A.11.2.4; A.11.2.8; A.11.2.9; A.12.2.1; A.12.6.2; A.13.2.1; A.14.1.1; A.14.2.1
Manipulace s HW	A.6.2.1; A.7.1.2; A.8.3.1; A.9.2; A.11.1.1; A.11.1.2; A.11.1.3; A.11.2.1; A.11.2.4; A.12.3.1
Špionáž nebo škodlivý kód	A.6.2.1; A.6.2.2; A.7.1.2; A.8.1.3; A.9.1.1; A.9.1.2; A.9.2; A.9.3.1; A.9.4.1; A.9.4.2; A.9.4.3; A.11.1.1; A.11.1.2; A.11.1.3; A.11.2.4; A.11.2.7; A.12.2.1; A.12.3.1; A.12.6.2; A.13.1.2; A.13.1.3; A.13.2.1; A.13.2.3; A.14.1.1
Selhání SH	A.12.2.1; A.14.1.1; A.14.2.1
Selhání HW	A.8.1.3; A.11.1.4; A.11.2.1; A.11.2.2; A.11.2.4; A.11.3.1

Poškození dat	A.6.2.1; A.8.1.3; A.8.3.1; A.9.1.1; A.9.1.2; A.9.2; 9.3.1; A.9.4.1; A.11.2.4; A.11.2.8; A.11.2.9; A.12.2.1; A.12.3.1; A.12.6.2; A.13.1.3; A.13.2.1; A.14.1.1
Nezákonné zpracování dat	A.8.1.3; A.8.3.1; A.9.1.1; A.9.1.2; A.9.2; A.9.4.1; A.11.1.3; A.11.2.4; A.11.2.7; A.11.2.8; A.11.2.9; A.12.2.1; A.12.4.1; A.13.1.2; A.13.1.3; A.13.2.1; A.13.2.3; A.14.1.1
Zneužití práv	A.6.2.1; A.6.2.2; A.7.1.2; A.9.1.1; A.9.1.2; A.9.2; A.9.3.1; A.9.4.1; A.9.4.3; A.11.1.2; A.11.1.3; A.11.2.8; A.11.2.9; A.12.4.1; A.13.1.3; A.13.2.1
Padělání práv	A.9.2
Chyba při použití	A.6.2.1; A.7.1.2; A.8.1.3; A.9.1.1; A.9.2; A.9.3.1; A.9.4.1; A.9.4.2; A.11.2.9; A.12.4.4; A.12.6.2; A.13.1.3; A.13.2.1; A.13.2.3

Tab. 10 Přehled aplikovaných opatření

Opatření
A.5 Politiky bezpečnosti informací
A.5.1.1 Politiky pro bezpečnost informací
A.5.1.2 Přezkoumání politik pro bezpečnost informací
A.6 Organizace bezpečnosti informací
A.6.1.1 Role a odpovědnosti bezpečnosti informací
A.6.2.1 Politika mobilních zařízení
A.6.2.2 Práce na dálku
A.7 Bezpečnost lidských zdrojů
A.7.1.2 Podmínky pracovního poměru
A.7.2.1 Odpovědnosti managementu organizace
A.7.2.2 Povědomí, vzdělávání a školení o bezpečnosti informací
A.8 Řízení aktiv
A.8.1.1 Seznam aktiv
A.8.1.2 Vlastnictví aktiv
A.8.1.3 Přípustné použití aktiv
A.8.2.1 Klasifikace informací
A.8.2.2 Označování informací
A.8.3.1 Správa výměnných médií
A.9 Řízení přístupu
A.9.1.1 Politika řízení přístupu
A.9.1.2 Přístup k sítím a síťovým službám
A.9.2 Správa a řízení přístupu uživatele
A.9.3.1 Použití tajných autentizačních informací
A.9.4.1 Omezení přístupu k informacím
A.9.4.2 Bezpečné postupy přihlášení
A.9.4.3 Systém správy hesel
A.11 Fyzická bezpečnost a bezpečnost prostředí
A.11.1.1 Fyzický bezpečnostní perimetr
A.11.1.2 Fyzické kontroly vstupu

A.11.1.3 Zabezpečení kanceláří, místností a vybavení
A.11.1.4 Ochrana před vnějšími a přírodními hrozbami
A.11.2.1 Umístění zařízení a jeho ochrana
A.11.2.2 Podpůrné služby
A.11.2.4 Údržba zařízení
A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení
A.11.2.8 Neobsluhovaná uživatelská zařízení
A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru
A.12 Bezpečnost provozu
A.12.1.1 Dokumentace provozních postupů
A.12.1.2 Řízení změn
A.12.2.1 Opatření na ochranu proti malwaru
A.12.3.1 Zálohování informací
A.12.4.1 Zaznamenávání událostí formou logů
A.12.4.4 Synchronizace hodin
A.12.6.2 Omezení instalace softwaru
A.13 Bezpečnost komunikací
A.13.1.2 Bezpečnost síťových služeb
A.13.1.3 Princip oddělení v sítích
A.13.2.1 Politiky a postupy při přenosu informací
A.13.2.3 Elektronické předávání zpráv
A.14 Akvizice, vývoj a údržba systému
A.14.1.1 Analýza a specifikace požadavků bezpečnosti informací
A.14.2.1 Politika bezpečného vývoje
A.18 Soulad s požadavky
A.18.1.4 Soukromí a ochrana osobních údajů

4.1.1 A.5 Politiky bezpečnosti informací

Cílem je poskytnout pokyny a podporu ze strany managementu pro bezpečnost informací v souladu s požadavky podnikatelské činnost firmy a příslušnými zákony a předpisy.

A.5.1.1 Politiky pro bezpečnost informací

První krok zavedení ISMS je definovaní směru bezpečnosti informací v dokumentu Politika bezpečnosti informací. Schválením tohoto dokumentu vedení společnosti vyjádří podporu pro zavedení bezpečnosti informací. Politika bezpečnosti informací musí být v souladu s požadavky společnosti i legislativy a zpřístupněna všem zaměstnancům a relevantním externím stranám. Dokument by měl obsahovat následující body:

- Cíle, rozsah a definovaný význam bezpečnosti informací pro společnost
- Definice základních bezpečnostních zásad, principů a pravidel
- Určení odpovědností a pravomocí pro řízení bezpečností informací
- Vyjádření zájmu o rozvoj a prohlubování bezpečnosti informací

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Vytvořenou politiku bezpečnosti informací je ze strany vlastníka bezpečnostní politiky vhodné v pravidelných intervalech nebo při významné změně ve společnosti aktualizovat a vyhodnocovat. Aktualizace je příležitostí ke zlepšení organizace bezpečnosti informací a přizpůsobit pravidla současným potřebám podniku.

4.1.2 A.6 Organizace bezpečnosti informací

Cílem je ustanovit řídící rámec pro zahájení řízení implementace a provozu bezpečnosti informací v rámci společnosti.

A.6.1.1 Role a odpovědnosti bezpečnosti informací

V souladu s politikou bezpečnosti informací je třeba přidělit odpovědnosti dle následujících funkcí:

- Představitel vedení – vykonává dohled nad ISMS a stanovuje politiku bezpečnosti informací
- Bezpečnostní manažer – rozvíjí a implementuje opatření k zabezpečení informací
- Vlastníci aktiv – odpovídají za správu a ochranu přidělených aktiv
- Administrátor – odpovídá a provádí bezpečnostní opatření v oblasti hardwaru i softwaru, včetně zajištění síťového připojení, antivirové ochrany, nastavení elektronické pošty
- Auditor ISMS – zaměstnanec organizace, který je povolán jako interní auditor ISMS

A.6.2.1 Politika mobilních zařízení

Bude vytvořena politika pro využívání mobilních zařízení, která bude obsahovat doporučení pro práci s mobilními zařízeními a doporučení pro případ krádeže nebo ztráty. Každý uživatel při převzetí zařízení potvrdí seznámení s touto politikou a převzetí odpovědnosti za svěřené zařízení.

Doporučení pro práci s mobilními zařízeními:

- přítomnost a pravidelná aktualizace antivirového programu
- pravidelná instalace bezpečnostních aktualizací
- pravidelně vytvářet záloh důležitých informací
- automatické uzamykání zařízení
- zabezpečení zařízení proti odcizení a ztrátě
- vzdálený přístup pouze po autorizaci
- nepřipojovat mobilní zařízení k neznámým zařízením nebo veřejným sítím
- stahovaní aplikací pouze z ověřených zdrojů

Doporučení v případě krádeže nebo ztráty mobilního zařízení:

- neprodleně informovat administrátora
- pomocí vzdáleného přístupu zamknout zařízení a případně smazat data
- změna přístupových údajů v souvislosti se zařízením
- zákaz přístupu do systému ze zařízení

A.6.2.2 Práce na dálku

Budou vypracovány pokyny, které budou obsahovat doporučení pro práci na dálku. Při převzetí se každý uživatel zaváže k dodržování těchto pokynů a k odpovědnosti za svěřená zařízení.

Doporučení pro práci na dálku:

- vzdálený přístup je možný pouze ze schválených zařízení
- více faktorové ověření (ID + heslo a bezpečnostní token např. dle obrázku 19)
- použití zařízení pouze pro činnosti spojené s výkonem práce
- v případě práce z domu jsou stanoveny minimální požadavky na zabezpečení přístupového bodu k síti
- zákaz připojování zařízení k veřejným sítím
- zákaz připojování externích výměnných médií
- aktualizace softwaru
- pravidelná kontrola zařízení administrátorem
- vyžadováno dodržování pokynů pro neobsluhovaná zařízení (A.11.2.8) a zásad prázdného stolu a prázdné obrazovky monitoru (A.11.2.9)

Obr. 19 RSA SecurID token [zdroj: vlastní]

4.1.3 A.7 Bezpečnost lidských zdrojů

Cílem bezpečnosti lidských zdrojů je zajistit, aby si byli zaměstnanci a smluvní strany vědomi svých povinností. Výběrem vhodných kandidátů lze snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků společnosti.

A.7.1.2 Podmínky pracovního poměru

Pracovní smlouvy uzavřené se zaměstnanci a smluvními stranami s přístupem k aktivům obsahují závazek o mlčenlivosti a odpovědnosti za svěřená aktiva a jsou podepsány před zpřístupněním aktiv. Součástí dohody o mlčenlivosti je stanovena odpovědnost za bezpečnost informací po ukončení pracovního poměru. V případě, že se zaměstnanec dopustí narušení bezpečnosti informací bude s ním vedeno disciplinární řízení.

A.7.2.1 Odpovědnosti managementu organizace

Vedení společnosti bude požadovat od zaměstnanců a smluvních stran dodržování bezpečnosti informací v souladu se schválenou politikou (viz. A.5.1.1) a postupy společnosti. Management zajistí náležité informování zaměstnanců a smluvních stran o jejich rolích a odpovědnostech v oblasti bezpečnost informací před zpřístupněním neveřejných informací. Zaměstnanci budou mít přístup ke směrnicím a vzdělávání v oblasti plnění politiky bezpečnosti informací.

A.7.2.2 Povědomí, vzdělávání a školení o bezpečnosti informací

Bezpečností manažer vytvoří plán úvodních školení a pravidelného přeškolování. Školení je vhodné doplnit i o testování uživatelů např. prostřednictvím simulované phishingové kampaně nebo penetračního testování. Dále vytvoří komunikační kanál pro pravidelné informování uživatelů o změnách v politikách a postupech bezpečnosti informací.

Školení pokryje oblasti:

- vnitřní předpisy
- fyzická bezpečnost
- ochrana IT prostředků (PC, mobilní zařízení atd.)
- používání hesel
- bezdrátové sítě
- přenosná média
- internetové služby
- škodlivý kód a jeho šíření
- zvládání bezpečnostních incidentů
- nakládání s citlivými informacemi
- autorská práva a IT
- ochrana osobních údajů

4.1.4 A.8 Řízení aktiv

Cílem je u identifikovaných aktiv definovat odpovědnosti za přiměřenou ochranu a zajistit, aby informace získaly odpovídající úroveň ochrany s ohledem na význam pro společnost.

A.8.1.1 Seznam aktiv

Opatření vyžaduje identifikaci důležitých informačních aktiv společnosti, dokumentaci jejich významu. Seznam aktiv je vhodné aktualizovat pravidelně nebo při významné změně (např. při nákupu nového vybavení nebo změně informačního systému). Aktiva společnosti byla identifikována v kapitole 3.2.1.

A.8.1.2 Vlastnictví aktiv

Ke všem identifikovaným aktivům bude přiřazen vlastník, který má povinnost:

- zajistit, že aktiva jsou inventarizovaná
- zajisti, že aktiva jsou náležitě klasifikována a chráněna
- stanovit a pravidelně přezkoumávat omezení přístupu k důležitým aktivům a jejich klasifikaci, s přihlédnutím k platným politikám řízení přístupu
- zajistit správné zacházení, když je aktivum vymazáno nebo zničeno

A.8.1.3 Přípustné použití aktiv

Budou určena pravidla pro přípustné používání informačních aktiv a technických prostředků společnosti, např. zákaz kopírování citlivých informací společnosti na přenosná média. S těmito pravidly musí být seznámeni všechny relevantní strany.

A.8.2.1 Klasifikace informací

Jednotlivá aktiva budou svými vlastníky klasifikována na základě klasifikačního schématu dle tabulky 11.

Tab. 11 Klasifikace informací dle Doucek [7]

<table>
<tr><th colspan="3">Klasifikace</th><th colspan="2">Označení</th><th colspan="2">Základní popis</th></tr>
<tr><td colspan="3">Veřejné informace</td><td colspan="2">Veřejné informace | VER</td><td colspan="2">Informace, které jsou v souladu s politikou bezpečnosti informací odpovědnou osobou schválené ke zveřejnění</td></tr>
<tr><td rowspan="5">Neveřejné informace</td><td colspan="2">Interní informace</td><td colspan="2">Interní informace | INT</td><td colspan="2">Informace, jejichž zveřejnění může ohrožovat zájmy společnosti, ale nejsou chráněny legislativou nebo smluvně</td></tr>
<tr><td rowspan="4">Citlivé informace</td><td rowspan="3">Důvěrné informace</td><td rowspan="3">Důvěrné informace</td><td rowspan="3">DUV</td><td>osobní údaje</td><td>Informace chráněné na základě nařízení EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR)</td></tr>
<tr><td>obchodní tajemství</td><td>Informace chráněné na základě §504 zákona č. 89/2012 Sb., občanský zákoník</td></tr>
<tr><td>informace smluvních stran</td><td>Informace chráněné na základě smluvních nebo jiných požadavků</td></tr>
<tr><td rowspan="2">Přísně důvěrné informace</td><td rowspan="2">Přísně důvěrné informace</td><td rowspan="2">PDUV</td><td colspan="2">Informace charakteru obchodního tajemství, jejichž ohrožení vede k poškození strategických a klíčových zájmů společnosti</td></tr>
<tr><td>zvláštní kategorie osobních údajů (citlivé údaje)</td><td>Informace chráněné na základě článku 9 nařízení EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR)</td></tr>
</table>

A.8.2.2 Označování informací

Informace budou označovány na základě tabulky 12 a s tímto principem budou seznámeni zaměstnanci a třetí strany.

Tab. 12 Návrh opatření klasifikace informací dle Doucek [7]

Název a označení	Veřejné informace (Ver)	Interní informace (Int)	Důvěrné informace (Duv)	Přísně důvěrné informace (PDuv)
Označování	doporučené	doporučené	na 1. straně	všechny strany
Evidence počtu stran	není nutné	není nutné	číslo strany/počet stran celkem	číslo strany/počet stran celkem
Elektronické označení	doporučené	doporučené	doporučené	povinné
Předání elektronickou poštou (externí)	bez regulace	bez regulace	doporučeno šifrování	povinné šifrování
Předání elektronickou poštou (interní)	bez regulace	doporučeno šifrování	povinné šifrování	povinné šifrování

A.8.3.1 Správa výměnných médií

Pokyny pro správu výměnných médií:

- obsah médií, která mají být odstraněna učinit neobnovitelným
- ukládat média v bezpečném prostředí a v souladu s doporučením výrobce
- předcházet degeneraci médií a potřebná data přenášet na nová média
- vícenásobné kopie cenných dat ukládat na oddělená média
- přítomnost mechaniky pro výměnná média pouze v oprávněných případech
- monitorovat přenos informací na výměnná média

4.1.5 A.9 Řízení přístupu

Cílem je omezení přístupu k informacím a k vybavení pro jejich zpracování. Dále zajištění oprávněného přístupu nebo naopak zabránění neoprávněnému přístupu k systémům, aplikacím a službám.

A.9.1.1 Politika řízení přístupu

Vlastníci aktiv určí pravidla řízení přístupu, přístupová práva a omezení pro jednotlivé pozice ve vztahu k jejich aktivům na principu „obecně je zakázáno vše, co není výslovně povoleno“.

A.9.1.2 Přístup k sítím a síťovým službám

Ve všech prostorách společnosti je k dispozici Wifi síť. Tato síť bude nadále všem zařízením umožňovat pouze připojení k internetu, nikoliv k podnikové síti. Nově bude přístup k podnikovým sítím nebo síťovým službám umožněn po náležité autorizaci uživatele v samostatné síti a používání bude monitorováno.

A.9.2 Správa a řízení přístupu uživatelů

Je vytvořen formální postup pro správu a řízení uživatelských přístupů. Uživatel je podle tohoto postupu registrován pod jedinečnou identitou. Podle pozice zaměstnance jsou po úplné autorizaci zpřístupněna odpovídající oprávnění ke službám a systémům. Údaje o registracích a jejich oprávnění jsou evidovány, pravidelně přezkoumávány a v případě změny smluvního vztahu upraveny. V případě ukončení smluvního vztahu jsou odebrána veškerá přístupová oprávnění.

A.9.3.1 Použití tajných autentizačních informací

Všichni uživatelé jsou poučeni a je po nich vyžadováno:

- nezapisovat hesla na volně přístupná místa
- nesdílet hesla
- nepoužívat jedno heslo pro více přístupů
- používat různá hesla pro osobní a pracovní účely
- neukládat hesla v rámci přihlašování
- po prvním přihlášení změnit jednorázové heslo

A.9.4.1 Omezení přístupu k informacím

V souladu s politikou řízení přístupu je omezen a pravidelně kontrolován přístup k informacím a systémům ze strany jednotlivých uživatelů s ohledem na jejich přístupová práva.

A.9.4.2 Bezpečné postupy přihlášení

Pravidla pro bezpečné přihlášení:

- pro přihlašování k systémům a aplikacím používat pouze zařízení společnosti
- nikdy neukládat hesla a nepovolovat automatické přihlášení
- nezobrazovat heslo ani počet jeho znaků
- v rámci přihlašování by mělo být zobrazováno pouze minimum informací
- neměly by být přítomny žádné nápovědy nebo cokoliv co by se dalo zneužít
- proces přihlašovaní vykonávat až v případě, že jsou vyplněny všechny potřebné údaje
- v případě opakovaného přihlášení vytvořit bezpečnostní událost, a pokud bude překročen nastavený počet pokusů, tak přihlašování zablokovat a informovat zodpovědnou osobu
- používat vhodné a dostatečně bezpečné šifrování

A.9.4.3 Systém správy hesel

Systém správy hesel:

- vynutí použití ID a hesla pro přihlášení
- umožňuje uživatelům výběr a změnu vlastního hesla (počítá s chybami při zadávání)
- vynutí výběr kvalitního hesla (dle zásad bezpečného hesla)
- vynutí pravidelné změny hesla a zamezí opětovnému použití stejného hesla
- nezobrazuje hesla na obrazovce při zadávání
- ukládá soubory s hesly odděleně od dat aplikačních systémů

Zásady bezpečného hesla:

- délka hesla minimálně 8 znaků
- kombinace malých, velkých písmen, číslic a speciálních znaků
- nepoužívat hesla související s nějakou reálnou skutečností
- nepoužívat reálná slova
- střídat písmena, čísla a speciální znaky

4.1.6 A.11 Fyzická bezpečnost a bezpečnost prostředí

Opatření, která zabraňují neautorizovanému fyzickému přístupu do společnosti a možnému poškození nebo narušení informací a vybavení pro zpracování informací. Dále chrání před ztrátou, poškozením, krádeži nebo kompromitaci aktiv a možnému narušení činnosti společnosti.

A.11.1.1 Fyzický bezpečnostní perimetr

Pro ochranu prostor jsou určeny celistvé bezpečnostní perimetry chráněné před neoprávněným přístupem pomocí kontrolních mechanismů (např. ploty, mříže, alarmy, kamerový systém, zámky, čipové karty). Zabezpečení jednotlivých perimetrů by mělo zohledňovat význam chráněných aktiv.

A.11.1.2 Fyzické kontroly vstupu

Fyzické kontroly vstupu jsou zajišťovány recepcí a v době mimo provoz recepce prostřednictvím bezpečnostní agentury. Návštěvy budou nejen doprovázeny, ale i viditelně označeny a na recepci evidovány do knihy návštěv.

A.11.1.3 Zabezpečení kanceláří, místností a vybavení

Zaměstnanci jsou poučeni o zamykání kanceláří v době nepřítomnosti a náhradní klíče jsou zabezpečeny. Do serveroven bude zřízen přístup pomocí čipových karet a tím zajištěn a monitorován přístup pouze oprávněných osob. Záložní klíče od těchto prostor budou uchovávány v trezoru u odpovědného pracovníka a nebude umožněn přístup pomocí univerzálního klíče.

A.11.1.4 Ochrana před vnějšími a přírodními hrozbami

Společnost je chráněna před přírodními hrozbami dle platných požadavků legislativy. V bezprostřední blízkosti areálu společnosti se nachází Ivanovický potok, který má minimální průtok a je situován ve vybetonovaném korytě. Tento potok nemá stanovenu žádnou záplavovou oblast a nepředstavuje tak hrozbu.

A.11.2.1 Umístění zařízení a jeho ochrana

Cílem je zajištění bezpečnosti zařízení před nepříznivými vlivy životního prostředí a neoprávněného přístupu. Omezení fyzického přístupu je součástí předchozích opatření, ale další rizika plynou z životního prostředí, ve kterém se zařízení nacházejí. Je nutné umisťovat zařízení tak, aby byla zachována jejich fyzická bezpečnost a bezpečné podmínky provozu. Serverovny jsou klimatizovány a je hlídána teplota místností. U serverů, diskových polí a NAS disků je instalována přepěťová ochrana.

A.11.2.2 Podpůrné služby

Zařízení by měla být dostatečně chráněna před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb. Před výpadkem napájení budou chráněny jednotlivá PC záložním zdrojem (UPS), aby bylo možné uložit rozdělanou práci a bezpečně vypnout zařízení. Servery jsou vybaveny záložními zdroji s dostatečnou kapacitou pro umožnění řádného vypnutí. Pro případ výpadku internetového připojení je zajištěno více dodavatelů.

A.11.2.4 Údržba zařízení

Administrátor zajišťuje:

- pravidelnou kontrolu zařízení z důvodu udržení stálé dostupnosti a integrity
- údržbu v souladu s doporučenými servisními intervaly a specifikacemi výrobce
- provedení oprav autorizovaným servisem nebo autorizovanými pracovníky údržby
- vedení záznamů o všech podezřelých nebo skutečných chybách a o veškerých opravách a údržbách
- vyjmutí disku s neveřejnými informacemi nebo odstranění dat ze zařízení v případě opravy mimo prostory společnosti

A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení

Zařízení budou před likvidací nebo před opakovaným použitím prověřena, zda obsahují citlivá data nebo licencovaný software. Zařízení, která obsahují neveřejné informace a data budou fyzicky zničena nebo budou obsažené informace zničeny, vymazány nebo přepsány pomocí technik neumožňujících obnovení. Při malém počtu likvidovaných zařízení je vhodné zvolit externí firmu.

A.11.2.8 Neobsluhovaná uživatelská zařízení

Všichni uživatelé budou informováni o následujících bezpečnostních požadavcích a postupech pro ochranu neobsluhovaných zařízení:

- uzamčení počítače nebo mobilního zařízení, pokud se zařízení nepoužívá nebo se uživatel vzdálí
- odhlášení z aplikací a síťových služeb po skončení pracovní doby

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Všichni uživatelé budou informováni o následujících bezpečnostních požadavcích a postupech zásad prázdného stolu a prázdné obrazovky:

- uzamčení počítače při opuštění pracovního místa
- mimo dobu používání jsou veškeré neveřejné informace v jakékoliv podobě bezpečně uzamčeny
- média s neveřejnými informacemi jsou ihned odebírána z tiskáren

4.1.7 A.12 Bezpečnost provozu

Cílem bezpečnosti provozu je správné a bezpečné provozování vybavení pro zpracování informací. Je zapotřebí informace i vybavení pro jejich zpracování chránit před malwarem, data chránit před ztrátou, zaznamenávat události a generovat důkazy, zajistit integritu provozních systémů a zabránit využívání technických zranitelností.

A.12.1.1 Dokumentace provozních postupů

Pro provozní činnosti spojené s vybavením pro zpracování informací společnost stanoví, bude dokumentovat a dávat k dispozici provozní postupy. Tyto postupy budou dostupné všem zaměstnancům a zahrnují:

- vypnutí a zapnutí počítače
- zálohování
- údržbu zařízení
- zacházení s médii
- zacházení s poštou
- bezpečnost práce

A.12.1.2 Řízení změn

Společnost zavede postupy pro řízení a kontrolu změn podnikových procesů, vybavení pro zpracování informací a systémů s vlivem na bezpečnost informací. V případě významné změny budou stanoveny možné dopady z hlediska bezpečnosti informací a po realizaci ověřeno splnění požadavků na bezpečnost informací.

A.12.2.1 Opatření na ochranu proti malwaru

Ochrana před malwarem je založena na jeho detekci pomocí softwarových produktů, bezpečnostním povědomí uživatelů a odpovídajících opatřeních v oblasti řízení přístupu a změn.

Budou zavedena opatření:

- znemožněna instalace neautorizovaného softwaru (seznam povolených aplikací)
- znemožněno procházení podezřelých webových stránek (seznam nepovolených webových stránek)
- pravidelná aktualizace softwaru pro detekci malwaru
- uživatelé nesmí bez souhlasu administrátora vypínat antivirovou ochranu a firewall nebo měnit nastavení antivirového softwaru
- pravidelná školení uživatelů
- pravidelné přezkoumání PC, notebooků a mobilních zařízení s ohledem na neschválené soubory a doplňky
- formální politika na ochranu proti rizikům spojených se získáním souborů nebo softwaru z externích zdrojů
- připraveny plány pro zotavení se z útoku vyvolaného malwarem, včetně všech potřebných dat a záloh softwaru

Plán obnovy (Disaster Recovery Plan) obsahuje:

- minimální úroveň služeb přijatelnou pro užívání, provoz a správu systému
- dobu obnovení chodu (RTO) pro obnovení minimální úrovně poskytovaných služeb
- bod obnovení dat (RPO) - časové období pro zpětné obnovení dat
- ověřování obnovitelnosti a čitelnosti záloh
- osobu odpovědnou za jednotlivé činnosti
- potřebné zdroje
- kontakty na dodavatele

A.12.3.1 Zálohování informací

Politika zálohování bude zahrnovat požadavky společnosti na pravidelné zálohování informací, softwaru a systémů, na uchovávání a ochranu záloh a na postupy obnovy dat. Zálohovaným informacím je poskytnuta odpovídající úroveň fyzické i vnější ochrany a záložní média budou pravidelně testována na spolehlivé použití při obnově informací. Pravidlo 3-2-1 určuje prověřený postup pro zálohování:

- 3 kopie nebo verze
- 2 různá média
- 1 záloha mimo pracoviště nebo budovu společnosti

A.12.4.1 Zaznamenávání událostí formou logů

Formou logů mají být dokumentovány a pravidelně přezkoumávány záznamy o aktivitách uživatelů a o různých selháních. Administrátoři nemají oprávnění zasahovat do záznamů logů o svých vlastních aktivitách a všechny záznamy jsou chráněny proti neoprávněnému přístupu. Požadované době uchovávání záznamů bude uzpůsobeno velikost úložiště.

Záznamy obsahují:

- ID uživatele
- identifikaci zařízení a systému
- datum a čas přihlášení/ odhlášení
- použití systémových aplikací a nástrojů
- použití privilegií
- prohlížené soubory
- poplachy vyvolané systémem řízení přístupu

A.12.4.4 Synchronizace hodin

Čas je synchronizován ve všech relevantních systémech zpracování informací v celé společnosti na referenční čas.

A.12.6.2 Omezení instalace softwaru

Budou nastavena pravidla, kdy bude mít uživatel k dispozici zařízení s již předinstalovaným a nastaveným softwarem. Uživatel bude mít oprávnění instalovat pouze aplikace ze seznamu povolených, případně bude možnost instalace software uživatelem zcela zakázána.

4.1.8 A.13 Bezpečnost komunikací

Cílem je zajištění ochrany informací v sítích a při přenosu v rámci společnosti nebo externích subjektů.

A.13.1.2 Bezpečnost síťových služeb

Ve smlouvách o síťových službách jsou zahrnuty požadavky na bezpečnostní mechanismy, na úrovně služeb a na správu a řízení síťových služeb.

A.13.1.3 Princip oddělení v sítích

V sítích jsou odděleny skupiny informačních služeb, uživatelů a informačních systémů, které mohou komunikovat pouze v rámci dané sítě VLAN nebo jsou nastavena pravidla pro komunikaci mezi sítěmi. Segmentace sítě omezí dosah v případě průniku do sítě.

Návrh na rozdělení sítí

- Wifi pro přístup na internet v jednotlivých budovách
- Servery
- Účetní oddělení
- Administrativa
- Procesní oddělení
- Výrobní zařízení
- Výrobní oddělení
- Vývojové oddělení
- Správa sítě a IT

A.13.2.1 Politiky a postupy při přenosu informací

Budou zavedeny politiky, které definují postupy pro:

- ochranu přenášených informací před odposloucháváním, kopírováním, pozměněním, chybným přesměrováním nebo zničením
- detekci a ochranu před malware z elektronické komunikace
- ochranu neveřejných informací v přílohách elektronické komunikace
- odpovědnosti zaměstnanců a třetích stran za pomluvy, obtěžování, přeposílání řetězových zpráv apod.
- uchovávání a likvidaci podnikové korespondence
- doporučení zaměstnancům o přijetí preventivních opatření proti prozrazení neveřejných informací

A.13.2.3 Elektronické předávání zpráv

Zásady bezpečnosti elektronické komunikace:

- nereagovat na zprávy vyzívající ke změně hesla a nastavení nebo sdílení neveřejných informací
- při náznaku zneužití ihned kontaktovat administrátora
- nekomunikovat přes sociální média
- nenahrávat neveřejné informace na veřejná uložiště

4.1.9 A.14 Akvizice, vývoj a údržba systému

Cílem je implementace bezpečnosti informací jako nedílné součásti informačních systémů během celého životního cyklu.

A.14.1.1 Analýza a specifikace požadavků bezpečnosti informací

Požadavky na nové nebo na vylepšení stávajících informačních systémů zahrnují i bezpečnost informací v rámci celého životního cyklu systému.

Zásady provozní správy systémů:

- změny a aktualizace softwaru provádí pouze oprávněná osoba, dle stanovených postupů
- změny a aktualizace jsou dokumentovány

A.14.2.1 Politika bezpečného vývoje

Společnost při vlastním vývoji informačního systému podpory prodeje a manažerské nadstavby pro ERP systém má dbát na:

- bezpečné vývojové prostředí
- kontrolní body bezpečnosti v milnících projektu
- řízení verzí
- implementuje bezpečnostní požadavky pro danou fázi vývoje
- opravu zranitelných míst a jejich vyhledávání

4.1.10 A.18 Soulad s požadavky

Cílem je zamezit porušení právních, zákonných, předpisových nebo smluvních povinností, které mají souvislost s bezpečností informací nebo s obecnými požadavky na bezpečnost.

A.18.1.4 Soukromí a ochrana osobních údajů

Politika nakládání s osobními údaji je v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů.

4.2 Soubor opatření

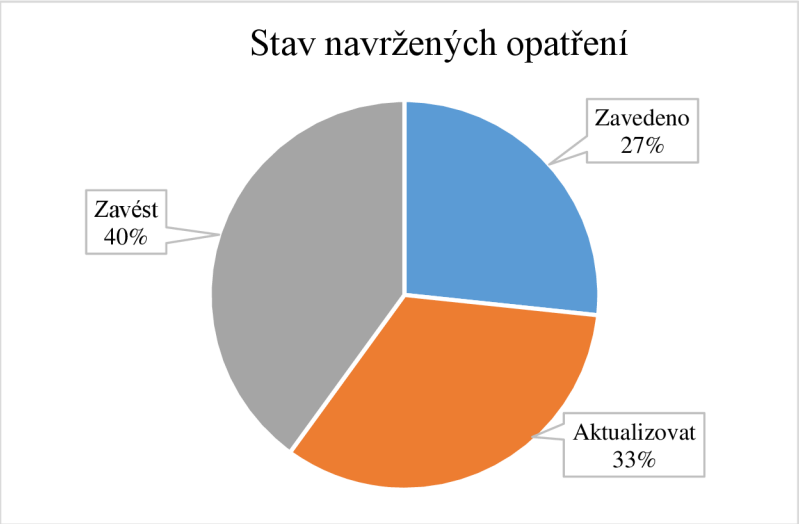
Společnost má v současné době zájem začít řešit bezpečnost informací především celkově a systematicky. V tabulce 13 jsou uvedena použitá opatření z přílohy A normy ČSN ISO/IEC 27001:2014 a k nim doplněn stav daného opatření ve společnosti. Některá z vybraných opatření jsou zavedena, jiná je potřeba aktualizovat (segmenty z navržených opatření jsou uplatněny, ale v nedostatečné míře, s nedostatečným důrazem nebo podle zastaralých principů) nebo zavést.

Tab. 13 Soubor bezpečnostních opatření dle ČSN ISO/IEC 27001:2014

Opatření	Stav
A.5 Politiky bezpečnosti informací	
A.5.1.1 Politiky pro bezpečnost informací	Zavést
A.5.1.2 Přezkoumání politik pro bezpečnost informací	Zavést
A.6 Organizace bezpečnosti informací	
A.6.1.1 Role a odpovědnosti bezpečnosti informací	Zavést
A.6.2.1 Politika mobilních zařízení	Aktualizovat
A.6.2.2 Práce na dálku	Aktualizovat
A.7 Bezpečnost lidských zdrojů	
A.7.1.2 Podmínky pracovního poměru	Zavedeno
A.7.2.1 Odpovědnosti managementu organizace	Zavést
A.7.2.2 Povědomí, vzdělávání a školení o bezpečnosti informací	Zavést
A.8 Řízení aktiv	

A.8.1.1 Seznam aktiv	Zavést
A.8.1.2 Vlastnictví aktiv	Zavést
A.8.1.3 Přípustné použití aktiv	Zavést
A.8.2.1 Klasifikace informací	Zavést
A.8.2.2 Označování informací	Zavést
A.8.3.1 Správa výměnných médií	Zavést
A.9 Řízení přístupu	
A.9.1.1 Politika řízení přístupu	Zavést
A.9.1.2 Přístup k sítím a síťovým službám	Aktualizovat
A.9.2 Správa a řízení přístupu uživatele	Zavedeno
A.9.3.1 Použití tajných autentizačních informací	Zavedeno
A.9.4.1 Omezení přístupu k informacím	Aktualizovat
A.9.4.2 Bezpečné postupy přihlášení	Aktualizovat
A.9.4.3 Systém správy hesel	Zavedeno
A.11 Fyzická bezpečnost a bezpečnost prostředí	
A.11.1.1 Fyzický bezpečnostní perimetr	Aktualizovat
A.11.1.2 Fyzické kontroly vstupu	Aktualizovat
A.11.1.3 Zabezpečení kanceláří, místností a vybavení	Aktualizovat
A.11.1.4 Ochrana před vnějšími a přírodními hrozbami	Zavedeno
A.11.2.1 Umístění zařízení a jeho ochrana	Zavedeno
A.11.2.2 Podpůrné služby	Aktualizovat
A.11.2.4 Údržba zařízení	Aktualizovat
A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení	Zavést
A.11.2.8 Neobsluhovaná uživatelská zařízení	Zavést
A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru	Zavést
A.12 Bezpečnost provozu	
A.12.1.1 Dokumentace provozních postupů	Zavést
A.12.1.2 Řízení změn	Aktualizovat
A.12.2.1 Opatření na ochranu proti malwaru	Aktualizovat
A.12.3.1 Zálohování informací	Aktualizovat
A.12.4.1 Zaznamenávání událostí formou logů	Aktualizovat
A.12.4.4 Synchronizace hodin	Zavedeno
A.12.6.2 Omezení instalace softwaru	Zavést
A.13 Bezpečnost komunikací	
A.13.1.2 Bezpečnost síťových služeb	Zavedeno
A.13.1.3 Princip oddělení v sítích	Zavedeno
A.13.2.1 Politiky a postupy při přenosu informací	Zavést
A.13.2.3 Elektronické předávání zpráv	Aktualizovat
A.14 Akvizice, vývoj a údržba systému	
A.14.1.1 Analýza a specifikace požadavků bezpečnosti informací	Zavedeno
A.14.2.1 Politika bezpečného vývoje	Zavedeno
A.18 Soulad s požadavky	
A.18.1.4 Soukromí a ochrana osobních údajů	Zavedeno

Na obrázku 20 je znázorněn stav vybraných opatření, kdy je patrný značný prostor pro zlepšení v podobě zavedení nebo aktualizaci opatření.



Obr. 20 Stav navržených opatření [zdroj: vlastní]

4.3 Zhodnocení opatření

Navržená opatření jsou především organizačního charakteru se zaměřením na lidský faktor a měla by být zaváděna postupně ve smyslu PDCA. Není nezbytné veškerá opatření zavádět okamžitě, protože už jenom povědomí o slabých místech, umožňuje s nimi pracovat a snížit tak rizika. Podle provedené analýzy největší rizika plynou ze škodlivého kódu, manipulace s přístupovými oprávněními, manipulace s daty a dokumenty a neúmyslné chyby uživatele.

Zavedením navržených politik vedení společnosti deklaruje zájem o komplexní řešení problematiky bezpečnosti informací. Dále definuje cíle a prostředky pro dosažení těchto cílů v jednotlivých oblastech bezpečnosti informací. Součástí politik budou i pokyny pro zaměstnance, které je žádoucí sestavit uživatelsky přívětivě. O zavedených politikách musí být zaměstnanci náležitě informováni a pravidelně proškolováni. Školení, vytvoření jasných pokynů a informování zaměstnanců o politikách bezpečnosti informací zredukuje hrozbu neúmyslné lidské chyby a zvýší povědomí o ostatních hrozbách. Technická opatření ke snížení vlivu škodlivého kódu jsou již do značné míry zavedena, ale bylo by vhodné je doplnit o větší segmentaci sítí. Hrozbu zneužití nebo padělání práv je vhodné řešit důsledným řízením přístupů k jednotlivým aktivům. Stanovení vlastníci aktiv určí nezbytnou míru jejich ochrany. Řízení přístupu k datům a dokumentům na okruh relevantních uživatelů omezuje i hrozbu neoprávněné manipulace. Pro případ poškození jsou data zálohována, ale důležitým bodem je vypracovat plán obnovy. Plán na obnovu systémů a dat by měl být jednou z priorit, obzvláště s ohledem na historii incidentů ve společnosti, které lze zavést i za současného stavu.

5 ZÁVĚR

Problematika bezpečnosti informací je velmi obsáhlá. Legislativa a normy musí dávat dostatečný prostor pro přizpůsobení rychlému vývoji. Tím jsou kladeny značné nároky na komplexní znalost problematiky, kterými ale běžně oddělení IT nedisponuje a nejslabším článkem, tak zůstává člověk – uživatel. Výsledkem těchto faktorů je, že aplikaci bezpečnosti informací na odpovídající úrovni se podnik často věnuje v případě, že je součástí nadnárodní společnosti se zavedenou politikou ISMS nebo management má zkušenosti s touto problematikou nebo je bezpečnosti informací řešena až zpětně po závažném incidentu.

Cílem této práce bylo popsat současný stav a trendy v kybernetické bezpečnosti, požadavky platných norem a harmonizovaných právních předpisů EU a ČR a vyhodnotit informační rizika ve vybrané strojírenské firmě.

Teoretická část obsahuje důležité pojmy. Jsou zde vyjmenovány související harmonizované právní předpisy EU a ČR, normy a postupy pro zavedení a provozování systému řízení bezpečnosti informací. Nejvýznamnějším harmonizovaným právním předpisem v je ČR zákon o kybernetické bezpečnosti, resp. vyhláška o kybernetické bezpečnosti. Dále jsou popsány vybrané normy, především z řady ISO/IEC 27k, a systém řízení bezpečnosti informací ISMS, který slouží pro zajištění odpovídající úrovně kybernetické bezpečnosti a bezpečnosti informací uvnitř organizace. Popsané normy z řady ISO/IEC 27k jsou vybrány na základě zaměření práce na výrobní společnost ve strojírenství. Nejpodrobněji jsou popsány ČSN ISO/IEC 27001:2014, ČSN ISO/IEC 27002:2014 a ČSN ISO/IEC 27005:2019, protože především podle těchto norem byla systémově řešena bezpečnost informací ve společnosti FERMAT.

V praktické části jsou vyhodnocena informační rizika ve firmě pomocí matice rizik, která vychází z identifikace a ohodnocení aktiv společnosti a hrozeb, která mohou poškodit tato aktiva. Především pro eliminaci nejzávažnějších rizik jsou navržena opatření se zaměřením na organizační opatření a snížení negativního vlivu lidského faktoru. Opatření jsou vybrána z přílohy A normy ČSN ISO/IEC 27001:2014 a navržena podle pokynů normy ČSN ISO/IEC 27002:2014 a odpovědí pracovníka společnosti. Práce poskytuje výběrový, ale ucelený a systematický přehled o bezpečnosti informací v jedné z poboček společnosti. Navržená opatření není nutné zavádět ihned všechna, základem je určit v managementu osobu odpovědnou za bezpečnost informací a zajistit odborníka nebo tým odborníků, který se bude věnovat zavedení a rozvoji ISMS v celé společnosti. Kromě zvýšení vlastní bezpečnosti tím společnost získá i možnost se začít s předstihem připravovat na chystané změny, které přinese aktualizace směrnice 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (tzv. NIS 2). Účelem směrnice je sjednocení úrovně zabezpečení, proto bude zásadním způsobem rozšířen okruh dotčených subjektů a zahrnuty i dodavatelské řetězce těchto subjektů. Výrobce strojů a strojních zařízení velikosti firmy FERMAT je v návrhu směrnice označen jako „důležitý subjekt“. Platnost nové směrnice se předpokládá od počátku roku 2022 a členské státy EU mají 18 měsíců od zveřejnění v úředním věstníku na převzetí do národní legislativy. V ČR by tato změna měla být realizována novelou zákona č. 181/2014 Sb. (ZoKB) a vyhlášky č. 82/2018 Sb. (VoKB). Zároveň by měla být v roce 2021, resp. 2022, dokončena aktualizace norem ISO/IEC 27001:2013 a ISO/IEC 27002:2013, která reaguje na vývoj v bezpečnosti informací.

6 SEZNAM POUŽITÝCH ZDROJŮ

[1] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015 [cit. 2021-03-10]. ISBN 978-80-7251-436-6.

[2] *Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě*. ISSN 1801-0393.

[3] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

[4] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o, 2019. ISBN 978-80-88168-34-8. Dostupné také z: https://www.pablikado.cz/dokument/vXmNgxSdmxSAenN4

[5] *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*.

[6] *ČSN ISO/IEC 27000:2020 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*.

[7] DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

[8] *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*. ISSN 1211-1244.

[9] *ČSN ISO/IEC 27032:2013 Informační technologie - Bezpečnostní techniky - Směrnice pro kybernetickou bezpečnost*.

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

[11] Blokové schéma k zákonu o kybernetické bezpečnosti. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. 2018 [cit. 2021-03-10]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

[12] *ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky*.

[13] SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

[14] *Řada norem ISO/IEC 27000* [online]. [cit. 2021-03-25]. Dostupné z: https://www.iso27000.cz/rac/homepage.nsf/CZ/ISO27000

[15] GOLL, Jan. *Zákon o kybernetické bezpečnosti versus ISO 27001: aneb jak vyhovět oběma normám* [online]. 2019 [cit. 2021-03-26]. Dostupné z: https://m.systemonline.cz/sprava-it/zakon-o-kyberneticke-bezpecnosti-versus-iso-27001.htm

[16] *Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*.

[17] *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2021-03-29]. Dostupné z: https://nukib.cz/cs/

[18] *ČSN ISO/IEC 27005:2018 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*.

[19] *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020*. 2021.

[20] *FERMAT* [online]. [cit. 2021-07-21]. Dostupné z: https://www.fermatmachinery.com/

7 SEZNAM ZKRATEK

ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
NIS	Network and Information Security
ISMS	Information Security Management System
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
ICT	Information and Communication Technologies
IS	Informační systém
IS/ICT	komplexní pojem zahrnující informační systémy a informační a komunikační technologie
SW	Software
HW	Hardware
UTC	Coordinated Universal Time
LAN	Local Area Network
CRM	Customer relationship management
ERP	Enterprise Resource Planning
DoS	Denial of service
DDoS	Distributed denial of service
PDCA	Plan – do – check – act
NBÚ	Národní bezpečnostní úřad
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
EU	Evropská unie
ES	Evropské společenství
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ČSN	Česká státní norma
COBIT	Control Objectives for Information and related Technology
ITIL	Information Technology Infrastructure Library
CRAMM	CCTA Risk Analysis and Management Method
VPN	Virtual Private Network
UPS	Uninterruptible Power Supply/Source

8 SEZNAM OBRÁZKŮ

Obr. 1 Vztah dat a informací dle Kolouch [4] 17
Obr. 2 Vztah informační a kybernetické bezpečnosti dle Doucek [7] 18
Obr. 3 Vztahy mezi pojmy bezpečnosti informací dle ČSN ISO/IEC 27032:2013 [9] 22
Obr. 4 Přiměřená bezpečnost za akceptovatelné náklady dle Ondrák [10] 22
Obr. 5 Výřez z blokového schématu k ZoKB dle NÚKIB [11] 26
Obr. 6 Vztahy mezi vybranými normami řady 27k dle ISO/IEC 27000:2020 [6] 28
Obr. 7 Životní cyklus kybernetické bezpečnosti dle Kolouch [4] 36
Obr. 8 PDCA model aplikovaný na procesy ISMS dle Kolouch [4] 37
Obr. 9 Budování ISMS dle Smejkal [13] 38
Obr. 10 Model měření bezpečnosti informací v organizace dle Doucek [7] 41
Obr. 11 Vztahy při řízení rizik dle Smejkal [13] 44
Obr. 12 Ilustrace procesu řízení rizik bezpečnosti informací dle ISO/IEC 27005:2019 [18] .. 45
Obr. 13 Činnosti ošetření rizika dle ČSN ISO/IEC 27005:2019 [18] 48
Obr. 14 Nejčastější typy kybernetických útoků v roce 2020 dle NÚKIB [19] 49
Obr. 15 Nejzávažnější typy kybernetických útoků 2020 dle NÚKIB [19] 50
Obr. 16 Vývoj kybernetických bezpečnostních incidentů řešených NÚKIB 2017–2020 [19] 50
Obr. 17 Lidské zdroje úmyslných hrozeb 54
Obr. 18 Zastoupení rizik v analýze [zdroj: vlastní] 57
Obr. 19 RSA SecurID token [zdroj: vlastní] 63
Obr. 20 Stav navržených opatření [zdroj: vlastní] 75

9 SEZNAM TABULEK

Tab. 1 Srovnání normy ČSN ISO/IEC 27001:2014 a vyhlášky č.82/2018 Sb. dle Goll [15].. 33
Tab. 2 Stupnice pro hodnocení aktiv 51
Tab. 3 Seznam a ohodnocení identifikovaných aktiv 52
Tab. 4 Stupnice pro hodnocení pravděpodobnosti výskytu hrozby 53
Tab. 5 Seznam a ohodnocení identifikovaných hrozeb 53
Tab. 6 Výběr z matice zranitelnosti 55
Tab. 7 Ohodnocení míry rizika 56
Tab. 8 Výběr z matice rizik 56
Tab. 9 Vybraná opatření pro řešení identifikovaných hrozeb 59
Tab. 10 Přehled aplikovaných opatření 60
Tab. 11 Klasifikace informací dle Doucek [7] 65
Tab. 12 Návrh opatření klasifikace informací dle Doucek [7] 66
Tab. 13 Soubor bezpečnostních opatření dle ČSN ISO/IEC 27001:2014 73

10 SEZNAM PŘÍLOH

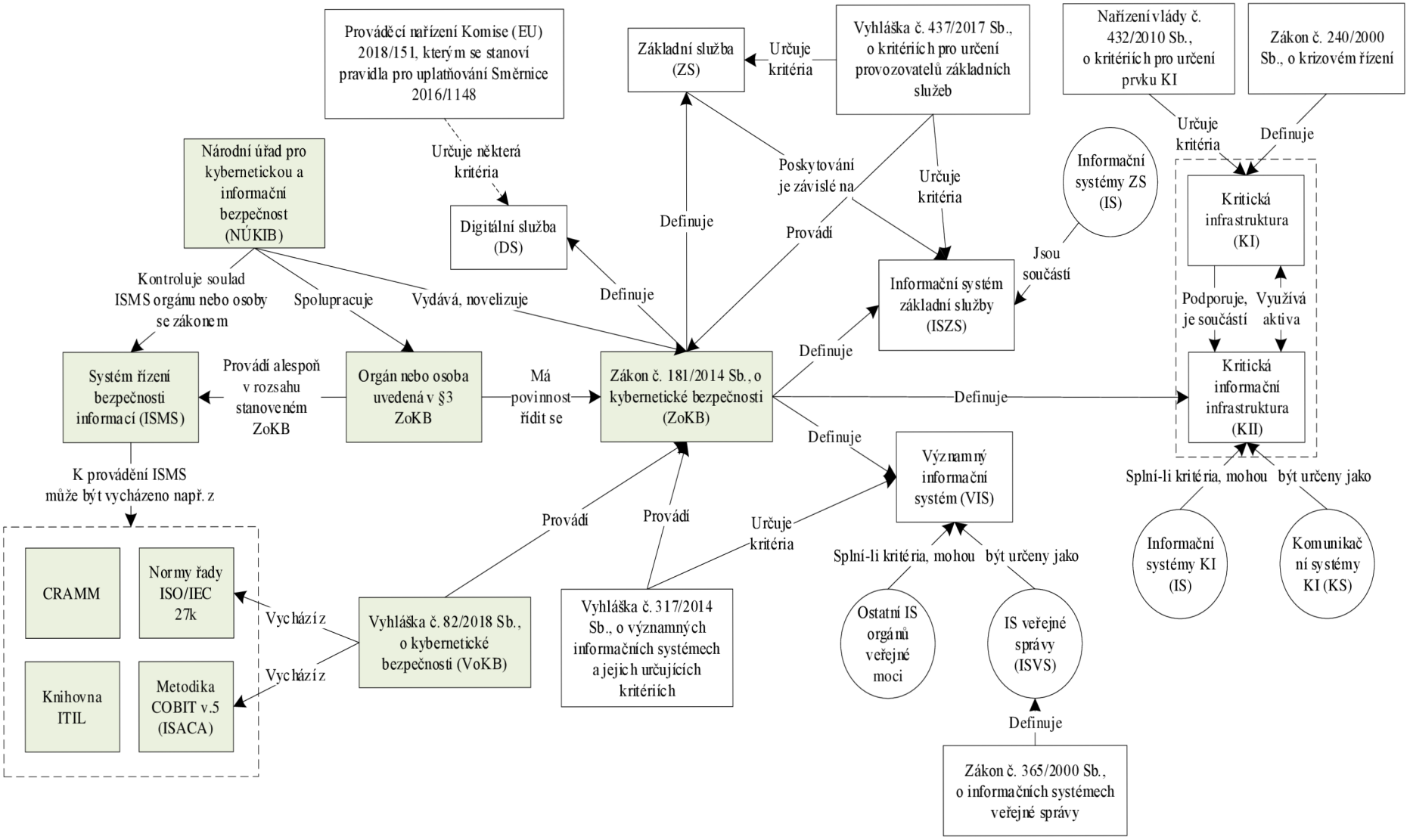
Příloha 1 – Úplné blokové schéma k ZoKB

Příloha 2 – Matice zranitelností

Příloha 3 – Matice rizik

Příloha 4 – Ukázka dotazníkového šetření

Příloha 1 – Úplné blokové schéma k ZoKB



Příloha 2 – Matice zranitelností

Zranitelnost (V)	Hrozba	Požár	Poškození vodou	Zničení zařízení nebo médií	Prach, koroze	Meteorologické jevy	Výpadek el. proudu	Výpadek internetového připojení	Výpadek síťových služeb	Krádež zařízení	Krádež dokumentů nebo médií	Manipulace s SW	Manipulace s HW	Špionáž nebo škodlivý kód	Selhání SW	Selhání HW	Poškození dat	Nezákonné zpracování dat	Zneužití práv	Padělání práv	Chyba při použití
Aktivum	T / A	1	1	2	2	1	3	3	4	2	3	2	2	4	2	2	3	2	3	3	4
Servery	4	3	3	3	2	3	2	2	2	4		2	3	4	2	3	4	3	3	4	3
Zálohovací NAS	4	3	3	3	2	3	2	2	2	4		2	3	4	2	3	4	3	3	4	3
PC a notebooky	3	3	2	3	3	2	2	2	2	3		3	3	4	3	3	3	2	3	3	3
Mobilní zařízení	3	1	1	3	2	2				3		2		3	2		2	2	3	3	3
Tiskárny	2	1	2		2	2				2		1	1		1	1					
Síťová infrastruktura	3	3	2	4	1	3	3		3	1		2			3						
Podnikový ERP systém	5								3		4	4		5	4		4	4	4	4	3
Systém pro podporu prodeje	4								3		3	4		5	4		3	3	2	2	2
Konstrukční SW	3											2		4	4				2		2
Operační systém	2											2		4	4				3	3	3
Kancelářské balíky	2							3	3			3			3				2	2	2
Antivirus	2											3			3						
Výrobní dokumentace	5	1	1	1		1					5			4			3	3	4	4	
Účetnictví	4	1	1	1		1					3			4			3	3	3	3	
Údaje o zaměstnancích	4	1	1	1		1					5			4			3	3	4	4	

Smluvní dokumentace	3	1	1	1		1					5			4			3	3	3	3		
Zálohy dat	4	3	3	2	2	3	1	2	2		5	3	3	5	2	3	3	3	3	3	4	
Připojení k internetu	3						2	3					2	3		2						
Webové stránky	1																		2	2		
Vzdálený přístup	2						3	3	3				3			3	3	2	4	4	3	
Elektronická pošta	3													4				2	3	3	2	
Budovy	4	4	4			2																

Příloha 3 – Matice rizik

Riziko (R)	Hrozba	Požár	Poškození vodou	Zničení zařízení nebo médií	Prach, koroze	Meteorologické jevy	Výpadek el. proudu	Výpadek internetového připojení	Výpadek síťových služeb	Krádež zařízení	Krádež dokumentů nebo médií	Manipulace s SW	Manipulace s HW	Špionáž nebo škodlivý kód	Selhání SW	Selhání HW	Poškození dat	Nezákonné zpracování dat	Zneužití práv	Padělání práv	Chyba při použití
Aktivum	T / A	1	1	2	2	1	3	3	4	2	3	2	2	4	2	2	3	2	3	3	4
Servery	4	12	12	24	16	12	24	24	32	32	0	16	24	64	16	24	48	24	36	48	48
Zálohovací NAS	4	12	12	24	16	12	24	24	32	32	0	16	24	64	16	24	48	24	36	48	48
PC a notebooky	3	9	6	18	18	6	18	18	24	18	0	18	18	48	18	18	27	12	27	27	36
Mobilní zařízení	3	3	3	18	12	6	0	0	0	18	0	12	0	36	12	0	18	12	27	27	36
Tiskárny	2	2	4	0	8	4	0	0	0	8	0	4	4	0	4	4	0	0	0	0	0
Síťová infrastruktura	3	9	6	24	6	9	27	0	36	6	0	12	0	0	18	0	0	0	0	0	0
Podnikový ERP systém	5	0	0	0	0	0	0	0	60	0	60	40	0	100	40	0	60	40	60	60	60
Systém pro podporu prodeje	4	0	0	0	0	0	0	0	48	0	36	32	0	80	32	0	36	24	24	24	32
Konstrukční SW	3	0	0	0	0	0	0	0	0	0	0	12	0	48	24	0	0	0	18	0	24
Operační systém	2	0	0	0	0	0	0	0	0	0	0	8	0	32	16	0	0	0	18	18	24
Kancelářské balíky	2	0	0	0	0	0	0	18	24	0	0	12	0	0	12	0	0	0	12	12	16
Antivirus	2	0	0	0	0	0	0	0	0	0	0	12	0	0	12	0	0	0	0	0	0
Výrobní dokumentace	5	5	5	10	0	5	0	0	0	0	75	0	0	80	0	0	45	30	60	60	0
Účetnictví	4	4	4	8	0	4	0	0	0	0	36	0	0	64	0	0	36	24	36	36	0
Údaje o zaměstnancích	4	4	4	8	0	4	0	0	0	0	60	0	0	64	0	0	36	24	48	48	0

Smluvní dokumentace	3	3	3	6	0	3	0	0	0	0	45	0	0	48	0	0	27	18	27	27	0
Zálohy dat	4	12	12	16	16	12	12	24	32	0	60	24	24	80	16	24	36	24	36	36	64
Připojení k internetu	3	0	0	0	0	0	18	27	0	0	0	0	12	36	0	12	0	0	0	0	0
Webové stránky	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	6	0
Vzdálený přístup	2	0	0	0	0	0	18	18	24	0	0	0	12	0	0	12	18	8	24	24	24
Elektronická pošta	3	0	0	0	0	0	0	0	0	0	0	0	0	48	0	0	0	12	27	27	24
Budovy	4	16	16	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Příloha 4 – Ukázka dotazníkového šetření

Politika z normy ČSN ISO/IEC 27001:2014	Odpověď	Návrh řešení
A.6 Organizace bezpečnosti informací		
A.6.2.1 Politika mobilních zařízení		
Je nastavena politika mobilních zařízení?	Ne	politiku zavést, seznámit s ní uživatele, některá doporučení jsou již aplikována
A.6.2.2 Práce na dálku		
Jsou v případě práce z domu stanoveny požadavky na zabezpečení?	Ne, jen pro připojení do naší sítě je nutné mít založen přístup přes VPN.	doplnit doporučení, bezpečnostní token jako součást více faktorového ověření
A.11 Fyzická bezpečnost a bezpečnost prostředí		
A.11.2.1 Umístění zařízení a jeho ochrana		
Je nějaká přepěťová ochrana zařízení? Nejen serverů	Jen důležitých zařízení.	zvážit UPS i pro PC
A.11.2.2 Podpůrné služby		
Je zajištěn záložní zdroj pro servery? A vícenásobný? Jak dlouho vydrží?	Ano. Jsou většinou dimenzovány, tak aby byl schopný server fungovat a proběhlo validní vypnutí.	zavedeno
Je zajištěn druhý poskytovatel internetového připojení?	Ano	zavedeno
A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení		
Jsou bezpečně vymazávána média? Jak se postupuje při likvidaci médií?	Není na to nastaven žádný postup.	při malém počtu likvidovaných zařízení je vhodnější zvolit externí firmu na profesionální likvidaci
A.11.2.8 Neobsluhovaná uživatelská zařízení		
Mají uživatelé povinnost si zamykat počítače, pokud se vzdálí a dodržují to?	Nikde to není písemně uvedeno.	seznámit zaměstnance v rámci školení a vyžadovat plnění
A.12 Bezpečnost provozu		
A.12.2.1 Opatření na ochranu proti malwaru		
Jsou vypracovány plány na obnovu po malwaru?	Ne	návrh plánu obnovy
A.12.3.1 Zálohování informací		
Jsou nějaké zálohy i mimo budovu firmy?	Ne. Zálohy jsou uchovávány na dvou zařízeních v různých budovách.	v rámci zavedení plánu na obnovu zvážit umístění potřebných záloh mimo budovy pobočky ve smyslu pravidla 3-2-1