

Návrh opatření a procesů v organizaci pro implementaci požadavků směrnice EU NIS2

Bc. Martin Chytka



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Bc. Martin Chytka
Osobní číslo: A23403
Studijní program: N0613A140022 Informační technologie
Specializace: Kybernetická bezpečnost
Forma studia: Kombinovaná
Téma práce: Návrh opatření a procesů v organizaci pro implementaci požadavků směrnice EU NIS2
Téma práce anglicky: Design of Measures and Processes in an Organization to Implement the Requirements of the EU directive NIS2

Zásady pro vypracování

- Provedte analýzu rizik zaměřenou na identifikaci kritických oblastí, které mohou být zranitelné vůči kybernetickým útokům. Zahrňte jak technické, tak organizační aspekty.
- Navrhněte vhodná technická a organizační opatření ke snížení úrovně rizik.
- Popište proces implementace navržených opatření v podniku. Zohledněte specifika podniku střední velikosti a zajistěte, aby byla opatření efektivně integrována do stávající infrastruktury.
- Navrhněte metody pro pravidelné monitorování a vyhodnocování účinnosti implementovaných opatření, s využitím různých nástrojů a technik.
- Vyhodnotte efektivitu navržených opatření.

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

Seznam doporučené literatury:

1. EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) [online], 2022. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555&from=CS>
2. POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY. Vládní návrh zákona o kybernetické bezpečnosti – EU, Sněmovní tisk 759/0 [online], 2024. Dostupné z: www.psp.cz/sqw/text/tiskt.sqw?0=9&CT=759&CT1=0
3. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Informace k novému zákonu [online], 2024. Dostupné z: <https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti>.

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **27. října 2024**

Termín odevzdání diplomové práce: **2. června 2025**



L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 17. listopadu 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne 28.5. 2025

.....
podpis autora

ABSTRAKT

Tato práce se zabývá návrhem implementace požadavků směrnice EU NIS2 do českého národního prostředí na základě nového zákona o kybernetické bezpečnosti. Jelikož se odhaduje, že pod regulaci na základě nového zákona bude nově spadat okolo 6 000 subjektů z řad podniků střední velikosti a někdy i menších, které se dosud touto problematikou nemusely zabývat, je předpoklad, že takovéto podniky mohou mít problémy s implementací požadavků nového zákona.

Proto je tato práce zaměřena na obecný případ poskytovatele služby splňujícího podmínky pro registraci regulované služby v režimu nižších povinností, tedy typicky podnik těsně přesahující počet 50 zaměstnanců a jehož druh poskytované služby vyjmenované zákonem pak společně v kombinaci s velikostí podniku zakládá důvod pro regulaci.

Klíčová slova: implementace zákona o kybernetické bezpečnosti, podnik střední velikosti

ABSTRACT

This thesis deals with the proposal for the implementation of the requirements of the EU NIS2 Directive into the Czech national environment based on the new Cybersecurity Act. Since it is estimated that around 6,000 medium-sized and sometimes smaller companies that have not had to deal with this issue before will be newly regulated under the new Act, it is assumed that such companies may have problems implementing the requirements of the new Act.

Therefore, this work focuses on the general case of a service provider meeting the conditions for registration of a regulated service under the lower obligations regime, i.e. typically a company with just over 50 employees and whose type of service provided as listed in the Act, together with the size of the company, establishes a reason for regulation.

Keywords: implementation of the Cybersecurity Act, medium-sized company

Na tomto místě bych chtěl poděkovat prof. Mgr. Romanu Jaškovi, Ph.D., DBA jakožto vedoucímu diplomové práce za ochotu, cenné rady a pomoc při psaní této práce.

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST.....	14
1 NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI, STAV SCHVALOVÁNÍ K DATU VYDÁNÍ TÉTO PRÁCE.....	15
1.1 STAV PROJEDNÁVÁNÍ NOVÉHO ZÁKONA V POSLANECKÉ SNĚMOVNĚ PČR.....	15
1.2 PROJEDNÁVÁNÍ NOVÉHO ZÁKONA V SENÁTU.....	17
1.3 ÚČINNOST NOVÉHO ZÁKONA.....	17
2 PODMÍNKY PRO REGISTRACI REGULOVANÉ SLUŽBY.....	18
3 POVINNOSTI A LHŮTY POSKYTOVATELE SLUŽBY SPLŇUJÍCÍ PODMÍNKY PRO REGISTRACI REGULOVANÉ SLUŽBY V REŽIMU NIŽŠÍCH POVINNOSTÍ.....	19
3.1 ZÁKLADNÍ LHŮTY SOUVISEJÍCÍ S REGISTRACÍ PODNIKU JAKO POSKYTOVATELE REGULOVANÉ SLUŽBY.....	19
4 PŘESTUPKY A POKUTY.....	21
4.1 PŘESTUPKY.....	21
4.2 POKUTY.....	22
5 BEZPEČNOSTNÍ OPATŘENÍ POSKYTOVATELE REGULOVANÉ SLUŽBY V REŽIMU NIŽŠÍCH POVINNOSTÍ.....	23
II PRAKTICKÁ ČÁST.....	33
6 ANALÝZA RIZIK NA ZÁKLADĚ INTERNÍHO AUDITU.....	34
6.1 ANALÝZA RIZIK FYZICKÉ BEZPEČNOSTI.....	35
6.1.1 Fyzická bezpečnost areálu podniku z hlediska přírodních událostí.....	35
6.1.2 Fyzická bezpečnost areálu podniku z hlediska vnější kriminality.....	36
6.1.3 Fyzická bezpečnost serverů, síťových prvků a uživatelských stanic.....	36
6.1.4 Fyzická bezpečnost tištěných dokumentů.....	37
6.2 ANALÝZA RIZIK Z HLEDISKA BEZPEČNOSTI PROVOZU A INCIDENT RESPONSE.....	37
6.3 ANALÝZA RIZIK Z HLEDISKA SÍŤOVÉ BEZPEČNOSTI.....	37
6.4 ANALÝZA RIZIK Z HLEDISKA BEZPEČNOSTI KONCOVÝCH ZAŘÍZENÍ.....	38
6.5 ANALÝZA RIZIK Z HLEDISKA BEZPEČNOSTI APLIKACÍ.....	38
6.6 ANALÝZA RIZIK Z HLEDISKA BEZPEČNOSTI UCHOVÁVANÝCH DAT.....	38
6.7 ANALÝZA RIZIK Z HLEDISKA KONTROLY IDENTIT A PŘÍSTUPOVÉ BEZPEČNOSTI.....	38
6.8 ANALÝZA RIZIK Z HLEDISKA BEZPEČNOSTI ZAMĚSTNANCŮ A JEJICH ŠKOLENÍ.....	38
7 ORGANIZAČNÍ OPATŘENÍ KE SNÍŽENÍ ÚROVNĚ RIZIK.....	39
7.1 ISMS.....	40
7.2 Klíčové prvky ISMS.....	40
7.3 Cíle ISMS A OBLASTI PŮSOBNOSTI.....	41
7.3.1 Cíle zavedení ISMS.....	41

7.3.2	Oblasti působnosti.....	42
7.4	ZODPOVĚDNOSTI A ROLE.....	42
7.4.1	Management.....	42
7.4.2	Bezpečnostní tým.....	43
7.4.3	Zaměstnanci.....	43
7.5	POLITIKY A POSTUPY.....	43
7.5.1	Politika přístupu k informacím.....	43
7.5.2	Ochrana dat.....	44
7.5.3	Správa identit a autentizace.....	44
7.6	ŘÍZENÍ RIZIK.....	44
7.6.1	Identifikace a hodnocení rizik.....	44
7.6.2	Opatření k minimalizaci rizik.....	45
7.7	ŘÍZENÍ INCIDENTŮ.....	45
7.7.1	Hlášení incidentů.....	45
7.7.2	Reakce na incidenty.....	46
7.8	KONTROLA A AUDITY.....	46
7.8.1	Pravidelné audity.....	46
7.8.2	Aktualizace směrnic.....	47
7.9	ŠKOLENÍ A POVĚDOMÍ O ISMS.....	47
7.9.1	Školení zaměstnanců.....	47
7.9.2	Kampaně pro zvyšování povědomí o bezpečnostních hrozbách.....	48
8	TECHNICKÁ OPATŘENÍ KE SNÍŽENÍ UROVNĚ RIZIK.....	49
8.1	FYZICKÁ BEZPEČNOST.....	49
8.2	BEZPEČNOST PROVOZU A INCIDENT RESPONSE.....	49
8.3	SÍŤOVÁ BEZPEČNOST.....	49
8.4	BEZPEČNOST KONCOVÝCH ZAŘÍZENÍ.....	49
8.5	BEZPEČNOST APLIKACÍ.....	50
8.6	BEZPEČNOST UCHOVÁVANÝCH DAT.....	50
8.7	KONTROLA IDENTIT A PŘÍSTUPOVÁ BEZPEČNOST.....	50
8.8	DALŠÍ JINDE NEUVEDENÁ TECHNICKÁ OPATŘENÍ.....	50
8.8.1	Segmentace sítě.....	50
8.8.2	Základní nastavení routerů a switchů.....	51
9	NÁVRH IMPLEMENTACE OPATŘENÍ V PODNIKU.....	52
9.1	ANALÝZA SOUČASNÉHO STAVU.....	52
9.2	NÁVRH OPATŘENÍ.....	52
9.3	PŘÍPRAVA INTERNÍ DOKUMENTACE A ŠKOLENÍ.....	52
9.4	TECHNICKÁ IMPLEMENTACE.....	53
9.5	KONTROLA A KONTINUÁLNÍ ZLEPŠOVÁNÍ.....	53
10	NÁVRH METOD PRO PRAVIDELNÉ MONITOROVÁNÍ	

A VYHODNOCOVÁNÍ ÚČINNOSTI ZAVÁDĚNÝCH OPATŘENÍ.....	54
10.1 AUTOMATIZOVANÝ MONITORING A ANALÝZA DAT.....	54
10.2 AUDITNÍ A KONTROLNÍ PROCESY.....	54
10.3 ANALÝZA A REPORTING BEZPEČNOSTNÍCH INCIDENTŮ.....	55
10.4 ZPĚTNÁ VAZBA A VZDĚLÁVÁNÍ ZAMĚSTNANCŮ.....	55
10.5 METODY ANALÝZY RIZIK A JEJICH VYHODNOCOVÁNÍ.....	55
11 NÁVRH METOD PRO VYHODNOCOVÁNÍ EFEKTIVITY ZAVÁDĚNÝCH OPATŘENÍ.....	57
11.1 STANOVENÍ METRIK EFEKTIVITY.....	57
11.2 TESTOVÁNÍ A SIMULACE HROZEB.....	57
11.3 SBĚR DAT A ANALÝZA.....	57
11.4 INTERNÍ A EXTERNÍ AUDITY.....	58
11.5 KONTINUÁLNÍ ZLEPŠOVÁNÍ.....	58
ZÁVĚR.....	59
SEZNAM POUŽITÉ LITERATURY.....	61
SEZNAM TABULEK.....	63
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	64
SEZNAM PŘÍLOH.....	65

ÚVOD

Tato práce je zaměřena na poskytovatele služby splňujícího podmínky pro registraci regulované služby v režimu nižších povinností, podnik těsně přesahující počet 50 zaměstnanců nebo jinak řečeno dle doporučení Komise 2003/361/ES [1] tzv. roční pracovní jednotky (RPJ), tzn. jedná se dle tohoto doporučení z hlediska velikosti o tzv. podnik střední velikosti a jehož druh poskytované služby vyjmenované zákonem pak společně v kombinaci s velikostí podniku zakládá důvod pro regulaci.

Zároveň ale takový podnik z titulu své malé velikosti není nijak zvlášť ekonomicky silným subjektem a zároveň z hlediska kybernetické bezpečnosti nebyl dosud nijak regulován. Tzn. tato situace je pro podnik nová a nepředpokládá se, že by dosud měl finanční a personální kapacity se tímto problémem zabývat. Režim nižších povinností je sice mírnější varianta regulace, ale zároveň pro podnik, který nově spadá pod regulaci, může znamenat vysoké finanční náklady se zavedením nových povinných opatření nákupem potřebných technologií, nebo personálně potřebou kvalifikovaných odborníků vlastních, nebo externě najímaných a / nebo dalšími souvisejícími náklady. Cílem práce je zanalyzovat situaci ve středním podniku před implementací zákona o kyberbezpečnosti a dle výchozího stavu navrhnout organizační a technická opatření nutná pro implementaci zákona o kyberbezpečnosti v podniku.

Pro účely této práce tedy budeme uvažovat fiktivní výrobní podnik těsně překračující hranici 50 zaměstnanců, zaměřením své produkce zatím spadající do režimu nižších povinností, předtím pod žádnou kyberbezpečnostní regulaci nespadal a na tomto poli je nováčkem. Podnik ovšem plánuje získat certifikáty pro možnost dodávek spadajících pod státní ověřování jakosti, čímž by v horizontu několika let mohl začít spadat do režimu vyšších povinností. Pro možnost zahrnutí opatření fyzické bezpečnosti v této práci můžeme uvažovat, že z hlediska své polohy se nachází v nížině, v záplavové oblasti, obecně tedy například v oblasti střední Moravy, která byla zasažena ničivými povodněmi v r. 1997.

I TEORETICKÁ ČÁST

1 NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI, STAV SCHVALOVÁNÍ K DATU VYDÁNÍ TÉTO PRÁCE

Návrh zákona o kybernetické bezpečnosti a prováděcích vyhlášek pro implementaci směrnice EU NIS2 do českého národního prostředí spadá do kompetence Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). NIS2 přináší tolik podstatných změn stávajícího regulatorního rámce, že se NÚKIB rozhodl přistoupit k návrhu zcela nového zákona o kybernetické bezpečnosti a jeho vyhlášek.

Návrh nového zákona vychází jak ze znění předešlého zákona č. 181/2014 Sb. O kybernetické bezpečnosti, tak plní minimální požadavky dané evropskou bezpečností směrnicí NIS2. Změny dané směrnicí NIS2 tedy zavádí do českého právního řádu. Navíc reflektuje zkušenosti a poznatky, které NÚKIB za dobu své existence shromáždil.

Hlavním účelem této regulace je nastavení alespoň základní úrovně zabezpečení v organizacích, které poskytují své služby v ekonomicky, společensky či bezpečnostně významných odvětvích a splňují další kritéria významnosti. Rozsah regulovaných odvětví a konkrétních regulovaných služeb v těchto odvětvích byl směrnicí rozšířen, nový zákon se tedy bude vztahovat na výrazně širší množinu organizací. [3]

1.1 Stav projednávání nového zákona v Poslanecké sněmovně PČR

Přestože zákon zatím (ke konci května 2025) ještě není schválen v konečné podobě, je jeho návrh ve stavu, v jakém byl 13.5. 2025 postoupen do Senátu v současnosti nejdůležitějším směrodatným podkladem pro tuto práci.

25.4. 2025 byl Sněmovnou PČR ve 3. čtení schválen návrh zákona o kybernetické bezpečnosti.

3. čtení bylo nakonec naplánováno až na pořad 136. schůze PS PČR. Na webu PČR jsou záznamy ze schůze, ze kterých bylo možno sledovat schválené pozměňovací návrhy a také návrhy, které Sněmovnou schváleny nebyly.

Ve zkratce to výstižně popsal např. portál *Lupa.cz*: „Návrh prošel Sněmovnou ve znění, jaké prosazoval garanční výbor pro bezpečnost. (sněmovní tisk č. 759/10 [2]) Pravomoc rozhodovat o případném zákazu dodavatelů se přesunula z NÚKIBu na vládu. Oproti původnímu návrhu se také v zákoně omezila pravomoc vlády přijímat toto opatření jen

u kritických aktiv, s tím ale, že tuto pravomoc si může vláda kdykoliv svým nařízením sama rozšířit. Variantní pozměňovací návrhy poslankyně SPD Vladimíry Lesenské na teritoriální omezení úložišť pro uchování osobních dat zpracovávaných státem Sněmovna nepodpořila. Návrh kyberbezpečnostního zákona spolu s doprovodným změnovým zákonem teď bude posuzovat Senát. Jejich účinnost dolní komora už nyní posunula, namísto pevného data účinnosti od 1.7. 2025 nastavila aplikaci nových pravidel na začátek třetího kalendářního měsíce po jeho vyhlášení.“ [4]

Výčet pozměňovacích návrhů a jejich úspěšnost:

1. PN A17 – A26 - schválen,
2. PN A1 – A16 - schválen,
3. PN B9 - schválen,
4. PN B18 a B19 - neschválen,
5. PN B20 a B21 - stažen z projednávání,
6. PN C1 - neschválen,
7. PN C2 - neschválen,
8. Návrh zákona jako celek - schválen;

Podrobnější popis pozměňovacích návrhů je dostupný ve sněmovním tisku č. 759/9 [2]. Výše uvedené pozměňovací návrhy nemění znění zákona nijak výrazně až na změny popsané v článku portálu *Lupa.cz*. Z hlediska kybernetické bezpečnosti by bylo možno považovat za vhodné pozměňovací návrhy poslankyně Lesenské, která navrhovala opatření pro omezení ukládání osobních údajů občanů ČR spravované státem a veřejnoprávními subjekty na datových úložištích fyzicky umístěných v ČR, zákaz ukládání, nebo přenosu osobních údajů občanů ČR mimo území ČR a další podobná opatření. Z hlediska národní bezpečnosti se tato opatření jeví jako logická a oprávněná, ale návrh nebyl Sněmovnou podpořen.

Fyzická bezpečnost dat je prvním a základním kamenem jakékoli bezpečnosti kybernetické a jestliže budou data státu ukládána mimo území státu, je následné zajištění kybernetické bezpečnosti problémem, pokud firmy uchovávající tato data nebudou spadat pod českou jurisdikci, nebo alespoň pod jurisdikci EU.

1.2 Projednávání nového zákona v Senátu

V Poslanecké sněmovně byl zákon schválen a postoupen Senátu k dalšímu projednávání:

Poslanecká sněmovna postoupila dne 13.5. 2025 návrh zákona Senátu jako tisk 109, dokument 109/0.

Organizační výbor dne 13.5. 2025 stanovil garančním výborem Výbor pro zahraniční věci, obranu a bezpečnost a přikázal tisk k projednání: Výbor pro hospodářství, zemědělství a dopravu, Ústavně-právní výbor.

Projednávání tisku bylo zařazeno na pořad 11. schůze Senátu (od 11. 6. 2025) jako bod č. 1. [5]

V době psaní této práce je tedy nový zákon připraven k projednání v Senátu v podobě schválené poslanci se změnami, jak je uvedeno v textu výše. Změny se týkají znění samotného zákona v některých částech a týkají se v podstatě pouze změn v pravomocích k některým úkonům na úrovni mezi NÚKIB a vládou. Z tohoto hlediska tedy nemají vliv na implementaci v podnicích. Prováděcí právní předpisy k novému zákonu o kybernetické bezpečnosti byly 16.5. 2025 NÚKIBem odeslány do mezirezortního připomínkového řízení [6]. Zatím lze předpokládat, že do této ryze odborné části Senát nezasáhne, ale není známo, jaké výsledky vzejdou z meziresortního připomínkování.

Jelikož aktuálnější podklady zatím nejsou k dispozici, je v tuto chvíli nutno se Senátním tiskem č. 109 [7] a s vyhláškami předanými k meziresortnímu připomínkování pracovat jako s dostatečně vhodnými kandidáty na finální znění zákona.

1.3 Účinnost nového zákona

V současné podobě znění návrhu zákona je účinnost nového zákona nastavena v § 73:

Tento zákon nabývá účinnosti prvním dnem třetího kalendářního měsíce následujícího po jeho vyhlášení. [7]

2 PODMÍNKY PRO REGISTRACI REGULOVANÉ SLUŽBY

Dle předpokladů uvedených v anotaci, pro potřeby této práce budeme nadále uvažovat výrobní podnik, který má tyto výchozí parametry:

- Podnik dle klasifikace CZ-NACE spadá do odílu 30 - Výroba ostatních dopravních prostředků a zařízení,
- podnik má 50 a více zaměstnanců (RPJ) během 2 po sobě jdoucích účetních období dle doporučení Komise 2003/361/ES [1], z tohoto důvodu se bude jednat o podnik střední velikosti.

Podmínky pro registraci regulované služby nastávají za následujících okolností, vyjmenovány jsou zde jen ty, které se týkají v této práci uvažovaného podniku:

- *§ 4 odst. 1a zákona - jde o službu, která je významná pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v České republice v některém z vyjmenovaných odvětví,*
- Ve znění zákona se v tomto případě jedná o *§ 4 odst. 1A, bod 3) zákona - výrobní průmysl*, v samotné vyhlášce, která je součástí zákona se pak jedná o *§ 3 Rozdělení poskytovatelů podle poskytovaných regulovaných služeb do režimů podle § 8 odst. 1 zákona – oddíl přílohy k vyhlášce č. 7.5 Výroba ostatních dopravních prostředků a zařízení ve smyslu oddílu 30 klasifikace CZ-NACE*. O tomto případě vyhláška říká: *výrobce ostatních dopravních prostředků a zařízení ve smyslu oddílu 30 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.*

3 POVINNOSTI A LHŮTY POSKYTOVATELE SLUŽBY SPLŇUJÍCÍ PODMÍNKY PRO REGISTRACI REGULOVANÉ SLUŽBY V REŽIMU NIŽŠÍCH POVINNOSTÍ

Lze předpokládat, že nový zákon o kybernetické bezpečnosti vstoupí v účinnost v průběhu roku 2025, nebo začátkem roku 2026. Od data vstoupení zákona v účinnost budou mít poskytovatelé služeb, na které bude zákon nově pohlížet jako na poskytovatele regulované služby různé lhůty na splnění podmínek se zákonem souvisejících. Dodržování těchto lhůt je zásadním prvkem implementace nového zákona a je třeba je mít v podniku pod kontrolou.

3.1 Základní lhůty související s registrací podniku jako poskytovatele regulované služby

Mezi povinnosti se zákonem danou lhůtou patří:

- § 6 odst. 1 - *Poskytovatel služby splňující podmínky pro registraci regulované služby podle § 4 odst. 1 je pro účely vydání rozhodnutí o registraci regulované služby povinen ohlásit tuto službu Úřadu (NÚKIB) nejpozději do 60 dnů ode dne, kdy ke splnění podmínek došlo (v zákoně je tento krok označen též jako samoidentifikace),*
- § 6 odst. 2 - *Úřad (NÚKIB) rozhodne o registraci regulované služby v případě, že jsou splněny podmínky pro registraci regulované služby podle § 4 odst. 1 nebo § 5,*
- § 9 odst. 1 - *Poskytovatel regulované služby je povinen hlásit Úřadu (NÚKIB) změny regulované služby, které mohou vést ke změně režimu jejího poskytovatele, nejpozději do 60 dnů ode dne, kdy ke změně regulované služby došlo,*
- § 11 odst. 1 - *Poskytovatel regulované služby nejpozději do 30 dnů ode dne doručení rozhodnutí o registraci regulované služby hlásí*
 - a. *kontaktní údaje, kterými se rozumí identifikační údaje fyzických osob, které jsou oprávněny jednat za poskytovatele regulované služby ve věcech upravených tímto zákonem, a*
 - b. *doplňující údaje, kterými se rozumí informace o vlastnické struktuře poskytovatele regulované služby, technické údaje týkající se regulované služby a informace o jejím geografickém rozšíření a přeshraničním poskytování,*

- *§ 13 odst. 4 - Poskytovatel regulované služby začne plnit povinnost zavádět a provádět bezpečnostní opatření podle § 13 odst. 2 pro každou regulovanou službu nejpozději do 1 roku ode dne doručení rozhodnutí o registraci regulované služby,*
- *§ 15 odst. 4 - Poskytovatel regulované služby začne plnit povinnost hlásit kybernetické bezpečnostní incidenty podle § 15 odst. 1 a 2 pro každou regulovanou službu nejpozději do 1 roku ode dne doručení rozhodnutí o registraci regulované služby. [7]*

4 PŘESTUPKY A POKUTY

Dalším podstatným prvkem implementace nového zákona je, aby podnik byl dobře informován o sankcích, které mohou plynout z případných nesplnění zákonných požadavků. Zákonem jsou definovány přestupky a následné sankce ve formě pokut.

4.1 Přestupky

Poskytovatel regulované služby v režimu nižších povinností se dopustí přestupku tím, že

- a. neohlásí změnu regulované služby podle § 9 odst. 1,*
- b. neohlásí kontaktní nebo doplňující údaje nebo jejich změnu podle § 11,*
- c. neurčí za účelem vymezení stanoveného rozsahu všechna primární aktiva podle § 12 odst. 2 písm. a) nebo podpůrná aktiva podle § 12 odst. 2 písm. c), nebo jejich určení pravidelně nepřezkoumá nebo neaktualizuje podle § 12 odst. 5,*
- d. neposoudí za účelem vymezení stanoveného rozsahu, zda primární aktiva určená podle § 12 odst. 2 písm. a) souvisí s poskytováním regulované služby, nebo toto posouzení pravidelně nepřezkoumá nebo neaktualizuje podle § 12 odst. 5,*
- e. neeviduje aktiva podle § 12 odst. 3,*
- f. nezavede nebo neprovede bezpečnostní opatření podle § 13 odst. 2 nebo § 18 odst. 1,*
- g. nevybírá svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření nebo nezahrnuje požadavky vyplývající z bezpečnostního opatření do smlouvy s dodavatelem v rozporu s § 13 odst. 5,*
- h. nepředloží prvotní hlášení o incidentu podle § 16 odst. 1 nebo nedoplní některý z údajů o incidentu podle § 16 odst. 3 nebo nenahlásí kybernetický bezpečnostní incident podle § 18 odst. 2,*
- i. neposkytne informace nebo součinnost při zvládnutí incidentu podle § 17 odst. 3,*
- j. nesplní povinnost nebo zákaz informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem stanovený rozhodnutím podle § 19 odst. 1,*
- k. neinformuje uživatele regulované služby o významné hrozbě nebo krocích, které může uživatel služby učinit v reakci na ni, podle § 19 odst. 2,*

- l. nesplní povinnost uloženou rozhodnutím o výstraze podle § 21 odst. 1,*
- m. nesplní reaktivní protiopatření uložené podle § 23 odst. 1 nebo § 23 odst. 4,*
- n. neoznámí provedení reaktivního protiopatření nebo jeho výsledek podle § 23 odst. 6, nebo*
- o. nesplní povinnost uloženou nápravným opatřením podle § 56 odst. 1. [7]*

4.2 Pokuty

Za výše uvedené přestupky lze uložit pokutu do:

- a. 250 000 000 Kč nebo až do výše 2 % čistého celosvětového ročního obratu dosaženého podnikem podle čl. 101 a 102 Smlouvy o fungování Evropské unie, jehož je obviněný součástí, za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 1 písm. a), c) až m) a o), nebo odstavce 3 písm. a), b), f) nebo g),*
- b. 175 000 000 Kč nebo až do výše 1,4 % čistého celosvětového ročního obratu dosaženého podnikem podle čl. 101 a 102 Smlouvy o fungování Evropské unie, jehož je obviněný součástí, za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 2 písm. a), c) až m) nebo o),*
- c. 100 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. b) nebo odstavce 3 písm. c), d) nebo h),*
- d. 50 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. n), odstavce 2 písm. b), nebo odstavce 3 písm. e), nebo*
- e. 35 000 000 Kč, jde-li o přestupek podle odstavce 2 písm. n). [7]*

5 BEZPEČNOSTNÍ OPATŘENÍ POSKYTOVATELE REGULOVANÉ SLUŽBY V REŽIMU NIŽŠÍCH POVINNOSTÍ

Pro podniky střední velikosti a v některých případech i pro menší podniky, které budou podle nového zákona nyní spadat do regulace, může být tato nová situace organizačně i finančně značně nepříznivou. Pro začátek je tedy jistě vhodné identifikovat minimální množinu opatření tak, aby byly všechny minimální zákonné podmínky splněny a aby těmito opatřeními nebyla vážně narušena činnost podniku. Tedy začít se zákonným minimem a postupně dle potřeb podniku další opatření přidávat, pokud budou nezbytná. *Závěrečná zpráva z hodnocení dopadů regulace (RIA)* [2] uvádí: „*odhady počtu povinných osob v důsledku změny jejich identifikace v návaznosti na obsah směrnice hovoří o minimálním počtu 6 000 povinných osob podle návrhu zákona, zaváděná kritéria rozdělení těchto povinných osob do režimů pak vedou k odhadům v poměru cca 1:5, tj. 1 000 poskytovatelů regulované služby v režimu vyšších povinností a 5 000 poskytovatelů regulované služby v režimu nižších povinností*“. Je tedy možné, že do regulace v režimu vyšších povinností může v některých případech spadat podnik střední velikosti a nebo i mikropodnik, pokud by těžiště jejich poskytovaných služeb zakládalo důvod k regulaci. Pro úplný začátek implementace zákona v podniku, který dosud neměl žádnou zkušenost s regulací kybernetické bezpečnosti je ovšem vhodné předpokládat, že podniky střední velikosti a menší budou spadat do regulace v režimu nižších povinností. Návrh zákona uděluje roční lhůtu ode dne doručení rozhodnutí o registraci regulované služby na implementaci požadavků a plnění dalších povinností a je jistě výhodné mít připravenou základní sadu opatření, které je možno nasadit téměř okamžitě. Vhodným zdrojem informací jak tento stav zajistit jsou mimo samotného zákona i jeho prováděcí vyhlášky, pro tento případ konkrétně *Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*. [2]

Jelikož ještě zákon není finálně schválen, vyhláška zatím nemá konečnou podobu a ani své číslo, ale lze předpokládat, že pokud zákon prošel 3. čtením, velké změny v technické části zřejmě nebudou a pokud by byly, budou dokumentované vyznačením změn. Požadavky vyhlášky lze rozdělit na:

- organizační opatření, která nepředstavují žádnou nebo jen malou finanční zátěž
- technická opatření, která mohou vyžadovat i značné finanční investice

Souhrn minimálních požadavků lze z této vyhlášky citovat výběrem paragrafů a jejich odstavců takto:

„§ 4 Systém zajišťování minimální kybernetické bezpečnosti

(1) Povinná osoba v rámci zajišťování kybernetické bezpečnosti

2) vždy zavede a provádí alespoň bezpečnostní opatření podle § 4 odstavce 2 až odstavce 7, § 5, § 6 a § 11.“ (tyto odstavce a paragrafy vyhlášky následují níže za tímto odstavcem)

„(2) Povinná osoba

a) zpracuje přehled bezpečnostních opatření požadovaných touto vyhláškou podle přílohy č. 1, který obsahuje alespoň

1. přehled všech bezpečnostních opatření, která byla povinnou osobou zavedena, včetně popisu jejich zavedení,

2. přehled všech bezpečnostních opatření, která budou povinnou osobou zavedena, včetně termínů pro jejich zavedení, priority jejich zavedení, určení osoby odpovědné za jejich zavedení a

3. přehled všech bezpečnostních opatření, která nebyla zavedena, včetně odůvodnění jejich nezavedení,

b) alespoň jednou ročně provede a dokumentuje vyhodnocení účinnosti zavedených bezpečnostních opatření, včetně aktualizace přehledu bezpečnostních opatření,

c) uchovává jednotlivé přehledy bezpečnostních opatření, alespoň po dobu 4 let.

(3) Povinná osoba určí osobu odpovědnou za kybernetickou bezpečnost, která v oblasti kybernetické bezpečnosti odpovídá za řízení a rozvoj kybernetické bezpečnosti, dohled nad stavem kybernetické bezpečnosti a komunikaci s vrcholným vedením, přičemž pověřena může být osoba, která pro tuto činnost

a) bez zbytečného odkladu absolvuje odborné školení podle § 6 písm. g)“ (viz § 6 vyhlášky v textu níže) „nebo

b) prokáže odbornou způsobilost v oblasti kybernetické bezpečnosti.

(4) Povinná osoba v rámci zajišťování kybernetické bezpečnosti řídí bezpečnostní politiku a bezpečnostní dokumentaci, zejména

a) vytvoří a schválí relevantní bezpečnostní politiku a vede relevantní bezpečnostní dokumentaci k opatřením uvedeným v § 4 až 14.“ (§ 4, § 5, § 6 a § 11 jsou součástí tohoto textu citace z vyhlášky, další paragrafy obsahují témata:

- § 7 Řízení kontinuity činností
- § 8 Řízení přístupu
- § 9 Řízení identit a jejich oprávnění
- § 10 Detekce a zaznamenávání kybernetických bezpečnostních událostí
- § 12 Bezpečnost komunikačních sítí
- § 13 Aplikační bezpečnost
- § 14 Kryptografické algoritmy)

Je nutno říci, že obecná formulace „...vytvoří a schválí relevantní bezpečnostní politiku a vede relevantní bezpečnostní dokumentaci k opatřením uvedeným v §...“ tedy v dalších celých 7 paragrafech, není příliš užitečným a konkrétním návodem jak postupovat. Bude proto potřeba se na tomto místě zastavit a rozebrat si § 7 až § 14 podrobněji, ale vzhledem k rozsáhlosti uvedených paragrafů a s ohledem na minimalizaci nejdůležitějších činností, pokud možno stručně s tím, že znění jednotlivých paragrafů zde nebude uváděno celé, ale jen v důležitých bodech.

§ 7 Řízení kontinuity činností - z hlediska požadavku § 4 odst. 4 a) je paragrafem požadujícím organizační opatření, které nepředstavuje velkou finanční zátěž a je možno požadované odpovědnosti a povinnosti stanovit poměrně libovolně adekvátně potřebám podniku rozhodnutím kompetentních osob vrcholného vedení podniku za spolupráce IT oddělení, do jehož kompetence spadá technická realizace vydaného rozhodnutí. Nejdůležitějším konkrétním požadavkem § 7 je výňatek z bodu:

„c) ...vytváří pravidelné zálohy informací, dat, konfigurací a nastavení technických aktiv...“

K tomuto bodu ovšem není nutno z hlediska požadavku § 4 odst. 4 a) jen „vytvořit a schválit relevantní bezpečnostní politiku“, ale stejně jako ostatní organizační požadavky § 7 je zřejmě možno ho realizovat již s dostupnými prostředky podniku.

§ 8 Řízení přístupu – opět se jedná o organizační opatření. Řízení přístupu k IT prostředkům, nebo obecně k podnikovým aktivům je v současnosti již běžným standardem. Z tohoto hlediska asi nejvíce vypovídajícím bodem, čím se paragraf zabývá, je bod:

„(1) Povinná osoba řídí přístup k aktivům, v rámci řízení přístupu

a) přidělí každému uživateli a administrátorovi přístupujícímu k aktivům přístupová práva a oprávnění na úroveň nezbytně nutnou k výkonu práce, a jedinečný identifikátor daného typu účtu, přičemž odděluje uživatelské a administrátorské účty jedné osoby, ...“

tento stav lze při řízení ICT v podnicích dnes považovat za standardní a ani ostatní body není nutno nějak speciálně vysvětlovat. Blíže k technickým opatřením má ještě bod:

„(2) Povinná osoba v rámci fyzické bezpečnosti zamezí neoprávněnému přístupu ke svým aktivům a předchází poškození, krádeži, neoprávněným zásahům, zneužití aktiv a přerušení poskytování regulované služby.“

Podniky mají jistě zájem na zabezpečení svého majetku před krádežemi a poškozením a již z hlediska případných smluv s pojišťovnami musí mít své prostory zabezpečeny na dostatečné úrovni a taktéž § 8 lze asi rovnou zrealizovat, nebo ho vést jako splněn.

§ 9 Řízení identit a jejich oprávnění – tento paragraf je také veskrze o organizačních opatřeních, ale již o něco více zahrnuje i nutnost nějaké technické implementace těchto opatření. Některé odstavce a body uvádějí dnes již standardní záležitosti, které není třeba zvlášť zmiňovat, ale některé požadavky mohou z hlediska dnešní praxe ve středních a menších podnicích být problémem. Z hlediska požadavku § 4 odst. 4 a) *„(Povinná osoba)...vytvoří a schválí relevantní bezpečnostní politiku a vede relevantní bezpečnostní dokumentaci k opatřením uvedeným v § 4 až 14.“* by proto bylo vhodné jednodušší požadavky přímo implementovat, nebo jen zaevidovat jako splněné a ty složitější v dokumentaci (*Příloha č. 1 vyhlášky Přehled bezpečnostních opatření*) uvést jako výhledově plánované s hodnotou *nezavedeno* a s případným uvedením termínu zavedení v budoucnu. Z požadavků § 9 je zde tedy nutno zmínit ty náročnější, které je třeba vést v patrnosti a mohly by představovat vysoké finanční náklady na pořizování nových technologií, tedy:

„(2) Povinná osoba pro ověření identity administrátorů a uživatelů využívá autentizační mechanismus, který je založený na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů.“

Tento požadavek je sice např. na městských úřadech dnes již vcelku běžným jevem, určitě je běžným např. v elektronickém bankovníctví pro zabezpečení přístupů na účet, ale v podnicích od střední velikosti níže je asi jevem vzácným. Při představě, že by se při požadavku „§ 9

(1) Povinná osoba pro řízení identit, přístupových práv a oprávnění používá nástroj, který zajišťuje...

... b) opětovné ověření identity po stanovené době nečinnosti“

a při znalosti reakcí úředníků např. městských úřadů na toto obtěžující chování systému a při představě, že by se tak mělo dít po každém automatickém odhlášení ze systému, které je nastaveno třeba na 5 min. nečinnosti, je těžko si představit reakce např. dílenského mistra ve výrobě. V dnešní době i ty nejnižší THP pozice, nikterak příliš vzdálené od dělnických, musí mít přístup do podnikového systému a pracovat s ním efektivně.

Požadavek § 9 odst. (2) je sice zatím možno odložit využitím odstavců:

„(3) Povinná osoba do doby využívání autentizačního mechanismu založeného na vícefaktorové autentizaci podle odstavce 2, využívá autentizaci pomocí kryptografických klíčů nebo certifikátů.

(4) Povinná osoba do doby využívání autentizačního mechanismu pomocí kryptografických klíčů nebo certifikátů podle odstavce 3, využívá nástroj založený na autentizaci pomocí identifikátoru účtu a hesla a stanoví pravidla, která vynucují

a) délky hesla alespoň“

1. 12 znaků pro účty uživatelů,

2. 17 znaků pro účty administrátorů,

3. 22 znaků pro účty technických aktiv, ...“

ale požadavek na „vícefaktorovou autentizaci s nejméně dvěma různými typy faktorů“ je zatím dán vyhláškou a za současné situace je tedy jen otázkou času nutnosti jeho zavedení. Na druhou stranu ovšem lze tento požadavek zatím fakticky odložit „na neurčito“, což je pro podnik, který je v začátcích zavádění kybernetické bezpečnosti jakási dočasná úleva.

Z § 9 lze tedy v začátku implementovat jen požadavky dle ostatních méně náročných odstavců paragrafu, *odst. (2)* zatím jen uvést v seznamu dle *Příloha č. 1* jako nezaveden a nahradit ho použitím *odst. (4)*.

§ 10 Detekce a zaznamenávání kybernetických bezpečnostních událostí – požadavky § 10 jsou ryze technického rázu, ale většina z nich je v dnešní době praktikována standardně jako součást běžné správy ICT a hlavními nástroji zajišťujícími tyto požadavky mohou být firewally a antivirové software. Jediným odstavcem, který vyžaduje nasazení něčeho jiného, než běžně používaného software je:

„(2) Povinná osoba zaznamenává bezpečnostní a relevantní provozní události v souladu s odstavcem 1 a u těchto událostí zaznamenává zejména následující

- a) datum a čas včetně specifikace časového pásma,*
- b) typ činnosti,*
- c) jednoznačnou identifikaci technického aktiva a identifikaci účtu původce a*
- d) úspěšnost nebo neúspěšnost činnosti.“*

pro splnění tohoto požadavku je možno nasadit nějaký IDPS a SIEM software, pokud v podniku dosud nasazen nebyl, pak to vyžaduje vyčlenění finančních prostředků na nákup a implementaci systému a potřebné nastavení. Pokud by se jednalo o problém, bylo by zřejmě možno pro začátek opět zařadit nasazení IDPS a SIEM do výhledu plánovaných opatření v seznamu *Příloha č. 1 vyhlášky Přehled bezpečnostních opatření*.

§ 12 Bezpečnost komunikačních sítí – tento paragraf je taktéž převážně technického rázu a mimo některá organizační, nebo snáze zjistitelná opatření obsahuje jeden zásadní požadavek na návrh architektury podnikové sítě:

„Povinná osoba pro ochranu bezpečnosti komunikační sítě, a to zejména jejího síťového perimetru

a) zajistí segmentaci komunikační sítě, včetně oddělení provozního a zálohovacího prostředí,...“

Pokud podnik dosud používal nějakou formu „ploché“ sítě, tak tento požadavek na segmentaci může znamenat nutnost její kompletní rekonstrukce. Servery a další velké hardware bude možno zřejmě ponechat na svých místech, ale bude nutno zcela nově navrhnout propojení všech prvků v síti. S tím bude souviset také nákup menšího síťového hardware, např. nových switchů a routerů a takto komplexní zásah je potřeba si dobře rozmyslet a naplánovat. Střední a menší podniky tuto rekonstrukci pravděpodobně svěří odborné firmě jako kompletní dodávku. Od toho se také bude odvíjet cena zakázky

a závislost podniku na dodavatelské firmě. Toto se zatím jeví jako jeden z finančně nejnáročnějších zásahů na implementaci nového zákona a bylo by zřejmě opět vhodné zařadit požadavek na segmentaci sítě do výhledu plánovaných opatření v seznamu *Příloha č. 1 vyhlášky Přehled bezpečnostních opatření*.

§ 13 Aplikační bezpečnost – tento paragraf je taktéž převážně technického rázu a jeho implementace také může přinést vysoké finanční náklady. Ty souvisí především s odstavcem:

„Povinná osoba v rámci zajištění aplikační bezpečnosti regulované služby

... b) u technických aktiv, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována

1. vede jejich evidenci,

2. zavede bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti a

3. omezí jejich komunikaci v komunikační síti na nezbytně nutnou,“

V mnohých středních a menších podnicích je možno se setkat nejen např. ještě s MS Windows 8 na uživatelských stanicích, ale např. i s MS Windows Server 2012. Znění *§ 13 odst. b) 3.* by v podstatě znamenalo nemožnost jejich použití pro trvalý provoz a nutnost nákupu nového software. Ve větších počtech licencí to znamená nejen velké finanční náklady, ale i vyšší implementační pracnost. Opět by zřejmě bylo vhodné zařadit tento požadavek do výhledu plánovaných opatření v seznamu *Příloha č. 1 vyhlášky Přehled bezpečnostních opatření*.

§ 14 Kryptografické algoritmy – vzhledem k tomu, že mj. ČVUT v Praze se již začátkem r. 2024 připojila k síti IBM Quantum a v superpočítačovém centru IT4Innovations VŠB - TU Ostrava již od jara 2025 probíhaly práce na přípravě provozu prvního kvantového počítače v ČR, stávají se kvantové počítače i v ČR realitou. O to více může být v dnešní denní praxi středních a menších podniků problematickým odstavcem:

„(2) Povinná osoba zajišťuje bezpečnou

a) hlasovou, audiovizuální a textovou komunikaci, a to včetně e-mailové komunikace, a

b) nouzovou komunikaci v rámci organizace.“

Menší a střední podniky, z nichž se mnohé kryptografií dosud příliš nezabývaly, vkročí přímo do doby, kdy budou muset alespoň začít uvažovat o tom, že existuje i nějaká kryptografie postkvantová. V roce 2024 byly v USA institutem NIST vydány standardy FIPS (Federal Information Processing Standards) a tyto budou v USA pro vládní účely od roku 2030 povinné. Standardy NIST pravděpodobně přijme posléze i EU.

Na úrovni dosud běžné kryptografie se dá říci, že e-mailová komunikace zřejmě bude šifrovaná standardně pomocí TLS, pokud podnik používá pro interní telefonickou komunikaci služeb mobilních operátorů, pak by bylo pod toto možno zahrnout i požadované položky komunikace *hlasová, audiovizuální, textová i nouzová*.

Nyní po výčtu činností souvisejících s dokumentací k opatřením v § 4 až 14 se tedy opět můžeme vrátit k pokračování citace vyhlášky § 4:

„(4) Povinná osoba v rámci zajišťování kybernetické bezpečnosti řídí bezpečnostní politiku a bezpečnostní dokumentaci, zejména...

...b) pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci a zajišťuje jejich aktuálnost.

c) Povinná osoba dodržuje a vynucuje dodržování pravidel a postupů stanovených v bezpečnostní politice a bezpečnostní dokumentaci podle odst. 4 písm. a).

(5) Povinná osoba v návaznosti na stanovení rozsahu řízení kybernetické bezpečnosti podle § 13 zákona, dále v rámci řízení aktiv stanoví a zavádí pravidla ochrany a přípustné způsoby používání aktiv.

(6) Povinná osoba při uzavírání smlouvy s dodavatelem zajistí, aby smlouvy s těmito dodavateli obsahovaly relevantní oblasti uvedené v příloze č. 2 k této vyhlášce.

(7) Povinná osoba v souvislosti s plánovanou akvizicí, vývojem a údržbou technických aktiv stanoví bezpečnostní požadavky v oblasti kybernetické bezpečnosti a vymáhá jejich dodržování, přičemž vychází zejména z požadavků na bezpečnostní opatření podle této vyhlášky.

§ 5 Požadavky na vrcholné vedení

- a) je prokazatelně poučeno o jeho povinnostech a rozsahu odpovědností,
- b) prokazatelně absolvuje školení podle § 6 písm. c),
- c) zajistí dostupnost zdrojů potřebných pro zajišťování kybernetické bezpečnosti v souladu s přehledem bezpečnostních opatření a
- d) se prokazatelně seznamuje se stavem plnění bezpečnostních opatření podle přehledu bezpečnostních opatření podle § 4 odst. 2 písm. a).

§ 6 Bezpečnost lidských zdrojů

Povinná osoba v rámci bezpečnosti lidských zdrojů

- a) stanoví politiku bezpečného chování uživatelů, v rámci které zohledňuje relevantní témata uvedená v příloze č. 3 této vyhlášky, (Příloha č. 3 k vyhlášce, uvádí seznam témat - Doporučená témata pro rozvoj bezpečnostního povědomí, tento seznam není třeba dále rozvádět)
- b) stanoví pravidla rozvoje bezpečnostního povědomí uživatelů, administrátorů a osoby odpovědné za kybernetickou bezpečnost, včetně pravidel pro tvorbu hesel dle § 9,
- c) zajistí poučení vrcholného vedení o jeho povinnostech, o bezpečnostní politice zejména v oblasti zajišťování kybernetické bezpečnosti formou vstupních a pravidelných školení,
- d) v souladu s pravidly rozvoje bezpečnostního povědomí provádí vstupní školení v oblasti kybernetické bezpečnosti,
- e) v souladu s pravidly rozvoje bezpečnostního povědomí provádí pravidelná školení v oblasti kybernetické bezpečnosti,
- f) vede přehledy o školeních a vede seznamy osob podle písm. c) a d), které školení absolvovaly,
- g) zajistí potřebná odborná teoretická i praktická školení administrátorů a osoby odpovědné za kybernetickou bezpečnost v souladu s jejich pracovní náplní,

- h) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osoby odpovědné za kybernetickou bezpečnost a*
- i) stanoví pravidla a postupy pro řešení případů porušení bezpečnostní politiky.*

§ 11 Řešení kybernetických bezpečnostních incidentů

(1) Povinná osoba v rámci řešení kybernetických bezpečnostních událostí a incidentů

- a) zajistí, že uživatelé, administrátoři, osoby odpovědné za kybernetickou bezpečnost, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti,*
- b) vytvoří metodiku pro posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, včetně posuzování významnosti dopadu kybernetického bezpečnostního incidentu v souladu s § 15, (§ 15 Stanovení významnosti dopadu kybernetického bezpečnostního incidentu – tento paragraf patří mezi organizační opatření a není potřeba ho dále rozvádět)*
- c) zajistí posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů v souladu s metodikou podle písmene b),*
- d) zajistí detekci kybernetických bezpečnostních událostí a dále při jejich detekci používá nástroje podle § 10, (postup v případě § 10 popsán v předešlém textu)*
- e) zajistí řešení kybernetických bezpečnostních incidentů,*
- f) zajistí hlášení kybernetického bezpečnostního incidentu s významným dopadem podle § 16 zákona, (viz návrh zákona, není třeba dále rozvádět)*
- g) zajistí vytvoření závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu s významným dopadem podle § 17 zákona (viz návrh zákona, není třeba dále rozvádět), včetně popisu příčiny vzniku kybernetické bezpečnostního incidentu s významným dopadem, pokud je známa.*

II PRAKTICKÁ ČÁST

6 ANALÝZA RIZIK NA ZÁKLADĚ INTERNÍHO AUDITU

Pro analýzu rizik z hlediska možnosti ohrožení bezpečnosti by měl nejprve proběhnout interní audit nastavení bezpečnostních politik a opatření a obecně všech nástrojů přicházejících v úvahu z hlediska možných druhů hrozeb. Kybernetickou bezpečnost je možno rozdělit do několika oblastí, které pokrývají různé aspekty ochrany dat, systémů a infrastruktury. Mezi hlavní oblasti patří:

- **fyzická bezpečnost** – ochrana fyzických zařízení a prostor, např. zabezpečení serverů a další síťové infrastruktury, použití a nastavení ochranných prvků, jako např. fyzická ochrana perimetru, použití kamerových systémů atd.,
- **bezpečnost provozu a incident response** – monitorování systémů, nasazení IDPS a SIEM software, detekce hrozeb a rychlá reakce na bezpečnostní incidenty,
- **síťová bezpečnost** – ochrana přenosu dat a komunikace šifrováním, použití access listů, různých druhů software, jako např. antivirů, firewallů, prevence proti DDoS útokům, atd.,
- **bezpečnost cloudových služeb** – ochrana dat uložených v cloudu pomocí bezpečnostních politik, monitoring a dodržování legislativy,
- **bezpečnost koncových zařízení** – ochrana počítačů, mobilních zařízení a IoT před malwarem (zvláště před nebezpečným ransomwarem) a neoprávněným přístupem,
- **bezpečnost aplikací** – zajištění ochrany softwaru před zranitelnostmi, jako např. SQL injection, XSS útoky a zabezpečení API,
- **bezpečnost dat** – šifrování, zálohování a ochrana proti úniku citlivých informací,
- **identita a přístupová bezpečnost** – správa uživatelských oprávnění, vícefaktorová autentizace a ochrana proti neoprávněnému přístupu,
- **bezpečnost zaměstnanců a školení** – prevence lidských chyb, osvěta o phishingu a sociálním inženýrství.

Z výše uvedených bodů je jasné, že se jedná o komplexní problematiku, která vyžaduje nasazení adekvátních kapacit finančních prostředků, lidských zdrojů a času. Přitom jen málokterému ze jmenovaných bodů je možno se vyhnout, podnik střední velikosti se může vyhnout v podstatě např. jen používání cloudových služeb, proto tento bod v analýze rizik je prozatím možno vynechat. Ostatně ukládání citlivých firemních dat na cizím úložišti může být samo o sobě bezpečnostním rizikem.

6.1 Analýza rizik fyzické bezpečnosti

I v případě kybernetické bezpečnosti je třeba začít prvním krokem a to je zajištění fyzické bezpečnosti. V případě ICT prvků se jedná zejména o fyzickou bezpečnost serverů, síťové infrastruktury a koncových stanic, ale i pro tu je základní fyzické zabezpečení areálu podniku na prvním místě.

Nemusí se jednat přímo o napadení, nebo kybernetický útok, i přírodní vlivy, nebo katastrofy mohou ohrozit dostupnost firemních služeb. V prostředí ČR pak zvláště zkušenosti s rozsáhlými a ničivými povodněmi za posledních cca 30 let jasně ukazují, že je nutno s tímto případem počítat. Po velkých povodních v r. 1997 města a kraje podnikly mnoho opatření, do protizáplavových opatření bylo hodně investováno, což se mnohde kladně projevilo v letech 2010 a 2024, ale např. povodně v r. 2024 zase poničily jiné oblasti, které nebyly dříve tolik zasaženy, viz např. smrtelné následky na Krnovsku. Naopak poměrně vzácným jevem je zemětřesení. Tropické teploty kolem 35 °C a více během léta nepřesáhnou např. 20 dní v roce a nízké teploty pod -20 °C také nejsou příliš časté. Vzdušné jevy jako uragány a bouřkové celly také nejsou příliš časté, ale v r. 2023 byla ČR postižena lokální vichřicí ve velmi malém prostorovém rozsahu, ale s fatálními následky pro lokální zástavbu a infrastrukturu a i se smrtelnými následky. To vše může nějakou formou ohrozit dostupnost služeb podniku. Např. důležité serverovny je proto vhodné buď vůbec nestavět v záplavových oblastech, nebo pokud je to nezbytné, tak s výrazným zabezpečením už od stádia projektu, např. tak že ve spodních patrech budov není důležitá infrastruktura a samotné servery se nacházejí až třeba ve 2. patře.

6.1.1 Fyzická bezpečnost areálu podniku z hlediska přírodních událostí

- Pravděpodobnost zaplavení při povodni - podnik se nachází v záplavové oblasti a v minulosti již byl zaplaven. Při povodních v září 2024 (uvažujeme teoretický podnik na střední Moravě) podnik zaplaven nebyl, protipovodňová opatření zajištěná krajem a městem zafungovala, ale je nutno brát v úvahu, že výška hladiny v roce 2024 nedosáhla úrovně roku 1997, kdy podnik zaplaven byl. Hladina vody tehdy dosahovala cca 1 – 1,5 metru. Je ovšem potřeba zmínit, že i v roce 2024 byly zaplaveny některé technologické prostory nacházející se pod úrovní terénu. Toto zaplavení neohrozilo provoz podniku, ale z prostor pod úrovní terénu bylo potřeba vodu vyčerpat,

- pravděpodobnost ohrožení extrémními teplotami - velmi nízká,
- pravděpodobnost ohrožení bouřkovou cellou hurikánu – velmi nízká, ale vzhledem k náhodnosti a rychlosti vzniku tohoto jevu se narozdíl od předešlých ohrožení nedá předpovídat, což radikálně snižuje možnost včasných příprav na hrozící událost,
- pravděpodobnost zemětřesení - velmi nízká, zemětřesení v ČR bývají na nízké úrovni škály Richterovy stupnice a často bez následků, ale tento jev se také nedá předpovídat.

Z výše uvedené analýzy rizik přírodních vlivů je pro podnik reálnou hrozbou možnost zaplavení za povodně a je potřeba této situaci přizpůsobit umístění alespoň kritických síťových prvků – viz další kapitoly.

6.1.2 Fyzická bezpečnost areálu podniku z hlediska vnější kriminality

- Areál podniku je oplocen, pěší vstup do areálu je střeženou branou s vrátnicí, vstup cizích osob je evidován,
- vjezd vozidel do areálu je taktéž střeženou branou s vrátnicí, je evidován a vjíždět mohou jen vybraná určená vozidla a při vjezdu i odjezdu je vozidlo kontrolováno,
- areál podniku je střežen nepřetržitou strážní službou 24/7, zajišťovanou externí civilní bezpečnostní agenturou.

Takto zajištěná opatření se pro běžný stupeň předpokládaného ohrožení jeví jako dostatečná.

6.1.3 Fyzická bezpečnost serverů, síťových prvků a uživatelských stanic

- Servery a další důležité síťové prvky jsou umístěny v uzamykatelných místnostech, nebo v uzamykatelných skříních,
- po zkušenostech s povodněmi z devadesátých let jsou důležité síťové prvky umístěny ve vyšších patrech, nebo pokud v přízemí, pak ve výšce 2 m od podlahy,
- přístup k důležité síťové infrastruktuře mají jen pověřené osoby

- uživatelské stanice nejsou nijak výjimečně fyzicky chráněny, ochrana před zásahem nepovolané osoby je možná pouze uzamykáním místností při odchodu odpovědných osob a jinak se uživatelské stanice nachází běžně v perimetru střeženého areálu

Takto zajištěná opatření se pro běžný stupeň předpokládaného ohrožení jeví jako dostatečná, zvláštní opatření proti riziku přírodních vlivů lze považovat také za přiměřená a dostatečná.

6.1.4 Fyzická bezpečnost tištěných dokumentů

Tištěné dokumenty nepatří přímo do oblasti kybernetické bezpečnosti, ale je možné, že některé dokumenty by mohly obsahovat informace umožňující průnik do systému. Proto i na ně je třeba brát zřetel.

- Tištěné dokumenty se nacházejí v uzamykatelném archivu,
- přístup do archivu mají jen určené osoby, čímž je zabezpečeno, že za běžné situace nemají do archivu přístup nepovolané osoby.

Takto zajištěná opatření se pro běžný stupeň předpokládaného ohrožení jeví jako dostatečná.

6.2 Analýza rizik z hlediska bezpečnosti provozu a incident response

Monitorování systémů, nasazení IDPS a SIEM software, detekce hrozeb a rychlá reakce na bezpečnostní incidenty vycházejí z požadavků nového zákona o kybernetické bezpečnosti. Podnik zatím žádné IDPS a SIEM systémy nepoužívá a pro splnění požadavku zákona je bude potřeba zavést.

6.3 Analýza rizik z hlediska síťové bezpečnosti

Podnik má v běžném provozu nasazený access listy, antivirové systémy a firewally. Přenos dat a komunikace je šifrována ve webovém provozu přes HTTPS (TLS/SSL) a v e-mailovém provozu běžně používaným standardem TLS, zajišťujícím šifrovaný přenos e-mailových zpráv mezi poštovními servery. Žádné další metody pro šifrování e-mailové komunikace, jako např. S/MIME, nebo PGP nejsou zatím používány, prevence proti DDoS útokům není také zatím nijak zavedena.

6.4 Analýza rizik z hlediska bezpečnosti koncových zařízení

Jako základ ochrany proti malware je nasazen antivirový systém, ochranu proti neoprávněnému přístupu zajišťují bezpečnostní politiky a autentizace přístupů do systémů uvedené v textu níže.

6.5 Analýza rizik z hlediska bezpečnosti aplikací

Zajištění ochrany softwaru před zranitelnostmi, jako např. SQL injection, XSS útoky a zabezpečení API není z majoritní části v náplni práce podnikového IT oddělení a očekává se, že bezpečnost aplikací z hlediska jejich vnitřní struktury zajistí pravidelné aktualizace používaného software. Při případné potřebě pracovat s SQL dotazy je pak nutno postupovat podle obvyklých doporučení pro tyto případy.

6.6 Analýza rizik z hlediska bezpečnosti uchovávaných dat

V podniku je zaveden systém pravidelného zálohování, šifrování ukládaných dat zatím není prováděno. Ochranu proti úniku citlivých informací zajišťují bezpečnostní politiky a autentizace přístupů do systémů uvedené v textu níže.

6.7 Analýza rizik z hlediska kontroly identit a přístupové bezpečnosti

V podniku jsou zavedeny bezpečnostní politiky, nastavení rolí pro přístup do systémů a je zajištěna autentizace přístupů do systémů, je zavedena správa uživatelských oprávnění, čímž je zajištěna ochrana proti neoprávněnému přístupu. Vícefaktorová autentizace zatím není zavedena.

6.8 Analýza rizik z hlediska bezpečnosti zaměstnanců a jejich školení

Pro zajištění prevence lidských chyb probíhají ve firmě pravidelná školení a osvěta o různých druzích sociálního inženýrství a o dalších metodách útoků zneužívajících lidské chyby.

7 ORGANIZAČNÍ OPATŘENÍ KE SNÍŽENÍ ÚROVNĚ RIZIK

Z hlediska zavádění organizačních opatření ke snížení úrovně rizik kybernetické bezpečnosti existuje několik mezinárodních standardů, které podniky mohou využít jako podklady pro organizační opatření ke snížení kybernetických rizik. Mezi nejvýznamnější patří:

- ISO/IEC 27001 – norma pro systémy řízení informační bezpečnosti (ISMS), stanovuje požadavky na řízení bezpečnostních rizik,
- ISO/IEC 27002 – podrobné pokyny pro implementaci bezpečnostních opatření v rámci ISMS,
- ISO/IEC 27005 – zaměřuje se na řízení rizik informační bezpečnosti a poskytuje metodiku pro jejich identifikaci a zmírnění dopadů rizik,
- NIST Cybersecurity Framework – rámec vyvinutý americkým institutem NIST, pomáhá organizacím identifikovat, chránit, detekovat, reagovat a zotavit systémy po kybernetických incidentech.

V českém národním prostředí jsou také k dispozici normy přejaté a zveřejněné jako součást českého normalizačního systému. Podniky tedy mohou zavádět opatření podle ISO/IEC a mohou využít odpovídající ČSN verzi, která je harmonizovaná s evropskými a mezinárodními standardy, rozdíly mezi jednotlivými verzemi jsou:

- ISO/IEC – mezinárodní norma vytvořená Mezinárodní organizací pro normalizaci (ISO) a Mezinárodní elektrotechnickou komisí (IEC),
- EN ISO/IEC – evropská verze normy ISO/IEC, kterou přebírají členské státy Evropského výboru pro normalizaci (CEN),
- ČSN EN ISO/IEC – česká národní norma, která odpovídá evropské normě EN a je identická s mezinárodní ISO/IEC.

Vhodným postupem pro zavedení organizačních opatření ke snižování úrovně rizik je nastavení bezpečnostních politik podniku a následně pak zavedení systému řízení informační bezpečnosti (ISMS). Zavedením ISMS také podnik, či organizace demonstruje závazek k ochraně svých aktiv a ke splnění regulačních požadavků na kybernetickou bezpečnost.

7.1 ISMS

ISMS (Information Security Management System) je systematický přístup k řízení bezpečnostních rizik v organizaci a k ochraně důvěrných, strategických, nebo jinak důležitých informací a dat podniku, nebo obecně jakékoli informace podniku, jejichž ztráta, únik, nedostupnost pro oprávněné osoby, nebo neoprávněná změna by mohly ohrozit plynulost poskytování služeb podniku, fungování podniku jako takového, mohly by být zneužity k útoku na bezpečnost produktů podniku, nebo vést k jakémukoli jinému bezpečnostnímu incidentu.

Tento systém zahrnuje procesy, pravidla a technologie, které jsou navrženy k minimalizaci rizik souvisejících s narušením informační bezpečnosti.

Zavedení ISMS v podniku se obvykle řídí normou ISO/IEC 27001, což je doporučovaný standard pro správu informační bezpečnosti. Pro úspěšnou implementaci ISMS je také doporučováno použít metodiku založenou na PDCA cyklu (Plan – Do – Check - Act), jehož detailní popis není součástí tohoto textu, ale všechny jeho podstatné záležitosti jsou zahrnuty do textu dále a již jeho název mnohé napovídá. Jedná se o obecný postup, který může být použit i v jakýchkoli jiných oblastech lidské činnosti. Co se týče konkrétních pokynů a metodik, jsou vhodným zdrojem především:

- ISO/IEC 27005: konkrétní pokyny pro řízení rizik informační bezpečnosti, pro organizace, které chtějí implementovat komplexní proces řízení rizik zaměřený na identifikaci aktiv a kontrolních opatření. Typicky pro podniky s důrazem na ochranu dat a na soulad s předpisy.
- NIST SP 800-30: metodika hodnocení rizik, která se zaměřuje na řízení rizik IT, pro organizace, které potřebují zaměřit své řízení rizik na kybernetické hrozby a zranitelnosti, zejména pro firmy, které se potýkají s hrozbami v oblasti IT infrastruktury a průmyslové automatizace.

7.2 Klíčové prvky ISMS

Klíčové prvky ISMS dají shrnout, do 3 bodů, které se jsou základními stavebními kameny pro ISMS.

Tyto v bodech vyjádřené a dle závažnosti seřazené klíčové prvky by se daly popsat jako:

- DŮVĚRNOST - zajištění stavu, že chráněné informace jsou přístupné pouze oprávněným osobám
- DOSTUPNOST - zajištění stavu, že chráněné informace jsou pro oprávněné uživatele k dispozici, kdykoli je to potřeba
- INTEGRITA - zajištění stavu, že chráněné informace jsou úplné, přesné a nejsou neoprávněně měněny

Tedy pokud je správně pochopena podstata věci, je pak snazší vybrat, nasadit, řídit a regulovat potřebné nástroje k jejímu zajištění. V tomto případě se výše uvedené body dají nazvat požadavkem na stav věci a ISMS je poté nástroj k dosažení tohoto stavu. Z hlediska důležitosti a publikovatelnosti mohou mít podnikové informace charakter důvěrné, interní a veřejné, dále v textu budou všechny druhy označovány souhrnně jako podnikové informace. Ty mohou spadat pod různé stupně úrovně ochrany, nebo pod žádný stupeň.

7.3 Cíle ISMS a oblasti působnosti

7.3.1 Cíle zavedení ISMS

- Zajištění ochrany podnikových informací proti neoprávněnému přístupu, neoprávněným změnám a nedostupnosti, nebo úplné ztrátě – Podnikové informace jsou chráněny před jakoukoli neoprávněnou změnou, nedostupností, nebo ztrátou, důvěrné a interní informace jsou kromě toho navíc ještě chráněny před jakýmkoli neoprávněným přístupem. Veřejné informace jsou chráněny před jakoukoli neoprávněnou změnou, nedostupností, nebo ztrátou, pokud se nacházejí v interním systému podniku, zejména pro případ, kdy by mimo podnik vznikly problémy s jejich důvěryhodností a protože je potřeba mít kdykoli k dispozici ověřené zálohy informací, které jsou veřejně publikovatelné a jsou přebírány třetími stranami jako oficiální podnikové dokumenty, např. manuály k podnikovým produktům. Jsou používány moderní technologie a postupy k zabezpečení systémů a dat, šifrování, pravidelné zálohování a řízený přístup ke správě uživatelských oprávnění. Každý přístup k podnikovým informacím je monitorován a zaznamenáván, aby byla zajištěna jejich bezpečnost a integrita.

- Stanovení zásad pro řízení informační bezpečnosti v podniku - Veškeré činnosti spojené s informační bezpečností jsou v podniku řízeny podle stanovených zásad, které určují, jakým způsobem se přistupuje k ochraně důležitých informací. Každý zaměstnanec je pravidelně školen a informován o nejlepších postupech, které je třeba dodržovat pro zajištění bezpečnosti firemních dat a informačních systémů.

7.3.2 Oblasti působnosti

Všichni zaměstnanci, dodavatelé a partneři, kteří mají přístup k informačním systémům a k datům společnosti

- Zaměstnanci: Každý zaměstnanec podniku, bez ohledu na pozici, nebo oddělení, je povinen dodržovat zásady informační bezpečnosti. To zahrnuje i školení a pravidelné aktualizace znalostí v oblasti bezpečnosti.
- Dodavatelé: Všichni externí dodavatelé, kteří poskytují služby nebo produkty podniku a mají přístup k firemním informačním systémům nebo datům, musí rovněž dodržovat všechny stanovené bezpečnostní postupy. Při sjednávání smluv s dodavateli jsou zahrnuty bezpečnostní požadavky, které je třeba respektovat.
- Partneři: obchodní partneři, se kterými podnik sdílí informace nebo systémy v rámci spolupráce, jsou také zavázáni dodržovat bezpečnostní standardy. Partnerské smlouvy obsahují klauzule o informační bezpečnosti, aby byla zajištěna ochrana podnikových dat.

7.4 Zodpovědnosti a role

7.4.1 Management

- Schvalování a podpora bezpečnostních politik a směrnic - Management podniku je zodpovědný za schvalování bezpečnostních politik a směrnic a také aktivně podporuje jejich implementaci a dodržování.
- Přidělování zdrojů potřebných k implementaci ISMS – Management podniku je zodpovědný za přidělování finančních, technologických a lidských zdrojů potřebných pro efektivní implementaci systému řízení informační bezpečnosti.

7.4.2 Bezpečnostní tým

- Monitorování a hodnocení účinnosti bezpečnostních opatření - Bezpečnostní tým podniku je zodpovědný za průběžné monitorování všech bezpečnostních opatření a jejich hodnocení. To zahrnuje provádění pravidelných auditů, testování zranitelností a sledování bezpečnostních incidentů.
- Zajištění školení a povědomí o informační bezpečnosti - Bezpečnostní tým podniku má rovněž na starosti organizaci školení pro zaměstnance o nejnovějších bezpečnostních postupech a technologiích, pracuje také na zvyšování povědomí o informační bezpečnosti napříč podnikem, například prostřednictvím informačních kampaní o pravidelných aktualizacích bezpečnostních procesů a nastavení.

7.4.3 Zaměstnanci

- Dodržování bezpečnostních politik a směrnic - Každý zaměstnanec podniku má povinnost dodržovat všechny stanovené bezpečnostní politiky a směrnice. To zahrnuje používání bezpečnostních nástrojů a postupů při práci s firemními daty a systémy, a také aktivní snahu o minimalizaci rizik spojených s informačními hrozbami.
- Hlášení bezpečnostních incidentů - Zaměstnanci podniku jsou povinni na určeném kontaktním místě okamžitě hlásit jakékoli bezpečnostní incidenty nebo podezřelé aktivity.

7.5 Politiky a postupy

7.5.1 Politika přístupu k informacím

Řízení přístupu k podnikovým informacím na základě role a potřeby - Přístup k podnikovým informacím je řízen na základě role a potřeby. Každý uživatel systému má přidělenou úroveň přístupu odpovídající jeho pracovním povinnostem a potřebám. Přístupová práva jsou pravidelně revidována a aktualizována s cílem minimalizovat riziko neoprávněného přístupu k důvěrným, nebo interním informacím. Uživatelé jsou povinni používat své přihlašovací údaje odpovědně a nesmí je sdílet s dalšími osobami.

7.5.2 Ochrana dat

Klasifikace dat a stanovení opatření k ochraně dat - Data v podniku jsou klasifikována podle úrovně důležitosti a publikovatelnosti, což představuje kategorie důvěrná, interní a veřejná. Pro úroveň důvěrná a interní jsou definována specifická bezpečnostní opatření, která zahrnují šifrování dat, řízení přístupu k datům, zálohování a bezpečné ukládání. Pravidelně se provádí kontroly a audity.

7.5.3 Správa identit a autentizace

Zavedení silného ověřování a řízení přístupu pro všechny uživatele - Pro všechny uživatele v podniku je zavedeno ověřování, které v opodstatněných případech zahrnuje vícefaktorovou autentizaci. Uživatelé mají správcem nastavena silná hesla, která jsou v předepsaných cyklech měněna. Správa identit zahrnuje také řízení životního cyklu uživatelských účtů, které zahrnuje zakládání, aktualizaci a zrušení účtů podle potřeb organizace. Pravidelně se provádí kontrola a aktualizace přístupových práv, aby se zajistilo, že každý uživatel má přístup pouze k těm informacím a systémům, které jsou nezbytné pro jeho práci.

7.6 Řízení rizik

7.6.1 Identifikace a hodnocení rizik

Pravidelná analýza rizik spojených s informačními aktivy - v podniku se ve stanovených intervalech, nebo v případě důležitých změn v organizační struktuře, v technologickém prostředí, nebo v externích faktorech, které by mohly ovlivnit bezpečnost informačních aktiv, provádí analýza rizik, která zahrnuje identifikaci hrozeb a zranitelností, hodnocení pravděpodobnosti jejich výskytu a stanovení potenciálního dopadu na podnik. Tento proces zahrnuje:

- Identifikaci rizik: Shromažďování informací o možných hrozbách, které by mohly ohrozit informační aktiva, a zranitelnostech, které by tyto hrozby mohly využít.
- Hodnocení rizik: Analýza pravděpodobnosti výskytu identifikovaných hrozeb a zranitelností a jejich možného dopadu na organizaci.
- Dokumentace rizik: Vytvoření záznamů o identifikovaných rizicích, jejich hodnocení a plánech na jejich řízení.

7.6.2 Opatření k minimalizaci rizik

Zavedení technických a organizačních opatření k minimalizaci rizik:

(Tyto body jsou podrobněji rozvedeny v jiných kapitolách, zde jen stručně)

- Technická opatření: Implementace technických řešení - šifrování dat, access list, firewall, antivirové programy, software pro detekci a prevenci narušení (IDPS), bezpečnostní informační systém (SIEM), pravidelné aktualizace softwaru a systémů.
- Organizační opatření: Zavedení potřebných postupů a procesů, školení zaměstnanců v oblasti bezpečnosti informací, vytváření a udržování politik přístupu k informacím, plánování kontinuity činností a reakce na incidenty.
- Pravidelné hodnocení a zlepšování: Pravidelné kontroly a audity bezpečnostních opatření s cílem identifikovat slabiny a provádět jejich nápravu. Neustálé zlepšování bezpečnostních postupů a technologií na základě získaných zkušeností a změn v hrozbách.

7.7 Řízení incidentů

7.7.1 Hlášení incidentů

Zajištění mechanismu pro rychlé hlášení bezpečnostních incidentů - Zaměstnanci v podniku jsou na pravidelných školeních informováni o postupech hlášení incidentů s povinností okamžitého hlášení jakýchkoli podezřelých aktivit nebo bezpečnostních problémů. Postupy pro hlášení incidentů zahrnují:

- Kontaktní bod: Určení jednoho nebo více kontaktních míst (např. bezpečnostní tým, IT oddělení), kterým lze incidenty hlásit.
- Formulář hlášení incidentů: Poskytnutí standardizovaného formuláře pro hlášení incidentů, který zahrnuje důležité informace jako datum a čas incidentu, popis události, identifikace postižených systémů a navrhovaná opatření.
- Školení a informovanost: Pravidelné školení zaměstnanců o postupech hlášení incidentů a významu rychlého hlášení.

7.7.2 Reakce na incidenty

Definování postupů pro vyšetřování a řešení bezpečnostních incidentů - Reakční plán v podniku obsahuje následující kroky:

- Inicializace reakce: Po přijetí hlášení incidentu je aktivován reakční tým, který zahájí vyšetřování.
- Izolace a zmírnění: Jsou vydána okamžitá opatření k izolaci postižených systémů a minimalizaci dopadu incidentu, odpojení infikovaných zařízení ze sítě apod.
- Vyšetřování: vyšetření incidentu za účelem identifikace příčiny, rozsahu a dopadu, sběr důkazů, analýzu logů a provedení forenzních analýz.
- Komunikace: Informování relevantních stran dle stupně závažnosti incidentu (vedení, NÚKIB, zákazníci) o incidentu a postupu řešení.
- Obnova: Opatření k obnovení postižených systémů do původního stavu, zajištění, že všechny zranitelnosti byly odstraněny a všechny ovlivněné systémy byly bezpečně obnoveny.
- Zhodnocení a dokumentace: Po ukončení řešení incidentu je provedeno zhodnocení reakčního postupu a jsou zadokumentovány všechny kroky a závěry. Tato dokumentace slouží k identifikaci slabín a ke zlepšení budoucích postupů pro řízení incidentů.

7.8 Kontrola a audit

7.8.1 Pravidelné audit

Pravidelné hodnocení a auditování ISMS a bezpečnostních politik – Tento proces v podniku zahrnuje následující kroky:

- Plánování auditu: Vytvoření plánu auditů, který zahrnuje frekvenci a rozsah kontrol jednotlivých oblastí ISMS.
- Provádění auditu: Provádění detailní analýzy všech aspektů ISMS, včetně kontroly dokumentace, sledování dodržování politik a postupů a vyhodnocení technických a organizačních opatření.
- Zpráva z auditu: Vytvoření zprávy, která zahrnuje nálezy z auditu, identifikované nesrovnalosti a doporučení pro nápravná opatření.

- Nápravná opatření: Implementace doporučených nápravných opatření a následné sledování jejich efektivity.

7.8.2 Aktualizace směrnic

Revize a aktualizace směrnic na základě výsledků auditů a měnících se rizik - Tento proces v podniku zahrnuje:

- Přezkoumání výsledků auditů: Analýza nálezů z auditů a identifikace oblastí, které vyžadují aktualizaci nebo zlepšení.
- Aktualizace směrnic: Revize stávajících politik a postupů a jejich aktualizace na základě získaných poznatků a změn v rizikových faktorech.
- Komunikace změn: Informování všech relevantních stran o provedených změnách a zajištění, že jsou nově aktualizované směrnice dostupné a srozumitelné pro všechny zaměstnance.
- Školení: Organizace školení pro zaměstnance s cílem seznámit je s nově zavedenými změnami a zajistit, že budou schopni tyto změny efektivně aplikovat v praxi.

7.9 Školení a povědomí o ISMS

7.9.1 Školení zaměstnanců

Pravidelná školení všech zaměstnanců v oblasti informační bezpečnosti - Tento proces v podniku zahrnuje:

- Úvodní školení: Všichni noví zaměstnanci musí absolvovat úvodní školení v oblasti informační bezpečnosti, které zahrnuje základní zásady bezpečnosti, politiky organizace a praktické kroky k ochraně podnikových informací.
- Pravidelné školení: Všichni zaměstnanci jsou povinni absolvovat pravidelná školení, která zahrnují aktualizace o nových hrozbách a změnách v bezpečnostních postupech organizace.
- Specifická školení: Zaměstnanci, kteří pracují s chráněnými informacemi nebo mají klíčové bezpečnostní role, musí absolvovat specifická školení zaměřená na jejich oblast odpovědnosti.

- Testování a hodnocení: Po každém školení je prováděno testování znalostí zaměstnanců, aby bylo zajištěno, že informace byly správně pochopeny a jsou schopni je aplikovat v praxi.

7.9.2 Kampaně pro zvyšování povědomí o bezpečnostních hrozbách

Organizace kampaní a aktivit zaměřených na zvýšení povědomí o bezpečnostních hrozbách - Tento proces v podniku zahrnuje:

- Pravidelná komunikace: Vydávání pravidelných newsletterů nebo oznámení s informacemi o aktuálních bezpečnostních hrozbách, nových bezpečnostních postupech a best practices.
- Tematické kampaně: Organizování specifických kampaní zaměřených na konkrétní hrozby, jako je phishing, ransomware, nebo bezpečnost mobilních zařízení.
- Simulované útoky: Pravidelné provádění simulovaných útoků (např. phishingové kampaně) za účelem testování připravenosti zaměstnanců a identifikace oblastí, kde je potřeba další školení.
- Bezpečnostní akce a události: Organizace workshopů, seminářů a konferencí zaměřených na bezpečnost informací, kde mohou zaměstnanci získat aktuální informace a sdílet zkušenosti a best practices.

8 TECHNICKÁ OPATŘENÍ KE SNÍŽENÍ UROVNĚ RIZIK

V kapitole 8) *Analýza rizik na základě interního auditu* je popis současného stavu podniku z hlediska technické úrovně kybernetické bezpečnosti a v kapitole 5) *Bezpečnostní opatření poskytovatele regulované služby v režimu nižších povinností* je mj. i výčet technických požadavků z vyhlášky zákona. Porovnáním současného stavu s požadavky dostaneme poměrně jasný přehled o tom, co je potřeba změnit. Níže budou uvedeny pouze ty oblasti, které spadají do technické části. Potřeba zavedení opatření je rozdělena na tři stupně:

- **vysoká** – potřeba zavedení opatření je pro splnění požadavků zákona primární a je nutno toto zavést opatření co nejdříve
- **střední** - potřeba zavedení opatření je pro splnění požadavků zákona důležitá, ale lze o nějaký čas odložit, je vhodné toto opatření vést v plánu budoucích opatření
- **nízká** - potřeba zavedení opatření není pro splnění požadavků zákona zásadní, opatření je možno odložit na delší dobu

8.1 Fyzická bezpečnost

Úroveň nastavení fyzické bezpečnosti podniku lze v tomto případě považovat za přiměřenou a dostatečnou, za nezměněného stavu potenciálních rizik stačí udržovat současnou úroveň.

8.2 Bezpečnost provozu a incident response

Podnik zatím nepoužívá žádné IDPS a SIEM systémy a pro splnění požadavku zákona je bude potřeba zavést. Potřebu zavedení lze vyhodnotit stupněm **vysoká**.

8.3 Síťová bezpečnost

Podnik zatím nepoužívá žádné další metody (mimo TLS) pro šifrování e-mailové komunikace, jako např. S/MIME, nebo PGP a prevence proti DDoS útokům není také zatím nijak zavedena. Zavedení těchto prostředků ochrany lze vyhodnotit stupněm **střední**.

8.4 Bezpečnost koncových zařízení

Úroveň nastavení ochrany koncových zařízení proti malware a proti neoprávněnému přístupu v podniku lze v tomto případě považovat za přiměřenou a dostatečnou, za nezměněného stavu potenciálních rizik stačí udržovat současnou úroveň.

8.5 Bezpečnost aplikací

Úroveň nastavení ochrany aplikací proti SQL injection, XSS útokům a zabezpečení API v podniku lze v tomto případě považovat za přiměřenou a dostatečnou a při zajištění pravidelných aktualizací používaného software a v případě potřeby pracovat s SQL dotazy při postupu podle obvyklých doporučení pro tyto případy stačí udržovat současnou úroveň.

8.6 Bezpečnost uchovávaných dat

Úroveň nastavení ochrany ukládaných dat lze v tomto případě považovat za přiměřenou a dostatečnou, šifrování ukládaných dat zatím není prováděno. Za nezměněného stavu potenciálních rizik stačí udržovat současnou úroveň s výhledem na zavedení šifrování. Potřebu zavedení šifrování lze vyhodnotit stupněm *nízká*.

8.7 Kontrola identit a přístupová bezpečnost

Úroveň nastavení ochrany kontroly identit a přístupové bezpečnosti lze v tomto případě považovat za přiměřenou a dostatečnou, vícefaktorová autentizace zatím není zavedena. Za nezměněného stavu potenciálních rizik stačí udržovat současnou úroveň s výhledem na zavedení vícefaktorové autentizace. Potřebu jejího zavedení lze vyhodnotit stupněm *nízká*.

8.8 Další jinde neuvedená technická opatření

Metod, postupů, strategií a jak komplexně zajistit kybernetickou bezpečnost je mnoho a některé nebyly v předešlých textech zmiňovány, také mj. proto, že jejich působnost může spadat do více oblastí a jejich zavedením je možno řešit více bodů z výše jmenovaných.

V této části proto budou zmíněna další doporučení bez dalšího dělení do oblastí působnosti dle bodů výše. Některá opatření jsou požadována vyhláškou zákona přímo a některé lze doporučit jako best practices jako doplňující a nebo i stejně zásadní jako opatření vyhláškou vyžadovaná.

8.8.1 Segmentace sítě

Segmentace sítě je jedním z nejnákladnějších technických požadavků vyhlášky k novému zákonu, jak je zmíněno již v předešlém textu znění vyhlášky „...*Povinná osoba... a) zajistí segmentaci komunikační sítě, včetně oddělení provozního a zálohovacího prostředí,...*“. Pro tento požadavek je vhodné použít VLAN jakožto prostředek virtuální segmentace sítě. Pro segmentaci je ovšem nutno použít jen vhodné aktivní prvky, které umožňují určitou úroveň zabezpečení. Konkrétně se jedná např. o tzv. managed switche, s pokročilými možnostmi správy a konfigurace sítě, čímž nabízí administrátorům monitorovat, konfigurovat a spravovat jednotlivé porty, bez čehož není zabezpečení možné.

8.8.2 Základní nastavení routerů a switchů

Při budování nové sítě, nebo při rekonstrukci sítě na segmentovanou je vhodné již od začátku provést základní nastavení routerů a switchů tak, aby byly nastaveny bezpečnostní mechanismy:

- Nastavení **port security** - omezení počtu MAC adresy na koncových portech s detekcí narušení a zajištěním vypnutí portu na stanovenou dobu se zotavením po nastavené době,
- nastavení **DHCP Snooping** s přiřazením autorizovaného DHCP serveru,
- nastavení **ARP inspection** s detekcí narušení a zajištěním vypnutí portu na stanovenou dobu se zotavením po nastavené době,
- autentizaci PC pomocí **802.1X** proti radius serveru,
- porty, které nebudou osazeny koncovými stanicemi/servery by měly být trvale vypnuté,
- použití monitorovacího serveru pro monitoring aktivních prvků s přístupem ke switchům a routerům, s nasazením monitorovacího software.

9 NÁVRH IMPLEMENTACE OPATŘENÍ V PODNIKU

Implementace bezpečnostních opatření v podniku je časově, kapacitně a finančně náročným zásahem do běhu IT infrastruktury a má zásadní vliv na funkčnost celého podniku. V dnešní době, jsou podniky na funkčnosti sítí zcela závislé a jakékoli i drobné výpadky mohou přinést finanční ztráty, při velkých výpadcích i rozsáhlé škody. Proto je taková změna kritickým krokem, měla by být dobře promyšlena a naplánována na všech úrovních řízení podniku a poté by měla probíhat podle předem stanoveného harmonogramu. V bodech se plán postupu implementace dá vyjádřit např. v těchto bodech:

9.1 Analýza současného stavu

- Identifikace klíčových aktiv podniku - data, systémy, infrastruktura,
- vyhodnocení rizik a určení nejzranitelnější oblasti,
- vyhodnocení souladu současných opatření se zákonnými požadavky.

9.2 Návrh opatření

- Výběr vhodných technických a organizačních bezpečnostní opatření,
- vyhodnocení kompatibility navržených opatření s existující IT infrastrukturou podniku,
- příprava plánu změn a odpovědnosti jednotlivých oddělení.

9.3 Příprava interní dokumentace a školení

- Aktualizace interních bezpečnostních politik a postupů,
- školení zaměstnanců v oblasti kybernetické bezpečnosti a zvyšování povědomí o hrozbách,
- zajištění jasné komunikace nových pravidel a odpovědností v podniku.

9.4 Technická implementace

- Aktualizace softwaru a nasazení nových dosud nezavedených bezpečnostních prvků,
- testování implementovaných opatření před ostrým provozem.

9.5 Kontrola a kontinuální zlepšování

- Pravidelný audit bezpečnostních opatření,
- simulace kybernetických útoků, penetrační testy a reakční scénáře,
- kontinuální sledování nových hrozeb a přizpůsobování opatření aktuálním trendům.

Všechny výše uvedené body jsou závislé na aktuální situaci v podniku a jeho časových, kapacitních a finančních možnostech. Pro případ ukázkového podniku uvažovaného v této práci je v kapitole 8) *Analýza rizik na základě interního auditu* nastíněn stav podniku, ale každý jiný podnik může mít organizační a síťovou strukturu tak jinou, že kromě obecných bodů nelze doporučit konkrétnější kroky, jakým způsobem opatření implementovat.

10 NÁVRH METOD PRO PRAVIDELNÉ MONITOROVÁNÍ A VYHODNOCOVÁNÍ ÚČINNOSTI ZAVÁDĚNÝCH OPATŘENÍ

Aby byla zajištěna správná implementace požadavků nového zákona o kybernetické bezpečnosti, je vhodné vytvořit systematický přístup k monitorování a vyhodnocování účinnosti přijatých opatření. Metody a techniky, které lze použít lze popsat následovně:

10.1 Automatizovaný monitoring a analýza dat

- **Security Information and Event Management (SIEM)** - nasazení těchto systémů zajistí sběr, vyhodnocování a korelace bezpečnostních událostí v reálném čase,
- **Intrusion Detection / Prevention Systems (IDPS)** – nasazení systému pro sledování síťového provozu a identifikace anomálií,
- **Vulnerability Management Tools** – nasazení nástrojů pro pravidelné skenování systému na zranitelnosti.

10.2 Auditní a kontrolní procesy

- **Interní audit** - pro pravidelné prověřování souladu se zákonnými požadavky a interními bezpečnostními politikami je vhodné zavést systém pravidelných interních auditů,
- **penetrační testování** – simulace kybernetických útoků pro ověření účinnosti zavedených opatření, tento typ testování je ovšem potřeba dobře rozvážit, neboť by mohl přinést různá další rizika,
- **Red teaming** – testování reakce na útoky pomocí simulace reálných kybernetických hrozeb. V tomto případě se jedná o pokročilejší a komplexnější test než běžný penetrační test, protože zahrnuje i taktiky sociálního inženýrství, fyzické bezpečnosti a dlouhodobého plánování útoků. Red team zde představuje skupina odborníků na bezpečnost, kteří se chovají jako skuteční útočníci, hledají slabiny v systémech, pokoušejí se proniknout do sítí a obcházejí bezpečnostní opatření. Cílem není způsobit škodu, ale odhalit nedostatky a pomoci organizaci se lépe chránit. V širší podobě mohou být týmy dva, ještě ve spolupráci s Blue teamem, což je tým obránců, kteří se snaží útoky detekovat a zastavit. Dohromady tvoří purple teaming, kde si obě skupiny mohou následně vyměňovat poznatky.

10.3 Analýza a reporting bezpečnostních incidentů

- **Incident response system** – sledování a vyhodnocování bezpečnostních incidentů, jejich příčiny a reakce na ně,
- **forenzní analýza** – zpětné vyhodnocování kybernetických incidentů pro odhalení slabých míst,
- **zpětná vazba z bezpečnostních událostí** – využití poznatků z předchozích incidentů pro zlepšení opatření.

10.4 Zpětná vazba a vzdělávání zaměstnanců

- **Pravidelná školení** – vzdělávání zaměstnanců o aktuálních kybernetických hrozbách a správných bezpečnostních postupech a chování zaměstnanců,
- **simulované phishingové útoky** – testování připravenosti zaměstnanců na sociální inženýrství, toto testování je také dobře rozvážit a připravit, mohlo by přinést další rizika,
- **bezpečnostní awareness kampaně** – informování o nových typech hrozeb a s nimi souvisejících doporučených opatřeních.

10.5 Metody analýzy rizik a jejich vyhodnocování

- **Risk Assessment Frameworks** – aplikace metod jako ISO/IEC 27005 nebo NIST Risk Management Framework.
- **Continuous Risk Monitoring** – pravidelné přehodnocování bezpečnostních opatření na základě změn v infrastruktuře a hrozbách,
- **bezpečnostní metriky a KPI** – sledování výkonu bezpečnostních opatření pomocí kvantifikovatelných ukazatelů.

Návrh metod pro monitorování a vyhodnocování účinnosti opatření je taktéž závislý na kapacitách podniku, schopnostech pracovníků na jednotlivých pozicích a následně i na finančních možnostech podniku a záleží, co si který podnik vybere a použije. Pro efektivní monitoring je vhodné kombinovat výše uvedené metody a pravidelně upravovat strategie podle aktuálních bezpečnostních trendů. Některé body, jako např. zavedení systémů SIEM

a IDPS vyplývají z požadavků zákona, na některé další, např. na forenzní analýzy pravděpodobně nebude v podniku střední velikosti dostatek volných kapacit. Penetrační testování podnik střední velikosti, pokud by se se pro ně rozhodl, zřejmě nebude provádět svépomocí a zajištění externí firmou může přinést různá další rizika. Naopak bezpečnostní školení a informování o nových typech hrozeb a doporučených opatřeních je jednou ze schůdných cest i pro menší podniky.

11 NÁVRH METOD PRO VYHODNOCOVÁNÍ EFEKTIVITY ZAVÁDĚNÝCH OPATŘENÍ

Vyhodnocování efektivity navržených opatření v rámci implementace nového zákona o kybernetické bezpečnosti je zásadní pro zajištění funkčnosti a účinnosti opatření. Možné postupy a metody mohou být např. tyto:

11.1 Stanovení metrik efektivity

Nejprve je třeba definovat kritéria, podle kterých se bude hodnotit účinnost opatření. Může se jednat např. o tato kritéria:

- Počet bezpečnostních incidentů před a po zavedení opatření,
- rychlost reakce na hrozby (čas mezi detekcí a řešením incidentu),
- shoda s legislativními požadavky (splnění všech povinných parametrů zákona),
- uživatelská zkušenost a provozní dopad (jak opatření ovlivňují běžný provoz podniku),
- náklady na implementaci a provoz oproti přínosům.

11.2 Testování a simulace hrozeb

Pro vyhodnocování efektivity mohou být také užitečné pravidelné testy, jako např.:

- Simulované útoky na systémy pro ověření jejich odolnosti - penetrační testy,
- simulované scénáře reálných kybernetických útoků, tzv. Red team cvičení,
- analýzy reakcí na phishingové kampaně a další sociální inženýrství.

11.3 Sběr dat a analýza

- V této oblasti je vhodné využívat SIEM systémy pro sledování logů a analýzu bezpečnostních událostí,
- zpracovávat zpětnou vazbu od zaměstnanců, administrátorů a bezpečnostních týmů,
- vyhodnocovat vývoj počtu bezpečnostních incidentů po implementaci opatření.

11.4 Interní a externí audity

V podniku je také vhodné provádět pravidelné interní kontroly nastavení procesů a opatření.

- Externí audity bezpečnostních opatření nezávislými odborníky,
- ověřování shody se standardy ISO/IEC 27001, NIST Cybersecurity Framework, CIS Controls. případně dalšími vhodnými.

11.5 Kontinuální zlepšování

Jako i v jiných bodech uvedených v předešlém textu, i zde je také doporučováno použít metodiku založenou na PDCA cyklu (Plan – Do – Check - Act), což je cyklus pravidelného ověřování, vyhodnocování a následně změn již zavedených opatření. Je tedy vhodné:

- Na základě získaných výsledků upravovat opatření tak, aby odpovídala aktuálním hrozbám,
- implementovat nové technologie, které mohou zvýšit úroveň ochrany,
- školit zaměstnance v oblasti kybernetické bezpečnosti, aby zavedená opatření správně dodržovali.

ZÁVĚR

Tato práce je zaměřena na podnik střední velikosti spadající do režimu nižších povinností a cílem bylo podat základní informaci nově regulovaným subjektům o tom, jak v nově vzniklé situaci postupovat a jak se pokusit předpokládané nemalé finanční náklady alespoň rozdělit na delší časové období.

V kontextu nového zákona o kybernetické bezpečnosti je zřejmé, že regulace poskytování služeb v digitálním prostředí přinese v ČR nově cca 6 000 dosud neregulovaným subjektům náklady na implementaci zákonných požadavků, které dle kvalifikovaných odhadů mohou dosahovat celkové výše blíží se 100 miliardám korun.

Bezpečnostní opatření poskytovatelů regulovaných služeb se mohou stát základním pilířem ochrany před kybernetickými hrozbami, analýzy rizik prováděné na základě interních auditů umožňují identifikaci slabých míst a mohou stanovit kroky k jejich eliminaci. Organizační opatření zaměřená na snižování úrovně rizik mohou hrát zásadní roli ve strategii prevence, zatímco technická opatření mohou představovat konkrétní technologická řešení pro ochranu informačních aktiv.

Praktická implementace opatření v podniku, aby byla efektivní, by měla být ovšem systematická, přičemž klíčovým faktorem je pravidelné monitorování a vyhodnocování účinnosti zavedených bezpečnostních prvků. Metody pro vyhodnocování efektivity opatření jsou nezbytné nejen pro samotné zajištění kybernetické bezpečnosti, ale také pro její dlouhodobé udržení a adaptaci na nové typy hrozeb.

Přesto, že požadavky na implementaci zákonných opatření jistě přinesou zvýšení ochrany informačních systémů, mohou pro menší podniky znamenat významný zásah do jejich fungování a do celkové ekonomické situace. Povinnosti a lhůty poskytovatelů služeb nově definují jasné mantinely pro jejich zavádění a další finanční hrozbou pro menší podniky jsou sankce za přestupky a systém pokut v případě neplnění zákonných požadavků a nedodržování zákonných regulací.

Celkově lze říci, že kybernetická bezpečnost je dynamický proces, který vyžaduje neustálou pozornost, inovaci a spolupráci mezi regulátory, poskytovateli služeb a uživateli. Úspěšná implementace bezpečnostních opatření bude představovat právní povinnost, ale také významný krok ke kybernetické ochraně podniků a organizací v současném digitalizovaném světě. Nutnost nedobrovolných investic do rekonstrukce síťové infrastruktury, která ze zákona fakticky vyplývá a kteréžto zákon vlastně podnikům nařizuje, ovšem menším podnikům na finančním zdraví rozhodně nepřidá.

SEZNAM POUŽITÉ LITERATURY

- [1] EVROPSKÁ UNIE. *Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*. Online. 2022. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555&from=CS> [cit. 2025-03-01]
- [2] POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY. *Vládní návrh zákona o kybernetické bezpečnosti - EU, Sněmovní tisk 759/0*. Online. 2024. Dostupné z: www.psp.cz/sqw/text/tiskt.sqw?O=9&CT=759&CT1=0 [cit. 2025-04-26]
- [3] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Průvodce novým zákonem o kybernetické bezpečnosti*. Online. 2025. Dostupné z: <https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti> [cit. 2025-05-26]
- [4] LUPA.CZ. *Sněmovna schválila nová pravidla kybernetické bezpečnosti, zakazovat dodavatele bude moci vláda*. Online. 2025. Dostupné z: www.lupa.cz/aktuality/snemovna-schvalila-nova-pravidla-kyberneticke-bezpecnosti-zakazovat-dodavatele-bude-moci-vlada [cit. 2025-04-26]
- [5] POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY. *Vládní návrh zákona o kybernetické bezpečnosti - EU, Sněmovní tisk 759/0*. Online. 2024. Dostupné z: www.psp.cz/sqw/historie.sqw?o=9&t=759 [cit. 2025-05-27]
- [6] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Návrhy prováděcích právních předpisů*. Online. 2025. Dostupné z: <https://portal.nukib.gov.cz/pruvodce-novym-zaknem-o-kyberneticke-bezpecnosti/navrhy-provadecich-pravnich-predpisu> [cit. 2025-05-26]
- [7] SENÁT PČR. *Senátní tisk č. 109*. Online. 2025. Dostupné z: www.senat.cz/xqw/xervlet/pssenat/historie?action=detail&value=5456 [cit. 2025-05-26]

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

802.1X	protokol umožňující zabezpečení přístupu do počítačové sítě
API	Application programming interface
ARP	Address Resolution Protocol
CEN	Evropský výbor pro normalizaci
ČSN	Česká státní norma
DHCP	Dynamic Host Configuration Protocol
EN	Evropská norma
FIPS	Federal Information Processing Standards
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technologies
IDPS	Intrusion Detection Protection System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Informační technologie
KPI	Key performance indicator
MAC	Media Access Control
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PGP	Pretty good privacy
PS PČR	Poslanecká sněmovna Parlamentu ČR
RPJ	Roční pracovní jednotka
S/MIME	Secure/Multipurpose Internet Mail Extensions
SIEM	Security Information and Event Management
SSL	Secure socket layer
SQL	Structured query language
TLS	Transport Layer Security
THP	technicko-hospodářský pracovník
XSS	Cross site scripting

SEZNAM PŘÍLOH