Kybernetická bezpečnost s implementací GDPR ve vybraných organizacích

Bc. Ondřej Moravec

2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Ondřej Moravec**
Osobní číslo:	**A17265**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Kybernetická bezpečnost s implementací GDPR ve vybraných organizacích**
Téma anglicky:	**Cybernetic Security with GDPR Implementation in Selected Organisations**

Zásady pro vypracování:

1. **Pojednejte o současném stavu kybernetické bezpečnosti v České republice.**
2. **Analyzujte obecné nařízení o ochraně osobních údajů.**
3. **Stanovte kontext využití obecného nařízení o ochraně osobních údajů s uplatněním kybernetické bezpečnosti.**
4. **Analyzujte vybraný subjekt v souvislosti s požadavky na ochranu osobních údajů.**
5. **Vypracujte návrh opatření pro zvýšení kybernetické bezpečnosti pro vybraný subjekt.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **NULÍČEK, M., DONÁT J., a kolektiv. GDPR / Obecné nařízení o ochraně osobních údajů (2016/679/EU). Wolters Kluwer ČR, 2017. ISBN 978-80-75527-65-3.**
2. **ŽÚREK, Jiří. Praktický průvodce GDPR. ANAG, 2017. ISBN 978-80-75540-97-3.**
3. **Council of the European Union. European Council. 2015. Dostupné : http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.**
4. **General Data Protection Regulation, Evropská komise. 2016. Dostupné z:http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.**
5. **Paul, von dem Bussche, Axel. The EU General Data Protection Regulation (GDPR). Springer International Publishing. 2017. ISBN 978-3-319-57958-0.**
6. **CALDER, Alan, EU GDPR: A Pocket Guide. IT Governance Publishing. 2016. ISBN: 978-184928831.**

Vedoucí diplomové práce: **doc. Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **30. listopadu 2018**

Termín odevzdání diplomové práce: **17. května 2019**

Ve Zlíně dne 14. prosince 2018

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Diplomová práce na téma „Kybernetická bezpečnost s implementací GDPR ve vybraných organizacích“ pojednává v teoretické části o kybernetické bezpečnosti v České republice ve vazbě na předmětnou legislativu a popisuje kybernetickou bezpečnost v Evropské unii. Blíže charakterizuje pojem GDPR a důvod jeho zavedení. Jsou zde popsány přístupy a metody analýzy rizik, se kterými bude dále pracováno v praktické části.

V praktické části je věnována pozornost kybernetické bezpečnosti a GDPR vy vybraných organizacích. Jsou zde popsány firemní struktury. Poté jsou vymezeny bezpečnostní hrozby vybraných firem a na základě zvolených hrozeb realizovány analýzy rizika. Následně byly vytvořeny GAP analýzy systému řízení bezpečnosti informací a poté na samotné GDPR vy firmách. Na základě vyhodnocených GAP analýz byly navrženy vhodná opatření.

Klíčová slova: Obecné nařízení o ochraně osobních údajů, informační bezpečnost, kybernetická bezpečnost, analýza rizik, GAP analýza, KARS analýza

ABSTRACT

Diploma thesis on topic "Cyber Security with Implementation of GDPR in selected organizations" deals with cyber security in the Czech Republic in relation to the legislation in question and describes cyber security in the European Union. It characterizes the term GDPR and the reason for its introduction. There are described approaches and methods of risk analysis, which will be further worked in the practical part.

In the practical part, attention is paid to cyber security and GDPR by selected organizations. The security threats of selected companies are defined and risk analyzes are carried out on the basis of selected threats. Subsequently they were created GAP analysis on ISMS and GDPR and then create the appropriate measures.

Keywords: General Data Protection Regulation, Information Security, Cyber Security, risk analyse, GAP analyse, KARS analyse

PODĚKOVÁNÍ

Děkuji panu Ing. Martinovi Hromadovi, Ph.D. při vedení diplomové práce za odborné rady, věcné připomínky a vstřícnost při konzultacích a vypracování diplomové práce, které mi pomohly tuto práci zkompletovat. Dále bych chtěl poděkovat mé rodině, kteří mě při vytváření této práce podpořili.

"Never give up, because when you think it's all over, is the moment where everything starts."

(Jim Morrison)

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

OBSAH

ÚVOD

Kybernetická bezpečnost patří mezi základní přístupy k bezpečnosti dnešní moderní doby, kdy je v podstatě vše řízeno pomocí informačních technologií propojených internetovým propojením. Doba se rychle vyvíjí a je nezbytné na nové trendy adekvátně reagovat vhodnými opatřeními, jako je tomu u ochrany citlivých dat fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů neboli GDPR.

Téma této diplomové práce se zabývá problematikou kybernetické bezpečnosti v souladu s účinností GDPR ve vybraných organizacích. GDPR je účinná od 25. 5. 2018, kdy zároveň došlo k novelizaci Zákona č. 101/2000 Sb., o ochraně osobních údajů. Celé GDPR se dá chápat jako ucelený soubor pravidel na ochranu dat na území Evropské unie a případné poskytování těchto informací mimo EU.

V teoretické části je věnována pozornost současnému stavu kybernetické bezpečnosti v České republice a GDPR, které má přidanou hodnotu ke kybernetické bezpečnosti. V první kapitole bude popsán vývoj a chápání kybernetické bezpečnosti až po aktuální stav. Bude popsána Národní strategie kybernetické bezpečnosti pro Českou republiku, která řeší základní strategii bezpečnosti v kybernetickém prostředí a budou popsány zákony, patřící do kybernetické bezpečnosti. V rámci vztahů s EU bude popsána směrnice Network and Information Security, jejímž hlavním účelem je zvýšit kybernetickou ochranu pro členské státy EU. Druhá kapitola se zabývá GDPR jako přidanou hodnotou kybernetické bezpečnosti. Třetí kapitola bude pojednávat o hrozbách ve formě katalogu hrozeb pro kybernetickou bezpečnost a poté budou prezentovány konkrétní metody pro analýzu rizik, se kterými se bude pracovat v praktické části. Poslední kapitola teoretické části se bude zabývat východisky a opatřeními kybernetické bezpečnosti s vazbou na GDPR.

Cílem praktické části bude analýza, která pojedná o skutečnosti, zda po roce fungování GDPR sledované firmy nastavily svoji politiku na ochranu osobních údajů relevantně. Budou představeny vybrané společnosti a pro každou společnost bude vypracován katalog hrozeb a na základě takto zjištěných hrozeb bude vyhotovena KARS analýza, která určí, jaká rizika jsou pro daný systém „nejnebezpečnější“. Dále bude realizován návrh analýzy systému řízení bezpečnosti informací a GDPR formou GAP analýzy, kterou by firmy měly vyplnit na základě předložených a zjištěných skutečností. Poté dojde k vyhodnocení GAP analýzy a bude navržena forma minimalizace rizik na přijatelnou úroveň. Poslední kapitola se bude zabývat návrhy opatření pro praktické zvýšení kybernetické bezpečnosti.

I. TEORETICKÁ ČÁST

1 SOUČASNÝ STAV KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE

Kapitola pojednává o současném stavu kybernetické bezpečnosti České republiky a charakterizuje její vývoj a chápání až po aktuální stav. V kapitole je věnovaná pozornost terminologickému vymezení pojmů, které jsou pojeny s kybernetickou bezpečností a které budou zmiňovány v této diplomové práci.

Dále je zde popsáno nařízení Evropské unie NIS (Network Information Security), které má vazbu na kybernetický zákon a jehož hlavním cílem je zvýšení kybernetické ochrany členských států, harmonizace právní úpravy a vytvoření jednotného standartu v kybernetické bezpečnosti. V kapitole je popsáno rozdělení subjektů, a to v souvislosti s provozovateli základní služby a poskytovateli digitální služby.

Poté je rozepsán strategický dokument s názvem Národní strategie kybernetické bezpečnosti ČR na období let 2015 až 2020, kde jsou více rozebrány vize, principy a výzvy. Následuje popis funkce, která spočívá ve zvolených zásadách, které chce Česká republika splnit během pěti let. Uvádí se a diskutuje o nedostatečném zabezpečení malých a středních podniků v kyberprostoru apod.

Konec kapitoly rozepisuje právní rámec kybernetické bezpečnosti spolu s kybernetickým zákonem a jím spojenými vyhláškami.

1.1 Kybernetická bezpečnost v České republice

Kybernetická bezpečnost je také známá pod pojmem informační bezpečnost. Spadají do ní všechna technická zařízení, jako jsou počítače, mobily, tablety, kamery, tiskárny a další zařízení, která mohou být pachatelem zneužita [1].

Kybernetická bezpečnost je mimo jiné pojena s kybernetickou kriminalitou. Jedná se o protiprávní činnost, kde hlavním cílem útoků je technické zařízení. Pachatele je obtížné dopátrat, jelikož útoky často bývají přesměrovány z jiných serverů [2].

1.1.1 Vývoj kybernetické bezpečnosti v České republice

Za počátek a impulz, kdy se začala brát kybernetická bezpečnost v České republice více na vědomí, se dá považovat summit NATO, konaný v Praze v roce 2002, kde bylo upozorněno na potřebu posílit kybernetickou obranu a ochranu informační a komunikační technologie (ICT systémů) [1].

S rostoucím počtem kybernetických útoků byl v roce 2008 vydán dokument Cyber Defense Policy, který řeší, jak by členské státy NATO měly reagovat na kybernetické útoky a je zde kladen důraz na centralizovanou kybernetickou ochranu [1].

V České republice mělo kybernetickou ochranu v kompetenci Ministerstvo informatiky, které fungovalo až do roku 2007, kdy bylo sloučeno s Ministerstvem vnitra. Toto sloučení neumožnilo naplnit závazky pro kybernetickou bezpečnost, proto bylo v roce 2011 vytvořeno Národní centrum kybernetické bezpečnosti, které zesílilo svůj potenciál za pomoci sjednocení CZ.NIC a Národního bezpečnostního týmu CSIRT.CZ. Tomu předcházelo schválení „Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011–2015“ a „Akčního plánu opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011–2015“ [1].

Čím větší hodnotu informace mají, tím by měla být věnována větší pozornost jejich zabezpečení a zvolena vhodná bezpečnostní opatření. V České republice toto ošetřuje legislativa v podobě Kybernetického zákona a Evropské normy pro zajištění kolektivní ochrany a Evropské kritické infrastruktury.

1.1.2 Chápání kybernetické bezpečnosti

Všeobecné chápání kybernetické bezpečnosti v České republice je upravováno zákonem o kybernetické bezpečnosti č. 181/2014 Sb. S pomocí tohoto zákona je možné u vybraných subjektů odhalovat jejich slabiny, ale zároveň zajistit reálnou schopnost detekce pokročilých hrozeb v budoucnu.

V rámci chápání kybernetické bezpečnosti se musí brát na vědomí, že kybernetický prostor nezná hranic a útoky od útočníků mohou přicházet odkudkoliv. Vyspělé země vnímají tento trend jako významnou hrozbu a připravují vhodnou právní úpravu a rámec. Ale pouze vydání relevantních institucionálních nástrojů nestačí, jelikož se může stát, že než dojde k vydání platného zákona, technologie může pokročit a daná legislativa se může stát neúčelnou.

1.1.3 Princip kybernetické bezpečnosti

Primární princip kybernetické bezpečnosti spočívá v nastavení jistoty k zajištění zabezpečeného, chráněného a odolného kyberprostoru za účelem zajištění dostupnosti, důvěrnosti a integrity dat.

Pokud dojde k narušení kyberprostoru, může hrozit neautorizovaná manipulace či získání přístupu do databází, jejichž obsah je existenčně důležitý pro fungování společnosti.

1.1.4 Terminologie

Aktivum – je vše co má pro vlastníka hodnotu.

Analýza hrozeb – zkoumání činnosti, která může negativně ovlivnit kvalitu služby IT.

Analýza rizik – proces, u kterého se chápe povaha rizika a zároveň je zvolena vhodná úroveň rizika.

Bezpečnost dat – počítačová bezpečnost aplikovaná na data.

Bezpečnostní audit – nezávislé testování činností, přičemž se zkoumá a identifikuje aktuální stav procesů a opatření k detekování narušení bezpečnosti a současně přináší návrhy jakýchkoliv indikovaných změn pro řešení. Dělí se na externí nebo interní.

Bezpečnostní incident – za bezpečnostní incident je považována hrozba při porušení bezpečnostní politiky, zásad anebo standartních pravidel provozu, například neoprávněný přístup k informacím nebo datům.

Bezpečnostní událost – je taková událost, která svým způsobem vede k narušení informačních systémů a technologií, které jsou nastaveny pro její ochranu.

Bezpečnostní zranitelnost – je úmyslná chyba anebo chyba v softwaru, která může být zneužita útočníkem.

Dostupnost – informace jsou dostupné pouze osobám, které mají oprávnění, případně jsou dohledatelné pomocí prostředků jako je např. internet.

Důvěrnost – dané informace nejsou dostupné neoprávněným jednotlivcům či určitým procesům.

Integrita dat – jistota, že data nebyla změněna.

Kritická informační infrastruktura – informační a komunikační systémy, které při nefunkčnosti mohou způsobit dopad na bezpečnost státu.

Kritická infrastruktura – služby, které jsou důležité pro chod státu a při narušení stability by mohly mít významný dopad na bezpečnost státu, jeho ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.

Kybernetická bezpečnost – opatření pro zajištění ochrany kybernetického prostoru.

Kybernetický prostor – digitální prostředí, ve kterém vzniká a probíhá výměna informací pomocí sítí elektronických komunikací [3].

1.2 Směrnice Network and Information Security

Kybernetický zákon funguje ve vazbě na směrnici NIS (Network and Information Security)

Hlavním účelem této směrnice je zvýšit kybernetickou ochranu pro členské státy, harmonizovat právní úpravu a zároveň vytvořit jednotný standart v kybernetické bezpečnosti. České republiky se tato směrnice prakticky nedotkla, jelikož už byl vytvořen kybernetický zákon a došlo pouze k novelizaci tohoto zákona [4].

Mezi hlavní přínosy Směrnice patří rámec pro vytvoření mezinárodní spolupráce pro účely snadnější výměny informací mezi členskými státy. Dále ukládá členským státům povinnost vytvořit příslušné orgány, které se zabývají kybernetickou bezpečností [5].

Směrnice NIS charakterizuje subjekty na provozovatele základní služby a poskytovatele digitální služby. V následující části budou tyto subjekty detailněji popsány [6].

1.2.1 **Provozovatel základní služby**

Provozovatel základní služby je orgán nebo osoba, která se zabývá fungováním společenských a ekonomických činností a zároveň je závislá na sítích nebo informačních systémech pro poskytování základních služeb. Za službu je brána jakákoli služba informační společnosti, převážně poskytována za určitou finanční částku [4].

Narušení těchto sítí a služeb by mohlo mít negativní dopad na činnosti následujících odvětví:

- **Energetika** – elektřina, ropa, zemní plyn
- **Doprava** – letecká doprava, železniční doprava, vodní doprava, silniční doprava
- **Bankovnictví**
- **Infrastruktura finančních trhů** – regulovaný trh
- **Zdravotnictví** – poskytovatelé zdravotní péče
- **Rozvody pitné vody** – dodavatel a distributor
- **Digitální infrastruktura** – výměnné uzly internetu, poskytovatelé služeb systému doménových jmen, rejstříky internetových domén nejvyšší úrovně [4]

1.2.2 Poskytovatel digitální služby

Poskytovatelé digitální služby jsou rozděleny do tří kategorií:

- **On-line tržiště** – umožnuje uzavírat on-line smlouvy prostřednictvím internetových stránek. Za on-line tržiště nelze brát stránky, které klienta přesměrují na další stránku.
- **Internetový vyhledávač** – umožňuje realizovat vyhledávání na všech stránkách, a to za pomocí zvoleného dotazu uživatele. Pomocí klíčových slov klient získá odkaz, na kterém by se mohl nacházet požadovaný obsah.
- **Cloud computing** – jedná se o digitální službu, umožňující přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, které lze sdílet [7].

1.3 Národní strategie kybernetické bezpečnosti ČR na období let 2015 až 2020

Národní strategie kybernetické bezpečnosti pro Českou republiku je bezpečnostní dokument, který řeší základní strategie bezpečnosti v kybernetickém prostředí.

Součástí strategie jsou vize, ve kterých je popsáno, které zásady si Česká republika stanovila jako priority. Klíčové body a cíle jsou popsány v principech a výzvách pro dané období.

1.3.1 Vize strategie kybernetické bezpečnosti

V dokumentu jsou stanoveny vize v podobě bodových úseků, které jsou stanoveny jako prioritní oblasti, kterých by mělo být dosaženo do roku 2020. Skládají se z devatenácti konkrétních bodů. Vzhledem k jejich rozsahu jsou v této podkapitole rozepsány pouze ty nejdůležitější z nich.

V dokumentu je kladen důraz na schopnost čelit nejnovějším kybernetickým hrozbám a rozvoji bezpečnostních složek státu za účelem včasného předcházení hrozbám v kyberprostoru. Dále je kladen důraz na to, aby Česká republika v rámci všech organizací, kterých je členem, patřila mezi organizace na přední příčce kybernetické bezpečnosti v rámci Evropy. Kolektivní obrana Severoatlantické aliance s mezinárodními partnery klade důraz na partnerství a plnění závazků z něho vyplývajících. Zajištění kritické informační infrastruktury jako hlavního prvku ochrany a bezpečnosti sítí a kyberprostoru podmiňuje nastavením nejvyššího zabezpečení [8].

1.3.2 Principy strategie kybernetické bezpečnosti

V principech je rozepsána ochrana základních lidských práv, svobod a principů demokratického právního státu, ve kterém je kladen důraz na dodržování svobody projevu, ochranu osobních dat a soukromí občanů a otevřenost přístupu k informacím. Budování důvěry a spolupráce mezi veřejným a soukromým sektorem a občanskou společností je vázáno na fakt, že kyberprostor je převážně v rukou soukromého sektoru a mezi těmito sektory by proto měla být pravidelná spolupráce. Česká republika se snaží o rozvoj kapacit k zajišťování kybernetické bezpečnosti, podporuje a navyšuje investice do výzkumu a vývoje v oblasti kybernetické bezpečnosti. Jednou z priorit je i posílení kooperace mezi orgány činnými v trestním řízení [8, 9].

1.3.3 Výzvy strategie kybernetické bezpečnosti

Mezi hlavní výzvu pro Českou republiku lze považovat skutečnost, že by Česká republika mohla sloužit jako testovací země, která by používala bezpečnostní technologie podobných států, což by umožnilo odhalit nedostatky vybraných bezpečnostních aspektů. Povědomí o vzrůstajícím počtu uživatelů internetu, informačních a komunikačních technologií by mohlo vést k nárůstu kritičnosti a výskytu selhání. A podobně je tomu u nárůstu mobilních zařízení, která nejsou chráněna, což zvyšuje pravděpodobnost mobilního malware. V potaz je brána změna protokolu IPv4 na IPv6. V této souvislosti se šíří i povědomí o nedostatečném zabezpečení malých a středních podniků v kyberprostoru.

Ve státním sektoru se bere za hrozbu i nevědomí vzrůstající závislosti obranných složek státu na informačních a komunikačních technologiích, čímž se zvyšují rizika dopadu na schopnost efektivně reagovat na hrozby v kyberprostoru [8, 9].

1.3.4 Právní rámec kybernetické bezpečnosti

Hlavním orgánem v oblasti kybernetické bezpečnosti v České republice je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) se sídlem v Brně. Jeho hlavním úkolem je provádění kontrolní činnosti a metodické podpory, jako je vydávání podpůrných materiálů a doporučení, týkající se problematiky kybernetické bezpečnosti.

Vláda ČR může pověřit NÚKIB provedením analýzy stavu kybernetické bezpečnosti. Tento úřad má na starost také typový plán narušení bezpečnosti kritické informační infrastruktury. S dozorem nad kybernetickou bezpečností se často pojí pojmy CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team) [8, 9].

1.3.5 **Kybernetický zákon**

V České republice platí zákon č. 181/2014 Sb. o kybernetické bezpečnosti, který upravuje práva a povinnosti osob i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Jeho hlavním úkolem je zvýšit bezpečnost kybernetického prostoru.

Hlavním cílem je nastavení pravidel spolupráce mezi soukromým sektorem a veřejnou správou, stanovení základní úrovně bezpečnostních opatření, zlepšení detekce kybernetických bezpečnostních incidentů, zavedení procesu hlášení kybernetických bezpečnostních incidentů a systémů pro opatření k reakci. Dalším hlavním záměrem je stanovení role Národního bezpečnostního úřadu, kterému je svěřena konkrétní pravomoc v oblasti kybernetické bezpečnosti [10].

1.3.6 **Vyhláška č. 82/2018 Sb.**

Jedná se o nejnovější vyhlášku, která pojednává o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. Nahrazuje vyhlášku č. 316/2014 Sb., o kybernetické bezpečnosti, která byla nabytím účinností vyhlášky č. 82/2018 Sb. zrušena.

Předmětná vyhláška rozšiřuje okruh povinných osob a mění požadavky na ně a dále upravuje následující body:

a) obsah a strukturu bezpečnostní dokumentace,

b) obsah a rozsah bezpečnostních opatření,

c) typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,

d) náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,

e) náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,

f) vzor oznámení kontaktních údajů a jeho formu a

g) způsob likvidace dat, provozních údajů, informací a jejich kopií.[1] [11]

[1] [11] Vyhláška č. 82/2018 Sb., vyhláška o kybernetické bezpečnosti § 1

1.3.7 **Vyhláška č. 437/2017 Sb.**

Tato vyhláška zapracovává příslušný předpis Evropské unie, upravuje odvětvová a dopadová kritéria pro určení provozovatele základní služby a vymezuje významnost dopadu narušení základní služby v rámci zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1 zákona o kybernetické bezpečnosti [12].[2]

1.3.8 **Vyhláška č. 317/2014 Sb.**

Vyhláška o významných informačních systémech a jejich určujících kritériích, stanovuje významné informační systémy a jejich určující kritéria [13].

Náplní a ambicí kapitoly bylo objasnit současný stav kybernetické bezpečnosti České republiky a popis jeho vývoje až do aktuálního stavu. Byl popsán terminologický slovník často se vyskytujících pojmů v odborné literatuře a v této diplomové práci.

Bylo rozepsáno nařízení Evropské unie NIS, které má vazbu na kybernetický zákon a má za úkol harmonizovat právní úpravu a vytvořit jednotný standart v kybernetické bezpečnosti pro členské státy Evropské unie. Byly zde rozepsány subjekty jako provozovatelé základní služby a poskytovatelé digitální služby.

Byl popsán strategický dokument s názvem Národní strategie kybernetické bezpečnosti ČR na období let 2015 až 2020, kde jsou více rozebrány vize, principy a výzvy.

Závěrečná část patřila právním aspektům kybernetické bezpečnosti, jako je kybernetický zákon spolu s vyhláškami, týkajícími se problematiky kybernetické bezpečnosti v České republice.

[2] [12] Vyhláška č. 437/2017 Sb., vyhláška o kritériích pro určení provozovatele základní služby § 1

2 OBECNÉ NAŘÍZENÍ O OCHRANĚ FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ JAKO PŘIDANÁ HODNOTA KYBERNETICKÉ BEZPEČNOSTI

Kapitola pojednává o evropském nařízení General Data Protection Regulation (dále jen GDPR) o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, které se týká členských států Evropské unie. Samostatné GDPR nedefinuje, jak se má postupovat, ale co má být uděláno pro nakládání s daty.

Celé GDPR poté má přidanou hodnotu ke kybernetické bezpečnosti, z toho důvodu, že pro její naplnění je třeba splnit požadavky dané nařízením, např., aby každá firma měla správce a zpracovatele dat, nebo prováděla pseudonymizaci dat.

V případě nedodržení podmínek nařízení GDPR hrají hlavní roli sankce, které jsou děleny do dvou kategorií a jejichž hlavním účelem je donutit společnosti plnit toto nařízení.

2.1 Obecné nařízení o ochraně osobních údajů

GDPR začala svoji účinnost dnem 25. května 2018 a reaguje na původní směrnici EU o ochraně osobních údajů – Směrnice č. 95/46/ES [14]. Skládá se z 99 článků.

GDPR samo o sobě vede k zpřísnění automatizovaného zpracování osobních údajů a ochrany jednotlivců. Nahrazuje stávající zákon č.101/2000 Sb., o ochraně osobních údajů. Nástup GDPR byl podmíněn skutečností, že současná technologie postoupila kupředu a zpracování osobních údajů a zároveň jejich volný pohyb přestal splňovat očekávání v rámci bezpečnosti. GDPR se týká všech, kteří jakýmkoliv způsobem sbírají osobní údaje zákazníků, jak pro své klientské databáze, tak i například pro zasílání newsletterů [15].

Úřad pro ochranu osobních údajů v Česku byl vytvořen 1. června 2000 jako správní orgán, který představil zákon č. 101/2000 Sb., o ochraně osobních údajů, který platil až do nabytí platnosti GDPR [14].

2.1.1 **Osobní údaj**

Za osobní údaj se považuje jakákoliv informace, pomocí které se dá identifikovat fyzická osoba, což je např. jméno, příjmení, rodné číslo, bydliště, datum narození, věk, e-mailová adresa, IP adresa, videozáznam, telefonní číslo, číslo řidičského průkazu, číslo cestovního pasu, číslo kreditní karty, fotografický záznam, příjem ze zaměstnání apod [16].

2.1.2 Zvláštní kategorie osobních údajů

GDPR dělí osobní údaje na zvláštní kategorie, a to z toho důvodu, že by mohly být některé osoby poškozeny či diskriminovány jak ve společnosti, tak i v zaměstnání. Údaje by měly být zpracovávány jen v zvláštních a jasně stanovených případech.

Z takových údajů by se dal určit rasový původ, politické názory, náboženské vyznání, filozofické přesvědčení, členství v organizacích, zpracování genetických či biometrických údajů, zdravotní stav, sexuální život anebo orientace [17].

2.1.3 Souhlas

Souhlas se zpracováním osobních údajů musí být založen na svobodné vůli a dotyčná osoba musí být informována o tom, že s těmito informacemi bude nadále zacházeno. Musí být zřejmé, že osoba ze své svobodné vůle potvrdila souhlas se zpracováním údajů, např. na internetu, což je aplikováno zaškrtnutím políčka na příslušné stránce. Daná osoba má právo na odvolání souhlasu kdykoliv, bez udání důvodu, a správce je povinen tato data vymazat. Samotná délka souhlasu není stanovena a je třeba brát v potaz, na co byl původní souhlas udělen [18].

U dětí platí jiná pravidla na zpracování údajů. V GDPR jsou děti chápany jako osoby mladší 16 let. Pro zpracování jejich údajů je zapotřebí souhlas rodičů. V případě, kdy dítě nemá rodiče, je potřebný souhlas osoby, která vykonává rodičovskou zodpovědnost. Hlavním důvodem je to, že děti si nemusí být vědomy rizik a důsledků, plynoucích ze zpracování jejich osobních údajů. Problémem s udělením souhlasu rodičů může nastat v případě, kdy nedojde k názorové shodě obou rodičů [19].

Jednotlivé státy Evropské unie mohou pro souhlas dítěte schválit i nižší věk než 16 let, ale nesmí přesáhnout 13 let. V České republice je občan veden jako dítě až do dosažení věku 15 let.

2.1.4 Správce a zpracovatel

Každému zpracování osobních údajů musí být přidělen správce, který odpovídá za dodržování pravidel GDPR. Za správce se stanoví fyzická či právnická osoba, orgán veřejné moci nebo agentura. Správce aplikuje dostatečná opatření, aby nedošlo ke ztrátě, zničení a zneužití osobních údajů a postupně monitoruje a kontroluje, jak zpracovávání dat probíhá [15].

Za zpracovatele je považován každý subjekt, který zpracovává osobní údaje. Provádí pouze takové operace, kterými ho pověřil správce. Zároveň platí, že správce nemůže být zpracovatelem [14].

2.1.5 **Pseudonymizace a automatizace údajů**

Pod pojmem pseudonymizace se rozumí proces, kdy každý konkrétní údaj má přiřazen svůj unikátní kód neboli pseudonym a je uchováván odděleně od databáze. To vede k většímu zabezpečení údajů. Pokud se neautorizovaná osoba dostane k databázi, nebude schopna identifikovat, koho se dané údaje týkají.

Pro automatizované zpracování údajů se používá výpočetní technika, aniž by došlo k zásahu ze strany pracovníků [14].

2.1.6 **Sankce**

Při porušení nařízení GDPR jsou stanoveny přísné peněžité tresty, které jsou rozděleny do dvou skupin. Sankce musí mít formu takovou, aby byly přiměřené a účinné a aby plnily funkci odrazující:

a) Pokuta může být vyčíslena do výše 10 000 000 euro, nebo do výše 2 % celosvětového ročního obratu, pokud se jedná o firmu.
b) Pokuta může být vyčíslena do výše až 20 000 000 euro, nebo do výše 4 % celosvětového ročního obratu, pokud se jedná o firmu [15].

2.2 Vztah GDPR a kybernetické bezpečnosti

GDPR má blízký vztah ke kybernetické bezpečnosti, jelikož většina údajů je uchovávána a zpracovávána pomocí technických zařízení. Narušení těchto zařízení za pomocí rozsáhlých hackerských útoků či sabotáži na pracovišti může vést k úniku informací. Jednou z priorit týkající se úschovy informací musí být stabilní bezpečnost sítě a zajištění stavu, kdy pravděpodobnost proniknutí k těmto údajům je na minimální úrovni.

Pro implementaci GDPR je požadováno, aby si firmy definovaly, za jakých okolností data uchovávají, a pro tento účel zajistily vhodné zabezpečení těchto informací. Proto musí aplikovat vhodnou analýzu pro zjištění stavu zabezpečení, např. GAP analýzu, a zjistit, jaká data jsou zpracovávána. Další variantou mohou být tzv. penetrační testy, které analyzují zranitelnosti IT infrastruktury a odolnost vůči neautorizovaným útokům.

Dalším krokem je relevantní reakce na analýzu a vytvoření vhodného návrhu řešení v oblasti informačních technologií.

V posledním stádiu by mělo dojít k přezkoumání, zda byly podchyceny všechny prvky a systém je zabezpečen. Ke zvolení vhodného opatření může pomoci certifikace ISO 27001, která popisuje, jak identifikovat a analyzovat rizika.

2.2.1 Nahlášení bezpečnostního incidentu

V případě porušení zabezpečení osobních údajů je správce povinen do 72 hodin tuto skutečnost nahlásit Úřadu pro ochranu osobních údajů a vypracovat záznam o bezpečnostním incidentu (elektronicky, za pomocí internetových formulářů anebo dopisem). Podle zákona č. 181/2014 Sb. se za bezpečnostní kybernetický incident považuje událost, která může způsobit narušení bezpečnosti informací a dostupnosti síťové infrastruktury. Jedná se nejčastěji o DoS útoky, skenování portů či samostatné útoky na uživatele jako jsou Phishing, e-mailové podvody apod [13].

Za bezpečnostní kybernetický incident není považováno to, že správce zjistí virus v počítači, zaměstnanec obdrží nevyžádanou poštu, dojde k odcizení výpočetní techniky s důležitými daty anebo zneužití přístupového jména a hesla [13].

Kapitola měla seznámit s nařízením GDPR jako přidanou hodnotou kybernetické bezpečnosti za podmínek jím stanovených, jako je například zpracovávání souhlasu fyzické osoby či určení povinností správcům a zpracovatelům. Celé GDPR se týká těch subjektů, které jakýmkoliv způsobem sbírají osobní údaje zákazníků a dále s daty pracují. V případě nedodržení podmínek nařízení GDPR udává přísné sankce, které mají funkci odrazující.

3 HROZBY A OBECNÉ ZÁSADY ANALÝZY RIZIK KYBERNETICKÉ BEZPEČNOSTI A GDPR

Celkové hrozby se mohou projevovat mnoha způsoby. Nejčastěji lze hovořit o vnějších a vnitřních hrozbách, které mohou ohrozit bezpečnost a stabilitu celého systému.

Základem pro správnou implementaci požadavků GDPR je detailní porovnání aktuálního stavu ochrany osobních údajů s požadavky definovanými nařízením, přičemž organizace by měla být povinna stanovit si kritéria pro určování, zda daná rizika mohou či nemohou být akceptovatelná. Je důležité si uvědomit hrozby, které mohou ohrozit samotný chod společnosti. K tomuto účelu by měl sloužit katalog hrozeb, ve kterém jsou definovány hrozby a četnost výskytu daných jevů. Katalog hrozeb pro vybrané firmy bude použit v praktické části.

Pro následnou identifikaci a předcházení těmto hrozbám slouží analýzy, které umožňují předcházet určitým vlivům. U GDPR jsou často zmiňované a doporučované DPIA analýza a GAP analýza, které jsou zaměřené na ochranu a zpracování osobních údajů. Mnohdy se analýzy provádějí tak, že simulují útok hackera případně záměrný útok od zaměstnanců. Příkladem takové analýzy je penetrační test.

3.1 Katalog hrozeb kybernetické bezpečnosti

Katalog hrozeb je sestaven na základě možných pravděpodobností výskytu určitých hrozeb na pracovišti, kde by mohlo dojít k ohrožení chodu celé společnosti či odcizení důležitých dat, jako jsou např. klientské databáze.

Vzhledem k zaměření práce bude dále diskutováno o detailnějším chápání kybernetických útoků s vazbou na GDPR.

3.1.1 Informační a počítačové hrozby

Mezi informačními a počítačovými hrozby často bývají zmiňovány určité malwary a ransomware. Jedná se o software, který má v sobě zabudovaný škodlivý kód, díky kterému pachatel může zneužít počítač pro poškození či sledování aktivity uživatele. Z napadeného počítače může vzniknout prostředek, který útočník využije pro šíření malwaru na jiné počítače. K odhalení Malware může pomoci výrazně vysoká spotřeba CPU a GPU a časté přehřátí zařízení. Toto mohou být první příznaky, signalizující přítomnost malware pro šifrování kryptogramů [21].

Dalším druhem informační hrozby je tzv. Phishing. Jde o kybernetické útoky, které jsou navrženy tak, aby bylo možno získat osobní údaje, jako jsou přihlašovací údaje a přístupová hesla. Většina útoku je řízená přes email a snaží se, aby napadený jednal pod tlakem a tudíž rychle [21].

3.1.2 Závady zařízení

Závadu zařízení lze brát za technickou závadu počítače, při které dojde k nefunkčnosti jednoho z prvků. To může mít za následek komplexní selhání systému či jeho funkčnosti a poté může dojít k zranitelnosti dat na daném technickém zařízení. Příkladem může být technická závada síťového rozhraní, selhání napájení, selhání aplikačního programového vybavení.

3.1.3 Komunikační hrozby

Komunikační hrozba může nastat v případě, kdy třetí strana zachytává datový provoz sítě, aniž by o tom uživatel věděl, případně vložením škodlivých programů, jako je např. malware.

3.1.4 Lidský faktor

Lidský faktor bývá nejčastějším faktorem poruch a závad. Například při nedodržení pracovních postupů na pracovišti či nevhodně stanovených pracovních postupech. Neznalost daného problému může být kritická v případě určitých hrozeb. Za hrozbu může být považován i zaměstnanec, který se snaží sabotovat bezpečnostní prvky.

3.1.5 Technická selhání

Mezi technické selhání lze zahrnout přerušení dodávky elektřiny či selhání záložních zdrojů napájení, při kterém by mohlo dojít k výpadku serverů či počítačů, či dlouhodobý výpadek internetového připojení a tím vzniklé omezení provádění prací nutných pro chod společnosti.

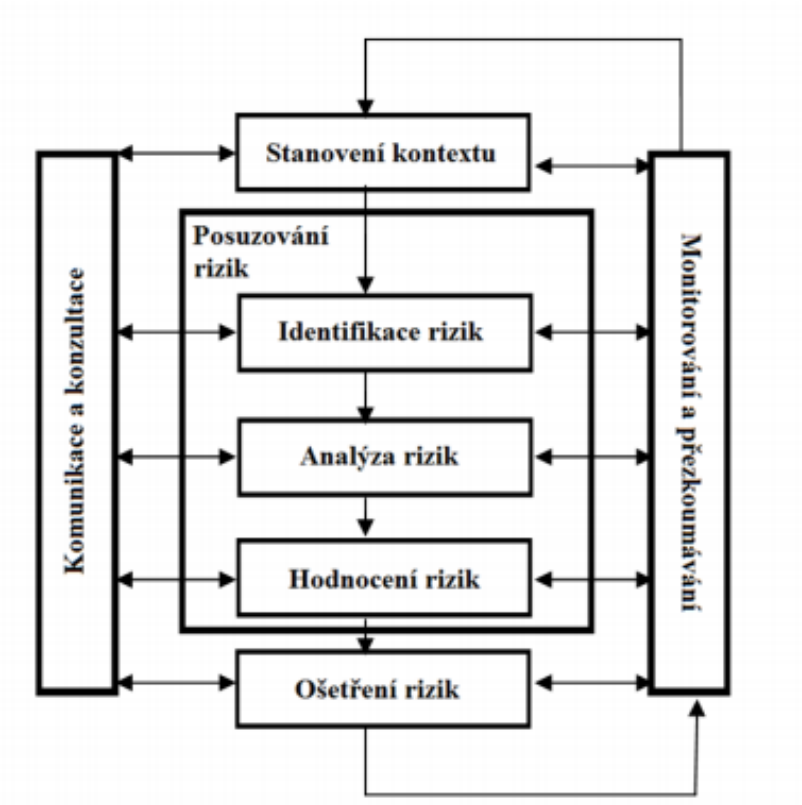
3.1.6 Logické hrozby

Mezi logické prvky se dá zařadit falšování uživatelské identity identifikovatelnými osobami či falšování uživatelské identity cizími osobami. Neoprávněné použití aplikací, které poté mohou zneužívat systémové prostředky nebo sloužit jako destruktivní a škodlivé programy.

3.2 Metody analýz rizik

Analýza rizik je spojena s nalezením možných pravděpodobností hrozeb a celkově se používá k identifikaci a eliminaci nalezených hrozeb. Existuje spousta analýz, jak tyto hrozby identifikovat, jako je what – if analýza, penetrační testy, DPIA, PHA, GAP analýza či kontrolní listy. Všechny zmiňované analýzy budou rozebrány v této kapitole.

Příkladem pro metody hodnocení rizik může být vytvořeno pomocí mezinárodní normy ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. Celé normy ISO 2700x jsou mezinárodně uznávané standardy, které slouží k zajištění bezpečnosti informací proti počítačovým podvodům a spolu s GDPR se zaměřují i na ochranu dat. Příkladem ISO 27001 je postaveno na třech činnostech, které jsou důvěrnost, integrita a dostupnost.



Obr. 1: *Proces řízení rizik* [39]

Na obrázku 1 je zobrazen postup při hodnocení rizik, který spočívá v identifikaci možných rizik, poté je potřeba provést vhodné analýzy rizik a poté provést ošetření, přičemž neustále musí probíhat konzultace daného problému při hodnocení rizik. Při zvládnutí rizika proces musí být neustále monitorován a přezkoumáván a případně musí být vypracováno nové hodnocení rizik.

3.2.1 Posouzení vlivu na ochranu osobních údajů (DPIA)

Data Protection Impact Assessment (DPIA) je prostředek, který se používá pro posouzení vlivu na ochranu osobních údajů a zpracovává se pouze tehdy, pokud je pravděpodobnost, že by mohlo vzniknut větší riziko porušení práva svobody fyzických osob. Celé posouzení vychází ze Článku 35 GDPR.

Obsahově by DPIA měla mít popsán účel a oprávněné zájmy. Zároveň musí být aplikována před zahájením zpracováním údajů. Měla by posuzovat nezbytnost a přiměřenost zpracování a rizika pro práva a svobody vlastníků údajů. V konečné části by měla obsahovat opatření, pomocí kterého dojde k odstranění nebo snížení zjištěných rizik. V případě zjištění vysokého rizika by jako výstup DPIA měla být vyhotovena dokumentace, ve které budou popsána vhodná opatření k minimalizaci nalezených rizik [23].

Za provedení DPIA jsou odpovědní správci údajů i v tom případě, kdy pověří jinou osobu či outsourcingovou službu. Při nevypracování DPIA analýzy může být subjekt pokutován do výše 10 mil. eur nebo do výše 2 % z celosvětového ročního obratu [24].

3.2.2 Penetrační testy

Penetrační testy se používají pro zjištění úrovně zabezpečení systémů, určených pro zpracování údajů a ověřují zranitelnost informačních systémů v organizaci, například u on-line obchodování anebo u portálů internetových bankovnictví, proti hackerským útokům.

Provádí se z toho důvodu, že většina společností používá pro zpracování údajů technické zařízení. Výstupem penetračních testů jsou podrobné informace o bezpečnostní situaci, upozornění na skutečné a pravděpodobné útoky, návrhy na opatření pro zvýšení bezpečnosti. Dělí se na externí a interní v závislosti na tom, kde by se předpokládaný útočník mohl nacházet [25].

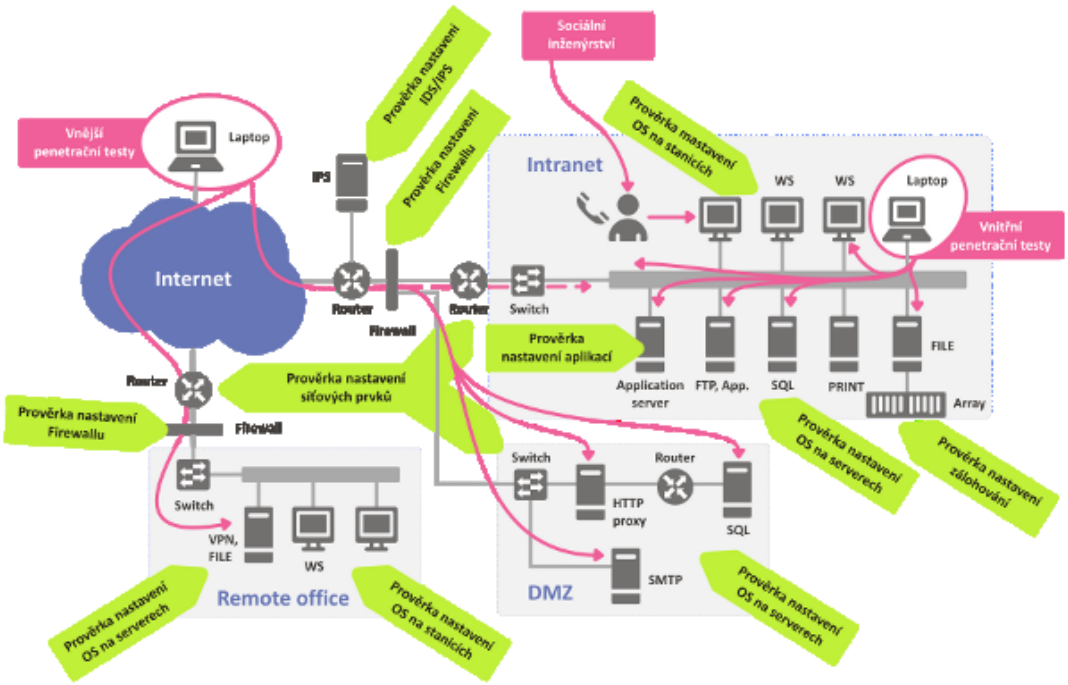
Celý test probíhá na základě vstupního plánování, kde se definují cíle a předmět testování. Poté se shromažďují informace o testovaném systému a identifikuje se jeho zranitelnost. Následně se provádí využití identifikované zranitelnosti [25]. Výsledkem je zpráva z testování s identifikovanými zranitelnostmi a jsou navržena optimální řešení pro eliminaci [26].

Celá struktura testování nemusí být vedena pouze jedním postupem testování. Celý postup může být vytvořen ve třech různých režimech. Mohou být provedeny následující testy:

Black-box – tester má přístup k testovanému prostředí bez sdělení jakýchkoliv informací o architektuře sítě. Tester simuluje útočníka z pohledu hosta nebo externího útočníka [26].

White-box – Testerovi byly sděleny podrobné informace o prostředí. Tester simuluje útočníka z pozice administrátora [26].

Grey-box – Jedná se o zkombinování předchozích režimů. Tester simuluje útok ze strany bývalého zaměstnance, partnera nebo dodavatele [26].



Obr. 2: *Způsoby provedení penetračních testů* [38]

3.2.3 GAP analýza

GAP analýza (označována také jako diferenční analýza) mapuje způsob zacházení s osobními údaji ve firmě v aktuálním stavu a v porovnání s ustanoveními GDPR. GAP analýza je dopadová analýza a nenahrazuje DPIA analýzu.

Výstup analýzy vytvoří poklad pro budoucí rozhodování, jaká opatření a v jakém časovém harmonogramu musí organizace přijmout a zároveň doporučí kroky, kterými by se organizace měla řídit v oblastech bezpečnosti, systému řízení ochrany osobních údajů, činností při zpracování osobních údajů, interních předpisů, řízení rizik třetích stran [27].

Implementace GAP analýzy je zdlouhavý proces, který zabere více než půl roku, a to primárně z důvodu měnících se trendů v IT řešeních. Délka implementace je také podmíněna přístupem zaměstnanců a jejich ochotou přijmout stanovená opatření.

3.2.4 What – If Analýza

What – if analýza (WFA) je analýza, která řeší události, pokud by nastaly, a ukazuje jejich budoucí následky. Jejím provedením se dá předejít hrozbám a rizikům. Její zpracování se řadí mezi ty jednoduší, ale za předpokladu, že na zodpovězení otázek a nalezení vhodných řešení bude spolupracovat tým expertů [28].

V GDPR a v rámci kybernetické bezpečnosti lze pokládat například otázky: Co se stane, když firmě budou odcizena data zákazníků. Co se stane, když zaměstnanec odcizí data. Co se stane, když firma neprovede pseudonymizaci údajů apod [28].

3.2.5 Předběžná analýza rizik – PHA

Předběžná analýza rizik (Preliminary hazard analysis) je analýza, která zkoumá všechna možná nebezpečí a náhodné události, které mohou vést k incidentu a zároveň hodnotí zjištěné nahodilé události podle jejich významnosti.

V GDPR by měla být uplatňována úvodní analýza informačních aktivit, a to převážně ve vztahu na připravenost před implementaci GDPR, kde se zjistí např. kde by mohlo dojít k problému se zpracováním osobních údajů a jak takovým jevům předcházet [29].

Cílem je nastavit číselné hodnoty pravděpodobnosti a dopadu rizik. Hodnoty se poté násobí a výsledky jsou rozděleny do kategorií vysoké úrovně rizika, nízké úrovně nebo zbytkové úrovně rizika. Příkladem předběžné analýzy je KARS analýza, která bere v potaz vzájemné působení rizik navzájem [29].

3.2.6 Audit a kontrolní listy

Před nástupem GDPR se doporučovalo provádět audit, díky kterému se dalo snadno zjistit, na jakou úroveň firmy splňují všechny nároky na bezpečnost dat. Za pomocí kontrolních listů se dají snadno odhalit chybějící části, zjistit odpovědné osoby a nalézt optimální řešení [30].

Výhodou těchto auditů je, že se dají provádět online a výsledkem je report, který popisuje chybějící či nevyhovující oblasti. Otázky jsou sestaveny za pomocí sebehodnotících dotazníků.

Kapitola měla obeznámit s hrozbami a teoretickými východisky analýzy rizik. Byl popsán katalog hrozeb za účelem detailnějšího chápání kybernetických hrozeb a útoků s vazbou na GDPR. Každý subjekt by měl mít implementovaný proces řízení a hodnocení rizik, který může být proveden za pomoci mezinárodních norem ČSN ISO/IEC 2700x. Prioritou subjektů by dále mělo být neustálé zlepšování prostředí v souladu s právními normami a předpisy. Subjekty by si měly jasně definovat a dokumentovat řadu základních bezpečnostních pravidel, procesů a rizik. Pro identifikaci, analýzu a hodnocení těchto rizik slouží celé spektrum metod. Pro účel kybernetické bezpečnosti a v souvislosti se zaměřením práce na GDPR byla popsána metoda DPIA, GAP analýza, What – if analýza, PHA, audit a kontrolní listy.

4 VÝCHODISKA A OPATŘENÍ KYBERNETICKÉ BEZPEČNOSTI S VAZBOU NA GDPR

Opatření kybernetické bezpečnosti na vazbu GDPR by mělo probíhat po vyhodnocení hrozeb a po vytvoření analýz pro kybernetickou bezpečnost a GDPR. Měla by být vybrána vhodná řešení, která eliminují budoucí ohrožení a zavádění bezpečnostních opatření. Problematika poté může nastat u GDPR, které nedefinuje, jaká opatření zvolit ze strany technické a organizační. Je tedy kladen důraz na správce, aby zavedli opatření, která splňují zásady a standarty ochrany pro práci s osobními údaji. ISO 27001 je vhodným prostředkem pro vytvoření politiky k minimalizaci bezpečnostních rizik.

Jelikož GDPR nedefinuje konkrétní technické prostředky na zvolení správné úrovně zabezpečení dat, je ISO 27001 vhodným prostředkem pro vytvoření politiky k minimalizaci bezpečnostních rizik. To, že se firma snaží splňovat požadavky na bezpečnost, se může následně kladně projevit ve vztahu k zákazníkům a dodavatelům [31].

U firem, které měly implementovanou normu ISO 27001, došlo k snadnějšímu přechodu na GDPR, protože ISO 27001 byla mnohokrát prezentována jako model, kterým je vhodné se řídit. GDPR a ISO 27001 mají srovnatelná pravidla pro ochranu dat, jako je důvěrnost údajů, posouzení rizik, oznámení o porušení integrity apod. ISO 27001 se dá aplikovat do soukromého i veřejného sektoru [32].

4.1 Bezpečnostní opatření dle zákona č. 181/2014Sb.,

Kybernetické bezpečnostní opatření je definováno v kybernetickém zákonu a je definováno jako „*souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru*[3]*“.* Jedná se tedy o úkony, které pomáhají naplnit v kybernetickém prostoru aspekty bezpečnosti informací v informačních systémech [33].

Bezpečnostní opatření jsou dle zákona dělena na organizační opatření a technická opatření.

4.1.1 Organizační opatření

Organizační opatření jsou rozdělena na systém řízení bezpečnosti informací, řízení rizik, bezpečnostní politiku, organizační bezpečnost, stanovení bezpečnostních požadavků pro

[3] Zákon č.181/2014 Sb., o kybernetické bezpečnosti § 4

dodavatele, řízení aktiv, bezpečnost lidských zdrojů, řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému, řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému, akvizici, vývoj a údržbu kritické informační infrastruktury a významných informačních systémů, zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, řízení kontinuity činností a kontrolu a audit kritické informační infrastruktury a významných informačních systémů [33].

Příkladem u řízení rizik může být snaha o omezení pravděpodobnosti výskytu možných rizik a jejich eliminace a předpoklad výskytu do budoucna (např. snaha firmy omezit hackerské útoky).

Příkladem v bezpečnostní politice je určitý souhrn norem, pravidel, která má mít definována každá společnost pro zajištění naprosté bezpečnosti. Může se jednat jak o bezpečnost pracovníků, tak o zajištění technických prostředků proti ztrátě dat.

4.1.2 **Technická opatření**

Technická opatření jsou taková opatření, která zahrnují fyzickou bezpečnost, nástroj pro ochranu integrity komunikačních sítí, nástroj pro ověřování identity uživatelů, nástroj pro řízení přístupových oprávnění, nástroj pro ochranu před škodlivým kódem, nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů, nástroj pro detekci kybernetických bezpečnostních událostí, nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, aplikační bezpečnost, kryptografické prostředky, nástroj pro zajišťování úrovně dostupnosti informací a bezpečnost průmyslových a řídicích systémů [33].

Jako příklad nástroje pro ochranu před škodlivým kódem lze brát všechny softwarové nástroje, navržené pro ochranu před škodlivým kódem, který by mohl způsobit narušení bezpečnosti informací v informačních systémech a narušení bezpečnosti služeb. V případě, kdy nejsou data chráněna, hrozí infekce mezi klienty prostřednictvím e – mailu či jiné formy sdílení dat [34].

Příkladem fyzické bezpečnosti je zavedení fyzických opatření ve firmě pro zabránění či ztížení přístupu neoprávněné osoby k utajovaným nebo osobním informacím. Dané místo je zabezpečené a může být nakládáno s utajovanými informacemi, například s daty zákazníků [35].

4.2 Kybernetická opatření komerčních subjektů

Samostatná bezpečnost firem v oblasti kybernetiky patří mezi složitější, a to z toho důvodu, že mnoho firem má zastaralé technické zařízení s nevhodně řešenou počítačovou sítí. Mnoho z nich nepokládá bezpečnost kyberprostoru za důležitou a nechce do ní investovat potřebné prostředky.

V případě útoku hackera firmy poté hledají optimální řešení pro eliminaci problému a minimalizaci dopadů. V minulosti při kybernetickém útoku některé firmy nehlásily napadení Úřadu pro ochranu osobních údajů, a statistiky z tohoto důvodu nebyly přesné a údaje spíše zkreslené. K tomu by v současné době nemělo docházet z důvodu povinnosti hlásit incidenty do 72 hodin [14].

Podle studie Průzkumu hospodářské kriminality bylo za poslední rok (2018) zaznamenáno méně kybernetických útoků na území České republiky oproti zemím střední a východní Evropy a světovému průměru. Přičemž mezi hlavními aspekty narušení patřil sám zaměstnanec, který svým nedbalým jednáním nainstaloval škodlivý malware [36].

Pří zavádění bezpečnostních opatření by firma měla brát v úvahu zásady typu kolik se používá systémů v organizaci a poté vzít v potaz i technologický vývoj. Bezpečnostní opatření by mělo reflektovat na pracovní praktiky organizace (např. zaměstnanec pracující z domova) [14].

Kapitola pojednávala o obecných východiscích kybernetické bezpečnosti a GDPR. Je zřejmé, že pokud by došlo k únikům informací, lze předpokládat rozsáhlý dopad na fungování společnosti.

Jednou z povinností subjektů je zajistit takový stav, aby pravděpodobnost neoprávněného zneužití a použití dat byla minimalizována na co nejnižší úroveň. Subjekty mají mnoho způsobů, jak analyzovat úroveň zabezpečení, například pomocí posouzení vlivu na ochranu osobních údajů či GAP analýzou či provedením penetračních testů, která simulují hackerské útoky.

Problémem může být skutečnost, že samostatné GDPR nedefinuje, jaká vhodná opatření zvolit, a proto každá firma může v podstatě zvolit jakoukoliv metodu zabezpečení, kterou uzná za vhodnou pro splnění určitých podmínek, popřípadě použít mezinárodní normu ISO 27001, která má srovnatelná pravidla pro ochranu dat jako GDPR.

SHRNUTÍ TEORETICKÉ ČÁSTI

Cílem teoretické části této práce bylo pojednat o současném stavu kybernetické bezpečnosti v rámci České republiky Byl popsán vývoj a chápaní kybernetické bezpečnosti. V rámci členství české republiky v EU byla věnována kapitola směrnici NIS, která slouží jako jednotný standart v kybernetické bezpečnosti pro členské státy a dále byla věnována pozornost provozovatelům základních služeb a poskytovatelům digitálních služeb. V rámci strategií České republiky byla popsána Národní strategie kybernetické bezpečnosti na období 2015 až 2020 (její vize, principy a výzvy). Byla popsána odpovídající legislativa pro kybernetickou bezpečnost, jako je kybernetický zákon a tomu určené vyhlášky. Jako součástí kapitoly byl sestaven terminologický slovník s často se vyskytujícími výrazy v kybernetické bezpečnosti, které jsou zároveň používány v této diplomové práci.

Dalším cílem bylo pojednat o obecném nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a ve vztahu ke kybernetické bezpečnosti. Kapitola pojednávala o důvodu zavedení Směrnice č. 95/46/ES a o skutečnosti, že současná technologie postoupila kupředu a dřívější nakládání s osobními údaji a zároveň jejich volný pohyb přestalo splňovat očekávání v rámci bezpečnosti. GDPR má blízký vztah ke kybernetické bezpečnosti a mezi priority pro zpracování informací klade stabilní bezpečnost sítě a zajištění takového stavu, kdy pravděpodobnost proniknutí k těmto údajům je na minimální úrovni a zároveň popisuje postup v případě hackerského útoku.

Pro stanovení podmínek pro využití GDPR s uplatněním kybernetické bezpečnosti byl vytvořen katalog hrozeb pro kybernetickou bezpečnost, který byl sestaven na základě pravděpodobností výskytů kybernetických hrozeb na vazbu GDPR. Pro zjištění těchto hrozeb byly popsány metody pro analýzy rizik, a to konkrétně what – if analýza, penetrační testy, DPIA, PHA, GAP analýza či kontrolní listy. Kapitola upozorňovala na mezinárodní normy ČSN ISO/IEC 2700x, které slouží pro zajištění bezpečnosti informací proti počítačovým podvodům a jsou doporučovány jako téměř dokonalý prostředek pro splnění podmínek pro zavedení GDPR.

V praktické části bude pracováno s analýzami hrozeb, které jsou zapotřebí k analýze bezpečnosti firem. Bude použita GAP analýza v podobě checklistu a pro samostatné hrozby bude vytvořen katalog hrozeb, které poté budou realizovány KARS analýzou.

II. PRAKTICKÁ ČÁST

5 PŘEDSTAVENÍ VYBRANÝCH SUBJEKTŮ

Diplomová práce se ve své praktické části zabývá vypracováním zásad kybernetické bezpečnosti s vazbou na GDPR pro vybrané subjekty, které pracují s informacemi a daty. Vybrané subjekty musí od 25. 5. 2018 plnit nařízení GDPR a musí mít určitá bezpečnostní opatření proti neoprávněné manipulaci a nakládaní s daty.

Pro tuto práci jsou zvoleny dvě společnosti s charakterem malý a velký podnik (pro relevantnější přehled souvislostí nařízení GDPR). Nejmenované subjekty poskytly pro účely diplomové práce informace a opatření týkající se firemní kultury za předpokladu jejich anonymizace z důvodu zachování ochrany obchodního tajemství.

V minulosti patřilo k prioritám zabezpečit společnost a její majetek tím, že byly aplikovány bezpečnostní prvky, které ochraňovaly majetek převážně před fyzickým odcizením či poškozením. V souvislosti s rychlým vývojem počítačových technologií a nutnosti modernizace se hrozby přesunuly do vnitřních prostor a bezpečnost se začala řešit i na místech, s kterými se v minulosti nepočítalo.

5.1 Společnost A

Společnost A je akciová společnost, která se zabývá distribucí energetiky a tepelné techniky, výrobou, distribucí elektřiny a technikou pro ochranu ovzduší. Společnost neprovozuje e-shop a nevyužívá metody a postupy přímého marketingu a zároveň neposkytuje osobní údaje mimo ČR.

5.1.1 **Struktura společnosti**

Struktura společnosti je složená z nejvyššího managementu, ve kterém se nachází tři vysoce postavení pracovníci, kteří ručí za chod organizace jako celku a vytváří strategie pro rozvoj společnosti. Dále jsou zde tři útvary o celkovém počtu šesti lidí, kde se personál stará o fungování společnosti jako celku od naplňování přijímacího řízení až po zajišťování BOZP na všech pracovištích. V posledním stupni hierarchie je pět divizí, které jsou samostatné a nezávislé na ostatních divizích. V čele každé divize je její ředitel, který je zodpovědný vrcholovému managmentu a má svého zástupce, který je mu podřízený. Každá divize má určitý počet zaměstnanců (10-20), kteří plní specifický popis práce.

Celkový počet zaměstnanců je 110 a v případě poptávky trhu je společnost schopna navýšit své kapacity na 155 zaměstnanců. Společnost operuje na celém území České republiky

s občasnými výjezdy na montáže do zemí EU. Práce s daty to této firmy je komplikovaná vzhledem k její velikosti.

Nejvyšší pozice je zastoupena managementem společnosti a je sestavena ze tří funkcí:

- Generální ředitel;
- Finanční ředitel;
- Obchodní ředitel.

Útvary jsou složeny z:

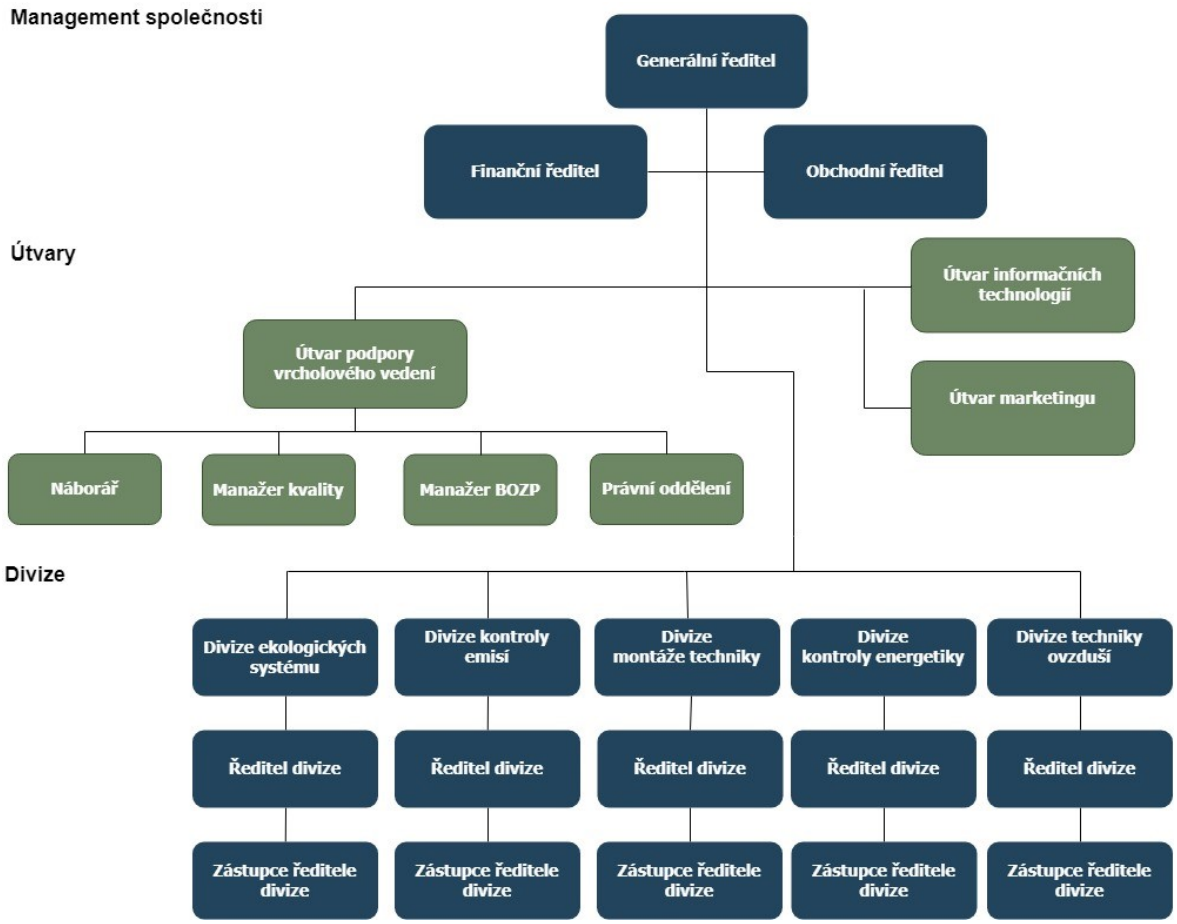
- Útvaru podpory vrcholového vedení, který je složen z náboráře, manažera kvality, manažera BOZP a z právního oddělení;
- Útvaru informačních technologií;
- Útvaru marketingu.

Odbory jsou složeny z:

- Odboru hospodářské správy;
- Odboru ekonomiky;
- Odboru financování a controllingu.

Divize se rozdělují na:

- Divizi ekologických systému;
- Divizi kontroly energetiky;
- Divizi montáže techniky;
- Divizi kontroly emisí;
- Divizi techniky ovzduší.



Obr. 3: *Struktura společnosti A* [zdroj: vlastní]

5.1.2 **Práce s daty**

Ve společnosti jsou zpracovávány osobní údaje týkající se výroby, prodeje, distribucí a pozáručního servisu jejich vlastních výrobků, dále údaje, související se zajištěním lidských zdrojů a správou majetku. Osobní údaje jsou sbírány především za účelem plnění smlouvy nebo pro splnění právní povinnosti společnosti. Údaje o zdravotním stavu zaměstnanců jsou zpracovávány v podobě údaje o aktuální schopnosti vykonávat práci na určeném pracovním místě. Z pohledu biometrických údajů společnost pracuje s informacemi v oblasti BOZP pro vedení přehledu o výdeji osobních ochranných pomůcek u vybrané skupiny zaměstnanců. V omezeném rozsahu využívány údaje o jejich zdravotním stavu.

Společnost vede souhrnný rejstřík trestů zaměstnanců pouze v případě, kdy je trestný čin spáchán vůči společnosti, popřípadě je společnost účastníkem trestního řízení.

Společnost zpracovává mzdové agendy zaměstnanců a osobní údaje dětí zaměstnanců a jejich rodinných příslušníků. Společnost nezpracovává žádné další osobní údaje zvláštních

kategorií. Ve společnosti není aplikováno automatizované zpracovávání osobních údajů a jejích následná pseudonymizace.

5.2 Společnost B

Společnost B je společnost s ručením omezeným a zabývá se manipulačními prostředky, zvedacími zařízeními a kolejovou technikou. Společnost provozuje e-shop a využívá metody a postupy přímého marketingu. Prostředky jsou zasílané pomocí přepravní služby či s využitím osobního odběru.

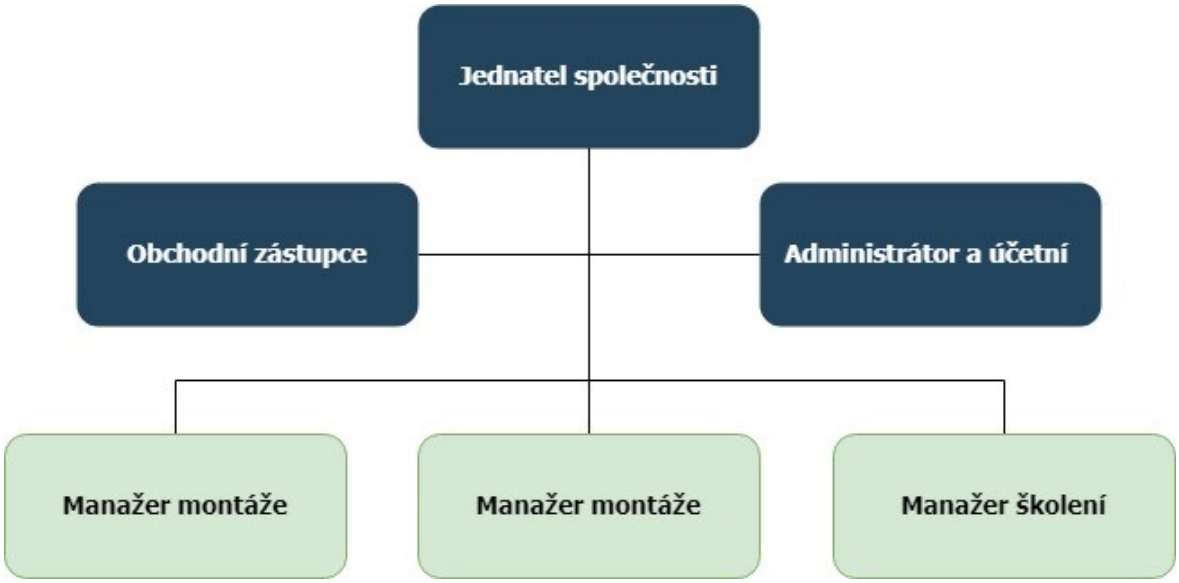
V rámci svého portfolia nabízí služby a servisování manipulačních prostředků podle aktuálních vyhlášek, předpisů a certifikací. Její působení je převážně v Jihomoravském kraji. V případě volných kapacity je schopná provádět montáž i mimo kraj působnosti, tudíž působí na území celé České republiky a data neposílá mimo Evropskou unii. Počet zaměstnanců je 15.

Informace a data jsou převážně zpracovávána pomocí online obchodu, který tvoří 65 % příjmů společnosti. Data jsou též zpracovávána při provádění montážních prací a provádění školení.

5.2.1 **Struktura společnosti**

Složení společnosti je následující:

- Jednatel společnosti;
- Obchodní zástupce;
- Administrátor a účetní = fakturace a administrativa;
- 2 Manažeři montáže;
- Manažer školení;
- 8 montážních dělníků.



Obr. 4: *Struktura společnosti B* [zdroj: vlastní]

5.2.2 **Práce s daty**

Při zpracovávání osobních dat jsou zpracovávány informace jako je jméno, příjmení, emailová adresa, telefon k vytvoření nabídky služeb, informace o nabídce či za účelem odpovědi na dotaz položený pomocí webové stránky. Informace jsou zpracovávány po dobu jednání o uzavření smlouvy mezi klientem a společností po dobu jednoho roku. Společnost doposud neřešila porušení zabezpečení osobních údajů. Společnost nepracuje s rozsáhlými datovými soubory, kde by případné narušení ochrany osobních údajů vyvolalo riziko pro jakoukoli skupinu fyzických osob.

Cílem kapitoly bylo představit firmy A a B, které budou použity jako vzorové firmy pro účel této diplomové práce, popsat jejich strukturu a způsob, jak pracují s daty. Záměrně byla vybrána vzorová firma A jako příklad „velké“ firmy a firma B jako příklad „malé firmy“.

6 ANALÝZA SOUČASTNÉHO STAVU KYBERNETICKÉ BEZPEČNOSTI A OCHRANY OSOBNÍCH ÚDAJŮ

Pro vypracování a naplnění zadání diplomové práce je nutné analyzovat podmínky současného stavu společností ve vazbě na kybernetickou bezpečnost a následovné naplnění požadavků pro GDPR, které poté bude pojeno s další kapitolou, pojednávající o provedení určitých opatření.

Realizace analýzy současného stavu je vypracována ve vazbě na pokyny norem ISO EN 2700x, které jsou podpůrným materiálem pro vytvoření optimálního stavu a naplnění podmínek kybernetické bezpečnosti a GDPR.

Organizace by neměly zapomínat na nutnost neustálého zlepšování vhodnosti, přiměřenosti a efektivnosti systému řízení bezpečnosti informací [37].

Přiložené GAP analýzy jsou vzorové a nevyplněné. Přímá vyhodnocení od firem se nacházejí v přílohové části pro obě společnosti A, B.

6.1 Návrh na realizaci

Po společné domluvě s vybranými subjekty bylo za nejlepší řešení pro splnění požadavků problematiky stanoveno vypracování a provedení systémového prověření formou bezpečnostního projektu zaměřeného na posouzení stávající úrovně bezpečnosti a navržení opatření za účelem zajištění dostačující úrovně kybernetické ochrany ve společnosti. Zároveň je snahou zjistit úrovně zajišťující dostatečné oprávněné zájmy společnosti, a to v přímé návaznosti na posouzení zajištění v souladu s nařízení EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Identifikace a hodnocení by mělo sloužit jednak jako doporučená forma a zároveň jako jedna z možných metod, jak provádět analýzy stavu kybernetické bezpečnosti s účinností GDPR. Informace o společnostech a jejich struktura byly uvedeny v kapitole 5 Představení vybraných společností.

6.1.1 Cíl praktické části práce

Cílem práce je obeznámit společnosti s možnými nedostatky v působnosti kybernetické bezpečnosti a GDPR a zvýšit povědomí o skutečnosti, že každá dnešní společnost shromažďuje, zpracovává, uchovává a přenáší informace. Je zapotřebí vědět, že informace

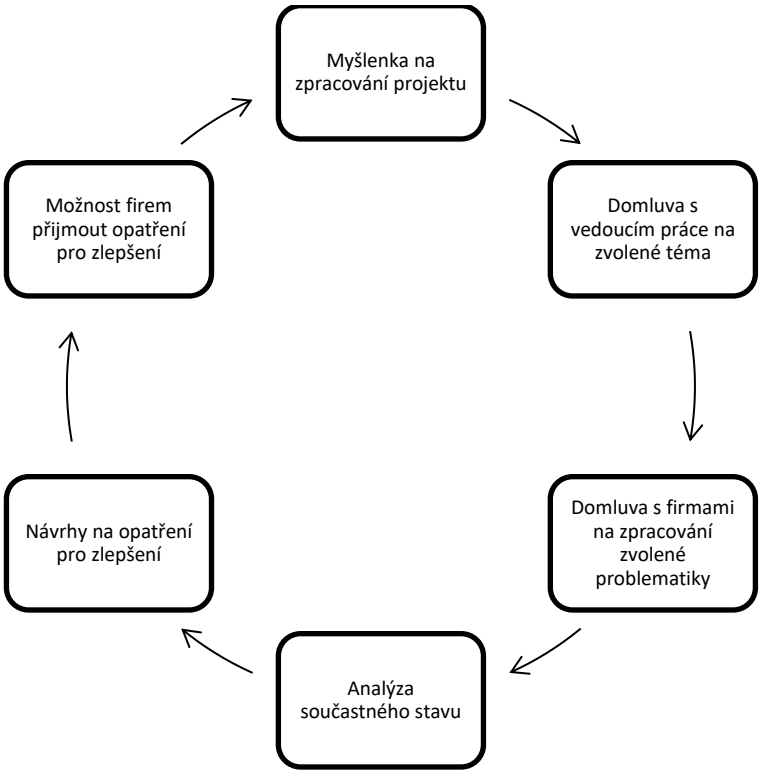
a související procesy, systémy, sítě a lidé jsou důležitá aktiva pro dosažení cílů organizace. Společnost jako celek samotný často čelí řadě rizik, která mohou ovlivnit fungování aktiv. Zároveň jsou firmy povinny uschovávat dokumentované informace o výsledcích posuzování rizik ve vazbě na bezpečnost informací.

6.1.2 **Základní rizika implementace návrhu**

Samostatný návrh této práce může zaniknout už na samotném začátku, a to z důvodů jako: nedostatek finančních zdrojů potřebných k realizaci projektu, nedostatek lidí pro realizaci projektu či lidí, kteří z nějakého důvodu nesdělí informace, týkající se jejich současného stavu, nedostatek času na realizaci a aplikaci vytvořených řešení, neprovádění kontrol pro získání přehledu o aktuálním stavu společnosti.

6.1.3 **Náklady a životní cyklus diplomové práce**

Náklady na diplomovou práci jsou na minimální úrovni z toho důvodu, že celé zpracování slouží jako výstup diplomové práce v praktické části. Vybrané firmy poskytly veškeré informace, potřebné pro vypracování této diplomové práce. Jako externí zpracovatel firemních informací provedu v rámci této diplomové práce bezpečnostní analýzy, týkající se kybernetické bezpečnosti a náročnosti na GDPR.



Obr. 5: *Životní cyklus diplomové práce* [zdroj: vlastní]

Životní cyklus na vypracování projektu je postaven na myšlence „Naplánuj – Udělej – Zkontroluj – Zasáhni", kde byla nutná domluva s vedoucím práce, zda je možné realizovat následující zadání. Další fází bylo získat společnosti, které by byly ochotny spolupracovat a být přínosem pro danou problematiku, ve kterých by proběhla analýza stavu kybernetické bezpečnosti a GDPR. Výstupem poté jsou návrhy na opatření a zlepšení stávajícího stavu. Samostatnou výzvou je zjištění, zda společnosti dané návrhy přijmou. Celá práce by měla sloužit jako podnět pro podobné téma diplomové práce.

6.2 Identifikace a hodnocení rizik pro společnosti

Prvním krokem je provedení identifikace a hodnocení rizik. Každá společnost má stanovena určitá opatření, ale pro zjištění všech souvislostí se bude pracovat s hrozbami, u kterých je zřejmá vazba na aplikaci a soulad s požadavky vnitřních směrnic.

Důležité je, aby v oblasti bezpečnosti informací bylo umožněno systému řízení organizace následující:

a) uspokojovat požadavky zákazníků a dalších zúčastněných stran;

b) zlepšovat plány a činnosti organizace;

c) splňovat cíle bezpečnosti informací organizace;

d) vyhovovat předpisům, legislativě a oborovým normám;

e) řídit informační aktiva organizovaně, a tak usnadnit a umožnit neustálé zlepšování a úpravy ve vztahu ke stávajícím cílům organizace[4] [37].

Jako první krok je tedy zapotřebí identifikovat všechny možné typy a rozsahy osobních údajů, se kterými je pracováno uvnitř společnosti, včetně souvisejících účelů zpracování.

- Pravděpodobnosti uplatnění potenciální hrozby pro daný typ zpracování;
- Zranitelnosti osobních údajů při uplatnění rizika;
- Dopad rizika na subjekt údajů.

[4] ČSN EN ISO/IEC 27000

6.2.1 **Katalog hrozeb pro společnost A**

Tab. 1: *Pravděpodobnost výskytu hrozby* [zdroj: vlastní]

Kategorie (% šance na výskyt)		**Popis**
1	Časté (70-100 %)	Existuje možnost častého výskytu. Působení rizika – působí trvale.
2	Pravděpodobné (50-70 %)	Výskyt rizika lze očekávat častěji.
3	Občasné (20-50 %)	Výskyt rizika lze očekávat několikrát.
4	Ojedinělé (5-20 %)	Je možné, že riziko se vyskytne několikrát během životního cyklu objektu.
5	Nepravděpodobné (1-5 %)	Nepříliš jisté, že se riziko vyskytne, ale možné. Lze předpokládat, že nebezpečí se může výjimečně vyskytnout.
6	Nemožné (0-1 %)	Extrémně nemožné, že se riziko vyskytne. Lze předpokládat, že nebezpečí se nevyskytne.

Zvolené hodnoty v Tab. 1 byly sestaveny v rámci expertního odhadu a vzájemnou komunikací s odborníky na bezpečnost ve firmě A. Tabulka slouží pouze jako přidaná hodnota pro katalog hrozeb v Tab. 2, aby bylo znázorněno, jak často se hrozba vyskytuje, aby následné opatření minimalizovalo riziko na přijatelnou úroveň.

Tab. 2: *Katalog hrozeb pro společnost A* [zdroj: vlastní]

Index	Riziko	Šance na výskyt
1.	Malware a ransomware	**2**
2.	Nefunkčnost IS	**3**
3.	Nedodržování pracovních postupů	**2**
4.	Výpadky dodávek el. energie	**3**
5.	Výpadky serverů/ cloudových úložišť	**5**
6.	Výpadky internetového připojení	**4**
7.	Falšování identity zaměstnanců	**4**
8.	Proniknutí cizích osob do areálu	**3**
9.	Neodborná manipulace s ICT zařízení	**5**
10.	Krádež firemních materiálů	**2**
11.	Poškození prostoru zaměstnancem	**3**
12.	Nevědomost zaměstnanců, jak pracovat s firemními ICT prostředky	**1**
13.	Pracovní úrazy způsobené nedodržováním BOZP	**2**
14.	Únik informací	**3**
15.	Hackerský útok	**1**

Katalog hrozeb pro firmu A byl vyhotoven za podmínek posouzení možných hrozeb na pracovištích, kde sídlí management a kde je pracováno s ICT technologií a daty zaměstnanců. Do katalogu hrozeb pro firmu A nejsou zahrnuty divize, které byly znázorněny v obr.3.

Dále s identifikovanými hrozbami bude konfrontována KARS analýza, která slouží pro analýzu hrozeb s využitím souvztažnosti. KARS analýza je kvalitativní analýza rizik. Cílem využití metody KARS je rozhodnout o tom, která rizika jsou pro daný systém „nejnebezpečnější“ a proto je nutné se jimi zabývat přednostně.

Na základě vytvořené tabulky je pracováno se zvolených hrozbami, po řádcích, a to vždy zleva doprava. Na základě, zda určitá hrozba může vyvolat jinou hrozbu:

1 – existuje-li reálná možnost, že riziko Ri může vyvolat riziko Rj

0 – neexistuje-li reálná možnost, že riziko Ri může vyvolat riziko Rj

Riziko Ri nemůže vyvolat samo sebe!

Tab. 3 *KARS analýza pro firmu A* [zdroj: vlastní]

	Malware a ransomware	**Nefunkčnost počítačů**	**Nedodržování pracovních postupů**	**Výpadky dodávek el. energie**	**Výpadky serverů/ cloudových úložišť**	**Výpadky internetového připojení**	**Falšování identity**	**Proniknutí cizích osob do areálu**	**Neodborná manipulace s ICT zařízení**	**Krádež firemních materiálů**	**Poškození prostoru**	**Nevědomost zaměstnanců, jak**	**Pracovní úrazy způsobené**	**Únik informací**	**Hackerský útok**	**Σ**	**% šance výskytu**
Malware a ransomware	X	1	1	0	1	0	1	0	1	1	0	1	0	1	1	9	64
Nefunkčnost počítačů	1	X	1	1	1	1	1	1	1	1	0	1	0	1	1	12	86
Nedodržování pracovních postupů	1	1	X	1	1	1	1	1	1	1	1	1	1	1	1	14	100
Výpadky dodávek el. energie	0	1	0	X	1	1	0	1	0	1	0	0	0	0	0	5	36
Výpadky serverů/ cloudových úložišť	1	1	1	0	X	0	0	0	0	0	0	1	0	1	1	6	43
Výpadky internetového připojení	0	1	0	0	1	X	0	0	0	0	0	1	0	0	0	3	21
Falšování identity zaměstnanců	1	1	1	0	0	0	X	1	0	1	1	1	1	1	1	10	71
Proniknutí cizích osob do areálu	1	1	1	1	1	1	0	X	0	1	1	0	1	1	1	11	78
Neodborná manipulace s ICT zařízení	1	1	0	0	1	1	0	1	X	0	0	0	1	1	1	8	57
Krádež firemních materiálů	1	1	0	1	1	1	1	1	0	X	0	0	0	1	1	9	64
Poškození prostoru	0	0	1	0	0	0	0	1	0	0	X	0	1	1	1	5	36
Nevědomost zaměstnanců, jak pracovat s firemními ICT prostředky	1	1	1	1	1	1	1	0	1	1	0	X	0	1	1	11	78
Pracovní úrazy způsobené nedodržování m BOZP	0	0	1	0	0	0	0	0	1	0	0	0	X	0	0	2	14
Únik informací	1	1	0	0	1	1	1	1	1	1	0	1	0	X	1	10	71
Hackerský útok	1	1	0	0	1	1	1	0	0	1	0	1	0	1	X	8	57
Σ	10	12	8	5	11	9	7	8	6	9	3	8	5	9	11		
% šance výskytu	71	86	57	36	78	64	50	57	43	64	21	57	36	64	78		

Po vyhodnocení vzájemně působících hrozeb jsou vypočítané koeficienty aktivit (K_{ari}) a pasivit (K_{pri}) jednotlivých rizik sečteny u každé hrozby do Σ a vypočítán koeficient aktivity výskytu vzorcem:

Výpočet pro hrozbu Malware a ransomware vodorovně (Kari):

$$P = \frac{\Sigma}{(\text{počet hrozeb}) - 1} \times 100\ [\%]$$

$$P = \frac{10}{(15) - 1} \times 100\ [\%]$$

$$P = 71\ [\%]$$

Výpočet pro hrozbu Malware a ransomware svisle (Kpri):

$$P = \frac{\Sigma}{(\text{počet hrozeb}) - 1} \times 100\ [\%]$$

$$P = \frac{9}{(15) - 1} \times 100\ [\%]$$

$$P = 64\ [\%]$$

Po vypočítání všech zbylých hrozeb je vytvořena tabulka koeficientu aktivit a pasivit. Pro sloupec hrozeb Kari a pro řádek hrozeb Kpri.

Tab. 4: *Tabulka koeficientů aktivity a pasivity*

Riziko	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
Kari (%)	71	86	57	36	78	64	50	57	43	64	21	57	36	64	78
Kpri (%)	64	86	100	36	43	21	71	78	57	64	36	78	14	71	8

Následovně je rozdělena plocha grafu na kvadranty tak, aby se do I. kvadrantu (pravý horní roh) dostalo 80 % všech analyzovaných rizik.

Pokud chceme osu O_1 vést tak, aby vyhovovala výše požadované podmínce 80 %, bude se jednat o rovnoběžku s osou y v bodě:

$$O_1 = \frac{\text{Kari}(max) - \text{Kpri}(\min)}{100} \times 80$$

$$O_1 = \frac{86 - 8}{100} \times 80$$

$$O_1 = 62{,}4$$

Pro osu O_2, která bude rovnoběžkou s osou x, vypočteme její průsečík osy x podle adekvátního vztahu:

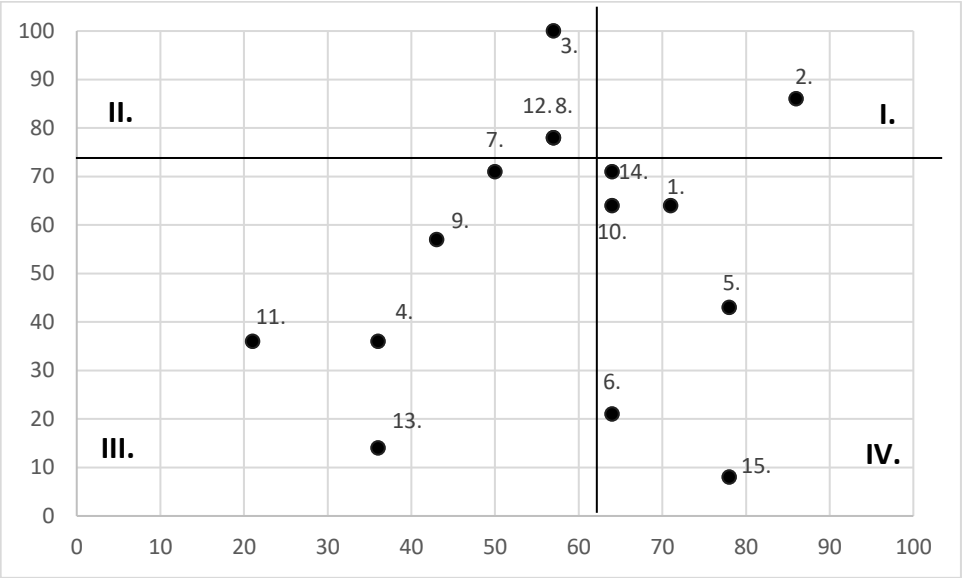
$$O_2 = \frac{\text{Kpri}(max) - \text{Kpri}(\text{min})}{100} \times 80$$

$$O_2 = \frac{100 - 8}{100} \times 80$$

$$O_2 = 73{,}6$$

Poté je celý graf rozdělen podle O_1 a O_2 na kvadráty I, II, III, IV.

- Kvadrát č. I. znázorňuje primárně a sekundárně nebezpečná rizika
- Kvadráty č. II a III. znázorňují sekundárně nebezpečná rizika
- Kvadrát č. IV. znázorňuje relativní bezpečnost vzniku hrozeb



Obr. 6: *Grafický výstup KARS analýzy pro firmu A* [zdroj: vlastní]

Mezi hlavní hrozby vyplývající z analýzy KARS patří hrozba nefunkčnosti počítačů. To svědčí o tom, jak je ve firmě důležitý stabilní a neporuchový technický systém. Při nefunkčností všech prostředků by firma nebyla schopna fungovat a při dlouhodobém výpadků systému by mohlo dojít k velkým finančním ztrátám firmy.

Mezi další rizika nebezpečí se zařadily tyto hrozby: nedodržování pracovních postupů, proniknutí cizích osob do areálu, neznalost zaměstnanců, jak pracovat s firemními ICT prostředky, únik informací, hackerský útok, malware a ransomware, výpadky serverů/ cloudových úložišť, výpadky internetového připojení, hackerský útok.

Celkově lze chápat, že někteří zaměstnanci nedodržují pravidla či neví, jak pracovat s ICT prostředky anebo je nemají přiděleny. Tím však může dojít k spouštěči ostatních zmiňovaných hrozeb, např. stáhnutí malwaru a ransomware, úniku informací, úspěšným hackerským útokům. Jelikož ve firmě tato pravidla nejsou nastavena, bude snahou na závěr přijít s návrhem řešení tohoto nedostatku.

Proti výpadkům internetových připojení a výpadku serverů musí firma neustále rozvíjet snahu pro pravidelnou aktualizaci a dle svých finančních možností investovat do těchto zařízení.

6.2.2 **Katalog hrozeb pro společnost B**

Tab. 5: *Pravděpodobnost výskytu hrozby* [zdroj: vlastní]

Kategorie (% šance na výskyt)		**Popis**
1	Časté (70-100 %)	Existuje možnost častého výskytu. Nebezpečí působí trvale.
2	Pravděpodobné (50-70 %)	Výskyt nebezpečí lze očekávat často.
3	Občasné (20-50 %)	Výskyt nebezpečí lze očekávat několikrát.
4	Ojedinělé (5-20 %)	Je možné, že se vyskytne několikrát během životního cyklu objektu.
5	Nepravděpodobné (1-5 %)	Nepříliš jisté, že se vyskytne, ale možné. Můžeme předpokládat, že nebezpečí se může výjimečně vyskytnout.
6	Nemožné (0-1 %)	Extrémně nemožné, že se vyskytne. Lze předpokládat, že nebezpečí se nevyskytne.

Hodnoty pro Tab. 5 jsou vypracované stejným postupem jak pro Tab. 1 z důvodu snadnější analýzy a vzájemného porovnání. Tabulka slouží pouze jako přidaná hodnota pro katalog hrozeb pro firmu B.

Tab. 6*: Katalog hrozeb pro společnost B* [zdroj: vlastní]

Index	**Riziko**	**Šance na výskyt**
1.	Výpadek E-shopu	**3**
2.	Hackerský útok	**2**
3.	Nemoc zaměstnanců	**2**
4.	Opoždění doručení zboží	**4**
5.	Pracovní úrazy způsobené nedodržováním BOZP	**3**
6.	Reklamace	**3**
7.	Výpadky dodávek el. energie	**4**
8.	Malware a ransomware	**2**
9.	Výpadky internetového připojení	**3**
10.	Špatná image na trhu	**5**
11.	Konkurence	**4**
12.	Únik osobních údajů klientů	**3**
13.	Ztráta dokumentů	**2**
14.	Sabotáž	**4**

Tab. 7: *KARS analýza pro firmu B* [zdroj: vlastní]

	Výpadek E-shopu	**Hackerský útok**	**Nemoc zaměstnanců**	**Opoždění doručení**	**Pracovní úrazy způsobené**	**Reklamace**	**Výpadky dodávek el.**	**Malware a**	**Výpadky internetového připojení**	**Špatná image na trhu**	**Konkurence**	**Únik osobních údajů klientů**	**Ztráta dokumentů**	**Sabotáž**	**Σ**	**% šance výskytu**
Výpadek E-shopu	X	1	0	1	0	0	0	0	0	1	1	0	0	0	4	31
Hackerský útok	1	X	0	1	0	0	0	1	1	1	1	1	1	1	9	69
Nemoc zaměstnanců	0	0	X	1	0	0	0	0	0	0	1	0	0	0	2	15
Opoždění doručení zboží	0	0	0	X	0	1	0	0	0	1	1	0	0	1	4	30
Pracovní úrazy způsobené nedodržováním BOZP	0	0	1	1	X	1	0	0	0	1	1	0	0	1	6	46
Reklamace	0	0	0	1	0	X	0	0	0	1	1	0	0	0	3	23
Výpadky dodávek el. energie	1	0	0	1	1	0	X	0	1	0	0	0	1	1	6	46
Malware a ransomware	1	1	0	1	0	1	0	X	0	1	1	1	1	0	8	62
Výpadky internetového připojení	1	0	0	1	0	0	0	0	X	1	1	0	1	0	5	38
Špatná image na trhu	1	1	0	1	0	1	0	0	0	X	1	0	0	0	5	38
Konkurence	1	1	0	0	0	0	0	1	0	1	X	1	1	1	7	54
Únik osobních údajů klientů	1	0	0	1	0	1	0	0	0	1	1	X	1	1	7	54
Ztráta dokumentů	1	1	0	1	1	0	0	1	0	1	1	1	X	0	8	62
Sabotáž	1	1	0	1	1	1	1	1	1	1	0	1	1	X	11	85
Σ	9	5	1	12	3	5	1	4	3	11	11	5	7	5		
% šance výskytu	69	38	8	92	23	38	8	31	23	84	84	38	54	38		

Pro výpočet koeficientů aktivit a pasivit a následných pomocných os pro pokrytí minimálně 80 % hrozeb je používaná stejná metoda jako v KARS analýze pro firmu A, ve které byl popsán postup zpracování hodnot.

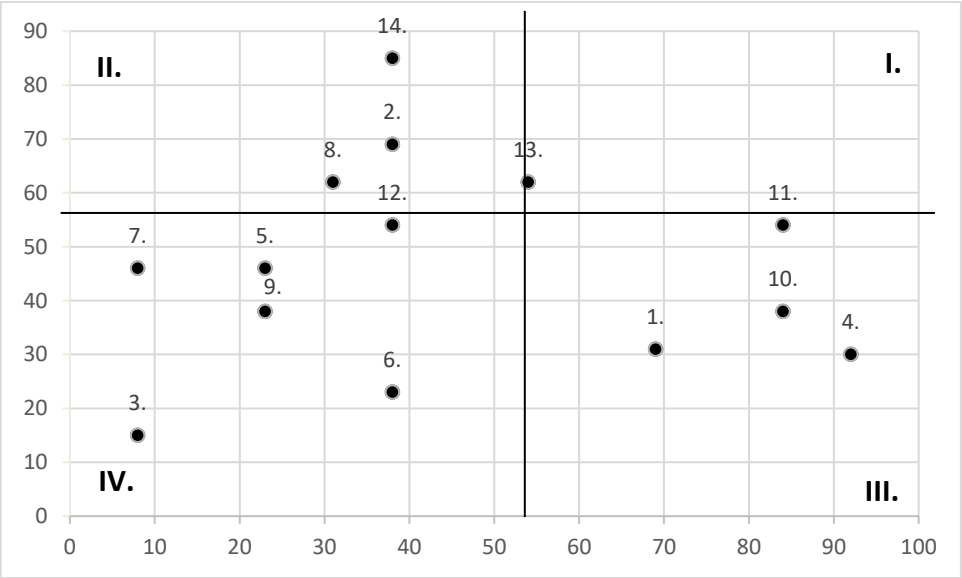
Tab. 8: *Tabulka koeficientů aktivity a pasivity rizik pro firmu B* [zdroj: vlastní]

Riziko	1	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.
Kari (%)	69	38	8	92	23	38	8	31	23	84	84	38	54	38
Kpri (%)	31	69	15	30	46	23	46	62	38	38	54	54	62	85

$$O_{(1)} = \frac{\text{Kari}(max) - \text{Kpri}(\min)}{100} \times 80 \qquad O_{(2)} = \frac{\text{Kpri}(max) - \text{Kpri}(\min)}{100} \times 80$$

$$O_{(1)} = \frac{82-15}{100} \times 80 \qquad O_{(2)} = \frac{85-15}{100} \times 80$$

$$O_{(1)} = 53{,}6\ \% \qquad O_{(2)} = 56\ \%$$



Obr. 7: *Grafický výstup KARS analýzy pro firmu* B [zdroj: vlastní]

Pro firmu B nebyla zjištěna primární rizika nebezpečí, ale byly zjištěny hraniční hodnoty hrozby ztráty dokumentů a ohrožení konkurencí, která by mohla převzít klienty.

Mezi sekundární rizika nebezpečí se zařadila sabotáž, únik osobních údajů klientů, špatná image na trhu, malware a ransomware, opoždění doručení zboží, hackerský útok.

Výskytu vyhodnocených hrozeb lze předejít pomocí používání cloudových úložišť, která mohou sloužit i pro archivaci vyřazených dokumentů.

6.2.3 **Návrh GAP analýzy na ISMS**

Pro zhodnocení stávajícího stavu společnosti a splnění dalšího bodu zadání diplomové práce je zapotřebí provést analýzu zaměřenou na prostředí firmy, která je spojena se zacházením s ISMS (Systém řízení bezpečnosti informací). Celý ISMS představuje neustálý přístup k ustanovení, implementaci, provozování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací organizace tak, aby byly dosaženy její cíle. Celé ISMS by mělo být postaveno na procesu posuzování a řízení rizik na přijatelnou úroveň.

Každá firma byla oslovena s žádostí o vyplnění vytvořených dotazníků. Jejich vyplněním byly pověřeny zodpovědné osoby ve firmě. Všechny vyhodnocené GAP analýzy jsou uvedeny jako přílohy této diplomové práce. Vyhodnocení analýz se nachází v kapitole 7 podkapitole 7.2.1

ISMS je definováno celou skupinou norem ISO/IEC 2700x a je plně kompatibilní se systémy managementu jakosti a lze jej jednoduše integrovat do celkového systému řízení organizace. Mezi jeho výhody patří stanovení optimálního poměru mezi náklady a dosaženou úrovní zabezpečení informačních aktiv organizace, snížení rizik, souvisejících s nedostupností informací, minimalizace nebezpečí úniku dat a ochrana stability organizace a Průběžné sledování a hodnocení aktuální úrovně informační bezpečnosti.

Tab. 9: *GAP analýza na ISMS* [zdroj: vlastní]

GAP ANALÝZA-KONTROLNÍ SEZNAM ISMS ANALÝZA ZA ÚČELEM NALEZENÍ NESROVNALOSTÍ MEZI CÍLI DOSAŽENÝMI A POŽADOVANÝMI. ANALÝZA SE ZAMĚŘUJE TAKÉ NA PROZKOUMÁNÍ A ODKRYTÍ PŘÍLEŽITOSTÍ				
Kontrolovaná oblast/zadání: úvodní kontrola stavu GDPR a systémového zajištění souladu **Kontrolovaná organizace:** **Upozornění**: Odpověď ANO je přípustná pouze v případech, kdy kontrolované požadavky jsou odpovídající požadované úrovni a doloženy VS (vedení společnosti) dokumentovanými informacemi – důkazy.		**ANO**	**NE**	**Irelevantní oblast**
1.	Je v organizaci zpracován relevantní kontext organizace pro zajištění souladu s požadavky GDPR?	☐	☐	☐
2.	Jsou VS v SM vydány, revidovány a sdíleny Politiky pro řízení oblasti GDPR, a to i pro případy krizí, havárií a katastrof?	☐	☐	☐

3.	Jsou VS ustanoveny Politiky pro implementování primárních opatření zaměřených na zajištění oprávněných zájmů organizace a soulad s požadavky GDPR, zákonů ČR a se smluvními požadavky?	☐	☐	☐
4.	Jsou definovány a přiděleny v SM ISMS odpovědnosti v oblasti GDPR informací a jsou uživatelé informací prokazatelně proškoleni o své odpovědnosti za jejich ochranu?	☐	☐	☐
5.	Jsou stanovena bezpečnostní opatření (T, O, S) na ochranu osobních údajů, které jsou přístupné, zpracovávané, ukládané v místech pro práci i na dálku včetně mobilních zařízení?	☐	☐	☐
6.	Obsahují pracovní smlouvy a dále obchodní smlouvy ustanovení o povinnostech zaměstnanců a smluvních stran o jejich odpovědnostech za bezpečnost informací?	☐	☐	☐
7.	Je stanoven v SM ISMS systém požadování plnění požadavků a systém kontrol plnění povinností a postihů v ISMS v souladu s Politikami a postupy?	☐	☐	☐
8.	Jsou v SM ISMS dokumentovaným způsobem identifikována aktiva organizace a definovány odpovědnosti k jejich přiměřené ochraně?	☐	☐	☐
9.	Je v SM ISMS zaveden systém identifikace a vyhodnocování zdrojů nebezpečí a z nich vyplývajících rizik/hrozeb s metodikou úrovně opatření pro dosažení jejich přijatelnosti?	☐	☐	☐
10.	Jsou všechny v SM ISMS informace klasifikovány s ohledem na zákonné požadavky, jejich hodnotu, kritičnost a citlivost vůči neoprávněnému prozrazení nebo modifikaci?	☐	☐	☐
11.	Jsou zavedeny postupy pro správu výměnných médií v souladu se schématem klasifikace informací přijatým organizací?	☐	☐	☐
12.	Je zaveden v SM ISMS systém řízení přepravy a nakládání s médii a jejich bezpečnou likvidací, pokud nejsou dále upotřebitelná, v souladu s formalizovanými postupy?	☐	☐	☐
13.	Je ustavena v SM ISMS politika a řízení oprávnění/autorizace přístupu uživatelů podle jejich rozličné úrovně oprávnění k informačním sítím, síťovým službám podle jejich rizikovosti?	☐	☐	☐
14.	Je vytvořena a implementována politika pro používání kryptografických opatření na ochranu informací, a to po dobu jejich celého životního cyklu?	☐	☐	☐

15.	Je vytvořena a implementována politika předcházení neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací?	☐	☐	☐
16.	Jsou stanoveny politiky a opatření pro předcházení hrozbám – ztrát, poškození, krádežím nebo kompromitaci aktiv a přerušení činností organizace.	☐	☐	☐
17.	Jsou pro bezpečnost provozu IT – útoky – snížení rizika neoprávněného přístupu, malwary – zavedena a řízena opatření a odděleny sítě pro prostředí provozu, vývoje aj.?	☐	☐	☐
18.	Jsou záložní kopie informací, softwaru a binárních obrazů systému pořizovány a testovány v pravidelných intervalech podle nastaveného systému pro danou oblast?	☐	☐	☐
19.	Jsou systémově pořizovány, uchovány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací?	☐	☐	☐
20.	Jsou vytvořeny, popsány v SM ISMS a implementovány postupy řízené instalace softwaru na provozních systémech?	☐	☐	☐
21.	Je zaveden a implementován systém k ochraně informací v systémech a aplikacích a jsou v tomto smyslu sítě řízeny, spravovány a kontrolovány?	☐	☐	☐
22.	Je zaveden IT systém získání informací o zranitelností systémů, hodnocení úrovně ohrožení organizace, připravena proaktivní i reaktivní opatření na zvládání souvisejících rizik a incidentů?	☐	☐	☐
23.	Je zaveden, aplikován a kontrolován řízený systém bezpečnosti informací při jejich přenosu v rámci organizace, s externími subjekty a daty zpřístupněnými vně subjektu?	☐	☐	☐
24,	Je zaveden v rámci ISMS systém pro monitoring, přezkoumávání a audit služeb dodavatelů, kde se nedají vyloučit zdroje nebezpečí pro oblast ISMS?	☐	☐	☐
25.	Je uvnitř organizace zaveden systém provádění kontrol a testování funkčnosti systému ISMS?	☐	☐	☐

6.2.4 **Návrh GAP analýzy na GDPR**

Pro splnění požadavků na ISMS je zapotřebí zjistit, zda jsou požadavky na ochranu fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů aplikovatelné.

Vyhodnocené analýzy vybraných společností jsou jako přílohy této diplomové práce. Vyhodnocení analýz se nachází v kapitole 7 podkapitole 7.2.2

Tab. 10: *Kontrolní seznam na GDPR* [zdroj: vlastní]

GAP ANALÝZA-KONTROLNÍ SEZNAM GDPR **ANALÝZA ZA ÚČELEM NALEZENÍ NESROVNALOSTÍ MEZI CÍLI DOSAŽENÝMI A POŽADOVANÝMI. ANALÝZA SE ZAMĚŘUJE TAKÉ NA PROZKOUMÁNÍ A ODKRYTÍ PŘÍLEŽITOSTÍ KE ZLEPŠENÍ**				
<u>Kontrolovaná oblast/zadání</u>: úvodní kontrola stavu GDPR a systémového zajištění souladu Organizace při implementaci požadavků obvykle postupují formou projektu, kdy postupně zavádějí požadavky nařízení GDPR. **Upozornění: Tento seznam navazuje kontinuálně na požadavky pro řízení ISMS** **Upozornění**: Odpověď ANO je přípustná pouze v případech, kdy kontrolované požadavky jsou odpovídající požadované úrovni a doloženy VS (vedení společnosti) dokumentovanými informacemi – důkazy.		**ANO**	**NE**	**Irelevantní oblast**
1.	Je rozsah systému řízení ochrany osobních údajů dostupný jako dokumentované a řízené informace?	☐	☐	☐
2.	Zahrnuje systém řízení ochrany osobních údajů specifikaci řízených dokumentovaných informací požadovaných GDPR?	☐	☐	☐
3.	Obsahují pracovní smlouvy a obchodní smlouvy ustanovení o povinnostech zaměstnanců a smluvních stran o jejich odpovědnostech za GDPR?	☐	☐	☐
4.	Jsou uzavřeny smlouvy o ochraně OÚ s dodavateli služeb, kteří jsou dotčení povinnostmi v oblasti GDPR např: IT, poskytovatelé PLS, zákazníci, dodavatelé služeb, auditoři atd. dle kontextu	☐	☐	☐
5.	Je v SM řízení hrozeb v oblasti GDPR zaveden systém identifikace zdrojů nebezpečí a z nich vyplývajících rizik/hrozeb s metodikou úrovně opatření pro dosažení jejich přijatelnosti?	☐	☐	☐
6.	Má organizace nastaveny postupy/procesy pro řešení neshod v oblasti ochrany osobních údajů?	☐	☐	☐
7.	Jsou pro všechny identifikované operace nebo soubor operací s osobními údaji nebo soubory osobních údajů stanoveny postupy za účelem jejich řízené ochrany, používání a ukládání?	☐	☐	☐

8.	Je vytvořen a průběžně aktualizován Registr osobních údajů se specifikací vlastníků, rizik a požadované úrovni ochrany?	☐	☐	☐
9.	Je stanovena klasifikace ochrany jednotlivých osobních údajů podle klasifikace rizik?	☐	☐	☐
10.	Je vytvořen a aktualizován řídící dokument SM o spisové a archivační činnosti osobních údajů?	☐	☐	☐
11.	Jsou zpracovávány/definovány zvláštní kategorie údajů podle článku 9 GDPR?	☐	☐	☐
12.	Jsou stanoveny v SM povinnosti a postupy zajišťující Zákonnost zpracování dle Článek 6 GDPR?	☐	☐	☐
13.	Jsou systémově zajištěny správcem údajů od dotčených subjektů dokumentovaná či zjevná potvrzení (doložitelná) o svolení/souhlasu ke zpracování údajů dle Článek 7 GDPR?	☐	☐	☐
14.	Je systémově a technicky zabezpečeno, že subjekt údajů má právo svůj souhlas kdykoli odvolat a v souvislosti s tím bude ze strany správce údajů adekvátně postupováno?	☐	☐	☐
15.	Je nastaven systém řízení GDPR v organizaci i pro případy zpracování osobních údajů dítěte?	☐	☐	☐
16.	Jsou přijata opatření, aby byly poskytnuty subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem veškeré informace o zpracování osobních údajů?	☐	☐	☐
17.	Jsou přijata opatření, pokud se osobní údaje týkající se SÚ údajů získávají od SÚ, že poskytne správce v okamžiku získání OÚ subjektu údajů stanovené informace podle článku 13 GDPR?	☐	☐	☐
18.	Jsou přijata systémová opatření, pokud se osobní údaje poskytované v případě, že osobní údaje nebyly získány od subjektu údajů, že bude postupováno podle článku 14. GDPR?	☐	☐	☐
19.	Jsou přijata systémová opatření, že Subjekt údajů získá od správce údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím podle článku 15 GDPR?	☐	☐	☐

20.	Jsou přijata systémová opatření, že správce bez zbytečného odkladu opraví nepřesné osobní údaje? S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení dle článku 16 GDPR?	☐	☐	☐
21.	Jsou přijata systémová opatření, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají dle článku 17 GDPR?	☐	☐	☐
22.	Jsou přijata systémová opatření, aby správce omezil zpracování v kterémkoli z případů definovaných v článku 18 GDPR?	☐	☐	☐
23.	Jsou přijata systémová opatření, že správce oznámí jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s článkem 16, čl. 17 odst. 1 a článkem 18, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí, že správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje? Článek 19	☐	☐	☐
24.	Jsou přijata systémová opatření, že správce Subjektu umožní získat osobní údaje, které se ho týkají, jež poskytl správci, a předat tyto údaje jinému správci v souladu	☐	☐	☐
25.	Je systémově zajištěno, řešení pro naplnění souladu s článkem 21 GDPR, a to na právo vznést námitku?	☐	☐	☐
26.	Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká 22	☐	☐	☐
27.	Je systémově zajištěno, že správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků – čl. 24 GDPR.	☐	☐	☐
28.	S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.	☐	☐	☐
29.	Je systémově zajištěno, že správce zavádí jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů?	☐	☐	☐

30.	Jsou zavedeny technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné?	☐	☐	☐
31.	V případě společných správců jsou zpracována transparentní ujednání vymezující podíly na odpovědnosti za plnění povinností podle GDPR, zejména pokud jde o výkon práv subjektu údajů?	☐	☐	☐
32.	Jsou zavedeny systémové postupy pro zpracovávání záznamů o činnostech zpracování, za něž odpovídá, a to v rozsah článku 30 GDPR?	☐	☐	☐
33.	Jsou stanovena a provedena vhodná technická a organizační opatření, aby byla zajištěna úroveň zabezpečení odpovídající daným rizikům s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob?	☐	☐	☐
34.	Jsou stanoveny mechanismy, že při jakémkoliv porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí toto dozorovému úřadu dle článku 33 GDPR?	☐	☐	☐
35.	Jsou stanoveny mechanismy, že je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů dle článku 34 GDPR.	☐	☐	☐
36.	Je systémově zajištěno, pokud je pravděpodobné, že určitý druh zpracování, bude mít za následek vysoké riziko pro práva a svobody fyzických osob, že provede správce před zpracováním posouzení vlivu zamýšlených operací dle článku 35 GDPR. (Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení)	☐	☐	☐
37.	Jsou správně zhodnocena kritéria pro jmenování pověřence pro ochranu osobních údajů? 37	☐	☐	☐
38.	Je stanovena osoba odpovědná za SM řízení osobních údajů a hlášení incidentů?	☐	☐	☐
39.	Jsou pověřenci pro ochranu osobních údajů zajištěny práva a pravomoci, aby byl náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů? 38.	☐	☐	☐
40.	Je pověřenec kompetentní a náležitě proškolen?	☐	☐	☐

41.	Je uvnitř organizace zaveden systém provádění kontrol a testování funkčnosti opatření GDPR?	☐	☐	☐
42.	Je stav systémových opatření, kontrolních mechanismů a dosažená úroveň odpovídající případnému vydaní osvědčení o souladu a dosažení odpovídající úrovně od nezávislého orgánu/organizace? 42	☐	☐	☐

Kapitola měla za cíl provést analýzu aktuálního stavu bezpečnosti ve vybraných firmách za pomocí zvolených analýz. Byly vytvořeny katalogy hrozeb, které mohou svým způsobem ohrozit fungování firem. Na základě vyhodnocených hrozeb byla vytvořena KARS analýza, ve které se vypočítá, která rizika jsou pro daný systém „nejnebezpečnější“. Dále byly zpracovány GAP analýzy na ISMS a GDPR v organizacích. Výsledky analýz jsou v příloze diplomové práce. V následující kapitole budou popsány jak zjištěné nedostatky, tak doporučená opatření pro firmy.

7 VZÁJEMNÉ POROVNÁNÍ HROZEB A VYHODNOCENÍ GAP ANALÝZY ZVOLENÝCH SPOLEČNOSTÍ

V předchozí kapitole byly provedeny vhodné analýzy rizik, ze kterých mohou vyplývat určitá nebezpečí pro dané firmy. V následující kapitole dojde k porovnání zjištěných hrozeb u firem A, B.

Dále bude pojednáváno o výsledcích GAP analýz, které firmy zhotovily. Bude zobrazena otázka, která byla označena „Ne“ a poté popsáno vhodné řešení pro eliminaci hrozby. Pro eliminaci ISMS lze postupovat podle normy ISO 2700x. Pro opatření GDPR je vhodné najít řešení dle požadavků směrnice č. 95/46/ES.

7.1 Hrozby

Při porovnání hrozeb u firem A, B lze rozdělit hrozby podle jejich závažnosti. U vyhodnoceních analýz se ukázalo, že firmy, ať už jsou malých či velkých organizačních struktur, čelí neustálým hrozbám kybernetické bezpečnosti v podobě hackerských útoků či útokům malware a ransomware, které poté mohou vyvolat ostatní hrozby, jak vyplývá z vypracovaného katalogu hrozeb.

Firmy často uváděly, že významná je i četnost opakování hrozeb v souvislosti s nevědomostí zaměstnanců, jak pracovat s firemními ICT prostředky, nedodržováním podmínek BOZP a nedodržováním pracovních postupů. To poté může mít za následek nesprávnou funkčnost ICT prostředků a ohrožení dat (například když zaměstnanec odejde od počítače, aniž by realizoval jeho uzamčení a umožní tak cizí osobě snadný přístup k datům). Dále poměrně často dochází k vědomému vypínání testu antivirového programu v jeho průběhu.

7.2 Vyhodnocení GAP analýzy

Porovnáním GAP analýz na ISMS bylo zjištěno, že firmy mají poměrně dobře nastavenou politiku systému řízení bezpečnosti informací s menšími nedostatky, které na eliminaci nejsou finančně ani časově náročné. Pro poskytnutí optimálního řešení pro eliminaci hrozeb jsou pod otázkami uvedena optimální řešení. Pro ISMS jsou řešení znázorněna v podobě norem ISO 27001.

Pro naplnění požadavků GDPR bylo objeveno několik nedostatků, které je třeba aktuálně řešit, a to z toho důvodu, aby nedošlo k postihu ze strany dozorového úřadu a zároveň nastala

maximalizace ochrany naplňování GDPR ve firmách. Součástí hodnocení je i návrh optimálního řešení pro zlepšení vyhodnocených nedostatků.

7.2.1 **ISMS analýza**

Ve firmě A analýza odhalila, že nejsou pravidelně přezkoumávány logy událostí, zaznamenávající aktivity uživatelů. Pro firmu B bylo identifikováno více nedostatků, a to v podobě znění pracovní smlouvy, nebylo zvyšováno povědomí o bezpečnosti informací a nedocházelo k informování o změnách v bezpečnosti informací. Nebylo příliš dobře pracováno s kryptografickými opatřeními na ochranu informací pomocí kryptografických klíčů. A dále je třeba zlepšit současný stav opatření provozu IT a detekci malwarů.

Ve shrnutí obě organizace dosáhly optimálního stavu mezi vynaloženými náklady a dosaženou úrovní zabezpečení informačních aktiv.

Pro firmu A se v analýze ukázaly nedostatky v 19 otázce:

Tab. 11: *Otázka č. 19 v GAP analýze na ISMS* [zdroj: vlastní]

19.	Jsou systémově pořizovány, uchovány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací?

Řešení:

- *Musí být pořizovány, uchovány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.*
- *Prostředky pro zaznamenávání formou logů a logy musí být chráněny proti zfalšování a neoprávněnému přístupu*
- *Aktivity systémového administrátora a systémového operátora musí být logovány a logy chráněny a pravidelně přezkoumávány*
- *Hodiny všech důležitých systémů pro zpracování informací musí být v rámci organizace nebo bezpečnostních domén synchronizovány s jediným referenčním zdrojem času*[5]

[5] ISO 27001 Systém managementu bezpečnosti informací

Pro firmu B se v analýze ukázaly nedostatky v otázkách č. 6, 14, 17:

Tab. 12: *Otázka č. 6 v GAP analýze na ISMS* [zdroj: vlastní]

6.	Obsahují pracovní smlouvy a dále obchodní smlouvy ustanovení o povinnostech zaměstnanců a smluvních stran o jejich odpovědnostech za bezpečnost informací?

Řešení:

- *Vedení organizace musí po všech zaměstnancích a smluvních stranách požadovat dodržování bezpečnosti informací v souladu s ustavenými politikami a postupy v organizaci.*
- *Všichni zaměstnanci organizace, a je-li to relevantní i smluvní strany, musí s ohledem na svou pracovní náplň dostávat odpovídající vzdělávání a školení pro zvyšování povědomí bezpečnosti informací a musí být pravidelně informováni o změnách v politikách a postupech bezpečnosti informací*
- *Musí existovat formální proces disciplinárního řízení k přijetí opatření vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací*[6]

Tab. 13: *Otázka č. 19 v GAP analýze na ISMS* [zdroj: vlastní]

14.	Je vytvořena a implementována politika pro používání kryptografických opatření na ochranu informací, a to po dobu jejich celého životního cyklu?

Řešení:

- *Musí být vytvořena a implementována politika pro používání kryptografických opatření na ochranu informací*
- *Politika pro používání, ochranu a dobu existence kryptografických klíčů musí být vytvořena a implementována po celou dobu jejich životního cyklu.* [7]

Tab. 14*: Otázka č. 17 v GAP analýze na ISMS* [zdroj: vlastní]

17.	Jsou pro bezpečnost provozu IT – útoky – snížení rizika neoprávněného přístupu, malwary – zavedena a řízena opatření a odděleny sítě pro prostředí provozu, vývoje aj.?

[6] ISO 27001 Systém managementu bezpečnosti informací
[7] ISO 27001 Systém managementu bezpečnosti informací

Řešení:

- *Na ochranu proti malwaru musí být implementována opatření na jeho detekci, prevenci a obnovu, a to ve spojení s odpovídajícím bezpečnostním povědomím uživatelů*[8]

7.2.2 Vyhodnocení GDPR analýza

Výsledky GAP analýzy na GDPR odhalily několik nedostatků u každé z firem: Firma A využila pro implementaci GDPR specializovanou firmu, které se zabývá problematikou řešení GDPR. Pro firmu B implementace GDPR probíhala za pomocí vhodně vybraných opatření tak, aby byly splněny všechny požadované podmínky.

Pro firmu A se v analýze ukázaly nedostatky v GDPR u otázek 16,21 a 29

Tab. 15: *Otázka č. 16 v GAP analýze na GDPR* [zdroj: vlastní]

16.	Jsou přijata opatření, aby byly poskytnuty subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem veškeré informace o zpracování osobních údajů?

Navržené řešení: společnost nemá vytvořeny dostačující pracovní postupy pro poskytnutí transparentních informací, sdělení a postupů pro výkon práv subjektu údajů. To může mít za následek nedostatečné ověření identity žadatele, zejména při podání žádosti o poskytnutí informací elektronickou cestou. Problémy by mohly nastat při předání informací neoprávněné osobě a mohl by hrozit postih ze strany dozorového úřadu. Proto je třeba vytvořit postupy ověřování oprávněnosti žádosti za pomoci jednoduchých a jasných jazykových prostředků. Je třeba postupovat podle článků 12, 13 a 14 GDPR. Je třeba přidat popis o totožnosti a kontaktní údaje správce a jeho případného zástupce a právní důvod pro zpracování osobních údajů a účely zpracování, popřípadě doplnit dobu, po kterou budou osobní údaje uloženy a případně právo vznést námitku.

Tab. 16: *Otázka č. 21 v GAP analýze na GDPR* [zdroj: vlastní]

21.	Jsou přijata systémová opatření, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají dle článku 17 GDPR?

[8] ISO 27001 Systém managementu bezpečnosti informací

Navržené řešení: společnost nemá vytvořeny pracovní postupy, podle nichž by provedla výmaz osobních údajů v souladu s čl. 17 GDPR. To může mít za následek nemožnost včas a řádně vymazat informace související se zpracováním osobních údajů. Je třeba definovat odpovídající procesy včetně určení odpovědnosti za jejich realizaci, jako je např. v podání žádosti na výmaz realizovat tuto činnost do jednoho měsíce bez zbytečného odkladu od podání a to tak, aby došlo k výmazu osobních údajů.

Tab. 17: *Otázka č. 29 v GAP analýze na GDPR* [zdroj: vlastní]

29.	Je systémově zajištěno, že správce zavádí jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů?

Navržené řešení: v současné době není pseudonymizace osobních údajů využívána. Společnost nezpracovává rozsáhlé datové soubory. Změny většího charakteru by měly za následek nekoordinované procesy, chybí jasný plán, termíny, odpovědnost. Avšak společnost má zpracovány postupy, směrnice pro řízení dokumentů a údajů, a to v souladu s požadavky ČSN EN ISO 9001:2016 Systémy managementu kvality. Přesto by mohlo dojít k postihu ze strany dozorového úřadu. Proto je důležité vypracovat požadavky, které budou implementovány do systému managementu kvality, která má přímou návaznost na GDPR, aby byla eliminována možnost postihu ze strany dozorového úřadu.

Pro firmu B se v analýze ukázaly nedostatky v GDPR u otázek 5, 18, 41

Tab. 18: *Otázka č. 5 v GAP analýze na GDPR* [zdroj: vlastní]

5.	Je v SM řízení hrozeb v oblasti GDPR zaveden systém identifikace zdrojů nebezpečí a z nich vyplývajících rizik/hrozeb s metodikou úrovně opatření pro dosažení jejich přijatelnosti?

Navržené řešení: společnost nemá vytvořen a zaveden systém řízení hrozeb v oblasti GDPR, včetně metodiky identifikace souvisejících možných zdrojů nebezpečí. Pro eliminaci tohoto bodu je vhodné vytvořit vnitřní systémovou metodiku, ve formátu závazného vnitřního předpisu, který nastaví kritéria a parametry pro uvedenou oblast v rozsahu specifikace způsobu implementace a řízení navrženého systému, kritérií pro identifikaci, hodnocení a řízení zdrojů nebezpečí dané oblasti, eliminací nepřijatelných hrozeb – případně jejich snížení na přijatelnou úroveň. Dále stanovení povinností a odpovědností pro jednotlivé realizační a řídící zaměstnance a související fyzické osoby. Jako nedílnou součást uvedeného systému je doporučeno stanovit kontrolní mechanismy a postupy ověřující shodu

s nastavenými kritérií navrženého systému. I za tuto oblast je doporučeno stanovit odpovědné zaměstnance a uvážit systém ověřování funkčnosti stanovených postupů nezávislým kontrolním subjektem. Dále je ke zvážení pro vedení firmy B, zda aplikovat systémové standarty využívané oblasti ISMS (řada norem ČSN EN ISO 2700x) a vytvořit pro dané oblasti integrovaný systém řízení (ISŘ).

Tab. 19: *Otázka č. 18 v GAP analýze na GDPR* [zdroj: vlastní]

18.	Jsou přijata systémová opatření, pokud se osobní údaje poskytované v případě, že osobní údaje nebyly získány od subjektu údajů, že bude postupováno podle článku 14. GDPR

Navržené řešení: společnost nemá vytvořeny pracovní postupy, podle nichž by poskytla subjektu údajů informace související se zpracováním jeho osobních údajů. To může mít za následek nemožnost včas a řádně poskytnout subjektu údajů informace, související se zpracováním jeho osobních údajů. Zpracovat formou vnitřní řídící dokumentace pracovní postup, který ošetří systémové zajištění oprávněného zájmu dotčených subjektů údajů v souladu s požadavky článku 14 GDPR, zvláště se zvláštním zřetelem a důrazem nastavení identifikace všech možných vlastních zdrojů/úložišť osobních údajů vztažených k možným subjektům údajů, jejíž osobní údaje získal, zpracovával nebo zpracovává či jiným způsobem bylo či je správcem osobních údajů nakládáno. Se zvláštním zřetelem věnovat pozornost specifikaci účelu zpracování osobních údajů, právnímu základu zpracování jejich kategorií včetně kategorií dalších příjemců, nezbytnou dobu uložení a zdroj k získání osobních údajů. V uvedené řídící dokumentaci musí být dále definovány jednoznačně lhůty a forma sdílení uvedených informací. V přiměřeném rozsahu budou dále správcem údajů v uvedené řídící dokumentaci specifikovány postupy a povinnosti pověřených osob, které budou zajišťovat přenos těchto informací tak, aby byl zajištěn soulad s požadavky článku 14 s GDPR i s přihlédnutím k variantám, že výše uvedené povinnosti nebudou aplikovány, pokud a do té míry, kdy je možno aplikovat vyloučení poskytnutí uvedených údajů tak, jak je specifikováno v odstavci 5 uvedeného článku 14 GDPR.

Tab. 20: *Otázka č. 41 v GAP analýze na GDPR* [zdroj: vlastní]

41.	Je uvnitř organizace zaveden systém provádění kontrol a testování funkčnosti opatření GDPR?

Navržené řešení: nebyly identifikovány/předloženy systémové kontrolní mechanismy a ani jiné metody ověřování funkčnosti potřebných opatření směřujících k ověřování, že je zabezpečen kontinuální soulad s požadavky GDPR, a to v rozsahu odpovídajícím rozsahu

nakládání s údaji, uvedenými firmou B. Zpracovat metodiku provádění kontrol ověřování a testování funkčnosti implementovaného systému řízení jednotlivých stanovených procesů směřujících k docílení souladu s požadavky GDPR, případně dotčených zákonných předpisů či oprávněných požadavků zákazníků a dále také věnovat pozornost specifikaci typu kontrol vůči dodavatelům, např. formou smluvních podmínek požadovat možnost provedení zákaznického auditu – v tomto případě zvážit zohlednění situace, kdy dodavatel má uvedenou oblast prokazatelně zajištěnou systémem řízení, např. jako součást ISMS.

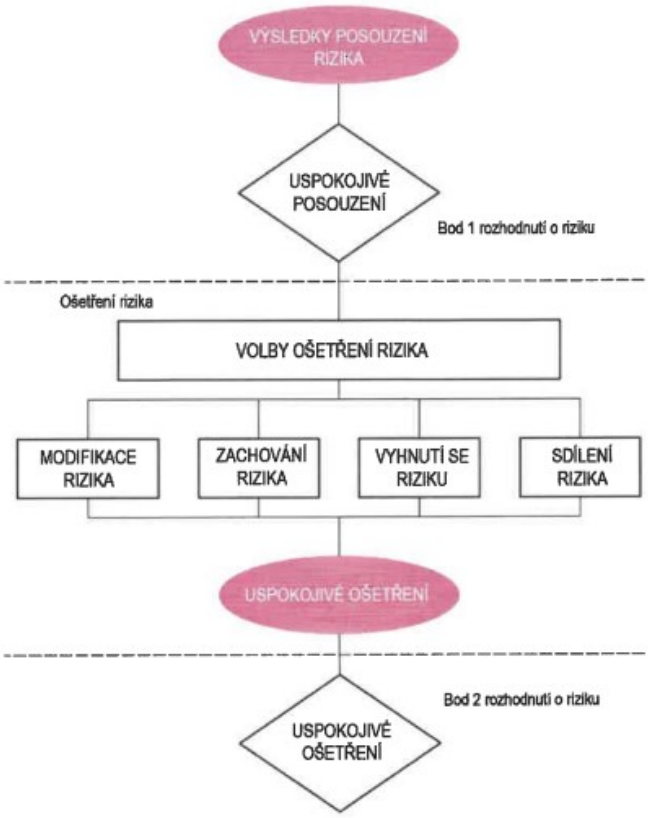
Náplní kapitoly bylo porovnat hrozby, které by mohly mít vzájemnou spojitost s ohrožením firem. Ve výsledku bylo zjištěno, že nejnebezpečnější hrozbou v kybernetickém prostoru, kde se nachází hackeři, malware, ransomware, a zároveň i zaměstnanci, kteří jsou ti, co často mohou za výskyt těchto hrozeb, jelikož neví (nejsou dostatečně seznámeni a proškoleni), jak správně zacházet s ICT prostředky a tím zvyšují šanci, že se tyto hrozby stanou realitou.

Dále byla snaha vyhodnotit firmami vyplněné GAP analýzy na ISMS a GDPR, a zároveň bylo navrženo vhodné řešení, jak takto zjištěné nedostatky odstranit. Pro ISMS lze řešení provést za pomocí norem ISO 27001, u GDPR bylo vytvořeno optimální řešení, které vyhovuje směrnici GDPR.

8 NÁVRHY OPATŘENÍ PRO ZVÝŠENÍ KYBERNETICKÉ BEZPEČNOSTI NA PRACOVIŠTÍCH FIREM

V předchozích kapitolách došlo k analýze, vyhodnocení a porovnání rizik a hrozeb pro zvolené společnosti, přičemž hlavním problémem se ukázala být neznalost zaměstnanců, jak pracovat s ICT prostředky, možný výskyt malware a ransomware, ztráta dokumentů a nestabilní internet.

Po zjištění problému je třeba reagovat a přijmout patřičná opatření pro minimalizaci rizik na přijatelnou úroveň. Organizace by měly uschovávat potřebné informace v dokumentové formě jako možný důkaz o ohrožení společnosti.



Obr. 8: *Možnosti ošetření rizik* [22]

Návrhy opatření budou realizované tak, aby pomohly eliminovat hrozby na přijatelnou úroveň a zároveň byly přínosem pro firmy v rámci kybernetické bezpečnosti.

8.1.1 Eliminace hrozby: nevědomost, jak pracovat s firemními ICT prostředky

Eliminace této hrozby by mohla umožnit odvrácení dalších zmiňovaných hrozeb. Uživatelem ICT je každý zaměstnanec společnosti, který přichází do styku s ICT a jeho daty,

nezávisle na tom, zda má právo data modifikovat, vkládat, kopírovat, mazat nebo jenom nahlížet. Každý uživatel ICT je možným nositelem rizika, aniž by za to vědomě nesl zodpovědnost.

Řešením proto může být tzv. kodex chování pro ICT na pracovišti, který by zaměstnanci museli potvrdit podpisem při nástupu do zaměstnání, a zároveň by zaměstnavatel měl kontrolovat, zda dochází k plnění těchto kodexů, případně pravidelnému proškolování. Povinností zaměstnance je brát v potaz, že poškozením či neodbornou manipulací může dojít k ohrožení celé společnosti. V případě prokázaní porušení tohoto kodexu hrozí zaměstnanci určité finanční sankce od momentu jejího vzniku.

Vypracovaný kodex slouží k eliminaci těch nejběžnějších hrozeb, které mohou zaměstnanci vědomě či nevědomě způsobovat. Společnost by měla provést jeho rozšíření a provádět pravidelná školení.

Každý uživatel musí dodržovat pravidla popsána v tomto kodexu

1. Dodržování všech manuálů a provedeného zaškolení, které je stvrzeno podpisem
2. Přihlašovat se vždy jen pod svým uživatelským účtem, které mu bylo předáno při nástupu do zaměstnání.
3. Nešířit a nestahovat nelegální SW.
4. Neprohlížet stránky s erotickou, rasistickou, násilnou tématikou.
5. Informace chráněné heslem nesdělovat žádné jiné osobě.
6. Automaticky provádět kontrolu na přítomnost virů pro všechny přijaté soubory, a to včetně souborů na výměnných médiích, stažených z internetu nebo připojených k emailu před jejich otevřením.
7. Při opuštění místnosti, kde se nachází PC zaměstnance, realizovat jeho uzamčení, aby nedošlo k neoprávněnému přístupu.
8. V případě bezpečnostního incidentu okamžitě informovat oprávněnou osobu o vzniku tohoto incidentu.
9. Není dovoleno umožnit práci jiné osobě pod svým uživatelským účtem anebo pracovat pod cizí identitou.
10. Nenechávat důležité materiály volně dostupné.
11. Nepředávat jakékoliv informace o zjištěných slabinách a nedostatcích osobám, které nejsou oprávněné tyto problémy řešit.
12. Nepoužívat služební email pro soukromou poštu.

13. Neukončovat běh antivirového programu
14. Tisk na tiskárně slouží pouze pro tisk prostředků potřebných pro firemní účely. Je zakázáno tisknout věci pro osobní účel.

Datum: ……. Jméno a příjmení: …….

Podpis: ……

8.1.2 **Eliminace hrozby: malware a ransomware**

K odhalení Malware může pomoci výrazně vysoká spotřeba CPU a GPU a časté přehřátí zařízení. Toto mohou být první příznaky, signalizující přítomnost malware pro šifrování kryptogramů [21]. Příznakem může být i to, že nelze stahovat nebo instalovat antivirový program. V případě odhalení malware či ransomware je třeba ihned odpojit počítač od internetu a nepoužívat jej a pokud je to možné, uvést jej do nouzového režimu, aby nedošlo k šíření škodlivého softwaru.

Už samotná ochrana proti malware a ransomware by měla být aplikována ve firewallech, ve kterých se dají nastavit bezpečnostní pravidla pro bezpečnost sítě. Firewally se poté rozdělují na hardwarové a softwarové. Hardwarové firewally nacházejí uplatnění u menších firem až středních velikostí.

Druhy firewallů:

- Filtrování paketů (Access Control List) – nejpočetnější druh firewallů, který provádí kontrolu paketů a zároveň podle požadavků může omezovat přístupy. Pokročilejší verzí je stavový firewall, který sleduje příchozí a odchozí pakety za určitou dobu ve čtvrté a nižší vrstvě.
- Proxy firewall – jedná se o nejbezpečnější typy firewallů z toho důvodu, že pracují v aplikační vrstvě modelu OSI
- Firewally nové generace – jedná se o firewally, které bezpečně rozpoznávají a blokují promyšlené hackerské útoky. Poskytují maximální ochranu a zároveň neomezují uživatele v používání internetu.

Jednou z podmínek správného fungování je provádění pravidelných aktualizací a pravidelných antivirových kontrol.

U počítačů by mělo být nastaveno a hlídáno to, zda není vypnutá brána firewallu. Jedním z preventivních opatření může být nastavení antivirů na pravidelnou analýzu v určitý čas, např. každý pátek v 10:00. Pro větší ochranu je dobré zvolit pravidelné zálohování, aby v případě výskytu malware byly důležité informace zachovány. Optimálním řešením jsou dvě zálohy – jedna by měla být offline a druhá by měla být online, nejlépe v cloudu.

Ve firmách je vhodné, aby administrátor ICT prostředků měl všechny ICT prostředky zaheslované z toho důvodu, aby zaměstnanci používali prostředky pouze pro pracovní účely a aby úmyslně či neúmyslně neinstalovali aplikace z neznámých zdrojů. U Windows 10 je možné nastavit, aby uživatele nemohli instalovat nic, kromě ověřených aplikací z Microsoft Store.

8.1.3 Eliminace hrozby: Ztráta dokumentů a odcizení firemních dokumentů a únik osobních údajů klientů

Proti ztrátě dokumentů jako jsou například objednávky, faktury, odvolávky, příjemky, expediční příkazy, dodací listy, avízo o platbě, vratky, katalogy zboží, ceníky, přehledy a další dokumentované informace/záznamy v písemné či elektronické podobě, které vychází z požadavků dotčených právních předpisů, smluvních povinností a požadavků jednotlivých stanovených procesů, je nutno zvolit ochranná opatření, a to podle stanovené klasifikace jejich důležitosti a seznamu možných zdrojů nebezpečí a úrovně hrozeb v případě aktivace specifikovaných i doposud neidentifikovaných zdrojů nebezpečí.

Navrženou optimální formou zálohy dokumentů je jejich převod z papírové formy do digitálního formátu (digitalizace dokumentů), a to z důvodu jejich následného efektivního řízení, sdílení, dohledatelnosti. Dokumenty jsou k dispozici kdekoliv, pokud jsou nahrané v na vhodném prostředku, jako je např. Cloud. Dochází tedy ke snížení až eliminaci hrozby/rizika ztrát potřebných dat, informací a důkazů o dosažených souladech s požadavky dotčených předpisů a stanovených procesů v systému řízení firmy, a to na přijatelnou úroveň.

Jako další opatření pro snížení ztráty dokumentů je možno navrhnout, aby každý dokument nezbytně se vyskytující v písemné/tištěné podobě dle požadavků jednotlivých stanovených procesů firmy a své klasifikace důležitosti, měl jasně definovanou metodiku zabezpečení. Tato metodika by mohla akceptovat základní standardy, které se opírají o systém evidence, který umožní neprodleně identifikovat ztrátu či zneužití, dále systémovou autorizaci oprávněných fyzických osob/zaměstnanců k nakládání s určitými typy dokumentů, a to ve

stanoveném řetězci posloupnosti jejich stanoveného pohybu a definovanou odpovědnost za jejich prokazatelný posun/předání na další pozici či místo uložení.

Další opatření mohou spočívat v autorizaci použití kopírovacích zařízení s identifikátory uživatele, včetně nastavení přístupových práv pro jednotlivé uživatele a řízení přístupu, umožňujícího nastavit limity uživatelského profilu. Vhodné je i využití dostupných softwarových nástrojů nabízejících funkcionalitu pro archivaci dokumentů jako jsou faktury, smlouvy či jiné dokumenty potřebné pro uchování.

Nelze opomenout, že každá firma je dále povinna ze zákona určité dokumenty ukládat po stanovenou dobu ve spisovnách a některé i archivovat – viz například požadavky zákonů

- Zákon č. 563/1991 Sb. o účetnictví
- Zákon č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů
- Zákon č. 235/2004 Sb. o dani z přidané hodnoty
- Zákon č. 582/1991 Sb. o organizaci a provádění sociálního zabezpečení
- Zákon č. 258/2000 Sb. o ochraně veřejného zdraví
- Zákon č. 262/2006 Sb. zákoník práce
- Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění

Pro převedení těchto dokumentů do digitální podoby je nutno, aby byla zajištěna jejich důvěryhodnost pro platnost archivovaných dokumentů, a to v podobách jako je:

- Věrohodnost původu,
- Neporušenost obsahu,
- Čitelnost. [40]

Řešením pro archivaci účetních dokladů může být to, aby společnost měla elektronický podpis a časové razítko pro věrohodnost dokumentů.

Řešením pro archivaci elektronické smlouvy se zákazníky a dokumenty podepsané se zaměstnanci může být software s vlastnostmi důvěryhodného archivu.

Jednoduchou formou zřízení časového razítka je u České pošty, ve které se dá definovat, kolik razítek bude použito za měsíc. Cena se odvíjí podle počtu razítek, čím více je časových razítek, tím nižší je cena této služby.

Maximální počet razítek za měsíc	Měsíční paušální cena	Doplatek za 1 razítko
	Cena s DPH 21%	Cena s DPH 21%
100	290,40 Kč	2,42 Kč
350	822,80 Kč	1,94 Kč
1000	1 936 Kč	1,45 Kč
3 500	4 840 Kč	1,21 Kč
10 000	12 100 Kč	0,97 Kč
35 000	33 880 Kč	0,73 Kč
100 000	72 600 Kč	0,48 Kč

Obr. 9: *Cena časového razítka u České pošty* [41]

8.1.4 **Eliminace hrozby: výpadky internetového připojení**

Hrozby, spojené s výpadky internetového připojení, mohou mít jednoduché řešeny. Nestabilnímu internetu lze předejít změnou dodavatele, který zajistí stabilní rychlost a kvalitu internetu.

Samotné chyby už mohou být přednastaveny v samotném routeru, kde mohou být vadné nebo nefunkční porty. Zvyšující se množství technických zařízení jako jsou např. mobilní telefony, nemusí routery stíhat pokrývat všechny zařízení. Případně Wi-Fi router může být umístěn dále od zařízení, které pak nestíhá spolehlivě pokrýt signál.

Podniky často využívají různé další funkce, než většina uživatelů v domácnostech potřebuje, např. vzdálený přístup, VPN.

Náplní kapitoly bylo přijít s vhodnými východisky na eliminaci hrozeb týkajících se kybernetické bezpečnosti, které byly zjištěny v předchozí kapitole, pojednávající o identifikaci hrozeb. S průběžným vývojem technologií je třeba, aby firmy byly neustále připraveny čelit novým výzvám a promyšleným hackerským útokům.

Nejdůležitějším východiskem z této situace je to, aby případné nebezpečí nepocházelo zevnitř firmy, kde zaměstnanci mohou způsobit svým vědomým i nevědomým chováním ve vztahu k zaměstnavateli velké škody. Je třeba neustálým proškolováním upozorňovat na možné negativní následky tohoto chování.

ZÁVĚR

Vývoj kybernetické bezpečnosti se datuje od vzniku prvních prvků IT prostředků. Protože zloději stále hledají možnosti, jak se dostat k snadnému výdělku, našli příležitost i v kyberprostoru, který využívá až půl populace světa. IT prostředky s možností fungování internetu se dnes už berou jako samozřejmost. Co má pro hackera nepochybně velkou hodnotu, jsou osobní údaje uživatelů, kteří používají internet. Na to musela reagovat i Evropská unie v podobě Směrnice na „Ochranu fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů“ a celé nařízení má přidanou hodnotu ke kybernetické bezpečnosti.

Cílem této diplomové práce bylo popsat problematiku kybernetické bezpečnosti s účinností GDPR ve vybraných organizacích.

Teoretická část byla rozdělena do čtyř kapitol, kde bylo cílem popsat kybernetickou bezpečnost v České republice a poté v Evropě a zároveň seznámit čtenáře s nařízením GDPR. Součástí teoretické části bylo popsání přístupu a skutečnosti týkající se úsilí, vynaloženého na eliminaci hrozeb, popis hrozeb, které mohou v kyberprostoru nastat za pomocí katalogu hrozeb, popsat určité metody, které lze použít k zjištění těchto hrozeb, jako jsou what – if analýza, penetrační testy, DPIA, PHA, GAP analýza či kontrolní listy. Popsat, jak případné analýzy probíhají za pomocí mezinárodní normy ISO 2700x. Poslední kapitola v teoretické části se věnovala opatřením kybernetické bezpečnosti na vazbu GDPR.

Praktická část byla soustředěna na aplikaci vědomostí z teoretické části do reálného prostředí. Pro naplnění praktické části byly vybrány dvě firmy, které mají odlišnou vnitřní charakteristiku, popis činnosti a počet zaměstnanců. Cílem bylo nalézt a seznámit společnosti s možnými nedostatky v kontextu kybernetické bezpečnosti a GDPR, a zvýšit jejich povědomí o vlastních nedostatcích. Pro zpřesnění byly poznatky hrozeb v kybernetickém prostoru znázorněny v KARS analýze, a to pro firmu A i B. Pro uplatnění poznatků z GDPR byla vyhotovena GAP analýza, v rámci, které musely firmy vyplnit dotazníky. GAP analýza byla vytvořena pomocí checklistu na ISMS a GDPR. Po vyplnění checklistů došlo k analýze výsledků a tvorbě vhodného návrhu na případné řešení. Pro vyhodnocené nedostatky byla popsána opatření pro každou společnost samostatně. Opatření pro ISMS analýzu byla nalezena v mezinárodní normě ISO 2700x a pro GDPR byla snaha přijít s návrhem vhodného řešení.

SEZNAM POUŽITÉ LITERATURY

[1] HRŮZA, Petr. *Kybernetická bezpečnost.* Brno : Univerzita obrany, 2012. ISBN 978-80-7231-914-5.

[2] KOLOUCH, Jan. *CyberCrime.* Praha : CZ.NIC, 2016. ISBN 978-80-88168-18-8.

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

[4] Kučínský, Adam. Zákon o kybernetické bezpečnosti a směrnice NIS. *Interní auditor: čtvrletník Českého institutu interních auditorů.* Březen, 2016.

[5] Zákon o kybernetické bezpečnosti a směrnice NIS. Praha : Národní bezpečnostní úřad Národní centrum kybernetické bezpečnosti, 2016.

[6] *Stát rozšíří adresáty zákona o kybernetické bezpečnosti, spadnou do něj vyhledávače i některé e-shopy* [online]. [cit. 5.2.2019]. Dostupné z: http://www.ceska-justice.cz/2016/09/stat-rozsiri-adresaty-zakona-o-kyberneticke-bezpecnosti-spadnou-nej-vyhledavace-nektere-e-shopy/

[7] NÚKIB *Podpůrný materiál k identifikaci poskytovatelů digitálních služeb* [online]. [cit. 7.2.2019]. Dostupné z: https://gdpr-dpo.webnode.cz/_files/200000138-6d2346e1ca/Poskytovatel%20digit%C3%A1ln%C3%AD%20slu%C5%BEby.pdf

[8] NBU *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* [online]. [cit. 9.2.2019]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

[9] *Národní strategie kybernetické bezpečnosti České republiky 2015-2020* – studentský portál o bezpečnosti [online]. [cit. 9.2.2019]. Dostupné z: http://www.securityoutlines.cz/narodni-strategie-kyberneticke-bezpecnosti-ceske-republiky-na-obdobi-let-2015-2020/

[10] SMEJKAL, Vladimír. *Jaké povinnosti vyplývají pro orgány veřejné moci ze zákona o kybernetické bezpečnosti?* [online]. [cit. 9.2.2019]. Dostupné z: https://www.mvcr.cz/soubor/smejkal-v-pdf.aspx

[11] Vyhláška č. 82/2018 Sb., vyhláška o kybernetické bezpečnosti.

[12] Vyhláška č. 437/2017 Sb., vyhláška o kritériích pro určení provozovatele základní služby

[13] Vyhláška č. 317/2014 Sb., Vyhláška o významných informačních systémech a jejich určujících kritériích

[14] NEZMAR, Luděk. *GDPR: praktický průvodce implementací.* Praha : Grada Publishing, 2017. 978-80-271-0668-4.

[15] Základní příručka k GDPR: Úřad pro ochranu osobních údajů. [online]. 2013 [cit. 12.2.2019]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744

[16] GUARD7. Bezpečnost práce a požární ochrana [online]. [cit. 12.2.2019]. Dostupné z: http://www.guard7.cz/gdpr/osobni-udaje

[17] GUARD7. Bezpečnost práce a požární ochrana [online]. [cit. 12.2.2019]. Dostupné z: http://www.guard7.cz/gdpr/zvlastni-kategorie-osobnich-udaju

[18] GUARD7. Bezpečnost práce a požární ochrana [online]. [cit. 12.2.2019]. Dostupné z: http://www.guard7.cz/gdpr/zvlastni-kategorie-osobnich-udaju

[19] GDPR Rodičovský souhlas [online]. [online]. [cit. 12.2.2019]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/rodicovsky-souhlas/

[20] Základní příručka k GDPR: Oblasti zpracování osobních údajů: [online]. [cit. 13.2.2019]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=1267

[21] 5 nejčastějších útoků na malé firmy [online]. [cit. 18.3.2019]. Dostupné z: https://www.itsec-nn.com/5-nejcastejsich-utoku-na-male-firmy/

[22] ČSN ISO/IEC 27005 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. Česká technická norma.

[23] SPIR / GDPR [online]. [cit. 25.2.2019]. Dostupné z: http://gdpr.spir.cz/?p=10

[24] Posouzení vlivu na ochranu osobních údajů podle – Sbírka zákonů, judikatura, právo [online]. [cit. 25.2.2019]. Dostupné z: https://www.epravo.cz/top/clanky/posouzeni-vlivu-na-ochranu-osobnich-udaju-podle-gdpr-105892.html

[25] Penetrační testy webových aplikací [online] [cit. 26.2.2019]. Dostupné z: https://www.krucek.cz/cz/penetracni-testy-webovych-aplikaci/

[26] Penetrační testy infrastruktury sítě, webových aplikací a internetových služeb [cit. 26.2.2019]. Dostupné z: https://tns.cz/it-produkty-a-sluzby/penetracni-testy/

[27] BEŇKOVÁ, Karin a Jiří CÍSEK. Představení služeb Konica Minolta GDPR [online]. 28. 6. 2017, [cit. 25.2.2019]. Dostupné z: https://www.konicaminolta.cz/fileadmin/content/cz/Business_Solutions/meta/GDPR/2017-06-28_Prezentace_GDPR_seminar.pdf

[28] Co – když analýza (What-if Analysis) [online]. [cit. 26.2.2019]. Dostupné z: https://managementmania.com/cs/co-kdyz-analyza-what-if-analysis

[29] TĚŠITELOVÁ, Vladimíra, Radek POLICAR a Ladislav DUŠEK. Jak implementovat v ambulantní sféře NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY 2016/679 [online]. 1.3.2018 [cit. 2.3.2019]. Dostupné z: http://uzis.cz/system/files/u44/gdpr_AMBUL_20180301_metodika_implementace_ambulantni_sfera.pdf

[30] GDPR Audit Tool. Online a zdarma. [cit. 2.3.2019]. Dostupné z: https://www.ceskenoviny.cz/pr/zpravy/gdpr-audit-tool-online-a-zdarma/1571035

[31] GDPR and ISO 27001 Mapping: Is ISO 27001 Enough for GDPR Compliance [cit. 2.19.2019]. Dostupné z: https://blog.netwrix.com/2018/04/26/gdpr-and-iso-27001-mapping-is-iso-27001-enough-for-gdpr-compliance/

[32] ISO 27001 Systém managementu bezpečnosti informací [online]. [cit. 3.3.2019]. Dostupné z: https://managementmania.com/cs/iso-27001

[33] Zákon č.181/2014 Sb., o kybernetické bezpečnosti

[34] KODET, Jaroslav. Kybernetický zákon: Využijte naplno open source nástroje [online]. 1.4.2015 [cit. 11.3.2019]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[35] Informace k fyzické bezpečnosti [online]. [cit. 11.3.2019]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/1014-informace/

[36] Pulling fraud out of the shadows Global Economic Crime and Fraud Survey 2018 – Czech results [online]. [cit. 2.3.2019]. Dostupné z: https://www.pwc.com/cz/en/sluzby/forenzni-sluzby/global-economic-crime-survey.html

[37] ČSN EN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. Česká technická norma.

[38] Penetrační testy [online]. [cit. 5. 4.2019]. Dostupné z: https://www.aec.cz/cz/produkty-a-sluzby/Stranky/penetracni-testy.aspx

[39] ČSN ISO 31000. Management – Principy a směrnice. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010

[40] Zákon č. 235/2004 Sb. Zákon o dani z přidané hodnoty

[41] Ceník časových razítek [online]. [cit. 20.4.2019]. Dostupné z: http://www.postsignum.cz/casova_razitka.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
ICT	Informační a komunikační technologie
GDPR	Obecné nařízení o ochraně osobních údajů
ČR	Česká republika
EU	Evropská unie
NIS	Network Information Security
NATO	Severoatlantická aliance
IP	Internet Protocol
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CPU	Central processing unit
GPU	Graphic Processing Unit
DPIA	Data Protection Impact Assessment
GAP	Diferenční analýza
PHA	Preliminary hazard analysis
KARS	Kvalitativní analýza souvztažnosti rizik
ISO	International Organization for Standardization
IT	Informační teologie
ISMS	Information Security Management System

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Vyhodnocená Gap analýza na ISMS od firmy A

Vyhodnocená Gap analýza na ISMS od firmy B

Vyhodnocený kontrolní seznam na GDPR od firmy A

Vyhodnocený kontrolní seznam na GDPR od firmy B

VYHODNOCENÁ GAP ANALÝZA NA ISMS OD FIRMY A

GAP ANALÝZA-KONTROLNÍ SEZNAM ISMS

ANALÝZA ZA ÚČELEM NALEZENÍ NESROVNALOSTÍ MEZI CÍLI DOSAŽENÝMI A POŽADOVANÝMI.
ANALÝZA SE ZAMĚŘUJE TAKÉ NA PROZKOUMÁNÍ A ODKRYTÍ PŘÍLEŽITOSTÍ

Kontrolovaná oblast/zadání: úvodní kontrola stavu GDPR a systémového zajištění souladu **Kontrolovaná organizace:** **Upozornění**: Odpověď ANO je přípustná pouze v případech, kdy kontrolované požadavky jsou odpovídající požadované úrovni a doloženy VS (vedení společnosti) dokumentovanými informacemi – důkazy.		**ANO**	**NE**	**Irelevantní oblast**
1.	Je zpracován v organizaci relevantní kontext organizace pro zajištění souladu s požadavky GDPR?	☒	☐	☐
2.	Jsou VS v SM vydány, revidovány a sdíleny Politiky pro řízení oblasti GDPR, a to i pro případy krizí, havárií a katastrof?	☒	☐	☐
3.	Jsou VS ustanoveny Politiky pro implementování primárních opatření zaměřených na zajištění oprávněných zájmů organizace a soulad s požadavky GDPR, zákonů ČR a se smluvní požadavky?	☒	☐	☐
4.	Jsou definovány a přiděleny v SM ISMS odpovědnosti v oblasti GDPR informací a jsou uživatelé informací prokazatelně proškolení o své odpovědnosti za jejich ochranu?	☒	☐	☐
5.	Jsou stanovena bezpečnostní opatření (T, O, S) na ochranu osobních údajů, které jsou přístupné, zpracovávané, ukládané v místech pro práci, i na dálku, včetně mobilních zařízení?	☒	☐	☐
6.	Obsahují pracovní smlouvy a dále obchodní smlouvy ustanovení o povinnostech zaměstnanců a smluvních stran o jejich odpovědnostech za bezpečnost informací?	☒	☐	☐
7.	Je stanoven v SM ISMS systém požadování plnění požadavků a systém kontrol plnění povinností a postihů v ISMS v souladu s Politikami a postupy?	☒	☐	☐
8.	Jsou v SM ISMS dokumentovaným způsobem identifikována aktiva organizace a definovány odpovědnosti k jejich přiměřené ochraně?	☒	☐	☐

9.	Je v SM ISMS zaveden systém identifikace a vyhodnocování zdrojů nebezpečí a z nich vyplývajících rizik/hrozeb s metodikou úrovně opatření pro dosažení jejich přijatelnosti?	☒	☐	☐
10.	Jsou všechny v SM ISMS informace klasifikovány s ohledem na zákonné požadavky, jejich hodnotu, kritičnost a citlivost vůči neoprávněnému prozrazení nebo modifikaci?	☒	☐	☐
11.	Jsou zavedeny postupy pro správu výměnných médií v souladu se schématem klasifikace informací přijatým organizací?	☒	☐	☐
12.	Je zaveden v SM ISMS systém řízení přepravy a nakládání s médii, a jejich bezpečnou likvidací, pokud nejsou dále upotřebitelná, v souladu s formalizovanými postupy?	☒	☐	☐
13.	Je ustavena v SM ISMS politika a řízení oprávnění/autorizace přístupu uživatelů podle jejich rozličné úrovně oprávnění k informačním sítím, síťovým službám podle jejich rizikovosti?	☒	☐	☐
14.	Je vytvořena a implementována politika pro používání kryptografických opatření na ochranu informací, a to po dobu jejich celého životního cyklu?	☒	☐	☐
15.	Je vytvořena a implementována politika předcházení neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací?	☒	☐	☐
16.	Jsou stanoveny politiky a opatření pro předcházení hrozbám – ztrát, poškození, krádežím nebo kompromitaci aktiv a přerušení činností organizace?	☒	☐	☐
17.	Jsou pro bezpečnost provozu IT – útoky – snížení rizika neoprávněného přístupu, malwary – zavedena a řízena opatření a odděleny sítě pro prostředí provozu, vývoje aj.?	☒	☐	☐
18.	Jsou záložní kopie informací, softwaru a binárních obrazů systému pořizovány a testovány v pravidelných intervalech podle nastaveného systému pro danou oblast?	☒	☐	☐
19.	Jsou systémově pořizovány, uchovávány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací?	☐	☒	☐
20.	Jsou vytvořeny, popsány v SM ISMS a implementovány postupy řízené instalace softwaru na provozních systémech?	☒	☐	☐

21.	Je zaveden a implementován systém k ochraně informací v systémech a aplikacích a jsou v tomto smyslu sítě řízeny, spravovány a kontrolovány?	☒	☐	☐
22.	Je zaveden IT systém získání informací o zranitelností systémů, hodnocení úrovně ohrožení organizace, připravena proaktivní i reaktivní opatření na zvládání souvisejících rizik a incidentů?	☒	☐	☐
23.	Je zaveden, aplikován a kontrolován řízený systém bezpečnosti informací při jejich přenosu v rámci organizace, s externími subjekty a daty zpřístupněnými vně subjektu?	☒	☐	☐
24,	Je zaveden v rámci ISMS systém pro monitoring, přezkoumávání a audit služeb dodavatelů, kde se nedají vyloučit zdroje nebezpečí pro oblast ISMS?	☐	☐	☒
25.	Je uvnitř organizace zaveden systém provádění kontrol a testování funkčnosti systému ISMS?	☒	☐	☐

VYHODNOCENÁ GAP ANALÝZA NA ISMS OD FIRMY B

GAP ANALÝZA-KONTROLNÍ SEZNAM ISMS

ANALÝZA ZA ÚČELEM NALEZENÍ NESROVNALOSTÍ MEZI CÍLI DOSAŽENÝMI A POŽADOVANÝMI.
ANALÝZA SE ZAMĚŘUJE TAKÉ NA PROZKOUMÁNÍ A ODKRYTÍ PŘÍLEŽITOSTÍ

	Kontrolovaná oblast/zadání: úvodní kontrola stavu GDPR a systémového zajištění souladu **Kontrolovaná organizace:** **Upozornění**: Odpověď ANO je přípustná pouze v případech, kdy kontrolované požadavky jsou odpovídající požadované úrovni a doloženy VS (vedení společnosti) dokumentovanými informacemi – důkazy.	**ANO**	**NE**	**Irelevantní oblast**
1.	Je zpracován v organizaci relevantní kontext organizace pro zajištění souladu s požadavky GDPR?	☒	☐	☐
2.	Jsou VS v SM vydány, revidovány a sdíleny Politiky pro řízení oblasti GDPR, a to i pro případy krizí, havárií a katastrof?	☒	☐	☐
3.	Jsou VS ustanoveny Politiky pro implementování primárních opatření zaměřených na zajištění oprávněných zájmů organizace a soulad s požadavky GDPR, zákonů ČR a se smluvní požadavky?	☒	☐	☐
4.	Jsou definovány a přiděleny v SM ISMS odpovědnosti v oblasti GDPR informací a jsou uživatelé informací prokazatelně proškolení o své odpovědnosti za jejich ochranu?	☒	☐	☐
5.	Jsou stanovena bezpečnostní opatření (T, O, S) na ochranu osobních údajů, které jsou přístupné, zpracovávané, ukládané v místech pro práci, a i na dálku včetně mobilních zařízení?	☒	☐	☐
6.	Obsahují pracovní smlouvy a dále obchodní smlouvy ustanovení o povinnostech zaměstnanců a smluvních stran o jejich odpovědnostech za bezpečnost informací?	☐	☒	☐
7.	Je stanoven v SM ISMS systém požadování plnění požadavků a systém kontrol plnění povinností a postihů v ISMS v souladu s Politikami a postupy?	☒	☐	☐
8.	Jsou v SM ISMS dokumentovaným způsobem identifikována aktiva organizace a definovány odpovědnosti k jejich přiměřené ochraně?	☒	☐	☐

9.	Je v SM ISMS zaveden systém identifikace a vyhodnocování zdrojů nebezpečí a z nich vyplývajících rizik/hrozeb s metodikou úrovně opatření pro dosažení jejich přijatelnosti?	☒	☐	☐
10.	Jsou všechny v SM ISMS informace klasifikovány s ohledem na zákonné požadavky, jejich hodnotu, kritičnost a citlivost vůči neoprávněnému prozrazení nebo modifikaci?	☒	☐	☐
11.	Jsou zavedeny postupy pro správu výměnných médií v souladu se schématem klasifikace informací přijatým organizací?	☒	☐	☐
12.	Je zaveden v SM ISMS systém řízení přepravy a nakládání s médii, a jejich bezpečnou likvidací, pokud nejsou dále upotřebitelná v souladu s formalizovanými postupy?	☒	☐	☐
13.	Je ustavena v SM ISMS politika a řízení oprávnění/autorizace přístupu uživatelů podle jejich rozličné úrovně oprávnění k informačním sítím, síťovým službám podle jejich rizikovosti?	☒	☐	☐
14.	Je vytvořena a implementována politika pro používání kryptografických opatření na ochranu informací, a to po dobu jejich celého životního cyklu?	☐	☒	☐
15.	Je vytvořena a implementována politika předcházení neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací?	☒	☐	☐
16.	Jsou stanoveny politiky a opatření pro předcházení hrozbám – ztrát, poškození, krádežím nebo kompromitaci aktiv a přerušení činností organizace?	☒	☐	☐
17.	Jsou pro bezpečnost provozu IT – útoky – snížení rizika neoprávněného přístupu, malwary – zavedenyaa řízena opatření a odděleny sítě pro prostředí provozu, vývoje aj.?	☐	☒	☐
18.	Jsou záložní kopie informací, softwaru a binárních obrazů systému pořizovány a testovány v pravidelných intervalech podle nastaveného systému pro danou oblast?	☐	☐	☒
19.	Jsou systémově pořizovány, uchovány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací?	☒	☐	☐
20.	Jsou vytvořeny, popsány v SM ISMS a implementovány postupy řízené instalace softwaru na provozních systémech?	☐	☐	☒

21.	Je zaveden a implementován systém k ochraně informací v systémech a aplikacích a jsou v tomto smyslu sítě řízeny, spravovány a kontrolovány?	☒	☐	☐
22.	Je zaveden IT systém získání informací o zranitelností systémů, hodnocení úrovně ohrožení organizace, připravena proaktivní i reaktivní opatření na zvládání souvisejících rizik a incidentů?	☒	☐	☐
23.	Je zaveden, aplikován a kontrolován řízený systém bezpečnost informací při jejich přenosu v rámci organizace, s externími subjekty a daty zpřístupněnými vně subjektu?	☒	☐	☐
24,	Je zaveden v rámci ISMS systém pro monitoring, přezkoumávání a audit služeb dodavatelů, kde se nedají vyloučit zdroje nebezpečí pro oblast ISMS?	☒	☐	☐
25.	Je uvnitř organizace zaveden systém provádění kontrol a testování funkčnosti systému ISMS?	☒	☐	☐

VYHODNOCENÝ KONTROLNÍ SEZNAM NA GDPR OD FIRMY A

GAP ANALÝZA-KONTROLNÍ SEZNAM GDPR ANALÝZA ZA ÚČELEM NALEZENÍ NESROVNALOSTÍ MEZI CÍLI DOSAŽENÝMI A POŽADOVANÝMI. ANALÝZA SE ZAMĚŘUJE TAKÉ NA PROZKOUMÁNÍ A ODKRYTÍ PŘÍLEŽITOSTÍ KE ZLEPŠENÍ				
<u>Kontrolovaná oblast/zadání</u>: úvodní kontrola stavu GDPR a systémového zajištění souladu Organizace při implementaci požadavků obvykle postupují formou projektu, kdy postupně zavádějí požadavky nařízení GDPR. **Upozornění: Tento seznam navazuje kontinuálně na požadavky pro řízení ISMS** **Upozornění**: Odpověď ANO je přípustná pouze v případech, kdy kontrolované požadavky jsou odpovídající požadované úrovni a doloženy VS (vedení společnosti) dokumentovanými informacemi – důkazy.		**ANO**	**NE**	**Irelevantní oblast**
1.	Je rozsah systému řízení ochrany osobních údajů dostupný jako dokumentované a řízené informace?	☒	☐	☐
2.	Zahrnuje systém řízení ochrany osobních údajů specifikaci řízených dokumentovaných informací požadovaných GDPR?	☒	☐	☐
3.	Obsahují pracovní smlouvy a obchodní smlouvy ustanovení o povinnostech zaměstnanců a smluvních stran o jejich odpovědnostech za GDPR?	☒	☐	☐
4.	Jsou uzavřeny smlouvy o ochraně OÚ s dodavateli služeb, kteří jsou dotčení povinnostmi v oblasti GDPR např: IT, poskytovatelé PLS, zákazníci, dodavatelé služeb, auditoři atd. dle kontextu	☒	☐	☐
5.	Je v SM řízení hrozeb v oblasti GDPR zaveden systém identifikace zdrojů nebezpečí a z nich vyplývajících rizik/hrozeb s metodikou úrovně opatření pro dosažení jejich přijatelnosti?	☒	☐	☐
6.	Má organizace nastaveny postupy/procesy pro řešení neshod v oblasti ochrany osobních údajů?	☒	☐	☐
7.	Jsou pro všechny identifikované operace nebo soubor operací s osobními údaji nebo soubory osobních údajů stanoveny postupy za účelem jejich řízené ochrany, používání a ukládání?	☒	☐	☐
8.	Je vytvořen a průběžně aktualizován Registr osobních údajů se specifikací vlastníků, rizik a požadované úrovni ochrany?	☒	☐	☐

9.	Je stanovena klasifikace ochrany jednotlivých osobních údajů podle klasifikace rizik?	☒	☐	☐
10.	Je vytvořen a aktualizován řídící dokument SM o spisové a archivační činnosti osobních údajů?	☒	☐	☐
11.	Jsou zpracovávány/definovány zvláštní kategorie údajů podle článku 9 GDPR?	☒	☐	☐
12.	Jsou stanoveny v SM povinnosti a postupy zajišťující Zákonnost zpracování dle Článek 6 GDPR	☒	☐	☐
13.	Jsou systémově zajištěny správcem údajů od dotčených subjektů údajů dokumentovaná či zjevná potvrzení (doložitelná) o svolení/souhlasu ke zpracování údajů dle Článek 7 GDPR?	☒	☐	☐
14.	Je systémově a technicky zabezpečeno, že subjekt údajů má právo svůj souhlas kdykoli odvolat a v souvislosti s tím bude ze strany správce údajů adekvátně postupováno?	☒	☐	☐
15.	Je nastaven systém řízení GDPR v organizaci i pro případy zpracování osobních údajů dítěte?	☒	☐	☐
16.	Jsou přijata opatření, aby byly poskytnuty subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem veškeré informace o zpracování osobních údajů?	☐	☒	☐
17.	Jsou přijata opatření, pokud se osobní údaje týkající se SÚ údajů získávají od SÚ, že poskytne správce v okamžiku získání OÚ subjektu údajů stanovené informace podle článku 13 GDPR?	☒	☐	☐
18.	Jsou přijata systémová opatření, pokud se osobní údaje poskytované v případě, že osobní údaje nebyly získány od subjektu údajů, že bude postupováno podle článku 14. GDPR?	☒	☐	☐
19.	Jsou přijata systémová opatření, že Subjekt údajů získá od správce údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím podle článku 15 GDPR?	☒	☐	☐
20.	Jsou přijata systémová opatření, že správce bez zbytečného odkladu opraví nepřesné osobní údaje. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení dle článku 16 GDPR?	☒	☐	☐

21.	Jsou přijata systémová opatření, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají dle článku 17 GDPR?	☐	☒	☐
22.	Jsou přijata systémová opatření, aby správce omezil zpracování, v kterémkoli z případů definovaných v článku 18 GDPR?	☒	☐	☐
23.	Jsou přijata systémová opatření, že správce oznámí jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s článkem 16, čl. 17 odst. 1 a článkem 18, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí, že správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje? Článek 19	☒	☐	☐
24.	Jsou přijata systémová opatření, že správce Subjektu umožní získat osobní údaje, které se ho týkají, jež poskytl správci, a předat tyto údaje jinému správci v souladu	☒	☐	☐
25.	Je systémově zajištěno řešení pro naplnění souladu s článkem 21 GDPR, a to na právo vznést námitku?	☒	☐	☐
26.	Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká – čl. 22 GDPR	☒	☐	☐
27.	Je systémově zajištěno, že správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků – čl. 24 GDPR?	☒	☐	☐
28.	S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.	☒	☐	☐
29.	Je systémově zajištěno, že správce zavádí jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů?	☐	☒	☐
30.	Jsou zavedeny technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné?	☒	☐	☐

31.	V případě společných správců jsou zpracována transparentní ujednání vymezující podíly na odpovědnosti za plnění povinností podle GDPR, zejména pokud jde o výkon práv subjektu údajů?	☒	☐	☐
32.	Jsou zavedeny systémové postupy pro zpracovávání záznamů o činnostech zpracování, za něž odpovídá, a to v rozsahu článku 30 GDPR?	☒	☐	☐
33.	Jsou stanovena a provedena vhodná technická a organizační opatření, aby byla zajištěna úroveň zabezpečení odpovídající daným rizikům s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob?	☒	☐	☐
34.	Jsou stanoveny mechanismy, že při jakémkoliv porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí toto dozorovému úřadu dle článku 33 GDPR?	☒	☐	☐
35.	Jsou stanoveny mechanismy, že je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů dle článku 34 GDPR.	☒	☐	☐
36.	Je systémově zajištěno, pokud je pravděpodobné, že určitý druh zpracování, bude mít za následek vysoké riziko pro práva a svobody fyzických osob, že provede správce před zpracováním posouzení vlivu zamýšlených operací dle článku 35 GDPR. (Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení)	☒	☐	☐
37.	Jsou správně zhodnocena kritéria pro jmenování pověřence pro ochranu osobních údajů? 37	☒	☐	☐
38.	Je stanovena osoba odpovědná za SM řízení osobních údajů a hlášení incidentů?	☒	☐	☐
39.	Jsou pověřenci pro ochranu osobních údajů zajištěny práva a pravomoci, aby byl náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů? Čl. 38.	☒	☐	☐
40.	Je pověřenec kompetentní a náležitě proškolen?	☒	☐	☐
41.	Je uvnitř organizace zaveden systém provádění kontrol a testování funkčnosti opatření GDPR?	☒	☐	☐
42.	Je stav systémových opatření, kontrolních mechanismů a dosažená úroveň odpovídající případnému vydaní osvědčení o souladu a dosažení odpovídající úrovně od nezávislého orgánu/organizace? Čl. 42	☒	☐	☐

VYHODNOCENÝ KONTROLNÍ SEZNAM NA GDPR OD FIRMY B

GAP ANALÝZA-KONTROLNÍ SEZNAM GDPR ANALÝZA ZA ÚČELEM NALEZENÍ NESROVNALOSTÍ MEZI CÍLI DOSAŽENÝMI A POŽADOVANÝMI. ANALÝZA SE ZAMĚŘUJE TAKÉ NA PROZKOUMÁNÍ A ODKRYTÍ PŘÍLEŽITOSTÍ KE ZLEPŠENÍ				
<u>Kontrolovaná oblast/zadání</u>: úvodní kontrola stavu GDPR a systémového zajištění souladu Organizace při implementaci požadavků obvykle postupují formou projektu, kdy postupně zavádějí požadavky nařízení GDPR. **Upozornění: Tento seznam navazuje kontinuálně na požadavky pro řízení ISMS** **Upozornění**: Odpověď ANO je přípustná pouze v případech, kdy kontrolované požadavky jsou odpovídající požadované úrovni a doloženy VS (vedení společnosti) dokumentovanými informacemi – důkazy.		**ANO**	**NE**	**Irelevantní oblast**
1.	Je rozsah systému řízení ochrany osobních údajů dostupný jako dokumentované a řízené informace?	☒	☐	☐
2.	Zahrnuje systém řízení ochrany osobních údajů specifikaci řízených dokumentovaných informací požadovaných GDPR?	☒	☐	☐
3.	Obsahují pracovní smlouvy a obchodní smlouvy ustanovení o povinnostech zaměstnanců a smluvních stran o jejich odpovědnostech za GDPR?	☒	☐	☐
4.	Jsou uzavřeny smlouvy o ochraně OÚ s dodavateli služeb, kteří jsou dotčení povinnostmi v oblasti GDPR např: IT, poskytovatelé PLS, zákazníci, dodavatelé služeb, auditoři atd. dle kontextu	☒	☐	☐
5.	Je v SM řízení hrozeb v oblasti GDPR zaveden systém identifikace zdrojů nebezpečí a z nich vyplývajících rizik/hrozeb s metodikou úrovně opatření pro dosažení jejich přijatelnosti?	☐	☒	☐
6.	Má organizace nastaveny postupy/procesy pro řešení neshod v oblasti ochrany osobních údajů?	☒	☐	☐
7.	Jsou pro všechny identifikované operace nebo soubor operací s osobními údaji nebo soubory osobních údajů stanoveny postupy za účelem jejich řízené ochrany, používání a ukládání?	☒	☐	☐
8.	Je vytvořen a průběžně aktualizován Registr osobních údajů se specifikací vlastníků, rizik a požadované úrovni ochrany?	☒	☐	☐

9.	Je stanovena klasifikace ochrany jednotlivých osobních údajů podle klasifikace rizik?	☒	☐	☐
10.	Je vytvořen a aktualizován řídící dokument SM o spisové a archivační činnosti osobních údajů?	☒	☐	☐
11.	Jsou zpracovávány/definovány zvláštní kategorie údajů podle článku 9 GDPR?	☒	☐	☐
12.	Jsou stanoveny v SM povinnosti a postupy zajišťující Zákonnost zpracování dle Článek 6 GDPR	☒	☐	☐
13.	Jsou systémově zajištěny správcem údajů od dotčených subjektů údajů dokumentovaná či zjevná potvrzení (doložitelná) o svolení/souhlasu ke zpracování údajů dle Článek 7 GDPR?	☒	☐	☐
14.	Je systémově a technicky zabezpečeno, že subjekt údajů má právo svůj souhlas kdykoli odvolat a v souvislosti s tím bude ze strany správce údajů adekvátně postupováno?	☒	☐	☐
15.	Je nastaven systém řízení GDPR v organizaci i pro případy zpracování osobních údajů dítěte?	☒	☐	☐
16.	Jsou přijata opatření, aby byly poskytnuty subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem veškeré informace o zpracování osobních údajů?	☒	☐	☐
17.	Jsou přijata opatření, pokud se osobní údaje týkající se SÚ údajů získávají od SÚ, že poskytne správce v okamžiku získání OÚ subjektu údajů stanovené informace podle článku 13 GDPR?	☒	☐	☐
18.	Jsou přijata systémová opatření, pokud se osobní údaje poskytované v případě, že osobní údaje nebyly získány od subjektu údajů, že bude postupováno podle článku 14. GDPR?	☐	☒	☐
19.	Jsou přijata systémová opatření, že Subjekt údajů získá od správce údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím podle článku 15 GDPR?	☒	☐	☐
20.	Jsou přijata systémová opatření, že správce bez zbytečného odkladu opraví nepřesné osobní údaje. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení dle článku 16 GDPR?	☒	☐	☐

21.	Jsou přijata systémová opatření, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají dle článku 17 GDPR?	☒	☐	☐
22.	Jsou přijata systémová opatření, aby správce omezil zpracování, v kterémkoli z případů definovaných v článku 18 GDPR?	☒	☐	☐
23.	Jsou přijata systémová opatření, že správce oznámí jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s článkem 16, čl. 17 odst. 1 a článkem 18, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí, že správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje? Článek 19	☒	☐	☐
24.	Jsou přijata systémová opatření, že správce Subjektu umožní získat osobní údaje, které se ho týkají, jež poskytl správci, a předat tyto údaje jinému správci v souladu	☒	☐	☐
25.	Je systémově zajištěno řešení pro naplnění souladu s článkem 21 GDPR, a to na právo vznést námitku?	☒	☐	☐
26.	Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká – čl. 22	☒	☐	☐
27.	Je systémově zajištěno, že správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků – čl. 24 GDPR?	☒	☐	☐
28.	S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.	☒	☐	☐
29.	Je systémově zajištěno, že správce zavádí jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů?	☒	☐	☐
30.	Jsou zavedeny technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné?	☒	☐	☐

31.	V případě společných správců jsou zpracována transparentní ujednání vymezující podíly na odpovědnosti za plnění povinností podle GDPR, zejména pokud jde o výkon práv subjektu údajů?	☐	☐	☒
32.	Jsou zavedeny systémové postupy pro zpracovávání záznamů o činnostech zpracování, za něž odpovídá, a to v rozsahu článku 30 GDPR?	☒	☐	☐
33.	Jsou stanovena a provedena vhodná technická a organizační opatření, aby byla zajištěna úroveň zabezpečení odpovídající daným rizikům s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob?	☒	☐	☐
34.	Jsou stanoveny mechanismy, že při jakémkoliv porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí toto dozorovému úřadu dle článku 33 GDPR?	☒	☐	☐
35.	Jsou stanoveny mechanismy, že je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů dle článku 34 GDPR.	☒	☐	☐
36.	Je systémově zajištěno, pokud je pravděpodobné, že určitý druh zpracování, bude mít za následek vysoké riziko pro práva a svobody fyzických osob, že provede správce před zpracováním posouzení vlivu zamýšlených operací dle článku 35 GDPR. (Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení)	☒	☐	☐
37.	Jsou správně zhodnocena kritéria pro jmenování pověřence pro ochranu osobních údajů? 37	☒	☐	☐
38.	Je stanovena osoba odpovědná za SM řízení osobních údajů a hlášení incidentů?	☒	☐	☐
39.	Jsou pověřenci pro ochranu osobních údajů zajištěny práva a pravomoci, aby byl náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů? 38.	☒	☐	☐
40.	Je pověřenec kompetentní a náležitě proškolen?	☒	☐	☐
41.	Je uvnitř organizace zaveden systém provádění kontrol a testování funkčnosti opatření GDPR?	☐	☒	☐
42.	Je stav systémových opatření, kontrolních mechanismů a dosažená úroveň odpovídající případnému vydaní osvědčení o souladu a dosažení odpovídající úrovně od nezávislého orgánu/organizace? Čl. 42	☒	☐	☐