VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

METODIKA ASISTOVANÉHO ZHODNOCENÍ
METHODOLOGY OF A SECURITY AUDIT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Hana Kroupová**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Hana Kroupová**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2018/19

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Metodika asistovaného zhodnocení

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrh řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je vytvořit jednotnou metodiku, která má za úkol pomoci při sestavování asistovaných zhodnocení jako prostředku zjištění stavu informační a kybernetické bezpečnosti ve společnostech.

Základní literární prameny:

ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky, Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů, Praha: Český normalizační institut, 2014.

DOUCEK Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7.

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

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Tato diplomová práce se zabývá asistovaným zhodnocením. Záměrem práce je vytvořit metodiku, která může pomoci při zpracování asistovaných zhodnocení a zjištění aktuálního reálného stavu kybernetické a informační bezpečnosti ve společnosti. Teoretická část se věnuje základním pojmům a terminologii, která se týká kybernetické a informační bezpečnosti. Vlastní návrh obsahuje popis jednotlivých oblastí metodiky asistovaného zhodnocení.

Klíčová slova

asistované zhodnocení, kybernetická bezpečnost, informační bezpečnost, systém řízení bezpečnosti informací, kybernetický bezpečnostní incident, kritická informační infrastruktura, významný informační systém

Abstract

The master‘s thesis is focused on security audit. The aim of this thesis is to create methodology, which might help with creating security audits and research current condition of cybernetic and information security in a business establishment. Theoretical part explains basic terms and concepts about cyber and information security. Own interpretation consist description of methodological areas of security audit.

Keywords

security audit, cyber security, information security, information security management system, cyber security incident, critical information infrastructure, important information system

Bibliografická citace

KROUPOVÁ, Hana. *Metodika asistovaného zhodnocení* [online]. Brno, 2019 [cit. 2019-05-06]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119719. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 10. května 2019

……

podpis studenta

Poděkování

Touto cestou bych ráda poděkovala mému vedoucímu bakalářské práce Ing. Petru Sedlákovi za veškeré cenné informace, rady, dohled a ochotu. Také bych chtěla poděkovat za trpělivost a pomoc mé oponentce Ing. Haně Sobotkové, DiS., rodině, partnerovi a přátelům.

OBSAH

ÚVOD

Málokdo z nás by si dokázal představit život bez moderních informačních a komunikačních technologií. Usnadňují nám každodenní život, výkon povolání nebo kontakt s přáteli, kteří bydlí na druhé straně zeměkoule. Mají i své temné stránky jako je například kybernetická kriminalita. Technologie jsou den ode dne vyspělejší a záleží jen na nás, jak moc je necháme zasáhnout do našeho soukromí.

Nacházíme se v době, kdy začínají domácnosti ovládat chytré věci, společnost využívá chytrých zařízení, které se dají nosit na těle, auta přemýšlejí za nás a lidská práce se nahrazuje automatizovanými stroji. Kybernetická a informační bezpečnost je čím dál častěji skloňovaným pojmem. Rychlost a zároveň i dostupnost přenášených informací a dat se za posledních 20 let výrazně navýšila a uživatelé se nezajímají, kam jsou jejich data přenášena natož, aby je zajímali, zda jsou bezpečně uchovávána. Všichni uživatelé, využívající moderní technologie, by měli mít na paměti, že rizika a hrozby se jich týkají také a měli by se proti nim aktivně bránit. Narušení bezpečnosti může být způsobeno lidskou chybou, přírodní katastrofou, technickým problémem nebo úmyslným útokem a systém bude vždy tak silný, jak je silný jeho nejslabší článek.

Neméně důležitá je také ochrana informací ve společnostech před únikem a zneužitím dat zákazníků nebo organizace samotné. Každý rok velmi výrazně roste počet útoků včetně nákladů na jejich nápravu. V roce 2018 vzrostl počet útoků pomocí ransomware o 43% a v číslech to bylo o 935 383 útoků více než v roce 2017. Z důvodu ochrany dat se začínají organizace zajímat o bezpečnost, ať už kvůli povinnosti nebo dobrovolně. Společnosti a veřejné instituce mají ale stále problém s kybernetickou bezpečností. Podle průzkumů je úspěšný každý třetí phishingový útok a každý pátý malware. Typickými chybami, které se vyskytují v nadnárodních, středních i malých společnostech jsou například slabá hesla, zranitelnosti ve webových aplikacích nebo nedostatečné filtrování síťového provozu. Pro odstranění těchto nedostatků se doporučuje zpracování firemních směrnic a seznámení zaměstnanců s principy a postupy řešení kybernetické bezpečnosti v organizaci.

Pro zlepšení kybernetické bezpečnosti ve společnostech vzniklo asistované zhodnocení, které vyhodnocuje reálný stav a tato diplomová práce se bude zabývat vytvořením metodiky asistovaného zhodnocení.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Ne vždy je jednoduché vyznat se v odborných pojmech a nařízeních, které by organizace měli nebo neměli splňovat a i proto bylo mým cílem vytvořit jednotnou metodiku pro zpracování asistovaných zhodnocení. Metodika může sloužit jako příručka nebo podpůrné vodítko pro tvorbu a vyhodnocování asistovaných zhodnocení.

Cílem této diplomové práce je vytvořit jednotnou metodiku, která má za úkol pomoci při sestavování asistovaných zhodnocení jako prostředku zjištění stavu informační a kybernetické bezpečnosti ve společnostech.

Protože je pojem asistovaného zhodnocení celkem neznámý a ve spoustě pojmů mají i odborníci nejasnosti, tak jsem v teoretických východiscích práce uvedla základní pojmy a legislativu, ze které asistované zhodnocení vychází a jsou nezbytné pro orientaci v problematice. Zabývám se také rozdílem mezi kybernetickou a informační bezpečností, protože to jsou další dva pojmy, které jsou problematické i pro odbornou společnost. Ve zkratce také představím normalizační instituce a také instituce, které se zabývají kybernetickou a informační bezpečností v České republice. Asistované zhodnocení je řešeno nejen zákonem a vyhláškou o kybernetické bezpečnosti, ale i normou ISO/IEC řady 27 000 a své nařízení má i část GDPR. Rozeberu i další pojmy, které se v asistovaném zhodnocení vyskytují jako analýza a řízení rizik, autentizační protokol IEEE 802.1X, audit kybernetické bezpečnosti a certifikace a log management.

Analytická část práce se zabývá základním členěním asistovaného zhodnocení, jak byla metodika tvořena a dokumenty nezbytnými k vytvoření metodiky. Popíšu strukturu jednotlivých tabulek, které využívám v celém návrhu vlastního řešení a jaké mohou být varianty hodnocení zavedení opatření. V poslední části využívám statistického výstupu analýzy aktuálního stavu zavedení opatření založenou na 34 vzorcích.

Pro návrh jsem použila Pomůcku k auditu bezpečnostních opatření podle zákona o kybernetické bezpečnosti. Organizační a technická opatření jsem rozdělila na jednotlivé oblasti. Každá z oblastí má krátký teoretický úvod na začátku každé podkapitoly. Následuje tabulka se všemi povinnostmi z jednotlivých oblastí, a který ze subjektů musí danou povinnost splňovat. U vybraných povinností jsem popsala, co by měly organizace splňovat, aby dosáhly na hodnocení „aplikováno“. GDPR je zpracováno velmi podobně.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V teoretických východiscích práce se budu zabývat základními pojmy, které se budou vyskytovat v celé diplomové práci. Zaměřím se především na základní termíny a pojmy z asistovaného zhodnocení včetně aktuální legislativy a nařízení GDPR, ze kterých asistované zhodnocení vychází. Dále popíšu normalizační instituce a instituce v České republice, které se zabývají problematikou kybernetické bezpečnosti. Popíši také analýzu rizik, audit a certifikaci a v neposlední řadě vysvětlím, co to vlastně asistované zhodnocení je a k čemu slouží.

1.1 Základní pojmy

Tato část bude obsahovat základní teoretické pojmy, které budu zmiňovat a často používat v celé své diplomové práci, a proto považuji za důležité se s nimi seznámit.

Dostupnost

Dostupností rozumíme „*zajištění přístupnosti k informaci oprávněnému uživateli v požadovaný okamžik*“ (1, s. 15).

Integrita

Integritou rozumíme „*zajištění správnosti a úplnosti informace*“ (1, s. 15).

Důvěrnost

Důvěrností rozumíme „*zajištění přístupnosti k informaci pouze oprávněnému uživateli*“ (1, s. 15).

Aktivum

Všechny zdroje (hmotné i nehmotné), které mají hodnotu pro organizaci a mají být chráněny (1).

Bezpečnostní událost

Bezpečnostní událost je „*identifikovaný stav systému, služby nebo sítě ukazující na možnost porušení bezpečnostní politiky nebo selhání bezpečnostních opatření*“ (1, s. 17).

Bezpečnostní incident

Bezpečnostní incident je „*pojem označující nějakou nestandardní či nepříjemnou bezpečnostní událost, která vede k narušení pravidel bezpečnosti v organizaci*“ (1, s. 17).

Hrozba

Hrozba je událostí, která má schopnost „*ohrozit bezpečnost nebo zneužít zranitelnost*“ (1, s. 15). Může způsobit nežádoucí incident, který by poškodil systém, organizaci nebo aktivum. Dělení podle působení na aktivum:

- operační systém,
- aplikace,
- databáze,
- síť,
- klient (2).

Zranitelnost

Slabé místo nebo nedostatek, které může aktivum mít. V tomto místě se může uplatnit hrozba (1).

Riziko

Riziko je „*kombinace hrozby a zranitelnosti s dopadem na aktivum*“ (1, s. 16).

1.2 Legislativa

Mezi legislativu, která se zabývá kybernetickou a informační bezpečností spadá zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, zákon č. 205/2017 Sb., novela zákona o kybernetické bezpečnosti, směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS) a nová vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti (3).

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

Návrh zákona o kybernetické bezpečnosti (ZKB) předložil Národní bezpečnostní úřad a tento zákon vstoupil do platnosti 1. ledna 2015. Kybernetický zákon upravuje *„práva a povinnosti osob, jakož i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti*“ (3). Hlavními cíli zákona je:

- bezpečnostní opatření,
- detekce kybernetických bezpečnostních incidentů,
- hlášení kybernetických bezpečnostních incidentů,
- systém opatření k reakci na kybernetické bezpečnostní incidenty,
- upravit činnost dohledových pracovišť (národní a vládní CERT) (3).

Dělení subjektů podle zákonu o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti určuje dělení subjektů podle významnosti. Rozděluje subjekty na 2 typy:

- **Kritická informační infrastruktura (KII)** – výrobní i nevýrobní systémy a služby. Nefunkčnost těchto systémů a služeb by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva a má nejpřísnější regulace (plnění celého ZKB),
- **Významný informační systém (VIS)** – je spravovaný orgánem veřejné moci, ale není součástí KII. Pokud by byla narušena informační bezpečnost, tak to může ohrozit nebo omezit výkon působnosti těchto orgánů (3, 4).

1.2.2 Směrnice NIS

Celým názvem se tato směrnice nazývá jako směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Tato směrnice má za úkol *„harmonizovat právní úpravu členských států v oblasti bezpečnosti sítí a informačních systémů a zavést jednotný standard úrovně kybernetické bezpečnosti s cílem zlepšení fungování vnitřního trhu.*“ (3) Některé povinnosti, které jsou ve směrnici NIS řešeny, jsou již zakotveny v ZKB. Směrnice NIS definuje 2 nové typy povinných subjektů:

- **Provozovatelé základních služeb (PZS)** – alternativa KII,
- **Poskytovatelé digitálních služeb (PDS)** (4).

Provozovatel základních služeb může být soukromý nebo veřejný subjekt z daného odvětví. Základní službou je chápána služba, která je závislá na elektronických komunikačních sítích nebo informačních systémech. Pokud by došlo k narušení služby, tak by mohlo dojít k významnému dopadu na zabezpečení společenských nebo ekonomických činností v těchto odvětvích:

- energetika,
- doprava,
- bankovnictví,
- infrastruktura finančních trhů,
- zdravotnictví,
- vodní hospodářství,
- digitální infrastruktura,
- chemický průmysl (4).

Digitální službou rozumíme službu, která poskytuje službu informační společnosti, která je upravena zákonem. Jsou to informační společnosti, které provozují:

- **on-line tržiště** – uzavírání on-line kupních smluv nebo smluv o poskytnutí služeb pomocí internetové stránky on-line tržiště nebo internetové stránky prodávajícího, který využívá služeb on-line tržiště,
- **internetového vyhledávače** – na základě dotazu uživatele (klíčové slovo, sousloví nebo jiné zadání) se provede vyhledávání na všech internetových stránkách a následně služba nabídne odkazy s požadovaným obsahem,
- **cloud computingu** – přístup k rozšiřitelnému a přizpůsobitelnému uložišti nebo výpočetním zdrojům (mohou být sdíleny) (4).

1.2.3 Vyhláška 82/2018 Sb., o kybernetické bezpečnosti

Aktuální vyhláška č. 82/2018 Sb. nahradila předchozí vyhlášku č. 316/2014 Sb. (VKB). Úprava vstoupila do platnosti 21. května 2018 a je stanovena Národním úřadem pro kybernetickou a informační bezpečnost. Tato vyhláška upravuje:

- obsah a strukturu bezpečnostní dokumentace,
- obsah a rozsah bezpečnostních opatření,
- typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
- náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
- náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
- vzor oznámení kontaktních údajů a jeho formu,
- způsob likvidace dat, provozních údajů, informací a jejich kopií (tento bod se přidal s aktualizací vyhlášky) (4).

Hlášení kybernetického bezpečnostního incidentů může být buď elektronickou formou, nebo v listinné podobě pomocí formuláře. V případě využití elektronické formy je možno využít formuláře zveřejněného na stránkách Úřadu, e-mailu na adresu elektronické pošty Úřadu, datové zprávy do datové schránky Úřadu nebo pomocí určeného datového rozhraní. Pokud není možné využít elektronickou formu, tak je vhodné použít listinné podoby na adresu Národního centra kybernetické bezpečnosti nebo Národního úřadu pro kybernetickou a informační bezpečnost (4).

Typy kybernetických bezpečnostních incidentů podle dopadu:

- narušení důvěrnosti aktiv,
- narušení integrity aktiv,
- narušení dostupnosti aktiv,
- kombinace dopadů (4).

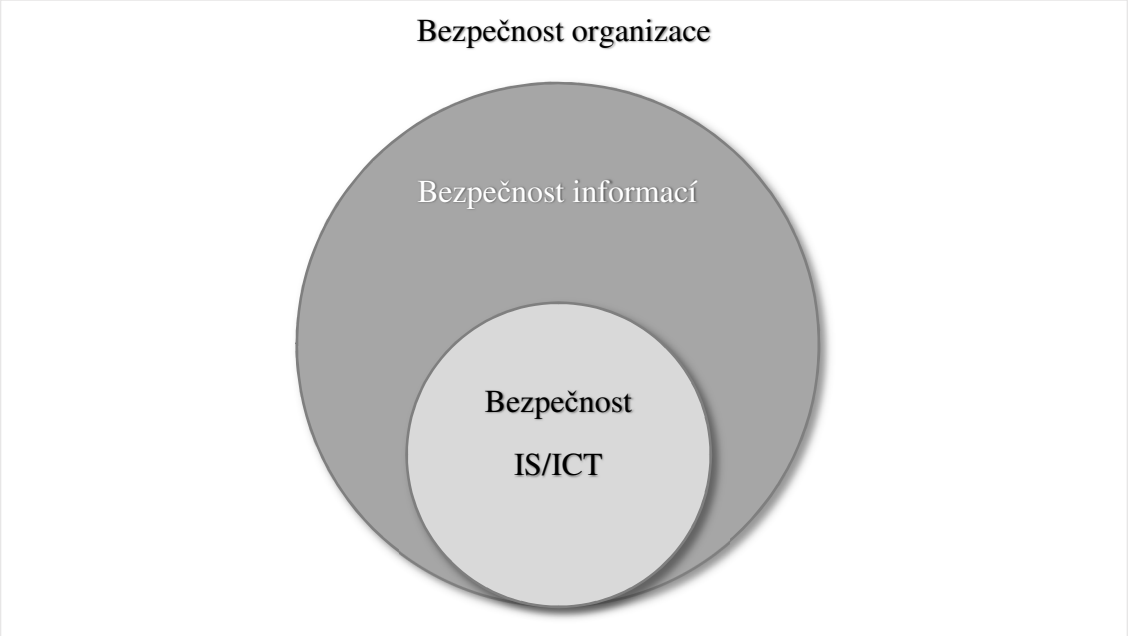
1.3 Kybernetická a informační bezpečnost

Kybernetická bezpečnost se zabývá celým kybernetickým prostorem. Kybernetický prostor je prostředí, ve kterém vznikají, zpracovávají se a vyměňují informace a je tvořený informačními systémy, službami a komunikačními sítěmi. Tento pojem zahrnuje také právní, organizační, technické a vzdělávací prostředky, které směřují k ochraně kybernetického prostoru. V názvosloví má spoustu lidí i odborníků nesrovnalosti a myslí si, že kybernetická a informační bezpečnost jsou totožné pojmy. To je poměrně rozšířený omyl. Kybernetická a informační bezpečnost se mohou překrývat,

ale liší se perimetrem. V České republice se o kybernetickou bezpečnost stará Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) (4).

Informační bezpečnost nebo také bezpečnost informací se zabývá celou organizací (fyzickou, personální, organizační i komunikační bezpečností). Vychází z normy ISO/IEC 27 002. Informační bezpečnost má zabezpečit ochranu aktiv před poškozením, krádeží, přírodní katastrofou apod. Informační bezpečnost má za úkol zajistit:

- dostupnost,
- integritu,
- důvěrnost (4).



Obr. 1: Vztahy bezpečnosti v organizaci

(Zdroj: vlastní zpracování dle: 1, s. 14)

1.4 Normalizační instituce

Normalizačních institucí je několik a dělí se na nadnárodní a celosvětové, evropské, národní a další. Okruh, pro který vydávají standardy a normy je standardizace bezpečnosti IT na různých úrovních.

1.4.1 Nadnárodní a světové

Světové organizace jako ISO, IEC a ITU mají na starost vydávání celosvětových tzv. základních norem a velmi úzce spolupracují (1).

International Organization for Standardization (ISO)

Podporuje a rozvíjí standardizační aktivity po celém světě. Cílem je především zjednodušit směnu zboží a služeb a spolupracovat na aktivitách, které se týkají intelektu, vědy, technologií a ekonomie (1).

International Electrotechnical Comission (IEC)

Další ze světových organizací. Cílem této organizace je příprava a vydávání mezinárodních norem z elektrotechnických, elektronických a dalších oborů (telekomunikace, elektřina, magnetismus, výroba a distribuce energií, terminologie, měření atd.) (1).

International Telecommunications Union (ITU)

Organizace ITU spadá do OSN. ITU má zásluhy na nových technologiích jako jsou mobilní technologie nebo Internet. Aktuálně se zaměřují na stavební prvky infrastruktury a na multimediální systémy, které spojují hlas, data, zvuk a video. Dále spravuje radiové frekvence (1).

1.4.2 Evropské

Mezi evropské normalizační instituce se řadí CEN, CENELEC a ETSI. CENELEC spolupracuje s organizacemi CEN a ETSI (1).

Comité Européen Normalisation (CEN)

V Evropě se o podporu harmonizace norem stará právě organizace CEN. Podporují bezpečnost a technické porozumění a umožňují funkčnost výrobků, systémů a služeb. Má několik CEN/ISSS technických komisí, které se zabývají IT bezpečností (1).

Comité Européen de Normalisation Eléctrotechnique (CENELEC)

Tato organizace vytvořila nový sektor, který se zabývá ICT a všechny aktivity související s normalizací informačních a komunikačních technologií sem přemístila (1).

European Telecommunications Standards Institute (ETSI)

Cílem organizace ETSI je vytváření telekomunikačních norem, které se týkají Evropy (1).

1.4.3 Národní

I jednotlivé státy mají své normalizační instituce, které se zabývají informačními technologiemi a vytváří vlastní národní normy. Většina těchto organizací je členem v ISO a/nebo IEC (1).

American National Standards Institute (ANSI)

Tento institut je v USA. Nevytváří své národní normy, ale zajišťuje vývoj pomocí konsensu s kvalifikovanými skupinami (1).

British Standard Institute (BSI)

BSI je britským institutem, který je tvořen odborníky s vysokou kvalifikací a zkušenostmi. Po vydání návrhu normy ji kdokoliv může okomentovat (lhůta 60 dní) a pro projednání těchto komentářů je norma publikována (1).

Český normalizační institut (ČSNI)

ČSNI spadá pod Ministerstvo průmyslu a obchodu a zastupuje naše zájmy v mezinárodních a evropských normalizačních institutech. Je členem v organizacích ISO, IEC, CEN, CENELEC a ETSI. Zabývá se především tvorbou, vydáváním, distribucí českých technických norem, poskytování informací o technických normách a již zmíněné zastupování v národních a evropských normalizačních institucích (1).

1.4.4 Další

Další jmenované instituce jsou IEEE a NIST, které se zaměřují a vydávají normy, které se specializují na technologie a IT bezpečnost.

Institute of Electrical and Electronics Engineers (IEEE)

Tato instituce se specializuje především na technické oblasti (počítačové inženýrství, biomedikální technologie, telekomunikace, spotřební elektronika atd.).

Normy, které tato organizace vydává, jsou ve většině případů mezinárodní. Jejich normy se zabývají také IT bezpečností a operačních systémů (IEEE 802.1x) (1).

National Institute for Standards and Technology (NIST)

Posláním této instituce je vývoj a podpora standardů, které se zabývají měřicími technikami a technologiemi. Cílem těchto standardů je zvýšit produktivitu, usnadnit obchod a zlepšit život (1).

1.5 Instituce v ČR

Následující instituce se zabývají kybernetickou a informační bezpečností v České republice.

1.5.1 Národní bezpečnostní úřad (NBÚ)

NBÚ byl zřízen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. Spadá mezi ústřední úřady i správní úřady a má výkonnou moc. NBÚ je správním úřadem pro oblast ochrany utajovaných informací a bezpečnostní způsobilosti. Hlavními úkoly NBÚ je vydávání osvědčení fyzickým osobám i podnikatelům a dokladů o bezpečnostní způsobilosti fyzickým osobám (5).

Národní CSIRT (Computer Security Incident Response Team) je vykonáván veřejnoprávní smlouvou s NBÚ a stal se pověřencem v problematice kybernetické bezpečnosti. CSIRT plní úlohu národního CERT. Od roku 2011 je provozován sdružením CZ.NIC. Funkce CSIRT:

- detekce průniku,
- distribuce poradenství,
- SAE (budování bezpečnostního povědomí),
- sdílení informací (4, 6).

1.5.2 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

NÚKIB je „*ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a telekomunikačních systémů a kryptografické ochrany*“ (7). Tento úřad vznikl v roce 2017 a to na základě zákona č. 205/2017 Sb. Je správním úřadem pro oblasti:

- kybernetická bezpečnost,
- ochrana utajovaných informací (informační a komunikační systémy),
- kryptografická ochrana,
- problematika ohledně navigačního systému Galileo (7).

1.5.3 Národní centrum kybernetické bezpečnosti (NCKB)

NCKB je sekcí, která spadá pod Národní úřad kybernetické a informační bezpečnosti. Toto centrum zajišťuje hlavně:

- činnost Vládního CERT České republiky,
- prevenci před kybernetickými hrozbami proti KII, VIS, PZS atd.,
- osvětová a vzdělávací činnost,
- spolupráce s národními a mezinárodními organizacemi,
- výzkum a vývoj v oblasti kybernetické bezpečnosti,
- vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímaní příslušných nápravných a preventivních opatření atd. (3).

1.6 ISO/IEC 27 000

Tato řada norem se zabývá bezpečností informací. Všechny normy, které spadají do této řady, mají stejnou strukturu a pravidla. Řada 27 000 obsahuje více než tři desítky norem, z nichž základními normami jsou především normy:

- ISO 27 000 – definice pojmů a slovník s terminologií,
- ISO 27 001 – norma, která se týká ISMS,
- ISO 27 002 – souhrn nejlepších praktik pro bezpečnost informací,
- ISO 27 003 – příručka pro návrh a zavedení ISMS,
- ISO 27 004 – měření,
- ISO 27 005 – řízení rizik bezpečnosti informací,
- ISO 27 006 – požadavky na orgány provádějící audit a certifikaci ISMS,
- ISO 27 007 – doporučení k provádění auditů (8).

Specifické řady norem využívají také různé subjekty, které spadají do kritické informační infrastruktury (KII) nebo významných informačních systémů (VIS). Tyto normy patří mezi specifické normy:

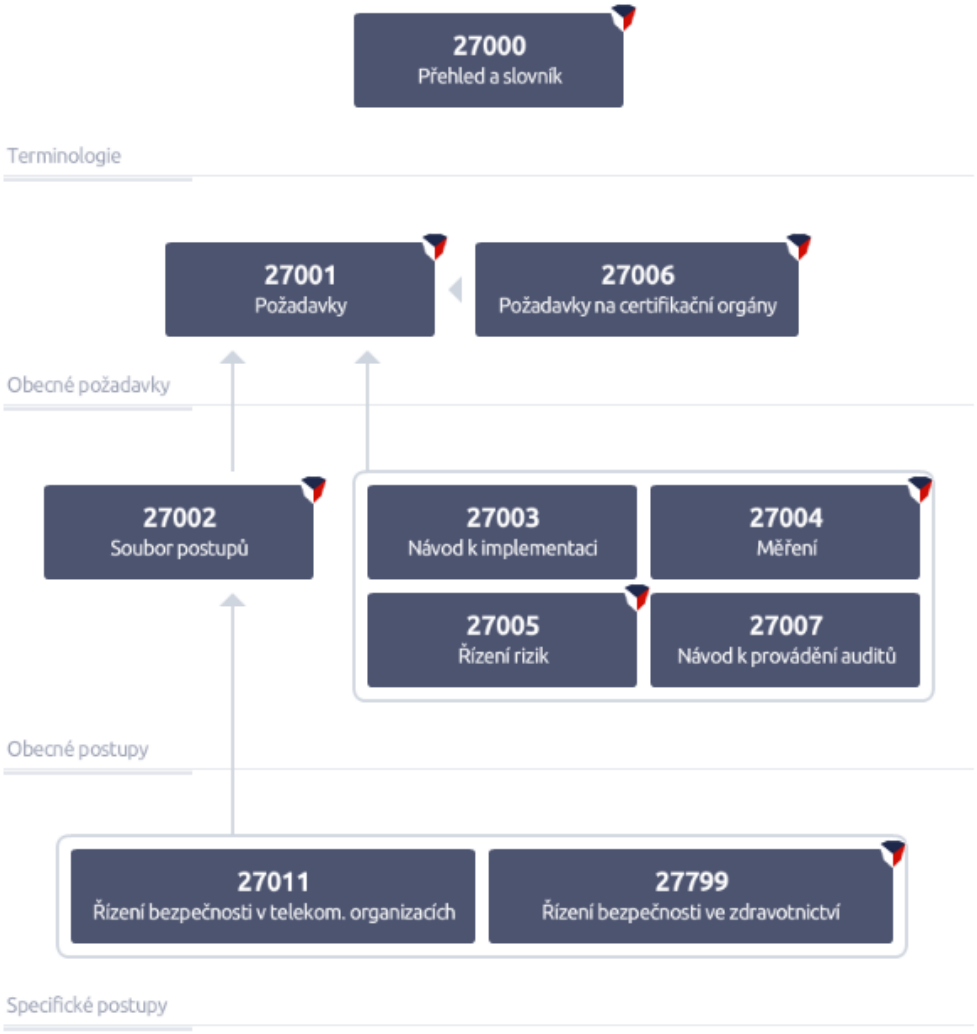
- ISO 27 010 – doporučení pro sdílení informací mezi subjekty KII,
- ISO 27 011 – telekomunikační operátoři,
- ISO 27 017 – cloud computing,
- ISO 27 018 – poskytovatelé cloudových služeb,
- ISO 27 019 – energetika,
- ISO 27 099 – zdravotnictví (8).

Další normy z řady ISO 27 000 se týkají některých oblastí, které jsou obsaženy i v asistovaném zhodnocení. Další normy jsou:

- ISO 27 031 – kontinuita činnosti organizace,
- ISO 27 032 – zabezpečení kyberprostoru,
- ISO 27 033 – bezpečnost sítí,
- ISO 27 034 – aplikační software,
- ISO 27 035 – řízení bezpečnostních incidentů,
- ISO 27 036 – řízení dodavatelů
- ISO 27 039 – systémy IDS a IPS (8).

Více než desítka norem je připravována a jedná se hlavně o neustále se rozvíjející prostředí a nové technologie, které se musí ošetřit bezpečnostními opatřeními. Jsou to například tyto připravované normy:

- ISO 27 030 – zabezpečení Internet of Things (IoT),
- ISO 27 045 – bezpečnost v systémech big data,
- ISO 27 100 – přehled kybernetické bezpečnosti,
- ISO 27 551 – autentizace anonymních entit,
- ISO 27 555 – mazání osobních dat (8).



Obr. 2: Zjednodušené schéma bezpečnostních norem

(Zdroj: 9)

1.7 General Data Protection Regulation (GDPR)

V češtině se tento pojem dá přeložit jako Obecné nařízení o ochraně údajů. Vstoupilo v platnost dne 25. května 2018. GDPR se týká všech subjektů a organizací, které sbírají, uchovávají a zpracovávají osobní údaje osob z členských zemí EU. Osobním údajem může být nějaký informace o člověku (např. jméno, příjmení, datum narození, adresa, atd.). Některé společnosti budou muset zavést povinnou osobu DPO. Zavedení GDPR není jednorázovou akcí a je dobré i v tomto případě používat PDCA cyklus pro neustálé monitorování a zlepšování (4).

Aby organizace splňovala soulad s GDPR měli by správci a zpracovatelé zavést technické, organizační a procesní opatření, které se týkají především oblastí:

- implementace ochrany dat,
- vypracování posouzení vlivu na ochranu osobních údajů (DPIA),
- zavedení pozice pověřence pro ochranu osobních údajů (DPO),
- zavedení pseudonymizace osobních údajů,
- záznamy o činnostech zpracování,
- konzultace s dozorovým orgánem (9).

1.7.1 Pseudonymizace

Pseudonymizací je myšleno *„zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu člověku bez použití dodatečných informací, které jsou uchovávány odděleně a chráněny proti opětovnému přiřazení k původním údajům“* (9).

1.7.2 Data Protection Officer (DPO)

Český překlad pro tuto pozici je pověřenec pro ochranu osobních údajů. Postavení této pozice ve firmě je nezávislé. Někteří správci a zpracovatelé osobních údajů mají povinnost mít zřízenou takovou pozici. Jiní mají možnost dobrovolně zavést tuto pozici. DPO nesmí zpracovávat osobní údaje. DPO poskytuje poradenství, pro všechny zaměstnance, kteří ve firmě zpracovávají osobní údaje (příp. vedení), je prostředníkem mezi organizací, dozorovým orgánem a veřejností, monitoruje soulad s nařízením GDPR a posuzuje vliv na ochranu osobních údajů. Povinnost zřízení pozice DPO je v následujících situacích:

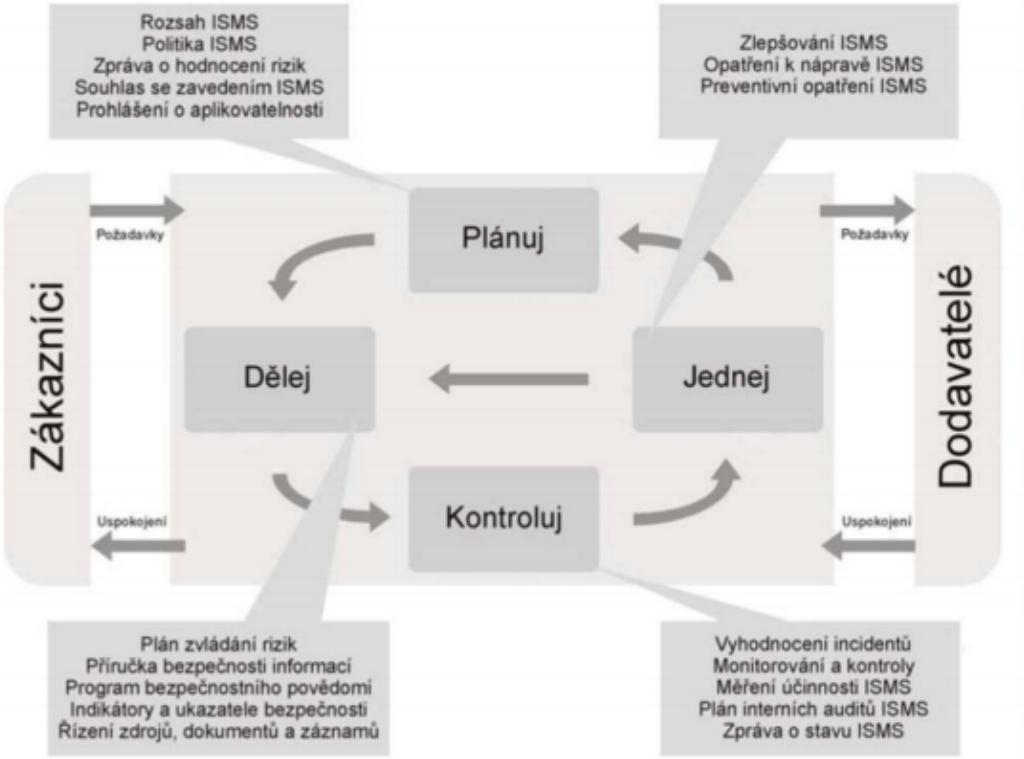
- zpracování osobních údajů u orgánů veřejné moci nebo veřejný subjekt (kromě soudů),
- správce nebo zpracovatel osobních údajů provádí zpracování, které vyžaduje pravidelné a systematické monitorování osob,
- správce nebo zpracovatel osobních údajů zpracovává osobní údaje, které spadají do zvláštních kategorií údajů (genetické, biometrické údaje, rozsudky v trestných věcech nebo trestní činy) (10).

1.7.3 Data Protection Impact Assessment (DPIA)

Jedno z opatření posuzující vliv na ochranu osobních údajů. Toto opatření je definované v článku 35 GDPR. V případě, že se v organizaci rozhodnou zpracovávat osobní údaje, tak by měla organizace také posoudit, jak mohou zpracováním zasáhnout do práv a svobod lidí (ovlivnit jejich životy). Metodika pro zpracování DPIA je vytvořena pracovní skupinou WP29. DPIA není analýza rizik (4).

1.8 Systém řízení bezpečnosti informací (ISMS)

Norma definuje ISMS jako *„součást řízení organizace, založená na přístupu k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací“* (1, s. 66). Je to tedy systematický a řízený proces, který má na starosti trvale zlepšovat bezpečnost informací v souladu s normou ISO/IEC 27 000. Cílem systému řízení bezpečnosti informací je zajistit triádu CIA - dostupnost, integritu a důvěrnost. Kromě zajištění kompatibility s jinými organizacemi, ochraně informací partnerů a zákazníků nebo možnost získat mezinárodní certifikát je hlavním přínosem splnění požadavků Kybernetického zákona. ISMS využívá Demingova modelu (PDCA cyklus) (1).



Obr. 3: PDCA model aplikovaný na ISMS

(Zdroj: 11, s. 7)

Metoda PDCA cyklu může být použita u kvality výrobků, služeb, procesů atd. V případě aplikace na ISMS má PDCA cyklus tyto čtyři etapy:

- **Plan** – ustanovení ISMS,
- **Do** – zavádění a provoz ISMS,
- **Check** – monitorování a přezkoumání ISMS,
- **Act** – údržba a zlepšování ISMS (1).

Je to tedy nikdy nekončící proces, který se musí neustále opakovat, aby mělo ISMS smysl a neustále se zlepšovalo. PDCA model může být aplikován na všechny procesy, které se týkají ISMS (1).

1.8.1 Prohlášení o aplikovatelnosti (SoA)

Prohlášení o aplikovatelnosti (Statement of Applicability) je dokument, který společnost vytváří po analýze rizik a je ve třetí etapě zavádění ISMS. V případě, že společnost usiluje o certifikaci ISMS je také dokumentem nutným. Jeho obsahem jsou

informace a definice opatření, která byla nebo nebyla implementována a proč. Prohlášení aplikovatelnosti je definováno normou ISO/IEC 27 001 – 4.2.1 j (4).

1.9 Analýza rizik

Analýza rizik má za úkol identifikovat zranitelná místa, definovat působící hrozby, stanovit rizika ke zranitelnému místu a hrozbě, snížení rizik pomocí adekvátních opatření, identifikace a popis existujících a plánovaných opatření a odhad rizik. Využívá se informací pro odhad míry rizika a určení jeho zdrojů. Její rozdělení je na 4 přístupy:

- **hrubá úroveň** – určení kritických systémů,
- **neformální přístup** – pragmatická analýza rizik,
- **kombinovaný přístup** – nejprve hrubá úroveň a poté detailní,
- **podrobný přístup** – detailní analýza rizik (2).

Fáze analýzy rizik jsou 3:

1. **fáze analýzy rizik** – ocenění datových aktiv, software, hardware,
2. **fáze analýzy rizik** – ohodnocení hrozeb a zranitelností, výpočet míry rizika probíhá společně s oceněním aktiv,
3. **fáze analýzy rizika** – určení vhodných a adekvátních opatření na základě výpočtu míry rizika a rozdělení opatření na IT bezpečnost, komunikační bezpečnost, personální bezpečnost, administrativní bezpečnost a fyzickou bezpečnost (2).

1.9.1 Aktiva

Základní definici pro aktivum jsem již uvedla v kapitole Základní pojmy. Aktiva se mohou dělit na různé skupiny, které reprezentují rozsah ISMS:

- informační aktiva,
- hardwarová aktiva,
- softwarová aktiva,
- služby poskytované prostřednictvím informačních systémů (2).

Pro stanovení hodnoty aktiva se nejčastěji využívá součtový algoritmus, protože je nejjednodušší. V případě aktiva je vhodné použít následující vzorec, kdy škála hodnot nabývá hodnot od 1 do 5:

$$\frac{dostupnost + důvěrnost + integrita}{3}$$

Po tomto výpočtu pak můžeme aktivum zařadit do následující stupnice:

Tab. 1: Stupnice pro aktiva a hodnotící kritéria

(Zdroj: 2)

1	Bezvýznamné riziko	Žádný dopad
2	Akceptovatelné riziko	Zanedbatelné ztráty
3	Nízké riziko	Potíže a finanční ztráty
4	Nežádoucí riziko	Vážné potíže a velké ztráty
5	Nepřijatelné riziko	Existenční potíže

1.9.2 Výpočet míry rizika

Výpočet může být proveden pomocí dvou metod. První z nich obsahuje dva parametry a druhá obsahuje parametry tři. První metoda pomocí dvou parametrů má následující vzorec:

$$R = PI \times D$$

R je míra rizika, PI je pravděpodobnost incidentu a D je dopad. Pravděpodobnost vzniku a existence rizika má 5 hodnot. Tyto hodnoty jsou uvedeny v tabulce č. 2 (2).

Tab. 2: Hodnoty pravděpodobnosti rizika

(Zdroj: 2)

1	Nahodilá
2	Nepravděpodobná
3	Pravděpodobná
4	Velmi pravděpodobná
5	Trvalá

Druhá metodou, která počítá míru rizika pomocí tří parametrů má následující vzorec:

$$R = T \times A \times V$$

R je míra rizika, T je pravděpodobnost hrozby, A je hodnota aktiva a V je zranitelnost. Po tomto výpočtu míry rizika je potřeba stanovit hranice stupňů rizika a riziku přidělit skupinu, kam patří podle tabulky č. 3 (2).

Tab. 3: Hranice různých stupňů rizika

(Zdroj: 2)

0 – 10	Bezvýznamné riziko
11 – 20	Akceptovatelné riziko
21 – 30	Mírné riziko
31 – 60	Nežádoucí riziko
61 – 120	Nepřijatelné riziko

1.9.3 Řízení kybernetických rizik

Řízení rizik je procesem, který slouží k identifikaci a kvantifikaci rizik. Norma, která se věnuje této problematice, je ISO/IEC 27 005. Po identifikaci a ohodnocení je třeba rozhodnout i o opatřeních a zvládání rizik. Je to komplexní proces a skládá se z několika na sebe navazujících částí, kterými jsou:

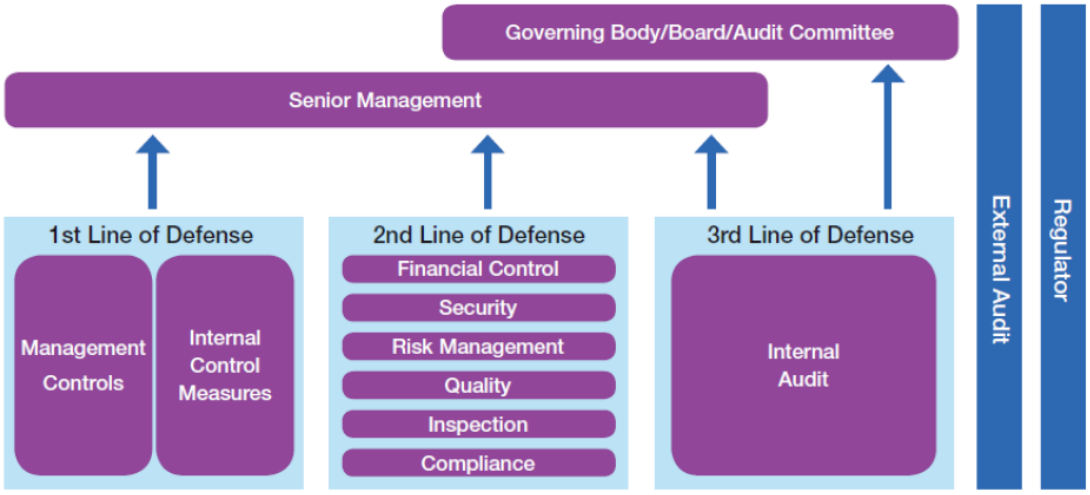
- stanovení kontextu,
- analýza rizik,
- vyhodnocení rizika,
- zvládání rizik (2).

Obr. 4: Cyklus řízení rizik

(Zdroj: Vlastní zpracování dle: 1)

Řízení kybernetických rizik není řešeno IT oddělením, ale je potřeba zřídit pozici Chief Information Security Officer (CISO) – manažer informační bezpečnosti a Data Protection Officer (DPO) – pověřenec pro ochranu osobních údajů. Při řízení kybernetický rizik je potřeba definovat strategii a určit míru rizika, které je přijatelné. Včasná identifikace a detekce rizika poskytuje organizaci značnou výhodu při přípravě a implementaci protiopatření. Používá se tří stupňový model řízení rizik:

- **1. stupeň ochrany** – bezpečnostní politiky a standardy (denní ISMS) – management,
- **2. stupeň ochrany** – CISO kompetence – risk management,
- **3. stupeň ochrany** – kontrola prvních dvou stupňů – interní audit (4).



Obr. 5: Institute of Internal Auditor's koncept řízení kybernetických rizik

(Zdroj: 4)

1.9.4 Opatření

Bezpečnostní opatření nám slouží k minimalizaci rizik. Bezpečnostní opatření je *„proces, procedura, technický prostředek atd.“* (2). Opatření se vytváří po identifikaci a ohodnocení rizik. Existují také katalogy ochranných opatření, které definují nejčastější obecná opatření pro ochranu IT systému.

Druhy opatření jsou následující:

- preventivní,
- detekce a reakce,
- podpůrná (1).

1.9.5 Plán zvládání rizik (RTP)

V plánu zvládání rizik jsou zaznamenány informace o realizaci navržených opatření, jednotlivým opatřením jsou přiřazeny priority a je sestaveno pořadí, termíny a odpovědnosti. Při sestavování plánu je vhodné posoudit cenu opatření (cena by neměla přesahovat případné ztráty) a vybrat opatření, která mají širokou působnost. Pokud rizika spadají do skupiny bezvýznamná nebo akceptovatelná je dobré se zamyslet, jestli by nebylo lepší je akceptovat než pro ně vymýšlet opatření a investovat náklady (12).

1.9.6 Bring Your Own Device (BYOD)

Tento pojem je aktuálně velkým trendem a tématem při řešení bezpečnosti. Jedná se o mobilní zařízení uživatelů, což naznačuje i překlad „Přines si své zařízení“. Je potřeba provést analýzu jaká data mají uživatelé ve svých zařízeních a tím provést i analýzu rizik. Poté je potřeba zavést pravidla, jak mohou uživatelé zacházet s firemními daty (bezpečné zacházení i technická opatření). Do mobilních zařízení je dobré zavést systémy centrální správy (MDM – Mobile Device Management) nebo systémy proti úniku dat (DLP – Data Loss Prevention). Ideální je v případě mobilních zařízení využít vícestupňového zabezpečení (např. MDM + kontejnerizace) (12).

1.10 IEEE 802.1X

Tento pojem je protokolem v autentizaci v počítačových sítích. Principem tohoto protokolu je povolení pouze výměny autentizačních informací a zbytek komunikace je blokován. Řízení přístupu má tři části:

- **supplicant** – klientská aplikace, která se snaží připojit do sítě,
- **autentizátor** – aplikace ověřující klienta (síťová strana),
- **autentizační server** – poskytuje autentizační údaje autentizátoru (2).

Suplikant (program na klientově stanici) zajišťuje výměnu uživatelského jména a hesla. V případě úspěšné autentizace dojde k odblokování stanice a může probíhat komunikace. Protokol IEEE 802.1X ověřuje identitu uživatele a ne jeho hardware (2).

1.11 Audit kybernetické bezpečnosti

Audit je definován jako *„systematický, nezávislý a dokumentovaný proces získávání důkazů a jejich hodnocení pro stanovení rozsahu splnění požadovaných kritérií“* (1, s. 130). Toto hodnocení určuje, zda byla kritéria splněna či nikoliv. Audit je prováděn alespoň 1x ročně (dozorový audit). Audit může být interní (organizace provádí sama) nebo externí (organizace se vztahem k auditované společnosti nebo nezávislá organizace). Audit prováděný třetí stranou (externí nezávislou organizací) slouží jako podklad pro certifikaci. Audit má následující fáze:

- zahájení auditu,
- přezkoumání dokumentace,
- provádění auditu na místě,
- vyhotovení zprávy o auditu,
- dokončení auditu (1).

1.12 Certifikace

Pojem certifikace znamená *„potvrzení shody systému řízení dle požadavků norem“* (1, s. 130). Recertifikace probíhá po 3 letech. Certifikace má následující průběh:

- volba certifikačního orgánu a navázání obchodního vztahu,
- certifikační audit – posouzení dokumentace,
- certifikační audit – nalezení shody s požadavky normy,
- doporučení o udělení certifikátu,
- udělení certifikátu certifikační radou (1).

1.13 Log management

Log managementem se zabývá směrnice NIST SP 800-92:2006 – Guide to Computer Security Log Management. Log je záznam. Obsahuje hardware, software, síť a média, které generují, vysílají, ukládají, analyzují a nakládají s log daty. Infrastruktura má 3 stupně:

- **Generování logů** – zdroj generuje logy a posílá je log serveru,
- **Analýza a ukládání logů** – log server přijímá logy, data jsou přenášena v reálném čase, pokud server přijímá logy z více zdrojů, tak se nazývá sběrač nebo agregátor, data jsou ukládána na stejném nebo separátním úložišti,
- **Sledování logů** – konzole pro monitorování a zobrazení výsledků automatizované analýzy (4).

Důležitou podmínkou při sběru logů je synchronizace času (PTP server). Syslog je protokol, který se využívá pro specifikaci vstupního logu a transportní mechanismus (4).

1.13.1 SIEM

SIEM je *„centralizovaný systém, který sbírá, monitoruje, ukládá a spravuje bezpečnostní události“* (4). Tyto bezpečnostní události jsou reprezentovány logovacími záznamy (logy). Cílem je vyšší efektivnost práce bezpečnostních analytiků, auditorů a manažerů. Je dobré pro SIEM vytvořit provozní příručku, která má návaznost na řízení kontinuity činnosti (BCM - Business Continuity Management) Logy se mohou sbírat dvěma způsoby:

- **Bez agenta** – log data z individuálních zařízení bez speciálního software,
- **S agentem** – softwarový agent je nainstalovaný na zařízení, které je určené ke sběru log dat (4).

SIEM server umí analyzovat data z různých zdrojů a používá prioritizaci (třídy zpráv, zdroj zpráv, IP adresa, četnost zápisů) a umí poskytovat log data v různých formátech (GUI, bezpečnostní znalostní báze, sledování postupu při incidentu). Server SIEM komunikuje s agentem pomocí TCP protokolu kryptovaně (4).

1.13.2 IDS/IPS

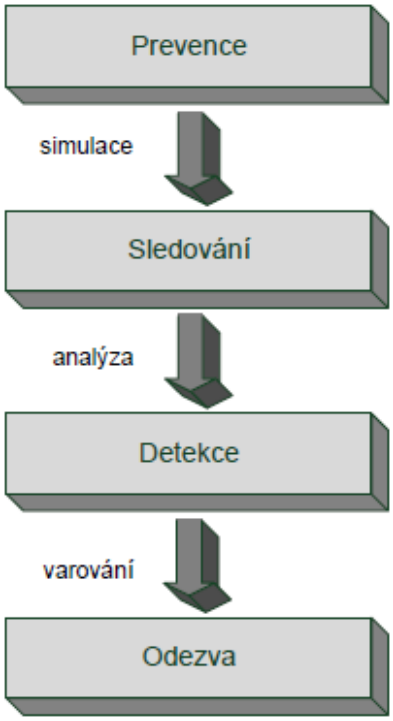
Intrusion Detection and Prevention Systems *„jsou systémy proti detekci a prevenci průniku bezpečnostních incidentů“* (2). Mají na starosti monitoring sítě a operačního systému před škodlivou činností (2).

IDS mají za úkol monitorovat provoz sítě s cílem odhalit podezřelé aktivity. Pokud je odhalena neobvyklá aktivita, tak systém vygeneruje varování (alert), provede

zápis do logu, upozorní administrátora a případně zablokuje neobvyklou činnost. V případě, že je systém pasivní, tak nijak nezasahuje do funkčnosti sítě a pouze vygeneruje varování a provede zápis do logu. IDS hlídá útoky zevnitř sítě. Rozdělit systémy IDS lze na dva druhy:

- uzlově orientované systémy detekce odhalení průniku,
- síťově orientované systémy detekce odhalení průniku (2).

Signatura je vzorec, který vyhledává anomálie v síťové infrastruktuře nebo serveru. Vektor útoku je cestou, kterou útočník využívá (nejčastější vektor útoku je využití zranitelnosti prohlížeče). Senzor je hlavním prvkem IDS, který detekuje škodlivý či nebezpečný kód a odhaluje nebezpečí (2).



Obr. 6: Aktivity IDS

(Zdroj: 2)

IPS zajišťují detekci a prevenci průniku. Jsou to zařízení monitorující síť a aktivity operačního systému z pohledu škodlivé činnosti. Hlavní rozdíl od IDS je, že systém IPS je zařazen přímo do síťové cesty (in-line) a může tak aktivně předcházet a blokovat nežádoucí a nebezpečný provoz sítě. Hlavní funkce:

- identifikace škodlivé činnosti,
- záznam o jejím průběhu,
- blokování škodlivé činnosti,
- nahlášení škodlivé činnosti (2).

1.14 Asistované zhodnocení

Asistované zhodnocení je málo známý pojem, ale neméně důležitý pro vytvoření jednotného rámce pro zhodnocení stavu bezpečnostních opatření a provádění auditu bezpečnostních opatření. Je to model vytvořený na principu dotazníku, který má za úkol zjištění reálného stavu informační a kybernetické bezpečnosti, bezpečnostních opatření a GDPR ve společnosti. Asistované zhodnocení zahrnuje tyto právní předpisy:

- **Zákon č. 181/2014 Sb.**, o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB),
- **Vyhláška č. 82/2018 Sb.**, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (VKB),
- **Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018**, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148 (4, 13).

Jak jsem již zmínila v předchozím odstavci, tak tento model vyhodnocuje řízení kybernetické a informační bezpečnosti v organizaci, bezpečnostní opatření podle zákonu o kybernetické bezpečnosti a vyhlášce o kybernetické bezpečnosti a v neposlední řadě také plnění GDPR. Asistované zhodnocení respektuje členění vycházející z kybernetického zákona a vyhlášky. Autorem jsou NCKB a poté NÚKIB. Asistované zhodnocení je rozčleněno na technická a organizační opatření a přidáno je k němu i rozšíření GDPR. Po převedení stavu zavedení opatření na grafický výstup je výstupem manažerské zhodnocení reálného stavu (4).

Cílem asistovaného zhodnocení je vytvořit tzv. „Auditní checklist“, který má za úkol poskytnout souhrnný rámec povinností, které musí splňovat jednotlivé typy subjektů, které jsou definovány zákonem č. 181/2014 Sb. a směrnicí NIS. Plnění

povinností musí být v souladu se zákonem o kybernetické bezpečnosti. Jedná se o tyto typy subjektů:

- správce a provozovatele kritické informační infrastruktury (KII),
- správce a provozovatele významného informačního systému (VIS),
- správce a provozovatele informačního systému základní služby,
- poskytovatele digitální služby (4, 13).

2 ANALÝZA PROBLÉMU A SOUČASNÉ SITUACE

V této části se budu zabývat, jak byla metodika tvořena a podobou tabulek asistovaného zhodnocení a k tomu přílohy GDPR, variantami hodnocení zavedení opatření a jako poslední v analýze porovnám zavedení podle subjektů KII, VIS a GDPR.

Asistované zhodnocení zahrnuje 26 oblastí, které dohromady obsahují 315 otázek. Asistované zhodnocení je první fází před zavedením systému řízení bezpečnosti informací. Kompletní asistované zhodnocení se nachází v **příloze č. 1 a č. 2**. Oblasti, které obsahuje asistované zhodnocení, se dělí na organizační a technická opatření. Toto členění je striktní a je dané systémem řízení bezpečnosti informací (ISMS) a VKB. Členění má následující podobu:

Organizační opatření

- Systém řízení bezpečnosti informací (ISMS),
- Řízení rizik,
- Bezpečnostní politika,
- Organizační bezpečnost,
- Stanovení bezpečnostních požadavků pro dodavatele,
- Řízení aktiv,
- Bezpečnost lidských zdrojů,
- Řízení provozu a komunikací,
- Řízení přístupu a bezpečné chování uživatelů,
- Akvizice, vývoj a údržba,
- Zvládání bezpečnostních událostí a incidentů (incident handling),
- Řízení kontinuity činnosti (BCM),
- Kontrola a audit kybernetické bezpečnosti,

Technická opatření

- Fyzická bezpečnost,
- Bezpečnost komunikačních sítí,
- Správa a ověřování identit,
- Řízení přístupových oprávnění,

- Ochrana před škodlivým kódem,
- Ochrana integrity komunikačních sítí,
- Zaznamenávání událostí informačního a komunikačního systému (uživatelů a administrátorů),
- Detekce kybernetických bezpečnostních událostí,
- SIEM,
- Aplikační bezpečnost,
- Kryptografie,
- Průmyslové, řídící a obdobné specifické systémy,

Rozšíření o problematiku GDPR

- Ochrana osobních údajů (GDPR),
    - Osobní údaje,
    - Kodexy chování,
    - Závazná podniková pravidla,
    - Záznamy o činnostech zpracování,
    - Posouzení vlivu dopadu na ochranu osobních údajů,
    - Právo na přenositelnost údajů. (4)

2.1 Tvorba metodiky

Aktuálně neexistuje žádný jednotný postup nebo rámec pro řešení asistovaného zhodnocení a každý si ho, pokud vůbec, řeší po svém. Z toho důvodu zpracovávám tuto diplomovou práci, která by v budoucnu mohla pomoci při vytvoření jednotného návrhu řešení. Pro vlastní návrh řešení byl použit dokument, který byl sestaven v Národním centru kybernetické bezpečnosti a nazývá se Pomůcka k auditu bezpečnostních opatření podle zákona o kybernetické bezpečnosti.

Podle dokumentu jsou rozděleny a seřazeny jednotlivé oblasti asistovaného zhodnocení a u každé z otázek je uvedeno, pro který ze subjektů je povinnost určena, a která část zákona řeší jednotlivé povinnosti. Jednotlivé oblasti jsou stručně okomentovány (např. čeho se daná oblast týká, co je v ní řešeno, co oblast obsahuje atd.). Následuje tabulka, která má definovanou strukturu podle toho, jestli se týká organizačních nebo technických opatření (struktura podle tabulky č. 1) nebo se týká

GDPR (struktura podle tabulky č. 2). Pod tabulkou se nachází komentáře k jednotlivým povinnostem.

2.2 Struktura tabulek č. 7-31

Všechny tabulky, které jsou obsaženy v návrhové části a týkají se organizačních a technických opatření, jsou rozděleny podle oblastí, které jsou danou tabulkou řešeny. Tabulky obsahují 5 sloupců:

- kritická informační infrastruktura,
- významný informační systém,
- povinnost,
- zákon / norma,
- hodnocení.

První dva sloupce určují, který ze subjektů podle zákonu o kybernetické bezpečnosti musí danou povinnost splňovat. Povinnost obsahuje popis povinnosti. Sloupec označený jako zákon / norma určuje, kterým předpisem je povinnost upravována. Hodnocení není uvedeno v návrhu řešení, ale až v příloze, která obsahuje kompletní podobu asistovaného zhodnocení.

Tab. 4: Vzorová tabulka pro asistované zhodnocení
(Zdroj: vlastní zpracování)

KII	VIS	Povinnost	Zákon / norma	Hodnocení

2.3 Struktura tabulek č. 32-37

Tabulky řešící GDPR mají jinou strukturu než zbytek tabulek, protože GDPR by měla splňovat každá organizace, která zpracovává osobní údaje osob z EU. Rozdělení na subjekty podle zákona o kybernetické bezpečnosti by zde nemělo význam. Tabulky týkající se GDPR mají 3 sloupce:

- povinnost,
- zákon / norma,
- hodnocení.

V prvním sloupci povinnost je opět popsán popis dané povinnosti. Druhý sloupec obsahuje zákon nebo normu, které povinnost upravují. Hodnocení není uvedeno v návrhu řešení, ale až v příloze, která obsahuje kompletní podobu asistovaného zhodnocení.

Tab. 5: Vzorová tabulka pro GDPR

(Zdroj: vlastní zpracování)

Povinnost	**Zákon / norma**	**Hodnocení**

2.4 Varianty hodnocení zavedení opatření

V tabulce č. 3 jsou uvedené varianty, které jsou při vytváření asistovaného zhodnocení použity.

Tab. 6: Varianty stavu zavedení opatření

(Zdroj: 4)

Aplikováno
Částečně aplikováno
Neaplikováno
Neaplikovatelné
Nerelevantní

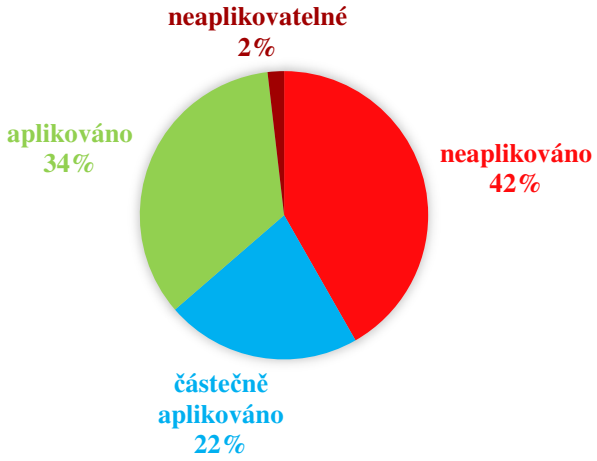
2.5 Statistická analýza

Každá ze společností spadá do jiného subjektu a musí splňovat a implementovat jiné povinnosti, proto je porovnání provedeno pomocí procentuálních hodnot pro snazší porovnání. Tyto společnosti zpracovaly asistované zhodnocení a zhodnotili tak aktuální reálný stav bezpečnosti ve společnosti.

2.5.1 Souhrnné hodnocení na všech vzorcích

Na **grafu č. 1** můžeme vidět provedení analýzy na 34 vzorcích vypracovaných asistovaných zhodnocení. Jak je vidět, tak neaplikovaných opatření je 42%, což je opravdu velká část těchto opatření. Nerelevantní opatření nejsou uvažovány. Na opatření,

která jsou neaplikována, by se společnosti měly zaměřit a soustředit se na jejich aplikování. V tom by měla pomoci metodika pro zpracování asistovaných zhodnocení. Společnosti si pomocí metodiky zjistí, které oblasti a konkrétní povinnosti nemá aplikované a má možnost na těchto neaplikovaných povinnostech pracovat.



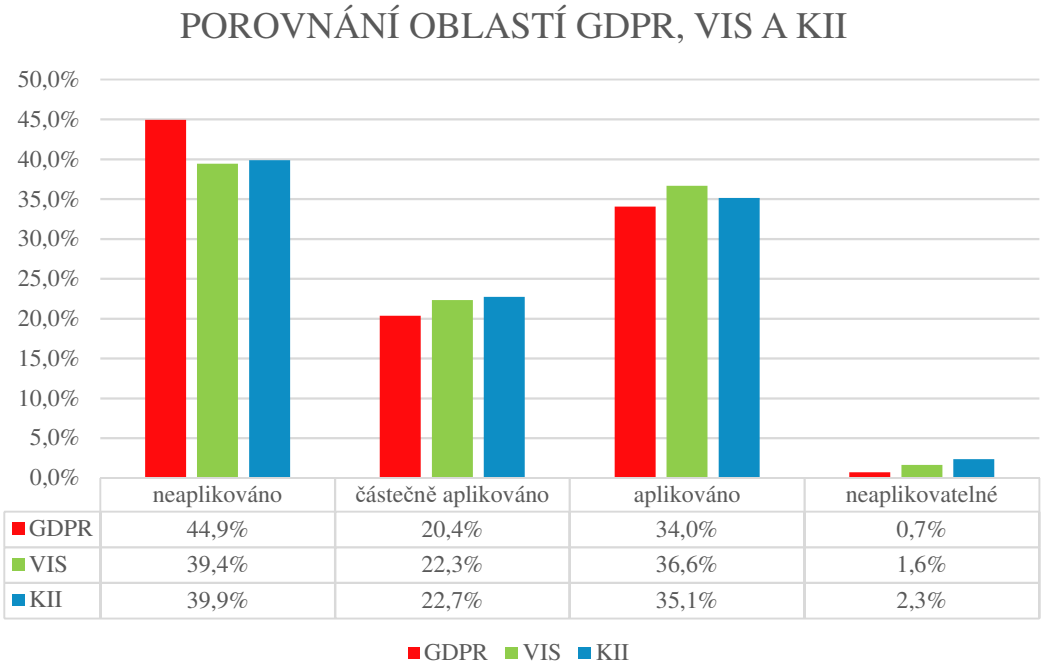
Graf 1: Souhrnné hodnocení na všech vzorcích

(Zdroj: 14)

2.5.2 Porovnání oblastí GDPR, VIS a KII

Z **grafu č. 2** je vidět, že nejvíce povinností je neaplikovaných. Nerelevantní hodnocení opět nebylo uvažováno a počet vzorků je stejný jako v případě grafu výše. Z pohledu na graf je jasné, že je potřeba zavedení jednotného rámce asistovaného zhodnocení včetně popisu povinností pro lepší porozumění respondenty a tím i zavedení všech povinností, které se týkají jednotlivých subjektů.

Dále je z grafu zřejmé, že v aplikaci povinností jsou nejdůslednější správci významných informačních systémů. Podobně dobře jsou na tom i správci kritické informační infrastruktury. Naopak GDPR má nejhorší procentuální výsledek v aplikovaných, částečně aplikovaných i neaplikovaných opatřeních. Stále ovšem zbývá velké procento neaplikovaných povinností u všech subjektů.



	neaplikováno	částečně aplikováno	aplikováno	neaplikovatelné
GDPR	44,9%	20,4%	34,0%	0,7%
VIS	39,4%	22,3%	36,6%	1,6%
KII	39,9%	22,7%	35,1%	2,3%

Graf 2: Porovnání oblastí GDPR, VIS a KII

(Zdroj: 14)

3 VLASTNÍ NÁVRH ŘEŠENÍ

Cílem, a tím i vlastním návrhem řešení, bude vytvoření obecného a jednotného rámce pro zpracování asistovaných zhodnocení. Metodika je vytvořena za pomoci dokumentu s názvem Pomůcka k auditu bezpečnostních opatření podle zákona o kybernetické bezpečnosti, který poskytuje rámec bezpečnostních opatření a slouží jako podpůrné vodítko. Každá společnost je jiná, a tak může obsahovat všechny popsané oblasti bezpečnostních opatření nebo pouze jejich část. Tyto oblasti vychází ze zákona o kybernetické bezpečnosti (ZKB) a z vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb. (VKB). Dělení subjektů vymezuje zákon o kybernetické bezpečnosti. Prvním důležitým krokem tedy je zvolit pro systém správnou kategorii podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů. Tedy zařazení mezi významné informační systémy (VIS), informační a komunikační systémy kritické informační infrastruktury (KII) nebo informační systémy základní služby. Metodika tedy bude sloužit jako vodítko a pomocný podklad, nikoliv jako daný předpis. Výstupem asistovaného zhodnocení je zhodnocení reálného stavu řízení kybernetické a informační bezpečnosti, bezpečnostních opatření podle ZKB a VKB a plnění GDPR ve společnosti. Pro vrcholový management doporučuji výstup ve formě grafů pro lepší porozumění.

Důležitým krokem při realizaci asistovaného zhodnocení je sejít se se zástupci společnosti, kteří nám sdělí základní informace a pomohu nám zorientovat se a vymezit oblasti, které je potřeba řešit. Na samém počátku je důležité, aby vrcholový management společnosti souhlasil s vypracováním asistovaného zhodnocení. V další fázi je potřeba zjistit kde společnost sídlí, kolik má zaměstnanců, s kterými respondenty a kdy se bude asistované zhodnocení řešit, klíčové služby a ICT, jaké oblasti řeší společnost formou outsourcingu, regulace, jestli se řešilo již ISMS, seznam dodavatelů atd. Dokument s asistovaným zhodnocením obsahuje také doporučení analytika, který zpracovává asistované zhodnocení, rizika, dokumenty, které budou potřeba a na co se změřit při implementaci.

3.1 Organizační opatření

Část, která řeší organizační opatření, je tvořena 13 oblastmi a vybrané oblasti se týkají např. zaměstnanců, rizik a jejich opatření, identifikace a ohodnocení aktiv, komunikace, školení, kontroly souladu s dokumentací a směrnicemi atd.

3.1.1 Systém řízení bezpečnosti informací

Tento systém využívá Demingova modelu – PDCA cyklus. ISMS vychází z mezinárodní normy ISO/IEC 27001. Norma ISO/IEC 27001 poskytuje podporu pro *„ustavení, zavádění, provozování, monitorování, udržování a zlepšování ISMS“* (1). Přijetí ISMS je strategickým rozhodnutím vrcholového managementu společnosti. Navržení a zavedení ISMS musí být v souladu s cíli společnosti, bezpečnostními požadavky, zavedenými procesy, ale také s velikostí a strukturou společnosti. ISMS se posuzuje z pohledu zainteresovaných stran (11).

Tab. 7: Oblast řízení bezpečnosti informací
(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X		Je stanoven rozsah ISMS.	VKB, § 3, odst. 1 a)
X	X	Je zaveden proces řízení rizik.	VKB, § 3, odst. 1 b), odst. 2 a)
X	X	Jsou vytvořeny, schváleny a zavedeny bezpečnostní politiky v oblasti ISMS a také jsou zavedena příslušná bezpečnostní opatření.	VKB, § 3, odst. 1 c), odst. 2 b)
X		Jsou zavedeny procesy: - monitorování účinnosti bezpečnostních opatření, - vyhodnocování vhodnosti a účinnosti bezpečnostní politiky, - vyhodnocení účinnosti ISMS.	VKB, § 3, odst. 1 d), odst. 1 e), odst. 1 g)
X		Audit kybernetické bezpečnosti je proveden minimálně 1x ročně.	VKB, § 3, odst. 1 f)
X		Aktualizace ISMS a související dokumentace je prováděna na základě zjištění auditů / penetračních testů.	VKB, § 3, odst. 1 h)
X		Je řízen provoz a zdroje ISMS, zaznamenávají se činnosti spojené s ISMS a se souvisejícím řízení rizik.	VKB, § 3, odst. 1 i)

KII	VIS	Povinnost	Zákon / norma
	X	Nejméně 1x za 3 roky je provedena aktualizace zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí.	VKB, § 3, odst. 2 c)

V této oblasti asistovaného zhodnocení se hodnotí, zda má organizace určený rozsah ISMS. Rozsahem je myšlen seznam aktiv a jejich garantů, ale také to, co se řešit nebude. Také je určeno, kterých částí organizace se ISMS týká.

U bezpečnostní politiky je třeba stanovit pravidla a postupy pro řízení dokumentace a náležitosti dokumentů, řízení zdrojů a provozu systému, řízení bezpečnosti informací, provádění auditů kybernetické bezpečnosti, přezkoumání ISMS a pro nápravná opatření a zlepšování ISMS. Je také nutné popsat, jakým způsobem se politika schvaluje, reviduje, uchovává a přezkoumává.

Zavedení procesu monitorování účinnosti bezpečnostních opatření znamená, že musí být uvedeno co, jak a kdy je monitorováno a měřeno, jak probíhá analýza a vyhodnocení monitorování a měření, kdo je odpovědný a kdy bude analýza monitorování a měření vyhodnocena. Vyhodnocení monitorování a měření by mělo obsahovat výsledky, metriky, záznamy o nápravných a preventivních opatřeních. Z údajů o přezkoumávání ISMS by mělo vykazovat zlepšování a plnění cílů. V organizaci může být zaveden tzv. Program měření ISMS. Využití výsledků by mělo být pouze zainteresovanými stranami.

Audit kybernetické bezpečnosti je prováděn podle plánu auditů (nejméně 1x ročně) a z předchozích auditů jsou vedeny a dokumentovány záznamy.

Aktualizace ISMS a související dokumentace je prováděna po vyhodnocení účinnosti, kontrol a auditů, přezkoumání rizik nebo po změnách. Tato aktualizace musí odpovídat i údajům v RTP (plán zvládání rizik) a SoA (prohlášení o aplikovatelnosti), auditních a kontrolních zprávách, zprávách o hodnocení účinnosti a s řízením změn. Kontrola aktualizace ISMS je provedena pomocí doložení aktualizovaných dokumentů, procesů a procedur.

U řízení provozu a zdrojů ISMS je potřeba v organizaci hledat záznamy o zdrojích, které mohou být lidské, materiální atd., záznamy o rozpočtu. Také je potřeba ověřit, že jsou zdroje řízeny (identifikace, plánování, zpřístupnění, používání, monitorování atd.). Při rozhodování o zdrojích ISMS by měla být hodnocena současná a předešlá výkonnost.

3.1.2 Řízení rizik

Řízení rizik popisuje norma ISO/IEC 27005. Norma má pouze informativní charakter a není přesnou příručkou pro zpracování řízení rizik. Pro malé informační systémy (např. jedna pracovní stanice s utajovanými informacemi maximálně do stupně utajení Vyhrazené) byla vypracována zjednodušená metodika hodnocení rizik (1).

Tab. 8: Oblast řízení rizik

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Jsou stanoveny metodiky pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik.	VKB, § 4, odst. 1 a), odst. 2 a)
X	X	Je prováděna identifikace a hodnocení důležitosti aktiv, která patří do rozsahu ISMS, podle § 8 (Řízení aktiv) minimálně v rozsahu přílohy č. 1 k VKB a výstupy jsou zapracovány do zprávy o hodnocení aktiv a rizik.	VKB, § 4, odst. 1 b), odst. 2 b)
X	X	Je prováděna identifikace rizik, při kterých jsou zohledňovány hrozby a zranitelnosti, jsou posuzovány možné dopady na aktiva. Tato rizika jsou hodnocena minimálně v rozsahu podle přílohy č. 2 k VKB. Jsou určena a schválena přijatelná rizika a je zpracována zpráva o hodnocení aktiv a rizik.	VKB, § 4, odst. 1 c), odst. 2 c)

KII	VIS	Povinnost	Zákon / norma
X	X	Na základě bezpečnostních potřeb a výsledků hodnocení rizik je zpracováváno prohlášení o aplikovatelnosti (SoA).	VKB, § 4, odst. 1 d), odst. 2 d)
X	X	Je zpracovaný a zavedený plán zvládání rizik (RTP), který obsahuje cíle a přínosy bezpečnostních opatření. Je určena osoba odpovědná za prosazování bezpečnostních opatření. Jsou určeny potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními.	VKB, § 4, odst. 1 e), odst. 2 e)
X	X	Bez zbytečného odkladu jsou zohledňována reaktivní a ochranná opatření vydaná NBÚ v hodnocení rizik a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, jsou doplněny plány zvládání rizik.	VKB, § 4, odst. 1 f), odst. 2 f)
X	X	Řízení rizik je zajištěno jinými způsoby (než jak je stanoveno v odstavci 1 a 2) a orgán a osoba doložil(a), že použitá opatření zajišťují stejnou nebo vyšší úroveň řízení rizik.	VKB, § 4, odst. 3

KII	VIS	Povinnost	Zákon / norma
X	X	Při hodnocení rizik jsou zváženy hrozby, související s: - porušením bezpečnostní politiky, provedením neoprávněných činností, - zneužitím oprávnění ze strany uživatelů a administrátorů, - poškozením nebo selháním technického anebo programového vybavení, - zneužitím identity fyzické osoby, - užíváním programového vybavení v rozporu s licenčními podmínkami, - kybernetickým útokem z komunikační sítě, - škodlivým kódem (například viry, spyware, trojské koně), - nedostatky při poskytování služeb IS/KS KII nebo VIS, - narušením fyzické bezpečnosti, - přerušením poskytování služeb elektronických komunikací nebo dodávek elektrické energie, - zneužitím nebo neoprávněnou modifikací údajů, - trvale působícími hrozbami, - s odcizením nebo poškozením aktiva.	VKB, § 4, odst. 4 a), odst. 4 b), odst. 4 c), odst. 4 d), odst. 4 e), odst. 4 f), odst. 4 g), odst. 4 h), odst. 4 i), odst. 4 j), odst. 4 k), odst. 4 l)

KII	VIS	Povinnost	Zákon / norma
X		Při hodnocení rizik jsou zváženy hrozby, související s: - porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany administrátorů KII, - pochybením ze strany zaměstnanců, - zneužitím vnitřních prostředků, sabotáží, - dlouhodobým přerušením poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb, - nedostatkem zaměstnanců s potřebnou odbornou úrovní, - cíleným kybernetickým útokem pomocí sociálního inženýrství, použitím špionážních technik, - zneužitím vyměnitelných technických nosičů dat.	VKB, § 4, odst. 6 a), odst. 6 b), odst. 6 c), odst. 6 d), odst. 6 e), odst. 6 f), odst. 6 g)

KII	VIS	Povinnost	Zákon / norma
X	X	Zváženy zranitelnosti, související s: - nedostatečnou ochranou vnějšího perimetru, - nedostatečným bezpečnostním povědomí uživatelů a administrátorů, - nedostatečnou údržbou IS/KS KII nebo VIS, - nevhodným nastavením přístupových oprávnění, - nedostatečnými postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, - nedostatečným monitorováním činností uživatelů a administrátorů a neschopností odhalit jejich nevhodné nebo závadné způsoby chování, - s nedostatečným stanovením bezpečnostních pravidel, nepřesným nebo nejednoznačným vymezením práv a povinností uživatelů, administrátorů a bezpečnostních rolí.	VKB, § 4, odst. 5 a), odst. 5 b), odst. 5 c), odst. 5 d), odst. 5 e), odst. 5 f), odst. 5 g)
X		Zváženy zranitelnosti, související s: - nedostatečnou ochranou ICT, - nevhodnou bezpečnostní architekturou, - nedostatečnou mírou nezávislé kontroly, - neschopností včasného odhalení pochybení ze strany zaměstnanců.	VKB, § 4, odst. 7 a), odst. 7 b), odst. 7 c), odst. 7 d)

Cílem metodik pro identifikaci a hodnocení aktiv a rizik je vytvořit seznam aktiv a jejich klasifikaci (hodnocení důležitosti…). Následně je nutné vytvořit i klasifikaci rizik, metody pro hodnocení rizik a kritéria pro přijatelnost rizik. K vytvoření kritérií pro

přijatelnost rizik můžeme využít přílohy vyhlášky o kybernetické bezpečnosti. Hodnocení rizik v ICT by mělo být v souladu s hodnocením rizik organizace.

Ve zprávě o hodnocení aktiv a rizik musí být uvedeny zohledňované hrozby, zranitelnosti a posouzeny dopady. Zprávy o hodnocení aktiv a rizik musí obsahovat i stupnice, které jsou použity pro určení úrovně dopadu a jejich popis.

V prohlášení o aplikovatelnosti (SoA) je uvedeno, jaká opatření společnost zavedla proti jakým rizikům. Může v něm být také uvedeno, jaká opatření z něj byla vyloučena podle ISO 27 000, příloha A.

Plán zvládání rizik (RTP) je určitý „projektový plán“. Tento plán obsahuje odpovědnosti za daná opatření, časový rámec, potřebné zdroje a vazby mezi riziky.

3.1.3 Bezpečnostní politika

Tato oblast je souhrnem pravidel, směrnic a zvyklostí, které určují způsoby, jak jsou aktiva v organizaci včetně citlivých informací řízena, chráněna a distribuována. Pro společnost je to základní dokumentace pro zabezpečení organizace. Bezpečnostních politik je 22 (1).

Zajišťuje také úroveň důvěrnosti, autenticity a integrity dat a také se stará o bezpečnost transakcí v distribuovaném prostředí. Požadavkem pro úplnost bezpečnostní politiky je dokument, který zahrnuje všechny významné oblasti informační bezpečnosti v organizaci (viz. tabulka č. 9) a tento dokument je v souladu s Organizačním řádem. Bezpečnostní politika musí být stanovena v relevantních oblastech asistovaného zhodnocení s ohledem na danou společnost.

Tab. 9: Oblast bezpečnostních politik

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Je stanovena bezpečnostní politika v oblasti systému řízení bezpečnosti informací.	VKB, § 5, odst. 1 a), odst. 2 a)
X	X	Je stanovena bezpečnostní politika v oblasti organizační bezpečnosti	VKB, § 5, odst. 1 b), odst. 2 b)
X		Je stanovena bezpečnostní politika v oblasti řízení vztahů s dodavateli.	VKB, § 5, odst. 1 c)

KII	VIS	Povinnost	Zákon / norma
	X	Je stanovena bezpečnostní politika v oblasti řízení dodavatelů.	VKB, § 5, odst. 2 c)
X	X	Je stanovena bezpečnostní politika v oblasti klasifikace aktiv.	VKB, § 5, odst. 1 d), odst. 2 d)
X	X	Je stanovena bezpečnostní politika v oblasti bezpečnosti lidských zdrojů.	VKB, § 5, odst. 1 e), odst. 2 e)
X	X	Je stanovena bezpečnostní politika v oblasti řízení provozu a komunikací.	VKB, § 5, odst. 1 f), odst. 2 f)
X	X	Je stanovena bezpečnostní politika v oblasti řízení přístupu.	VKB, § 5, odst. 1 g), odst. 2 g)
X	X	Je stanovena bezpečnostní politika v oblasti bezpečného chování uživatelů.	VKB, § 5, odst. 1 h), odst. 2 h)
X	X	Je stanovena bezpečnostní politika v oblasti zálohování a obnovy.	VKB, § 5, odst. 1 i), odst. 2 i)
X		Je stanovena bezpečnostní politika v oblasti bezpečného předávání a výměny informací.	VKB, § 5, odst. 1 j)
X		Je stanovena bezpečnostní politika v oblasti řízení technických zranitelností.	VKB, § 5, odst. 1 k)
X		Je stanovena bezpečnostní politika v oblasti bezpečného používání mobilních zařízení.	VKB, § 5, odst. 1 l)
X	X	Je stanovena bezpečnostní politika v oblasti poskytování a nabývání licencí programového vybavení a informací.	VKB, § 5, odst. 1 m), odst. 2 j)
X		Je stanovena bezpečnostní politika v oblasti dlouhodobého ukládání a archivace informací.	VKB, § 5, odst. 1 n)
X	X	Je stanovena bezpečnostní politika v oblasti ochrany osobních údajů.	VKB, § 5, odst. 1 o), odst. 2 k)
X		Je stanovena bezpečnostní politika v oblasti fyzické bezpečnosti.	VKB, § 5, odst. 1 p)
X		Je stanovena bezpečnostní politika v oblasti bezpečnosti komunikační sítě.	VKB, § 5, odst. 1 q)

KII	VIS	Povinnost	Zákon / norma
X	X	Je stanovena bezpečnostní politika v oblasti ochrany před škodlivým kódem.	VKB, § 5, odst. 1 r), odst. 2 m)
X	X	Je stanovena bezpečnostní politika v oblasti nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.	VKB, § 5, odst. 1 s), odst. 2 n)
X		Je stanovena bezpečnostní politika v oblasti využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.	VKB, § 5, odst. 1 t)
X	X	Je stanovena bezpečnostní politika v oblasti používání kryptografické ochrany.	VKB, § 5, odst. 1 u), odst. 2 l)
X	X	Je pravidelně hodnocena účinnost bezpečnostní politiky. Bezpečnostní politika je pravidelně aktualizována.	VKB, § 5, odst. 3

Bezpečnostní politika v ISMS obsahuje cíle, principy a potřeby pro ISMS a také koncept ICT bezpečnosti ve společnosti. Společnost si také stanoví rozsah a hranice ISMS. Dále jsou stanoveny pravidla a postupy pro řízení dokumentace, pro řízení zdrojů a provozu ISMS, pro provádění auditů kybernetické bezpečnosti, pro přezkoumávání ISMS a pro nápravná opatření a zlepšování ISMS. Další informace, které potřebuje společnost určit, jsou obchodní, právní a jiné požadavky, závazek managementu, náležitosti dokumentu, popis, schvalování, revize, uchovávání a přezkoumávání politiky, metody řízení dokumentů a zaměření na konkrétní skupiny lidí (všichni zaměstnanci, určitý úsek atd.).

Organizační bezpečnost určuje bezpečnostní role a jejich práva a povinnosti. Také tato bezpečnostní politika obsahuje požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí.

Pro vytvoření politiky v řízení vztahů s dodavateli a řízení dodavatelů je třeba stanovit bezpečnostní požadavky pro dodavatele. Ty jsou popsány v kapitole Stanovení bezpečnostních požadavků pro dodavatele. Mimo jiné je třeba definovat pravidla a

principy pro výběr dodavatelů, pro hodnocení rizik dodavatelů, pro provádění kontroly zavedení bezpečnostních opatření (zákaznický audit) a pro hodnocení dodavatelů. Stanoveny jsou i náležitosti, které musí obsahovat smlouvy o úrovni poskytovaných služeb, způsoby a úrovně realizace bezpečnostních opatření a určení vzájemné smluvní odpovědnosti.

Klasifikace aktiv je prováděna pomocí určení a evidence primárních aktiv včetně stanovení garanta aktiva. Primární aktiva jsou hodnocena podle důležitosti z hlediska důvěrnosti, dostupnosti a integrity. Podpůrná aktiva jsou identifikována, hodnocena a evidována a opět je u nich určen garant. Následně jsou určeny vazby mezi primárními a podpůrnými aktivy. Společnost určí pravidla ochrany jednotlivých úrovní aktiv (způsoby rozlišování jednotlivých úrovní, pravidla pro manipulaci a evidenci aktiv podle jednotlivých úrovní a přípustné způsoby používání aktiv) a způsoby, jak spolehlivě smazat nebo zničit technické nosiče dat.

Bezpečnost lidských zdrojů obsahuje pravidla pro rozvoj bezpečnostního povědomí a způsoby hodnocení, způsoby a formy poučení uživatelů, garantů aktiv, administrátorů a bezpečnostních rolí. Spadá sem i bezpečnostní školení nových zaměstnanců, pravidla pro řešení případ porušení bezpečnostní politiky ISMS, pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice (vrácení svěřených aktiv, odebrání práv při ukončení pracovního vztahu nebo změna přístupových práv při změně pracovní pozice).

Bezpečnostní politika řízení provozu a komunikací stanovuje pravomoci a odpovědnosti, které se týkají bezpečného provozu, postupy bezpečného provozu, požadavky a standardy bezpečného provozu, řízení technických zranitelností a pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů.

Řízení přístupu zahrnuje princip minimálních oprávnění a princip minimální potřeby znát. Dále je také potřeba stanovit požadavky na řízení přístupu, životní cyklus přístupu, řízení privilegovaných oprávnění (administrátorských účtů), řízení přístupu pro mimořádné situace a pravidelné přezkoumávání přístupových oprávnění (včetně rozdělení jednotlivých uživatelů v přístupových skupinách).

Bezpečné chování uživatelů je politika, která je zaměřena na bezpečnost uživatelů a na bezpečné chování uživatelů. Dále obsahuje pravidla pro bezpečné nakládání s aktivy a hesly, bezpečné použití elektronické pošty, bezpečné chování na internetu a sociálních sítích, bezpečný vzdálený přístup a bezpečnost ve vztahu k mobilním zařízením.

Bezpečnostní politika zálohování a obnovy se zaměřuje na to, jakým způsobem je zajištěna ochrana dat proti ztrátě. Obsahuje také plán záloh a jejich kontrolu, požadavky na zálohování a obnovu, pravidla, postupy zálohování, obnovy a testování zálohování a obnovy a pravidla bezpečného uložení záloh.

Politika bezpečného předávání a výměny informací definuje přijatelnou míru a způsob bezpečného předávání a výměny informací, postupy při přenosu informací, dohody o přenosu informací, elektronické předávání informací dohody o utajení nebo mlčenlivosti (NDA) a pravidla pro využití kryptografické ochrany.

Řízení technických zranitelností řeší, jak je zajištěno včasné zjištění technické zranitelnosti a jakým způsobem jsou následně přijata související opatření proti patřičným rizikům. V této oblasti je také potřeba mít přehled o software, který je instalován a hardware, který je používán. Souvisí také s politikou, která má na starosti aplikační bezpečnost. Dále tato oblast řeší pravidla pro omezení instalace programového vybavení a pravidla a postupy vyhledávání opravných programových balíčků, testování oprav programového vybavení a nasazení oprav programového vybavení.

Politika bezpečného používání mobilních zařízení obsahuje popis zvládání rizik spojených s používáním mobilních zařízení, prací na dálku atd. Obsahuje pravidla a postupy pro bezpečné používání mobilních zařízení i těch, které nejsou majetkem správce (BYOD).

Poskytování a nabývání licencí programového vybavení a informací řeší správy licencí, způsoby nabývání licencí, seznam a evidenci licencí k programům a informacím. Společnost má definována pravidla a postupy pro kontrolu dodržování licenčních podmínek.

Bezpečnostní politika dlouhodobého ukládání a archivace informací obsahuje pravidla a postupy archivace dokumentů a záznamů, ochranu archivovaných dokumentů a záznamů a politiku přístupu k archivovaným dokumentům a záznamům.

Ochrana osobních údajů znamená povinnost zabezpečit všechny osobní údaje, které se ve společnosti nacházejí, a to podle nařízení o ochraně osobních údajů neboli GDPR. Tomuto nařízení je potřeba přizpůsobit všechna technická i organizační opatření a vyhodnotit bezpečnostní rizika, která mohou nastat při zavádění opatření.

Bezpečnostní politika fyzické bezpečnosti obsahuje pravidla pro ochranu objektů, pro kontrolu vstupu osob, pro ochranu zařízení a také detekci narušení fyzické bezpečnosti.

Politika bezpečnosti komunikační sítě definuje pravidla a postupy pro zajištění bezpečnosti sítě, pro řízení přístupů v rámci sítě (např. IEEE 802.1X) a pro ochranu vzdáleného přístupu k síti. Také určuje práva a povinnosti za bezpečný provoz sítě.

Ochrana před škodlivým kódem obsahuje pravidla a postupy pro ochranu komunikace mezi vnitřní a vnější sítí, ochranu serverů a sdílených datových úložišť a ochranu jednotlivých pracovních stanic.

Nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí obsahuje pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí neboli log management a také obsahuje provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí.

Využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí stanovuje pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních vlastností nástroje typu SIEM a pravidelnou aktualizaci těchto pravidel.

Používání kryptografické ochrany určuje úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu. Tato politika obsahuje pravidla kryptografické ochrany informací při přenosu po komunikačních sítích, při uložení na mobilní zařízení nebo vyměnitelný technický nosič dat a systém správy klíčů.

Revize a účinnost bezpečnostních politik je pravidelně hodnocena. Ověřuje se, jestli aktualizace bezpečnostních politik prováděna v závislosti na vyhodnocení účinnosti.

3.1.4 Organizační bezpečnost

Organizační bezpečnost stanovuje a definuje bezpečnostní role podle Vyhlášky o kybernetické bezpečnosti. Jedná se o role, které se nachází v následujících odstavcích (4).

Výbor kybernetické bezpečnosti je zodpovědný za rozvoj a vývoj kybernetické bezpečnosti, tvoří rámec kybernetické bezpečnosti, její směrování a zásady, definuje role a odpovědnosti ISMS, definuje požadavky na reporting a kontrolu ISMS a má na starosti také aktuální stav kybernetické bezpečnosti (4).

Manažer kybernetické bezpečnosti má na starosti odpovědnosti za řízení ISMS, pravidelný reporting a komunikaci s vrcholovým managementem, předkládání zpráv o hodnocení rizik a aktiv, plánu zvládání rizik a prohlášení o aplikovatelnosti, poskytování pokynů při jakékoliv fázi dodavatelských vztahů v ICT, komunikuje s GovCERT nebo CSIRT, podílí se na řízení rizik, koordinuje řízení incidentů a vyhodnocuje vhodnost a účinnost bezpečnostních opatření. Dále musí mít odpovídající znalosti, zkušenosti, vzdělání, praxi a certifikaci (4).

Architekt kybernetické bezpečnosti odpovídá za návrh implementace bezpečnostních opatření a zajišťuje architekturu bezpečnosti. Navíc musí opět mít znalosti, zkušenosti, vzdělání, praxi a odpovídající certifikaci (4).

Auditor kybernetické bezpečnosti provádí audit kybernetické bezpečnosti a opět je potřeba, aby měl dostatečné znalosti, zkušenosti, praxi, vzdělání a odpovídající certifikaci (4).

Garant aktiva je zodpovědný za rozvoj, použití a bezpečnost aktiva a musí spolupracovat s ostatními osobami, které vykonávají bezpečnostní role. Navíc by měl mít dostatek zkušeností (4).

Tab. 10: Oblast organizační bezpečnosti

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Je zavedena organizační bezpečnost, v rámci které je určen výbor pro řízení kybernetické bezpečnosti a bezpečnostní role včetně jejích práv a povinností souvisejících s ICT.	VKB, § 6, odst. 1)
X		Je určena bezpečnostní role: manažer kybernetické bezpečnosti / ISMS manažer.	VKB, § 6, odst. 2 a)
X		Je určena bezpečnostní role: architekt kybernetické bezpečnosti.	VKB, § 6, odst. 2 b)
X		Je určena bezpečnostní role: auditor kybernetické bezpečnosti.	VKB, § 6, odst. 2 c)
X		Je určena bezpečnostní role: garant aktiva.	VKB, § 6, odst. 2 d)
	X	Bezpečnostní role jsou určeny přiměřeně.	VKB, § 6, odst. 3
X	X	Je určen výbor pro řízení kybernetické bezpečnosti.	VKB, § 6, odst. 7
X	X	Je zajištěno odborné školení osob, které zastávají bezpečnostní role (v souladu s plánem budování bezpečnostního povědomí).	VKB, § 6, odst. 8

Určení výboru je dokument, který obsahuje a vymezuje složení, práva a povinnosti. Tento dokument musí být schválený statutárním zástupcem společnosti.

Manažer kybernetické bezpečnosti a architekt kybernetické bezpečnosti jsou osoby, které musí splňovat požadavky o praxi a musí být proškoleny (doloženo záznamem o školení - certifikát a prokázání praxe – čestné prohlášení o praxi). Výkon těchto rolí je definován dokumentem, který je opět schválený statutárním zástupcem společnosti a obsahuje práva, povinnosti a kompetence manažera nebo architekta kybernetické bezpečnosti.

Auditor kybernetické bezpečnosti má stejné požadavky jako manažer a architekt kybernetické bezpečnosti, ale je oddělen od ostatních rolí v kybernetické bezpečnosti.

Zda jsou bezpečnostní role určeny přiměřeně je velmi individuální, takže záleží, jak bude výpověď respondenta zapadat do kontextu.

Školení (včetně opakování) je zahrnuto v plánu rozvoje bezpečnostního povědomí a musí odpovídat tomuto plánu. Analytik kontroluje dokumentaci o provedeném školení (prezenční listiny, certifikát, potvrzení lektora nebo jiný doklad).

3.1.5 Stanovení bezpečnostních požadavků pro dodavatele

Oblast požadavků pro dodavatele řeší bezpečnostní opatření pro smluvní vztahy včetně výběru dodavatelů. Smlouvy s dodavateli obsahují následující ustanovení:

- ustanovení o bezpečnosti informací (z hlediska důvěrnosti, dostupnosti a integrity),
- ustanovení o oprávnění používat data,
- ustanovení o autorství programového kódu (popř. programových licencí),
- ustanovení o kontrole a auditu dodavatele,
- ustanovení upravující řetězení dodavatelů,
- ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,
- ustanovení o řízení změn,
- ustanovení o souladu smluv s obecně závaznými právními předpisy,
- ustanovení o povinnosti dodavatele informovat povinnou osobu o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
- ustanovení o povinnosti dodavatele informovat povinnou osobu o způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,
- ustanovení o povinnosti dodavatele informovat povinnou osobu o významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv (popř. změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem),

- ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy,
- specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy,
- specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli,
- specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,
- pravidla pro likvidaci dat,
- ustanovení o sankcích za porušení povinností (15).

Tab. 11: Oblast stanovení bezpečnostních požadavků pro dodavatele

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Jsou stanovena pravidla pro dodavatele, která zohledňují potřeby řízení bezpečnosti informací, a řídí své dodavatele nebo jiné externí subjekty, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti IS nebo KS KII a VIS. Rozsah zapojení dodavatelů na rozvoji, provozu nebo zajištění bezpečnosti IS nebo KS KII a VIS je dokumentován písemnou smlouvou, jejíž součástí je ustanovení o bezpečnosti informací.	VKB, § 7, odst. 1
X		U dodavatelů je před uzavřením smlouvy prováděno hodnocení rizik, která jsou spojena s podstatnými dodávkami.	VKB § 7, odst. 2 a)
X		U dodavatelů je uzavírána smlouva o úrovni služeb (SLA), která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.	VKB § 7, odst. 2 b)

KII	VIS	Povinnost	Zákon / norma
X		U dodavatelů se provádí pravidelné hodnocení rizik a pravidelná kontrola zavedených bezpečnostních opatření u poskytovaných služeb jsou zjištěné nedostatky odstraněny nebo je po dohodě s dodavatelem zajištěno jejich odstranění.	VKB § 7, odst. 2 c)

Smlouvy obsahují pravidla pro dodavatele, další externí subjekty a jak probíhá výběr dodavatelů. Je potřeba smluvně stanovit jak bude řešena a jaký bude mít rozsah bezpečnost informací. Dále je nutné dokumentovat rozsah zapojení dodavatelů na provozu, rozvoji a bezpečnosti (přístupy k IS/KS, předávání dat, pravidla pro změny nastavení, jejich oznamování a dokumentace těchto změn a v neposlední řadě také garance za dostupnost, důvěrnost a integritu).

Hodnocení rizik u dodavatelů je dokument, kde je zpracována analýza rizik a zpráva o hodnocení rizik.

Smlouva o úrovni služeb dodavatelů obsahuje způsob a úroveň realizace bezpečnostních opatření a stanovuje odpovědnost za vedení a kontrolu bezpečnostních opatření. Obsahuje také sankce za nedodržení této smlouvy.

V případě pravidelného hodnocení rizik je potřeba doložit, že toto hodnocení je pravidelně prováděno a jak často je prováděno. U kontroly bezpečnostních opatření u služeb je potřeba určit kdo ji provádí.

3.1.6 Řízení aktiv

Oblast řízení aktiv je řešena normou ČSN ISO/IEC 27001. Tato norma řeší dvě skupiny opatření, kterými jsou odpovědnost za aktiva a klasifikace informací (1).

Odpovědnost za aktiva obsahuje:

- evidence aktiv,
- vlastnictví aktiv (každé aktivum má odpovědného vlastníka),
- přípustné použití aktiv (pravidla používání aktiva) (1).

Klasifikace informací (slouží k ochraně utajovaných skutečností) obsahuje:

- doporučení pro klasifikaci,
- označování a nakládání s informacemi (podle druhů) (1).

Klasifikace probíhá podle klasifikačního schématu. Nejčastěji používaná schémata jsou pro komerční sféru a státní sektor. Komerční sféra využívá 4 stupňů klasifikace - důvěrné, soukromé, citlivé a veřejné. Státní sektor má stupňů 5 - přísně tajné, tajné, důvěrné, citlivé, ale neklasifikované a neklasifikované (1).

Tab. 12: Oblast řízení aktiv

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Jsou identifikována a evidována primární aktiva.	VKB, § 8, odst. 1 a)
X	X	Jsou určeni jednotliví garanti aktiv, kteří jsou odpovědní za primární aktiva.	VKB, § 8, odst. 1 b)
X	X	Je hodnocena důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a tato aktiva jsou zařazena do jednotlivých úrovní minimálně v rozsahu podle přílohy č. 1 k VKB.	VKB, § 8, odst. 1 c)

KII	VIS	Povinnost	Zákon / norma
X	X	Při hodnocení důležitosti primárních aktiv je především posuzováno: - rozsah a důležitost osobních údajů nebo obchodního tajemství, - rozsah dotčených právních povinností nebo jiných závazků, - rozsah narušení vnitřních řídících a kontrolních činností, - poškození veřejných, obchodních nebo ekonomických zájmů, - možné finanční ztráty, - rozsah narušení běžných činností orgánu a osoby, - dopady spojené s narušením důvěrnosti, integrity a dostupnosti, - dopady na zachování dobrého jména nebo ochranu dobré pověsti.	VKB, § 8, odst. 2 a), odst. 2 b), odst. 2 c), odst. 2 d), odst. 2 e), odst. 2 f), odst. 2 g), odst. 2 h)
X		Jsou identifikována a evidována podpůrná aktiva.	VKB, § 8, odst. 3 a)
X		Jsou určeni garanti aktiv, kteří jsou odpovědní za podpůrná aktiva.	VKB, § 8, odst. 3 b)
X		Jsou určeny vazby mezi primárními a podpůrnými aktivy a hodnoceny důsledky závislostí mezi primárními a podpůrnými aktivy.	VKB, § 8, odst. 3 c)

KII	VIS	Povinnost	Zákon / norma
X	X	Jsou stanovena pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že: - jsou určeny způsoby rozlišování jednotlivých úrovní aktiv, - jsou stanovena pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv, - jsou stanoveny přípustné způsoby používání aktiv.	VKB, § 8, odst. 4 a) 1., 2., 3.
X	X	Jsou zavedena pravidla ochrany odpovídající úrovni aktiv.	VKB, § 8, odst. 4 b)
X	X	Jsou určeny způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv.	VKB, § 8, odst. 4 c)

U řízení aktiv je potřeba stanovit metodiku pro identifikaci a hodnocení aktiv. K tomu patří i vytvoření stupnice pro hodnocení primárních aktiv a určení garantů aktiv s jejich odpovědnostmi. U hodnocení důležitosti primárních aktiv je třeba se ujistit, že je vycházeno i z bodů, které spadají do VKB, §8, odst. 2.

Podpůrná aktiva musí mít také stanovenou metodiku pro identifikaci a hodnocení aktiv, vytvořenou stupnici pro hodnocení podpůrných aktiv a určení garantů aktiv s jejich odpovědnostmi. Navíc je potřeba definovat vazby mezi primárními a podpůrnými aktivy (matice vazeb, stromové schéma atd.).

Musí být popsáno povolené i zakázané použití aktiv. Pravidla by se měla určit, dokumentovat a implementovat. Pravidla ochrany pro jednotlivé úrovně musí být formalizována. Formalizován musí být i postup bezpečné likvidace dat a nosičů dat.

3.1.7 Bezpečnost lidských zdrojů

Oblast bezpečnosti lidských zdrojů se může nazývat také jako personální bezpečnost a pracuje tedy s lidským faktorem. Systém je tak slabý jako jeho nejslabší článek, což je ve většině případů právě lidský faktor, a tak se tato oblast nesmí podcenit (1).

Bezpečnost lidských zdrojů je rozdělena na 3 části a to podle životního cyklu pracovního vztahu. Tyto 3 části jsou před vznikem pracovního vztahu, během pracovního vztahu a po změně nebo zániku pracovního vztahu (1).

Před vznikem pracovního vztahu je třeba definovat a zdokumentovat bezpečnostní role včetně odpovědností, které tato role má a to podle bezpečnostní politiky. Nový zaměstnanec také musí, kvůli bezpečnosti, projít prověrkami (osobní doklady, kvalifikace, vzdělání, školení) (1).

Tab. 13: Oblast bezpečnosti lidských zdrojů
(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Je stanoven plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a jsou určeny osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny.	VKB, § 9, odst. 1 a)
X	X	V souladu s plánem rozvoje bezpečnostního povědomí je zajištěno poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení.	VKB, § 9, odst. 1 b)
X	X	Je zajištěna kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.	VKB, § 9, odst. 1 c)

KII	VIS	Povinnost	Zákon / norma
X	X	Je zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.	VKB, § 9, odst. 1 d)
X	X	O školení jsou vedeny přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.	VKB, § 9, odst. 2)
X		Jsou stanovena pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů.	VKB, § 9, odst. 3 a)
X		Je hodnocena účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí.	VKB, § 9, odst. 3 b)
X		Jsou určena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.	VKB, § 9, odst. 3 c)
X		Je zajištěna změna přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.	VKB, § 9, odst. 3 d)

Plán rozvoje bezpečnostního povědomí obsahuje termíny potřebných školení a také osoby, které jsou odpovědné školení provádět. Školení by měla být vstupní a následně by se měla pravidelně opakovat. Také musí být uvedeno, jak často se školení opakují a stanoveny termíny školení. Školení by měla být pro uživatele, administrátory a jednotlivé bezpečností role. Výstupem jsou záznamy o školení, prezenční listiny, výpis z e-learningu nebo rozhovor se zaměstnanci.

Kontrola dodržování bezpečností politiky se provádí pro jednotlivé skupiny, jako jsou uživatelé, administrátoři a jednotlivé bezpečností role. Musí být uvedeno, kdo

dodržování bezpečnostních politik kontroluje a jestli bude kontrola prováděna namátkově nebo pravidelně. Jsou vedeny záznamy o kontrole, což jsou protokoly, kárná řízení, sledování činnosti uživatelů a technické prostředky. Nakonec proběhne srovnání bezpečností politiky se způsobem kontroly. V bezpečnostní politice musí být uvedeno oprávnění ke kontrole.

U zajištění vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu musí být evidováno, kdo má přidělena jaká aktiva a přístupy. Tato evidence se nachází buď v pracovních smlouvách, nebo interních předpisech. Také musí být určena doba, do kdy mají být svěřená aktiva a přístupy odebrány. Týká se to přístupových oprávnění do objektů i do systémů KII nebo VIS. Následně se toto odebrání ověřuje na IT oddělení. Opět musí být určena osoba, která to kontroluje a jestli je kontrola prováděna pravidelně nebo namátkově. Proces odebrání přístupů a aktiv je dokumentován (personální – IT oddělení). Ověřuje se také soulad dokumentovaného postupu a reálného stavu.

U přehledů o školení musí být uvedeno, kde jsou tyto přehledy vedeny a v jaké formě a také jestli odpovídají plánu rozvoje bezpečnostního povědomí. V přehledech je uveden předmět školení a seznam osob, které se ho zúčastnily (prezenční listiny, záznamy z e-learningu nebo dotázání se zaměstnanců).

Stanovena jsou i pravidla pro určení osob, které budou zastávat bezpečnostní role. Je také určeno kde a v jaké formě jsou pravidla stanovena a kdo je kontroluje. Musí se také kontrolovat, jestli pravidla odpovídají reálnému stavu (jestli záznamy o tom, kdo vykonává bezpečnostní role, odpovídají pravidlům).

Účinnost plánu rozvoje bezpečnostního povědomí musí být hodnocena a musí být určeno kde a v jaké formě se hodnocení vyskytuje, kdo tento plán hodnotí a jak často je toto hodnocení prováděno. Pro hodnocení účinnosti plánu rozvoje bezpečnostního povědomí jsou definovány metriky pro měření účinnosti (např. snížení počtu incidentů po školení) a následně se podle metrik provádí vyhodnocování. Následovat by měla opatření, která jsou vytvořena na základě zjištění z hodnocení účinnosti.

U řešení případů porušení stanovených bezpečnostních pravidel musí být především tato pravidla definována. Opět se určí kde a v jaké formě jsou tato pravidla

stanovena, kdo je hodnotí nebo projednává a stanoveny jsou také sankce za porušení pravidel. Zaznamenávají se také protokoly o porušení a zprávy o kárném řízení.

Proces změny přístupových oprávnění při změně postavení uživatele, administrátora nebo osoby, která zastává bezpečnostní roli, musí být popsán. Stanoví se pravidla provádění změn a změny jsou dokumentovány. Dále je potřeba vědět, jak rychle jsou přístupová oprávnění měněna.

3.1.8 Řízení provozu a komunikací

Oblast řízení provozu a komunikací obsahuje 10 skupin opatření, které podporují bezpečný provoz IS/ICT. Těmito 10 skupinami jsou:

- provozní postupy a odpovědnosti (dokumentace, řízení změn, oddělení povinností a oddělení vývoje, testování a provozu),
- řízení dodávek třetích stran (outsourcing – dodávky služeb (SLA), monitorování a přezkoumávání služeb, řízení změn),
- plánování a přejímání systémů (řízení kapacit, rutinní provoz IS),
- škodlivé programy a mobilní kódy (antivirová strategie),
- zálohování informací (plán zálohování, dodržení plánu, testování čitelnosti záloh, správné uložení záloh),
- správa bezpečnosti sítě (síťová opatření, bezpečnost interních i externích síťových služeb) – viz ISO/IEC 27033,
- bezpečnost při zacházení s médii (správa, likvidace, manipulace s informacemi, bezpečnost systémové dokumentace),
- výměna informací mezi organizací a partnery (postupy a politiky, dohody, bezpečnost při přepravě, elektronické zprávy, vzdálený přístup),
- služby elektronického obchodu (využívání elektronických služeb, on-line transakce, veřejné informace),
- monitorování provozu (tvorba auditních záznamů, monitorování IS, ochrana záznamů, administrátorský a operátorský deník, záznam selhání, synchronizace hodin) (1).

Tab. 14: Oblast řízení provozu a komunikací

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Pomocí technických nástrojů, uvedených ve VKB v § 21 až 23 ZKB, jsou detekovány kybernetické bezpečnostní události, jsou pravidelně vyhodnocovány získané informace a na zjištěné nedostatky je reagováno v souladu s: Zvládání kybernetických bezpečnostních událostí a incidentů (VKB § 13).	VKB, § 10, odst. 1
X	X	Je zajištěn bezpečný provoz informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému. Za tímto účelem jsou stanoveny provozní pravidla a postupy.	VKB, § 10, odst. 2
X	X	Je prováděno pravidelné zálohování a prověřování použitelnosti provedených záloh.	VKB, § 10, odst. 4

KII	VIS	Povinnost	Zákon / norma
X		Provozní pravidla a postupy orgánu a osoby obsahují: - práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů, - postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů, - postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech, - spojení na kontaktní osoby, které jsou určeny jako podpora při řešení neočekávaných systémových nebo technických potíží, - postupy řízení a schvalování provozních změn, - postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.	VKB, § 10 odst. 3 a), odst. 3 b), odst. 3 c), odst. 3 d), odst. 3 e), odst. 3 f)
X		Je zajištěno oddělení vývojového, testovacího a produkčního prostředí.	VKB, § 10, odst. 5 a)

KII	VIS	Povinnost	Zákon / norma
X		Jsou řešena reaktivní opatření vydaná NBÚ tím, že orgán a osoba: - posuzuje očekávané dopady reaktivního opatření na informační systém kritické informační infrastruktury nebo komunikační systém kritické informační infrastruktury a na zavedená bezpečnostní opatření, vyhodnocuje možné negativní účinky a bez zbytečného odkladu je oznamuje NBÚ, - stanovuje způsob rychlého provedení reaktivního opatření, který minimalizuje možné negativní účinky, a určuje časový plán jeho provedení.	VKB, § 10, odst. 5 b)
X		Je zajištěna bezpečnost a integrita komunikačních sítí a bezpečnost komunikačních služeb podle Nástroje pro ochranu integrity komunikačních sítí (VKB § 17).	VKB, § 10, odst. 6 a)
X		Jsou určena pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi.	VKB, § 10, odst. 6 b)
X		Výměna a předávání informací je prováděna na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla jsou dokumentována.	VKB, § 10, odst. 6 c)

KII	VIS	Povinnost	Zákon / norma
X		S ohledem na klasifikaci aktiv je prováděna výměna a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací.	VKB, § 10, odst. 6 d)

Detekování kybernetických bezpečnostních událostí se realizuje sběrem logů (záznamů) a jeho analýzou. Je nutné, aby bylo uvedeno, jakým způsobem je log management řešen a jestli je právě log management a detekce bezpečnostních událostí v souladu s politikou společnosti.

Pravidelné zálohování a prověřování použitelnosti těchto záloh obsahuje plán záloh, skutečnou existenci záloh a také jakým způsobem probíhá ověřování nebo testování záloh.

Povinnosti osob, které zastávají bezpečnostní role, administrátorů a uživatelů musí být definovány a to například pomocí RACI matice v politice.

3.1.9 Řízení přístupu a bezpečné chování uživatelů

Tato oblast řeší především řízení přístupu zejména k IS/ICT a rozdělit ho lze na:

- řízení přístupu uživatelů (přístupová práva),
- řízení přístupu k síti a síťovým službám,
- řízení přístupu k operačnímu systému,
- řízení přístupu k aplikacím,
- řízení dálkového přístupu (1).

Existují 3 základní principy řízení přístupu IS a tou je **identifikace** (rozpoznání entity systémem), **autentizace** (ověření identifikace entity nebo zprávy) a posledním principem je **autorizace** (ověření oprávnění pro vstup do systému nebo aplikace) (1).

Tab. 15: Oblast řízení přístupu a bezpečného chování uživatelů

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Na základě provozních a bezpečnostních potřeb je řízen přístup k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a každému uživateli je přiřazen jednoznačný identifikátor.	VKB, § 11, odst. 1
X	X	Jsou přijata opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů a administrátorů informačního systému kritické informační struktury, komunikačního systému kritické informační infrastruktury a významného informačního systému podle Nástroje pro ověřování identity uživatelů (VKB § 18) a Nástroje pro řízení přístupových oprávnění (VKB § 19), a která brání ve zneužití těchto údajů neoprávněnou osobou.	VKB, § 11, odst. 2)
X		Přistupujícím aplikacím je přidělen samostatný identifikátor.	VKB, § 11, odst. 3 a)
X		Přidělování administrátorských oprávnění je omezeno.	VKB, § 11, odst. 3 b)
X		Přidělování a odebírání přístupových oprávnění je prováděno v souladu s politikou řízení přístupu.	VKB, § 11, odst. 3 c)
X		Je prováděno pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích.	VKB, § 11, odst. 3 d)

KII	VIS	Povinnost	Zákon / norma
X		Je využíván nástroj pro ověřování identity uživatelů (VKB § 18) a nástroj pro řízení přístupových oprávnění (VKB § 19).	VKB, § 11, odst. 3 e)
X		Jsou zavedena bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými povinná osoba nedisponuje.	VKB, § 11, odst. 3 f)

Jednotlivým uživatelům a aplikacím, které jsou přiřazeny konkrétním lidem, musí být přiděleny jednotlivé identifikátory. Pozor si společnost musí dát na sdílená hesla Wi-Fi atd. Zamezit se musí také sdílené přístupy. Toto přidělování jednotlivých identifikátorů musí být v souladu s politikou bezpečnosti lidských zdrojů, politikou řízení přístupu, politikou bezpečného chování uživatelů, politikou bezpečného používání mobilních zařízení, politikou bezpečnosti komunikační sítě, politikou rozvoje bezpečnostního povědomí a s politikou bezpečného používání kryptografické ochrany.

Musí být určena osoba, která je pověřená správou identifikačních údajů uživatelů a taky musí být definováno, kde a jak tyto identifikační údaje spravuje. Tyto údaje jsou v souladu s politikou bezpečnosti lidských zdrojů, s politikou řízení přístupů, s identity managementem (IdM) a access managementem (AM).

V případě správy identifikačních údajů aplikací musí být opět určena osoba a kde a jak tyto identifikační údaje spravuje. Správa identifikačních údajů aplikací je v souladu s politikou řízení přístupů.

V případě přidělování administrátorských oprávnění je určena osoba, která oprávnění může přidělovat. Dále je definováno na základě, čeho jsou administrátoři určováni, seznam oprávnění administrátora a existence role tzv. „superadministrátora“. Pokud již není role administrátora nutná, je tato role odebrána. Administrátoři mají i běžný uživatelský účet, který má pouze běžná oprávnění.

Revidování nebo odebírání přístupových oprávnění je v souladu se změnou pracovního zařazení, odchodem zaměstnance (dočasným nebo stálým). Kontrola se provádí porovnáním reálného stavu s politikou řízení přístupu a personálním stavem kontrolované společnosti.

Je potřeba určit kdo, kde a jak provádí pravidelné přezkoumání nastavení přístupových opatření. Následně také jak jsou výstupy z těchto kontrol dokumentovány.

Bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení případně i využití technických zařízení, kterými povinná osoba nedisponuje, musí být v souladu s politikou řízení přístupu, kde musí být řešeno bezpečné používání mobilních zařízení. Definován musí být koncept Bring Your Own Device (BYOD) a implementace autentizace v počítačové síti IEEE 802.1X. Na reálný stav se následně analytik dotazuje u uživatelů.

3.1.10 Akvizice, vývoj a údržba

Oblast akvizice, vývoje a údržby má různé požadavky a s tím i požadavky na bezpečnost, které souvisejí se softwarovými aplikacemi, implementací a údržbou. Tato oblast se dělí na:

- bezpečnostní požadavky IS (aplikace již na nákup a pořízení IS),
- správnost zpracování v aplikacích (validace, kontrola integrity),
- kryptografická opatření (správa klíčů – generování, distribuce, uložení aktualizace, archivace, ničení),
- bezpečnost systémových souborů (softwarový audit, kontrola malware, omezení),
- bezpečnost procesů vývoje a podpory (únik informací),
- řízení technických zranitelností (instalace bezpečnostních záplat a ověření funkčnosti) (1).

Tab. 16: Oblast akvizice, vývoje a údržby

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Jsou stanoveny bezpečnostní požadavky na změny informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému spojené s jejich akvizicí, vývojem a údržbou a jsou zahrnuty do projektu akvizice, vývoje a údržby systému.	VKB, § 12, odst. 1
X		Jsou identifikována, hodnocena a řízena rizika související s akvizicí, vývojem a údržbou informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury. Pro postupy hodnocení a řízení rizik se použijí metodiky podle řízení rizik (VKB § 4) odst. 1 písm. a) obdobně.	VKB, § 12, odst. 2 a)
X		Je zajištěna bezpečnost vývojového prostředí a zároveň je zajištěna ochrana používaných testovacích dat.	VKB, § 12, odst. 2 b)
X		Je prováděno bezpečnostní testování změn informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury před jejich zavedením do provozu.	VKB, § 12, odst. 2 c)

Bezpečnostní požadavky na změny ICT se nachází v dokumentaci k realizovaným projektům a tato dokumentace je v souladu s politikou řízení dodavatelů, politikou bezpečnosti lidských zdrojů, politikou řízení přístupu a politikou bezpečného předávání a výměny informací.

Rizika, která souvisí s akvizicí, vývojem a údržbou systému se musí také řídit. Musí být tedy vypracována analýza rizik nebo případně plán zvládání rizik. Uvažují se rizika, která jsou spojeny s dodavateli v oblasti akvizice, vývoje a údržby. Bezpečnostní požadavky a další opatření, které vyplývají z analýzy rizik, by měla být zahrnuta v zadávací dokumentaci v případě dodavatelského řešení i řešení v rámci společnosti.

V oblasti bezpečnosti vývojového prostředí a ochrany používaných dat je potřeba určit kde a jak bude vývoj nebo testování probíhat a určit jaká data jsou použita pro testování. Musí být určeno i řízení přístupu do testovacího prostředí.

Bezpečnostní testování změn je standardizováno. Informace o tom, kdo a jak toto testování provádí a včetně standard jsou uvedeny v rámci předpisu. Určit se musí i komu se výsledky tohoto testování změn reportují a jaký je postup při vyhodnocování výsledků testování změn.

3.1.11 Zvládání kybernetických bezpečnostních událostí a incidentů

Tato oblast může být pojmenována také jako incident handling. Zvládání kybernetických bezpečnostních incidentů a událostí je děleno na dvě skupiny:

- **uživatelé** (hlášení bezpečnostních incidentů),
- **bezpečnostní odborníci** (zvládání bezpečnostních incidentů a kroky k nápravě) (1).

Spadá sem také bezpečnostní povědomí, které se v praxi dělí na 3 úrovně:

- **vysoká** (velmi dobře informovaní pracovníci),
- **střední** (dobře informovaní pracovníci s menšími zkušenostmi),
- **nízká** (nízké povědomí i většiny pracovníků) (1).

Bezpečnostní událost je stav, který byl identifikován a narušuje pravidla bezpečnostní politiky. Může nastat, ale nemusí. **Bezpečnostní incident** už je událost, která narušuje bezpečnost IS. Bezpečnostní incident už je problém, který nastal (1).

Prostředek k rozpoznání vážnosti bezpečnostního incidentu se nazývá systém zvládání bezpečnostních incidentů (SIMS). Má 4 fáze životního cyklu, kterými jsou:

- detekce události,

- identifikace, rozhodnutí a příprava řešení,
- řešení bezpečnostního incidentu,
- vyhodnocení incidentu (analýza, která vede k poučení) (1).

Tab. 17: Oblast zvládání kybernetických bezpečnostních událostí a incidentů

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Jsou přijata nezbytná opatření, která zajistí oznamování kybernetických bezpečnostních událostí u informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a o oznámeních jsou vedeny záznamy.	VKB, § 13, a)
X	X	Je připraveno prostředí pro vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních událostí detekovaných technickými nástroji podle Nástroje pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů (VKB § 21), Nástroje pro detekci kybernetických bezpečnostních událostí (VKB § 22), Nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí (VKB § 23), je prováděno jejich vyhodnocení a jsou identifikovány kybernetické bezpečnostní incidenty.	VKB, § 13, b)

KII	VIS	Povinnost	Zákon / norma
X	X	Je prováděna klasifikace kybernetických bezpečnostních incidentů, je přijímáno opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu, je prováděno hlášení kybernetického bezpečnostního incidentu podle § 32 a je zajištěn sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu.	VKB, § 13, c)
X	X	Jsou prošetřeny a určeny příčiny kybernetického bezpečnostního incidentu, je vyhodnocena účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení jsou stanovena nutná bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.	VKB, § 13, d)
X	X	Zvládání kybernetických bezpečnostních incidentů je dokumentováno.	VKB, § 13, e)

V případě kybernetických bezpečnostních událostí je třeba, aby byli uživatelé, administrátoři i jednotlivé bezpečnostní role seznámeni s pravidly a nezbytnými opatřeními hlášení a vedli záznamy oznámení. Je potřeba ověřit, zda jsou záznamy oznámení opravdu vedeny. Měl by existovat i proces hlášení, což je hierarchie postupů přes zaměstnance, který pracuje se systémem až po zaměstnance, který tyto hlášení posílá govCERT.

Při vyhodnocování, evidenci nebo řešení oznámených incidentů je potřeba mít stanovená pravidla a postupy pro vyhodnocování incidentů a mít nástroj na vyhodnocování, kategorie a typy incidentů.

U klasifikace kybernetických bezpečnostních incidentů musí být vytvořena tabulka, kde jsou uvedeny všechny možné incidenty, jejich klasifikace, opatření a úložiště podkladů pro analýzu. Tyto incidenty jsou fyzicky tříděny buď nějakým nástrojem, nebo manuálně.

Jak již bylo uvedeno, tak bezpečnostní incidenty jsou dokumentovány. Je nutné definovat, jak a kým jsou tyto záznamy zpracovávány. Analytik, který zpracovává asistované zhodnocení, proces zvládání incidentu kontroluje pomocí dokumentů se záznamy o bezpečnostních událostech a incidentech.

Dokumentace o zvládání kybernetických bezpečnostních incidentů má definované pravidla a postupy pro evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů. Také se kontroluje jak, kde a kým je dokumentováno a také kdo má k této dokumentaci přístup. Analytik kontroluje průběh procesu dokumentace.

Podle zákonu o kybernetické bezpečnosti má za úkol systém spadající do KII nebo VIS povinnost hlásit kybernetické bezpečnostní incidenty bezodkladně po jejich detekci Národnímu bezpečnostnímu úřadu.

3.1.12 Řízení kontinuity činnosti (BCM)

V oblasti řízení kontinuity činnosti jsou vedením společnosti vytvořeny postupy a prostředí, které zajišťuje kontinuitu, obnovu klíčových procesů a činností organizace na definovanou minimální úroveň. Je to vytvořeno pro případ např. výpadku napájení, požáru, přírodní katastrofy atd. Řízení kontinuity činnosti ochraňuje zájmy zainteresovaných stran (např. podílníků, akcionářů atd.) a navíc chrání dobré jméno společnosti. Norma BS 25999 stanovuje jednotný standard pro BCM (1).

Distaster recovery (DR) plán je součást metodik a procesů Business Continuity Plan nebo Incident Management. Jsou to procesy, politiky a postupy, které se týkají zajištění a obnovy provozu infrastruktury, která je pro organizaci kritická, po katastrofě (přírodní nebo zaviněná člověkem). DR je také podmnožinou BCM. Ve zkratce je DR plán příručka pro obnovení kritických aplikací po živelných pohromách nebo jiných zásadních událostech v co nejkratším čase a s minimálními výdaji a riziky (1).

Tab. 18: Oblast řízení kontinuity činnosti

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Jsou stanoveny práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role.	VKB, § 14, odst. 1 a)
X	X	Jsou stanoveny cíle řízení kontinuity činností formou určení: - minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, - doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, - doby obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu.	VKB, § 14, odst. 1 b) 1., 2., 3.
X	X	Je stanovena strategie řízení kontinuity činností, která obsahuje naplnění cílů podle písmene b).	VKB, § 14, odst. 1 c)
X		Jsou vyhodnocovány a dokumentovány možné dopady kybernetických bezpečnostních incidentů a posouzena možná rizika související s ohrožením kontinuity činností.	VKB, § 14, odst. 2 a)

KII	VIS	Povinnost	Zákon / norma
X		Jsou stanoveny, aktualizovány a pravidelně testovány plány kontinuity činností informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.	VKB, § 14, odst. 2 b)
X		Jsou realizována opatření pro zvýšení odolnosti informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickému bezpečnostnímu incidentu a je využíván Nástroj pro zajišťování úrovně dostupnosti podle Nástroj pro zajišťování úrovně dostupnosti (VKB § 26).	VKB, § 14, odst. 2 c)
X		Jsou stanoveny a aktualizovány postupy pro provedení opatření vydaných NBÚ podle § 13 a 14 ZKB, ve kterých je zohledněno: - výsledky hodnocení rizik provedení opatření, - stav dotčených bezpečnostních opatření, - vyhodnocení případných negativních dopadů na provoz a bezpečnost informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury.	VKB, § 14, odst. 2 d), 1., 2., 3.

Práva a povinnosti garantů aktiv, administrátorů a osob, které vykonávají jednotlivé bezpečnostní role, musí být stanovena v politice řízení kontinuity činností. Také o těchto právech a povinnostech musí zaměstnanci, kterých se to týká, vědět. Analytik si tuto skutečnost může zkontrolovat pomocí interních směrnic, záznamů o seznámení se s povinnostmi nebo přímo dotazu na zaměstnance.

Minimální úrovně poskytovaných služeb musí být stanoveny včetně klíčových procesů. Je potřeba také definovat, co je potřeba pro zajištění minimální úrovně poskytovaných služeb. Zohlednit je to také potřeba v SLA (Service Level Agreement) nebo OLA (Operational Level Agreement). Doba obnovení chodu musí být jasně definována a s ní, i jestli se vztahuje na celý rozsah kontrolovaného systému. Zohledněno by to mělo být opět v SLA. Pro dobu obnovení chodu se použije metrika RTO (Recovery Time Objective). Doba obnovení dat musí mít stanovený termín. Pro dobu obnovení dat se používá metrika RPO (Recovery Point Objective). Disaster recovery plan je dobré aplikovat jako součást politik ISMS.

Strategie řízení kontinuity činnosti je stanovena a musí obsahovat cíle, které jsou zmíněné v předchozím odstavci (minimální úroveň poskytovaných služeb, doba obnovení minimálního chodu a doba obnovení dat).

U vyhodnocování a dokumentování dopadů incidentů a posuzování rizika, které souvisí s ohrožením kontinuity činností, je potřeba určit, kde jsou tyto informace uvedeny, kdo je má v kompetenci a také aktuálnost dokumentu, ve kterém se tyto informace nacházejí.

Plány kontinuity musí být stanoveny (kde se nachází a pod jakým názvem), musí být aktualizovány (jak často, kdy naposledy a kdo to má v kompetenci) a testovány (jak často, kdy naposledy, s jakým výsledkem a jestli nastalo zlepšení).

3.1.13 Kontrola a audit kybernetické bezpečnosti

Při kontrole je kladen důraz na soulad s pravidly a požadavky. Tento soulad se dělí na tři skupiny:

- soulad s právními normami (předpisy související s bezpečností informací a ochranou dat, ochrana duševního vlastnictví, ochrana záznamů organizace, ochrana osobních údajů, prevence před zneužitím a kryptografická opatření),
- soulad s bezpečnostními politikami, normami a technická shoda,
- hlediska auditu IS. (1)

Tyto tři skupiny tedy podléhají třem základním kontrolám:

- Soulad dokumentace ISMS s normou ISO/IEC 27001:2014,

- Soulad skutečného fungování ISMS s dokumentací ISMS,
- Účinnost a výkonnost ISMS. (1)

Audit je proces, který probíhá systematicky, nezávisle a je dokumentovaný. Pomocí něj se získávají důkazy a hodnocení, aby se mohlo stanovit, jestli společnost splnila požadovaná kritéria. Audit kybernetické bezpečnosti se musí konat periodicky (nejméně však 1x ročně) a prověřuje připravenost IS a personál na situace, kterým by bylo možné předejít. Audit má 5 základních oblastí, kterými jsou:

- Funkcionalita IS,
- Provozní bezpečnostní politika,
- Vyhodnocování provozních statistik,
- Vzdělávání správců a uživatelů,
- Zálohování a profylaxe. (1)

Tab. 19: Oblast kontroly a auditu kybernetické bezpečnosti
(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Je posouzen soulad bezpečnostních opatření s obecně závaznými právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a VIS a určena opatření pro jeho prosazování.	VKB, § 15, odst. 1 a)
X	X	Jsou prováděny a dokumentovány pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol jsou zohledněny v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.	VKB, § 15, odst. 1 b)

KII	VIS	Povinnost	Zákon / norma
X		Je zajištěno provedení auditu kybernetické bezpečnosti osobou s odbornou kvalifikací podle § 6 odst. 6 VKB (auditor kybernetické bezpečnosti), která hodnotí správnost a účinnost zavedených bezpečnostních opatření.	VKB, § 15, odst. 2
X		Pro IS nebo KS KII je prováděna kontrola zranitelnosti technických prostředků pomocí automatizovaných nástrojů a jejich odborné vyhodnocování a je reagováno na zjištěné zranitelnosti.	VKB, § 15, odst. 3

Bezpečnostní politiky by měly obsahovat obecně závazné právní, vnitřní a jiné předpisy, smluvní závazky, které se týkají dané oblasti a společnosti. Pojem „bezpečnostní opatření jsou v souladu“ znamená, že není narušeno soukromí zaměstnanců nebo ohrožena jejich bezpečnost, je zachováno obchodní tajemství a soulad se smlouvami s dodavateli atd. Společnost musí dbát na promítnutí zákonů a vyhlášek do ISMS. Společnost stanoví, jak počítá s úpravami smluv, předpisů a zapracování procesu do směrnic. Při auditu by mělo docházet ke kontrole souladu.

Bezpečnostní politika systému řízení bezpečnosti informací jsou pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací. Dokumentace z tohoto přezkoumání je zpráva z přezkoumání systému řízení bezpečnosti informací. V této dokumentaci se řeší pravidelná školení a jejich vyhodnocování, úpravy, kontrola událostí a incidentů, které jsou způsobeny zaměstnanci. Pokud se události nebo incidenty vyskytují často, tak se mění školení nebo jsou upraveny hrozby.

Pro audit jsou stanoveny postupy a metriky. Audit je naplánovaný dopředu, jsou uvedeny práva a kompetence auditora a kdo tímto auditorem je, případně jeho role v organizaci. Následně je určeno jak, kým a kdy se hodnocení výsledků auditu zkoumá. Případně jestli jsou k tomu použity nějaké kontrolní mechanizmy.

Kontrola zranitelnosti technických prostředků se ověřuje funkcionalitou antiviru, RSS čtečky, databáze zranitelností na webu, stahování aktualizací atd. Také jaká je reakce na nalezené zranitelnosti a jak jsou hodnoceny.

3.2 Technická opatření

Druhá část zahrnuje oblasti z technických opatření. Těchto opatření je 12. Technická opatření řeší zabezpečení budov jako celku i jejich jednotlivých částí, ochranu sítě pomocí firewallu, routingu nebo segmentace sítě, systém pro tvorbu silných hesel, přístup k aplikacím a datům, princip tvorby logů, bezpečnost aplikací, kryptografické prostředky nebo ochrana v průmyslovém prostředí.

3.2.1 Fyzická bezpečnost

Oblast fyzické bezpečnosti začíná u zabezpečení společnosti jako celku (fyzický bezpečnostní perimetr, kontrola fyzického přístupu, zabezpečení prostorů a prostředků, vnější hrozby a vliv prostředí, práce v zabezpečených oblastech, veřejný přístup a prostory pro nakládku a vykládku). U zařízení se používají bezpečnostní opatření, které chrání prvky infrastruktury ICT (umístění zařízení a ochrana, podpůrná zařízení typu UPS nebo klimatizace, ochrana kabelových rozvodů, pravidelná údržba, zařízení mimo organizaci, bezpečná likvidace a přemístění majetku). Aby fyzická bezpečnost měla smysl, tak oba typy opatření by měla fungovat současně a v kombinaci (1).

Do oblasti fyzické bezpečnosti patří i smazaní dat. Tato část má 3 metody:

- mazaní dat pomocí softwarových nástrojů,
- mazání elektromagnetickým impulsem,
- fyzická likvidace (1).

Tab. 20: Oblast fyzické bezpečnosti

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Jsou přijata nezbytná opatření k zamezení neoprávněného vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.	VKB, § 16, odst. 1 a)
X	X	Jsou přijata nezbytná opatření k zamezení poškození a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.	VKB, § 16, odst. 1 b)
X	X	Je předcházeno poškození, krádeži nebo kompromitaci aktiv nebo přerušení poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.	VKB, § 16, odst. 1 c)
X		Jsou uplatněny prostředky fyzické bezpečnosti pro zajištění ochrany na úrovni objektů.	VKB, § 16, odst. 2 a)

KII	VIS	Povinnost	Zákon / norma
X		Jsou uplatněny prostředky fyzické bezpečnosti pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor, ve kterých jsou umístěna technická aktiva informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury.	VKB, § 16, odst. 2 b)

Společnost má vymezené prostory, kde je zamezený přístup. Tyto vymezené prostory musí být definovány v bezpečnostní politice fyzické bezpečnosti a musí odpovídat skutečnosti. K této oblasti musí být také vypracována analýza rizik. Z analýzy rizik vyplynou bezpečnostní opatření, která musí být popsána, zavedena, realizována a dodržena. Důležité je také ověření přístupů do vymezených prostor (kdo je má a kdo je opravdu potřebuje). Zajistit se také musí, co je potřeba k zajištění minimální úrovně poskytovaných služeb.

Opatření k zamezení poškození a zásahům, opatření pro předcházení poškození, krádeži nebo kompromitaci aktiv nebo přerušení poskytovaných služeb, opatření pro zajištění ochrany na úrovni objektů a opatření pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor s technickými aktivy musí být definována v bezpečnostní politice fyzické bezpečnosti, a také musí být uvedeno, na základě čeho jsou definována (nejčastěji analýza rizik). Následně musí tato naplánovaná opatření odpovídat reálnému stavu a musí být funkční.

3.2.2 Nástroj pro ochranu integrity komunikačních sítí

Základním nástrojem pro ochranu integrity komunikačních sítí je v první řadě správně navržená topologie sítě, což se týká i síťových prvků, které umí síť segmentovat a filtrovat provoz. Mezi tyto síťové prvky mohou patřit firewally, routery a ethernetové switche. Pro segmentaci sítě VLAN lze použít managovatelná síťová zařízení (16).

Tab. 21: Oblast nástroje pro ochranu integrity komunikačních sítí

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, je zavedeno(a): - řízení bezpečného přístupu mezi vnější a vnitřní sítí, - segmentace zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí, - použití kryptografických prostředků (Kryptografické prostředky (VKB § 25)) pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií, - opatření pro odstranění nebo blokování přenášených dat, která neodpovídají požadavkům na ochranu integrity komunikační sítě.	VKB, § 17, odst. 1 a), odst. 1 b), odst. 1 c), odst. 1 d)
X		Jsou využívány nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.	VKB, § 17, odst. 2

Řízení bezpečného přístupu mezi vnější a vnitřní sítí se dá řídit pomocí ACL (Access Control List), routingu, segmentace, firewall atd. Opatření pro odstranění nebo blokovaní přenášených dat, které neodpovídají požadavkům na ochranu integrity, mohou

být provedena pomocí zařízení IPS (Intrusion Prevention Systems), které umí sledovat, rozpoznat, zaznamenávat, blokovat a hlásit škodlivou činnost.

Nástroji pro ochranu integrity vnitřní komunikační sítě jsou VLAN, firewall, demilitarizované zóny (DMZ) atd.

3.2.3 Nástroj pro ověřování identity uživatelů

Pro nástroje pro ověřování identity uživatelů je charakteristické, že jsou konfigurovatelné a modulární, aby bylo jejich využití možné v široké nabídce systémů. Pro ověřování identity uživatelů mohou být použity nástroje RADIUS, KERBEROS nebo IEEE 802.1X. Tyto zmíněné nástroje mají za úkol donutit uživatele použít heslo, které má určitou složitost (1, 16).

Tab. 22: Oblast nástroje pro ověřování identity uživatelů
(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Jsou používány nástroje pro ověření identity uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému.	VKB, § 18, odst. 1

KII	VIS	Povinnost	Zákon / norma
X	X	Nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem, zajišťuje: - minimální délku hesla osm znaků, - minimální složitost hesla tak, že heslo bude obsahovat alespoň tři z následujících čtyř požadavků: 1. nejméně jedno velké písmeno, 2. nejméně jedno malé písmeno, 3. nejméně jednu číslici nebo 4. nejméně jeden speciální znak, který není uveden v bodech 1 až 3, - maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.	VKB, § 18, odst. 3 a), odst. 3 b), odst. 3 c)
X	X	Nástroj pro ověřování identity uživatelů je zajištěn jinými způsoby, než jaké jsou stanoveny v odstavcích 3 až 5, a orgán a osoba doložil(a), že použitá opatření zajišťují stejnou nebo vyšší úroveň odolnosti hesla.	VKB, § 18, odst. 5
X		Je používán nástroj pro ověřování identity, který: - zamezuje opětovnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin, - provádí opětovné ověření identity po určené době nečinnosti.	VKB, § 18, odst. 4 a) 1., 2.

KII	VIS	Povinnost	Zákon / norma
X		Využívá nástroj pro ověřování identity administrátorů. V případě, že tento nástroj využívá autentizaci heslem, zajistí prosazení minimální délky hesla patnáct znaků při dodržení požadavků podle odstavce 3 písm. b) a c).	VKB, § 18, odst. 4 b)

Síla hesla a prvků, které by heslo mělo obsahovat je popsáno výše v tabulce č. 22. Problematika síly hesel, zamezení opětovnému použití již používaných hesel a automatické odhlášení při nečinnosti by měli být obsaženy v některém z vnitřních dokumentů. Případně mít správě nakonfigurovaný nástroj pro řešení správy uživatelů a přístupu, který si tato pravidla vynutí. To platí i pro hesla administrátorů, kteří musí mít heslo dlouhé minimálně 15 znaků.

Více faktorová analýza by měla být dokumentována v bezpečnostní politice řízení přístupu a také by měla být zahrnuta v analýze rizik.

3.2.4 Nástroj pro řízení přístupových oprávnění

Nástroj řídí jednotlivé uživatele nebo skupiny uživatelů a kombinuje je s nástroji, která přidělují práva k adresářům, souborům nebo datům a nastavení atributů. Pro správu přístupových oprávnění je doporučen AAA protokol (16).

Tab. 23: Oblast nástroje pro řízení přístupových oprávnění

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Je používán nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění: - pro přístup k jednotlivým aplikacím a datům, - pro čtení dat, pro zápis dat a pro změnu oprávnění.	VKB, § 19, odst. 1 a), odst. 1 b)
X		Je používán nástroj pro řízení přístupových oprávnění, který zaznamenává použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik.	VKB, § 19, odst. 2

Nástroj řízení přístupových oprávnění pro přístup k jednotlivým aplikacím a datům má nastavena oprávnění uživatelů nebo rolí na úrovni aplikací a operačního systému. Dále má nastavený firewall pro řízení přístupu na základě IP adres. Nástroj pro řízení přístupových oprávnění pro čtení dat, zápis dat a pro změnu oprávnění má nastavené oprávnění na úrovní operačního systému.

Použit je i nástroj, který zaznamenává použití přístupových oprávnění. To znamená, že tento nástroj generuje logy (záznamy) o použití přístupových oprávnění. Také je potřeba definovat, kde a jak jsou tyto logy zpracovávány.

3.2.5 Nástroj pro ochranu před škodlivým kódem

Tyto nástroje by měly být nasazeny na všech zařízeních bez ohledu na to, jaký systém používají. I když je známo, že operační systémy Unixového typu nejsou tolik náchylné na napadení, tak i přesto můžou tento škodlivý kód šířit.

Je potřeba se chránit před škodlivým kódem, který může být šířen e-mailem (v poslední době častá praktika) nebo webem. V případě e-mailu je potřeba mít nástroj, který dokáže kontrolovat zprávy včetně příloh (ideálně i šifrovaných). Před škodlivým kódem

z webu je dobré použít HTTP proxy server, který používá antivir a umožňuje nastavit filtrování na základě URL adresy, klíčových slov nebo typu souboru (16).

Další ochranou může být blokování síťového provozu v datové infrastruktuře i v koncových stanicích. Provoz by měl být povolen pouze pro aplikace, které jsou legitimní. Ostatní by měly být zakázány (16).

Nástroje před škodlivým kódem by měly být nasazeny všude, tzn. od serveru přes síťový prvek až po koncovou stanici (16).

Tab. 24: Oblast nástroje pro ochranu před škodlivým kódem

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Pro řízení rizik spojených s působením škodlivého kódu je používán nástroj pro ochranu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému před škodlivým kódem, který zajistí ověření a stálou kontrolu: - komunikace mezi vnitřní sítí a vnější sítí, - serverů a sdílených datových úložišť, - pracovních stanic. Je prováděna pravidelná aktualizace nástroje pro ochranu před škodlivým kódem, jeho definic a signatur.	VKB, § 20, odst. 1 a), odst. 1 b), odst. 1 c)

Pro komunikaci mezi vnitřní a vnější sítí je nasazen firewall nebo antivir, IPS, IDS nebo sondy. Firewall nebo antivir musí být aktuální, zapnutý a aktualizovaný na všech perimetrech sítě (web, e-mail). Analytik má pak za úkol porovnat reálný stav s bezpečnostní politikou ochrany před škodlivým kódem např. jak často dochází k aktualizacím, specifikace, co je kontrolováno, pravidla aktualizace antiviru.

U serverů a sdílených datových úložišť je potřeba znát celkový počet těchto zařízení a počet serverů, na kterých je nasazen antivir. Analytik opět hledá rozdíl mezi reálným stavem a bezpečnostní politikou ochrany před škodlivým kódem a dotazuje se, jak probíhá stálá kontrola. Oblast serverů a sdílených datových úložišť (včetně procesu přidání nového serveru) je obsažena v analýze rizik.

Počet pracovních stanic a počet pracovních stanic, na kterých je nasazen antivir je opět potřeba znát, tak jako průběh stále kontroly. Určený by měl být proces přidání nové pracovní stanice a proces odpojení od vnitřní sítě. Jako nástroj pro ochranu může být použit personální firewall, host-based IPS nebo IDS.

Pravidla provádění pravidelné aktualizace antiviru musí být jasně popsána v bezpečnostní politice ochrany před škodlivým kódem včetně jeho definic a signatur. Pravidla pro jednotlivé případy jsou popsány výše. Následně se srovnávají záznamy databáze s reálným stavem (poslední aktualizace jádra, databáze antiviru, stanic, serverů…).

3.2.6 Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů

V této oblasti je důležitým předpokladem synchronizace času pro případ vyšetřování kybernetických incidentů. Dalším předpokladem je správná konfigurace systému, který tvoří logy (záznamy), tak aby byl v souladu s legislativou. Logy mohou být následně zpracovávány pomocí SIEM, IPS nebo IDS pro detekci, omezení dopadu nebo prevenci kybernetických incidentů (16).

Tab. 25: Oblast nástroje pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Je používán nástroj pro zaznamenávání činností informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, který zajišťuje: - sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti, - ochranu získaných informací před neoprávněným čtením nebo změnou.	VKB, § 21, odst. 1 a), odst. 1 b)

KII	VIS	Povinnost	Zákon / norma
X	X	Pomocí nástroje pro zaznamenávání činnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému je (jsou) zaznamenáváno(y): - přihlášení a odhlášení uživatelů a administrátorů, - činnosti provedené administrátory, - činnosti vedoucí ke změně přístupových oprávnění, - neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů, - zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, - automatická varovná nebo chybová hlášení technických aktiv, - přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností, - použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.	VKB, § 21, odst. 2 a), odst. 2 b), odst. 2 c), odst. 2 d), odst. 2 e), odst. 2 f), odst. 2 g), odst. 2 h)

KII	VIS	Povinnost	Zákon / norma
X	X	Nejméně jednou za 24 hodin je prováděna synchronizace jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.	VKB, § 21, odst. 4
X		Záznamy činností zaznamenané podle odst. 2 jsou uchovávány nejméně po dobu tří měsíců.	VKB, § 21, odst. 3

Společnost musí mít popsaný proces sběru logů. Přístup, vytváření a případně mazání logů musí mít jasně definovaná pravidla. Tyto procesy musí být opět popsané a kontroluje se, jestli je možné logy neoprávněně číst nebo měnit. Analytik chce zaznamenávání těchto procesů vidět.

V případě přihlášení a odhlášení uživatelů a administrátorů existují logy, které zaznamenávají jejich přihlášení v databázi. Analytik toto zaznamenávání kontroluje. Také kontroluje nastavení group policy jednotlivých skupin uživatelů. Jak je uvedeno v kapitole Řízení přístupu a bezpečné chování uživatelů, tak administrátor musí mít vytvořený i běžný účet pro případ, že zrovna nepotřebuje práva administrátora. Dále jsou do logů zaznamenávány změny přístupových oprávnění podle rolí, snaha uživatelů o změnu nastavení zařízení, přístupu k softwaru nebo neúspěšné snahy o přístup, zahájení a ukončení činností technických aktiv, automatická varování a hlášení o chybách technických aktiv, logy činností a pokusů o manipulaci se záznamy o činnostech, změny nástroje pro zaznamenávání činností a logy mechanismů identifikace a autentizace včetně změn údajů pro přihlášení.

V případě synchronizace jednotného systémového času pro technická aktiva musí existovat systém (ToE, WTD, GPS, polarizované pulsy, NTP…), který je nastaven tak, aby právě jednou za 24 hodin došlo k synchronizaci času. Analytik se dotazuje, jak dochází k této synchronizaci a u kterých zařízení dojde k aktualizaci času.

Je určeno po jakou dobu se mají logy uchovávat a pro toto uchovávání logů jsou nastavena pravidla.

3.2.7 Nástroj pro detekci kybernetických bezpečnostních událostí

Nasazení systému IDS je třeba nejen v rámci vnitřní komunikační sítě, ale i v rámci serverů v informačním a komunikačním systému (16).

Tab. 26: Oblast nástroje pro detekci kybernetických bezpečnostních událostí
(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případné zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.	VKB, § 22, odst. 1
X		Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí ověření, kontrolu a případně zablokování komunikace: - v rámci vnitřní komunikační sítě, - serverů patřících do informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.	VKB, § 22, odst. 2 a), odst. 2 b)

Nástrojem pro detekci kybernetických bezpečnostních událostí je myšleno zařízení IDS. Tento systém sleduje, rozpoznává, zaznamenává, blokuje a nahlašuje škodlivou činnost.

3.2.8 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Tento nástroj umožňuje monitoring, ukládání a správu bezpečnostních událostí, které jsou reprezentovány pomocí záznamů (logů). Sběr probíhá ze zařízení, která se nachází v infrastruktuře. Těmto nástrojům se může říkat také nástroje typu SIEM. Cílem

je efektivnější práce pro bezpečnostní analytiky, auditory a manažery při řízení rizik. Hlavní funkce těchto systému jsou analytické, archivační a vyhodnocovací (2).

Je dobré mít pro tento systém zpracovanou provozní příručku a také, aby byl systém navázán na řízení kontinuity činnosti (BCM) (2).

Tab. 27: Oblast nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X		Je používán nástroj pro sběr a průběžné vyhodnocování kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajišťuje: - integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury, - poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech v informačním systému kritické informační infrastruktury nebo komunikačním systému kritické informační infrastruktury, - nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí.	VKB, § 23, odst. 1 a), odst. 1 b), odst. 1 c)

KII	VIS	Povinnost	Zákon / norma
X		Je zajištěna pravidelná aktualizace nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování.	VKB, § 23, odst. 2 a)
X		Je zajištěno využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.	VKB, § 23, odst. 2 b)

Nástrojem pro sběr a průběžné vyhodnocování kybernetických bezpečnostních událostí je myšlen nástroj typu SIEM. Toto řešení musí být integrované. Musí umět posílat automatická varování a reporty pro klíčové zaměstnance (analytik, manažer kybernetické bezpečnosti, manažer ISMS, manažer CISO).

3.2.9 Aplikační bezpečnost

Aplikační bezpečnost je oblastí, na kterou spousta organizací zapomíná nebo ji řeší minimálně. Kvůli rychlému nasazování aplikací do rutinního provozu se často vyskytují bezpečnostní chyby. Aplikační bezpečnost se dá řešit buď v projektové fázi, nebo v rutinním provozu (1).

Aplikační bezpečnost v projektové fázi je mnohem efektivnější a může společnosti snížit náklady na testování nebo doplňování bezpečnosti v rutinním provozu. Všechny úrovně aplikací musí být testovány a je jedno, jak jednoduchá nebo složitá aplikace je. Je mnoho důvodů, proč je aplikační bezpečnost podceněna nebo selže (např. není chráněna firewallem, špatně použitý firewall, nepochopení šifrovací technologie, pro vývojáře je důležitější funkcionalita, vzhled atd.) (1).

V případě aplikační bezpečnosti v rutinním provozu probíhají testy a analýzy na již identifikovaných existujících zranitelnostech. Hledají se běžné i složité chyby například pomocí revize zdrojových kódů (1).

Tab. 28: Oblast aplikační bezpečnosti
(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Jsou prováděny bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.	VKB, § 24, odst. 1
X		Je zajištěna trvalá ochrana aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou.	VKB, § 24, odst. 2 a)
X		Je zajištěna trvalá ochrana transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.	VKB, § 24, odst. 2 b)

Ke každé aplikaci musí existovat dokumentace, která je označena verzí (vytváření revize dokumentace při zásahu do aplikace). Dokumentace obsahuje přehled testů, které byly provedeny, což slouží jako report výsledků. Ověřování může probíhat pomocí auditovacích a penetračních nástrojů.

V případě trvalé ochrany aplikací, informací a transakcí musí být nastaven firewall. Sleduje se chování aplikací, které je abnormální. Omezení přístupu k aplikacím a informacím je nastaveno pomocí oprávnění pro uživatele (na základě identifikace). V případě trvalé ochrany transakcí je potřeba, aby mohla být prováděna současná editace více uživateli.

3.2.10 Kryptografické prostředky

Kryptografie je část kryptologie. Zabývá se převodem srozumitelné zprávy do nesrozumitelné podoby a naopak (1).

Tab. 29: Oblast kryptografických prostředků

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	Pro používání kryptografické ochrany je (jsou) stanovena: - úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu, - pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat.	VKB, § 25, odst. 1 a) 1., 2.
X	X	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik jsou používány kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a prokázání odpovědnosti za provedené činnosti.	VKB, § 25, odst. 1 b)
X		Pro používání kryptografických prostředků je stanoven systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů.	VKB, § 25, odst. 2 a)
X		Jsou používány odolné kryptografické algoritmy a kryptografické klíče; v případě nesouladu s minimálními požadavky na kryptografické algoritmy uvedenými v příloze č. 3 k této vyhlášce řídí rizika spojená s tímto nesouladem.	VKB, § 25, odst. 2 b)

Pravidla kryptografické ochrany informací zahrnují ochranu komunikace a šifrování v mobilních zařízeních.

V případě předávání nebo ukládání dat jde o to, aby nebyly použity zranitelné protokoly a algoritmy.

Pro kryptografické prostředky systémů správy klíčů jsou použity certifikační autority.

Pokud není nalezen soulad s minimálními požadavky na kryptografické algoritmy, je potřeba rizika spojena s tímto nesouladem řídit. Společnost musí určit, kdo tento nesoulad vyhodnocuje a zda nejsou zranitelné používané autentizační mechanismy, hashe, komunikační protokoly atd.

3.2.11 Nástroj pro zajišťování úrovně dostupnosti

Předepsaná dostupnost musí být zajištěna pomocí záloh (kontrola čtení záloh) a redundance, které zajistí dostupnost náhradního aktiva v daném čase (16).

Tab. 30: Oblast nástroje pro zajišťování úrovně dostupnosti

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X	X	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik je používán nástroj pro zajišťování úrovně dostupnosti informací.	VKB, § 26, odst. 1

KII	VIS	Povinnost	Zákon / norma
X		Je používán nástroj pro zajišťování úrovně dostupnosti informací, který zajišťuje: - dostupnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury pro splnění cílů řízení kontinuity činností, - odolnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost, - zálohování důležitých technických aktiv informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury: 1. využitím redundance v návrhu řešení, 2. zajištěním náhradních technických aktiv v určeném čase.	VKB, § 26, odst. 2 a), odst. 2 b), odst. 2 c)

Potřebná úroveň dostupnosti informací je zajištěna pomocí záloh a redundance, které jsou závislé na rizicích.

3.2.12 Bezpečnost průmyslových a řídicích systémů

Průmyslová bezpečnost je velmi důležitým prvkem a je potřeba vytvořit a aplikovat maximálně kvalitní bezpečností opatření. Důležitým parametrem je práce v reálném čase. Další parametry, které jsou v této specifické oblasti zakotveny, musí splňovat odolnost proti:

- teplu,
- vlhku a vodě,
- agresivnímu prostředí,

- mechanickým vlivům,
- elektromagnetickému rušení (1).

Z toho vyplývá, že pasivní i aktivní prvky jsou pro taková prostředí upraveny. Kabely jsou zodolněné a mají speciální nebo armovaný plášť. Konektory mají odolné krytí nebo jsou speciální (např. průmyslový konektor M12). Datové rozvaděče jsou speciální nebo s DIN lištami. Aktivní prvky se vyrábí bez ventilátorů, aby se prach a nečistoty nemohly dostat dovnitř, mohou se montovat na DIN lišty, mohou být máčeny ve speciálních lacích nebo mít speciální voděodolný plášť (1).

Dalším prvkem typickým pro průmyslovou bezpečnost je redundance a to hned v několika úrovních. Redundance se provádí topologická (alternativní linka v případě poruchy), zařízení (transport dat využívá dvou nezávislých tras) a napájení (1).

Topologie v průmyslovém prostředí se vrací k sériovému zapojení a používá se napojení na jednu linku (liniové zapojení). Pokud je redundance zavedena, tak se z topologie vytvoří kruh (1).

Tab. 31: Oblast bezpečnosti průmyslových a řídicích systémů

(Zdroj: 13)

KII	VIS	Povinnost	Zákon / norma
X		Pro bezpečnost průmyslových a řídicích systémů, které jsou informačním systémem kritické informační infrastruktury nebo komunikačním systémem kritické informační infrastruktury anebo jsou jejich součástí, jsou používány nástroje, které zajišťují: - omezení fyzického přístupu k síti a zařízením průmyslových a řídicích systémů, - omezení propojení a vzdáleného přístupu k síti průmyslových a řídicích systémů, - ochranu jednotlivých technických aktiv průmyslových a řídicích systémů před využitím známých zranitelností, - obnovení chodu průmyslových a řídicích systémů po kybernetickém bezpečnostním incidentu.	VKB, § 27, a), b), c), d)

Omezení fyzického přístupu k sítí a zařízením průmyslových a řídicích systémů je podmíněno kladením důrazu na prosazování bezpečnostní politiky řízení přístupu. Běžný uživatelský provoz musí být oddělen od provozu průmyslového a řídicího (pokud je to reálné). Řídí se také přístup dodavatelů nebo jiných externích pracovníků. Jsou použity ochranné prvky proti fyzickému poškození. Případně je možné ad-hoc testování.

Omezení propojení a vzdáleného přístupu k síti průmyslových a řídicích systémů vychází z politiky bezpečného chování uživatelů, kde jsou definována omezení a možnosti pro připojení externích přenosných médií. Správně nakonfigurovány musí být také aktivní síťové prvky. Přístup je umožněn pouze definované skupině zařízení nebo uživatelů.

Ochrana jednotlivých technických aktiv průmyslových a řídicích systémů je realizována fyzickou bezpečností a to konkrétně řízením přístupu. Firmware musí být aktualizovaný buď automaticky, nebo manuálně a musí být stanovena perioda, kontrolující osoba a dohlížející osoba.

Obnovení chodu průmyslových a řídicích systémů po kybernetickém bezpečnostním incidentu je definováno pomocí DRP (Disaster Recovery Plan), který musí obsahovat všechny náležitosti (RTO, RPO atp.).

3.3 GDPR

Jak jsem uvedla v teoretických východiscích práce, tak zkratka GDPR znamená General Data Protection Regulation nebo česky Obecné nařízení o ochraně osobních údajů. V platnost toto nařízení vstoupilo 25. května 2018, ale přijato bylo již v roce 2016. GDPR musí splňovat každý subjekt, který sbírá, uchovává nebo zpracovává osobní údaje osob z EU. I GDPR využívá PDCA cyklu jako model ISMS (4).

3.3.1 Osobní údaje

Zpracování osobních údajů znamená, že s osobními údaji nebo jejich soubory byly provedeny nějaké operace (např. shromažďování, zaznamenávání, uspořádání, strukturování, uložení, přizpůsobení, pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění pomocí přenosu, šíření nebo jiné zpřístupnění, seřazení, zkombinování, omezení, výmaz nebo zničení) (10).

Osobním údajem je jakákoliv informace, která se týká jakékoliv fyzické osoby. Mezi tyto údaje patří jméno, příjmení, rodné číslo, adresa, datum narození, ale i jakékoliv další fyzické, fyziologické, genetické, ekonomické, kulturní nebo společenské prvky. Dalším prvkem identifikace může být i přidělené číslo zaměstnance nebo jeho IP adresa (10).

Tab. 32: Oblast osobních údajů

(Zdroj: Vlastní zpracování)

Povinnost	**Zákon / norma**
Osobní údaje, které jsou zpracovávané organizací, jsou identifikovány.	GDPR, čl. 32, odst. 1
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, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku (opatření dle GDPR v závislosti na rizicích).	GDPR, čl. 32, odst. 1
Při zpracování osobních údajů se využívá pseudonymizace.	GDPR, čl. 32, odst. 1
Při zpracování osobních údajů se využívá šifrování osobních údajů.	GDPR, čl. 32, odst. 1
Při zpracování osobních údajů je zajištěna neustálá důvěrnost, integrita, dostupnost a odolnost systémů a služeb zpracování.	GDPR, čl. 32, odst. 1
Při zpracování osobních údajů je zajištěna schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.	GDPR, čl. 32, odst. 1
Při zpracování osobních údajů je zajištěn proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.	GDPR, čl. 32, odst. 1
Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.	GDPR, čl. 32, odst. 2

Povinnost	**Zákon / norma**
Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.	GDPR, čl. 32, odst. 4
Jsou vedeny záznamy o všech typech zpracování osobních údajů (např. i záznamy o přístupech ke čtení).	
Je provedeno posouzení vlivu na ochranu osobních údajů.	GDPR, čl. 35
Je přiřazena role DPO (Data Protection Officer).	GDPR, čl. 37 - 39
Je uveden způsob, pomocí kterého jsou evidovány a získávány souhlasy se zpracováním osobních údajů	
Souhlasy jsou uchovávány a aktualizovány.	
Dodavatelé garantují bezpečnost zpracovávaných osobních údajů.	
Osobní údaje jsou kategorizovány a rozděleny.	
Práce s osobními daty je zaznamenávána/monitorována.	
Data z call centra jsou uchovávána.	
Souhlasy jsou udělovány v souladu s GDPR.	
Je řešena bezpečnost dat organizace u dodavatelů pomocí smluvně dodavatelského řetězce.	
Nakládání s osobními daty zákazníků je dokumentováno.	
Vlastní databáze dat je uložena v CPE nebo v jiné databázi.	
Záloha dat je prováděna na více než 2 samostatné zálohy.	
Jsou vedeny záznamy o hromadném zpracování dat.	
Na základě písemného souhlasu k nakládání s osobními údaji jsou rozesílány marketingové letáky, upozornění a marketingové newslettery.	
Organizace disponuje marketingovými bázemi i vlastními.	

Povinnost	**Zákon / norma**
Osobní údaje jsou v databázi zákazníků a je vykonávána správa dle smluvních ujednání.	
Je stanovena role správce dat s popisem této role.	
Je stanovena role příjemce dat s popisem této role.	
Je stanovena role zpracovatele dat s popisem této role.	
Jsou zpracovávána osobní data a jsou ve vlastním systému organizace, který má přijata bezpečnostní opatření.	
Jsou evidovány osobní údaje pouze a výhradně ve vlastním systému společnosti.	
Jsou plněna zavedená pravidelná školení pro práci s osobními daty.	
Dokumentace k osobním datům je řešena pomocí zavedení ISMS nebo jiné směrnice.	
Je prováděn bezpečnostní audit IS, kde jsou obsažena osobní data.	
Jsou testována bezpečnostní opatření a jsou kontrolováni partneři a jejich způsob práce s osobními daty.	
Jsou k dispozici havarijní plány v případě porušení ochrany osobních údajů.	
Údaje o nákupech a využívaných službách jsou evidovány nebo jsou evidována data zákaznická a společnost je v roli zpracovatele osobních údajů (údaj o nákupu je osobním údajem). Oblast je řešena dokumentačně a z pohledu bezpečnosti osobních údajů.	
Jsou shromažďována data o IP adresách.	
Data jsou referencována s referencemi na konkrétní profily. Společnost také stanoví, kde jsou dodací nebo platební údaje zákazníka uloženy.	
Jsou prováděny pravidelné bezpečnostní audity IS a s nimi provázaná data.	

Povinnost	Zákon / norma
Data ve vlastních IS jsou bezpečně zpracovávána a uchovávána.	
Je zpracována kompletní přijímací dokumentace.	
Pokud společnost disponuje „papírovými osobními údaji“ je k těmto nestrojovým osobním údajům přistupováno podobně jako k těm strojovým osobním údajům.	

DPO (Data Protection Officer) musí být jmenován, pokud jsou údaje zpracovávány orgánem veřejné moci nebo je orgán veřejný subjekt, správce nebo zpracovatel provádí rozsáhlé pravidelné a systematické monitorování subjektů údajů (sledování a profilování na internetu), správce nebo zpracovatel provádí rozsáhlé zpracování zvláštní kategorie údajů (rasový nebo etnický původ, politické názory, náboženské nebo filosofické přesvědčení, odborovou příslušnost, zpracovávají genetická nebo biometrická data, údaje o zdraví, pohlavím životě nebo orientaci osoby) nebo zpracovávají údaje, které se týkají rozsudků v trestních věcech nebo trestních činů.

3.3.2 Osobní údaje - kodexy chování

Tato část GDPR se zaměřuje na tvorbu a implementaci kodexů chování od zpracovatelských subjektů. Tyto kodexy upravují způsoby zálohování a ukládání záloh, dostupné formáty a nosiče, IT konfiguraci a minimální přenosovou rychlost sítě, dobu k zahájení procesu a dobu, kdy jsou data k dispozici pro přenos, záruky v případě přístupu k údajům v případě, že dojde k úpadku poskytovatele služeb. Důležité je, aby tyto kodexy byly vytvořeny se všemi zainteresovanými stranami (uživatelé, poskytovatelé cloudových služeb, sdružení všech typů velikostí podniků) (17).

Tyto kodexy jsou následně využívány správci a poskytují jim podpůrný materiál správné praxe zpracování osobních údajů (10).

Tab. 33: Oblast osobních údajů – kodexy chování

(Zdroj: Vlastní zpracování)

Povinnost	Zákon / norma
Jsou zpracovány kodexy chování v souvislosti se zpracováním osobních údajů.	GDPR, čl. 40
Jsou dodržovány schválené kodexy chování.	GDPR, čl. 32, odst. 3
Je vydáno osvědčení podle čl. 40 GDPR.	GDPR, čl. 40, čl. 42

Kodexy chování jsou vypracovány, příp. upravovány nebo rozšiřovány pokud jde o:

- spravedlivé a transparentní zpracování,
- oprávněné zájmy (v konkrétních situacích sledováno správci),
- shromažďují osobní údaje,
- pseudonymizaci osobních údajů,
- informace poskytované veřejnosti a subjektům údajů,
- výkon práv subjektů údajů,
- informace, které jsou poskytovány dětem, jejich ochranu a způsob získávání souhlasu zákonného zástupce,
- opatření a postupy, které jsou uvedeny v článcích 24 a 25 a opatření k zajištění bezpečnosti v článku 32,
- ohlašování případů porušení zabezpečení osobních údajů dozorovým úřadům a subjektům údajů,
- předávání osobních údajů do třetích zemí nebo mezinárodním organizacím,
- mimosoudní vyrovnání a jiné postupy pro řešení sporů mezi správci a subjekty údajů v souvislosti se zpracováním tak, aby nebyla dotčena práva subjektů údajů v článcích 77 a 79.

3.3.3 Osobní údaje – závazná podniková pravidla

Jedná se o koncepci ochrany osobních údajů, která je dodržována správcem nebo zpracovatelem osobních údajů v případě, že předává osobní údaje (i jednorázově) jinému správci nebo zpracovateli v jiné zemi v rámci skupiny podniků nebo podniků, které mají stejnou hospodářskou činnost (10).

Tab. 34: Oblast osobních údajů – závazná podniková pravidla

(Zdroj: Vlastní zpracování)

Povinnost	**Zákon / norma**
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - strukturu a kontaktní údaje skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a každého z jejích členů, - předání údajů nebo soubor předání, včetně kategorií osobních údajů, typu zpracování a jeho účelů, typu dotčených subjektů údajů a určení dané třetí země nebo daných třetích zemí, - svoji právně závaznou povahu, a to interně i externě.	GDPR, čl. 47, odst. 2 a)
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - použití obecných zásad pro ochranu údajů, zejména účelové omezení, minimalizaci údajů, omezenou dobu uložení, kvalitu údajů, záměrná a standardní ochranu osobních údajů, právní základ pro zpracování, zpracování zvláštních kategorií osobních údajů, - opatření k zajištění zabezpečení údajů a požadavky ohledně dalšího předávání subjektům, které podnikovými pravidly nejsou vázány.	GDPR, čl. 47, odst. 2 d)

Povinnost	**Zákon / norma**
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - práva subjektů údajů v souvislosti se zpracováním jejich osobních údajů a prostředky jejich výkonu, včetně práva nebýt předmětem rozhodnutí založených výhradně na automatizovaném zpracování, včetně profilování, práva podat stížnost u příslušného dozorového úřadu, právní ochrany a případně i práva na odškodnění v případě porušení závazných podnikových pravidel.	GDPR, čl. 47, odst. 2 e)
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - přijetí odpovědnosti správcem nebo zpracovatelem usazeným na území některého členského státu za jakékoli porušení závazných podnikových pravidel kterýmkoli dotčeným členem neusazeným v Unii, - správce nebo zpracovatel se může této odpovědnosti zcela nebo zčásti zprostit, pouze pokud prokáže, že za okolnost, jež vedla ke vzniku škody, není daný člen odpovědný.	GDPR, čl. 47, odst. 2 f)
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - způsob poskytování informací o závazných podnikových pravidlech, zejména o ustanoveních uvedených v písmenech d), e) a f) tohoto odstavce, subjektům údajů, vedle informací uvedených v článcích 13 a 14.	GDPR, čl. 47, odst. 2 g)

Povinnost	**Zákon / norma**
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - úkoly všech pověřenců pro ochranu osobních údajů jmenovaných v souladu s článkem 37, nebo jakékoli jiné osoby či subjektu pověřeného monitorováním souladu se závaznými podnikovými pravidly v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a sledování školení a vyřizování stížností.	GDPR, čl. 47, odst. 2 h)
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - postupy pro vyřizování stížností.	GDPR, čl. 47, odst. 2 i)
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - mechanismy, které mají v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost zajistit ověřování souladu se závaznými podnikovými pravidly. Tyto mechanismy zahrnují audity ochrany údajů a metody zajištění opravných opatření pro ochranu práv subjektu údajů. Výsledky takového ověření by měly být oznámeny osobě nebo subjektu uvedenému v písmenu h) a radě řídícího podniku skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a na požádání by měly být zpřístupněny příslušnému dozorovému úřadu.	GDPR, čl. 47, odst. 2 j)

Povinnost	**Zákon / norma**
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - mechanismy pro podávání zpráv a pro zaznamenávání změn pravidel a hlášení těchto změn dozorovému úřadu.	GDPR, čl. 47, odst. 2 k)
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - strukturu a kontaktní údaje skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a každého z jejích členů, - mechanismus spolupráce s dozorovým úřadem, který zajistí dodržování pravidel každým členem skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost, zejména zpřístupňování výsledků ověřování opatření uvedených v písmenu j) dozorovému úřadu.	GDPR, čl. 47, odst. 2 l)
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - mechanismy pro podávání zpráv příslušnému dozorovému úřadu o právních požadavcích, kterým je člen skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost podřízen ve třetí zemi a které mohou mít podstatný negativní účinek na záruky poskytované závaznými podnikovými pravidly.	GDPR, čl. 47, odst. 2 m)
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - vhodnou odbornou přípravu v oblasti ochrany údajů pro pracovníky, kteří mají k osobním údajům trvalý nebo pravidelný přístup.	GDPR, čl. 47, odst. 2 n)

3.3.4 Osobní údaje – záznamy o činnostech zpracování

Tyto záznamy jsou vedeny především pro kontrolu, jestli je správně nakládáno a manipulováno s osobními údaji. Obsahují základní informace o zpracování, které bylo prováděno. Záznamy o činnostech zpracování ulehčují správcům orientaci ve zpracováních, které dělají (10).

Tab. 35: Oblast osobních údajů – záznamy o činnostech zpracování
(Zdroj: Vlastní zpracování)

Povinnost	**Zákon / norma**
Vedeny záznamy o činnostech zpracování OÚ: - jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů, - účely zpracování, - popis kategorií subjektů údajů a kategorií osobních údajů, - kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích.	GDPR, čl. 30
Vedeny záznamy o činnostech zpracování OÚ: - informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk.	GDPR, čl. 30
Vedeny záznamy o činnostech zpracování OÚ: - je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů, - je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.	GDPR, čl. 30

Povinnost	Zákon / norma
Vedeny záznamy o všech kategoriích činností zpracování prováděných pro správce, jež obsahují: - jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů, - kategorie zpracování prováděného pro každého ze správců, - informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk, - je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.	GDPR, čl. 30

Povinnosti, které jsou uvedeny ve článku 30 v odstavcích 1 a 2 se netýkají společnosti, která zaměstnává méně než 250 osob. Je to ovšem pouze pod podmínkou, že společnost nezpracovává údaje tak, že by nastalo riziko v narušení práv a svobod subjektů údajů, zpracování by nebylo jen příležitostné nebo by společnost zpracovávala speciální kategorie údajů, které jsou uvedeny v článku 9 odst. 1 nebo by se osobní údaje týkaly trestních rozsudků a trestných činů podle článku 10.

3.3.5 Osobní údaje – posouzení vlivu na ochranu osobních údajů

Posouzení se provádí v případě, kdy by mohlo nastat vysoké riziko pro narušení práv a svobod fyzických osob (např. v případě použití nových technologií). Posouzení musí být provedeno před zpracováním dat. Správce si vyžádá od DPO posudek, pokud je tato osoba stanovena. Posouzení vlivu na ochranu osobních údajů se požaduje:

- při systematickém a rozsáhlém vyhodnocování osobních údajů fyzických osob (u automatického zpracování a profilování),
- při rozsáhlém zpracování kategorií údajů nebo rozsudků v trestních věcech,
- při rozsáhlém systematickém monitorování veřejně přístupných prostor (10).

Tab. 36: Oblast osobních údajů – posouzení vlivu na ochranu osobních údajů

(Zdroj: Vlastní zpracování)

Povinnost	**Zákon / norma**
Ve společnosti probíhá automatické zpracování dat a profilování zákazníků (systematické a rozsáhlé zpracování dat).	
Společnost pracuje se zvláštními kategoriemi údajů (rasové, etnické, trestní, registry dlužníků apod.).	
Je prověřována platební schopnost klientů.	
Jsou vytvářeny marketingové profily zákazníků (např. dle jejich lokace).	
Zpracovávání údajů probíhá na základě automatizovaného rozhodování (může vést k diskriminaci některého ze zákazníků).	
Je monitorováno adresné chování zákazníků.	
Jsou zpracovávány lokalizační nebo platební údaje (i historické), které mohou být zneužity.	
Jsou zpracovávány rozsáhlé údaje (např. z důvodu cílení reklamy v e-shopech).	
Jsou zpracovávány nebo evidovány údaje dle územního rozsahu.	
Jsou zpracovávány údaje z propojených či kombinovaných souborů nebo databází, které obsahují osobní údaje a původem je více zdrojů (zpracování nad rámec původního účelu).	
Jsou zpracovávána data o zaměstnancích, zdravotně postižených nebo nezletilých.	

Povinnost	Zákon / norma
Je interně zaveden otisk prstu pro vstup na pracoviště.	
Data jsou předávána mimo EU.	
Data včetně osobních dat jsou přeshraničně předávána.	
Probíhá prověření zákazníků, kde se zákazník nemůže vyhnout nakládání s jeho daty (např. prověřování platební schopnosti či jeho ověření platební karty či totožnosti).	
Je stanoveno po jakou dobu jsou uchovávána data z call centra (z hovorů).	
Je stanoveno, kde probíhá zálohování a archivace dat z call centra.	
Společnost disponuje kapacitami a plánem na zpracování procesu a technologických opatření, která vyplývají z tvorby dokumentace doporučení DPIA.	
Společnost disponuje přesným popisem procesů, kterým se jako správce musí prokazovat vůči ÚOOÚ.	

3.3.6 Osobní údaje – právo na přenositelnost údajů

Právo na přenositelnost údajů je nové a díky němu je možné osobní údaje za určitých podmínek od správce získat ve strukturovaném a strojově čitelném formátu nebo požádat o poskytnutí jinému správci. Aby mohlo být uplatněno právo na přenositelnost, musí splňovat tyto podmínky:

- zpracování založené na právním důvodu, souhlasu či smlouvě,
- automatizované zpracování (10).

Tab. 37: Oblast osobních údajů – právo na přenositelnost údajů

(Zdroj: Vlastní zpracování)

Povinnost	Zákon / norma
Jsou rozlišovány kategorie dat (data aktivní a vědomě poskytnutá vs. data poskytnutá zákazníkem na základě využití služby).	

3.4 Ekonomické zhodnocení a přínos práce

V návrhové části jsem vytvořila metodiku asistovaného zhodnocení. V poslední části návrhu je potřeba vyčíslit předpokládanou cenu za vytvoření metodiky asistovaného zhodnocení a stanovit přínosy metodiky asistovaného zhodnocení.

Práce na asistovaném zhodnocení je vyčíslena pomocí hodinové sazby. Hodinovou sazbu jsem si stanovila na 1 000 Kč/hod. Na návrhu metodiky asistovaného zhodnocení jsem strávila 60 hodin, takže výsledná cena práce na asistovaném zhodnocení je 60 000 Kč. Další náklady, které se týkají provedení asistovaného zhodnocení, záleží na velikosti společnosti, oblasti podnikaní, jakou kybernetickou a informační bezpečnost již mají implementovanou, na rozpočtu společnosti a dalších faktorech. Cena se může pohybovat od 50 000 Kč až do 250 000 Kč. Částky jsou to opravdu vysoké, hlavně pro malé společnosti. Společnosti by se měly hlavně zamyslet nad tím, kolik by je stálo narušení dostupnosti, integrity a důvěrnosti dat způsobené kybernetickým incidentem nebo nesoulad se zákonem o kybernetické bezpečnosti, vyhláškou o kybernetické bezpečnosti nebo směrnicí NIS.

Hlavní přínos vidím ve vyvarování se sankcím, které hrozí v případě nesplnění zákona o kybernetické bezpečnosti, vyhlášky o kybernetické bezpečnosti nebo směrnice NIS. Například v případě, že je porušeno nebo nezavedeno nařízení GDPR jsou stanoveny sankce až 20 000 000 € nebo až 4% z celosvětového obratu daného odvětví. V případě subjektů KII a VIS, které nebudou vést dokumentaci, nebudou provádět nebo zavádět bezpečnostní opatření, neohlásí kybernetický incident, nesplní povinnosti Úřadu nebo nesplní povinnost uloženou nápravným opařením, mohou sankce dosahovat až 100 000 Kč. V případě neohlášení kontaktních údajů nebo jejich změny je stanovena sankce od 10 000 Kč.

Dalším přínosem je, pokud společnost splní všechny povinnosti z asistovaného zhodnocení a dostane se do souladu se zákonem o kybernetické bezpečnosti, vyhláškou o kybernetické bezpečnosti a směrnicí NIS. V tomto případě společnost ušetří náklady na auditní činnost, která probíhá formou služby. Tato služba poskytne společnosti zpětnou vazbu o stavu kybernetické a informační bezpečnosti, a jestli jsou výsledky v souladu. Cena se opět odvíjí od mnoha faktorů (velikost společnosti, odvětví...) a může se vyšplhat až na 500 000 Kč.

ZÁVĚR

Kybernetická i informační bezpečnost jsou a ještě budou důležitým tématem, protože války a útoky již neprobíhají pouze na zemi, ale právě i v kyberprostoru. Je potřeba v tomto ohledu vzdělávat nejen dospělé a zaměstnance, ale již děti od útlého věku. Zabezpečení organizace se stává čím dál více diskutovaným a aktuálním. Více připojených zařízení do Internetu znamená i více cílů pro potencionální útočníky.

Vlastní návrh je potřeba opřít o základní teoretické pojmy, aktuální legislativu, která dává striktní členění celému asistovanému zhodnocení a normy ISO/IEC řady 27 000. Tato řada norem řeší problematiku bezpečnosti informací. Důležité je uvést i instituce v České republice, které se stejnou problematikou zabývají. Dalšími základními pojmy vyskytujícími se v rámci asistovaného zhodnocení jsou GDPR, systém řízení bezpečnosti informací, analýza rizik a řízení rizik, autentizační protokol IEEE 802.1X, audit kybernetické bezpečnosti a certifikace nebo log management. Asistované zhodnocení není moc rozšířený pojem, takže jsem do teorie zavedla i stručné vysvětlení.

V analýze jsem se zaměřila na rozčlenění na organizační, technická opatření a GDPR. Tyto opatření se dále dělí na oblasti. Zaměřím se také na to, jak byla metodika tvořena, jaká je struktura tabulek. Uvedla jsem také stupnici variant hodnocení zavedení opatření a pomocí statistického výstupu jsem analyzovala aktuální stav zavedení opatření na vzorku 34 společností.

Návrh je rozdělen na 3 kapitoly, které řeší organizační opatření, technická opatření nebo GDPR. Tyto kapitoly jsou ještě dále děleny na podkapitoly, které označují jednotlivé oblasti asistovaného zhodnocení. Každá z oblastí je stručně teoreticky popsána. Následuje tabulka uvádějící, který ze subjektů musí splňovat jednotlivé povinnosti a pod tabulkou je popis povinností.

Cíl práce, který je uveden v zadání, byl splněn. Vytvořila jsem jednotnou metodiku pro zpracování asistovaných zhodnocení, která bude sloužit jako prostředek pro zjištění stavu kybernetické a informační bezpečnosti ve společnostech. Navíc se mi podařilo rozšířit zadání o stále aktuální problematiku GDPR. Doufám, že můj návrh bude sloužit jako podpůrný materiál při zpracování asistovaných zhodnocení ve společnostech.

SEZNAM POUŽITÝCH ZDROJŮ

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

(2) SEDLÁK, P. *Management informační bezpečnosti*. [přednáška]. Brno: VUT, Fakulta podnikatelská, 2018.

(3) Aktuální legislativa. *Národní centrum kybernetické bezpečnosti* [online]. [cit. 2019-04-15]. Dostupné z: https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/

(4) SEDLÁK, P. *Oborové managementy bezpečnosti IS.* [přednáška]. Brno: VUT, Fakulta podnikatelská, 2018.

(5) O nás. *Národní bezpečnostní úřad* [online]. [cit. 2019-04-18]. Dostupné z: https://www.nbu.cz/cs/o-nas/955-o-nas/

(6) O týmu CSIRT. *CSIRT* [online]. [cit. 2019-04-18]. Dostupné z: https://www.csirt.cz/page/3471/o-tymu-csirtcz/

(7) O úřadu. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2019-04-18]. Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu/

(8) Řada norem ISO/IEC 27 000. *Risk Analysis Consultants* [online]. © 2019 [cit. 2019-04-15]. Dostupné z: http://www.iso27000.cz/

(9) Bezpečnost. *Platforma kybernetické bezpečnosti* [online]. [cit. 2019-04-15]. Dostupné z: https://www.kybez.cz/

(10) Základní příručka k GDPR. *Úřad pro ochranu osobních údajů* [online]. © 2013 [cit. 2019-04-02]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=1&p1=3506

(11) ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky*. Praha: Český normalizační institut, 2014.

(12) Desatero úspěšného řízení rizik. *T-SOFT.cz* [online]. © 2017 [cit. 2019-04-18]. Dostupné z: http://www.tsoft.cz/desatero-uspesneho-rizeni/

(13) Pomůcka k auditu bezpečnostních opatření podle zákona o kybernetické bezpečnosti. *Národní centrum kybernetické bezpečnosti* [online]. © 2018 [cit. 2019-03-18]. Dostupné také z: https://www.govcert.cz/download/kii-vis/container-nodeid-580/vkbchecklistfinalv21rev.pdf

(14) HRUBEŠOVÁ, Gabriela. *Statistický výstup z asistovaných zhodnocení*. Brno, 2019. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/119720. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

(15) Požadavky na smlouvy s dodavateli. *Národní centrum kybernetické bezpečnosti* [online]. © 2018 [cit. 2019-03-18]. Dostupné také z: https://www.govcert.cz/download/kii-vis/Vyklad_pozadavku_na_smlouvy_s_dodavateli_v1.0.pdf

(16) KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje* [online]. [cit. 2019-03-23]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

(17) SEDLÁK, P. *Technologická bezpečnost ICT*. [přednáška]. Brno: VUT, Fakulta podnikatelská, 2019.

(18) ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů*. Praha: Český normalizační institut, 2014.

(19) Zákon č. 205/2017 Sb., zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony ze dne 7. června 2017.

(20) Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat ze dne 21. května 2018.

SEZNAM POUŽITÝCH ZKRATEK

ACL	Access Control List
AM	Access Management
ANSI	American National Standards Institute
BCM	Business Continuity Management
BSI	British Standard Institute
BYOD	Bring Your Own Device
CEN	Comité Européen Normalisation
CENELEC	Comité Européen de Normalisation Eléctrotechnique
CERT	Computer Emergency Response Team
CIA	Confidentiality - Integrity - Availability
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
ČSNI	Český Normalizační Institut
DMZ	Demilitarized Zone
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DR	Disaster Recovery
DRP	Disaster Recovery Plan
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GUI	Graphical User Interface

HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technologies
IdM	Identity Management
IDS	Intrusion Detection System
IEC	International Electrotechnical Comission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IS	Information System
ISMS	Information Security Management System
ISO	Internetional Organization for Standardization
IT	Information Technologies
ITU	International Telecommunications Union
KII	Kritická Infromační Infrastruktura
KS	Komunikační Systém
NBÚ	Národní Bezpečnostní Úřad
NCKB	Národní Centrum Kybernetické Bezpečnosti
NDA	Non-Disclosure Agreement
NIST	National Institute for Standards and Technology
NTP	Network Time Protocol
NÚKIB	Národní Úřad pro Kybernetickou a Informační Bezpečnost
OLA	Operational Level Agreement

OÚ	Osobní Údaje
PDS	Poskytovatelé Digitálních Služeb
PTP	Precision Time Protocol
PZS	Provozovatelé Základních Služeb
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RTP	Risk Treatment Plan
SAE	Secutity Awareness and Education
SIEM	Security Information and Event Management
SIMS	Security Incident Management System
SLA	Service Level Agreement
SoA	Statement of Applicability
TCP	Transmission Control Protocol
ToE	Time over Ethernet
UPS	Uninterruptible Power Supply
VIS	Významný Informační Systém
VKB	Vyhláška o Kybernetické Bezpečnosti
VLAN	Virtual LAN
WTD	Wireless Time Distribution
ZKB	Zákon o Kybernetické Bezpečnosti

SEZNAM GRAFŮ

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha č. 1: Kompletní podoba asistovaného zhodnocení

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Systém řízení bezpečnosti informací				
X		Je stanoven rozsah ISMS.	VKB, § 3, odst. 1 a)	
X	X	Je zaveden proces řízení rizik.	VKB, § 3, odst. 1 b), odst. 2 a)	
X	X	Jsou vytvořeny, schváleny a zavedeny bezpečnostní politiky v oblasti ISMS a také jsou zavedena příslušná bezpečnostní opatření.	VKB, § 3, odst. 1 c), odst. 2 b)	
X		Jsou zavedeny procesy: - monitorování účinnosti bezpečnostních opatření,	VKB, § 3, odst. 1 d), odst. 1 e), odst. 1 g)	
		- vyhodnocování vhodnosti a účinnosti bezpečnostní politiky,		
		- vyhodnocení účinnosti ISMS.		
X		Audit kybernetické bezpečnosti je proveden minimálně 1x ročně.	VKB, § 3, odst. 1 f)	
X		Aktualizace ISMS a související dokumentace je prováděna na základě zjištění auditů / penetračních testů.	VKB, § 3, odst. 1 h)	
X		Je řízen provoz a zdroje ISMS, zaznamenávají se činnosti spojené s ISMS a se souvisejícím řízení rizik.	VKB, § 3, odst. 1 i)	
	X	Nejméně 1x za 3 roky je provedena aktualizace zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí.	VKB, § 3, odst. 2 c)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Řízení rizik				
X	X	Jsou stanoveny metodiky pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik.	VKB, § 4, odst. 1 a), odst. 2 a)	
X	X	Je prováděna identifikace a hodnocení důležitosti aktiv, která patří do rozsahu ISMS, podle § 8 (Řízení aktiv) minimálně v rozsahu přílohy č. 1 k VKB a výstupy jsou zapracovány do zprávy o hodnocení aktiv a rizik.	VKB, § 4, odst. 1 b), odst. 2 b)	
X	X	Je prováděna identifikace rizik, při kterých jsou zohledňovány hrozby a zranitelnosti, jsou posuzovány možné dopady na aktiva. Tato rizika jsou hodnocena minimálně v rozsahu podle přílohy č. 2 k VKB. Jsou určena a schválena přijatelná rizika a je zpracována zpráva o hodnocení aktiv a rizik.	VKB, § 4, odst. 1 c), odst. 2 c)	
X	X	Na základě bezpečnostních potřeb a výsledků hodnocení rizik je zpracováváno prohlášení o aplikovatelnosti (SoA).	VKB, § 4, odst. 1 d), odst. 2 d)	
X	X	Je zpracovaný a zavedený plán zvládání rizik (RTP), který obsahuje cíle a přínosy bezpečnostních opatření. Je určena osoba odpovědná za prosazování bezpečnostních opatření. Jsou určeny potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními.	VKB, § 4, odst. 1 e), odst. 2 e)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X	X	Bez zbytečného odkladu jsou zohledňována reaktivní a ochranná opatření vydaná NBÚ v hodnocení rizik a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, jsou doplněny plány zvládání rizik.	VKB, § 4, odst. 1 f), odst. 2 f)	
X	X	Řízení rizik je zajištěno jinými způsoby (než jak je stanoveno v odstavci 1 a 2) a orgán a osoba doložil(a), že použitá opatření zajišťují stejnou nebo vyšší úroveň řízení rizik.	VKB, § 4, odst. 3	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X	X	Při hodnocení rizik jsou zváženy hrozby, související s: - porušením bezpečnostní politiky, provedením neoprávněných činností,	VKB, § 4, odst. 4 a), odst. 4 b), odst. 4 c), odst. 4 d), odst. 4 e), odst. 4 f), odst. 4 g), odst. 4 h), odst. 4 i), odst. 4 j), odst. 4 k), odst. 4 l)	
		- zneužitím oprávnění ze strany uživatelů a administrátorů,		
		- poškozením nebo selháním technického anebo programového vybavení,		
		- zneužitím identity fyzické osoby,		
		- užíváním programového vybavení v rozporu s licenčními podmínkami,		
		- kybernetickým útokem z komunikační sítě,		
		- škodlivým kódem (například viry, spyware, trojské koně),		
		- nedostatky při poskytování služeb IS/KS KII nebo VIS,		
		- narušením fyzické bezpečnosti,		
		- přerušením poskytování služeb elektronických komunikací nebo dodávek elektrické energie,		
		- zneužitím nebo neoprávněnou modifikací údajů,		
		- trvale působícími hrozbami,		
		- s odcizením nebo poškozením aktiva.		

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X		Při hodnocení rizik jsou zváženy hrozby, související s: - porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany administrátorů KII,	VKB, § 4, odst. 6 a), odst. 6 b), odst. 6 c), odst. 6 d), odst. 6 e), odst. 6 f), odst. 6 g)	
		- pochybením ze strany zaměstnanců,		
		- zneužitím vnitřních prostředků, sabotáží,		
		- dlouhodobým přerušením poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,		
		- nedostatkem zaměstnanců s potřebnou odbornou úrovní,		
		- cíleným kybernetickým útokem pomocí sociálního inženýrství, použitím špionážních technik,		
		- zneužitím vyměnitelných technických nosičů dat.		

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X	X	Zváženy zranitelnosti, související s: - nedostatečnou ochranou vnějšího perimetru,	VKB, § 4, odst. 5 a), odst. 5 b), odst. 5 c), odst. 5 d), odst. 5 e), odst. 5 f), odst. 5 g)	
		- nedostatečným bezpečnostním povědomí uživatelů a administrátorů,		
		- nedostatečnou údržbou IS/KS KII nebo VIS,		
		- nevhodným nastavením přístupových oprávnění,		
		- nedostatečnými postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,		
		- nedostatečným monitorováním činností uživatelů a administrátorů a neschopností odhalit jejich nevhodné nebo závadné způsoby chování,		
		- s nedostatečným stanovením bezpečnostních pravidel, nepřesným nebo nejednoznačným vymezením práv a povinností uživatelů, administrátorů a bezpečnostních rolí.		
X		Zváženy zranitelnosti, související s: - nedostatečnou ochranou ICT,	VKB, § 4, odst. 7 a), odst. 7 b), odst. 7 c), odst. 7 d)	
		- nevhodnou bezpečnostní architekturou,		
		- nedostatečnou mírou nezávislé kontroly,		
		- neschopností včasného odhalení pochybení ze strany zaměstnanců.		

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Bezpečnostní politika				
X	X	Je stanovena bezpečnostní politika v oblasti systému řízení bezpečnosti informací.	VKB, § 5, odst. 1 a), odst. 2 a)	
X	X	Je stanovena bezpečnostní politika v oblasti organizační bezpečnosti	VKB, § 5, odst. 1 b), odst. 2 b)	
X		Je stanovena bezpečnostní politika v oblasti řízení vztahů s dodavateli.	VKB, § 5, odst. 1 c)	
	X	Je stanovena bezpečnostní politika v oblasti řízení dodavatelů.	VKB, § 5, odst. 2 c)	
X	X	Je stanovena bezpečnostní politika v oblasti klasifikace aktiv.	VKB, § 5, odst. 1 d), odst. 2 d)	
X	X	Je stanovena bezpečnostní politika v oblasti bezpečnosti lidských zdrojů.	VKB, § 5, odst. 1 e), odst. 2 e)	
X	X	Je stanovena bezpečnostní politika v oblasti řízení provozu a komunikací.	VKB, § 5, odst. 1 f), odst. 2 f)	
X	X	Je stanovena bezpečnostní politika v oblasti řízení přístupu.	VKB, § 5, odst. 1 g), odst. 2 g)	
X	X	Je stanovena bezpečnostní politika v oblasti bezpečného chování uživatelů.	VKB, § 5, odst. 1 h), odst. 2 h)	
X	X	Je stanovena bezpečnostní politika v oblasti zálohování a obnovy.	VKB, § 5, odst. 1 i), odst. 2 i)	
X		Je stanovena bezpečnostní politika v oblasti bezpečného předávání a výměny informací.	VKB, § 5, odst. 1 j)	
X		Je stanovena bezpečnostní politika v oblasti řízení technických zranitelností.	VKB, § 5, odst. 1 k)	
X		Je stanovena bezpečnostní politika v oblasti bezpečného používání mobilních zařízení.	VKB, § 5, odst. 1 l)	
X	X	Je stanovena bezpečnostní politika v oblasti poskytování a nabývání licencí programového vybavení a informací.	VKB, § 5, odst. 1 m), odst. 2 j)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X		Je stanovena bezpečnostní politika v oblasti dlouhodobého ukládání a archivace informací.	VKB, § 5, odst. 1 n)	
X	X	Je stanovena bezpečnostní politika v oblasti ochrany osobních údajů.	VKB, § 5, odst. 1 o), odst. 2 k)	
X		Je stanovena bezpečnostní politika v oblasti fyzické bezpečnosti.	VKB, § 5, odst. 1 p)	
X		Je stanovena bezpečnostní politika v oblasti bezpečnosti komunikační sítě.	VKB, § 5, odst. 1 q)	
X	X	Je stanovena bezpečnostní politika v oblasti ochrany před škodlivým kódem.	VKB, § 5, odst. 1 r), odst. 2 m)	
X	X	Je stanovena bezpečnostní politika v oblasti nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.	VKB, § 5, odst. 1 s), odst. 2 n)	
X		Je stanovena bezpečnostní politika v oblasti využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.	VKB, § 5, odst. 1 t)	
X	X	Je stanovena bezpečnostní politika v oblasti používání kryptografické ochrany.	VKB, § 5, odst. 1 u), odst. 2 l)	
X	X	Je pravidelně hodnocena účinnost bezpečnostní politiky. Bezpečnostní politika je pravidelně aktualizována.	VKB, § 5, odst. 3	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Organizační bezpečnost				
X	X	Je zavedena organizační bezpečnost, v rámci které je určen výbor pro řízení kybernetické bezpečnosti a bezpečnostní role včetně jejích práv a povinností souvisejících s ICT.	VKB, § 6, odst. 1	
X		Je určena bezpečnostní role: manažer kybernetické bezpečnosti / ISMS manažer.	VKB, § 6, odst. 2 a)	
X		Je určena bezpečnostní role: architekt kybernetické bezpečnosti.	VKB, § 6, odst. 2 b)	
X		Je určena bezpečnostní role: auditor kybernetické bezpečnosti.	VKB, § 6, odst. 2 c)	
X		Je určena bezpečnostní role: garant aktiva.	VKB, § 6, odst. 2 d)	
	X	Bezpečnostní role jsou určeny přiměřeně.	VKB, § 6, odst. 3	
X	X	Je určen výbor pro řízení kybernetické bezpečnosti.	VKB, § 6, odst. 7	
X	X	Je zajištěno odborné školení osob, které zastávají bezpečnostní role (v souladu s plánem budování bezpečnostního povědomí).	VKB, § 6, odst. 8	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Stanovení bezpečnostních požadavků pro dodavatele				
X	X	Jsou stanovena pravidla pro dodavatele, která zohledňují potřeby řízení bezpečnosti informací, a řídí své dodavatele nebo jiné externí subjekty, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti IS nebo KS KII a VIS. Rozsah zapojení dodavatelů na rozvoji, provozu nebo zajištění bezpečnosti IS nebo KS KII a VIS je dokumentován písemnou smlouvou, jejíž součástí je ustanovení o bezpečnosti informací.	VKB, § 7, odst. 1	
X		U dodavatelů je před uzavřením smlouvy prováděno hodnocení rizik, která jsou spojena s podstatnými dodávkami.	VKB § 7, odst. 2 a)	
X		U dodavatelů je uzavírána smlouva o úrovni služeb (SLA), která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.	VKB § 7, odst. 2 b)	
X		U dodavatelů se provádí pravidelné hodnocení rizik a pravidelná kontrola zavedených bezpečnostních opatření u poskytovaných služeb jsou zjištěné nedostatky odstraněny nebo je po dohodě s dodavatelem zajištěno jejich odstranění.	VKB § 7, odst. 2 c)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Řízení aktiv				
X	X	Jsou identifikována a evidována primární aktiva.	VKB, § 8, odst. 1 a)	
X	X	Jsou určeni jednotliví garanti aktiv, kteří jsou odpovědní za primární aktiva.	VKB, § 8, odst. 1 b)	
X	X	Je hodnocena důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a tato aktiva jsou zařazena do jednotlivých úrovní minimálně v rozsahu podle přílohy č. 1 k VKB.	VKB, § 8, odst. 1 c)	
X	X	Při hodnocení důležitosti primárních aktiv je především posuzováno: - rozsah a důležitost osobních údajů nebo obchodního tajemství,	VKB, § 8, odst. 2 a), odst. 2 b), odst. 2 c), odst. 2 d), odst. 2 e), odst. 2 f), odst. 2 g), odst. 2 h)	
		- rozsah dotčených právních povinností nebo jiných závazků,		
		- rozsah narušení vnitřních řídících a kontrolních činností,		
		- poškození veřejných, obchodních nebo ekonomických zájmů,		
		- možné finanční ztráty,		
		- rozsah narušení běžných činností orgánu a osoby,		
		- dopady spojené s narušením důvěrnosti, integrity a dostupnosti,		
		- dopady na zachování dobrého jména nebo ochranu dobré pověsti.		
X		Jsou identifikována a evidována podpůrná aktiva.	VKB, § 8, odst. 3 a)	
X		Jsou určeni garanti aktiv, kteří jsou odpovědní za podpůrná aktiva.	VKB, § 8, odst. 3 b)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X		Jsou určeny vazby mezi primárními a podpůrnými aktivy a hodnoceny důsledky závislostí mezi primárními a podpůrnými aktivy.	VKB, § 8, odst. 3 c)	
X	X	Jsou stanovena pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že: - jsou určeny způsoby rozlišování jednotlivých úrovní aktiv,	VKB, § 8, odst. 4 a) 1., 2., 3.	
		- jsou stanovena pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv,		
		- jsou stanoveny přípustné způsoby používání aktiv.		
X	X	Jsou zavedena pravidla ochrany odpovídající úrovni aktiv.	VKB, § 8, odst. 4 b)	
X	X	Jsou určeny způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv.	VKB, § 8, odst. 4 c)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Bezpečnost lidských zdrojů				
X	X	Je stanoven plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a jsou určeny osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny.	VKB, § 9, odst. 1 a)	
X	X	V souladu s plánem rozvoje bezpečnostního povědomí je zajištěno poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení.	VKB, § 9, odst. 1 b)	
X	X	Je zajištěna kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.	VKB, § 9, odst. 1 c)	
X	X	Je zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.	VKB, § 9, odst. 1 d)	
X	X	O školení jsou vedeny přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.	VKB, § 9, odst. 2)	
X		Jsou stanovena pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů.	VKB, § 9, odst. 3 a)	
X		Je hodnocena účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí.	VKB, § 9, odst. 3 b)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X		Jsou určena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.	VKB, § 9, odst. 3 c)	
X		Je zajištěna změna přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.	VKB, § 9, odst. 3 d)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Řízení provozu a komunikací				
X	X	Pomocí technických nástrojů, uvedených ve VKB v § 21 až 23 ZKB, jsou detekovány kybernetické bezpečnostní události, jsou pravidelně vyhodnocovány získané informace a na zjištěné nedostatky je reagováno v souladu s: Zvládání kybernetických bezpečnostních událostí a incidentů (VKB § 13).	VKB, § 10, odst. 1	
X	X	Je zajištěn bezpečný provoz informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému. Za tímto účelem jsou stanoveny provozní pravidla a postupy.	VKB, § 10, odst. 2	
X	X	Je prováděno pravidelné zálohování a prověřování použitelnosti provedených záloh.	VKB, § 10, odst. 4	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X		Provozní pravidla a postupy orgánu a osoby obsahují: - práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů,	VKB, § 10 odst. 3 a), odst. 3 b), odst. 3 c), odst. 3 d), odst. 3 e), odst. 3 f)	
		- postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů,		
		- postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech,		
		- spojení na kontaktní osoby, které jsou určeny jako podpora při řešení neočekávaných systémových nebo technických potíží,		
		- postupy řízení a schvalování provozních změn,		
		- postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.		
X		Je zajištěno oddělení vývojového, testovacího a produkčního prostředí.	VKB, § 10, odst. 5 a)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X		Jsou řešena reaktivní opatření vydaná NBÚ tím, že orgán a osoba: - posuzuje očekávané dopady reaktivního opatření na informační systém kritické informační infrastruktury nebo komunikační systém kritické informační infrastruktury a na zavedená bezpečnostní opatření, vyhodnocuje možné negativní účinky a bez zbytečného odkladu je oznamuje NBÚ,	VKB, § 10, odst. 5 b)	
		- stanovuje způsob rychlého provedení reaktivního opatření, který minimalizuje možné negativní účinky, a určuje časový plán jeho provedení.		
X		Je zajištěna bezpečnost a integrita komunikačních sítí a bezpečnost komunikačních služeb podle Nástroje pro ochranu integrity komunikačních sítí (VKB § 17).	VKB, § 10, odst. 6 a)	
X		Jsou určena pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi.	VKB, § 10, odst. 6 b)	
X		Výměna a předávání informací je prováděna na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla jsou dokumentována.	VKB, § 10, odst. 6 c)	
X		S ohledem na klasifikaci aktiv je prováděna výměna a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací.	VKB, § 10, odst. 6 d)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Řízení přístupu a bezpečné chování uživatelů				
X	X	Na základě provozních a bezpečnostních potřeb je řízen přístup k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a každému uživateli je přiřazen jednoznačný identifikátor.	VKB, § 11, odst. 1	
X	X	Jsou přijata opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů a administrátorů informačního systému kritické informační struktury, komunikačního systému kritické informační infrastruktury a významného informačního systému podle Nástroje pro ověřování identity uživatelů (VKB § 18) a Nástroje pro řízení přístupových oprávnění (VKB § 19), a která brání ve zneužití těchto údajů neoprávněnou osobou.	VKB, § 11, odst. 2)	
X		Přistupujícím aplikacím je přidělen samostatný identifikátor.	VKB, § 11, odst. 3 a)	
X		Přidělování administrátorských oprávnění je omezeno.	VKB, § 11, odst. 3 b)	
X		Přidělování a odebírání přístupových oprávnění je prováděno v souladu s politikou řízení přístupu.	VKB, § 11, odst. 3 c)	
X		Je prováděno pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích.	VKB, § 11, odst. 3 d)	
X		Je využíván nástroj pro ověřování identity uživatelů (VKB § 18) a nástroj pro řízení přístupových oprávnění (VKB § 19).	VKB, § 11, odst. 3 e)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X		Jsou zavedena bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými povinná osoba nedisponuje.	VKB, § 11, odst. 3 f)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Akvizice, vývoj a údržba				
X	X	Jsou stanoveny bezpečnostní požadavky na změny informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému spojené s jejich akvizicí, vývojem a údržbou a jsou zahrnuty do projektu akvizice, vývoje a údržby systému.	VKB, § 12, odst. 1	
X		Jsou identifikována, hodnocena a řízena rizika související s akvizicí, vývojem a údržbou informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury. Pro postupy hodnocení a řízení rizik se použijí metodiky podle řízení rizik (VKB § 4) odst. 1 písm. a) obdobně.	VKB, § 12, odst. 2 a)	
X		Je zajištěna bezpečnost vývojového prostředí a zároveň je zajištěna ochrana používaných testovacích dat.	VKB, § 12, odst. 2 b)	
X		Je prováděno bezpečnostní testování změn informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury před jejich zavedením do provozu.	VKB, § 12, odst. 2 c)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Zvládání kybernetických bezpečnostních událostí a incidentů				
X	X	Jsou stanoveny bezpečnostní požadavky na změny informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému spojené s jejich akvizicí, vývojem a údržbou a jsou zahrnuty do projektu akvizice, vývoje a údržby systému.	VKB, § 13, a)	
X	X	Jsou identifikována, hodnocena a řízena rizika související s akvizicí, vývojem a údržbou informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury. Pro postupy hodnocení a řízení rizik se použijí metodiky podle řízení rizik (VKB § 4) odst. 1 písm. a) obdobně.	VKB, § 13, b)	
X	X	Je zajištěna bezpečnost vývojového prostředí a zároveň je zajištěna ochrana používaných testovacích dat.	VKB, § 13, c)	
X	X	Je prováděno bezpečnostní testování změn informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury před jejich zavedením do provozu.	VKB, § 13, d)	
X	X	Zvládání kybernetických bezpečnostních incidentů je dokumentováno.	VKB, § 13, e)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Řízení kontinuity činnosti				
X	X	Jsou stanoveny práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role.	VKB, § 14, odst. 1 a)	
X	X	Jsou stanoveny cíle řízení kontinuity činností formou určení: - minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,	VKB, § 14, odst. 1 b) 1., 2., 3.	
		- doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému,		
		- doby obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu.		
X	X	Je stanovena strategie řízení kontinuity činností, která obsahuje naplnění cílů podle písmene b).	VKB, § 14, odst. 1 c)	
X		Jsou vyhodnocovány a dokumentovány možné dopady kybernetických bezpečnostních incidentů a posouzena možná rizika související s ohrožením kontinuity činností.	VKB, § 14, odst. 2 a)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X		Jsou stanoveny, aktualizovány a pravidelně testovány plány kontinuity činností informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.	VKB, § 14, odst. 2 b)	
X		Jsou realizována opatření pro zvýšení odolnosti informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickému bezpečnostnímu incidentu a je využíván Nástroj pro zajišťování úrovně dostupnosti podle Nástroj pro zajišťování úrovně dostupnosti (VKB § 26).	VKB, § 14, odst. 2 c)	
X		Jsou stanoveny a aktualizovány postupy pro provedení opatření vydaných NBÚ podle § 13 a 14 ZKB, ve kterých je zohledněno: - výsledky hodnocení rizik provedení opatření,	VKB, § 14, odst. 2 d), 1., 2., 3.	
		- stav dotčených bezpečnostních opatření,		
		- vyhodnocení případných negativních dopadů na provoz a bezpečnost informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury.		

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Kontrola a audit kybernetické bezpečnosti				
X	X	Je posouzen soulad bezpečnostních opatření s obecně závaznými právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a VIS a určena opatření pro jeho prosazování.	VKB, § 15, odst. 1 a)	
X	X	Jsou prováděny a dokumentovány pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol jsou zohledněny v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.	VKB, § 15, odst. 1 b)	
X		Je zajištěno provedení auditu kybernetické bezpečnosti osobou s odbornou kvalifikací podle § 6 odst. 6 VKB (auditor kybernetické bezpečnosti), která hodnotí správnost a účinnost zavedených bezpečnostních opatření.	VKB, § 15, odst. 2	
X		Pro IS nebo KS KII je prováděna kontrola zranitelnosti technických prostředků pomocí automatizovaných nástrojů a jejich odborné vyhodnocování a je reagováno na zjištěné zranitelnosti.	VKB, § 15, odst. 3	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Fyzická bezpečnost				
X	X	Jsou přijata nezbytná opatření k zamezení neoprávněného vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.	VKB, § 16, odst. 1 a)	
X	X	Jsou přijata nezbytná opatření k zamezení poškození a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.	VKB, § 16, odst. 1 b)	
X	X	Je předcházeno poškození, krádeži nebo kompromitaci aktiv nebo přerušení poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.	VKB, § 16, odst. 1 c)	
X		Jsou uplatněny prostředky fyzické bezpečnosti pro zajištění ochrany na úrovni objektů.	VKB, § 16, odst. 2 a)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X		Jsou uplatněny prostředky fyzické bezpečnosti pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor, ve kterých jsou umístěna technická aktiva informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury.	VKB, § 16, odst. 2 b)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Nástroj pro ochranu integrity komunikačních sítí				
X	X	Pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, je zavedeno(a): - řízení bezpečného přístupu mezi vnější a vnitřní sítí,	VKB, § 17, odst. 1 a), odst. 1 b), odst. 1 c), odst. 1 d)	
		- segmentace zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí,		
		- použití kryptografických prostředků (Kryptografické prostředky (VKB § 25)) pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií,		
		- opatření pro odstranění nebo blokování přenášených dat, která neodpovídají požadavkům na ochranu integrity komunikační sítě.		
X		Jsou využívány nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.	VKB, § 17, odst. 2	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Nástroj pro ověřování identity uživatelů				
X	X	Jsou používány nástroje pro ověření identity uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému.	VKB, § 18, odst. 1	
X	X	Nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem, zajišťuje: - minimální délku hesla osm znaků,	VKB, § 18, odst. 3 a), odst. 3 b), odst. 3 c)	
		- minimální složitost hesla tak, že heslo bude obsahovat alespoň tři z následujících čtyř požadavků: 1. nejméně jedno velké písmeno, 2. nejméně jedno malé písmeno, 3. nejméně jednu číslici nebo 4. nejméně jeden speciální znak, který není uveden v bodech 1 až 3,		
		- maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.		
X	X	Nástroj pro ověřování identity uživatelů je zajištěn jinými způsoby, než jaké jsou stanoveny v odstavcích 3 až 5, a orgán a osoba doložil(a), že použitá opatření zajišťují stejnou nebo vyšší úroveň odolnosti hesla.	VKB, § 18, odst. 5	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X		Je používán nástroj pro ověřování identity, který: - zamezuje opětovnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin,	VKB, § 18, odst. 4 a) 1., 2.	
		- provádí opětovné ověření identity po určené době nečinnosti.		
X		Využívá nástroj pro ověřování identity administrátorů. V případě, že tento nástroj využívá autentizaci heslem, zajistí prosazení minimální délky hesla patnáct znaků při dodržení požadavků podle odstavce 3 písm. b) a c).	VKB, § 18, odst. 4 b)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Nástroj pro řízení přístupových oprávnění				
X	X	Je používán nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění: - pro přístup k jednotlivým aplikacím a datům,	VKB, § 19, odst. 1 a), odst. 1 b)	
		- pro čtení dat, pro zápis dat a pro změnu oprávnění.		
X		Je používán nástroj pro řízení přístupových oprávnění, který zaznamenává použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik.	VKB, § 19, odst. 2	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Nástroj pro ochranu před škodlivým kódem				
X	X	Pro řízení rizik spojených s působením škodlivého kódu je používán nástroj pro ochranu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému před škodlivým kódem, který zajistí ověření a stálou kontrolu: - komunikace mezi vnitřní sítí a vnější sítí,	VKB, § 20, odst. 1 a), odst. 1 b), odst. 1 c)	
		- serverů a sdílených datových úložišť,		
		- pracovních stanic.		
		Je prováděna pravidelná aktualizace nástroje pro ochranu před škodlivým kódem, jeho definic a signatur.		

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů				
X	X	Je používán nástroj pro zaznamenávání činností informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, který zajišťuje: - sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti,	VKB, § 21, odst. 1 a), odst. 1 b)	
		- ochranu získaných informací před neoprávněným čtením nebo změnou.		

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X	X	Pomocí nástroje pro zaznamenávání činnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému je (jsou) zaznamenáváno(y): - přihlášení a odhlášení uživatelů a administrátorů,	VKB, § 21, odst. 2 a), odst. 2 b), odst. 2 c), odst. 2 d), odst. 2 e), odst. 2 f), odst. 2 g), odst. 2 h)	
		- činnosti provedené administrátory,		
		- činnosti vedoucí ke změně přístupových oprávnění,		
		- neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,		
		- zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému,		
		- automatická varovná nebo chybová hlášení technických aktiv,		
		- přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,		
		- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.		

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X	X	Nejméně jednou za 24 hodin je prováděna synchronizace jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.	VKB, § 21, odst. 4	
X		Záznamy činností zaznamenané podle odst. 2 jsou uchovávány nejméně po dobu tří měsíců.	VKB, § 21, odst. 3	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Nástroj pro detekci kybernetických bezpečnostních událostí				
X	X	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případné zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.	VKB, § 22, odst. 1	
X		Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí ověření, kontrolu a případně zablokování komunikace: - v rámci vnitřní komunikační sítě,	VKB, § 22, odst. 2 a), odst. 2 b)	
		- serverů patřících do informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.		

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí				
X		Je používán nástroj pro sběr a průběžné vyhodnocování kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajišťuje: - integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury,	VKB, § 23, odst. 1 a), odst. 1 b), odst. 1 c)	
		- poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech v informačním systému kritické informační infrastruktury nebo komunikačním systému kritické informační infrastruktury,		
		- nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí.		
X		Je zajištěna pravidelná aktualizace nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování.	VKB, § 23, odst. 2 a)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
X		Je zajištěno využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.	VKB, § 23, odst. 2 b)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Aplikační bezpečnost				
X	X	Jsou prováděny bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.	VKB, § 24, odst. 1	
X		Je zajištěna trvalá ochrana aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou.	VKB, § 24, odst. 2 a)	
X		Je zajištěna trvalá ochrana transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.	VKB, § 24, odst. 2 b)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Kryptografické prostředky				
X	X	Pro používání kryptografické ochrany je (jsou) stanovena: - úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu,	VKB, § 25, odst. 1 a) 1., 2.	
		- pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat.		
X	X	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik jsou používány kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a prokázání odpovědnosti za provedené činnosti.	VKB, § 25, odst. 1 b)	
X		Pro používání kryptografických prostředků je stanoven systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů.	VKB, § 25, odst. 2 a)	
X		Jsou používány odolné kryptografické algoritmy a kryptografické klíče; v případě nesouladu s minimálními požadavky na kryptografické algoritmy uvedenými v příloze č. 3 k této vyhlášce řídí rizika spojená s tímto nesouladem.	VKB, § 25, odst. 2 b)	

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Nástroj pro zajišťování úrovně dostupnosti				
X	X	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik je používán nástroj pro zajišťování úrovně dostupnosti informací.	VKB, § 26, odst. 1	
X		Je používán nástroj pro zajišťování úrovně dostupnosti informací, který zajišťuje: - dostupnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury pro splnění cílů řízení kontinuity činností,	VKB, § 26, odst. 2 a), odst. 2 b), odst. 2 c)	
		- odolnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost,		
		- zálohování důležitých technických aktiv informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury: 1. využitím redundance v návrhu řešení, 2. zajištěním náhradních technických aktiv v určeném čase.		

KII	VIS	Povinnost	Zákon / norma	Hodnocení
Bezpečnost průmyslových a řídicích systémů				
X		Pro bezpečnost průmyslových a řídicích systémů, které jsou informačním systémem kritické informační infrastruktury nebo komunikačním systémem kritické informační infrastruktury anebo jsou jejich součástí, jsou používány nástroje, které zajišťují: - omezení fyzického přístupu k síti a zařízením průmyslových a řídicích systémů,	VKB, § 27, a), b), c), d)	
		- omezení propojení a vzdáleného přístupu k síti průmyslových a řídicích systémů,		
		- ochranu jednotlivých technických aktiv průmyslových a řídicích systémů před využitím známých zranitelností,		
		- obnovení chodu průmyslových a řídicích systémů po kybernetickém bezpečnostním incidentu.		

Příloha č. 2: Rozšíření o problematiku GDPR

Povinnost	**Zákon / norma**	**Hodnocení**
Osobní údaje		
Osobní údaje, které jsou zpracovávané organizací, jsou identifikovány.	GDPR, čl. 32, odst. 1	
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, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku (opatření dle GDPR v závislosti na rizicích).	GDPR, čl. 32, odst. 1	
Při zpracování osobních údajů se využívá pseudonymizace.	GDPR, čl. 32, odst. 1	
Při zpracování osobních údajů se využívá šifrování osobních údajů.	GDPR, čl. 32, odst. 1	
Při zpracování osobních údajů je zajištěna neustálá důvěrnost, integrita, dostupnost a odolnost systémů a služeb zpracování.	GDPR, čl. 32, odst. 1	
Při zpracování osobních údajů je zajištěna schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.	GDPR, čl. 32, odst. 1	
Při zpracování osobních údajů je zajištěn proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.	GDPR, čl. 32, odst. 1	
Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.	GDPR, čl. 32, odst. 2	

Povinnost	**Zákon / norma**	**Hodnocení**
Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.	GDPR, čl. 32, odst. 4	
Jsou vedeny záznamy o všech typech zpracování osobních údajů (např. i záznamy o přístupech ke čtení).		
Je provedeno posouzení vlivu na ochranu osobních údajů.	GDPR, čl. 35	
Je přiřazena role DPO (Data Protection Officer).	GDPR, čl. 37 - 39	
Je uveden způsob, pomocí kterého jsou evidovány a získávány souhlasy se zpracováním osobních údajů		
Souhlasy jsou uchovávány a aktualizovány.		
Dodavatelé garantují bezpečnost zpracovávaných osobních údajů.		
Osobní údaje jsou kategorizovány a rozděleny.		
Práce s osobními daty je zaznamenávána/monitorována.		
Data z call centra jsou uchovávána.		
Souhlasy jsou udělovány v souladu s GDPR.		
Je řešena bezpečnost dat organizace u dodavatelů pomocí smluvně dodavatelského řetězce.		
Nakládání s osobními daty zákazníků je dokumentováno.		
Vlastní databáze dat je uložena v CPE nebo v jiné databázi.		
Záloha dat je prováděna na více než 2 samostatné zálohy.		
Jsou vedeny záznamy o hromadném zpracování dat.		
Na základě písemného souhlasu k nakládání s osobními údaji jsou rozesílány marketingové letáky, upozornění a marketingové newslettery.		
Organizace disponuje marketingovými bázemi i vlastními.		
Osobní údaje jsou v databázi zákazníků a je vykonávána správa dle smluvních ujednání.		
Je stanovena role správce dat s popisem této role.		

Povinnost	Zákon / norma	Hodnocení
Je stanovena role příjemce dat s popisem této role.		
Je stanovena role zpracovatele dat s popisem této role.		
Jsou zpracovávána osobní data a jsou ve vlastním systému organizace, který má přijata bezpečnostní opatření.		
Jsou evidovány osobní údaje pouze a výhradně ve vlastním systému společnosti.		
Jsou plněna zavedená pravidelná školení pro práci s osobními daty.		
Dokumentace k osobním datům je řešena pomocí zavedení ISMS nebo jiné směrnice.		
Je prováděn bezpečnostní audit IS, kde jsou obsažena osobní data.		
Jsou testována bezpečnostní opatření a jsou kontrolováni partneři a jejich způsob práce s osobními daty.		
Jsou k dispozici havarijní plány v případě porušení ochrany osobních údajů.		
Údaje o nákupech a využívaných službách jsou evidovány nebo jsou evidována data zákaznická a společnost je v roli zpracovatele osobních údajů (údaj o nákupu je osobním údajem). Oblast je řešena dokumentačně a z pohledu bezpečnosti osobních údajů.		
Jsou shromažďována data o IP adresách.		
Data jsou referencována s referencemi na konkrétní profily. Společnost také stanoví, kde jsou dodací nebo platební údaje zákazníka uloženy.		
Jsou prováděny pravidelné bezpečnostní audity IS a s nimi provázaná data.		
Data ve vlastních IS jsou bezpečně zpracovávána a uchovávána.		
Je zpracována kompletní přijímací dokumentace.		
Pokud společnost disponuje „papírovými osobními údaji“ je k těmto nestrojovým osobním údajům přistupováno podobně jako k těm strojovým osobním údajům.		

Povinnost	Zákon / norma	Hodnocení
Osobní údaje – kodexy chování		
Jsou zpracovány kodexy chování v souvislosti se zpracováním osobních údajů.	GDPR, čl. 40	
Jsou dodržovány schválené kodexy chování.	GDPR, čl. 32, odst. 3	
Je vydáno osvědčení podle čl. 40 GDPR.	GDPR, čl. 40, čl. 42	

Povinnost	Zákon / norma	Hodnocení
Osobní údaje – závazná podniková pravidla		
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - strukturu a kontaktní údaje skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a každého z jejích členů,	GDPR, čl. 47, odst. 2 a)	
- předání údajů nebo soubor předání, včetně kategorií osobních údajů, typu zpracování a jeho účelů, typu dotčených subjektů údajů a určení dané třetí země nebo daných třetích zemí,		
- svoji právně závaznou povahu, a to interně i externě.		
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - použití obecných zásad pro ochranu údajů, zejména účelové omezení, minimalizaci údajů, omezenou dobu uložení, kvalitu údajů, záměrná a standardní ochranu osobních údajů, právní základ pro zpracování, zpracování zvláštních kategorií osobních údajů,	GDPR, čl. 47, odst. 2 d)	
- opatření k zajištění zabezpečení údajů a požadavky ohledně dalšího předávání subjektům, které podnikovými pravidly nejsou vázány.		
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - práva subjektů údajů v souvislosti se zpracováním jejich osobních údajů a prostředky jejich výkonu, včetně práva nebýt předmětem rozhodnutí založených výhradně na automatizovaném zpracování, včetně profilování, práva podat stížnost u příslušného dozorového úřadu, právní ochrany a případně i práva na odškodnění v případě porušení závazných podnikových pravidel.	GDPR, čl. 47, odst. 2 e)	

Povinnost	Zákon / norma	Hodnocení
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - přijetí odpovědnosti správcem nebo zpracovatelem usazeným na území některého členského státu za jakékoli porušení závazných podnikových pravidel kterýmkoli dotčeným členem neusazeným v Unii,	GDPR, čl. 47, odst. 2 f)	
- správce nebo zpracovatel se může této odpovědnosti zcela nebo zčásti zprostit, pouze pokud prokáže, že za okolnost, jež vedla ke vzniku škody, není daný člen odpovědný.		
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - způsob poskytování informací o závazných podnikových pravidlech, zejména o ustanoveních uvedených v písmenech d), e) a f) tohoto odstavce, subjektům údajů, vedle informací uvedených v článcích 13 a 14.	GDPR, čl. 47, odst. 2 g)	
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - úkoly všech pověřenců pro ochranu osobních údajů jmenovaných v souladu s článkem 37, nebo jakékoli jiné osoby či subjektu pověřeného monitorováním souladu se závaznými podnikovými pravidly v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a sledování školení a vyřizování stížností.	GDPR, čl. 47, odst. 2 h)	
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - postupy pro vyřizování stížností.	GDPR, čl. 47, odst. 2 i)	

Povinnost	Zákon / norma	Hodnocení
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - mechanismy, které mají v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost zajistit ověřování souladu se závaznými podnikovými pravidly. Tyto mechanismy zahrnují audity ochrany údajů a metody zajištění opravných opatření pro ochranu práv subjektu údajů. Výsledky takového ověření by měly být oznámeny osobě nebo subjektu uvedenému v písmenu h) a radě řídícího podniku skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a na požádání by měly být zpřístupněny příslušnému dozorovému úřadu.	GDPR, čl. 47, odst. 2 j)	
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - mechanismy pro podávání zpráv a pro zaznamenávání změn pravidel a hlášení těchto změn dozorovému úřadu.	GDPR, čl. 47, odst. 2 k)	
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - strukturu a kontaktní údaje skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a každého z jejích členů,	GDPR, čl. 47, odst. 2 l)	
- mechanismus spolupráce s dozorovým úřadem, který zajistí dodržování pravidel každým členem skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost, zejména zpřístupňování výsledků ověřování opatření uvedených v písmenu j) dozorovému úřadu.		

Povinnost	Zákon / norma	Hodnocení
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - mechanismy pro podávání zpráv příslušnému dozorovému úřadu o právních požadavcích, kterým je člen skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost podřízen ve třetí zemi a které mohou mít podstatný negativní účinek na záruky poskytované závaznými podnikovými pravidly.	GDPR, čl. 47, odst. 2 m)	
V rámci zpracovávání OÚ jsou stanovena závazná podniková pravidla vymezující: - vhodnou odbornou přípravu v oblasti ochrany údajů pro pracovníky, kteří mají k osobním údajům trvalý nebo pravidelný přístup.	GDPR, čl. 47, odst. 2 n)	

Povinnost	Zákon / norma	Hodnocení
Osobní údaje – záznamy o činnostech zpracování		
Vedeny záznamy o činnostech zpracování OÚ: - jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů,	GDPR, čl. 30	
- účely zpracování,		
- popis kategorií subjektů údajů a kategorií osobních údajů,		
- kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích.		
Vedeny záznamy o činnostech zpracování OÚ: - informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk.	GDPR, čl. 30	
Vedeny záznamy o činnostech zpracování OÚ: - je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů,	GDPR, čl. 30	
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.		

Povinnost	Zákon / norma	Hodnocení
Vedeny záznamy o všech kategoriích činností zpracování prováděných pro správce, jež obsahují: - jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů,	GDPR, čl. 30	
- kategorie zpracování prováděného pro každého ze správců,		
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk,		
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.		

Povinnost	Zákon / norma	Hodnocení
Osobní údaje – posouzení vlivu na ochranu osobních údajů		
Ve společnosti probíhá automatické zpracování dat a profilování zákazníků (systematické a rozsáhlé zpracování dat).		
Společnost pracuje se zvláštními kategoriemi údajů (rasové, etnické, trestní, registry dlužníků apod.).		
Je prověřována platební schopnost klientů.		
Jsou vytvářeny marketingové profily zákazníků (např. dle jejich lokace).		
Zpracovávání údajů probíhá na základě automatizovaného rozhodování (může vést k diskriminaci některého ze zákazníků).		
Je monitorováno adresné chování zákazníků.		
Jsou zpracovávány lokalizační nebo platební údaje (i historické), které mohou být zneužity.		
Jsou zpracovávány rozsáhlé údaje (např. z důvodu cílení reklamy v e-shopech).		
Jsou zpracovávány nebo evidovány údaje dle územního rozsahu.		
Jsou zpracovávány údaje z propojených či kombinovaných souborů nebo databází, které obsahují osobní údaje a původem je více zdrojů (zpracování nad rámec původního účelu).		
Jsou zpracovávána data o zaměstnancích, zdravotně postižených nebo nezletilých.		
Je interně zaveden otisk prstu pro vstup na pracoviště.		
Data jsou předávána mimo EU.		
Data včetně osobních dat jsou přeshraničně předávána.		
Probíhá prověření zákazníků, kde se zákazník nemůže vyhnout nakládání s jeho daty (např. prověřování platební schopnosti či jeho ověření platební karty či totožnosti).		
Je stanoveno po jakou dobu jsou uchovávána data z call centra (z hovorů).		

Povinnost	Zákon / norma	Hodnocení
Je stanoveno, kde probíhá zálohování a archivace dat z call centra.		
Společnost disponuje kapacitami a plánem na zpracování procesu a technologických opatření, která vyplývají z tvorby dokumentace doporučení DPIA.		
Společnost disponuje přesným popisem procesů, kterým se jako správce musí prokazovat vůči ÚOOÚ.		

Povinnost	Zákon / norma	Hodnocení
Osobní údaje – právo na přenositelnost údajů		
Jsou rozlišovány kategorie dat (data aktivní a vědomě poskytnutá vs. data poskytnutá zákazníkem na základě využití služby).		