Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra systémové analýzy

Studijní program: Aplikovaná informatika

Studijní obor: Podniková informatika

Audit kybernetické bezpečnosti

Autor diplomové práce: Bc. Jakub Janša

Vedoucí diplomové práce: doc. Ing. Vlasta Svatá, CSc.

Oponent diplomové práce: Ing. Mgr. Martin Zbořil

Rok odevzdání: 2018

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze kterých jsem čerpal.

V Praze dne 23. dubna 2018 .....

podpis

Poděkování

Rád bych poděkoval doc. Ing. Vlastě Svaté, CSc. za poskytnuté cenné rady, trpělivost, pozitivní přístup a ochotu při vedení mé diplomové práce.

Abstrakt

Diplomová práce se zabývá auditem podle návrhu novely vyhlášky o kybernetické bezpečnosti. Stěžejní oblasti práce jsou informační a kybernetická bezpečnost, řízení rizik a audit. Hlavním cílem je návrh auditu a vývoj nástroje v podobě webové aplikace pro podporu průběhu auditu. Teoretická část se věnuje výkladu klíčových pojmů definovaných relevantními zákony a normami, které souvisejí s ústředními tématy práce. V praktické části je provedena podrobná analýza novely vyhlášky o kybernetické bezpečnosti a výstupem práce je soupis kritérií, pomocí kterých lze ověřit, že přijatá opatření jsou v souladu s vyhláškou. Zároveň jsou identifikovány doplňující dokumenty související vyhláškou, které obsahují podrobnější informace. Nástroj, který je součástí práce, vychází z analýzy vyhlášky a podporuje průběh auditu.

Klíčová slova:

Zákon o kybernetické bezpečnosti, audit, ujištění, kybernetická bezpečnost, informační bezpečnost, aktivum, hrozba, zranitelnost, riziko, řízení rizik

Abstract

The diploma thesis deals with the audit according to the draft amendment of the Cyber Security Regulation. Key areas of work are information and cyber security, risk management and auditing. The main objective is to design audit and develop a tool in the form of a web application to support the audit. The theoretical part deals with the interpretation of key concepts defined by relevant laws and standards that are related to the central themes of the thesis. In the practical part, a detailed analysis of the amendment to the Cyber Security Regulation is made and the output of the thesis is an inventory of the criteria by which can be verified that the measures taken are in accordance with the Regulation At the same time, supplementary documents related to the Regulation, which contain more detailed information, are identified. The tool that is part of the work is based on the analysis of the Regulation and supports the process of the audit.

Keywords:

Law, audit, assurance, cybersecurity, information security, assets, threats, vulnerability, risk, risk management

Obsah

1 Úvod 1
1.1 Vymezení tématu práce a důvod výběru tématu 2
1.2 Charakteristika současného stavu problémové oblasti 3
1.3 Cíle práce 3
1.4 Metody dosažení práce 3
1.5 Předpoklady a omezení práce 3
1.6 Struktura práce 4
1.7 Přínosy práce 5
2 Komentovaná rešerše 6
3 Informační bezpečnost a kybernetická bezpečnost 8
3.1 Informační bezpečnost 8
3.2 Kybernetická bezpečnost 9
3.3 Vývoj regulace v oblasti kybernetické bezpečnosti v ČR 13
3.4 Zákon o kybernetické bezpečnosti a jeho prováděcí vyhlášky 15
3.4.1 Novely zákona a vyhlášek 16
3.4.2 Směrnice NIS 17
3.4.3 Další zákony a vyhlášky ve vztahu k ZoKB 19
3.4.4 Role 21
3.4.5 Osoby 22
3.4.6 Opatření v zákonu a vyhlášce 26
3.5 Systém řízení informační bezpečnost 27
3.6 Normy ISO 29
3.7 Obecné nařízení o ochraně osobních údajů 31
3.8 Bezpečnostní dokumentace a bezpečnostní politika 33
3.9 Deset kroků kybernetické bezpečnosti 39
3.10 Bezpečnostní hrozby 42
3.11 Problematické aspekty kybernetické bezpečnosti 44
3.12 Fenomén kybernetické a informační války 45
3.13 Lidský faktor 46
4 Řízení rizik 48

4.1 Řízení rizik podle normy ISO 31000, ISO 27001 a ISO 27005 ... 50
4.2 Stanovení kontextu ... 52
4.3 Identifikace a hodnocení aktiv ... 52
4.4 Identifikace hrozeb a zranitelností ... 53
4.5 Analýza rizik ... 55
4.6 Zvládání rizik ... 57
5 Audit ... 58
5.1 Co je to audit ... 58
5.2 Audit podle norem ISO ... 59
5.3 Role auditora ... 62
5.4 Institut auditu z pohledu poskytovatele služby auditu ... 64
5.5 Audit a jeho fáze podle ISO 19011 ... 66
5.5.1 Řízení programu auditu ... 67
5.5.2 Provádění auditu ... 68
5.5.3 Závěr z auditu a auditorská zpráva ... 71
5.6 Audit podle vyhlášky o kybernetické bezpečnosti ... 73
6 Analýza regulací ... 74
7 Návrh auditu kybernetické bezpečnosti ... 83
7.1 Nástroj na podporu auditu ... 85
7.2 Scénář používání nástroje pro podporu auditu ... 87
7.2.1 Doplněk nástroje ... 91
8 Závěr ... 94
Terminologický slovník ... 96
Seznam literatury a použitých zdrojů ... 98
Seznam obrázků ... 107
Seznam příloh ... 110

1 Úvod

Mnoho prací věnujících se informační a kybernetické bezpečnosti uvozují text tvrzením o vývoji technologií, jejich všudypřítomností a závislostí na těchto technologiích. Na tyto teze lze navázat skutečností, že rozvoj informatiky skýtá i potenciál zneužití a různých hrozeb. Dlouhodobým trendem je efektivně využít možností moderních technologií pro zvýšení výkonu a snížení nákladů v organizaci. Moderní informační a komunikační technologie staví na významných pokrocích, které se během svého bouřlivého rozvoje staly standardem a součástí většiny podnikání, fungování států a jeho složek i běžného společenského života v informační společnosti. Užitek poskytují, když plní očekávání uživatelů.

Jedním z mnoha milníků ve vývoji technologií je internet, který propojuje prakticky celý svět. Díky internetu lze komunikovat s celým světem v reálném čase, sdílet data, obchodovat, provádět platby a mnoho dalších aktivit. Internet je decentralizovaným zdrojem informací nejrůznějšího druhu. Jeho princip je založen na stále narůstajícím počtu do sítě připojených serverů a stanic, mezi kterými se přenášejí data. Přenášená data mohou mít různou podobu od obrázků, audio-video souborů, přes dokumenty, zprávy nebo obchodní transakce až k obsahu, který může být „závadný“. Příkladem dětská pornografie, kyberšikana, šíření malware a mnoho dalších. Pro uživatele je důležité umět s informacemi pracovat, protože internet negarantuje relevantnost informací, které uživatel požaduje, a může se setkat i s informacemi, pro které se používají termíny jako „fake news“ nebo „hoax“.

Organizace se snaží smysluplně a vhodně využívat možnosti technologií. Mnoho organizací je na informačních a komunikačních technologiích závislá, někdy dokonce kriticky a existenčně závislá. Kybernetický prostor se stává střetem útočící strany a strany, která se snaží útokům bránit. Organizace, která je v pozici bránící se strany, musí být připravena čelit možným hrozbám. Pro zajištění bezpečnosti je třeba zavést vhodná opatření. Vytvoření systému bezpečnosti informací vychází ze zkušeností, poučení se z minulosti, ale také z poznání sebe sama. Smyslem systému řízení bezpečnosti informací je zajistit odpovídající úroveň bezpečnosti, a být tak připraven zvládat bezpečnostní incidenty. Neodmyslitelnou součástí každého podnikání jsou různá rizika. Jejich projevy negativně působí na fungování organizace. Působení rizik ovlivňuje informační bezpečnost a má dopad na požadovaný a očekávaný stav dostupnosti, důvěrnosti a integrity.

Informace je komodita, která má svoji cenu a má i svoji důležitost pro své vlastníky. Proto není žádoucí, aby byla informace nechtěným způsobem měněna. Informace může mít svou hodnotu,

kterou je třeba náležitým způsobem chránit, ale zároveň by měla být dostupná všem, kdo s informací mají oprávnění pracovat. Skutečná hodnota informace může být zjištěna až když je pozdě, což může pro organizace znamenat problémy. Jsou známy případy, kdy nedostatečná ochrana dat a informací měla závažné dopady. Například v dubnu 2018 byl zaznamenán únik dat ze sociální sítě Facebook, při kterém útočníci získali osobní údaje miliónů uživatelů. Stejný problém se v roce 2017 dotkl i české společnosti MALL.CZ. Tehdy společnost přišla o tři čtvrtě milionu uživatelských údajů. Kromě úniku osobních údajů je problémem i únik důvěrných dat. Příkladem je únik dat, který postihl americkou zpravodajskou službu CIA, když servery WikiLeaks zveřejnily tajné dokumenty z jejich počítačů. Opačným problémem je odepření dostupnosti. V roce 2013 proběhl v České republice několikadenní útok na zpravodajské servery, e-shopy a dotkl se i některých internetových služeb, když narušil jejich dostupnost. Tyto problémy jsou jen krátkým výčtem možných bezpečnostních incidentů.

Zajištění bezpečnosti v kybernetickém prostoru znamená vypořádat se hrozbami mnoha různých forem a podob. Rozvoj technologií i množství zařízení připojených do sítě představují neskutečný potenciál jak pro obchodní příležitosti, tak i pro zajišťování nejrůznějších služeb. Zajištění bezpečnosti je nutnost a je prosazována zákony, směrnicemi a normami. Bezpečnost v organizaci utvářejí přijatá opatření, která usilují o minimalizaci hrozeb. I pitoreskní představa, že „smart“ spotřebič útočí na kritickou infrastrukturu se může stát realitou.

1.1 Vymezení tématu práce a důvod výběru tématu

Ústředním tématem této práce je kybernetická bezpečnost z pohledu auditu prováděného podle návrhu novely vyhlášky o kybernetické bezpečnosti. Bezpečnost prosazuje zákon o kybernetické bezpečnosti a jeho prováděcí vyhlášky. Znění zákona je významně ovlivněno směrnicí Evropského parlamentu a Rady (EU) 2016/1148. Prostřednictvím novel zákona a vyhlášek zapracovala Česká republika do svého právního prostředí nutné změny. S tématem práce také souvisejí normy z rodiny ISO 27000, ze kterých vychází především vyhláška o kybernetické bezpečnosti. Analýzy zákonů a norem jsou využity pro návrh auditu kybernetické bezpečnosti. Součástí práce je také nástroj na podporu auditu.

Důvod volby tohoto tématu je jeho významnost, aktuálnost a dále je podpořen i zájmem autora o oblasti, které s kybernetickou bezpečností, riziky a auditem souvisejí. Motivací je navrhnout prototyp nástroje pro řízení průběhu auditu a jeho další rozvoj za účelem zjednodušení provádění auditu.

1.2 Charakteristika současného stavu problémové oblasti

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti byl přijat v roce 2014 a je účinný od 1. ledna 2015. Od té doby byl zákon několikrát novelizován. Nejzásadnější změny, které ovlivnily podobu zákona, jsou reakcí na přijetí 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. Transpozice směrnice do českého právního prostředí byla provedena především zákonem č. 205/2017 Sb. Na úrovni prováděcí vyhlášky dosud[1] nutné změny nebyly přijaty. Pro soulad se směrnicí by tak Česká republika měla učinit do 10. května 2018. Poslední dostupné znění návrhu vyhlášky, použité pro účel této práce, je součástí příloh. Přijetí návrhu této vyhlášky by ovšem znamenalo nekonzistenci mezi opatřeními uvedeným v zákoně a opatřeními, jak je uvádí novela vyhlášky. Lze předpokládat, že nutné změny proběhnou současně. V roce 2018 byly také vydány revize některých ISO norem z řady 27000, které souvisejí se systémem řízením bezpečnosti informací, což je důsledkem vývoje v oblastech informační bezpečnosti.

1.3 Cíle práce

Cílem práce je představit témata kybernetické a informační bezpečnosti, řízení rizik a auditu a dále analýza zákonů a norem, které s uvedenými tématy souvisejí. Z těchto základů vychází hlavní cíl práce, a tím je návrh auditu kybernetické bezpečnosti a vývoj nástroje pro podporu průběhu auditu.

1.4 Metody dosažení cíle

Pro dosažení cílů je provedena rešerše diplomových prací, odborné literatury, best practices a dalších zdrojů informací, které se vztahují k tématu práce. Pro návrh auditu je provedena analýza zákonů a norem souvisejících s auditem a bezpečností informací. Metodou srovnání jsou identifikovány rozdíly, které s sebou nese novela vyhlášky o kybernetické bezpečnosti. Z výsledků analýzy je pomocí syntézy proveden návrh auditu a s ním související vývoj nástroje pro podporu provádění auditu.

1.5 Předpoklady a omezení práce

Návrh programu auditu předpokládá přijetí novely vyhlášky o kybernetické bezpečnosti a její obsahovou shodu s návrhem, který je uveden v příloze. Další předpoklady souvisejí s nástrojem pro provádění auditu. Nástroj je vyvinut jako webová aplikace. Pro je ho používání se předpokládá

[1] K 11. dubnu 2018

použití webového prohlížeče Google Chrome a připojení k internetu pro použití komponent třetích stran, včetně jejich dostupnosti. Dalším omezením nástroje je přímé sdílení dat mezi více uživateli. Sdílení suplují funkce importu a exportu dat. Samotná realizace nástroje předpokládá potřebné znalosti vývoje běžné webové aplikace.

1.6 Struktura práce

Diplomová práce je dělena do kapitol podle diskutovaných témat. Po úvodní kapitole následuje rešerše zdrojů zabývajících se stejnými i souvisejícími tématy. Druhou kapitolou je komentovaná rešerše, která se zabývá především diplomovými pracemi, nahlížejícími na kybernetickou bezpečnost podle zákona o kybernetické bezpečnosti z různých úhlů.

Následuje třetí kapitola, což je rozsáhlá stať o kybernetické a informační bezpečnosti, zákonu o kybernetické bezpečnosti a jeho prováděcích vyhláškách, včetně legislativního vývoje a vlivů, které měly dopad na znění zákona a vyhlášek. Zároveň jsou v této kapitole představeny významné ISO normy a další témata související s řízením bezpečnosti.

Čtvrtá kapitola se věnuje řízení rizik. Podrobněji bude v kapitole probrán rámec řízení rizik z pohledu ISO norem a procesů řízení rizik, včetně identifikace a hodnocení aktiv, hrozeb a zranitelností. Na tyto části navazuje analýza rizik a způsoby zvládání rizik.

V páté kapitole je představen audit jako pojem a jeho pojetí v ISO normách řady 9000, ve které jsou společně s normou ISO 19011 definice základních principů, procesů, postupů a vztahů auditu. Rovněž je v této kapitole popsána role auditora a pohled poskytovatele služby auditu. V závěru kapitoly je popsán audit podle novely vyhlášky o kybernetické bezpečnosti.

Obsahem šesté kapitoly je analýza novely vyhlášky o kybernetické bezpečnosti. V rámci této kapitoly jsou uvedeny popisy procesů určování povinných subjektů a jsou popsány vztahy mezi jednotlivými opatřeními. Dále tato kapitola obsahuje podrobný rozbor opatření pro audit a pro jednotlivá opatření jsou identifikovány významné související dokumenty. Výsledky analýzy jsou použitelné pro ověření souladu s novelou vyhlášky.

Na šestou kapitolu navazuje kapitola sedmá, která se zabývá návrhem auditu. Kromě popisu postupu auditu jsou zde využity výsledky z předchozích kapitol. Dále se kapitola věnuje nástroji na podporu provádění auditu. Kapitola zahrnuje popis nástroje a obsahuje i scénář pro použití nástroje.

1.7 Přínosy práce

Mezi přínosy této práce lze považovat představení novely vyhlášky a identifikaci rozdílů oproti vyhlášce, kterou má nahradit. Výstup lze využít pro účely revize stávajícího stavu k uvedení do souladu s novelizovanou vyhláškou. Práce může poskytnout výklad vyhlášky pro účely auditu i systému řízení bezpečnosti informací, a jako podklad pro zlepšování bezpečnosti. Tato práce může být rovněž základním zdrojem informací pro seznámení s řízením kybernetické bezpečnosti, řízením rizik a auditem.

Dalším přínosem je nástroj na podporu auditu, který je praktickým vyústěním této práce. Nástroj a jeho rozšiřující modul podporují provádění auditu kybernetické bezpečnosti. Nástroj obsahuje výsledky analýz z celé práce, a uživatel tato data může použít při práci s tímto nástrojem. Doplněk nástroje je vyvinut v souladu s novelou vyhlášky o kybernetické bezpečnosti a má přesah do oblasti správy a řízení aktiv a rizik.

2 Komentovaná rešerše

Publikací, které se primárně zaměřují na kybernetickou bezpečnost, je velmi omezené množství. Jedinou knihou, která se tomuto tématu komplexněji věnuje, je publikace *Zákon o kybernetické bezpečnosti: Komentář*. Dalšími zdroji informací jsou akademické práce. Jejich stručné rešerše jsou také obsahem této kapitoly.

Výkladem zákona o kybernetické bezpečnosti se zabývá (Maisner, Vlachová, 2015). Tato publikace se vztahuje ke znění zákona před jeho novelizací. Právě novely značně pozměnily zákon, a tím se tato publikace stala neaktuální. Přesto je dobrým zdojem, který zachycuje vývoj v oblastech kybernetické a informační bezpečnosti. Publikace vychází z Důvodové zprávy k Věcnému záměru zákonu o kybernetické bezpečnosti, kterou doplňuje komentáři. Minimální pozornost je věnována vyhláškám, které se zákonem souvisejí.

Na téma *Kybernetické bezpečnosti* nahlíží (Fleischmannová, 2015) z pohledu mezinárodních vztahů. Nejprve se autorka věnuje výkladu pojmů z oblasti bybernetické bezpečnosti a hrozeb. V další části srovnává vnímání kybernetické bezpečnosti v Číne a v USA a navazuje kapitolou o vzájemné spolupráci obou zemí v oblasti kybernetické bezpečnosti. Práce se dále věnuje analýze konfliktu, který mezi sebou Čína a USA vedly v roce 2001 a analyzuje dopady konfliktů na vzájemné vztahy mezi oběma zeměmi.

Kratochvíl (2013) se ve své diplomové práci *Kybernetický bezpečnost a legislativa ČR* zabývá legislativou, která má vztah ke kybernetické bezpečnosti. Autor ve své práci podrobně rozebírá související legislativu v rámci ČR i EU. Tato práce vznikala v době před přijetím zákona o kybernetické bezpečnosti a analyzuje jaký dopad může mít přijetí nového zákona na základě rozboru Věcného záměru zákonu o kybernetické bezpečnosti. V rámci práce jsou rovněž definovány důležité termíny z oblastí kybernetické bezpečnosti, kybernetické kriminality a dalších nelegálních činností.

V bakalářské práci se (Kohout, 2015) zabývá tématem *Návrhu bezpečnostní politiky informačních technologií v prostředí středně velké společnosti*. Autor velice srozumitelně a přehledně komentuje zákon o kybernetické bezpečnosti, související vyhlášky a ISO normy. Autor v práci postupuje z pohledu návrhu bezpečnostní politiky a identifikuje důležité aspekty, které by měla bezpečnostní politika zahrnovat. Součástí práce je i dotazník, který prostřednictvím sady otázek umožňuje získat základní informace o organizace a její vztah ke kybernetické bezpečnosti.

K problematice kybernetické bezpečnosti přistupuje (Kameníček, 2016) z pohledu podnikové informatiky. V úvodu práce uvádí přehled aktuálních hrozeb, které se týkají kybernetické bezpečnosti. Následuje kapitola, ve které definuje a stanoví kategorie podnikatelských subjektů, a ke každému subjektu přiřazuje hrozby, které na subjekt mohou působit. Na tyto zjištění navazuje přiřazením kategorií subjektů na vybrané příklady typových subjektů. Kromě toho pro každou kategorii subjektů identifikuje, jaké zákonné povinnosti se subjektu týkají a jaká doporučená opatření by měl subjekt přijmout pro ochranu bezpečnosti. V závěru práce se autor věnuje testování kybernetické bezpečnosti ve vztahu k různým hrozbám. Celá práce má vyústění v podobě návrhu metodické pomůcky pro zvýšení bezpečnosti v organizaci.

Ve své práci se Draganov (2016) zabývá tématem *Zákon o kybernetické bezpečnosti a jeho dopady na povinné subjekty*. Autor detailně analyzuje zákon o kybernetické bezpečnosti, věnuje se terminologii a vztahům k jiným zákonům a dalším dokumentům. Zabývá se i vývojem regulací kybernetické bezpečnosti v rámci České republiky i EU. Autor rovněž rozebírá zákon a vyhlášku o kybernetické bezpečnosti z hlediska dopadu na povinné subjekty. Mimo jiné se autor také zabývá kritikou zákona. Zmiňuje rozdílnou terminologii nebo diskutuje myšlenku, zda je nutností přijetí samostatného zákona, který by reguloval oblast kybernetické bezpečnosti. V praktické části práce se autor zabývá průzkumem, ve kterém zkoumá a ověřuje dopady zákona na povinné subjekty. V průzkumu se autor změřil na Krajské úřady.

Diplomová práce *Zavedení systému řízení bezpečnosti informací v praxi* (Bína, 2014) se zabývá přístupem k řízení bezpečnosti v organizaci. V teoretické části se autor věnuje pojmům a jejich výkladu, dále rozebírá zákony a ISO normy, ale věnuje se i dalším dokumentům jako je PCI (Payment Card Industry) HIPPA (Health Insurance Portability and Accountability Act) a SOX (Sarbanes – Oxley Act). V praktické části autor představuje vlastní návrh zavedení a provozování systému řízení bezpečnosti informací, respektive jeho vybraných oblastí. Autor zmiňuje také důležitost a význam přezkoumávání a zlepšování systému bezpečnosti s ohledem na nová zjištění, která souvisí s riziky i technologiemi.

3 Informační bezpečnost a kybernetická bezpečnost

Tato kapitola se věnuje termínům a důležitým tématům z oblasti informační bezpečnosti, kybernetické bezpečnosti, zákonů a regulací.

3.1 Informační bezpečnost

Informační bezpečnost je bezesporu jednou z nejdůležitějších oblastí snad všech organizací bez rozdílu typu nebo velikosti. Najít jednoduchou a výstižnou definici termínu informace je skoro nemožné. Nejprve je důležité definovat jiný termín, a tím je pojem data. *Data jsou vyjádření skutečností a myšlenek v předepsané podobě tak, aby je bylo možné uchovávat, přenášet a zpracovávat* (Porada, 2016, s. 395). Informace je podle Porady (2016) výsledkem zpracování dat, která má význam a hodnotu pro příjemce. (Gřivna, Polčák, 2008) nabízí formulaci, že informace může být opakem entropie. (Gála, Pour, Šedivá, 2009) uvádí pojetí informace jako zprávu o jevu, která u příjemce snižuje míru neznalosti o tomto jevu. Na informaci lze nahlížet různou úrovní pohledu podle uspořádání, interpretace a požití znaků. (Gála, Pour, Šedivá, 2009) rozlišují:

- syntaktickou úroveň, tedy vztahy mezi znaky,
- sémantickou úroveň, která se zabývá zkoumáním vztahu znaků k objektu, o kterém jsou znaky použity,
- pragmatickou úroveň, jenž se zabývá vztahem informace k příjemci.

V souvislosti s informační bezpečností i samotného zaměření této práce nelze vynechat pohled na informace uvedené v dokumentu (COBIT 4.1 Excerpt, 2007), kterými jsou požadavky na:

- účinnost (*effectiveness*) - zabývá se relevantními informacemi pro obchodní proces, jsou dodávány včas, správně, konzistentně a použitelně,
- efektivitu (*efficiency*) - poskytování informací nejvíce produktivním využitím zdrojů,
- soulad (*compliance*) - zabývá se dodržováním zákonů, předpisů a ujednání,
- spolehlivost (*reliability*) - týká se poskytování vhodných informací pro management,
- důvěrnost (*confidentiality*) - je ochrana citlivých informací před zneužitím,
- integritu (*integrity*) - týká se platnosti, přesnosti a úplnosti informací a
- dostupnost (*availability*) – informace jsou k dispozici podle potřeby.

Poslední tři požadavky jsou důležité pro definici informační bezpečnosti. Ještě před tím, než bude vysvětlen pojem informační bezpečnost, je třeba zvlášť vymezit termín bezpečnost. Její význam vysvětluje (Čermák, 2009) jako ochranu něčeho před zničením, poškozením nebo ztrátou. Nyní lze

přejít k definici pojmu informační bezpečnost. (Zákon č. 181/2014 Sb., 2018) a (ISO/IEC 27000, 2009) shodně uvádějí definici, která říká, že se jedná o zajištění důvěrnosti, integrity a dostupnosti informací a dat.

Z výše uvedeného lze charakterizovat informační bezpečnost jako soubor opatření, který má za úkol chránit informace před neoprávněným použitím a nežádoucím pozměňováním dat, aby požadovaná data byla kdykoliv dostupná uživatelům, kteří mají oprávnění s informacemi pracovat, a to s maximální snahou o zajištění žádoucí doby existence těchto informací.

Řízní informační bezpečnosti, ať už mají elektronickou nebo klasickou papírovou formu, nebo se jedná o znalosti zaměstnanců, znamená znát hodnotu a význam informací, což může (mimo jiné) představovat konkurenční výhodu. Naopak neschopnost ochránit informace může způsobit, že se organizace dostane do problémů, soudních sporů, nebo bude ohrožena reputace a dobrá pověst, což má své důsledky. Proto rozhodování o způsobech zajištění informační bezpečnosti musí být důležitým prvkem v řízení organizace. Ovšem přimět je k tomu může projev až bezpečnostního incidentu, a to už je pozdě. Osvícenější přístup k zajištění bezpečnosti v organizaci vychází ze znalosti zákonů a norem. Soulad s nimi minimalizuje případné problémy (Brechlerová, 2005).

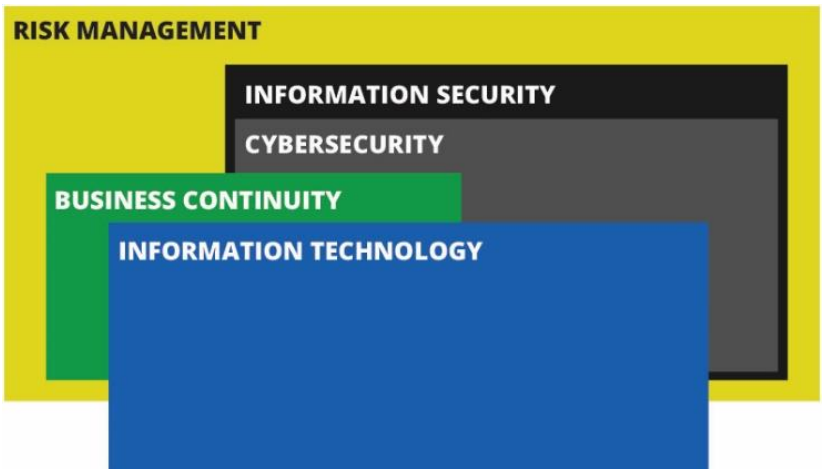
3.2 Kybernetická bezpečnost

Vysvětlení pojmu kybernetická bezpečnost (dále také KB) lze najít ve věcném záměru zákona o kybernetické bezpečnosti. Definuje ji jako: *souhrn právních, organizačních, technických, fyzických a vzdělávacích opatření namířených na zajištění nerušeného a bezvadného fungování kybernetického prostoru* (Věcný záměr zákona o kybernetické bezpečnosti, 2012, s. 56). Kybernetický prostor pak věcný záměr zákona vykládá jako*: digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními a komunikačními technologiemi, zahrnující připojení k veřejné síti (internet)* (Věcný záměr zákona o kybernetické bezpečnosti, 2012, s. 56). Další definice vykládá kybernetickou bezpečnost jako: *souhrn technologií, procesů a praktiky, jejichž cílem je ochrana sítí, počítačů, programů a dat před útoky, zničením nebo neautorizovaným přístupem. Jde o součást informační bezpečnosti* (Svatá, 2016, s. 49).

Jednotlivá vymezení definic kybernetické a informační bezpečnosti nejsou od sebe příliš vzdálená. (Kosutic, 2012) zmiňuje, že ačkoliv neexistují žádné oficiální postoje ohledně rozdílů mezi informační bezpečností a kybernetickou bezpečností, lze je interpretovat tak, že kybernetická bezpečnost je 95 % informační bezpečnosti. Rozdíl podle (Kosutic, 2012) spočívá v tom, že ochrana

informací zahrnuje bezpečnost týkající se informací na neelektronických médiích, zatímco kybernetická bezpečnost se zaměřuje pouze na informace v digitální podobě.

Charakter kybernetické bezpečnosti se podle normy ISO 27032 *vztahuje na opatření, která by zainteresované strany měly stanovit pro vytvoření a zachování bezpečnosti v kybernetickém prostoru* (ISO 27032, 2013, s. 17). Tato norma spojuje bezpečnost kybernetického prostoru s bezpečností Internetu, bezpečnosti sítí a také všeobecně s bezpečností informací. Rozdíl v kybernetické bezpečnosti oproti informační bezpečnosti vyplývá z normy ISO 27032, když uvádí, že *bezpečnost informací se zabývá ochranou důvěrnosti, integrity a dostupnosti informací všeobecně tak, aby sloužila potřebám uživatelů příslušných informací* (ISO 27032, 2013, s. 18), zatímco kybernetická bezpečnost je *zachování důvěrnosti, integrity a dostupnosti informace v kybernetickém prostoru* (ISO 27032, 2013, s. 12). Z tohoto lze vyvodit, že kybernetická bezpečnost je podmnožinou informační bezpečnosti a dále to naznačuje, že rozdílem je právě prostředí kybernetického prostoru. Bezpečnost tohoto prostředí lze zajistit přijetím vhodných opatření. Rozdílem kybernetické a informační bezpečnosti mohou být také specifická rizika, vyplývající z prostředí, kterých se rizika týkají, což je v případě kybernetického prostoru nehmotný prostor virtuálního světa.

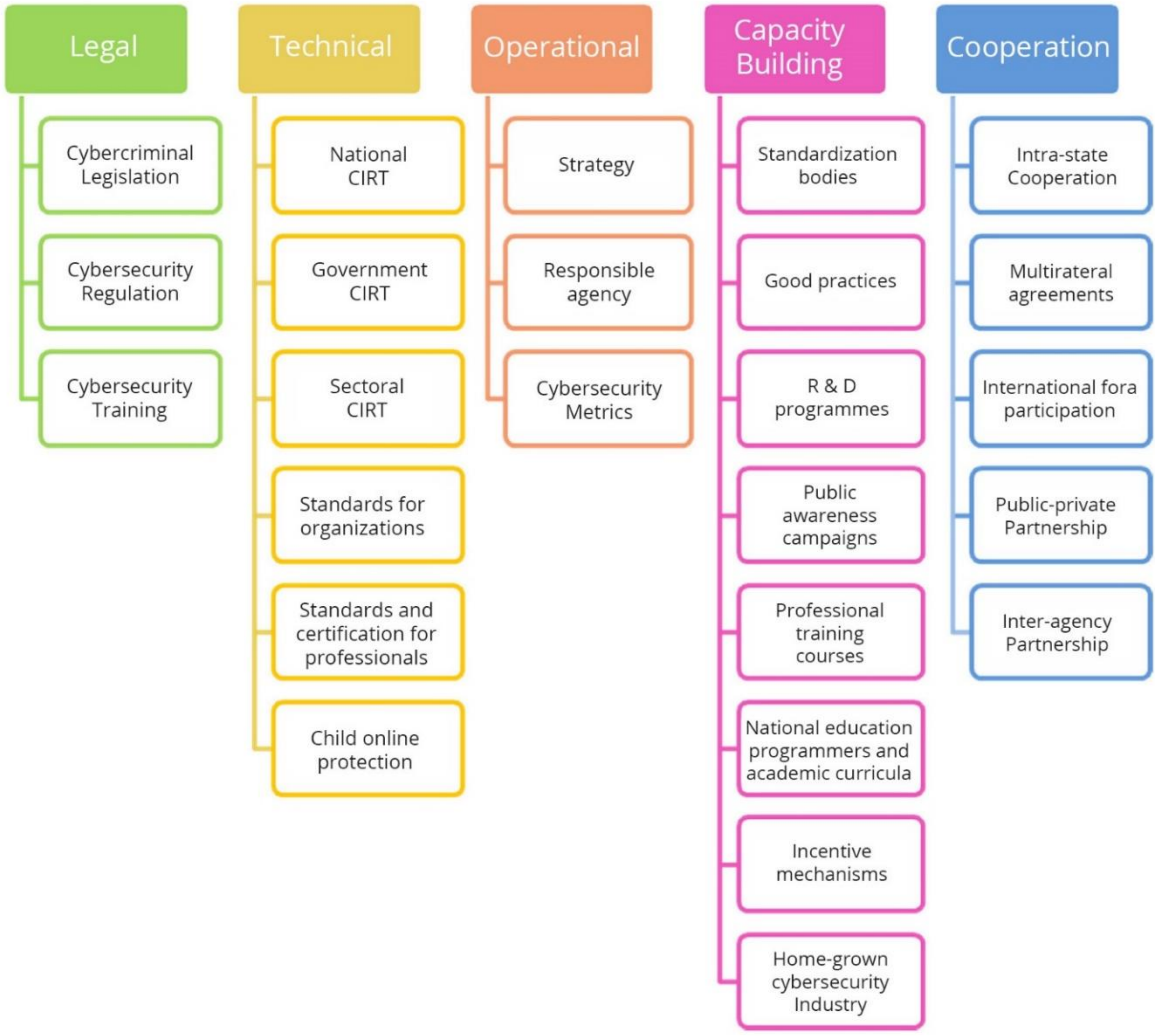


Obrázek 1: Vztah kybernetické a informační bezpečnosti. Zdroj: vlastní úprava podle (Kosutic, 2012)

Stav kybernetické bezpečnosti podle (Maisner, Vlachová, 2015) se může stát hodnotícím kritériem, což ovlivňuje konkurenceschopnost země při posuzování investory. Mezinárodní srovnání v oblasti kybernetické bezpečnosti a připravenosti na kybernetické útoky sledují žebříčky National Cyber Security Index[2] (NCSI) a Global Cybersecurity Index[3] (GCI). (Průša, 2017) připomíná, že oba žebříčky využívají rozdílnou metodologii a v obou hodnoceních byl posuzován rozdílný počet států zahrnutých do projektu. Zatímco je Česká republika zařazena do hodnocení obou žebříčků, není

[2] http://ncsi.ega.ee/ncsi-index/
[3] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx

tak tomu u mnoho dalších států, čímž je problematičtější srovnání obou indexů. Kritéria použitá pro hodnocení kybernetické bezpečnosti (viz Obrázek č. 2) se zaměřují na existenci národní strategie pro oblast kybernetické bezpečnosti, postižitelnosti kybernetické trestné činnosti, vzdělávací programy a osvětové aktivity a také funkční národní a vládní pracoviště CERT (Computer Emergency Response Team).



Obrázek 2: Hodnotící kritéria srovnávání kybernetické bezpečnosti Global Cybersecurity Index 2017. Zdroj: (Global Cybersecurity Index 2017, 2017)

Závěry, ke kterým obě srovnávací agentury dospěly, mají rozdílné výsledky z výše uvedených důvodů, což znázorňují Obrázky č. 3 a č. 4. Česká republika se umístila podle NCSI na 5. místě z 54 hodnocených zemí. V případě GCI zaujala Česká republika 35. příčku ze 165 států zahrnutých do srovnání. Pro srovnání je Německo podle NCSI první a podle GCI je až na 24. místě, Litva (dále srovnávaná forma bude uvedena jako NCSI/GCI) 2/57 pozice, Španělsko 3/54 pozice a Velká Británie na 4/14 pozice. Vzájemně nekorespondující výsledky lze přikládat tomu, že oblast kybernetické bezpečnosti má subjektivní vnímání, a to nejen v přístupu jednotlivých států, ale i hodnotících agentur a jejich metodik, existujících zákonů a standardů.

Rank	Country	NCSI Score	ISD Score	Ratio
1	Germany	**79.22**	81.95	-2.73
2	Lithuania	**77.92**	70.95	6.97
3	Spain	**77.92**	73.24	4.68
4	United Kingdom	**75.32**	83.96	-8.64
5	Czech Republic	**72.73**	69.37	3.36

Obrázek 3: Srovnání výsledků kybernetické bezpečnosti podle NCSI z 3. března 2018. Zdroj: (National Cyber Security Index, 2018)

Member State	Score	Global Rank
Singapore	0.925	1
United States of America	0.919	2
Malaysia	0.893	3
Oman	0.871	4
Estonia	0.846	5
Austria	0.639	30
Italy	0.626	31
China	0.624	32
Poland	0.622	33
Denmark	0.617	34
Czech Republic	0.609	35

Obrázek 4: Srovnání výsledků kybernetické bezpečnosti podle Global Cybersecurity Index 2017. Zdroj: (Global Cybersecurity Index 2017, 2017)

Oblast práva v oblasti kybernetické bezpečnosti v České republice představuje zákon č. 181/2014 Sb. o kybernetické bezpečnosti. Od 1. srpna 2017 funguje Národní Úřad pro Kybernetickou a Informační Bezpečnost (NÚKIB), který se novelou zákona číslo 205/2017 Sb., kterým změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti, vyčlenil z Národního bezpečnostního úřadu (dále také NBÚ). Úřad vznikl jako reakce na vzrůstající počet útoků na infrastrukturu a je autoritou v oblastech informační a kybernetické bezpečnosti. V této instituci pracují IT odborníci, právníci a další odborníci. Smyslem této instituce je podle (Jeziorský, 2017) „v prvé řadě prevence požáru, případně jeho rychlé uhašení". Oblasti hlavních činností, které NÚKIB vykonává je (Národní úřad pro kybernetickou a informační bezpečnost [NÚKIB] nedatováno a):

- provozovat Vládní CERT České republiky (GovCERT.CZ)
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy
- příprava bezpečnostních standardů pro informační systémy KII a VIS

- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti
- ochrana utajovaných informací v oblasti informačních komunikačních systémů
- kryptografická ochrana
- národní kontaktní místo PRS – jedna ze služeb evropského satelitního systému Galileo (NCPRS)

Mezi úkoly, které úřad vykonává, patří ochraňování fungování státu a jeho důležitých systémů, boj s kybernetickou kriminalitou a pátrání útočníků a ochrana národních utajovaných informací. Úřad se ve spolupráci s vysokými školami podílí na vzdělávání odborníků a také provozuje Kybernetický polygon. Cílem projektu KYPO je vytvoření prostředí pro školení, experimentování, zkoumání a vývoj metod k zajišťování bezpečnosti. Poznatky a zkušenosti mají přispět k ochraňování kritické informační infrastruktury proti útokům různých scénářů (Projekt Kybernetický polygon, nedatováno).

3.3 Vývoj regulace v oblasti kybernetické bezpečnosti v ČR

Běžnou praxí přijímání nových zákonů je, jak uvádí (Maisner, Vlachová, 2015), že regulovaná oblast již byla upravena existujícími právními předpisy. V případě vzniku zákona o kybernetické bezpečnosti takové regulace neexistovaly a autoři vytvářeli legislativní úpravu „na zelené louce“. Vznikal nový právní předpis, bez možnosti využití zkušeností s existující legislativou, která před tím regulovala oblast svého působení. Autoři se také museli vypořádat s nedostatkem judikatury. Před vznikem zákona o kybernetické bezpečnosti Česká republika řešila tuto oblast pomocí dokumentů, mezi které patří následující přehled, charakterizující vývoj v oblasti kybernetické bezpečnosti:

- Aktualizovaná koncepce boje proti organizovanému zločinu (2000)
- Koncepce boje proti trestné činnosti v oblasti informačních technologií (2001)
- Státní informační a komunikační politika e-Česko 2006 (2004)
- Národní strategie informační bezpečnosti České republiky (2005)
- Akční plán realizace opatření Národní strategie informační bezpečnosti České republiky (2007)
- Zřízení Mezirezortní koordinační rady pro oblast kybernetické bezpečnosti (2010)
- Memorandum o Computer Security Incident Response Team (CSIRT) České republiky se sdružením CZ.NIC

- Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011-2015 (2011)
- Přechod gesce nad kybernetickou bezpečností na NBÚ a zřízení Rady pro kybernetickou bezpečnost (2011)
- Schválení věcného záměru zákona o kybernetické bezpečnosti (2012)

Významnou úlohu měl při vzniku zákona Národní bezpečnostní úřad. Usnesením vlády České republiky č. 781 z 19. října 2011 byl Národní bezpečnostní úřad ustanoven národní autoritou a gestorem problematiky kybernetické bezpečnosti, a jako součást Národního bezpečnostního úřadu byl schválen vznik Národního centra kybernetické bezpečnosti. Dalším usnesením č. 382 ze dne 30. května 2012 vláda schválila návrh věcného záměru zákona o kybernetické bezpečnosti a zároveň bylo řediteli NBÚ uloženo předložit návrh zákona na základě věcného záměru. Věcný záměr říká, že *cílem zákona o kybernetické bezpečnosti je zvýšit bezpečnost kybernetického prostoru, nastavit mechanismus aktivní spolupráce mezi soukromým sektorem a veřejnou správou za účelem vyšší efektivity při řešení kybernetických bezpečnostních událostí a v této souvislosti zavést do praxe soubor oprávnění a povinností* (Věcný záměr zákona o kybernetické bezpečnosti, 2012, s. 6) a definuje kybernetickou bezpečnost jako *souhrn právních, organizačních, technických, fyzických a vzdělávacích opatření namířených na zajištění nerušeného a bezvadného fungování kybernetického prostoru* (Věcný záměr zákona o kybernetické bezpečnosti, 2012, s. 56).

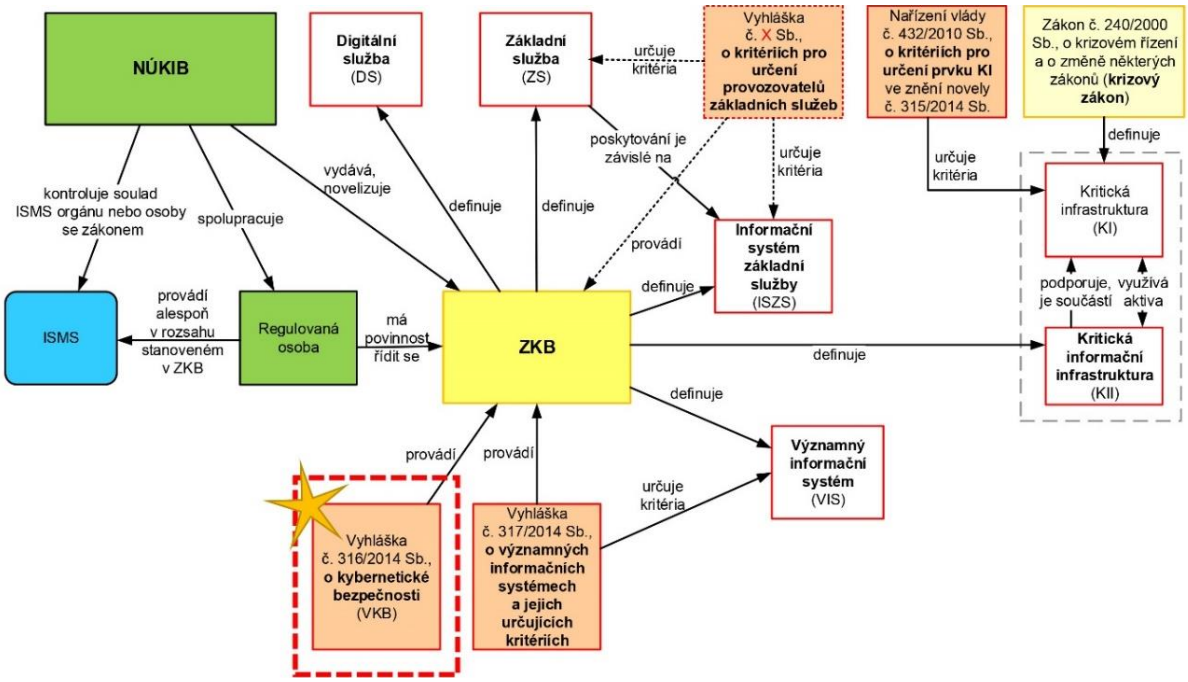
Předložený zákon byl po zapracování připomínek z Legislativní rady vlády přijat jako Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) (dále také ZoKB) s účinností tohoto zákona od 1. ledna 2015. Na tento zákon navazují jeho prováděcí vyhlášky 316/2014 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) (dále také VoKB) a vyhláška 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích. Zákon byl také již několikrát novelizován (podrobněji se novelám věnují kapitoly 3.4.1 Novely zákona a vyhlášek a také 3.4.2 Směrnice NIS) a stejně tomu je i v případě vyhlášek. NÚKIB na konci roku 2017 začal s přípravou novelizace vyhlášky 316/2014, do které se snažil zapojit i veřejnost. Cíle novelizace směřovaly k opravám chyb, celkovému zlepšení, aktualizace opatření a souladu s novelou ZoKB i směrnicí NIS (NÚKIB, nedatováno b). Národní bezpečnostní úřad také vypracoval na základě usnesení vlády č. 105 z 16. února 2015 Akční plán k dokumentu Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020, který má tyto hlavní cíle (Akční plán k Národní strategii kybernetické bezpečnosti, 2015):

- zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti
- aktivní mezinárodní spolupráce
- ochrana národní KII a VIS
- spolupráce se soukromým sektorem
- výzkum a vývoj / spotřebitelská důvěra
- podpora vzdělávání, osvěta a rozvoj informační společnosti
- podpora rozvoje schopností PČR vyšetřovat a postihovat informační kriminalitu
- právní úprava pro kybernetickou bezpečnost (vytváření právního rámce) účast na tvorbě a implementaci evropských a mezinárodních pravidel

Do budoucna lze předpokládat, že se zákon bude rozvíjet ve snaze předcházet novým formám útoků zapojením nových technologií detekce incidentů i útoků, rozšířením orgánů a osob, kteří se stanou povinnými subjekty, nebo povinností dodavatelů podílet se na řešení incidentů a jejich spolupráci při vydávání protiopatření a samozřejmě soulad platnou legislativou i s nařízeními EU.

3.4 Zákon o kybernetické bezpečnosti a jeho prováděcí vyhlášky

V předcházející kapitole byl vysvětlen vývoj regulací kybernetické bezpečnosti a orgánů, které dohlížejí na jejich dodržování. Dále bude zákon a jeho obsah diskutován podrobněji. Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Definuje a vymezuje důležité pojmy, práva a povinnosti pro povinné subjekty i Národní bezpečnostní úřad (Svatá, 2016). Na základě zákona 205/2017 Sb., v aktuálním, platném znění zákona 181/2014 Sb. o kybernetické bezpečnosti, přechází práva a povinnosti z Národního bezpečnostního úřadu na NÚKIB. Dále pro NÚKIB může být v následujícím textu používáno také označení Úřad, stejně tak je označován v zákoně i novelizovaných vyhláškách. Vyhláška č. 316/2014 Sb. o kybernetické bezpečnosti stále slovem Úřad myslí NBÚ. Tento stav bude novou vyhláškou upraven. Cílem zákona je zajištění bezpečného kybernetického prostoru, ochrana kritické informační infrastruktury a zajištění fungování státu, státní správy, základních potřeb obyvatel, ochrana zdraví a života lidí, zdravé ekonomiky a celkové stability. Ochrana kyberprostoru zajišťuje subjektům v české jurisdikci odpovídající nástroje a standardy pro řešení kybernetické bezpečnosti jejich sítí a systémů. Zákon o kybernetické bezpečnosti je, jak bylo uvedeno, prováděn vyhláškami 316/204, 317/2017 a dále vyhláškou 437/2017 Sb. Provázanost zákona a prováděcích vyhlášek zachycuje Obrázek č. 5.



Obrázek 5: Schematické znázornění vztahů k zákonu o kybernetické bezpečnosti: Zdroj: (Konečný, 2017)

3.4.1 Novely zákona a vyhlášek

Zákon o kybernetické bezpečnosti od nabytí účinnosti od 1. ledna 2015 byl několikrát novelizován. Poprvé byl měněn zákonem 104/2017 Sb. ze dne 8. března 2017 s účinností od 1. července téhož roku. Tato úprava zavádí pojem provozovatele systému, jakožto provozovatelé systému významného informačního systému (dále také VIS) nebo kritické informační infrastruktury (dále též KII) a patřičně byl upraven okruh povinných subjektů. Změna zákona subjekty opravňuje podle nového paragrafu § 6a odst. 1) pověřit jinou osobu nebo orgán provozováním funkčností zajišťujících technické a programové prostředky tvořící informační nebo komunikační systémy. Provozovatel má pak povinnosti podle zákona vůči správci, které se týkají předávání dat, provozních údajů a informací, po skončení provozování systémů data správci předat a zničit jejich kopie (Zákon č. 181/2014 Sb., 2018).

Změny v zákonu se týkají i řešení prohřešků vůči povinnostem provozovatele a Úřadu jsou dána práva, jenž může uplatnit k řízení sporu mezi správcem a provozovatelem, včetně sankcí, které může Úřad udělit podle § 25 ZoKB. Provozovatel je v rámci novelizace oprávněn hlásit bezpečnostní incidenty podle § 8. V rámci plnění přechodných ustanovení musí provozovatel oznámit kontaktní údaje, plnit povinnost hlásit bezpečnostní incidenty a zavést bezpečnostní opatření (Zákon č. 104/2017 Sb., 2017). Zákon č. 183/2017 Sb. a zákon č. 35/2018 Sb. nijak zásadně samotný zákon nemění, dotčena je jen formální úprava zákona a týká se záměny nadpisů a drobné korektury a změny (Zákon č. 183/2017 Sb., 2017).

Zatím poslední novelizace zákona o kybernetické bezpečnosti je provedena zákonem č. 205/2017 Sb., čímž se do českého legislativního prostředí (takzvanou transpozicí) zapracovala směrnice NIS (Network Information Security) a její opatření, která mají zajistit vysokou společnou úroveň bezpečnosti sítí a informačních systémů v Unii. Tato změna se výrazně dotkla celého zákona a byla zatím nejrozsáhlejší úpravou zákona o kybernetické bezpečnosti. Jsou zde kodifikovány především povinnosti a práva, které se týkají nových subjektů (provozovatel VIS nebo KII, správce a provozovatel základní služby a poskytovatel digitální služby), jakožto příjemců ZoKB, včetně změn paragrafů, dotčených rozšířením povinných subjektů. Novela se dotýká také práv a povinností Úřadu, přestupků a definic toho, jak se přestupku uvedená osoba dopustila, nebo systému udělování pokut a jejich výše (Zákon č. 205/2017 Sb., 2017).

Kromě zákona byla novelizovaná i vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích, a to vyhláškou č. 205/2016 Sb. Tato novela se dá bez nadsázky označit jako pouhá aktualizace. Ve dvou článcích je aktualizován seznam Významných informačních systémů, který je ve vyhlášce č. 317/2014 Sb. uveden jako příloha č. 1. Druhý článek stanovuje její účinnost, a to od 1. července 2016 (Vyhláška č. 205/2016 Sb., 2016).

Na přelomu roku 2017 a 2018 se připravovala také novela vyhlášky č. 316/ 20104 Sb. o kybernetické bezpečnosti. Přípravou se zabýval Národní úřad pro kybernetickou a informační bezpečnost, a k úpravám Úřad přizval odbornou veřejnost. Účinnost této nově připravované vyhlášky má být 10. května 2018 (NÚKIB, nedatováno c).

3.4.2 Směrnice NIS

Ve snaze zajistit jednotný přístup k zajištění minimální společné úrovně kybernetické bezpečnosti v Evropské unii byla Evropským parlamentem a Radou Evropské unie 6. července 2016 přijata směrnice NIS, tedy Směrnice Evropského parlamentu a Rady (EU) 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Jak uvádí (Duračinská, 2016) cílem směrnice je harmonizovat standardy u všech členských států, protože úroveň legislativy jednotlivých států je rozdílná. Směrnice v rámci minimální harmonizace umožňuje ponechat ta ustanovení, která jsou cílené k dosažení vyšší úrovně bezpečnosti. Od schválení a přijetí směrnice začala plynout transpoziční doba, což je období, ve kterém mají členské státy transponovat tuto směrnici do svého národního právního prostředí přijetím zákonů a prováděcích předpisů. Tato lhůta trvá do května roku 2018, tedy 21 měsíců od přijetí. Dalších 6 měsíců je pak vymezeno pro identifikaci provozovatelů základních služeb. V Tabulce č. 1 je

časová osa pro implementaci směrnice. V ní je uveden, jaký další postup a vývoj se týká směrnice NIS a v jakých termínech se tak má stát (Kučinský, 2016).

Tabulka 1: Průběh a výhled významných událostí spojených se směrnicí NIS.
Zdroj: (Directive on Security of Network and Information Systems, 2018)

Datum	Vstup v platnost + …	Milník
srpen 2016	-	Směrnice nabyla platnost
únor 2017	6 měsíců	Skupina pro spolupráci zahájila provoz
srpen 2017	12 měsíců	Přijetí provádění bezpečnostních a oznamovacích požadavků pro DSP
únor 2018	18 měsíců	Skupina pro spolupráci stanoví pracovní program
květen 2018	21 měsíců	Transpozice do národního práva
listopad 2018	27 měsíců	Lhůta pro členské státy, aby určily provozovatele základních služeb
květen 2019	33 měsíců (1 rok po transpozici)	Zpráva Komise posuzující soulad identifikace operátorů základních služeb členskými státy
květen 2021	57 měsíců (3 roky po transpozici)	Přezkoumání fungování směrnice ze strany Komise, se zvláštním zaměřením na strategickou a operační spolupráci, jakož i rozsah ve vztahu k provozovatelům základních služeb a poskytovatelům digitálních služeb

Skrze směrnici NIS se do zákona zařadily další subjekty, jimiž jsou provozovatelé základních služeb (PZS) a provozovatelé digitálních služeb (PDZ). Provozovatelé digitálních služeb jsou rozděleni do tří kategorií, a to na online tržiště, internetové vyhledavače a poskytovatele cloud computingu. Z těchto skupin, a jim nařízené regulace, budou vynechány podniky, které splňují kritérium mikropodniku (do 10 zaměstnanců a obratem či bilanční sumou do 2 milionu eur), nebo malého podniku (do 50 zaměstnanců a obratem či bilanční sumou do 10 milionu eur). Určení, kdo bude provozovatelem digitální služby, bude probíhat podle definic ze směrnice NIS. Evropská komise také zveřejnila prováděcí nařízení komise (EU) 2018/151 ze dne 30. ledna 2018, a tímto nařízením stanovuje pravidla pro uplatňování směrnice NIS. Toto nařízení (Prováděcí nařízení komise (EU) 2018/151, 2018) upřesňuje, co bude muset PDZ zohlednit při určování a přijímání opatření, které mají zajistit úroveň bezpečnosti sítí a informačních systémů a jaké parametry musí být zohledněny. Účinnost tohoto nařízení je od 10. května 2018 a je přímo aplikovatelné. Provozovatele základních služeb určuje Národní úřad pro kybernetickou a informační bezpečnost, a to podle vyhlášky č. 437/2017 Sb. Základní rozdělení je podle činností v odvětvích:

- energetika,
- doprava,
- bankovnictví,
- infrastruktura finančních trhů,

- zdravotnictví,
- vodní hospodářství,
- digitální infrastruktura a
- chemický průmysl.

Vyhláška (Vyhláška č. 437/2017 Sb., 2017) specificky definuje druh služby, speciální kritéria a upravuje odvětvová a dopadová kritéria pro každé z výše uvedených odvětví. Tato vyhláška je účinná od 1. února 2018.

Ze směrnice pro členské státy vyplývají také povinnosti (NIS Network Information Security, 2017):

- vytvořit národní rámce bezpečnosti sítí a informačních systémů, tj. strategii pro bezpečnost sítí a informačních systémů,
- zřídit tým/týmy CSIRT na národní úrovni,
- zřízení centrálního orgánu (ústřední kontaktní místo na úrovni Unie),
- účastnit se unijních kooperačních struktur – skupina pro spolupráci a síť CSIRT (CSIRT Network),
- zjistit, aby povinné subjekty přijaly nezbytná bezpečnostní opatření a hlásily incidenty,
- kontrolovat a vymáhat plnění povinností povinnými subjekty.

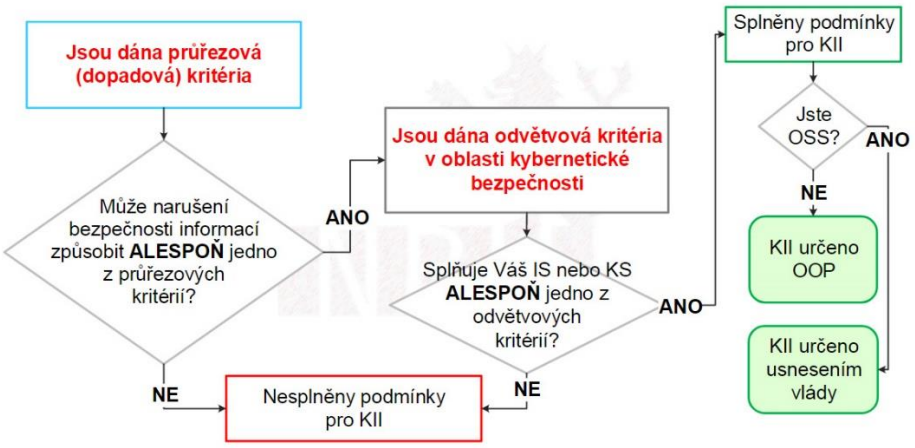
Směrnice NIS v České republice povede například i k tomu, že se sdružení CZ.NIC dotkne dvakrát, jako provozovatele základní služby registrující národní doménu nejvyšší úrovně, a jako národního CSIRT (Computer Security Incident Response Team) (Duračinská, 2016).

3.4.3 Další zákony a vyhlášky ve vztahu k ZoKB

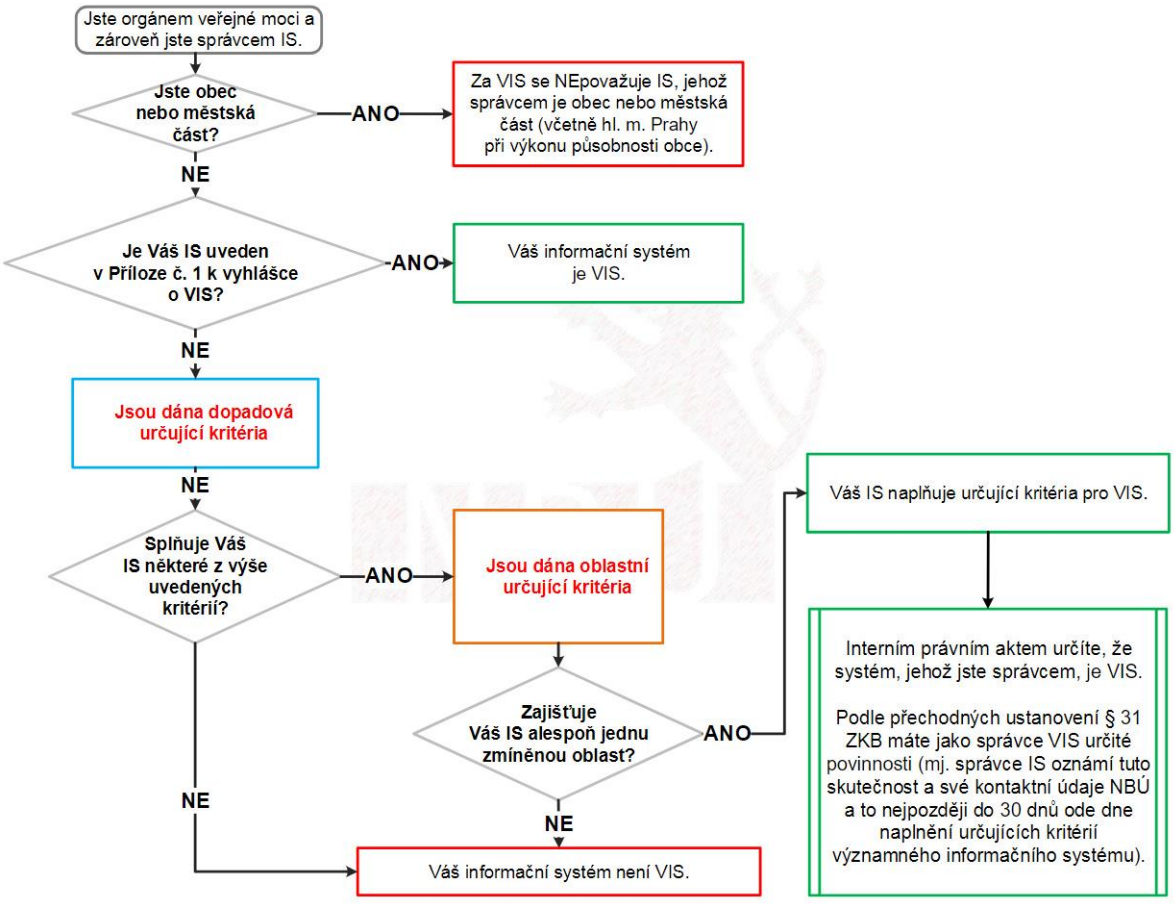
Zákon o kybernetické bezpečnosti z pohledu prováděcích vztahů a osob má dopad na správce a provozovatele VIS a KII a provozovatelé základních služeb. Významné informační systémy určuje vyhláška č. 317/2014 Sb. na základě dopadových a oblastních určujících kritérií. Součástí vyhlášky je příloha č. 1, která uvádí naplňující určující kritéria VIS. Pokud není subjekt součástí uvedeného seznamu, posuzuje naplnění určujících kritérií správce informačního systému. Proces určování subjektů významných informačních systémů je uveden na Obrázku č. 7.

Určení subjektů, které jsou v zákonu označovány jako správce a provozovatel informačního nebo komunikačního systému kritické informační infrastruktury, se provádí na základě nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury, jak zobrazuje Obrázek č. 6. Posuzovaná jsou kritéria, týkající se dopadu na lidské životy a zdraví, hospodářské ztráty, nebo

dopadu na veřejnost. Určení provozovatelů základních služeb je provedeno vyhláškou č. 437/2017 Sb.



Obrázek 6: Proces určení subjektů kritické infrastruktury. Zdroj: (Šmíd, nedatováno)



Obrázek 7: Proces určení subjektů VIS. Zdroj: (Šmíd, nedatováno)

Přijetí zákona o kybernetické bezpečnosti mělo také dopad na změny zákonů 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, 127/2005 Sb. o elektronických

komunikacích, 231/2001 Sb. o provozování rozhlasového a televizního vysílání a 106/1999 Sb. o svobodném přístupu k informacím.

3.4.4 Role

V rámci organizačních opatření je u subjektů KII a VIS podle § 6 odstavce 1 VoKB ustanoven výbor pro řízení kybernetické bezpečnosti, a jím jsou určeny bezpečnostní role, přičemž správce a provozovatel významného informačního systému tyto role určí přiměřeně. Role mohou vykonávat také externí subjekty (osobou s odbornou kvalifikací), jednotlivé role mohou přesahovat svým působením do jiných rolí, a také je možné, že jedna osoba může vykonávat více rolí současně. Jedinou výjimkou je role auditora. Tato role totiž musí být nezávislá na ostatních rolích řízení KB. Role v řízení kybernetické bezpečnosti (viz Obrázek č. 8) jsou:

- manažer kybernetické bezpečnosti,
- architekt kybernetické bezpečnosti,
- auditor kybernetické bezpečnosti,
- garant aktiva a
- role ve výboru KB.

Procesy	Výbor KB	Manažer KB	Architekt KB	Auditor KB	Garant (vlastník) aktiva
Celkové řízení a rozvoj KB	A	R	R		C
Systém řízení bezpečnosti informací	A	R	C		C
Návrh bezpečnosti informací	C	A	R		C
Implementace bezpečnosti informací	C	A	R		C
Zajištění rozvoje, použití a bezpečnosti aktiva		A	C		R
Audit KB	I	C	C	A/R	C

R - Responsible - je odpovědný
A - Accountable - je právně odpovědný
C - Consulted - konzultuje
I - Informed - je informován

Obrázek 8: RACI matice odpovědností za procesy řízení kybernetické bezpečnosti. Zdroj: (NUKIB, nedatováno d)

Auditor je osoba, která provádí audit kybernetické bezpečnosti. K výkonu této činnosti má potřebné vzdělání a praxi v provádění auditů KB minimálně 3 roky. Auditor v rámci svých povinností posuzuje soulad bezpečnostních opatření s právními předpisy, vnitřními předpisy, nebo jinými předpisy a smluvními závazky, vztahujícími se k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému. Určí opatření pro jeho prosazování, provádí a dokumentuje pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol zohlední v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik, a to nejméně jednou

ročně (Vyhláška č. 316/2014 Sb., 2016). Návrh nové vyhlášky ve svých přílohách uvádí doporučené požadavky na všechny role v řízení KB, včetně požadavků na znalosti, zkušenosti a praxi, doporučení na relevantní certifikáty nebo klíčové činnosti, které se týkají konkrétní role. Návrh nové vyhlášky je uveden v Příloze 1.

Svou významnou roli v rámci zákona má i Národní úřad pro kybernetickou a informační bezpečnost, který je ústředním správním úřadem nejen v oblasti kybernetické bezpečnosti, ale i oblasti, týkající se utajovaných informací podle příslušného zákona. Funkce, práva a povinnosti jsou Úřadu stanoveny zákonem o kybernetické bezpečnosti podle § 22.

3.4.5 Osoby

Jedním z možných způsobů, jak nahlížet na zákon a vyhlášku o kybernetické bezpečnosti, je pohled osoby, tedy povinného subjektu. Novela zákona o kybernetické bezpečnosti (provedená zákonem číslo 205/2017 Sb. zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění zákona č. 104/2017 Sb., a některé další zákony) rozšířila okruh orgánů a osob, kterým je v oblastech kybernetické bezpečnosti uložena povinnost dodržovat ze zákona vyplývající povinnosti. V dále uvedeném novelizovaném výčtu se jedná o orgány a osoby uvedené pod písmeny f) až h). Podle (Zákon č. 181/2014 Sb., 2018) jsou osoby a orgány vyjmenované v § 3 ZoKB:

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

V následující tabulce je souhrn povinností, které se týkají jednotlivých osob a znění těchto nařízení, jak jsou uvedena v zákoně o kybernetické bezpečnosti.

Tabulka 2: Povinnosti osob a orgánů podle § 3 ZoKB. Zdroj: (Zákon č. 181/2014 Sb., 2014)

Osoba podle § 3 ZoKB									Znění povinnosti
a	b	c	d	e	f	g	h	§	
							✔	3a	poskytovatel digitální služby, který poskytuje tuto službu v České republice, nemá sídlo v Evropské unii a neustavil si svého zástupce v jiném členském státě Evropské unie, je povinen ustavit si svého zástupce v České republice
		✔	✔	✔	✔			4	zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému a vést o nich bezpečnostní dokumentaci
							✔	4	zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby, přičemž tato bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, monitorování, audit, testování a soulad s mezinárodními předpisy
		✔	✔	✔	✔			4	zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži
		✔	✔	✔	✔	✔		4	ve smlouvě s poskytovatelem služeb cloud computingu zejména zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená Úřadem, a že budou mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro ně poskytovatel služeb cloud computingu uchovává včetně možnosti kontroly uchovávaných informací a dat v reálném čase
		✔	✔	✔	✔	✔		4	poskytovatel služby cloud computingu a uvedené orgány a osoby, které jsou orgány veřejné moci, si ve smlouvě dále dohodnou způsob a výši úhrady účelně vynaložených nákladů na zavedení bezpečnostních pravidel
		✔	✔	✔				4a	orgány a osoby, které se staly správci informačních nebo komunikačních systémů kritické informační infrastruktury nebo správci významných informačních systémů, a nejsou provozovateli tohoto systému, jsou povinny neprodleně a prokazatelně informovat provozovatele systému o této skutečnosti a o tom, že se tento provozovatel stal orgánem nebo osobou podle § 3 písm. c), d) nebo e)
		✔	✔					4a	orgány a osoby, které se staly správci nebo provozovateli informačních nebo komunikačních systémů kritické informační infrastruktury, jsou povinny neprodleně a prokazatelně informovat subjekt zajišťující síť elektronických komunikací, ke které je jejich předmětný informační nebo komunikační systém kritické informační infrastruktury připojen, o této skutečnosti a o tom, že se tento subjekt stal orgánem nebo osobou podle § 3 písm. b)

						✔		**4a**	orgány a osoby, které byly podle § 22a určené provozovateli základní služby a nejsou zároveň správci nebo provozovateli svých informačních systémů základní služby, jsou povinny správce nebo provozovatele tohoto informačního systému základní služby neprodleně a prokazatelně informovat o svém určení a o tom, že se dotčený správce nebo provozovatel stal orgánem nebo osobou podle § 3 písm. f)
	✔	✔	✔	✔	✔			**7**	povinnost detekovat kybernetické bezpečnostní události v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému
	✔	✔	✔	✔	✔			**8**	povinnost hlásit kybernetické bezpečnostní incidenty v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému, a to bezodkladně po jejich detekci; tím není dotčena informační povinnost podle jiného právního předpisu nebo přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů. V případě, že kybernetický bezpečnostní incident má významný dopad na kontinuitu poskytování základní služby, oznámí to provozovatel základní služby Národnímu úřadu pro kybernetickou a informační bezpečnost (Úřad)
							✔	**8**	bez zbytečného odkladu hlásit kybernetický bezpečnostní incident s významným dopadem na poskytování jeho služeb, pokud má přístup k informacím nezbytným pro posouzení významnosti tohoto dopadu
						✔		**8**	pokud má kybernetický bezpečnostní incident, který postihnul poskytovatele digitální služby, významný dopad na kontinuitu poskytování základní služby, je její provozovatel povinen tuto skutečnost Úřadu nahlásit.
	✔						✔	**8**	hlásí kybernetické bezpečnostní incidenty provozovateli národního CERT
		✔	✔	✔	✔	✔		**8**	hlásí kybernetické bezpečnostní incidenty Úřadu
✔	✔							**11**	provedení reaktivních opatření za stavu kybernetického nebezpečí nebo za nouzového stavu vyhlášeného na základě žádosti podle § 21 odst. 6
		✔	✔	✔	✔			**11**	provedení reaktivních opatření
		✔	✔	✔	✔			**11**	provedení ochranných opatření
✔	✔	✔	✔	✔	✔			**13**	bez zbytečného odkladu oznámit Úřadu provedení reaktivního opatření a jeho výsledek. Náležitosti oznámení stanoví prováděcí právní předpis
✔	✔						✔	**16**	kontaktní údaje a jejich změny oznamují provozovateli národního CERT
		✔	✔	✔	✔	✔		**16**	kontaktní údaje a jejich změny oznamují Úřadu
		✔	✔	✔	✔	✔		**16**	oznamují změny pouze těch údajů podle odstavce 1, které nejsou referenčními údaji vedenými v základních registrech, a to neprodleně
✔	✔							**29**	oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona
	✔							**29**	začnou plnit povinnost stanovenou v § 8 odst. 1 a 2 nejpozději do 1 roku ode dne nabytí účinnosti tohoto zákona

		✔	✔					**30**	oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou, začnou plnit povinnost stanovenou v § 8 odst. 1 a 4 nejpozději do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou a zavedou bezpečnostní opatření podle § 4 odst. 2 nejpozději do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou
				✔				**31**	oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne naplnění určujících kritérií významného informačního systému jejich informačních systémů, začnou plnit povinnost stanovenou v § 8 odst. 1 a 4 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému a zavedou bezpečnostní opatření podle § 4 odst. 2 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému.
		✔	✔	✔				**38**	oznámí kontaktní údaje podle § 16 zákona č. 181/2014 Sb. nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona; začne plnit povinnost stanovenou v § 8 odst. 1 a 3 zákona č. 181/2014 Sb. nejpozději do 6 měsíců ode dne nabytí účinnosti tohoto zákona a zavede bezpečnostní opatření podle § 4 odst. 2 zákona č. 181/2014 Sb. nejpozději do 6 měsíců ode dne nabytí účinnosti tohoto zákona. V případě zavedení bezpečnostních opatření má provozovatel nárok na úhradu nákladů spojených s přijetím bezpečnostního opatření; náklady provozovateli uhradí správce daného systému.
					✔			**38**	oznámí Úřadu do 30 dnů ode dne, kdy byly informovány podle § 4a odst. 3 zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, kontaktní údaje podle § 16 odst. 1 zákona č. 181/2014 Sb., ve znění účinném ke dni nabytí účinnosti tohoto zákona, a začnou nejpozději do 1 roku ode dne, kdy byly informovány podle § 4a odst. 3 zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, plnit ostatní povinnosti podle zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona; začnou nejpozději do 1 roku ode dne, kdy byly informovány podle § 4a odst. 3 zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, plnit ostatní povinnosti podle zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona
							✔	**38**	začne nejpozději do 1 roku ode dne nabytí účinnosti tohoto zákona plnit ostatní povinnosti podle zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona
		✔	✔	✔	✔			**38**	v případě, že podmínky jejich smluvního vztahu uzavřeného s dodavatelem pro jejich informační nebo komunikační systém nesplňují požadavky podle zákona č. 181/+B32:K512014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, a jeho prováděcích právních předpisů, uvést smluvní vztah do souladu s těmito požadavky do 1 roku ode dne nabytí účinnosti tohoto zákona

Prováděcí vyhláška 316/2014 Sb. o bezpečnostních opatření, kybernetických bezpečnostních incidentů, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) se věnuje hlavně osobám § 3 písm. c) a e) a zaměřuje se tedy na správce a provozovatele informačního nebo komunikačního systému kritické informační infrastruktury a správce a provozovatele významného informačního systému.

3.4.6 Opatření v zákonu a vyhlášce

Pro zaměření této práce je právě vyhláška o kybernetické bezpečnosti jedním z nejvýznamnějších dokumentů.

Zákon dělí opatření na organizační a technická. Na základě zmocňovacího ustanovení Úřad stanovuje jejich obsah a rozsah vyhláškou, která obsahuje prováděcí předpisy jednotlivých opatření. Zmiňovanou vyhláškou je vyhláška č. 316/2014 Sb., která má být novelizována v rámci provedení souladu se směrnicí NIS. Novela poměrně značně mění dopad pro významné informační systémy a bude mít dopad i na znění zákona (konkrétně § 5 ZoKB). Změny struktury opatření jsou uvedeny v Tabulce č. 3. Tato změna není nijak rozsáhlá, výraznější změny jsou v jednotlivých opatřeních. Zatímco ve vyhlášce 316/2014 Sb. je pro většinu opatření charakteristická dvojí úroveň konkrétních nařízení (z pohledu VIS a KII), novela vyhlášky rozdíly mezi VIS a KII významně omezuje. Rozdíly mezi VIS a KII, které z novely vyhlášky vyplývají jsou pouze tyto:

- subjekty podle § 3 písm. c), d) a f) zákona provedou hodnocení rizik alespoň jednou ročně, subjekty VIS hodnocení rizik provedou alespoň jednou za tři roky,
- subjekty podle § 3 písm. c), d) a f) zákona stanoví bezpečnostní role (garanty aktiv, auditora, manažera a architekta KB), subjekty VIS určí roli manažera kybernetické bezpečnosti, ostatní role určí přiměřeně okolnostem,
- subjekty podle § 3 písm. c), d) a f) zákona zajistí zastupitelnost bezpečnostních rolí, subjekty VIS zajistí jen zastupitelnost bezpečnostní role manažera kybernetické bezpečnosti,
- subjekty podle § 3 písm. c), d) a f) zákona na základě výsledků analýzy rizik podle odstavce 2 písm. b) rozhodnou o provedení penetračního testování nebo testování zranitelností, subjekty VIS se řídí požadavky přiměřeně,
- subjekty podle § 3 písm. c), d), f) a g) zákona při detekci kybernetických bezpečnostních událostí dále používají nástroje podle § 24, tato povinnost se subjektů VIS netýká,
- audit provádí subjekty VIS v pravidelných intervalech alespoň po 3 letech, v pravidelných intervalech alespoň po 2 letech v případě orgánu nebo osoby, které nejsou VIS,
- subjekty podle § 3 písm. c), d) a f) zákona v rámci ochrany před škodlivým provádí ochranná opatření podle nařízení, subjekty VIS tak učiní přiměřeně,
- subjekty podle § 3 písm. c), d) a f) zákona uchovávají záznamy událostí nejméně po dobu 24 měsíců, subjekty VIS je uchovávají nejméně po dobu 12 měsíců,

- subjekty podle § 3 písm. c), d) a f) zákona zajistí detekci kybernetických bezpečnostních událostí v rámci koncových stanic, mobilních zařízení, serverů, datových úložišť a výměnných datových nosičů, síťových aktivních prvků a obdobných aktiv, tato povinnost se subjektů VIS netýká,
- subjekty podle § 3 písm. c), d) a f) zákona používají nástroje pro průběžné vyhodnocení a sběr kybernetických bezpečnostních událostí, tato povinnost se subjektů VIS netýká.

Tabulka 3: Opatření ve vyhlášce 316/2014 Sb. a její chystané aktualizace.
Zdroj: Příloha č. 1 a (Vyhláška č. 316/2014 Sb., 2014)

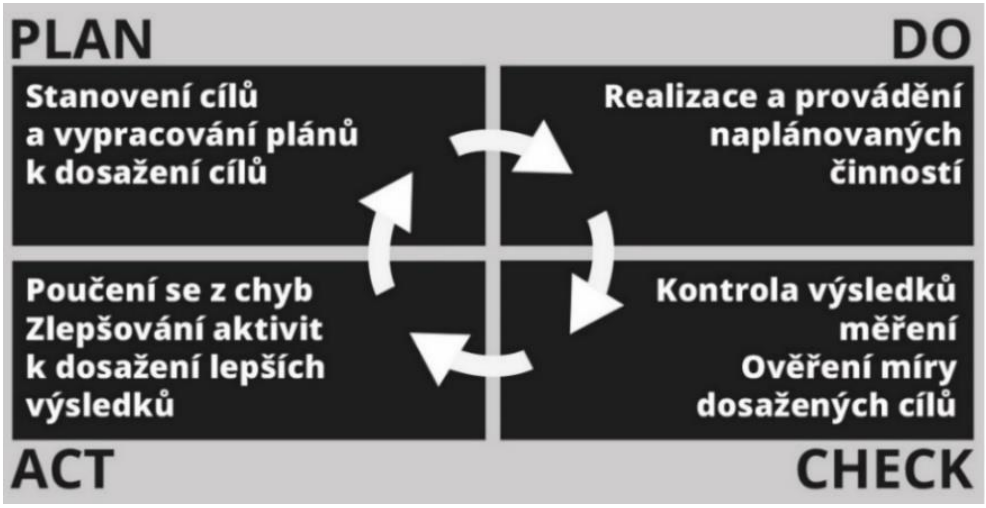
Opatření	316/2014 Sb.	Draft
Organizační		
systém řízení bezpečnosti informací	✓	✓
řízení rizik	✓	✓
bezpečnostní politika	✓	✗**
organizační bezpečnost	✓	✓
stanovení bezpečnostních požadavků pro dodavatele	✓	✓
řízení aktiv	✓	✓
bezpečnost lidských zdrojů	✓	✓
řízení provozu a komunikací	✓	✓
řízení přístupu a bezpečné chování uživatelů	✓	✓
akvizice, vývoj a údržba	✓	✓
zvládání kybernetických bezpečnostních událostí a incidentů	✓	✓
řízení kontinuity činností	✓	✓
kontrola a audit kritické informační infrastruktury a významných informačních systémů	✓	✓
bezpečnostní role	✗	✓
řízení změn	✗	✓
Technická		
fyzická bezpečnost	✓	✓
nástroj pro ochranu integrity komunikačních sítí	✓	✓
nástroj pro ověřování identity uživatelů	✓	✓
nástroj pro řízení přístupových oprávnění	✓	✓
nástroj pro ochranu před škodlivým kódem	✓	✓
nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů	✓	✓
nástroj pro detekci kybernetických bezpečnostních událostí	✓	✓
nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	✓	✓
aplikační bezpečnost	✓	✓
kryptografické prostředky	✓	✓
nástroj pro zajišťování úrovně dostupnosti	✓	✓
bezpečnost průmyslových a řídících systémů	✓	✓
digitální služby*	✗	✓

* - opatření týkající se poskytovatele digitální služby
** - bezpečnostní politika, není součástí opatření, ale je nařízením vyhlášky

3.5 Systém řízení informační bezpečnosti

Systém řízení informační bezpečnosti neboli ISMS (Information Security Management System) je součástí organizačních opatření, které je uvedeno ve VoKB v § 3 této vyhlášky. Je založen na přístupu k řízení rizik a při tom se využívají principy Demingova modelu PDCA (Plan – Do – Check – Act), který má čtyři etapy (Ondrák, Sedlák, Mazálek, 2013):

- ustavení ISMS (určuje rozsah a odpovědnosti),
- zavádění a provoz ISMS (prosazení vybraných bezpečnostních opatření),
- monitorování a přezkoumání ISMS (zajištění zpětné vazby a hodnocení řízení),
- údržba a zlepšování (odstraňování slabin a soustavné zlepšování).



Obrázek 9: PDCA cyklus podle ISO 27000.

Standardem systému řízení informační bezpečnosti je norma ISO 27001, která stanovuje požadavky bezpečnosti a je výchozím souborem kritérií pro certifikaci a audity. Splnění těchto požadavků organizace prokazuje odpovědnost k řízení bezpečnosti informací všem zainteresovaným stranám a buduje vzájemnou důvěru. Efektivní zavedení ISMS využívá základní principy, jako je povědomí o potřebě informační bezpečnosti, určení odpovědností, posuzování rizik a přijetí opatření pro dosažení přijatelné úrovně rizika a zajištění komplexního přístupu k řízení informační bezpečnosti a neustálé zlepšování ISMS.

Bezpečnost je důležitým a neoddělitelným prvkem provozování systémů a sítí, který nebývá vždy brán v úvahu při návrhu a vývoji informačních systémů a je pokládán za technické řešení (ISO 27001, 2014). To je však omezující řešení a může být neúčinné, pokud není podporováno vhodným systémem ISMS. Přijetí systému ISMS by mělo být strategickým rozhodnutím a je nezbytné, aby rozhodnutí bylo snadno integrováno, měřeno a aktualizováno v souladu s potřebami organizace. Při implementaci ISMS je třeba brát v úvahu strukturu, velikost, požadavky na bezpečnost, procesy, cíle a potřeby organizace a musí odrážet zájmy všech zúčastněných stran, jakými jsou zákazníci, dodavatelé, partneři a stakeholdeři (ISO 27001, 2014).

Pokud je systém řízení informační bezpečnosti správně zavedený a zásady bezpečnosti jsou dodržovány, poskytuje tyto přínosy (Tobolka, 2012):

- zabezpečení informací je integrální částí celého systému řízení organizace,
- hlavní faktory ovlivňující podnikatelskou soutěž, informace a jejich zabezpečení jsou v řízeném režimu,
- zaměstnanci jsou odpovědni za zabezpečení informací svých pracovišť i dat svých zákazníků,
- požadavek na kontinuální zlepšování zaručuje dlouhodobě efektivní řízení nákladů,
- prokázání přístupu k managementu bezpečnosti informací, a to i v komunikaci se zákazníky, investory, občanskou veřejností, státními i soukromými institucemi a dalšími zainteresovanými stranami,
- zprůhlednění důsledků incidentů a jejich snížení, odhalování rizik, neshod a incidentů s nežádoucími dopady na důvěrnost, integritu a dostupnost informací a tím i na chod organizace,
- zvýšení podnikatelské důvěryhodnosti pro investory, banky a pojišťovny,
- úspora na pokutách a jiných sankcích, spojených s únikem informací.

3.6 Normy ISO

Sada norem ISO 27000 se zabývá systémem informační bezpečnosti, a se zákonem o kybernetické bezpečnosti má společné to, že organizační a technická opatření zmíněná v ZoKB z normy ISO 27001 vycházejí. Souvisí i možností, že lze prokázat splnění požadavků zákona a vyhlášky certifikací provedenou akreditovaným certifikačním orgánem ve znění § 29 VoKB nebo podle § 3 odst. 2 novely vyhlášky. Základní strukturu norem zachycuje Obrázek č. 10 a jsou v něm naznačeny návaznosti jednotlivých norem právě na normu ISO 27001, která *specifikuje požadavky na ustavení, implementování, udržování a neustále zlepšování systému řízení bezpečnosti informací v rámci kontextu organizace* (ISO 27001, 2014, s. 7).

ISO 27000 – Tento dokument obsahuje definici základních termínů z oblasti bezpečnosti informací používaných v celé sadě ISO 27000. Obrázek č. 10 zobrazuje strukturu a provázanost jednotlivých norem v rámci ISMS.

ISO 27001 – Obsahem této normy je definice požadavků na bezpečnost informací. Vůči této normě se posuzuje splnění požadavků na vytvoření, implementaci, provoz, sledování, revize, udržování a zlepšování systémů řízení bezpečnosti informací v kontextu rizik organizace a stanovuje požadavky na provádění bezpečnostních kontrol. Jednotlivé cíle a opatření jsou odvozeny z normy ISO 27002.

ISO 27002 – Tato norma definuje opatření bezpečnosti informací pro 35 hlavních kategorií a obsahuje114 kontrol. Je souborem best pracitce opatření (nejlepších postupů) pro bezpečnost informací.

ISO 27003 – Účelem této normy je podpora zavedení procesu řízení bezpečnosti informací, aby bylo možné zainteresovaným stranám poskytnout ujištění o udržování rizik v přijatelných mezích. Doporučení uvedená v této normě poskytují rady, jak postupovat při vývoji plánu zavádění pro ISMS v souladu s normou ISO 27001. Další doporučení se věnují projektu zavádění systému ISMS do organizace a věnuje se kritickým aspektům úspěšného návrhu a zavádění.

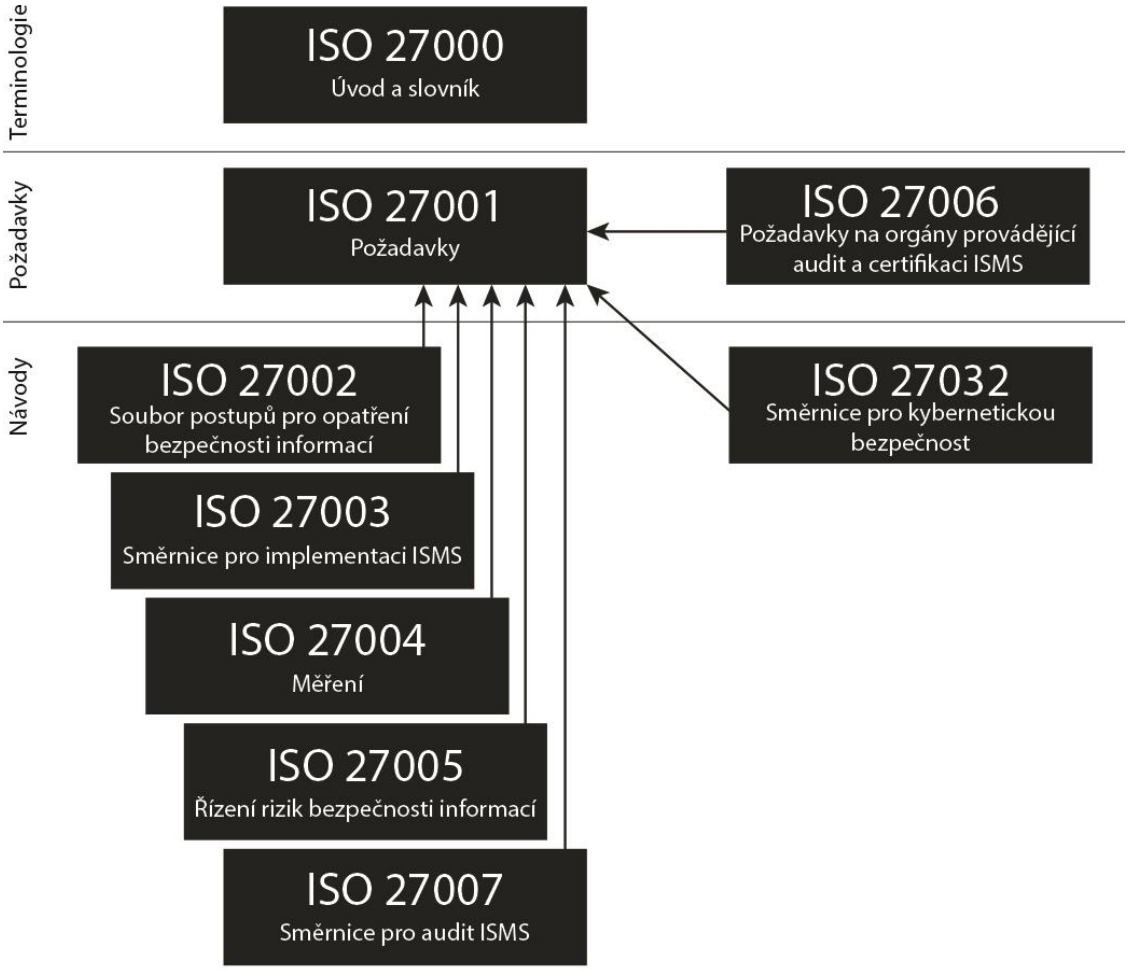
ISO 27004 – Poskytovaná doporučení v této normě se zaměřují na vývoj a používání metrik, která hodnotí účinnost zavedení systému ISMS a opatření, či skupin opatření.

ISO 27005 – Doporučení této normy se zaměřují na řízení rizik bezpečnosti informací v kontextu organizace a podporují koncept specifikovaný v ISO 27001. Norma se věnuje se identifikaci aktiv, hrozeb, stávajících opatření, zranitelnosti a následků jako identifikaci rizik pro následnou analýzu a hodnocení rizik a jejich ošetření.

ISO 27006 – Tato norma obsahuje doporučení pro orgány, které vykonávají audit a certifikaci systémů ISMS, doplňuje a rozšiřuje normu ISO 17021-1 (Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu – Část 1: Požadavky) a ISO 27001. Je určena k podpoře procesu akreditace certifikačních orgánů poskytujících certifikaci ISMS, a je možné ji použít jako kriteriální dokument pro akreditaci, interní hodnocení nebo jiné auditní procesy.

ISO 27007 – V této normě jsou uvedeny doporučení pro řízení programu auditu ISMS a provádění auditů v souladu s ISO 27001. Jsou zde uvedena doporučení navazující na normu ISO 19011 (směrnice pro auditování systémů managementu) a smyslem normy ISO 27007 je uvést audit systémů managementu do kontextu bezpečnosti informací a upřesnit konkrétní oblasti pro auditování ISMS.

ISO 27032 – Obsahem této normy jsou doporučení pro zlepšení stavu kybernetické bezpečnosti. Věnuje se technickým opatřením, zahrnující přípravu na útoky, detekování a monitorování útoků a reakce na útoky. Zaměřuje se také na spolupráci, která musí probíhat bezpečným způsobem, a poskytuje i rámec pro sdílení informací, koordinaci a zvládání incidentů.



Obrázek 10:Sada norem ISO 27000 a provázanost jednotlivých norem. Zdroj: (ISO 27000, 2009)

3.7 Obecné nařízení o ochraně osobních údajů

Informační bezpečnost podle zákona o kybernetické bezpečnosti a standardu ISO 27001 má ke GDPR (General Data Protection Resolution neboli Obecné nařízení o ochraně osobních údajů) blízko tím, že jedním z cílů je právě zajištění ochrany dat před neoprávněným přístupem a vytváří vhodné výchozí postavení, aby byly splněny požadavky GDPR a zajištění souladu s ním (Co přináší GDPR a jak je možné využít ISO 27001 a ZKB, nedatováno).

Přijetí normy ISO 27001 a soulad s touto směrnicí má za jeden z hlavních cílů minimalizovat rizika, týkající se bezpečnosti informací, a je tedy dobrým výchozím bodem k dosažení požadavků na ochranu osobních údajů podle GDPR. Využívají se k tomu přijatá opatření a politiky, která prováděním kontrol a testováním mají poskytovat důvěru a ujištění o skutečné bezpečnosti. Pravidelnou aktualizací plánů, které mají zajišťovat bezpečnost i aktualizací celého ISMS, probíhá neustále zlepšování bezpečnosti. Reaguje se tak na rizika, která vyplývají z vývoje prostředí, čímž poskytuje ucelený pohled na zabezpečení informací v organizaci. Normy ISO 27000 využívají soubor zásad, postupů, technologií a dokumentů týkajících se bezpečnosti informací, a v rámci

ISMS pomáhají řídit rizika, sledovat stav bezpečnosti prostřednictvím auditů a zlepšovat úroveň zabezpečení, týkající se nejen osobních údajů. Soulad s normami ISO 27000 dává najevo, že organizace podnikla kroky v oblastech bezpečnosti informací a přijala vhodná opatření ke zmírnění rizik, což lze doložit také certifikací – prokazatelným důkazem o přijetí nezbytných opatření a splnění požadavků na informační bezpečnost, zahrnující i ochranu osobních údajů pro ověření souladu s GDPR (EU General Data Protection Regulation - A Compliance Guide, 2016).

Obecné nařízení o ochraně osobních údajů je právní rámec, působící v evropském (unijním) prostoru, a souvisí se zpracováváním osobních údajů. Posláním tohoto rámce je především posílením práv občanů proti neoprávněnému zacházení s osobními údaji prostřednictvím organizačních, technických a bezpečnostních opatření pro používání a pohyby osobních údajů, které organizace musí zavést a realizovat, aby tato opatření vyhovovala požadavkům zákona potažmo nařízení. Implementace opatření obnáší určité náklady a vyžaduje potřebný čas na změny, které mohou být velmi náročné. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) nabude účinnosti 25. května 2018, a tím dojde ke změně legislativy českého právního systému, kterou v této oblasti představuje zákon č. 101/2000 Sb., o ochraně osobních (Žůrek, 2017). Nabytí účinnosti závisí hlavně na schopnosti včas zákon zavést.

Od přijetí směrnice v dubnu roku 2016 začalo přechodné období, které má poskytnout dostatečně dlouhou dobu zpracovatelům a správcům osobních údajů, aby došlo k uplatnění principu zodpovědnosti. Podle (Škorničková, nedatováno a) se týká oblastí:

- implementace záměrné a nezbytné ochrany dat,
- vypracování posouzení vlivu na ochranu osobních údajů neboli DPIA (Data Protection Impact Assessment),
- jmenování pověřence pro ochranu osobních údajů DPO (Data Protection Officer),
- zavedení tzv. pseudonymizace osobních údajů,
- vedení záznamů o činnostech zpracování,
- konzultace s dozorovým orgánem před samotným zpracováním osobních údajů.

V souvislosti s GDPR nelze vynechat definici co jsou podle této regulace osobní údaje. Za osobní údaje jsou považovány všechny informace, které se vztahují k identifikované, či identifikovatelné fyzické osobě. Které informace vedou k identifikaci nebo identifikovatelnosti nejsou taxativně

vymezeny. (Škorničková, nedatováno b) uvádí, že takové informace jsou samozřejmě jméno, pohlaví, věk a datum narození nebo osobní stav. Osobními údaji jsou:

- IP adresy,
- fotografický záznamy,
- genetické informace, analýzy biologických vzorků a osobní údaje dětí,
- biometrické údaje – tedy údaje, vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby,

a dále jsou to údaje o:

- rasovém či etnickém původu,
- politických názorech,
- náboženském nebo filozofickém vyznání,
- členství v odborech,
- zdravotním stavu,
- sexuální orientaci,
- trestních deliktech či pravomocném odsouzení.

Údaje, které jsou vyloučeny z působnosti GDPR jsou anonymizované údaje, údaje zemřelých osob a údaje zpracovávané pro osobní potřebu, pokud nebudou sdílené jiným osobám.

Nedodržení požadavků nebo jejich porušení pro povinné subjekty znamená, že jim může být uložena vysoká pokuta, která může být pro některé organizace likvidační. Udělení výše pokuty je ovlivněna několika faktory podle závažnosti porušení zásad. Přitom není přihlíženo k tomu, zda se jedná o organizaci s tisíci zaměstnanci nebo firmu s méně než deseti zaměstnanci. Maximální výše pokuty je 20 milionů eur nebo 4 % z celkového ročního obratu, přičemž se ukládá pokuta, která z nich je vyšší (Škorničková, nedatováno c).

3.8 Bezpečnostní dokumentace a bezpečnostní politika

Vyhláška 316/2014 Sb., resp. příloha vyhlášky č. 4 stanovuje doporučený obsah a strukturu bezpečnostní dokumentace a bezpečnostní politiky. Navrhovaná struktura je nezávazná a přístup, který povinné subjekty[4] zaujmou, je vždy na samotné organizaci. Jejich povinností je dodržení nařízení bezpečnostních opatření, které ukládá zákon, to je zavést a provádět bezpečnostní

[4] orgány nebo osoby uvedené v § 3 písm. c) až e) zákona

opatření a vést o nich bezpečnostní dokumentaci. To vyhláška doplňuje o požadavek, aby záznamy o provedených činnostech byly úplné, čitelné, snadno identifikovatelné, a aby se daly snadno vyhledat. Vyhláškou navrhovaná struktura zahrnuje témata jednotlivých dokumentů, která pokrývají určitou oblast. Tato doporučení shrnuje Tabulka č. 4. Organizace mohou strukturu přizpůsobovat, a tak bezpečnostní dokumentace nemá svůj standard, což ztěžuje objektivní a nezávislé posouzení. Bezpečnostní dokumentace v organizaci slouží jako rámec pro implementaci a řízení bezpečnosti. Je souborem zásad a pravidel, která utvářejí základní aspekty bezpečnosti a definují jasná pravidla práce s informačním systémem i s informacemi, jako takovými. Zpracování bezpečnostní dokumentace odpovídá charakteristikám organizací a všem okolnostem, které na bezpečnost působí. (Bezpečnostní dokumentace, nedatováno) uvádí jako příklad obsahu dokumentace tuto strukturu[5]:

- úvod, účel a definice pojmů,
- odpovědnosti a bezpečnostní zásady,
- organizování bezpečnosti,
- řízení a klasifikace aktiv,
- personální a fyzická bezpečnost,
- správa systémů,
- řízení přístupu,
- havarijní plánování,
- řízení používání software a používání informačního systému.

Jednou z oblastí posuzování pro certifikaci podle zákona č. 412/2005 Sb. pro nakládání s utajovanými informacemi je právě bezpečnostní dokumentace. Při její tvorbě lze vycházet ze zásad, které uvádí (Zásady tvorby bezpečnostní dokumentace informačních systémů určených k nakládání s utajovanými informacemi, 2017) pro systémy nakládající s utajovanými informacemi, které jsou provozovány v režimu stupně utajení Vyhrazené. V tomto pojetí jsou dokumenty vzájemně provázané a navazují na sebe. Dokumenty jsou seskupeny do oblastí bezpečnostní politiky, analýzy rizik, návrhu bezpečnosti a směrnic bezpečnosti.

Vyhláška, která nahradí vyhlášku č. 316/2014 Sb., mění pohled na bezpečnostní dokumentaci i bezpečnostní politiku. Rozdíly mezi oběma vyhláškami zachycuje Tabulka č. 4. formou změn. Tabulka zobrazuje změny z pohledu nové podoby vyhlášky. Nové pasáže jsou zobrazeny červenou

[5] tato struktura je ve zkrácené a upravené podobě

kurzívou. Vzhledem k tomu, že bezpečnostní dokumentace a bezpečnostní politika podle nové vyhlášky nerozděluje opatření na VIS a KII, tak i nová opatření již nejsou označena symbolem, kterých subjektů se týká. Vše, co bylo zrušeno nebo aktualizováno, je označeno přeškrtnutím, kde aktualizovaná část navazuje na změněnou část. Tímto způsobem lze tabulku použít k popisu bezpečnostní dokumentace a bezpečnostní politiky obou vyhlášek a zároveň sledovat, jaké změny mají nastat s účinností nové vyhlášky. Tabulka ale souběžně nezobrazuje oblasti rozdělené na doporučení pro bezpečnostní dokumentaci a pro bezpečnostní politiky kvůli přesunům a přejmenování některých oblastí. Názvy oblastí jsou uvedeny podle nové vyhlášky.

Tabulka 4: Doporučení struktura bezpečnostní dokumentace a bezpečnostní politika podle doporučení z vyhlášky 316/2014 ve srovnání s připravovanou novou podobou vyhlášky. Zdroj: Příloha č. 1 a (Vyhláška č. 316/2014 Sb., 2014)

Oblast	KII	VIS	Podrobné znění politiky nebo oblasti dokumentace
politika systému řízení bezpečnosti informací	✔	✔	a) Cíle, principy a potřeby řízení bezpečnosti informací. *b) Deklarace vrcholového vedení o vůdčí roli a závazku k řešení systému řízení bezpečnosti informací.* ~~b)~~ c) Rozsah a hranice systému řízení bezpečnosti informací. ~~c)~~ d) Pravidla a postupy pro řízení dokumentace. ~~d)~~ e) Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací. ~~e)~~ f) Pravidla a postupy pro provádění auditů kybernetické bezpečnosti. ~~f)~~ g) Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací. ~~g)~~ h) Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.
politika organizační bezpečnosti **	✔	✔	a) Určení bezpečnostních rolí a jejich práv a povinností, ~~1. práva a povinnosti manažera kybernetické bezpečnosti,~~ ~~2. práva a povinnosti architekta kybernetické bezpečnosti,~~ ~~3. práva a povinnosti auditora kybernetické bezpečnosti,~~ ~~4. práva a povinnosti garanta aktiv,~~ ~~5. práva a povinnosti výboru pro řízení kybernetické bezpečnosti.~~ b) Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí.
politika řízení dodavatelů **	✔	✔ *	a) Pravidla a principy pro výběr dodavatelů. ~~b) Pravidla pro hodnocení rizik dodavatelů.~~ b) Pravidla pro hodnocení rizik souvisejících s dodavateli. c) Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti. d) Pravidla pro provádění kontroly zavedení bezpečnostních opatření. e) Pravidla pro hodnocení dodavatelů.
politika řízení aktiv **	✔	✔	a) Identifikace, hodnocení a evidence primárních aktiv 1. určení a evidence jednotlivých primárních aktiv včetně určení jejich garanta, 2. hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti. b) Identifikace, hodnocení a evidence podpůrných aktiv 1. určení a evidence jednotlivých podpůrných aktiv včetně určení jejich garanta, 2. určení vazeb mezi primárními a podpůrnými aktivy. c) Pravidla ochrany jednotlivých úrovní aktiv 1. způsoby rozlišování jednotlivých úrovní aktiv, 2. pravidla pro manipulaci a evidenci aktiv podle úrovní aktiv, 3. přípustné způsoby používání aktiv. ~~d) Způsoby spolehlivého smazání nebo ničení technických nosičů dat.~~ d) Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií.
politika bezpečnosti lidských zdrojů **	✔	✔	a) Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení 1. způsoby a formy poučení uživatelů, 2. způsoby a formy poučení garantů aktiv, 3. způsoby a formy poučení administrátorů, 4. způsoby a formy poučení dalších osob zastávajících bezpečnostní role. b) Bezpečnostní školení nových zaměstnanců.

			c) Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací. d) Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice. 1. vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu, 2. změna přístupových oprávnění při změně pracovní pozice.
politika řízení provozu a komunikací **	✔	✔	a) Pravomoci a odpovědnosti spojené s bezpečným provozem. b) Postupy bezpečného provozu. c) Požadavky a standardy bezpečného provozu. ~~d) Řízení technických zranitelností.~~ ~~e)~~ d) Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů.
politika řízení přístupu **	✔	✔	a) Princip minimálních oprávnění/potřeba znát (need to know). b) Požadavky na řízení přístupu. c) Životní cyklus řízení přístupu. d) Řízení privilegovaných oprávnění. e) Řízení přístupu pro mimořádné situace. f) Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.
politika bezpečného chování uživatelů	✔	✔	a) Pravidla pro bezpečné nakládání s aktivy. b) Bezpečné použití přístupového hesla. c) Bezpečné použití elektronické pošty a přístupu na internet. d) Bezpečný vzdálený přístup. e) Bezpečné chování na sociálních sítích. f) Bezpečnost ve vztahu k mobilním zařízením.
politika zálohování a obnova **	✔	✔	a) Požadavky na zálohování a obnovu. b) Pravidla a postupy zálohování. c) Pravidla bezpečného uložení záloh. d) Pravidla a postupy obnovy. e) Pravidla a postupy testování zálohování a obnovy.
politika bezpečného předávání a výměny informací **	✔		a) Pravidla a postupy pro ochranu předávaných informací. b) Způsoby ochrany elektronické výměny informací. c) Pravidla pro využívání kryptografické ochrany.
politika řízení technických zranitelností **	✔		a) Pravidla pro omezení instalace programového vybavení, b) Pravidla a postupy vyhledávání opravných programových balíčků, c) Pravidla a postupy testování oprav programového vybavení, d) Pravidla a postupy nasazení oprav programového vybavení.
politika bezpečného používání mobilních zařízení	✔		a) Pravidla a postupy pro bezpečné používání mobilních zařízení. ~~b) Pravidla a postupy pro zajištění bezpečnosti zařízení, kterými orgán a osoba uvedená v § 3 písm. c) a d) zákona nedisponuje.~~ b) Pravidla a postupy pro zajištění bezpečnosti zařízení, která orgán nebo osoba, která je povinna zavést bezpečnostní opatření podle zákona, nemá ve své správě.
~~poskytování a nabývání licencí programového vybavení a informací~~	✔	✔	~~a) Pravidla a postupy nasazení programového vybavení a jeho evidence.~~ ~~b) Pravidla a postupy pro kontrolu dodržování licenčních podmínek.~~
politika dlouhodobého ukládání a archivace informací	✔		a) Pravidla a postupy archivace dokumentů a záznamů. b) Ochrana archivovaných dokumentů a záznamů. c) Politika přístupu k archivovaným dokumentům a záznamům.
politika ochrany osobních údajů	✔	✔	a) Charakteristika zpracovávaných osobních údajů. b) Popis přijatých a provedených organizačních opatření pro ochranu osobních údajů. c) Popis přijatých a provedených technických opatření pro ochranu osobních údajů.
politika fyzické bezpečnosti **	✔		a) Pravidla pro ochranu objektů. b) Pravidla pro kontrolu vstupu osob. c) Pravidla pro ochranu zařízení. d) Detekce narušení fyzické bezpečnosti.

politika bezpečnosti komunikační sítě **	✔		a) Pravidla a postupy pro zajištění bezpečnosti sítě. b) Určení práv a povinností za bezpečný provoz sítě. c) Pravidla a postupy pro řízení přístupů v rámci sítě. d) Pravidla a postupy pro ochranu vzdáleného přístupu k síti. e) Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů.
politika ochrany před škodlivým kódem	✔	✔	~~a) Pravidla a postupy pro ochranu komunikace mezi vnitřní a vnější sítí.~~ a) Pravidla a postupy pro ochranu síťové komunikace. b) Pravidla a postupy pro ochranu serverů a sdílených datových uložišť. c) Pravidla a postupy pro ochranu pracovních stanic.
politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí **	✔	✔	a) Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí. b) Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události. c) Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí.
politika využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí **	✔		a) Pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí. b) Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí. c) Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.
politika bezpečného používání kryptografické ochrany **	✔	✔	a) Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu. b) Pravidla kryptografické ochrany informací 1. při přenosu po komunikačních sítích, 2. při uložení na mobilní zařízení nebo vyměnitelný technický nosič dat, c) Systém správy klíčů.
zpráva z auditu kybernetické bezpečnosti**	✔		a) Cíle auditu kybernetické bezpečnosti. b) Předmět auditu kybernetické bezpečnosti. c) Kritéria auditu kybernetické bezpečnosti. d) Identifikování týmu auditorů a osob, které se auditu kybernetické bezpečnosti zúčastnily. e) Datum a místo, kde byly prováděny činnosti při auditu kybernetické bezpečnosti. f) Zjištění z auditu kybernetické bezpečnosti. g) Závěry auditu kybernetické bezpečnosti.
zpráva z přezkoumání systému řízení bezpečnosti informací**	✔		a) Vyhodnocení opatření z předchozího přezkoumání systému řízení bezpečnosti informací, b) Identifikace změn a okolností, které mohou mít vliv na systém řízení bezpečnosti informací. c) Zpětná vazba o výkonnosti řízení bezpečnosti informací 1. neshody a nápravná opatření, 2. výsledky monitorování a měření, 3. výsledky auditu, ~~4. naplnění cílů bezpečnosti,~~ 4. naplnění cílů systému řízení bezpečnosti informací d) Výsledky hodnocení rizik a stav plánu zvládání rizik. e) Identifikace možností pro neustálé zlepšování. f) Doporučení potřebných rozhodnutí, stanovení opatření a osob zajišťujících výkon jednotlivých činností.
metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik	✔	✔	a) Určení stupnice pro hodnocení primárních aktiv 1. určení stupnice pro hodnocení úrovní důvěrnosti aktiv, 2. určení stupnice pro hodnocení úrovní integrity aktiv, 3. určení stupnice pro hodnocení úrovní dostupnosti aktiv. b) Určení stupnice pro hodnocení rizik 1. určení stupnice pro hodnocení úrovní dopadu, 2. určení stupnice pro hodnocení úrovní hrozby, 3. určení stupnice pro hodnocení úrovní zranitelnosti, 4. určení stupnice pro hodnocení úrovní rizik, c) Metody a přístupy pro zvládání rizik. d) Způsoby schvalování přijatelných rizik.

zpráva o hodnocení aktiv a rizik**	✔	✔	a) Přehled primárních aktiv 1. identifikace a popis primárních aktiv, 2. určení garantů primárních aktiv, 3. hodnocení primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti. b) Přehled podpůrných aktiv (neplatí pro orgány a osoby uvedené v § 3 písm. e) zákona) 1. identifikace a popis podpůrných aktiv, 2. určení garantů podpůrných aktiv, 3. určení vazeb mezi primárními a podpůrnými aktivy, ~~c) Identifikování a hodnocení rizik~~ c) Hodnocení rizik 1. posouzení možných dopadů na aktiva, 2. hodnocení existujících hrozeb, 3. hodnocení existujících zranitelností, hodnocení existujících opatření, 4. stanovení úrovně rizika, porovnání této úrovně s kritérii pro přijatelnost rizik, 5. určení a schválení přijatelných rizik. d) Zvládání rizik 1. návrh způsobu zvládání rizik, 2. návrh opatření a jejich realizace.
prohlášení o aplikovatelnosti	✔	✔	a) Přehled vybraných bezpečnostních opatření včetně zdůvodnění jejich výběru a jejich vazby na identifikovaná rizika. b) Přehled zavedených bezpečnostních opatření.
plán zvládání rizik**	✔	✔	~~a) Obsah a cíle vybraných bezpečnostních opatření pro zvládání rizik.~~ a) Obsah a cíle vybraných bezpečnostních opatření pro zvládání rizik včetně vazby na konkrétní rizika. b) Potřebné zdroje pro jednotlivá bezpečnostní opatření pro zvládání rizik. c) Osoby zajišťující jednotlivá bezpečnostní opatření pro zvládání rizik. d) Termíny zavedení jednotlivých bezpečnostních opatření pro zvládání rizik. ~~e) Způsoby hodnocení úspěšnosti zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.~~ e) Způsob realizace bezpečnostních opatření.
plán rozvoje bezpečnostního povědomí	✔	✔	~~a) Obsah a termíny poučení uživatelů.~~ a) Obsah a termíny poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role. ~~b) Obsah a termíny poučení garantů aktiv (neplatí pro orgány a osoby uvedené v § 3 písm. e) zákona).~~ ~~c) Obsah a termíny poučení administrátorů (neplatí pro orgány a osoby uvedené v § 3 písm. e) zákona).~~ ~~d) Obsah a termíny poučení dalších osob zastávajících bezpečnostní role.~~ ~~e)~~ b) Obsah a termíny poučení nových zaměstnanců. c) Přehledy, které obsahují předmět jednotlivých školení a seznam osob, které školení absolvovaly. ~~f)~~ d) Formy a způsoby hodnocení plánu.
politika zvládání kybernetických bezpečnostních incidentů**	✔	✔	a) Definování kategorií kybernetického bezpečnostního incidentu. b) Pravidla a postupy pro evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů. c) Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů. d) Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti. *e) Evidence incidentů.*
politika řízení kontinuity činností**	✔	✔	a) Práva a povinnosti zúčastněných osob. b) Cíle řízení kontinuity činností 1. minimální úroveň poskytovaných služeb, 2. doba obnovení chodu, ~~3. bod obnovení chodu.~~ 3. doba obnovení dat c) Strategie řízení kontinuity činností pro naplnění cílů kontinuity. d) Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik. ~~e) Určení a obsah potřebných plánů kontinuity.~~ e) Určení a obsah potřebných plánů kontinuity a havarijních plánů. ~~f) Postupy pro realizaci opatření vydaných Národním bezpečnostním úřadem.~~ f) Postupy pro realizaci opatření vydaných Úřadem.

přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků	✔	✔	a) Přehled obecně závazných právních předpisů. b) Přehled vnitřních předpisů a jiných předpisů. c) Přehled smluvních závazků.
politika akvizice, vývoje a údržby			*a) Bezpečnostní požadavky pro akvizici, vývoj a údržbu* *b) Řízení zranitelností* *c) Politika poskytování a nabývání licencí programového vybavení a informací* *1) Pravidla a postupy nasazení programového vybavení a jeho evidence.* *2) Pravidla a postupy pro kontrolu dodržování licenčních podmínek.*
politika řízení změn			*a) Způsob a principy řízení významných změn v rámci orgánu nebo osoby, jejich procesech, informačních a komunikačních systémech.* *b) Přezkoumávání dopadů významných změn.* *c) Způsob vedení evidence a testování významných změn.*
prohlášení o aplikovatelnosti			*a) Přehled vyloučených bezpečnostních opatření požadovaných touto vyhláškou včetně zdůvodnění, proč nebyla aplikována.* *b) Přehled zavedených bezpečnostních opatření včetně způsobu jejich implementace.*
evidence změn			*a) Evidence životního cyklu významných změn.* *b) Záznamy o změnách konfigurace podpůrných aktiv*
hlášené kontaktní údaje			*a) Přehled hlášených kontaktních údajů.*
další doporučená dokumentace			*a) Topologie infrastruktury.* *b) Přehled síťových zařízení.*

* - řízení dodavatelů

** - očekává se vysoká úroveň důvěrnosti

3.9 Deset kroků kybernetické bezpečnosti

Zajímavý a fundovaný pohled na kybernetickou bezpečnost nabízí Národní technický úřad pro informační zabezpečení (CESG) britské vlády. V deseti krocích je popsaný směr, jak v organizaci dosáhnout zavedení bezpečnosti a její vysoké úrovně.

Vzdálený a mobilní přístup (Home and mobile working) – Vzdálený přístup do zabezpečené sítě může uživatelům skýtat výhodu, jako je neomezený přístup k informacím kdykoliv a odkudkoliv. Zároveň s výhodami je třeba vnímat i možná rizika, která je třeba zvládnout zavedením vhodných zásad a opatření. Rizika je nutné vyhodnotit, a vytvořit politiku pro práci v režimu vzdáleného připojení. Politiky by se měly dotknout způsobu autorizace, použití šifrování, minimalizace dat, která jsou ukládaná v zařízení, stanovením postupů při ztrátě zařízení a zvýšenému sledování aktivit a úrovní kontrol (10 Steps: Home and Mobile Working, 2016).

Řízení incidentů (Incident management) – Pokud nejsou v organizaci implementovány nástroje a politiky řízení bezpečnostních incidentů, lze předpokládat, že v případě incidentu nastane závažný problém. To se může projevit jako právní spor, finanční ztráty, újma na pověsti organizace, zhoršení vztahů s okolím, narušení běžného fungování a snížení výkonnosti nebo

ohrožení samotné existence organizace. Proces řízení incidentů napomáhá zlepšování odolnosti systémů, posiluje a stabilizuje kontinuitu, příznivě ovlivňuje důvěru zákazníků i všech zúčastněných stran a napomáhá snižovat potenciální dopady a škody. Obranou proti projevům bezpečnostních incidentů je efektivní schopnost reagovat na incidenty v celé organizaci stanovením rolí a odpovědností, zavedením mechanismů zálohování na fyzicky bezpečném místě a procesů obnovy dat. Fungující systém řízení incidentů využívá otestované plány řízení incidentů, kontinuity provozu a plánů obnovy (10 Steps: Incident Management, 2016).

Ochrana před škodlivým kódem (Malware protection) – Působení škodlivého kódu (malware) může poškodit systémy organizace například narušením fungování systémů a služeb, neoprávněným zacházením s daty, jejich nežádoucími změnami, zničením nebo znepřístupněním. Nezbytnými opatřeními je kontrola a dohled nad komunikací s vnějším světem prostřednictvím e-mailů, webů a výměnných zařízení. Opatření zahrnují instalaci antivirových programů, správu blacklistu nedoporučených či zakázaných webových stránek, řízení přístupů k portům USB, posouzení spustitelnosti maker a scriptů, správnou konfiguraci systému, aktualizaci nastavení firewallu, implementaci nástrojů ochrany a monitorování sítí nebo provoz dohledových aplikací (10 Steps: Malware Prevention, 2016).

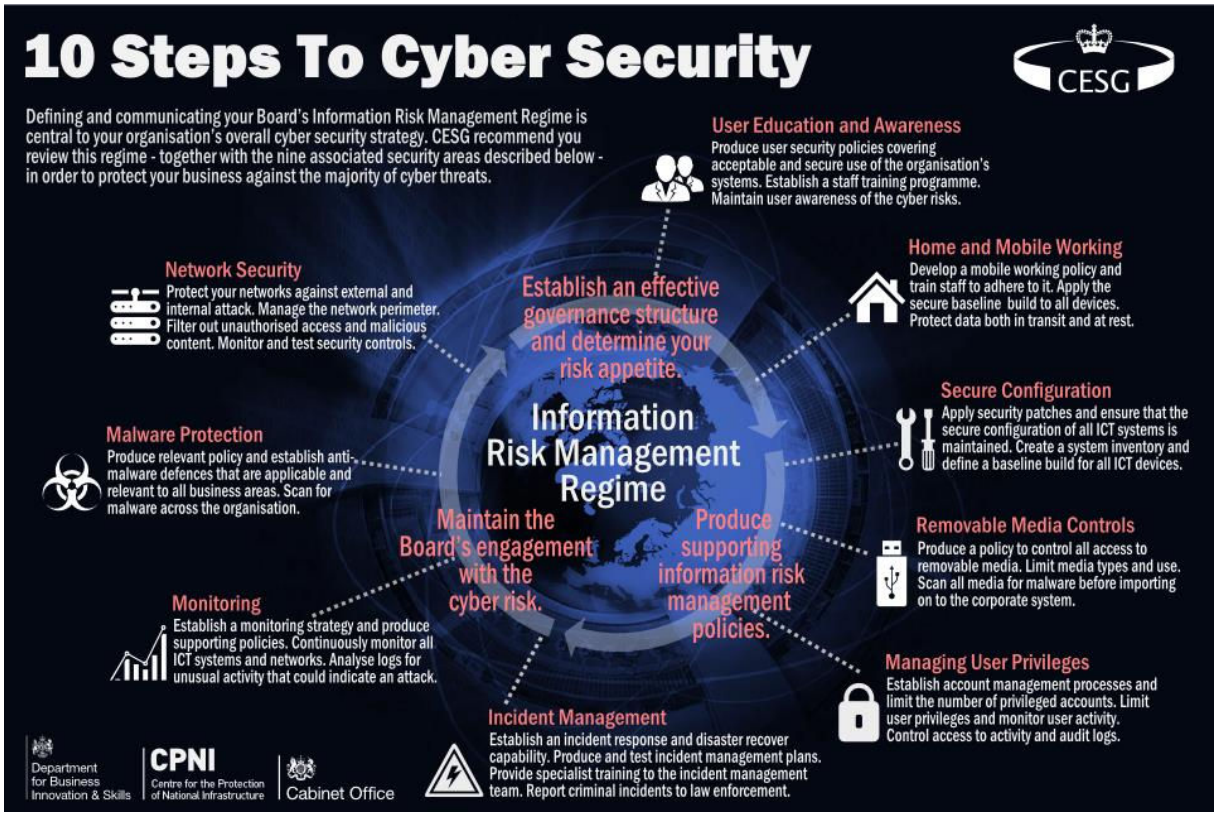
Řízení privilegovaných oprávnění (Managing user privileges) – Je důležité přesně vědět, jaká oprávnění uživatelé skutečně potřebují. Východiskem pro přidělování oprávnění je uplatnit politiku „nejmenších oprávnění“ a použít vhodný způsob přidělování systémových oprávnění, práv přístupu k datům, odpovídající konkrétním rolím a jejich potřebám. Pokud jsou přidělovaná práva silně privilegovaná, je nutností zajistit, aby nedošlo ke zneužití nebo ke změnám bezpečnostních kontrol pro přípravu budoucích útoků. Důležitá je aplikace efektivních procesů v případech změny role uživatele například odebrání rolí propouštěného zaměstnance (10 Steps: Managing User Privileges, 2016).

Monitorování (Monitoring) – Cílem monitorování systému je odhalovat pokusy, ale i útoky na systémy a služby, a zajistit tak účinnou a rychlou reakci. Monitorování zahrnuje sledování všech systémů a sítí, používá nástroje detekce narušení nebo sledování síťové komunikace a neobvyklé aktivity. Monitoring umožňuje zajistit, aby systémy byly řádně používány v souladu se zásadami organizace (10 Steps: Monitoring, 2016).

Síťová bezpečnost (Network security) – Systémy zapojené do internetu nebo do partnerských sítí mohou být vystaveny útokům. Důležité je rozpoznání, jaké příležitosti může útočník využít

k napadení infrastruktury, a tím snížit šance úspěchu útoku. Nedostatečně zabezpečená síť dává útočníkům příležitost k ohrožení systémů, což může vést k problémům ve fungování organizace nebo komunikaci s vnějším světem (s partnery a zákazníky) (10 Steps: Network Security, 2016).

Kontrola výměnných zařízení (Removable media controls) – Výměnná média většinou slouží k přenosu dat mezi stanicemi. Každá stanice může mít rozdílnou úroveň ochrany před malware, zvlášť pokud se medium připojilo ke stanici mimo organizaci, což zvyšuje riziko zanesení malware do prostředí organizace. Hrozbu představují data získaná z odcizeného media, nebo taky úmyslně poskytnutá data. Zvládání rizik vychází z omezení přenášení dat na výměnných mediích a používání šifrování. Při opětovnému použití média by mělo předcházet ověření, že původní data jsou prokazatelně smazána, a nehrozí jejich zneužití (10 Steps: Removable Media Controls, 2016).



Obrázek 11: Deset kroků kybernetické bezpečnosti. Zdroj: (10 Steps: Risk Management Regime, 2016)

Režim řízení rizik (Risk Management Regime) – Organizace spoléhají na technologie a systémy, a proto musí být posouzena a následně vyhodnocena jejich rizika. Zvládnutí rizik vychází z vytvořeného rámce řízení (podle Obrázku č. 11), politik řízení rizik a odpovědností za procesy řízení rizik. Výchozím krokem je analýza rizik a stanovení kategorií rizik (stupně od tolerovaných rizik až po zásadně nepřijatelná rizika), na to navazuje sestavení plánu řešení rizik a cílů, kterých má být dosaženo. V procesech řízení rizik je třeba přihlédnout ke změnám technologií a systémů. Rizika by měla být pravidelně přezkoumávána, aby bylo možné sledovat

účinnost opatření a současný stav. Kontroly bezpečnosti, aby zůstaly účinné, musí probíhat jako nepřetržitý proces, který zajistí žádoucí stav bezpečnosti a minimalizaci rizik (10 Steps: Risk Management Regime, 2016).

Bezpečná konfigurace (Secure configuration) – Oprávnění konfigurovat systémy by měla mít jen omezená skupina uživatelů s patřičnými právy a pověřením organizace. Nevhodně spravované systémy mohou být zranitelné, čímž se vytváří příležitost k napadení systému a jeho neoprávněným změnám. Bezpečnost vyžaduje odpovědný přístup využívání bezpečnostních záplat k eliminaci zneužití kritických chyb v softwaru, používání podporovaných verzí programového vybavení, stanovení postupů pro aktualizování bezpečnostních záplat a opravných balíků nebo správa inventáře hardwaru i softwaru. Důležité je pravidelné přehodnocení a prověření zranitelností, implementace zásad pro konfigurace a řízení změn, udržování spolehlivého a důvěryhodného systému správy povoleného softwaru a omezení instalace neoprávněných nebo nebezpečných aplikací (10 Steps: Secure Configuration, 2016).

Vzdělávání a povědomí uživatelů (User education and awareness) – Uživatelé představují jednu z nejkomplikovanějších oblastí řízení bezpečnosti. Pravidla bezpečnostních zásad by měla zajistit požadovanou minimální úroveň bezpečnosti. Uživatelé by měli být opakovaně seznámeni s bezpečnostní politikou a ve svém jednání si počínat v jejím souladu. Měli být si vědomi osobní odpovědnosti za dodržování zásad firemní bezpečnostní politiky (10 Steps: User Education and Awareness, 2016).

3.10 Bezpečnostní hrozby

Řízení kybernetické bezpečnosti má za cíl minimalizovat hrozby, které organizaci ohrožují, a proto je důležité vědět, jaké hrozby mohou chod organizace ovlivnit, a jaké mohou být její dopady. Co znamená bezpečnostní hrozba nejlépe vystihuje definice, která zní: *Potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb* (Jirásek, Novák, Požár,2015, s. 25).

Hrozby lze rozdělit do několika skupin. (Gála, Pour, Šedivá., 2009) klasifikují hrozby na:

- přírodní a fyzické,
- technické a technologické,
- lidské úmyslné a neúmyslné.

Všechny tyto hrozby mohou ovlivnit běžný provoz systémů a fungování organizace. Projev některé hrozby znamená porušení dostupnosti, důvěrnosti nebo integrity. Hrozby, ale také kybernetické útoky nelze zcela vyloučit, a proto je nezbytností připravenost a prevence. Kromě nejrůznějších technických poruch, které lze řešit správnou konfigurací a vhodně nastavenými procesy, na což je možné se relativně snadno připravit, je nutností detekovat i nejrůznější pokusy o útok na systémy a rychle, efektivně a správně reagovat vhodnými protiopatřeními. K tomu přispívá i analýza možných hrozeb a jejich detailní poznání. (Common threats to be aware of, 2017) se věnuje následujícím hrozbám:

Botnets – Termín botnet je složen ze dvou anglických slov bot (označení robota) a net (síť). Jedná se o softwarového agenta, který v případě úspěšného proniknutí do počítače stroj do jisté míry ovládne. Vytváří tak celou síť infikovaných počítačů označovaných jako "zombie". Síť infikovaných strojů je řízena centrálně svým původcem a podle povelů provádí nežádoucí činnost jako je rozesílání spamu (nevyžádané pošty), šíření malware nebo se takto ovládnutý stroj stane součástí koordinovaných útoků DDoS.

DoS (Denial of Service) – Odepření služby a jeho forma DDoS (Distributed Denial of Service) což je cílený útok na určitou webovou stránku nebo server, aby došlo k narušení jeho běžného fungování. Pro útoky typu opepření služby se běžně využívají zombie stroje, které odesílají velké množství dat nebo opakovaně odesílají požadavky, čímž se zatěžuje napadený stroj, a může dojít od zpomalení až k úplnému výpadku provozu. Tento typ útoku využívá skutečnost, že servery umí najednou zpracovat jen určité množství požadavků současně. Pokud je požadavků více, než je server schopen zpracovat, začnou se projevovat příznaky přetížení. Obrana proti tomuto typu útoku je přístup na dvou stranách. První je plošná ochrana počítačů před veškerým škodlivým software a správnou konfigurací. Druhou stranou je vzdělávání a odpovědnost uživatelů. Velmi komplikovaná je obrana před DDoS útokem. Napadená strana bude muset zvládnout ochránit svoje technologie, zálohovat a obnovit data, monitorovat provoz, rozpoznat útok a zmírňovat dopady na běžný provoz.

Hacking – Využívání slabin a bezpečnostních děr k získání neoprávněného přístupu k počítači. Problémem jsou snadně dostupné návody a informace o hackování. Hacking může být i legální, když se prostřednictvím hackování (Ethical Hacking) testuje bezpečnost systémů.

Malware – Malware je označení škodlivého kódu. Termín pochází ze zkrácení slov "malicious software". Malware je jedním z nejběžnějších způsobů infiltrace nebo poškození počítače

a zahrnuje formy jako jsou viry, červy, trojské koně, spyware a adware. Infikovaný počítač může nežádoucím a nechtěným způsobem nakládat s informacemi a narušovat fungování systémů.

Ransomware – Ransomware je druh malware, který omezí přístup k počítači a jeho souborům. Využívá k tomu proniknutí do počítačů, při kterém útočník zašifruje soubory a/nebo uzamkne obrazovku (Lockscreen) a zabrání v přístupu uživatelům. Pokud je počítač infikován, může dojít k zašifrování nejen místních (lokálních) disků, ale i síťových jednotek a dalších připojených úložných zařízení. Útočníci obvykle požadují výpalné, aby uživatel mohl získat zpět svůj přístup. Požadavky na platbu se občas i stupňují, aby se zvýšil tlak na napadené uživatele a přinutili je k úhradě požadované částky. Ovšem záruka, že počítač a data budou znovu přístupná, není ničím zaručená. Obranou může být správně pojaté zálohování.

Sabotáž – Jedním z nejznámějších příkladů strategického útoku je malware STUXNET. Tento malware se zaměřoval jen na specifické řídící jednotky Siemens napojené na centrifugy jaderných zařízení v Íránu. Útok neprováděl žádnou destruktivní činnost, ale naopak modifikoval řídící signály centrifug, což mělo za následek chybné fungování a větší opotřebení součástek (Řehka, 2017).

Špionáž – Bezpečnost státu může ohrozit napadení utajovaných nebo citlivých informací. (Řehka) například uvádí kauzu WikiLeaks. Tato kauza je spojena s Julianem Assangem, spoluzakladatelem serveru WikiLeaks, kde byly publikovány utajované vládní a korporátní materiály.

Kromě již existujících hrozeb, které mají řadu různých mutací a kategorií, se některé organizace snaží i predikovat nové typy. Například společnost Cisco (Roháček, 2017) předpovídá, že vznikne nový typ útoku tzv. DeOS (Destruction of Services), který má být mnohem ničivější. Tento útok má data nejen zničit, ale bude mít nepříznivý dopad i na obnovu dat. Jednodušší má být také podle předpovědí Cisca objednání útoků tzv. „ransomware jako služba“, nebo i dalších forem útoků.

Norma ISO 27005 uvádí v příloze C příklady typických hrozeb. Jednotlivé hrozby mají označený typ zdroje hrozby, který muže být náhodný, úmyslný nebo enviromentální (ISO 27005, 2013).

3.11 Problematické aspekty kybernetické bezpečnosti

Oblast kybernetické bezpečnosti se potýká s mnoha problematickými aspekty, které komplikují zachování stavu, ve kterém jsou hrozby eliminovány na nejnižší možnou (přijatelnou) míru. Významným faktorem, který znemožňuje problematiku v oblasti kybernetické bezpečnosti úspěšně vyřešit, je absence společné smlouvy, dohody či působnosti práva, která by zajistila snazší

dosažitelnost alespoň základní úrovně kybernetické bezpečnosti v mezinárodním měřítku. (Gřivna, Polčák, 2008) tento problém přikládají už tomu, že chybí vůle vytvoření takové dohody. Globální charakter kyberprostoru bez mezinárodních pravidel, zákonů ale i dohledu znamená problémy různých rozsahů, projevů a forem. Lokální prosazování aktuálně platné legislativy má sice svoje geografické hranice, ale interakce v kyberprostoru žádné hranice nevnímá.

Dalším problémem je nepřímá úměra toho, jak velký dopad může mít útok, za kterým stojí třeba jen jeden člověk. Ten s minimálním vybavením může díky snadné dostupnosti různých návodů útočit na stát a jeho infrastrukturu (nebo jiný cíl), což může mít dopad na desítky, stovky či tisíce lidí, případně může způsobit velké a rozsáhlé škody. Víceméně anonymní prostředí internetu přispívá k tomu, že útočník je jen těžko dohledatelný, může útočit na velké vzdálenosti, respektive bez omezení vzdálenosti, přes hranice států a kontinentů, navíc v situaci, kde v každé zemi platí jiný legislativní rámec.

Rozvoj technologií, jakými jsou IoT (Internet of Things) až IoE (Internet of Everything), znamená další značný nárůst zařízení, která budou zapojena do sítě internetu. Rizikem je nejen počet zařízení (např. jako potenciálních zdrojů DDoS útoků), ale i jejich zabezpečení a samotné používání. (Gartner, 2017) předpovídá do roku 2020 více než 20 miliard instalovaných IoT jednotek. Také technologie jako je cloud, vzdálený přístup nebo BYOD (Bring Your Own Device) s sebou nese určitá rizika, která vycházejí z pohybu dat do prostředí, které mají organizace jen stěží pod kontrolou. V případě cloudu organizace svěřují část svých aktiv třetí straně a stává se na ní určitou měrou závislá. I nositelná elektronika, spojená s fitness aplikací, stála za bezpečnostním rizikem. (Berlinger, Vazquez, 2018) uvádějí, že vojáci v Afganistanu v rámci udržování kondice při trénincích využívali aplikaci Strava, která zveřejňovala jejich běžecké trasy. Důsledkem bylo odhalení tajných základen a přístupových cest k nim.

3.12 Fenomén kybernetické a informační války

Kybernetický prostor nabývá na důležitosti a většina systémů je závislá na moderních technologiích, a proto informační a komunikační technologie mohou být strategicky využitelné i v rámci různých konfliktů. Jak uvádí (ČTK, 2016) NATO (North Atlantic Treaty Organization) na summitu ve Varšavě uznala kyberprostor jako operační oblast, ve kterém může probíhat střet, a zájmem obrany každého státu je ochránit „svůj kybernetický prostor“. Základní operační oblasti, které se rozšířily o kyberprostor, jsou země, voda a vzduch. Některé zdroje uvádějí jako operační oblast válečného střetu také vesmír.

Kybernetická válka je podle (Řehka, 2017) neoddělitelnou součástí informační války, která je prvkem takzvané čtvrté generace válčení. V tomto pojetí války se klade důraz na informace, informační působení a ovlivňování. Obzvláště v případech těchto typů konfliktů platí, že státním zájmem musí být schopnost ochránit svůj kybernetický prostor jako nezbytnost zachování fungování systémů z důvodů všeobecné závislosti na klíčových systémech. Informační válka je nástrojem, technikou či metodou válčení, a je součástí hybridní války, což ilustruje Obrázek č. 12.

Obrázek 12: Úrovně typů válek. Zdroj: Autor

Pojem hybridní války může být definován jako: *ozbrojený konflikt vedený kombinací nevojenských a vojenských prostředků s cílem jejich synergickým efektem přinutit protivníka k učinění takových kroků, které by sám o sobě neučinil* (Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy, 2016, s. 10) nebo jako *válku vedenou za souběžného, flexibilního a vysoce adaptabilního použití konvenčních a nekonvenčních metod, které se vzájemně podporují, jsou používány na všech úrovních a využívají všechny dostupné prostředky včetně nestátních aktérů, povstaleckého boje, terorismu, politických, ekonomických informačních a právních nástrojů, ale i nasazení vyspělých zbraňových systémů a působení v kybernetickém prostoru* (Řehka, 2017, s. 183). Pro jakýkoliv válečný konflikt je typická snaha o maximální kontrolu v dané oblasti (Ftorek, 2017). To potvrzuje i (Řehka) když uvádí, že faktorem úspěchu ve válce je informační převaha, která *umožňuje provádět v tomto prostředí vlastní operace bez efektivního odporu protivníka a na druhou stranu upírá obdobné možnosti protivníkovi* (Řehka, 2017, s. 43).

3.13 Lidský faktor

Profesionálové, kteří se zabývají bezpečností, vnímají lidský faktor za nejslabší článek celého systému. Při práci s informačními systémy je nutná autorizace, která je zpravidla řešena přístupovými údaji, a to uživatelským jménem a heslem. Právě heslo je slabým místem tohoto bezpečnostního opatření, které podle (Vyoral, 2017) podporuje i nechuť hesla měnit. VoKB stanovuje požadavky na heslo, které musí mít minimální délku 8 znaků a musí splňovat tři další požadavky ze čtyř (nejméně jedno velké písmeno, nejméně jedno malé písmeno, nejméně jednu

číslici, nejméně jeden znak, který není písmenem nebo číslicí). Typickým heslem, které tato pravidla plní je *Heslo.01*, které po vyhláškou stanovené maximální době platnosti sto dní lze zaměnit na *Heslo.02*, přičemž požadavky jsou splněny a zároveň je zachovaná vysoká míra zapamatovatelnosti hesla. V souvislosti s hesly je problém také sdělování hesel jiné osobě, nebo uchovávání hesla na nějakém médiu (například heslo napsané na papíře).

Další problém týkající se lidského faktoru je, že zaměstnanci zatajují kybernetické incidenty. (Dočekal, 2017) uvádí, že zaměstnanci se ve 40 % firem snaží incidenty utajit. Vychází z průzkumu, který zjistil, že za 46 % bezpečnostních incidentů jsou odpovědni právě zaměstnanci. Jsou přitom využívány slabiny, které s sebou nese právě lidský faktor. Řešení tohoto problému předpokládá vypracování pochopitelných a srozumitelných směrnic a proškolení zaměstnanců o kybernetické bezpečnosti, zvláště v oblasti hlášení incidentů, kdy je nutný rychlý zásah.

Člověk je také iniciátorem útoků. Pachatele kybernetických útoků lze podle (Smejkal, 2015) kategorizovat jako individuální útočníky, jejichž paleta motivů zahrnuje od zvědavosti a uspokojování ega až ke mstě. Další skupinou jsou ideologicky motivované skupiny, které cílí na své ideologické nebo reálné protivníky. Poslední kategorií je oblast státního terorismu, kam patří státní hackeři. Zvláštní skupinou jsou pachatelé počítačové kriminality s ryze ekonomickou motivací. Typické motivy trestné činnosti uvádí (Porada, 2016), když diskutuje otázku prospěchu z důsledků spáchaného činu. Za motivy považuje zejména:

- zjištné motivy (rychlé a zdánlivě bezpečné získání velkých částek peněz často zdůvodňované nízkým finančním oceněním pachatele),
- motivy vyplývající z konfliktů v mezilidských vztazích (msta, nenávist, závist atp.),
- touha po získání moci či výsadního postavení (prostřednictvím likvidace či diskreditace konkurentů atp.),
- touha dokázat svoji intelektuální převahu (nad tvůrci ochranných programů, nad nadřízeným pracovníkem, obecně nad zaměstnavatelem),
- touha překonat subjektivní pocit nedocenění svých schopností (například přáteli, kamarády, spolupracovníky, nadřízenými atp.),
- krycí motivy k utajení jiné trestné činnosti (například daňových úniků, zpronevěru svěřených hodnot atp.),
- snaha o vyniknutí v obchodní činnosti (například na kapitálovém trhu),
- politické motivy (diskreditace politických odpůrců atp.) nebo jiné ideologické důvody (náboženské, filosofické atp.).

4 Řízení rizik

Cílem této kapitoly je navázat na předchozí část o informační a kybernetické bezpečnosti tématem, které s bezpečností souvisí. Řízení rizik a řízení aktiv jsou neoddělitelnými opatřeními ve vyhlášce o kybernetické bezpečnosti. V této kapitole budou podrobněji diskutovány oblasti řízení rizik, související procesy a pozornost bude věnována také výkladu terminologie.

Riziko jako pojem má mnoho možných interpretací. Rizika, která souvisejí se zajištěním informační bezpečnosti, uvádějí (Smejkal, Rais, 2013) jako:

- pravděpodobnost či možnost vzniku ztráty, obecně nezdaru,
- variabilitu možných výsledků nebo nejistota jejich dosažení,
- možnost, že specifická hrozba využije specifickou zranitelnost systému,
- odchýlení skutečných a očekávaných výsledků,
- kombinace pravděpodobnosti události a jejího následku.

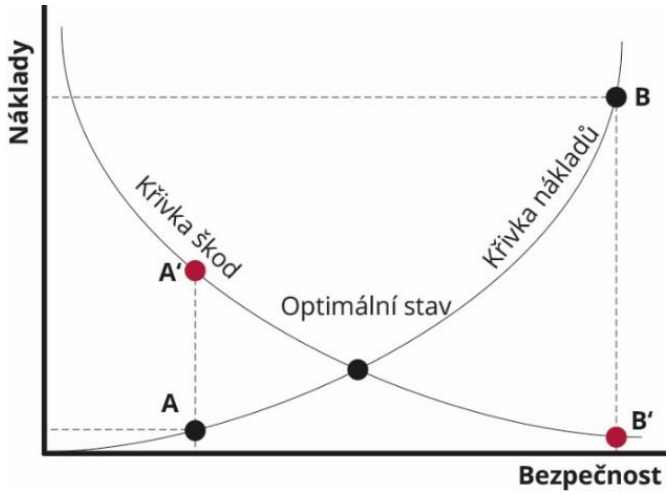
Poslední zmiňovaná definice je výkladem významu rizika, který platí také v normě ISO 27000. V ISO normě zabývající se managementem rizik je pak riziko chápáno jako *účinek nejistoty na dosažení cílů* (ISO 31000, 2010).

Podle uvedené definice rizika, která říká, že riziko je možnost, že specifická hrozba využije specifickou zranitelnost systému v případě překonání bezpečnostních opatření dochází narušení dostupnosti, důvěrnosti nebo integrity. Překonáním opatření, která jsou v kontextu zákona o kybernetické bezpečnosti chápána jako bezpečnostní incident nebo bezpečnostní událost, vede k možnosti vzniku škody nebo nějakého negativního projevu (Čermák, 2009). Čím je utvářen sytém působení rizik je nastíněn na Obrázku č. 13. Na tomto obrázku jsou použité vztahy a další pojmy, které budou dále blíže vyjasněny.

Obrázek 13: Mechanismus uplatnění rizika. Zdroj (Čermák, 2009)

Vztahy uvedené na obrázku naznačují způsob, jak riziko působí na komponenty nebo části systému, tedy aktiva, která vlastník používá a snaží se je zhodnocovat. Vlastník je osoba, která je pověřena správou aktiva a dohlíží na jeho bezproblémový stav, navíc *vlastník, který má prvořadý zájem na zachování kontinuity své společnosti, potřebuje vědět, jaká rizika ho ohrožují a jak jim čelit* (Čermák, 2009, s. 18). Podle vyhlášky o kybernetické bezpečnosti je vlastník označen jako garant aktiva s odpovědností za zajištění rozvoje, použití a bezpečnosti aktiva. Pro vlastníka má každé aktivum svou hodnotu, kterou vhodnými opatřeními ochraňuje před riziky, která by omezila nebo zcela vyloučila používat aktiva a zhodnocovat je. Smyslem přijímání opatření je účinným a efektivním způsobem snížit zranitelnost systémů a komponent tak, aby hrozby vyvolané agentem hrozby byly potlačeny na nejnižší možnou, přijatelnou úroveň (Čermák, 2009).

Zajištění požadovaného stavu bezpečnosti je pro organizace také nákladem, který musí být opodstatněný natolik, aby odpovídal požadované úrovni bezpečnosti, a přitom byl brán ohled na úroveň potenciálních škod. *Pokud k budování systému informační bezpečnosti přistupujeme systematicky a podle logicky navazujícího plánu, jsme schopni dosáhnout určité rovnováhy mezi vynaloženými náklady na bezpečnost a potencionálními škodami, které vyplývají ze známých rizik* (Nádeníček, 2006). Na Obrázku č. 14 je znázorněn vztah nákladů a možných následků v poměru k úrovni bezpečnosti.



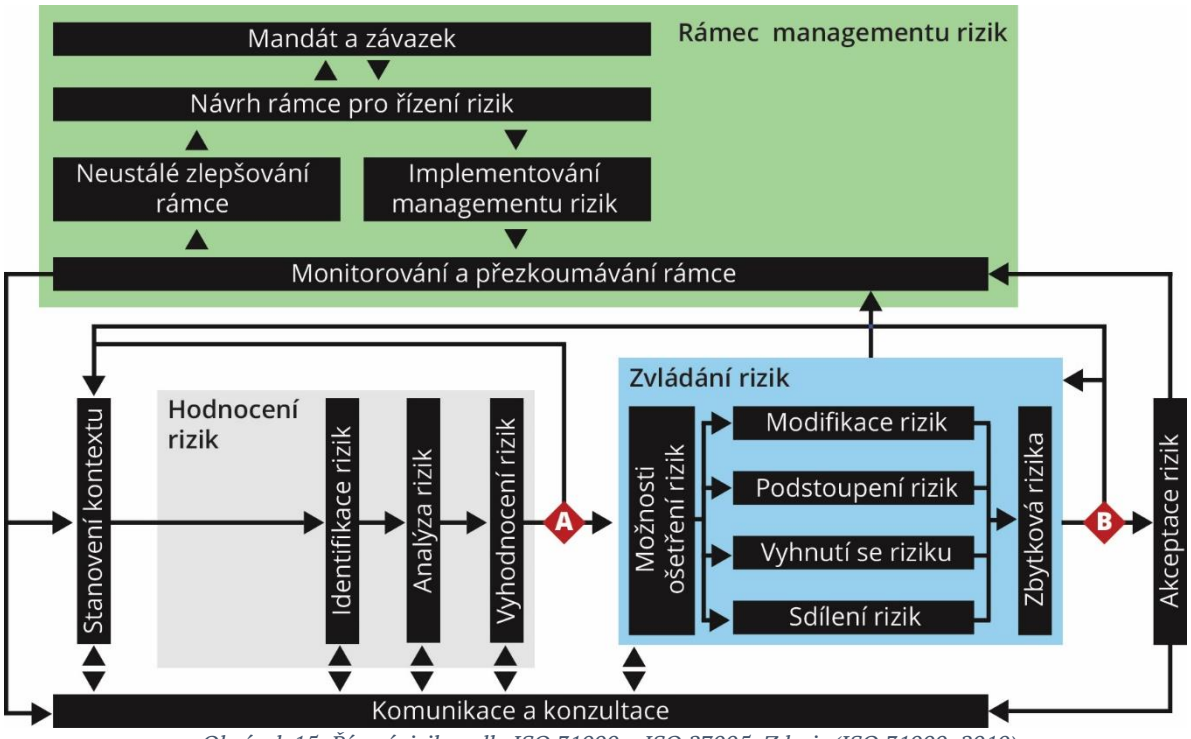
Obrázek 14: Optimum investic do bezpečnosti. Zdroj: (Čermák, 2009)

Optimální stav představuje stav efektivního poměru mezi veličinami. Obrázek ilustruje příklad, kdy vynaložené náklady zajišťují nízkou úroveň bezpečnosti (bod A) mohou mít za následek poměrně značné škody (bod A'). Samozřejmě absence jakékoliv bezpečnosti znamená, že škody mohou být velmi rozsáhlé. Oproti tomu velmi vysoká úroveň bezpečnosti znamená, že vynaložené náklady (bod B) mohou být velmi vysoké, přičemž škody, které by mohly vzniknout, jsou poměrně

nízké (bod B'). Škody sice budou stále nižší, ale cena bude stále více narůstat neúměrně ke zlepšení bezpečnosti, a to přitom nelze všechna rizika zcela vyloučit. Proto musejí organizace najít vhodnou a rozumnou rovnováhu mezi oběma veličinami. Bezpečnostní incident může podnítit k nesystematickým pokusům zlepšit stav bezpečnosti zaváděním izolovaných a přehnaných opatření (Nádeníček, 2006). Takové pokusy jsou neefektivní a zvyšují náklady na bezpečnost.

4.1 Řízení rizik podle normy ISO 31000, ISO 27001 a ISO 27005

Proces řízení rizik a jeho úspěšnost závisí na použitém rámci managementu rizik, který je má efektivně řídit. Atributem efektivního managementu rizik je neustálé zlepšování managementu rizik, ustanovení odpovědností za rizika, včetně způsobilosti řídit rizika, neustálá komunikace se všemi zainteresovanými stranami managementu rizik o úrovních rizika a opatřeních, integrace s řídícími procesy a zohledňování rizik při veškerém rozhodování v organizaci (ISO 31000, 2010).

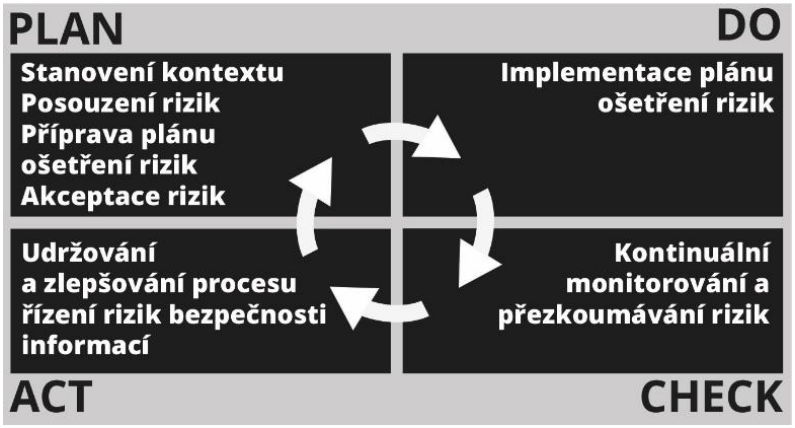


Obrázek 15: Řízení rizik podle ISO 31000 a ISO 27005. Zdroj: (ISO 31000, 2010)

Rámec managementu rizik, který je zobrazen na Obrázku č. 15, vyžaduje, aby vedení udělilo trvalý mandát pro zavedení procesu řízení rizik a jeho efektivní udržování a zachování. Rámec řízení rizik vyžaduje, aby návrh bral v úvahu vnitřní i vnější kontext organizace a všechny aspekty ovlivňující organizaci, a tak návrh odpovídal všem těmto okolnostem. Návrh rámce jasně stanoví cíle organizace a politiku řízení rizik, způsoby vnitřní a vnější komunikace, odpovědnosti, pravomoci a kompetence pro řízení rizik. Zohledňuje také, jaké zdroje budou pro průběh procesu řízení rizik potřeba. Implementace procesu managementu rizik uplatňuje plány řízení rizik jako součást všech

procesů a postupů. Ve fázi monitorování a přezkoumání rámce je pomocí indikátorů měřena výkonnost řízení rizik, sledují se pokroky vzhledem k plánu nebo odchylky od plánu, ověřuje se, zda rámec odpovídá svému účelu a přístupu k rizikům a hodnotí se efektivnost rámce. Výstupy měření a přezkoumávání jsou podkladem pro zlepšování rámce řízení rizik (ISO 31000, 2010).

Přístup, který uplatňuje ISO 27005 pro řízení rizik, vychází z PDCA cyklu systému řízení bezpečnosti informací (viz Obrázek č. 9). Proces řízení rizik bezpečnosti informací a jeho propojení s ISMS zobrazuje Obrázek č. 15.



Obrázek 16: PDCA cyklus řízení rizik podle ISO 27005. Zdroj (ISO 27005, 2013)

Řízení rizik bezpečnosti informací jsou *koordinované činnosti k vedení a řízení organizace s ohledem na rizika* (ISO 27005, 2013, s. 11). Účinný systém ISMS, odpovídající prostředí organizace, vyžaduje systematický přístup k identifikovaným potřebám v oblasti řízení rizika a měl by být v souladu bezpečností organizace jako celku, jeho částmi, jakýchkoliv informačních systémů a stávajících i plánovaných opatření. Řízení rizik by mělo přispět k tomu, aby (ISO 27005, 2013):

- byla provedena identifikace rizik,
- bylo provedeno posouzení rizik z hlediska jejich důsledků na činnosti organizace a pravděpodobnost jejich výskytu,
- byla pravděpodobnost a důsledky těchto rizik komunikovány a chápány,
- bylo při ošetření rizik stanoveno pořadí priorit,
- byla stanovena priorita u činností vedoucích k redukci výskytu rizik,
- byly do rozhodnutí o řízení rizik zapojeny i zainteresované strany, a aby o stavu řízení rizik byly stále informovány,
- byla sledována účinnost ošetření rizik,
- byla rizika a procesy ošetření rizik sledovány a pravidelně přezkoumávány,
- byly získávány informace ke zlepšení přístupu k řízení rizik,

- byli vedoucí pracovníci i zaměstnanci školeni v oblasti rizik a opatření přijímaných k jejich zmírnění.

4.2 Stanovení kontextu

Stanovení kontextu vychází z účelu řízení rizik, protože stanovení účelu ovlivňuje celý proces řízení rizik. Účelem může být podpora systému řízení bezpečnosti informací, soulad s legislativou, definice požadavků na bezpečnost služby nebo produktu případně může být účelem určení výchozích poznatků pro plánování zvládání bezpečnostních incidentů nebo kontinuity podnikání (BCM – Business Continuity Management). Kontext zahrnuje přístup, který bude uplatněn pro řízení rizik, a to stanovením, jaká budou kritéria hodnocení rizik, dopadu rizik a akceptace rizik. Stanovení kontextu rovněž definuje rozsah a hranice řízení rizik, aby bylo jasně určeno, která rizika budou v rámci procesu brána v úvahu, a také s odůvodněním uvést všechna vyloučení z procesu v uvedeném rozsahu. Zavádění procesu řízení rizik a účinné provozování systému řízení rizik samozřejmě vyžaduje podporu managementu. Celý proces řízení rizik v ISO 27005 předpokládá, že vedoucí pracovníci i zaměstnanci budou informování o rizicích a způsobech jejich ošetření ke zmírnění rizik. Aby incidenty a události bylo možné řešit co možná nejúčinněji, je informovanost vedoucích a zaměstnanců důležitým aspektem, stejně jako definování rolí a odpovědností, stanovení vztahů zainteresovaných stran, eskalace rozhodování a podpora rozvoje procesu řízení rizik (ISO 27005, 2013).

4.3 Identifikace a hodnocení aktiv

Aktivem je vše, co má pro organizaci nějakou hodnotu a působením hrozeb může být hodnota aktiva snížena. Rozdělení aktiv může být členěno podle toho, jestli mají hmotnou či nehmotnou podobu. Hmotná aktiva jsou například hardware nebo software, nehmotná aktiva představují například informace či know-how (Čermák, 2009). Norma ISO 27005 dělí aktiva na primární a podpůrná (na ně se primární aktiva spoléhají). Primární aktiva jsou obchodní procesy a činnosti a informace, podpůrná aktiva pak jsou hardware, software, sítě, pracovníci, lokalita a další. Pro potřeby řízení rizik je třeba identifikovat všechny aktiva a zařadit je do registru, který obsahuje jejich popis a vlastnosti. Každé aktivum musí mít přiděleného právě jednoho vlastníka.

Na identifikaci aktiv navazuje proces ohodnocení aktiv. Hodnocení využívá škály, které na základě určujících kritérií stanoví hodnotu aktiv. Hodnota aktiva může být stanovena například finančním vyjádřením, nebo muže být nějakou kvalitativní formou – stupnicí, která například zařadí aktiva podle hodnoty. Stupnice může třídit hodnoty od velmi nízké po velmi vysokou. Hodnotu aktiva

ovlivňuje také závislost na procesech nebo jiných aktivech. Rozsahy stupnic, stanovení počtu úrovní a jejich vyjádření závisí na specifických potřebách. Větší počet stupňů umožňuje jemnější zařazování hodnot aktiv, ale také to může přiřazování hodnot komplikovat. Použití kvalitativních nebo kvantitativních stupnic vychází z rozhodnutí organizace, které stanoví, jakou stupnici budou k hodnocení aktiv používat, případně jestli budou využívat obě. Výstupem řízení aktiv je *seznam aktiv a jejich hodnot vztahující se k vyzrazení (zachování důvěrnosti), modifikaci (zachování integrity, autentičnosti, nepopiratelnosti a odpovědnosti), nedostupnosti a destrukci (zachování dostupnosti a spolehlivosti) a nákladům na výměnu* (ISO 27005, 2013, s. 41). Při hodnocení aktiva se podle (Smejkal, Rais, 2013) berou v úvahu:

- pořizovací náklady či jiná hodnota aktiva,
- důležitost aktiva pro existence či chování subjektu,
- náklady na překlenutí případné škody na aktivu,
- rychlost odstranění případné škody na aktivu,
- jiná hlediska (mohou být specifická případ od případu).

4.4 Identifikace hrozeb a zranitelností

Fáze identifikace hrozeb vychází ze seznamu hrozeb, které by mohly ohrožovat aktiva. Seznam hrozeb může být sestaven na základě rešerší odborné literatury, vlastních zkušeností nebo vyhodnocením dřívějších analýz. Některé hrozby mohou souviset také se subjektem a jeho statusem (podnikatelský subjekt, orgán státu, neziskové organizace a jiné), postavením na trhu, hospodářských výsledků, záměrů podnikatele (Smejkal, Rais, 2013) nebo specifickými motivy. Příklady typických hrozeb a zranitelností uvádí ve svých přílohách norma ISO 27005. Posouzení technických zranitelností, které závisejí na kritičnosti informačních a komunikačních technologií, peněžních a personálních zdrojích, je možné provádět testy informačních systémů, které zahrnují metody (ISO 27005, 2013):

- automatizovaný nástroj pro skenování zranitelností,
- testování a vyhodnocení stavu bezpečnosti,
- penetrační testování,
- analýzy zdrojových kódů.

Na tomto místě je třeba zdůraznit, že předcházející text se věnoval rizikům obecněji, ale dále v textu budou pod pojmem rizika brána v úvahu jen rizika, která se týkají informací, informační bezpečnosti, informačních systémů a informačních a komunikačních technologií, tedy všeho, co

by na tyto oblasti mohlo mít nějaký identifikovatelný dopad. Posuzování hrozeb počítá s původem hrozby (viz kapitola 3.10 Bezpečnostní hrozby). Vznik hrozby má původ environmentální, náhodný nebo úmyslný čin a dále posuzování zahrnuje, jaké zranitelnosti by mohla hrozba využít. Příklad, který uvádí Čermák (2009) ukazuje, že blesk je environmentální hrozbou (v případě hrozby blesku lze vyloučit úmyslné a náhodné působení) a zranitelnými jsou v tomto případě aktiva hardwaru, sítí a prostorů[6] (například software využívá aktiva lokality, hardware, případně aktiva sítí, a hrozba blesku zasahuje právě je, což je věcí stanovení vzájemných závislostí aktiv). Další přístup k posuzování hrozeb zahrnuje rozsah a následný dopad. V případě požáru je rozdíl, jestli hoří celá budova, nebo její část. Pak mohou následně vzniknout navazující rizika v podobě možnosti poškození vodou při likvidaci požáru, nebo snížení úrovně zabezpečení chráněných prostor uvnitř perimetru. V hodnocení lze také určit na kterou složku bezpečnosti informací (dostupnost, důvěrnost, integrita) má hrozba dopad. Například přerušení komunikace má dopad na dostupnost, ale integrita a důvěrnost nemusí být dotčena.

Pokud je zaveden systém řízení rizik, a jedná se o opakovanou činnost identifikace hrozeb a zranitelností (ale stejně tak i identifikaci aktiv), lze podle (ISO 27005, 2013) využít již získané informace a vyhnout se tak zbytečné, opakované práci, nebo přijímání duplicitních opatření. Kompletně musí být zpracovány všechny aspekty, týkající se nových aktiv, a v případě změn provést přezkoumání vlivu těchto změn. Zdrojem informací jsou také výsledky provedených auditů, které poskytují zpětnou vazbu a pohled na účinnost zavedených opatření.

Možným způsobem, jak vyjádřit hrozby a zranitelnosti pro jednotlivá aktiva, je forma hodnotícího formuláře (Tabulka č. 5). Předpokládá se aktuální a vhodně spravovaný seznam aktiv, udržované seznamy hrozeb a zranitelností, které jsou využívány v procesu zpracování hodnocení všech hrozeb a zranitelností pro každé aktivum. Nezbytným vstupem pro hodnocení podle Tabulky č. 5 je definice všech používaných stupnic. Hodnocení aktiv je komplexní přehled možných rizik, a na základě výsledků z procesu hodnocení lze určit priority pro další postup řízení rizik. Pro možnost stanovení priorit všech aktivit obsahuje sloupec Riziko v Tabulce č. 5 pomocnou hodnotu, která počítá i s Hodnotou aktiva. Další vlastností tohoto způsobu hodnocení je, že je v něm počítáno se všemi hrozbami a všech možných zranitelností, které souvisí s konkrétní hrozbou pro každé aktivum. Takto hodnocená jsou všechna aktiva, což má za výstup kompletní přehled všech rizik a zároveň je východiskem pro analýzu rizik. Součástí výstupu by měl být i popis dopadu způsobený

[6] ISO 27005 nepoužívá termín prostory, ale lokality

ztrátou dostupnosti, důvěrnosti a integrity v podobě scénáře incidentu a jeho následků, jak doporučuje (ISO 27005, 2013).

Tabulka 5: Vyjádření hrozeb a zranitelností. Zdroj: Autor

Aktivum	Hodnota	Hrozba	Zranitelnosti	Pravděpodobnost	Dopad	Riziko	Opatření
Aktivum 1	5	Hrozba A	Zranitelnost 1	2	4	8/40	Opatření 1
			Zranitelnost 2	4	3	12/60	
			Zranitelnost 3	3	2	6/30	
			Zranitelnost 4	2	2	4/20	
		Hrozba B	Zranitelnost 5	4	3	12/60	
			Zranitelnost 6	3	4	12/60	Opatření 2
			Zranitelnost 7	1	1	1/5	
		Hrozba C	Zranitelnost 8	2	1	2/10	
			Zranitelnost 9	1	4	4/20	Opatření 3
			Zranitelnost 10	1	3	3/15	

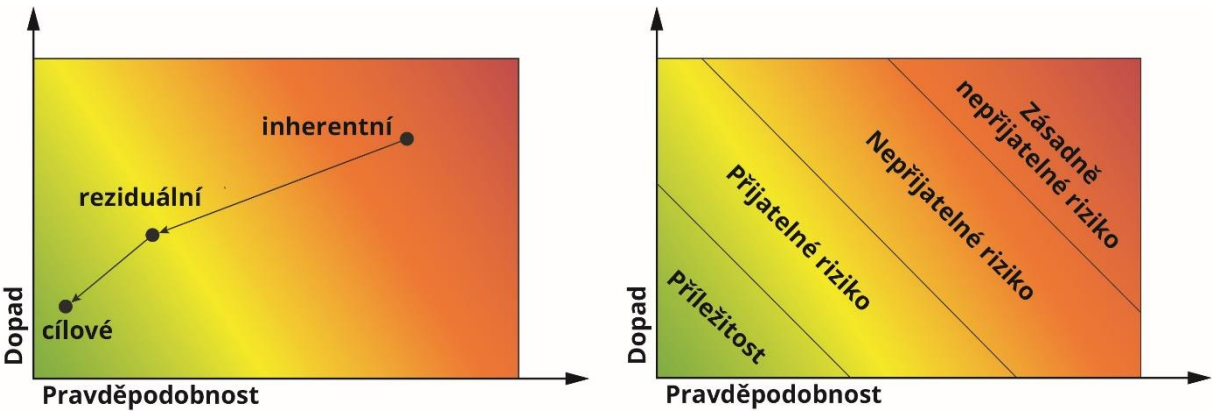
4.5 Analýza rizik

Pro účely analýzy rizik je nutné znát, jaké hrozby mohou využít některou ze zranitelností a jejich slabin, které by měly nějaký nepříznivý dopad na aktiva. Opět se lze odkázat na Obrázek č. 15, kde je zobrazen cyklus procesu řízení rizik. Na obrázku jsou vyznačeny body A a B, tedy kontrolní body procesu řízení rizik. Bod A je bodem rozhodnutí o uspokojivém hodnocení rizika. Pokud jsou získané informace z hodnocení rizik nedostatečné, bude nutné provést další opakovaná posouzení rizik. Opakované hodnocení rizik musí vycházet z revidovaného kontextu (ISO 27005, 2013). Tato část řízení rizik zahrnuje stanovení kontextu a hodnocení rizik. Výstup je posouzen z hlediska upokojivého hodnocení (vyznačeného bodu A).

V závislosti na okolnostech kritičnosti a rozsahu zranitelností volí organizace kvalitativní nebo kvantitativní metodiku analýzy rizik, případně kombinaci obou uvedených. Kvalitativní analýza využívá k popisu dopadu stupnice (například nízký, střední, vysoký) a spojuje dopad s kvalitativním vyjádřením pravděpodobností, s jakou by mohly incidenty nastat. Kvalitativní metodika je snadno pochopitelná, ale nese s sebou prvky subjektivní povahy, zvláště u zatřídění do hodnotících stupnic. Kvalitativní metodiky se využívají v případech, kdy je obtížná kvantifikace rizika. Kvantitativní metodiky pracuji s čísly, respektive s číselnými škálami. Tento způsob analýzy je závislý na dostupnosti konkrétních, aktuálních, přesných a úplných číselných hodnot, což může být zároveň nevýhodou této metodiky. Jako vstup pro posouzení následků uvažovaného dopadu rizika jsou výstupy z procesů identifikací a hodnocení aktiv, hrozeb a zranitelností, scénářů incidentů a výstup z analýzy rizik. Posouzení následků určuje, jaký dopad může mít následek

incidentu na organizaci a jejích fungování, náklady na obnovení provozu a ztráty v obchodních oblastech. Analýzy dopadů incidentů uvažují při hodnocení také jakou měrou se na aktivu projeví, zda bude aktivum ovlivněno jen částečně, nebo zda se vzájemné propojení aktiv projeví i dopadem na závislých aktivech. Samotný dopad incidentu je závislý na pravděpodobnosti, s jakou se daný scénář může projevit. Pravděpodobnost zohledňuje četnost možného výskytu za časovou jednotu a v úvahu jsou brány zkušenosti a statistiky, aspekty úmyslných a neúmyslných činů a vlastnosti samotných zranitelností (ISO 27005, 2013). Výstupem je přiřazení pravděpodobnosti každému z posuzovaných scénářů, například způsobem, který nastiňuje Tabulka č. 5.

Na každé riziko (scénář incidentu a jeho dopad) lze aplikovat nástroj mapy rizik. (Svatá, 2016) uvádí příklad mapy rizik, která je uvedena na Obrázku č. 17 v pravé části. Výsledné riziko v závislosti na pravděpodobnosti a dopadu rizika je vyjádřeno v mapě na základě obou veličin. Je tak graficky znázorněno, ve kterém pásmu rizikové oblasti se dané riziko nachází. Oblasti zahrnují pásma, jejichž parametry rizikového apetitu[7], určují, jaký postoj zastává organizace k rizikům, a pro každou organizaci jsou jiná. Vyhodnocení rizika, které bude zařazeno do oblasti „zásadně nepřijatelného rizika“ (viz pravá část Obrázku č. 17) vyžaduje maximální úsilí a okamžité řešení rizika. Zásadně nepřijatelná rizika by měly mít dopad na priority v řízení rizik. Riziko, které má vysokou pravděpodobnost a značný dopad, může být pro organizaci velkým problémem. Organizace proto musí přijmout taková opatření, aby nebyla vystavena tak vysoké míře rizika. Postup a cíl ošetření významných rizik je zobrazen v levé části Obrázku č. 17.



Obrázek 17: Mapa rizik. Zdroj: (Smejkal, Rais, 2013; Svatá, 2016)

V rámci přístupu k analýze rizik mohou organizace zvolit přístup, zda provedou analýzu s pomocí vlastních zdrojů, nebo využijí služeb externích specialistů. Rozdíly, které s sebou nese rozhodnutí,

[7] Stanovené prahové hodnoty v přístupu k riziku

jak organizace přistoupí k analýze rizik a možné výhody a nevýhody zvoleného přístupu shrnuje Tabulka č. 6.

Tabulka 6: Srovnání charakteristik interní a externí analýzy rizik. Zdroj: (Čermák, 2009)

Interní analýza rizik	Externí analýza rizik
znalost prostředí a procesů	zkušenosti z jiných společností
zachování důvěrnosti	porušení důvěrnosti
nutno koupit nebo vyvinout metodiku	není nutné kupovat nebo vyvíjet metodiku
nutno koupit nebo vyvinout nástroj	není nutné kupovat nebo vyvíjet nástroj
nutno mít nebo vyškolit vlastní odborníky	není nutné mít vlastní odborníky
všichni rozumí výstupům projektu	výstup projektu je nesrozumitelný
neschopnost vést interview	schopnost vést interview
nižší míra objektivity	vyšší míra objektivity
nižší cena	vyšší cena
více zatěžuje společnost	méně zatěžuje společnost

4.6 Zvládání rizik

Zvládání rizika, nebo podle terminologie normy ISO 27005 ošetření rizik bezpečnosti informací, je opět znázorněno na Obrázku č. 15 a v něm vyznačené sekci Zvládání rizik. Účinnost zvládání rizik je v obrázku naznačeno bodem B. Tento bod označuje na fázi procesu, který hodnotí, zda jsou přijatá opatření uspokojivá a zbytková rizika jsou akceptovatelná, což vychází z návrhu ošetření rizik. Možnosti ošetření rizika zahrnují (IOS 27005, 2013):

- **Modifikaci rizik** – přijaté změny v opatření nebo zavedení nových opatření má vést k tomu, že úroveň rizika bude přehodnoceno jako akceptovatelné.
- **Podstoupení rizik** – v tomto případě přijímá organizace rozhodnutí, že úroveň rizika je přijatelná a je splněno kritérium akceptace rizika.
- **Sdílení rizik** – sdílením rizika lze ve spolupráci s jinou stranou dosáhnout změny rizika. Změna rizika může znamenat snížení úrovně rizika, ale také vnik nových rizik a zvládání tohoto rizika může vyžadovat další ošetření rizik. Příkladem sdílení rizik je dohoda mezi obchodními partnery nebo pojištěním.
- **Vyhnutí se riziku** – tento přístup vyžaduje identifikaci podmínky, která umožní vyhnout se riziku například ukončením vysoce rizikových procesů nebo odstěhováním se z lokality, která je svým umístěním nevhodná pro bezproblémový chod organizace.

5 Audit

V předchozích kapitolách se práce věnovala kybernetické bezpečnosti a řízením rizik. Tato kapitola naváže na významnou oblast kybernetické bezpečnosti a řízení rizik. Touto oblastí je audit. Obsahem kapitoly je vysvětlení důležitých pojmů. Audit bude uveden do kontextu auditování systémů managementu a dále bude směřovat k auditu kybernetické bezpečnosti podle ISO norem a současné i budoucí legislativy.

5.1 Co je to audit

Audit je pojem, který je stále více používán, ale jeho význam nemusí být vždy správně pochopen. Slovo audit má původ v latině. Latinské sloveso auditus (sluch) je spojováno s historickým obdobím, kdy lidé neuměli číst ani psát, ale bylo zapotřebí správcům majetku sdělovat výsledky a stavy hospodaření. Později se v Řecku a Římě audit využíval jako způsob kontroly stavu veřejných účtů, tedy jakousi původní a výchozí podobou dnešních forem auditů, jako je finanční audit. Právě finanční audit je chápán jako základní druh auditu a z něj vycházející další formy auditů (Svatá, 2012). Definic auditu existuje více. Například (Slámečka, 2012) uvádí jako jedno z možných vysvětlení, že hlavní vlastností auditu je kritický pohled na systém, objektivní získávání a vyhodnocování důkazů, zjišťování souladu mezi zjištěným stavem a stanovenými kritérii a ujištění druhé strany o kvalitě. Výkladový slovník kybernetické bezpečnosti audit definuje jako *systematický, nezávislý a dokumentovaný proces k získání důkazů z auditu a jejich objektivní ohodnocení, aby se určil rozsah, v jakém jsou auditní kritéria splněna* (Jirásek, Novák, Požár, 2015, s. 20). V rámci významu auditu pro organizaci *představuje nezastupitelný nástroj zpětné vazby mezi vlastníky různých aktiv, okolím organizace, managementem a zaměstnanci, na které management deleguje svoje pravomoce* (Svatá, 2016, s. 13). Jak bylo zmíněno, finanční audit je považován za základní formu auditu. Smyslem a posláním auditu je podle (Poslání a smysl auditu, 2018) vyjádření názoru nezávislého, kvalifikovaného odborníka, který podává věrný a poctivý obraz skutečnosti s dostatečnou vypovídající schopností v rámci kontextu auditu a jeho zjištění. Přínosy auditu (dále už jen v kontextu bezpečnosti informací) spočívají podle (Lidinslý, a kol., 2008) v poskytnutí skutečného obrazu o fungování ve srovnání s obvyklým standardem a výstupy jsou průkazné, správné a obsahují doporučení pro rozvoj bezpečnosti informací systémů a akční plán jejich implementací, včetně popisu, požadavků, časové a finanční náročnosti a očekávaných přínosů. Výstupy z auditu pak mohou být pro management východiskem pro změny v systému. *Kontrola a audit IS/ICT představují organickou součást procesu zajištění bezpečnosti IS/ICT*

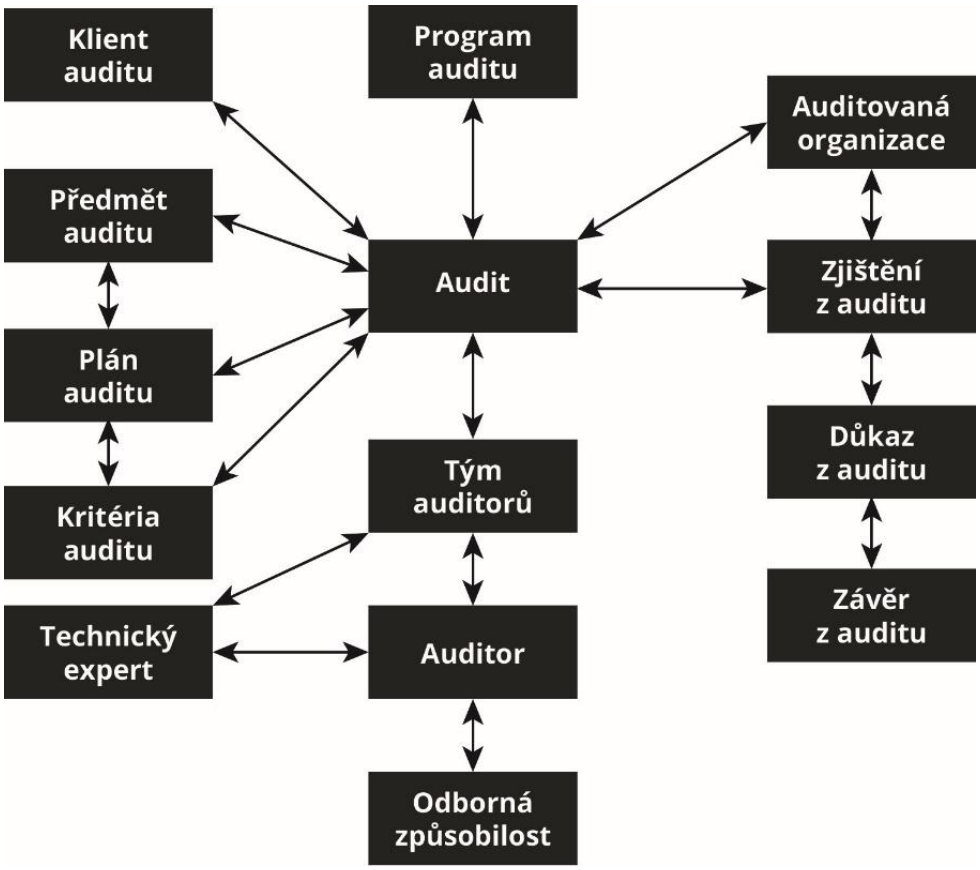
v organizaci. Jejich procesy přímo navazují na zavedení určité úrovně – standardů – bezpečnosti IS/ICT v organizaci a v delším časovém horizontu zaručují, že požadovaná (nastavená) úroveň bezpečnosti také dodržována (Doucek, 2004, s. 16).

Jak uvádí (Svatá, 2016) audit musí splňovat základní vlastnosti, jako je:

- **komplexnost** – musí postihnout všechny relevantní aspekty,
- **objektivnost** – musí se opírat o existující standardy, případně zkušenosti, pokud standardy neexistují,
- **nezávislost** – auditor nemá s objektem auditu ani se zadavatelem auditu žádné spojení, které by představovalo konflikt zájmů,
- **formalizovanost** – proces auditu se musí řídit metodikou a existujícími standardy.

5.2 Audit podle norem ISO

V rámci celé koncepce norem ISO (a jejich vzájemné provázanosti) lze najít základ v normě ISO 9000. V této normě jsou uvedeny důležité pojmy a vtahy, které jsou uvedeny na Obrázku č. 18 a v Tabulce č. 7.



Obrázek 18: Vztahy a pojmy týkající se auditu. Zdroj: (ISO 9000, 2005)

Tabulka 7: Důležité termíny. Zdroj: (ISO 9000, 2005)

Termín	Definice
audit	systematický, nezávislý a dokumentovaný proces pro získávání důkazů z auditu a pro jeho objektivní hodnocení s cílem stanovit rozsah, v němž jsou splněna kritéria auditu
program auditu	jeden audit nebo soubor několika auditů naplánovaných pro určitý časový rámec a zaměřených na specifický účel
kritéria auditu	soubor dílčích politik, postupů nebo požadavků používaných jako základ
důkaz z auditu	záznamy, konstatování skutečnosti nebo jiné informace, které souvisejí s kritérii auditu a jsou ověřitelné
zjištění z auditu	výsledky hodnocení shromážděných důkazů z auditu podle kritérií auditu
závěr z auditu	výstup z auditu poskytnutý týmem auditorů po zvážení cílů auditu a všech zjištění z auditu
klient auditu	organizace nebo osoba žádající o audit
auditovaná organizace	organizace, u které se provádí audit
auditor	osoba s prokázanými osobními vlastnostmi a odbornou způsobilostí k provádění auditu
tým auditorů	jeden nebo více auditorů, kteří provádějí audit podporovaných v případě potřeby technickými experty
technický expert	osoba, která poskytuje týmu auditorů specifické znalosti nebo odborné posudky
plán auditu	popis činností a uspořádání organizace auditu
předmět auditu	rozsah a vymezení auditu
odborná způsobilost	prokázané osobní vlastnosti a prokázaná schopnost aplikovat znalosti a dovednosti

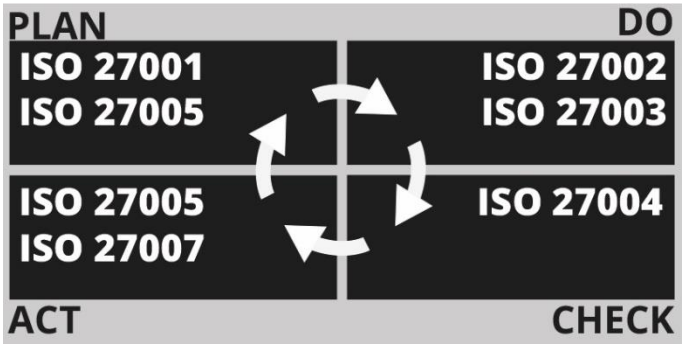
Vztahy uvedené na obrázku lze vysvětlit následujícím způsobem: Auditor je osoba s potřebnou kvalifikací a vhodnými vlastnosti pro výkon auditu. Může být součástí týmu auditorů. Tento tým podle potřeby komunikuje s experty a spolupráce zahrnuje poskytování odborných posudků, specifických znalostí nebo konzultací. Audit je prováděn na základě žádosti klienta, který o tuto službu má objektivní zájem. V rámci příprav a plánování auditu je identifikován předmět auditu, tedy jeho rozsah a vymezení auditu. Přípravy auditu vycházejí z kritérií, která se zakládají na politikách, postupech a požadavcích, a týkají se auditovaného systému. Organizace, u které vznikla potřeba uskutečnit audit systému, má zájem prostřednictvím auditem zjištěných výsledků ověřit, zda vyhovuje všem kritériím kladených na systém. Tato zjištění by měla být podpořena a doložena relevantními důkazy. Výstupem auditu je prezentování posouzených výsledků žadatelům, nebo odpovědným zástupcům auditované organizace.

V rámci řízení bezpečnosti informací podle ISO 27001 a ve svém důsledku i podle zákona o kybernetické bezpečnosti včetně jeho prováděcí vyhlášky je základem auditu norma ISO 27007. Tato norma uvádí kontext auditů do prostředí bezpečnosti informací. Audit podle ISO 27007 je

postaven na směrnici pro auditování systémů managementu (ISO 19011) a ta zase těží ze základů, které jsou v normě ISO 9000, jak tuto skutečnost ilustruje Obrázek č. 19.

Obrázek 19: Odkazování v normách. Zdroj: Autor

Systém řídících a kontrolních procesů, které mají za cíl provozovat, rozvíjet a zlepšovat systém řízení bezpečnosti informací, je postaven podle koncepce PDCA. Obrázek č. 20 popisuje, jak je v tomto cyklu začleněna norma ISO 27007. Fáze act (jednej) je agentem zlepšování, který je založen na vyhodnocování požadavků a opatření a poskytuje zpětnou vazbu.



Obrázek 20: ISO 27007 v procesech řízení bezpečnosti informací. Zdroj: Autor

Na tomto místě je třeba zmínit významnou vlastnost týkající se vazeb mezi různými ISO normami. Normy vznikají v různých obdobích a jsou ovlivňovány vývojem, který má dopad strukturu i obsah. Kromě běžně uváděného názvu normy jsou dalšími důležitými údaji normy: rok schválení a rok přijetí. Například norma ISO 19001 byla schválena 11. května 2011, publikována byla v listopadu 2011, česká mutace byla schválena 1. června 2012, datum účinnosti normy je od 1. července 2012 a její celý název je ISO 19011:2011. Normou citované dokumenty jsou tedy starší, než je sama norma ISO 19011:2011, a na ni se odkazují normy novější. Práce s normami neumožňuje práci tak, aby vždy odkazovaly na aktuální a platné dokumenty. Odkazy z ISO 27005:2011 se odvolávají na ISO 27001:2005, což je komplikovaný přístup k řízení bezpečnosti informací, protože poslední revize ISO 27001 byla vydána v září 2014 (publikována byla v říjnu 2013). V novějším vydání ISO 27001 je uplatněná rozdílná struktura a členění celého obsahu, navíc nutno brát v ohled změny týkající se aktuálnosti požadavků a opatření. Od dubna 2018 jsou platné normy ISO 27003 a 27004. Tyto normy odkazují už na 27001:2013.

Jak již bylo zmíněno, norma ISO 27007 je v sadě norem 27000 dokumentem, který se zabývá auditem systémů řízení bezpečnosti. Jedním z úkolů normy je adaptovat auditování systému managementu do prostředí bezpečnosti informací. Norma ISO 27007 kopíruje strukturu

i obsah normy ISO 19011. V pasážích, které jsou v ISO 19011 příliš obecné nebo neodpovídají požadavkům auditu bezpečnosti informací, uvádí ISO 27007 cíle a opatření do souvislosti s požadavky a cíli ISMS, věnuje se určení rozsahu programu auditu a definování cílů, předmětu a kritérií auditu.

5.3 Role auditora

Auditor musí splňovat vlastnosti, schopnosti, dovednosti a používat koherentní myšlení. Tyto vlastnosti jsou nezbytné pro provádění auditů. Pro provádění auditů se jedná o specifika, která jsou pro audit managementu bezpečnosti informací skutečně významná, aby závěry z auditu byly správné a přínosné. Jedná se o znalosti týkající se norem ISO (řada 27000, 19011, 17021, 9000 a další), zákonů a vyhlášek týkající se nejen bezpečnosti informací, ale i ochrany osobních údajů a dalších souvisejících zákonů, znalosti postupů, procesů a metod posuzování, řízení, monitorování a měření bezpečnosti informací (ISO 19011, 2011), specifik a typických rizik daného odvětví, ale také osobnostních a povahových rysů, jako jsou vlastnosti podle (ISO 17021-1, 2016):

- dodržování etických principů. tj. férovost, pravdivost upřímnost, poctivost a diskrétnost,
- otevřenost jiným názorům, tj. ochota zvážit alternativní myšlenky nebo jiné pohledy na věc,
- diplomacie, tj. takt při jednání s lidmi,
- ochota spolupracovat, tj. efektivně spolupracovat s dalšími,
- pozornost, tj. aktivně st uvědomovat fyzické okolí a okolní činnosti,
- vnímavost, tj. instinktivní povědomí o různých situacích a schopnost je pochopit,
- flexibilita, tj. rychlé přizpůsobení se různým situacím,
- vytrvalost, ti. vytrvalé soustředění se na splnění cílů,
- rozhodnost, ti. dosahováni včasných závěru založených na logickém zdůvodnění a analýzách,
- soběstačnost, tj. schopnost jednat a pracovat samostatně,
- profesionalita, tj. zdvořilé, svědomité a všeobecně vstřícné chování na pracovišti,
- morální kredit, tj. ochota jednat nezávisle a eticky i ve chvíli, kdy toto jednaní nemusí být vždy populární muže vest ke sporům nebo konfrontacím,
- organizace, tj. realizování efektivního řízeni času stanovovaní priorit, plánování a účinnost jednání.

Nežádoucí chování může mít vliv na audit a projevy závisí na konkrétní situaci. Během auditu se lidé s auditory střetávají při konzultacích, interview a při různých profesně společenských

setkáních. Napětí nebo jisté nesympatie pak mohou narušit důvěru k auditorům, a tím i k samotnému auditu. Budování pozitivních vztahů mezi auditory a zaměstnanci organizace je pro průběh auditu minimálně prospěšný.

Kvalifikační požadavky, které musí auditor splňovat, uvádí ve svých přílohách novelizovaná vyhláška kybernetické bezpečnosti. Doložením odborné kvalifikace může být uznávaná certifikace auditora označovaná jako CISA (Certified Information Security Auditor), kterou nabízí organizace Isaca stejně jako certifikace CRISC (Certified in Risc and Information Systém Controls). Kromě těchto certifikací vyhláška považuje za relevantní certifikace auditora také CIA (Certified Internal Auditor) a Lead Auditor ISMS (Lead Auditor Information Security Management System), která má velmi blízko k ISO normě 27001. Přesněji se jedná o certifikaci způsobilosti vést audit bezpečnosti informací právě podle normy ISO 27001.

Role auditora je také spjata s přístupem k auditu. Z pohledu průběhu auditu a působení auditora v organizaci norma (ISO 19011, 2011) dělí audit na:

- interní audit a
- externí audit, tj.
    - dodavatelský audit nebo
    - audit třetí stranou.

Interní audit (audit první stranou) je zajišťován vlastními silami v rámci organizace. Podle vyhlášky o kybernetické bezpečnosti je v rámci plnění povinností stanovení bezpečnostních rolí. V rámci těchto rolí musí být stanovena také role auditora kybernetické bezpečnosti[8]. Není zde jasně vymezeno, že osobou v roli auditora musí být interní zaměstnanec. Pokud je auditorem interní zaměstnanec, není zákonem ani vyhláškou stanovena nutnost jeho nezávislého postavení v rámci organizace, jako je tomu v zákonu 320/2001 Sb. o finanční kontrole[9]. V případech externího auditu se jedná o audity prováděné zákazníky u jejich dodavatelů (audit druhou stranou) a v rámci auditu mohou využít (stejně tak i pro audit první stranou) normu ISO 19011. Další formou externího auditu je audit třetí stranou. Ten může být prováděn pro účely auditu souladu se zákony nebo pro účely certifikace. Dokumenty s požadavky na orgány poskytující službu auditu mohou vycházet z normy ISO 27006 a ISO 17021-1, nebo i ISO 27021-6 a jiné.

[8] Podle § 6 odst. 3 písm. d; toto upravuje § 6 odst. 4 tak, že pro osoby uvedené v § 3 písm. e) zákona určí roli přiměřeně vzhledem k rozsahu a potřebám systému řízení bezpečnosti informací

[9] Podle § 28 a § 29 zákona 320/2001 Sb.; podle VoKB je podmínkou jen nestrannost od rolí manažera KB, architekta KB a garanty aktiv

S rolí auditora je také spjato jeho hodnocení, a podle (ISO 19011, 2011) je součástí auditu resp. fáze programu auditu. *Důvěryhodnost procesu auditu a schopnost dosahovat jeho cílů závisí na kompetencích jednotlivců zapojených do plánování a provádění auditu včetně auditorů a vedoucích týmu auditorů* (ISO 19011, 2011, s. 41). Hodnocení auditora zahrnuje prvky zpětné vazby. Hodnocení se týká od rozvoje znalostí až k přezkoumávání výsledků auditora a jím vyhotovených dokumentů a výsledků.

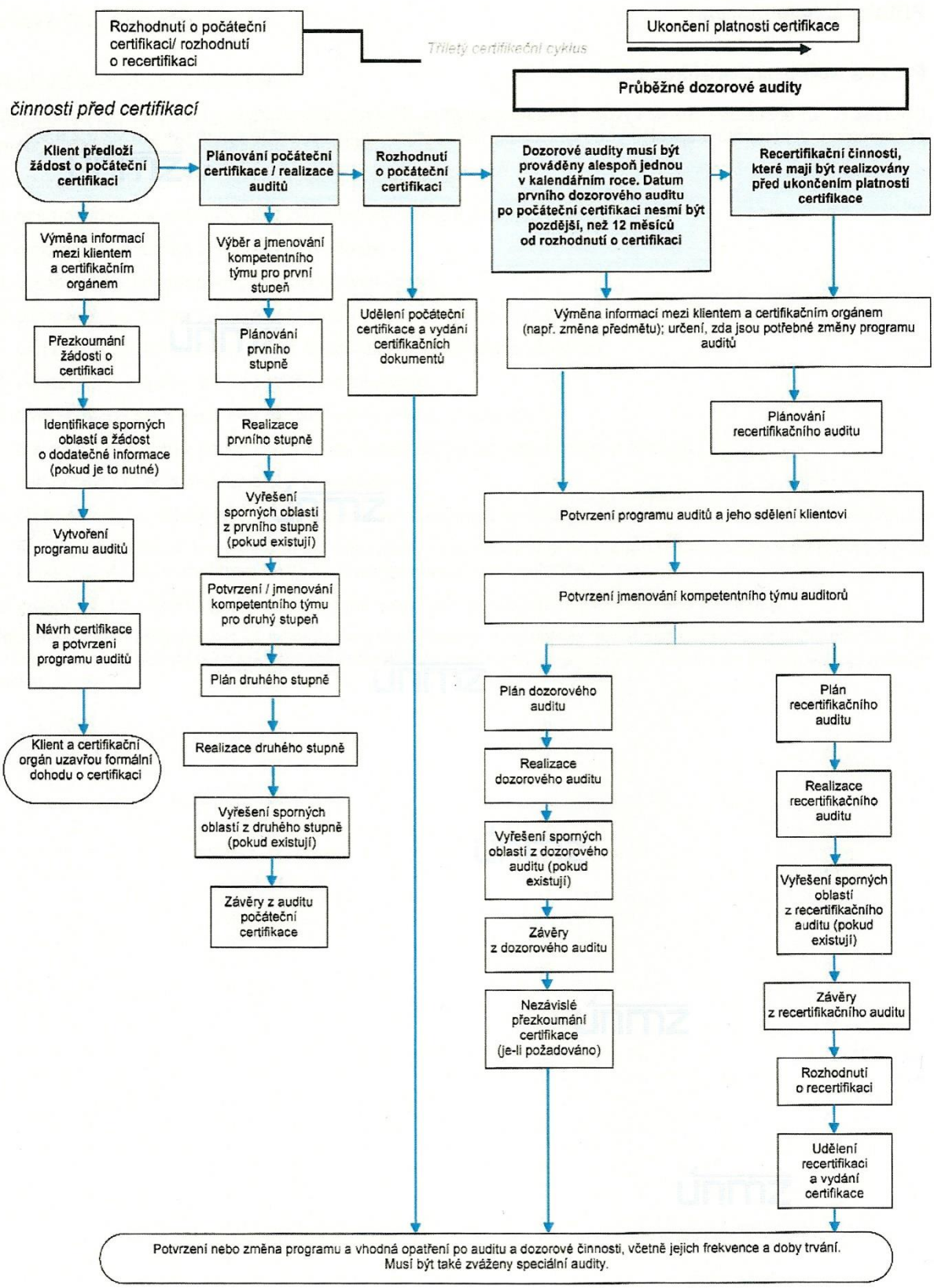
5.4 Institut auditu z pohledu poskytovatele služby auditu

Vyhláška o kybernetické bezpečnosti a řízení bezpečnosti informací podle ISO 27001 umožňují, že ISMS s platnou certifikací[10] dle ISO 27001 udělenou akreditovaným certifikačním orgánem je v souladu s požadavky vyhlášky.

Již bylo zmíněno, že v rámci bezpečnosti informací a auditu bezpečnosti informací existují normy ISO 17021-1 a ISO 27006. Jejich obsah je zaměřen na doporučení a požadavky, které orgány provádějící audity (podle ISO 27006 myšleno audity ISMS) musejí splňovat, aby podpořily proces akreditace organizace, která poskytuje certifikace – tedy audity třetí stranou (ISO 27006, 2015). Proces certifikace je zobrazen na Obrázku č. 21. Organizace poskytující certifikaci podle ISO 17021-1, které mají v rámci své působnosti zájem rozšířit portfolio nabízených služeb o certifikaci systémů bezpečnosti informací ISMS, musejí přijmout dodatečné požadavky a doporučení, které uvádí ISO 27006. V normě je explicitně zmíněno, jaké požadavky je nutno dodržet (shall) a jaké požadavky by měly být dodrženy (should) (ISO 27006, 2015).

Norma ISO 27006 udává jako svůj hlavní cíl *umožnit akreditačním orgánům její efektivní použití a harmonizaci s ostatními normami, podle kterých se provádí hodnocení certifikačních orgánů usilujících o akreditaci* (ISO 27006, 2015, s. 7). Stejně jako u norem týkající se auditu první a druhou stranou, které využívají normu ISO 27007 postavenou na základech ISO 19011, platí u norem týkajících se auditu třetí stranou obdobný způsob odkazování. Základní požadavky jsou uvedeny v ISO 17021-1. Norma ISO 27006 těchto základů využívá a významné aspekty a specifika upravuje pro prostředí související s ISMS. ISO 27006 zmiňuje například, že požadavky na auditory se zaměřují na znalost terminologie a s auditem ISMS souvisejících znalostí, zkušeností a dovedností. Do týmu auditorů jsou vybírání ti, kteří mají relevantní a aktuální zkušenosti. Jen tak lze plnit důvěryhodnost a správnost závěrů auditu z hlediska personálního obsazení.

[10] za podmínky uvedené v § 3 odst. 2 novelizované VoKB



Obrázek 21: Typický vývojový diagram procesu auditu a certifikace. Zdroj: (ISO 17021-1, 2016)

U auditu třetí stranou je nutnost zmínit požadavek, který říká, že pokud před zahájením organizace, poskytující službu auditu u auditované organizace v rámci přípravy programu auditu, zažádá o dokumenty, které jsou považovány za citlivé nebo důvěrné, a auditovaná organizace tyto dokumenty neposkytne, akreditující organizace posoudí relevantnost odmítnutí poskytnout dokumenty a zhodnotí adekvátnost auditu při absenci některých dokumentů. Závěrem může být, že nebude možné audit provést a o této skutečnosti musí klienta informovat.

5.5 Audit a jeho fáze podle ISO 19011

Norma je určena širokému spektru uživatelů, kteří mají zájem nebo potřebu provádět audity systémů managementu, ať už je důvodem zájem poznat, zjistit a ověřit skutečný stav systému, nebo je k tomu přiměje důsledek plynoucí ze smluvních podmínek nebo je organizace povinným subjektem legislativních nařízení a regulací. Norma je navržena s ohledem na flexibilitu použití a u organizací, které chtějí normu uplatnit, nezáleží na její velikosti, úrovni vyspělosti systému managementu nebo na specifických podmínkách auditované organizace od typu a složitosti specifik až k cílům a předmětu auditu. Norma také *zavádí koncepci rizik do auditování systémů managementu. Přijatý přístup se týká rizika, že proces auditu nedosáhne svých cílů a potenciální možnost narušení auditu narušit činnosti a procesy auditované organizace* (ISO 19011, 2011, s. 7).

Audit podle (ISO 19011, 2011) závisí na několika zásadách a principech, které z auditu vytvářejí spolehlivý a efektivní nástroj zpětné vazby a kontroly managementu. Umožňuje zlepšování systému na základě cílů politik a nástrojů managementu. Tyto principy vytvářejí předpoklad, že závěry, ke kterým audit dospěje, bude nezávislý a auditoři dospějí k podobným závěrům za předpokladu podobných okolností. Principy, které norma využívá:

- Integrita – auditoři pracují poctivě, svědomitě a odpovědně, prokazují kompetenci vykonávat audit a jeho úsudek by neměl být ovlivněn působení jakýchkoliv vlivů. Svůj úkol směřující k cílům auditu, vykonává v souladu s platnou legislativou a všech relevantních regulací.
- Spravedlivé prezentování – veškeré zjištění, zprávy a závěry auditu pravdivě a přesně odrážejí činnosti při auditu. Zároveň je nutností informovat o významných překážkách.
- Profesionální přístup – auditoři při výkonu svých povinností dbají, aby svěřené úkoly vykonávali s náležitou péčí a v souladu s významem a důležitostí. Veškerá rozhodnutí, ke kterým dospěje, mají být náležitě odůvodněné.

- Důvěrnost – auditor si musí být vědom, že informace, se kterými přijde do styku, jsou důvěrné. Tyto informace nesmí zneužít ke svému vlastnímu prospěchu, nebo nesmí důvěrné informace použít jakýmkoliv nevhodným způsobem, a tím způsobil auditované organizaci škodu.
- Průkaznost – závěry z auditu by měly být koncipovány na získaných dokumentech, důkazy by měly být ověřitelné. Audit může probíhat během omezeného časového období, a i zdroje během auditu jsou omezené, a proto mohou být využity důkazy založené na vzorcích. To může mít spojitost se spolehlivostí závěrů.
- Nezávislost – auditoři by měli být v rámci možností zcela nezávislí na auditované organizaci a zachovat nestrannost a vyloučit střety zájmů. Interní auditoři by měli mít zajištěnou nezávislost na manažerských funkcích, aby byla zachována důvěryhodnost auditu.

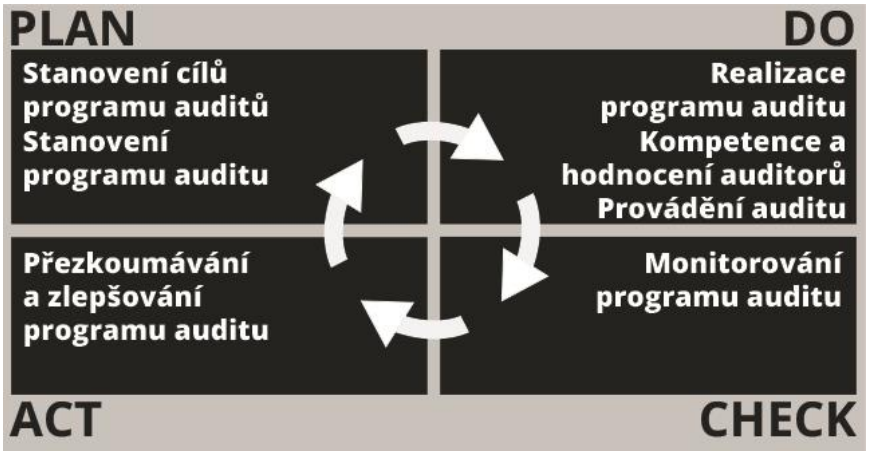
V normě ISO 27006 je uvedeno, které činnosti nejsou střetem zájmů, a certifikační orgán tyto činnosti může vykonávat bez narušení střetu zájmu. Jedná se například o provádění činností související se školením a přednáškami, zveřejnění vlastního výkladu požadavků norem, podle kterých provádí certifikaci nebo poskytování informací, které se zaměřují na připravenost před auditem.

5.5.1 Řízení programu auditu

Úkolem vrcholového vedení organizace je stanovení cílů programu auditu. Přihlíží se při tom i k tomu, že současně mohou probíhat také jiné programy, které mohou probíhat odděleně, současně nebo se vzájemně doplňovat. Program a jeho rozsah vychází z charakteristiky organizace a všech významných vlastností, které mají na systémy managementu vliv. Program a zdroje, které jsou důležité pro efektivní a účinné provádění auditů mohou zahrnovat:

- cíle programu auditů a jednotlivých auditů,
- rozsah, počet, druhy, doby trvání, místa, časové harmonogramy auditů,
- řízení programu auditů,
- kritéria auditů,
- metody auditů,
- výběr týmu auditorů,
- nezbytné zdroje, včetně cestování a ubytování,
- procesy pro zacházení s důvěrnými informacemi, bezpečností informací a další procesy.

Průběh řízení programu je zobrazen na Obrázku č. 22. Posuzování dosahování cílů auditů má zlepšovat dosahovaní programu auditu, jeho výsledků a samozřejmě cílů. Stanovení cílů programu auditu respektuje vztahy k partnerům, platnou legislativu, požadavky managementu a je sledován soulad mezi cíli a zjištěnými skutečnostmi.



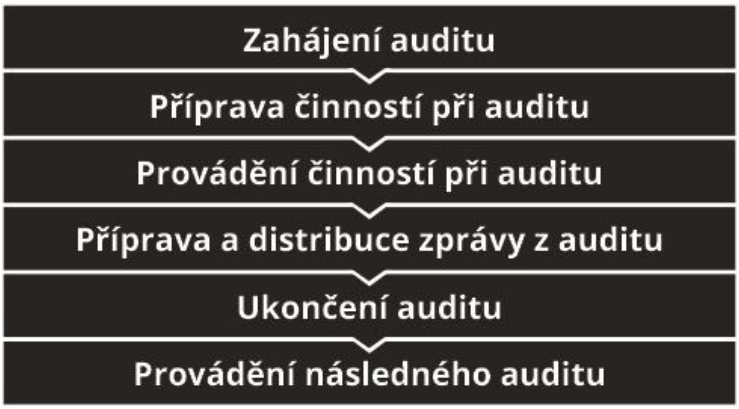
Obrázek 22: PDCA cyklus programu auditu. Zdroj: (ISO 19011, 2011)

V rámci stanovení programu auditů jsou určeny role, odpovědnosti osob řídících program auditu a jejich kompetence. V rámci svých povinností vedoucí osoba, řídící program auditů, vede komunikaci s vedením. Dále se stanovuje rozsah programu auditu, odpovídající podmínkám organizace, identifikují a hodnotí se rizika programu auditu, která jsou spojená s plánováním, zdroji, týmem auditorů, a se samotným průběhem auditu. Během stanovení postupů auditu se odpovědná osoba věnuje plánování a sestavováním harmonogramu, výběru členu týmu, zajišťuje bezpečnost a důvěrnost informací, provádí a zaznamenává audity. Identifikace zdrojů zahrnuje způsob financování a všech souvisejících výdajů, spojených s auditem, výběr metod auditu a dostupnost informačních a komunikačních technologií. Realizace programu auditu zahrnuje komunikaci během průběhu od oznámení přes pravidelné informování o průběhu. Osoba, řídící program auditu, realizuje a koordinuje všechny související činnosti pro bezproblémový průběh a zajišťuje potřebné zdroje. Monitorování je fáze, která hodnotí shodu s harmonogramy a cíli, výkonnost členů týmu a jejich schopnosti a poskytuje zpětnou vazbu systému řízení programu auditu (ISO 19011, 2011).

5.5.2 Provádění auditu

Průběh auditu a jeho návaznosti je naznačen na Obrázku č. 23. Zahájení auditu zahrnuje úvodní kontakt s auditovanou organizací. Během komunikace jsou diskutovány cíle a předmět auditu, způsoby komunikace, poskytování informací a podrobnější seznámení se všemi okolnostmi a náležitostmi auditu. V úvodní fázi mohou být vyžádány relevantní dokumenty pro jejich

prozkoumání. Dokumentace systému je *nedílnou součástí vybudování kompletního systému řízení bezpečnosti informačního systému a informačních a komunikačních technologií (IS/ICT) v organizaci je vytvoření dokumentace celého systému* (Doucek, 2005, s. 81*)*. Zkoumáním dokumentů lze získat nezbytný přehled o rozsahu dokumentace, seznámit se s výsledky předchozích auditů a shromáždit potřebné informace pro přípravu dalších kroků auditu.



Obrázek 23: Typické činnosti při auditu. Zdroj: (ISO 19011, 2011)

V rámci přípravy plánu auditu by měly být pokryty tyto oblasti (ISO 19011, 2011):

- cíle auditu,
- předmět auditu, včetně identifikace auditovaných organizačních a funkčních jednotek i procesů,
- kritéria auditu a jakékoliv referenční dokumenty,
- místa, termíny, časy a očekávané trvání činností při auditu, včetně jednání s vedením auditované organizace,
- použité metody auditu, včetně rozsahu vzorkování, které je nezbytné pro získávání dostatečných důkazů z auditu, a návrhu plánu vzorkování,
- role a odpovědnosti členů týmu auditorů a také průvodců[11] a pozorovatelů[12],
- přidělení vhodných zdrojů kritickým oblastem auditu,
- přípravy pracovních dokumentů (checklisty, plány vzorkování, formuláře pro záznamy informací a zjištění z auditu, které mohou být použity jako důkazy z auditu).

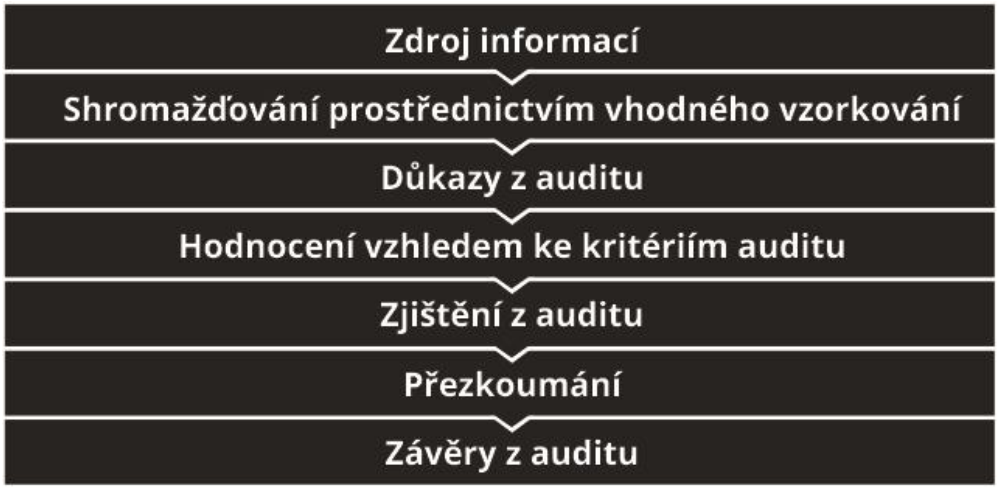
Samotné provádění auditu zahrnuje tyto činnosti (ISO 19011, 2011):

- představení účastníků, včetně průvodců, a naznačení jejich rolí,
- potvrzení cílů, předmětu a kritérií auditu,

[11] Průvodce je osoba, která pomáhá týmu auditorů a je jmenována auditovanou organizací Zdroj: (ISO 19011, 2011)

[12] Pozorovatel je osoba, která doprovází tým auditorů, ale neprovádí audit (tamtéž)

- potvrzení plánu auditu a všech dalších ujednání řešených s auditovanou organizací, jako je například datum a čas konání závěrečného jednání, jakýchkoli dalších porad týmu auditorů a managementu auditované organizace a všechny pozdější změny,
- představení metod, které budou využity k provádění auditu včetně upozornění, že důkazy z auditu budou založeny na vzorku dostupných informací,
- představení metod řízení rizik organizace, která mohou vzniknout následkem přítomnosti členů týmu auditorů,
- potvrzení formálních komunikačních kanálů mezi týmem auditorů a auditovanou organizací,
- potvrzení jazyka, který bude v průběhu auditu používán,
- potvrzení, že auditovaná organizace bude o průběhu auditu průběžně informována,
- potvrzení dostupnosti zdrojů a zařízení nezbytných pro tým auditorů,
- potvrzení záležitostí týkajících se důvěrnosti a bezpečnosti informací,
- potvrzení příslušných zdravotních, nouzových a bezpečnostních postupů platných pro tým auditorů,
- informace o metodách podávání zpráv, zjištěních z auditu, včetně jakéhokoli existujícího třídění,
- informace o podmínkách, za kterých smí být audit ukončen,
- informace o závěrečném jednání; informace o tom, jak v průběhu auditu nakládat s možnými zjištěními,
- informace o jakýchkoliv systémech pro zpětnou vazbu od auditované organizace ohledně zjištění nebo závěrů z auditu, včetně stížností nebo odvolání se.



Obrázek 24: Přehled procesu shromažďování a ověřování informací. Zdroj: (ISO 19011, 2011)

Během fáze shromažďování a ověřování informací se vhodnou vzorkovací metodou (která je v souladu s cíli, rozsahem a kritérii auditu) získávají potřebné a reprezentativní informace, a ty jsou hodnoceny vůči kritériím. Důkazy, které mají být akceptovány mohou být pouze ověřené informace. Ověřené důkazy pak slouží jako zjištění z auditu. Zároveň jsou zaznamenávány neshody včetně důkazů, které neshodu prokazují. Neshody by měly být ve spolupráci s auditovanou organizací přezkoumány a jednání a závěry obou stran mají být dokumentovány. Proces shromažďování a ověřování je zobrazen na Obrázku č. 24.

5.5.3 Závěr z auditu a auditorská zpráva

Během fáze přípravy záběrů z auditu tým auditorů na poradě jedná s cílem, aby prozkoumal všechny informace a zjištění, a porovnal je vůči kritériím a cílům auditu. Výstupem z auditu je zpráva, která má být odsouhlasena, a podle dohody může auditované organizaci poskytovat doporučení ke zlepšení. Závěry z auditu mohou zahrnovat (ISO 19011, 2011):

- rozsah shody systému managementu s kritérii auditu, včetně efektivnosti systému managementu při plnění stanovených cílů,
- efektivnost realizace, udržování a zlepšování systému managementu,
- způsobilost procesu přezkoumávání managementu, kterým je zajištěna trvalá vhodnost, přiměřenost, efektivnost a zlepšování systému managementu,
- dosažení cílů auditu, pokrytí předmětu auditu a splnění kritérií auditu,
- kořenové příčiny zjištění, je-li to zahrnuto v plánu auditu,
- obdobná zjištění z jiných oblastí, auditovaných pro účely identifikace trendů.

Na závěrečném jednání se setkávají vedoucí týmu auditorů se členy vedení auditované organizace a je jim odprezentováno, k jakým závěrům audit dospěl, včetně situací, které mohou snižovat důvěryhodnost závěrů z auditu. Průběh auditu a jeho výsledky jsou zpracovány do zprávy, která má poskytnout ucelený a přesný záznam z auditu, včetně všech náležitostí závěrečné zprávy. Zpráva je doručena adresátům auditu poté, co je odsouhlasena a schválena. Pokud neexistuje nařízení zveřejnit zprávu, nesmí auditující strana nic zveřejňovat. V závěrečné fázi je také dohodnutým způsobem naloženo s dokumenty týkající se auditu tedy jejich uložení nebo zničení. Ukončení auditu nastane ve chvíli, kdy jsou všechny naplánované činnosti dokončeny. Případně je audit ukončen podle dohodnutých podmínek s klientem auditu. Výstupem programu auditů je také sebereflexe týmu auditorů, která má zlepšovat program i odbornost členů týmu. U auditu (examination) je povinný výrok. Možné typy výroků jsou uveden v Tabulce č. 8.

Tabulka 8: Výrok auditora. Zdroj: (Poslání a smysl auditu, 2018; Svatá, 2016)

Závěrečný výrok auditora	
Finanční audit	Audit IT/ICT
Bez výhrad – auditor konstatuje, že účetní závěrka poskytuje podle jeho názoru ve všech významných (materiálních) ohledech věrný a poctivý obraz předmětu účetnictví v souladu s právními předpisy a příslušným rámcem účetního výkaznictví.	**Nekvalifikovaný výrok (bez výhrad)** – důkazy z auditu potvrzují ve všech aspektech očekávání a soulad s kritérii.
S výhradou – auditor konstatuje, že účetní závěrka podává podle jeho názoru věrný a poctivý obraz předmětu účetnictví v souladu s právními předpisy a příslušným rámce účetního výkaznictví s výjimkou skutečností, které popíše.	**Kvalifikovaný výrok (s výhradou)** – důkazy u auditu odráží, co se očekává s určitými nedostatky, které ale celkově významně neovlivňují příznivý výsledek (součástí zprávy musí být vysvětlení)
Záporný výrok – auditor konstatuje, že podle jeho názoru účetní závěrka nepodává věrný a poctivý obraz předmětu účetnictví v souladu s právními předpisy a příslušným rámcem účetního výkaznictví.	**Záporný výrok** – důkazy auditu nepotvrzují očekávání a soulad s kritérii (nejsou zavedeny adekvátní kontroly, nebo neexistuje velká pravděpodobnost, že cíle kontrol nejsou splněny)
Odmítnutí výroku – auditor konstatuje, že byl ve své činnosti omezen do takové míry, že nebyl schopen vydat svůj výrok.	**Zřeknutí se výroku (disclaimer)** – stanovisko nemůže být poskytnuto z důvodu nedostatečných důkazů (možný vliv nedekovaných slabin může být zásadní).

Závěrečná zpráva a její obsah závisí na druhu ujištění[13] a podle splnění očekávání auditované organizace. (Svatá, 2016) uvádí následující strukturu závěrečné zprávy (hvězdičkou uvedené části jsou ve zprávě povinné):

- Titulní strana* – pojmenování dokumentu pro určení jeho jasného obsahu.
- Identifikace auditorské firmy – V tomto dokumentu (identifikace je obvykle na hlavičkovém papíru s informacemi o auditorské organizaci) jsou uvedeny základní informace, jako je druh ujištění, doba dokončení, datum vyhotovení závěrečné zprávy a závěry, nebo výrok auditu. Na dokumentu je povinný podpis vedoucího auditorské organizace. Dokument slouží jako předávací stránka.
- Obsah – seznam kapitol zprávy.
- Úvod – stručné uvedení obsahu.
- Shrnutí – stručné manažerské shrnutí.
- Rozsah* – kapitola, která uvádí základní charakteristiky auditu, jako je objekt auditu, období, kdy audit probíhal, omezení, související standardy a kritéria.
- Cíle* – popis upřesňujících aspektů (na obecné úrovni) o objektu, který byl předmětem hodnocení.
- Metodika auditu* - podrobnější popis průběhu auditu, činností a kritérií, které jsou použity pro formulování závěrů.

[13] Ujištění je v tomto kontextu druhem ujištění. Audit je prověření vhledem k existujícím standardům, zatímco ujištění se vztahuje k cílům řízení. (Svatá, 2016, s.18)

- Výrok/závěr auditu* – výrok je povinný u auditu (examination) a jeho možné podoby shrnuje Tabulka č. 8. Ostatní typy ujištění neuvádějí ve zprávě výrok, ale jsou zde zformulovány závěry.
- Výsledky auditu – podrobnější výklad nálezů auditu. Tato část závisí na tom, zda je uvedena následnost (je odkazována) v předcházející části zprávy (Výrok/závěr auditu). V případě kvalifikovaného nebo záporného výroku je možní tuto část použít jako podklad pro nápravná opatření.
- Doporučení – zde se uvádí doplnění doporučení pro nápravná opatření.
- Reakce managementu – tato část závěrečné zprávy obsahuje vyjádření managementu na základě konceptu závěrečné zprávy. Reakce je pak součástí finální závěrečné zprávy.
- Odpověď auditora – zařazení této kapitoly závisí na existenci předchozí části zprávy (Reakce managementu) a navazuje na ní jakožto odpověď auditora na vyjádření managementu.

5.6 Audit podle vyhlášky o kybernetické bezpečnosti

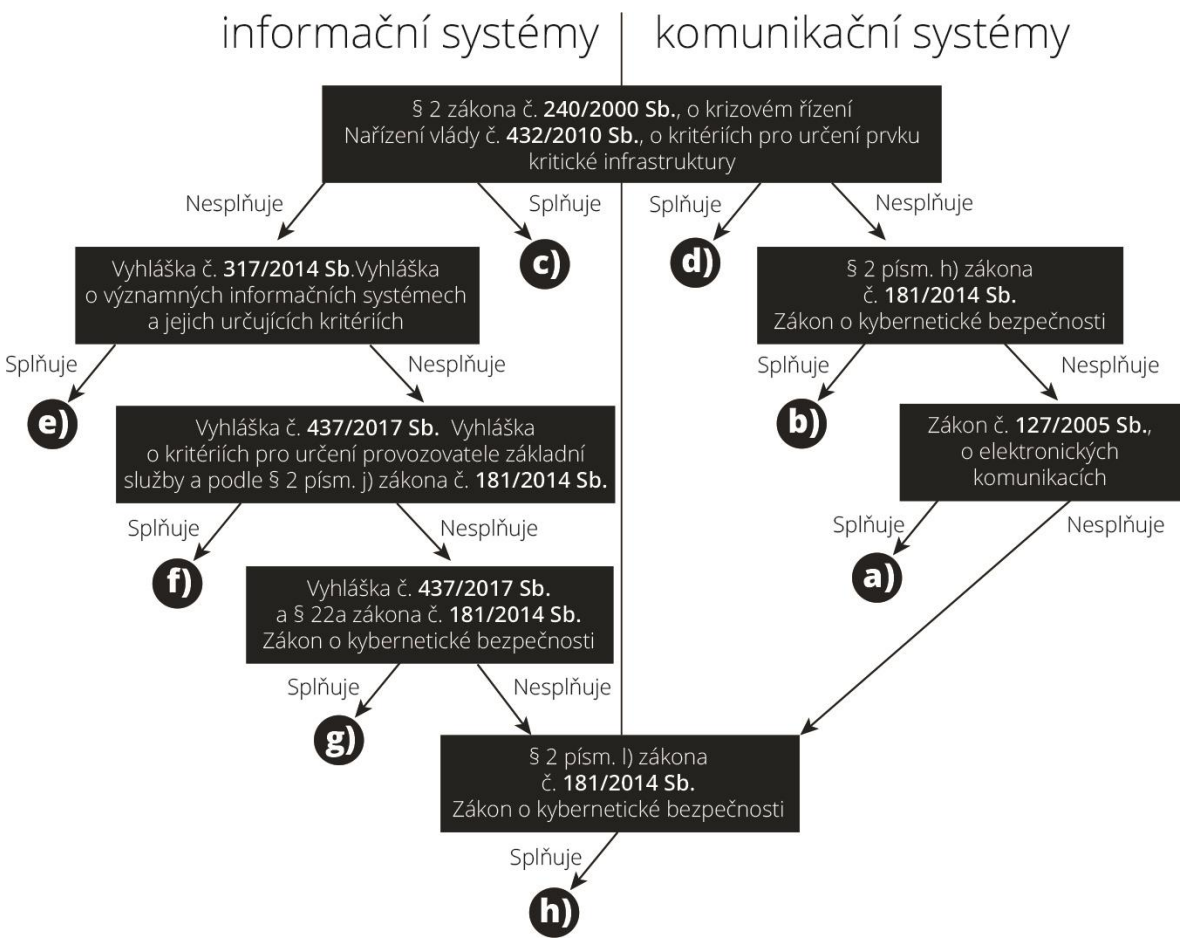
Vyhláška o kybernetické bezpečnosti nařizuje povinným subjektům, aby součástí organizačního opatření byl audit kybernetické bezpečnosti[14]. Zjištění, která jsou získána auditem poskytují podklady pro zlepšování bezpečnosti a aktualizují ISMS. V rámci vyhlášky je povinností povinného subjektu také personální obsazení důležitých rolí podle typu subjektu. Role auditora musí splňovat požadavky na odbornou způsobilost. Auditor nese odpovědnost za provádění auditu, přičemž k tomu musí být zajištěna jeho nestrannost na výkonu dalších rolí týkajících se bezpečnosti v organizaci. Audit je podle vyhlášky prováděn v pravidelných intervalech nebo v případech, kdy nastanou významné změny[15]. Průběh auditu musí být dokumentován a vyhláška specifikuje, jaké náležitosti musí zpráva z auditu kybernetické bezpečnosti obsahovat (viz Tabulka č. 4 - část zpráva z auditu kybernetické bezpečnosti). Výsledná zpráva se stává součástí bezpečnostní dokumentace. Pokud je osoba provozovatelem systému a provádí audit, pak je povinen seznámit s výsledkem auditu správce systému. Závěry auditu jsou zpětnou vazbou řízení bezpečnosti informací v organizaci a stávají se podklady pro identifikaci možných zlepšování ISMS.

[14] Podle § 3 odst. 1 písm. g návrhu novely je povinností zajistit provádění auditu dle § 15. Toto je chyba v draftu novely vyhlášky (tento dokument je uveden jako Příloha č. 1). Audit je v tomto dokumentu prováděn § 16. Tato chyba by měla být v rámci mezirezortního připomínkovacího řízení opravena.
[15] Významnou změnou je změna, která má nebo může mít vliv na bezpečnost informací a představuje vysoké riziko.

6 Analýza regulací

Analýzy, které jsou obsahem této kapitoly, podrobněji rozebírají vyhlášku o kybernetické bezpečnosti[16]. Zaměření této práce je především na audit kybernetické bezpečnosti a souvisí se zákonem o kybernetické bezpečnosti, a tedy především s jeho vyhláškou o kybernetické bezpečnosti, která má silnou vazbu na normu ISO 27001, ale i na normy s ní související.

Již bylo zmíněno (v kapitole 3.4.5 Osoby), lze na kybernetickou bezpečnost nahlížet z pohledu osoby. Určení osoby je pro audit kybernetické bezpečnosti významné v tom, že určuje rozsah auditu, ačkoliv, jak již bylo zmíněno (v kapitole 3.4.6 Opatření v zákonu a vyhlášce), je rozdílů mezi rozsahem pro KII a VIS (jakožto hlavními, nikoliv jedinými povinnými subjekty, na které vztahuje povinnost řídit se vyhláškou) méně než u vyhlášky č. 316/2014 Sb. Následující obrázek zjednodušeně zachycuje proces určení osoby nebo orgánu a povinností, které osobě nebo orgánu jsou zákonem uloženy. Proces určení osob nebo orgánů VIS a KII je také na Obrázcích č. 6 a 7.

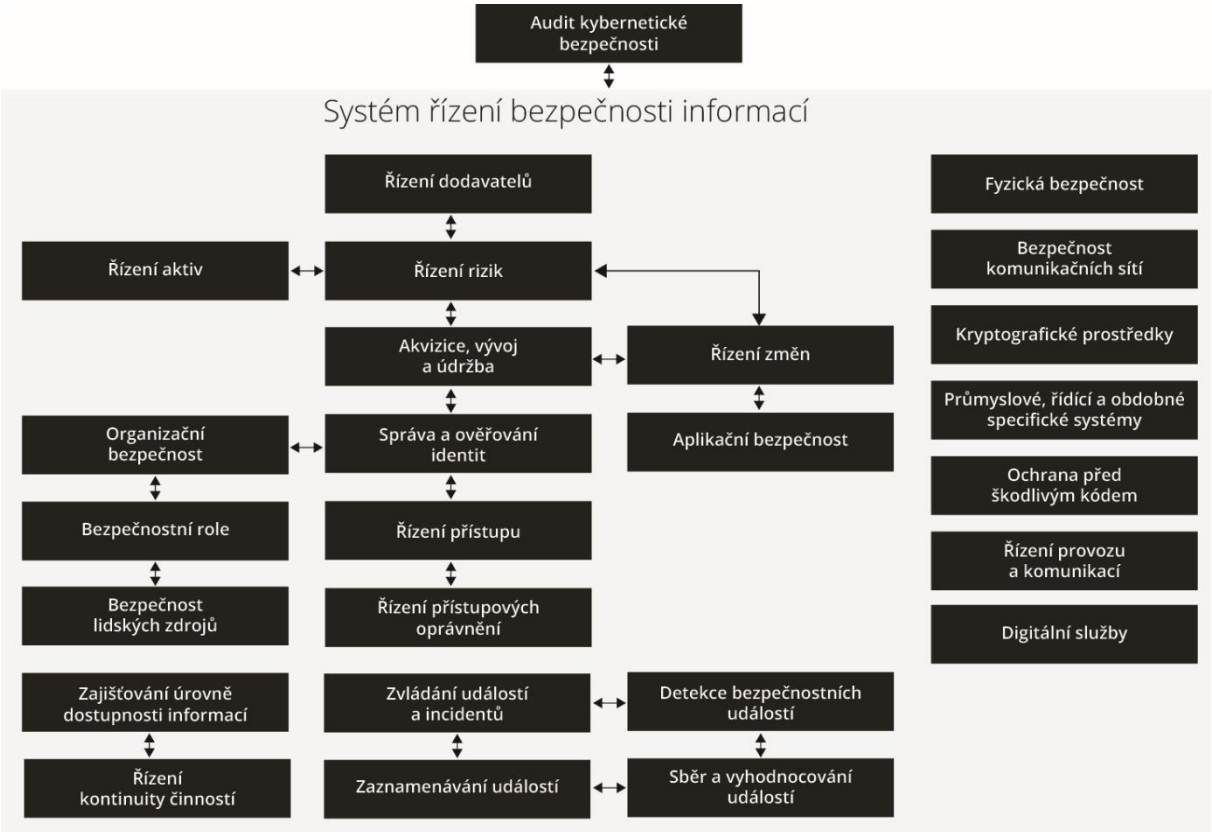


Obrázek 25: Zjednodušený proces určení povinného subjektu podle ZoKB. Zdroj: Autor

[16] Tato diplomová práce vznikala v době, kdy byla platná vyhláška o kybernetické bezpečnosti č. 316/2014, ale byla připravovaná její novela. Analýza se bude věnovat poslední dostupné verzi novely (k 24.3. 2018), a tato je součástí přílohy diplomové práce.

Na Obrázku č. 25 je aplikován pohled na osoby nebo orgány podle kritéria, zda se jedná o informační nebo komunikační systémy. Především z důvodu úplnosti stanovení všech povinných subjektů, je na obrázku uvedena i osoba nebo orgán, která je poskytovatelem digitální služby. Na poskytovatele digitální služby se v oblasti bezpečnostních opatření stanovených vyhláškou vztahuje opatření uvedené v § 29 novely vyhlášky Digitální služby (Příloha č. 1). Toto opatření má dopad pouze na poskytovatele digitální služby.

Oblast kybernetické bezpečnosti reguluje ZoKB, který (nejen) prostřednictvím VoKB do praxe zavádí sadu opatření, která mají zvýšit úroveň bezpečnosti. Zákonem jsou uloženy povinnosti pro osoby nebo orgány, které jsou shrnuty v Tabulce č. 2. V rámci těchto povinností je podle § 4 ZoKB zajištění bezpečnostních opatření. Osoby nebo orgány KII a VIS zavádí a provádí bezpečnostní opatření v rozsahu nezbytném a poskytovatel digitální služby v rozsahu přiměřeném okolnostem pro zajištění kybernetické bezpečnosti. Bezpečnostní opatření jsou významnou oblastí VoKB a jsou základními kritérii pro audit kybernetické bezpečnosti. Jejich provázanost shrnuje Obrázek č. 26. Vazby na obrázku zobrazují přesah opatření na související opatření. Zároveň jsou na obrázku shrnuta všechna organizační a technické opatření, která jsou uvedena ve vyhlášce (Příloha č. 1).



Obrázek 26: Vazby mezi opatřeními. Zdroj: Autor

Z pohledu systému řízení bezpečnosti informací tvoří bezpečnostní politiky, bezpečnostní opatření a bezpečnostní dokumentace pilíře bezpečnosti v kybernetickém prostoru. Nástrojem zpětné vazby je audit tohoto systému. V následující tabulce jsou shrnuty základní kritéria pro audit souladu[17] se zákonem o kybernetické bezpečnosti. V této tabulce jsou také označeny povinnosti pro konkrétní orgán nebo osobu označením, které uvádí § 3 ZoKB.

Tabulka 9: Základní kritéria auditu kybernetické bezpečnosti a jejich platnost pro orgán nebo osobu. Zdroj: Příloha č. 1

Opatření	Osoba							
§ 3 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Deklarace vůdčí role k podpoře kybernetické bezpečnosti			✓	✓	✓	✓		
Deklarace závazku vrcholového vedení k podpoře kybernetické bezpečnosti			✓	✓	✓	✓		
Stanovení rozsahu a hranice systému řízení bezpečnosti informací			✓	✓	✓	✓		
Určení, kterých organizačních částí a aktiv se systém řízení bezpečnosti informací týká			✓	✓	✓	✓		
Stanovení cíle systému řízení bezpečnosti informací			✓	✓	✓	✓		
Zavedení přiměřených bezpečnostních opatření			✓	✓	✓	✓		
Řízení rizik podle § 5 VoKB			✓	✓	✓	✓		
Existuje schválená bezpečnostní politika systému řízení bezpečnosti informací			✓	✓	✓	✓		
Bezpečnostní politika systému řízení bezpečnosti informací obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací			✓	✓	✓	✓		
Bezpečnostní politika systému řízení bezpečnosti informací na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku v dalších oblastech podle § 28 a zavedou příslušná bezpečnostní opatření			✓	✓	✓	✓		
Zajištění provedení auditu kybernetické bezpečnosti u informačního a komunikačního systému			✓	✓	✓	✓		
Zajištění pravidelného vyhodnocení účinnosti systému řízení bezpečnosti informací			✓	✓	✓	✓		
Významné změny se průběžně identifikují a následně podle § 11 řídí			✓	✓	✓	✓		
Systém řízení bezpečnosti informací je aktualizován			✓	✓	✓	✓		
Dokumentace systému řízení bezpečnosti informací je aktualizována			✓	✓	✓	✓		
Systém řízení bezpečnosti informací řídí provoz a zdroje systému řízení bezpečnosti informací			✓	✓	✓	✓		
§ 4 ŘÍZENÍ AKTIV	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Metodika pro identifikaci aktiv			✓	✓	✓	✓		
Metodika pro hodnocení aktiv			✓	✓	✓	✓		
Identifikace a evidence aktiv			✓	✓	✓	✓		
Určení a evidence garantů aktiv			✓	✓	✓	✓		
Hodnocení a evidence primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti			✓	✓	✓	✓		
Určení a evidence vazeb mezi primárními a podpůrnými aktivy			✓	✓	✓	✓		
Hodnocení důsledku závislostí mezi primárními a podpůrnými aktivy			✓	✓	✓	✓		
Hodnocení podpůrných aktiv			✓	✓	✓	✓		
Zavedení pravidel ochrany aktiv			✓	✓	✓	✓		
Stanovení přípustných způsobů používání aktiv			✓	✓	✓	✓		
Určení způsobu likvidace aktiva			✓	✓	✓	✓		
§ 5 ŘÍZENÍ RIZIK	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Stanovení metodiky hodnocení rizik			✓	✓	✓	✓		
Stanovení kritérií pro akceptovatelnost rizik			✓	✓	✓	✓		
Zpracování zprávy o hodnocení rizik			✓	✓	✓	✓		
Zpracování a zavedení plánu zvládání rizik			✓	✓	✓	✓		
Zavedení bezpečnostních opatření			✓	✓	✓	✓		
Hodnocení rizik alespoň jednou za tři roky					✓			
Hodnocení rizik alespoň jednou ročně			✓	✓		✓		
Seznámení vrcholového vedení s výstupy z procesu řízení rizik			✓	✓	✓	✓		

[17] Audit souladu/shody je komplexní kontrola dodržování platných právních předpisů organizací; soulad (compliance) jedna regulace nebo shoda (conformace) více regulací současně. (Svatá, 2016)

§ 6 ORGANIZAČNÍ BEZPEČNOST	a	b	c	d	e	f	g	h
Stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací			✔	✔	✔	✔		
Integrace systému řízení bezpečnosti informací do procesů organizace			✔	✔	✔	✔		
Prosazování neustálého zlepšování systému řízení bezpečnosti informací			✔	✔	✔	✔		
Smlouvy s fyzickými osobami zastávajícími bezpečnostní role a role administrátorů obsahují ustanovení o bezpečnosti informací			✔	✔	✔	✔		
Účast vrcholového vedení na testování plánů kontinuity činností			✔	✔	✔	✔		
Stanovení pravomocí bezpečnostních rolí, jejich práv a povinností			✔	✔	✔	✔		
Určení bezpečnostní role manažera kybernetické bezpečnosti			✔	✔	✔	✔		
Určení bezpečnostní role architekta kybernetické bezpečnosti			✔	✔		✔		
Určení bezpečnostní role garanta aktiva			✔	✔		✔		
Určení bezpečnostní role auditora kybernetické bezpečnosti			✔	✔		✔		
Určení zastupitelnosti rolí manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti			✔	✔		✔		
Určení zastupitelnosti role manažera kybernetické bezpečnost **					✔			
Určení rolí bezpečnosti informací (vyjma manažera KB)					✔			
§ 7 BEZPEČNOSTNÍ ROLE	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Manažer kybernetické bezpečnosti pravidelně informuje vrcholové vedení			✔	✔	✔	✔		
Manažer kybernetické bezpečnosti nevykonává role odpovědné za provoz informačních a komunikačních systémů			✔	✔	✔	✔		
Architekt kybernetické bezpečnosti nevykonává role odpovědné za provoz informačních a komunikačních systémů			✔	✔	✔	✔		
Výkon role auditora kybernetické bezpečnosti je oddělena od výkonu dalších bezpečnostních rolí			✔	✔	✔	✔		
Plnění kvalifikačních předpokladů osob zastávajících bezpečnostní role			✔	✔	✔	✔		
§ 8 ŘÍZENÍ DODAVATELŮ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Stanovení pravidel pro dodavatele			✔	✔	✔	✔		
Evidence své významných dodavatelů a informování dodavatelů o evidenci			✔	✔	✔	✔		
Seznámení dodavatelů s pravidly			✔	✔	✔	✔		
Kontrola dodržování pravidel bezpečnosti dodavateli			✔	✔	✔	✔		
Řízení rizik souvisejících s dodavateli			✔	✔	✔	✔		
Smlouvy uzavírané s významnými dodavateli obsahují relevantní oblasti související s řízením rizik			✔	✔	✔	✔		
Pravidelné přezkoumávání plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací			✔	✔	✔	✔		
Hodnocení rizik souvisejících s plněním předmětu výběrového řízení			✔	✔	✔	✔		
Stanovení způsobu a úrovně realizace bezpečnostních opatření a určení obsahu vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření			✔	✔	✔	✔		
Pravidelné hodnocení rizik a pravidelná kontrola zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany			✔	✔	✔	✔		
Zajištění řešení zjištěných nedostatků			✔	✔	✔	✔		
§ 9 BEZPEČNOST LIDSKÝCH ZDROJŮ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Stanovení plánu rozvoje bezpečnostního povědomí			✔	✔	✔	✔		
Určení osob odpovědných za realizaci jednotlivých činností, které jsou v plánu uvedeny			✔	✔	✔	✔		
Zajištění pravidelných odborných školení pro osoby zastávající bezpečnostní role			✔	✔	✔	✔		
Zajištění rozvoje bezpečnostního povědomí			✔	✔	✔	✔		
Kontrola dodržování bezpečnostních politik			✔	✔	✔	✔		
Předání odpovědnosti v případě ukončení smluvního vztahu			✔	✔	✔	✔		
Hodnocení účinnost plánu rozvoje bezpečnostního povědomí			✔	✔	✔	✔		
Pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel			✔	✔	✔	✔		
§ 10 ŘÍZENÍ PROVOZU A KOMUNIKACÍ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Zajištění bezpečného provozu informačního a komunikačního systému stanovením práv a povinností administrátorů, uživatelů a osob zastávajících bezpečnostní role			✔	✔	✔	✔		
Stanovení postupů pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů			✔	✔	✔	✔		
Stanovení postupů pro sledování kybernetických bezpečnostních událostí a opatření pro ochranu přístupu k záznamům o těchto událostech			✔	✔	✔	✔		
Stanovení postupů a pravidel pro ochranu před škodlivým kódem			✔	✔	✔	✔		
Řízení technických zranitelností			✔	✔	✔	✔		

Evidence a sdílení spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory			✔	✔	✔	✔		
Stanovení postupů pro řízení a schvalování provozních změn			✔	✔	✔	✔		
Stanovení postupů pro sledování, plánování a řízení kapacity lidských a technických zdrojů			✔	✔	✔	✔		
Stanovení postupů a pravidel pro ochranu informací a dat v průběhu celého životního cyklu			✔	✔	✔	✔		
Stanovení postupů a pravidel pro instalaci technických aktiv			✔	✔	✔	✔		
Provádění pravidelného zálohování a kontroly použitelnosti provedených záloh			✔	✔	✔	✔		
Stanovení postupů a pravidel pro zajištění bezpečnosti síťových služeb			✔	✔	✔	✔		
Pravidla a postupy jsou v rámci řízení provozu a komunikací aktualizována v souvislosti s prováděnými nebo plánovanými změnami			✔	✔	✔	✔		
Dodržování pravidel a postupů rámci řízení provozu a komunikací			✔	✔	✔	✔		
Zajištění oddělení vývojového, testovacího a provozního prostředí			✔	✔	✔	✔		
§ 11 ŘÍZENÍ ZMĚN	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Přezkoumávání dopadu změn			✔	✔	✔	✔		
Určování významných změn			✔	✔	✔	✔		
Dokumentace významných změn a jejich řízení			✔	✔	✔	✔		
Analýza rizik významných změn			✔	✔	✔	✔		
Přijímání opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami			✔	✔	✔	✔		
Aktualizace bezpečnostní politiky a bezpečnostní dokumentaci na základě významných změn			✔	✔	✔	✔		
Zajištění testování významných změn			✔	✔	✔	✔		
Zajištění možnosti navrácení změn do původního stavu			✔	✔	✔	✔		
Posouzení potřeby o provedení penetračního testování nebo testování zranitelností			✔	✔		✔		
Posouzení potřeby o provedení penetračního testování nebo testování zranitelností **					✔			
§ 12 ŘÍZENÍ PŘÍSTUPU	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Zajištění ochrany údajů, které jsou používány pro přihlášení			✔	✔	✔	✔		
Zajištění ochrany údajů proti zneužití neoprávněnou osobou			✔	✔	✔	✔		
Řízení přístupu k informačnímu a komunikačnímu systému na základě skupin a rolí			✔	✔	✔	✔		
Přidělování každému uživateli a administrátorovi přistupujícímu k informačnímu a komunikačnímu systému přístupová práva a oprávnění a jedinečný identifikátor			✔	✔	✔	✔		
Řízení přístupu k informačnímu a komunikačnímu systému řídí identifikátory, přístupová práva a oprávnění aplikací a technických účtů			✔	✔	✔	✔		
Zavedení bezpečnostních opatření pro řízení přístupu zařízení k prostředkům informačního a komunikačního systému			✔	✔	✔	✔		
Zavedení bezpečnostních opatření potřebných pro bezpečné používání mobilních zařízení			✔	✔	✔	✔		
Přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce			✔	✔	✔	✔		
Omezení a kontrola programových nástrojů, které mohou překonat systémové nebo aplikační kontroly			✔	✔	✔	✔		
Správa přístupových oprávnění v souladu s politikou řízení přístupu			✔	✔	✔	✔		
Pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí			✔	✔	✔	✔		
Využívání nástroje pro správu a ověřování identity			✔	✔	✔	✔		
Dodržování postupů pro používání privátních autentizačních informací			✔	✔	✔	✔		
Zajištění odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role			✔	✔	✔	✔		
Zajištění odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu			✔	✔	✔	✔		
Dokumentace přidělování a odebírání přístupových oprávnění			✔	✔	✔	✔		
§ 13 AKVIZICE, VÝVOJ A ÚDRŽBA	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Řízení rizik pro plánovanou akvizici, vývoj a údržbou informačního a komunikačního systému			✔	✔	✔	✔		
Řízení významných změn pro plánované akvizice, vývoj a údržbou informačního a komunikačního systému			✔	✔	✔	✔		
Stanovení bezpečnostních požadavků pro plánované akvizice, vývoj a údržbou informačního a komunikačního systému			✔	✔	✔	✔		

Zahrnutí bezpečnostních požadavků do projektu akvizice, vývoje a údržby			✔	✔	✔	✔		
Zajištění bezpečnosti vývojového a testovacího prostředí a zajištění ochrany používaných testovacích dat			✔	✔	✔	✔		
Provádění bezpečnostních testování významných změn před jejich zavedením do provozu			✔	✔	✔	✔		
Plnění požadavků pro ověření identity uživatelů u objektů akvizice nebo vývoje nástroj pro správu a ověřování identity			✔	✔	✔	✔		
§ 14 ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Přidělení odpovědnosti pro průběžnou detekci a vyhodnocování a pro koordinaci a zvládání kybernetických bezpečnostních incidentů			✔	✔	✔	✔		
Stanovení postupů pro průběžnou detekci a vyhodnocování a pro koordinaci a zvládání kybernetických bezpečnostních incidentů			✔	✔	✔	✔		
Definice a aplikace postupů pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu			✔	✔	✔	✔		
Oznamování neobvyklého chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti bezpečnosti informací			✔	✔	✔	✔		
Zajištění posuzování kybernetických bezpečnostních událostí			✔	✔	✔	✔		
Zavedení procesu detekce, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí			✔	✔	✔	✔		
Zavedení procesu zvládání kybernetických bezpečnostních incidentů a zvládání kybernetických bezpečnostních incidentů podle stanovených postupů			✔	✔	✔	✔		
Přijetí opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu			✔	✔	✔	✔		
Hlášení kybernetických bezpečnostních incidentů			✔	✔	✔	✔		
Hlášení kybernetických bezpečnostních incidentů *		✔						
Evidence záznamů o kybernetických bezpečnostních incidentech a o jejich zvládání			✔	✔	✔	✔		
Prošetření a určení příčiny kybernetického bezpečnostního incidentu			✔	✔	✔	✔		
Vyhodnocení účinnosti řešení kybernetického bezpečnostního incidentu			✔	✔	✔	✔		
§ 15 ŘÍZENÍ KONTINUITY ČINNOSTÍ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Stanovení práv a povinnosti administrátorů a osob zastávajících bezpečnostní role			✔	✔	✔	✔		
Vyhodnocení a dokumentace možných dopadů kybernetických bezpečnostních incidentů			✔	✔	✔	✔		
Posouzení možných rizik souvisejících s ohrožením kontinuity činností			✔	✔	✔	✔		
Stanovení cílů řízení kontinuity činností			✔	✔	✔	✔		
Stanovení politiky řízení kontinuity činností			✔	✔	✔	✔		
Vypracování a aktualizace plánu kontinuity činností související s provozováním informačního a komunikačního systému a souvisejících služeb			✔	✔	✔	✔		
Pravidelné testování plánu kontinuity činností související s provozováním informačního a komunikačního systému a souvisejících služeb			✔	✔	✔	✔		
Realizace opatření pro zvýšení odolnosti informačního a komunikačního systému			✔	✔	✔	✔		
§ 16 AUDIT KYBERNETICKÉ BEZPEČNOSTI	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Provádění a dokumentování auditu dodržování bezpečnostní politiky, včetně přezkoumání technické shody, a výsledky auditu zohlední v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik			✔	✔	✔	✔		
Posouzení souladu bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému			✔	✔	✔	✔		
Určení nápravných opatření pro zajištění souladu			✔	✔	✔	✔		
Provádění auditu					✔			
Provádění auditu			✔	✔		✔		
Výsledky auditu kybernetické bezpečnosti jsou předloženy správci daného informačního a komunikačního systému			✔	✔	✔	✔		
§ 17 FYZICKÁ BEZPEČNOST	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Zavedení opatření pro předcházení poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního a komunikačního systému			✔	✔	✔	✔		
Stanovení fyzického bezpečnostního perimetru ohraničující oblast uchovávání a zpracovávání informací a umístění technických aktiv informačního a komunikačního systému			✔	✔	✔	✔		
§ 18 BEZPEČNOST KOMUNIKAČNÍCH SÍTÍ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Zajištění segmentace komunikační sítě			✔	✔	✔	✔		

Zajištění řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě			✔	✔	✔	✔		
Zajištění bezpečnosti komunikace pomocí kryptografie			✔	✔	✔	✔		
Aktivní blokování nežádoucí komunikace			✔	✔	✔	✔		
Zajištění segmentace komunikační sítě			✔	✔	✔	✔		
§ 19 SPRÁVA A OVĚŘOVÁNÍ IDENTIT	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Používání nástroje správy identity uživatelů			✔	✔	✔	✔		
Autentizace pro ověření identity uživatelů, administrátorů a aplikací využívají autentizační mechanizmus			✔	✔	✔	✔		
§ 20 ŘÍZENÍ PŘÍSTUPOVÝCH OPRÁVNĚNÍ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Používání centralizovaného nástroje pro řízení přístupových oprávnění pro přístup k jednotlivým aktivům informačního a komunikačního systému			✔	✔	✔	✔		
Používání centralizovaného nástroje pro řízení přístupových oprávnění pro čtení dat, zápis dat a změnu oprávnění			✔	✔	✔	✔		
§ 21 OCHRANA PŘED ŠKODLIVÝM KÓDEM	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Zajištění použití nástroje pro nepřetržitou automatickou ochranu			✔	✔		✔		
Monitoring a řízení používání výměnných zařízení a datových nosičů			✔	✔		✔		
Řízení automatického spouštění obsahu výměnných zařízení a datových nosičů			✔	✔		✔		
Řízení oprávnění ke spouštění kódu			✔	✔		✔		
Provádění pravidelné a účinné aktualizace nástroje pro ochranu před škodlivým kódem			✔	✔		✔		
Přiměřené zajištění použití nástroje pro nepřetržitou automatickou ochranu					✔			
Přiměřený monitoring a řízení používání výměnných zařízení a datových nosičů					✔			
Přiměřené řízení automatického spouštění obsahu výměnných zařízení a datových nosičů					✔			
Přiměřené řízení oprávnění ke spouštění kódu					✔			
Přiměřené provádění pravidelné a účinné aktualizace nástroje pro ochranu před škodlivým kódem					✔			
§ 22 ZAZNAMENÁVÁNÍ UDÁLOSTÍ INFORMAČNÍHO A KOMUNIKAČNÍHO SYSTÉMU, JEHO UŽIVATELŮ A ADMINISTRÁTORŮ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Zaznamenávání bezpečnostních a provozních událostí důležitých aktiv informačního a komunikačního systému			✔	✔	✔	✔		
Aktualizace rozsahu aktiv, u kterých je zaznamenávání bezpečnostních a provozních událostí prováděno na základě hodnocení důležitosti aktiv			✔	✔	✔	✔		
Zaznamenávání bezpečnostních a provozních událostí nejméně po dobu 12 měsíců					✔			
Zaznamenávání bezpečnostních a provozních událostí nejméně po dobu 24 měsíců			✔	✔		✔		
§ 23 DETEKCE KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Zajištění ověření a kontroly přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi			✔	✔	✔	✔		
Zajištění ověření a kontroly přenášených dat na perimetru komunikační sítě			✔	✔	✔	✔		
Zajištění blokování nežádoucí komunikace			✔	✔	✔	✔		
Zajištění detekce kybernetických bezpečnostních událostí			✔	✔		✔		
Zajištění detekce kybernetických bezpečnostních událostí *		✔						
§ 24 SBĚR A VYHODNOCOVÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Používání nástroje pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí			✔	✔		✔		
§ 25 APLIKAČNÍ BEZPEČNOST	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Povedení penetračních testů informačního a komunikačního systému se zaměřením na důležitá aktiva před jejich uvedením do provozu			✔	✔	✔	✔		
Povedení penetračních testů informačního a komunikačního systému se zaměřením na důležitá aktiva v souvislosti s významnou			✔	✔	✔	✔		
Zajištění trvalé ochrany aplikací, informací a transakcí před neoprávněnou činností			✔	✔	✔	✔		
Zajištění trvalé ochrany aplikací, informací a transakcí před popřením provedených činností			✔	✔	✔	✔		
§ 26 KRYPTOGRAFICKÉ PROSTŘEDKY	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Používání aktuálně odolných kryptografických algoritmů a kryptografických klíčů			✔	✔	✔	✔		
Používání systému správy klíčů a certifikátů			✔	✔	✔	✔		
Prosazování bezpečného nakládání s kryptografickými prostředky			✔	✔	✔	✔		
Zohlednění doporučení v oblasti kryptografických prostředků vydaná Úřadem			✔	✔	✔	✔		
§ 27 ZAJIŠŤOVÁNÍ ÚROVNĚ DOSTUPNOSTI INFORMACÍ	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Zajištění dostupnost informačního a komunikačního systému			✔	✔	✔	✔		

Zajištění odolnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost			✔	✔	✔	✔		
Zajištění dostupnost důležitých technických aktiv informačního a komunikačního systému			✔	✔	✔	✔		
Zajištění redundance aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému			✔	✔	✔	✔		
§ 28 PRŮMYSLOVÉ, ŘÍDÍCÍ A OBDOBNÉ SPECIFICKÉ SYSTÉMY	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Používání technických a programových prostředků, které jsou určeny do specifického prostředí			✔	✔	✔	✔		
Omezení fyzického přístupu k zařízením průmyslových a řídících systémů a ke komunikační síti			✔	✔	✔	✔		
Vyčlenění komunikační sítě určené pro průmyslové a řídící systémy od ostatní infrastruktury			✔	✔	✔	✔		
Omezení a řízení vzdáleného přístupu k průmyslovým a řídícím systémům			✔	✔	✔	✔		
Ochrana jednotlivých technických aktiv průmyslových a řídících systémů před využitím známých zranitelností			✔	✔	✔	✔		
Obnovení chodu průmyslových a řídících systémů po kybernetickém bezpečnostním incidentu			✔	✔	✔	✔		
§ 29 DIGITÁLNÍ SLUŽBY	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
Zavedení bezpečnostních opatření podle prováděcího nařízení								✔

* Opatření na úrovni zákona
** Specifické opatření pro VIS a KII
Poznámka: sloupce a – h jsou označením osob nebo orgánů podle § 3 ZoKB

Kromě bezpečnostních opatření je součástí systému řízení bezpečnosti informací také stanovení bezpečnostní politiky a vedení bezpečnostní dokumentace. Vyhláška formuluje doporučený obsah jak politik, tak dokumentace. Souhrn je uveden v Tabulce č. 4.

Soulad s požadavky automaticky nezajišťuje plnou bezpečnost. Větší hloubka auditu se věnuje kontrolám procesů zajištujících bezpečnost prostřednictvím konkrétních opatření. Účinnost a efektivnost procesů v rámci auditu ověřují kontroly a testování procesů opatření. Pro ověření účinnosti a efektivnosti je vhodná detailnější znalost kontrolované oblasti (pro každé opatření) a souvisejících procesů. Doporučení a návody jsou uváděny v dokumentech, které se na konkrétní oblasti zaměřují. Následující tabulka uvádí přehled dokumentů, souvisejících s kybernetickou bezpečností. Zdrojem informací jsou především normy ISO 27002 a ISO 27032 a také i VoKB.

Tabulka 10: Související dokumenty. Zdroj: (ISO 27002, 2014; ISO 27032, 2013)

Opatření	Dokumenty
Systém řízení bezpečnosti informací	ISO 27000 ISO 27001 ISO 27002 ISO 27003
Řízení aktiv	ISO 19770 – Software asset management
Řízení rizik	ISO 31000 ISO 27005 ISO 16085 – Life cycle processes – Risk management
Organizační bezpečnost	
Bezpečnostní role	RACI
Řízení dodavatelů	ISO 27036 – Information security for supplier relationships ISO15443-2 – Security assurance framework

Bezpečnost lidských zdrojů	
Řízení provozu a komunikací	ISO 27010 – Information security management for inter–sector and inter–organizational communications ISO 27033 – Network security
Řízení změn	
Řízení přístupu	ISO 29146 – A framework for access management
Akvizice, vývoj a údržba	ISO 27005
Zvládání kybernetických bezpečnostních událostí a incidentů	ISO 27035 – Information security incident management ISO 24762 – Guidelines for information and communications technology disaster recovery services
Řízení kontinuity činností	ISO 22301 – Business continuity management systems ISO 27031 – Guidelines for information and communication technology readiness for business continuity ISO 22316 – Organizational resilience
Audit kybernetické bezpečnosti	ISO 9000 ISO 19011 ISO 27007 ISO 17021–1 ISO 17021–6 – Competence requirements for auditing and certification of business continuity management systems ISO 27006 ISO 15504 – Process assessment ISO 18045 – Methodology for IT security evaluation ISO 19791 – Security assessment of operational systems ISO 27008 – Guidelines for auditors on information security controls
Fyzická bezpečnost	ISO 30104 – Physical Security Attacks, Mitigation Techniques and Security Requirements
Bezpečnost komunikačních sítí	ISO 27033 ISO 18028 – IT network security
Správa a ověřování identit	24760–1 – A framework for identity management
Řízení přístupových oprávnění	ISO 29146 – A framework for access management
Ochrana před škodlivým kódem	
Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	ISO 27037 – Guidelines for identification, collection, acquisition and preservation of digital evidence
Detekce kybernetických bezpečnostních událostí	ISO 27035 ISO 27039 – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)
Sběr a vyhodnocování kybernetických bezpečnostních událostí	ISO 27037
Aplikační bezpečnost	ISO 27034 – Application security
Kryptografické prostředky	ISO 11770 – Key management ISO 18367 – Cryptographic algorithms and security mechanisms conformance testing ISO 20540 – Testing cryptographic modules in their operational environment (Under development) web NÚKIB
Zajišťování úrovně dostupnosti informací	ISO 20000 – Service management
Průmyslové, řídící a obdobné specifické systémy	
Digitální služby	nařízení Komise (EU) 2018/151

7 Návrh auditu kybernetické bezpečnosti

V rámci této kapitoly bude představen návrh auditu kybernetické bezpečnosti se zaměřením na nástroj, který je součástí této práce, a je navržen na podporu průběhu auditu.

Pro návrh auditu lze využít existující postupy, návody a doporučení. Pro účely této kapitoly bude návrh vycházet z dokumentu Information Systems Auditing: Tools and Techniques (2016). V tomto pojetí je audit rozdělen na tři fáze (tyto fáze jsou uvedeny na Obrázcích č. 27, 28 a 29):

1. plánování (Planing),
2. realizaci (Fieldwork and documentation),
3. reportování (Reporting).

Obrázek 27: Fáze plánování. Zdroj: (Information Systems Auditing: Tools and Techniques, 2016)

Pro fázi plánování jsou na Obrázku č. 27 uvedeny podrobnější kroky:

1. Určení předmětu auditu – vymezení oblasti nebo objetu auditu.
2. Definice cíle auditu – cílem může být zajištění souladu se zákonem se vztahem k předmětu auditu a jeho účelu.
3. Nastavení rozsahu auditu – určení systému, funkcí a organizačních jednotek, které se týkají auditu a zahrnují porozumění prostředí.
4. Předběžné plánování – krok určení konkrétního rozsahu, který je ovlivněn podle uvážení konkrétních vlivů a okolností, vztahující se k auditované organizaci, umístění, zařízení a dokumentaci.
5. Postupy auditu – etapa, která již pracuje s dostatkem informací o objektu pro určení postupů a vytvoření programu auditu.

V rámci předběžného plánování je třeba zohlednit:

- potřebné technické dovednosti a zdroje,
- rozpočet a postupy potřebné k dokončení zakázky,
- místa nebo zařízení, která mají být auditována,
- role a odpovědnosti auditorského týmu,

- časový rámec pro jednotlivé fáze auditu,
- zdroje informací pro testování nebo přezkoumání, jako jsou funkční vývojové diagramy, zásady, standardy, postupy a předchozí auditorské práce,
- kontaktní místa pro administrativní a logistické uspořádání,
- komunikační plán, který popisuje koho, kdy, jak často a za jakým účelem kontaktovat.

Fáze plánování auditu by měla zahrnovat aspekty (Information security audit, 2008):

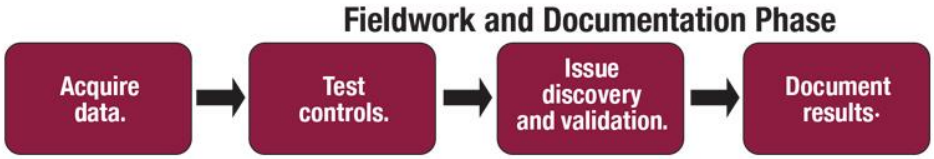
- dosažení strategických cílů auditu IS,
- veškeré možné právní předpisy a nařízení,
- organizace auditu v organizaci,
- zdroje (z hlediska času, financí a personálu),
- zvláštní podmínky a omezení organizace,
- archivaci dokumentace.

Podle dokumentu Information security audit (2008) plánování rozvrhne audit podle relativní potřeby času pro každý krok. Tabulka č. 11 zobrazuje odhad rozložení času potřebného pro audit.

Tabulka 11: Relativní časová náročnost auditu. Zdroj: (Information security audit, 2008)

Fáze	Činnost	Čas v %
Krok 1	Příprava auditu	5 %
Krok 2	Vytvoření plánu auditu	15 %
Krok 3	Revize dokumentů	20 %
Krok 4	Průběh auditu (examination)	35 %
Krok 5	Vyhodnocení	5 %
Krok 6	Příprava zprávy	20 %

Odhad času, který je potřebný pro provedení auditu resp. celkové doby trvání auditu, závisí (mimo jiné) na komplexnosti systému, velikosti organizace i množství a úroveň dokumentace.



Obrázek 28: Fáze provádění a dokumentace. Zdroj:(Information Systems Auditing: Tools and Techniques, 2016)

Další fáze (uvedená na Obrázku č. 28) se zabývá realizací a dokumentací auditu. Postup zahrnuje získávání potřebných dokumentů a jejich prostudování. Na základě zjištěných informací lze prověřit soulad prostřednictvím kontrol a veškerá zjištění jsou validována. Zároveň je celý průběh dokumentován, včetně všech kroků, zjištění a výsledků.

Zdrojem informací jsou podle dokumentu Information Systems Auditing (2016):

- předchozí auditorské zprávy,
- procesní mapy,
- síťové mapy,
- SLA,
- standardy a postupy procesů,
- seznam aktivních uživatelů,
- matice úrovní organizace,
- politiky,
- dokumentace vývoje softwaru,
- výukové manuály,
- seznam dodavatelů,
- seznam zaměstnanců včetně ukončených poměrů a nově přijatých zaměstnanců ve sledovaném období.

Obrázek 29: Fáze reportování. Zdroj:(Information Systems Auditing: Tools and Techniques, 2016)

Fáze reportování se zabývá shromažďováním podkladů a požadavků pro vytvoření závěrečné zprávy. Obsah a struktura závěrečné zprávy z auditu jsou popsány v kapitole 5.5.3 Závěr z auditu a auditorská zpráva.

7.1 Nástroj na podporu auditu

Ve fázi provádění auditu mohou auditoři využít různé podpůrné nástroje a checklisty. Součástí diplomové práce je také návrh nástroje pro podporu auditu. Tento nástroj funguje na principu checklistu a zároveň umožňuje základním způsobem vést dokumentaci průběhu auditu.

Nástroj podporuje průběh auditu v několika fázích. Výchozím bodem pro používání nástroje je nastavení – tedy příprava checklistu. V rámci tohoto nastavení je možné nastavit kritéria hodnocení souladu s vyhláškou o kybernetické bezpečnosti v oblastech bezpečnostní politiky, bezpečnostní dokumentace a bezpečnostních opatření. Nástroj již obsahuje návrh auditu, který zajišťují funkce nástroje „Nastavit na výchozí hodnoty“. Nastavení kritérií opatření je vytvořeno na podle kapitoly 6 Analýza regulací. Uživatel má také možnost pracovat s kritérii – spravovat je.

Nástroj kromě hodnocení souladu umožňuje i rozšíření. Toto rozšíření je zastoupeno doplňkem pro řízení aktiv a rizik, který vychází z novely vyhlášky o kybernetické bezpečnosti (Příloha č. 1). Získané výsledky z doplňku nástroje lze (podle rozhodnutí uživatele) připojit k výstupní zprávě z nástroje pro podporu auditu. Pokud jsou doplňkem vygenerovány výstupy, bude uživatel pouze vyzván, zda je požaduje zařadit jako přílohu ke zprávě. Princip rozšíření je založen na standardním odkazování mezi webovými stránkami. Rozšíření nástroje je samostatná webová stránka (aplikace), která s nástrojem pro podporu auditu sdílí všechna data. Sdílená data mohou být připojena k výstupu nástroje. Vygenerování podkladů hodnocení ze získaných informací připraví podklady pro výstupní zprávu auditu.

Nástroj řízení aktiv a rizik je doplněk, který vychází z novely vyhlášky o kybernetické bezpečnosti (Příloha č. 1). Tento doplněk umožňuje spravovat aktiva a hodnotit je pro potřeby řízení rizik souvisejících s aktivy. Doplněk není navržen jako auditní nástroj, ale jako správce pro řízení aktiv a rizik, který umožňuje vygenerovat výstup pro nástroj pro podporu auditu. Výstup nástroje kontroluje úplnost všech vyhláškou požadovaných záznamů, které je nutné evidovat pro každé aktivum. V části řízení rizik vede doplňkový nástroj správu rizik a všech povinných činností, které vyhláška požaduje.

Oba nástroje jsou vytvořeny jako webová aplikace a je použité skriptování na straně klienta. Nástroje sice vyžadují připojení k internetu, ale lze je upravit tak, aby fungovaly zcela off-line. Během používání nástroje nejsou přenášena žádná data prostřednictvím sítě internetu, ale možnost sdílení dat je nástrojem podporovaná. Vše funguje pouze ve webovém prohlížeči. Nástroj je speciálně navržen pro webový prohlížeč Google Chrome, a to je jediný požadavek pro používání těchto nástrojů. Není nutné kupovat a instalovat žádné další aplikace nebo doplňky.

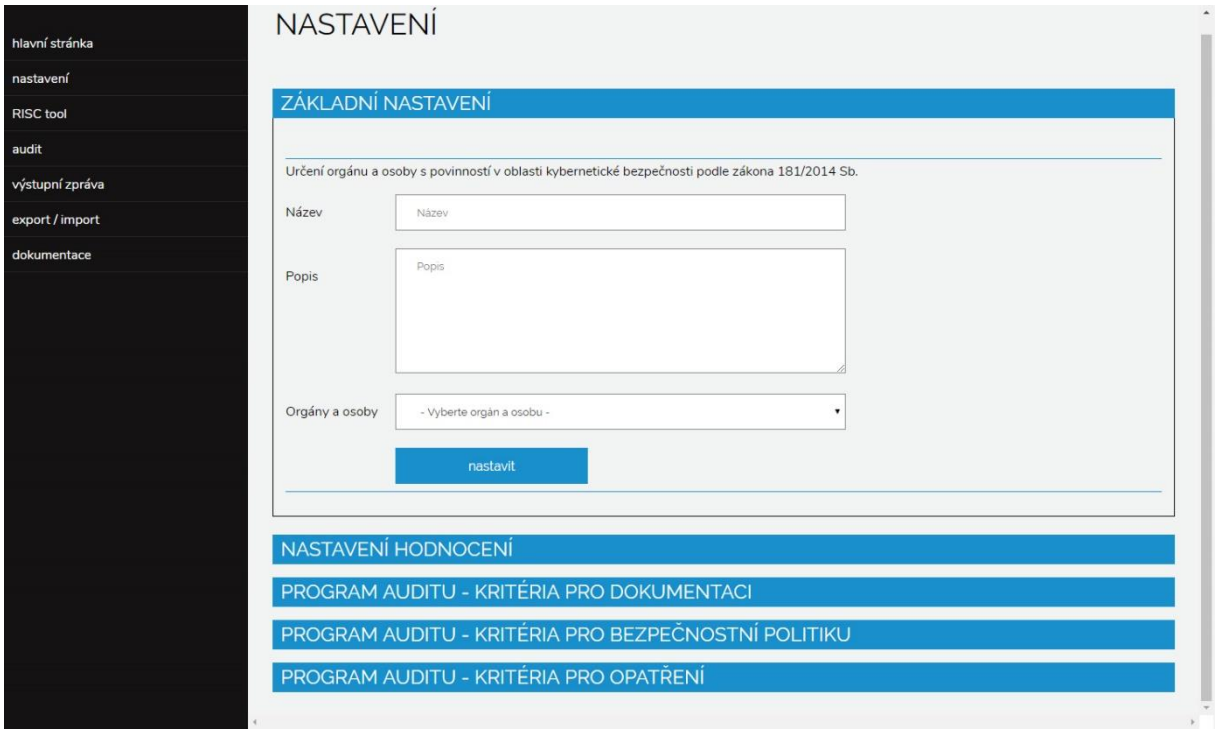
Nástroj je navržen pro použití na jednom zařízení a práce s daty je omezena pouze na použití na konkrétním zařízení, na kterém je nástroj používán. Úložiště dat se vztahuje k webovému prohlížeči, a proto nelze používat nástroj s více uživateli zároveň. Toto omezení částečně odstraňují funkce exportu a importu dat. Úložný prostor představuje také riziko bezpečnosti uložených dat. Informace, které auditor v rámci auditu získá, jsou důvěrné a nástroj data nijak nešifruje, aby nebyla pro člověka čitelná. Nástroj také pro přístup do aplikace nevyžaduje autentizaci. Tato rizika musí uživatel odstranit zajištěním fyzické bezpečnosti zařízení a zajištěním šifrování dat na úrovni úložného zařízení.

7.2 Scénář používání nástroje pro podporu auditu

Pro správné použití tohoto nástroje je doporučen tento postup:

1. Základní nastavení
2. Nastavení hodnocení
3. Nastavení kritérií programu auditu
4. Prověření souladu
5. Příprava podkladů pro výstupní zprávu

V rámci základního nastavení je nutné nejprve vyplnit název organizace, která je předmětem auditu a zvolit osobu nebo orgán, čímž se určí, jaká opatření musí osoba nebo orgán splnit, pro zajištění souladu s vyhláškou.



Obrázek 30: Základní nastavení. Zdroj: Autor

V rámci tohoto nastavení je provedena identifikace osoby nebo orgánu pro vytvoření programu auditu. Nastavení osoby nebo orgánu zajišťuje univerzálnost použití právě podle zvolené osoby. Výběr osoby nebo orgánu zajišťuje vytvoření programu podle zvolené hodnoty. Během auditu není doporučené měnit nastavení. Nastavení nástroje zobrazuje Obrázek č. 30.

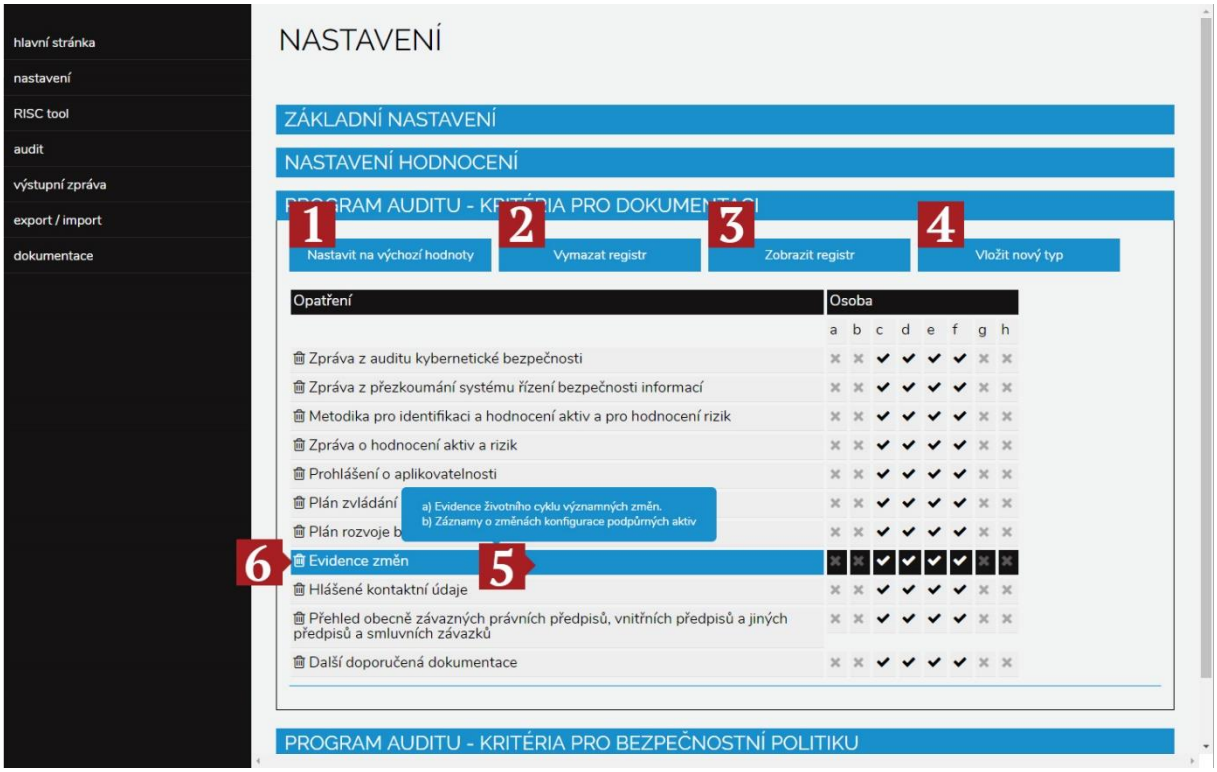
Další částí nastavení je stanovení hodnot použitelných pro hodnocení souladu. Nástroj používá dvě základní hodnoty:

- nezavedeno a
- zavedeno – plný soulad

Tyto hodnoty může uživatel nástroje upravit o další stupně hodnocení, které mohou být použity pro určení úrovně dosažení souladu s vyhláškou. V rámci nastavení i zde lze načíst přednastavené hodnoty. Tento číselník se nastavením výchozích hodnot rozšíří o:

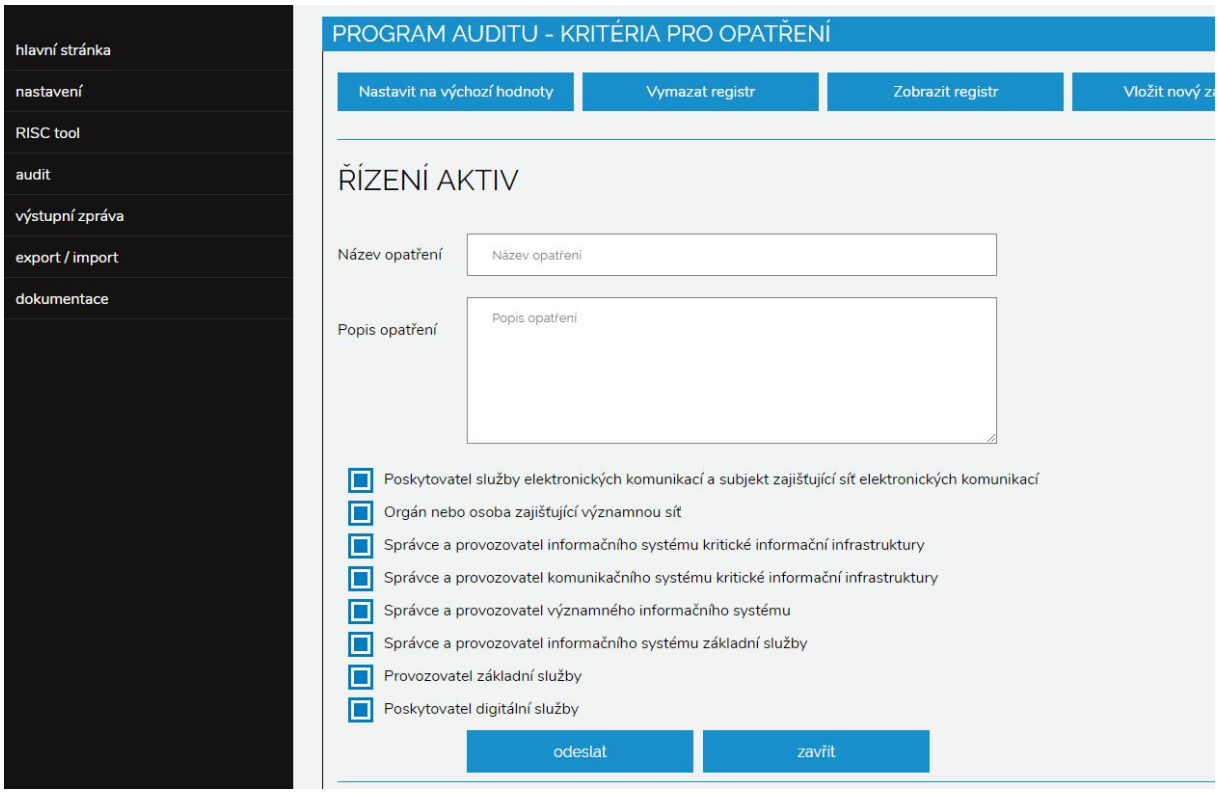
- neaplikovatelné,
- částečně zavedeno a
- v procesu zavádění.

Během používání nástroje se lze v rámci hodnocení souladu setkat ještě s další hodnotou „Nehodnoceno“, která značí, že hodnocení dosud nebylo provedeno.



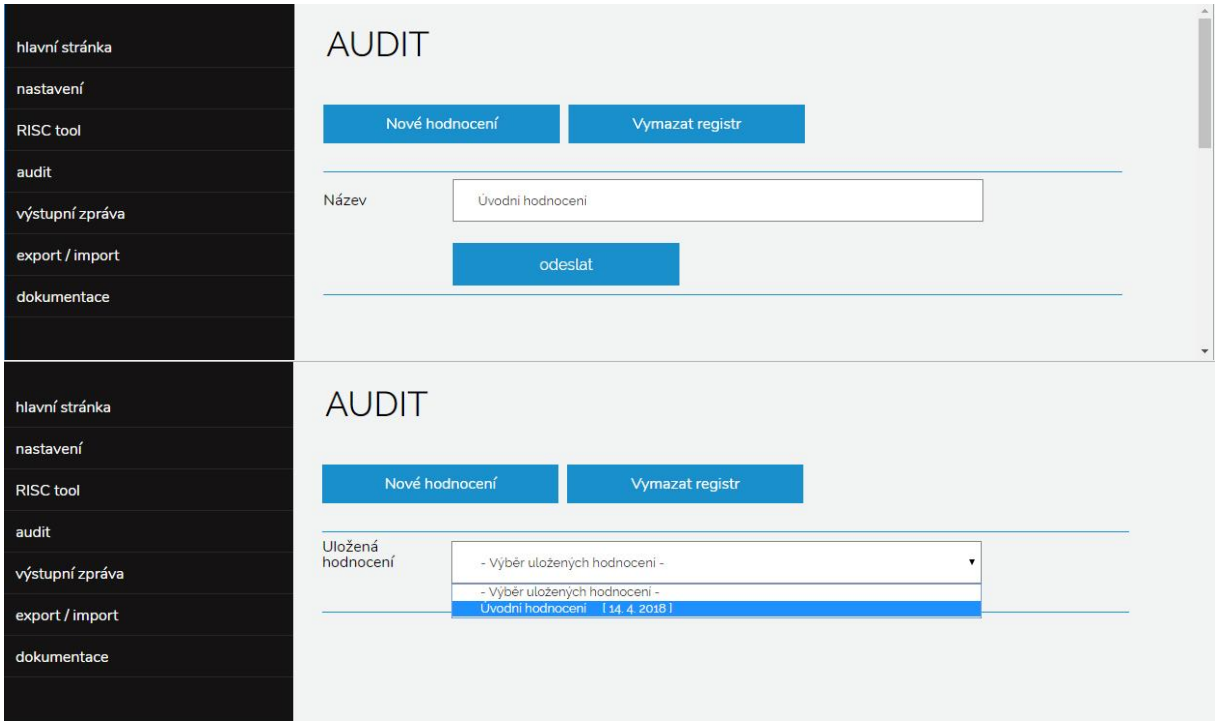
Obrázek 31: Práce s kritérii v nástroji. Zdroj: Autor

Na Obrázku č. 31 je ukázka práce s kritérii. Na obrázku jsou vyznačeny základní ovládací prvky. Pod číslem „1“ je funkce načtení výchozích hodnot. Uložené hodnoty obsahují ukázková data, nebo jsou jako výchozí data vloženy výsledky analýzy (například všechny kritéria programu auditu). Číslo „2“ je funkce, která vymaže všechna data v rámci spravované oblasti. Funkce Zobrazit registr, která je uvedena pod číslem „3“ zobrazí uložené hodnoty. Funkce pod číslem „4“ umožňuje vložit nový záznam do registru. Náhled poznámky je pod číslem „5“ a číslo „6“ je funkcí mazání dat.



Obrázek 32: Nové kritérium. Zdroj: Autor

Vložení nové hodnoty je zobrazeno na Obrázku č. 32. Pro nové kritérium je třeba vložit název. Je vhodné každé opatření srozumitelně popsat výstižným komentářem. Zároveň je pro každé opatření nutné určit osoby, kterých se dané opatření týká.

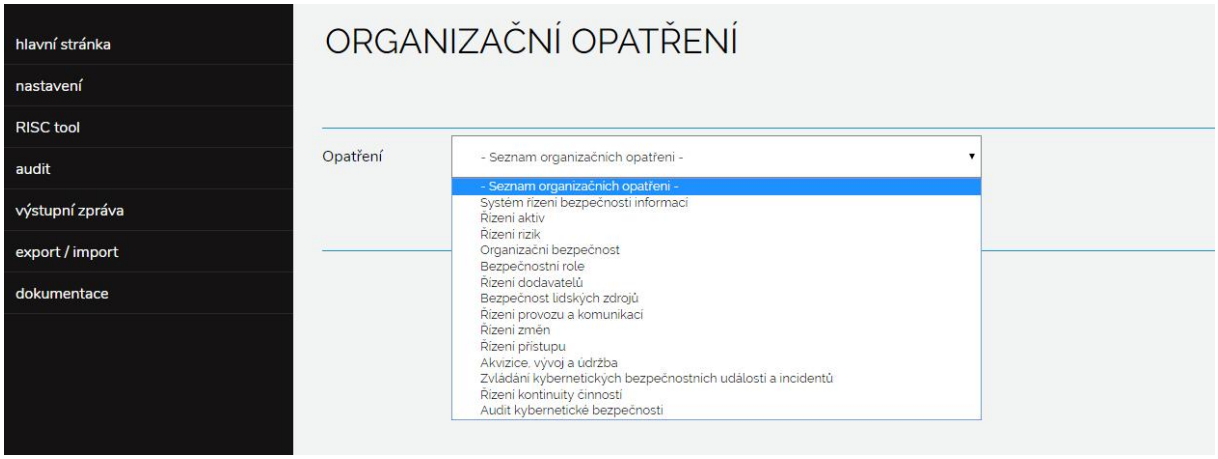


Obrázek 33: Vytvoření a výběr instance programu auditu. Zdroj: Autor

Samotné používání nástroje pro účely auditu kybernetické bezpečnosti je velmi nenáročné. Základním krokem je vytvoření instance programu auditu. Vytvoření nové instance je uvedeno na Obrázku č. 33 v horní části. Na základě nastavení osoby nebo orgánu a kritérií programu se sestaví checklist pro provádění prověření souladu. Instance je pro potřeby opakování posouzení shody nutné pojmenovat. Instance se pro větší přehlednost automaticky doplní o datum. Pro provedení posouzení shody je třeba vybrat, se kterou instancí programu auditu bude uživatel pracovat. Výběr instance, se kterou bude uživatel pracovat je naznačen na Obrázku č. 33 v dolní části obrázku. Ověření souladu s použitím nástroje je rozdělena do čtyř sekcí:

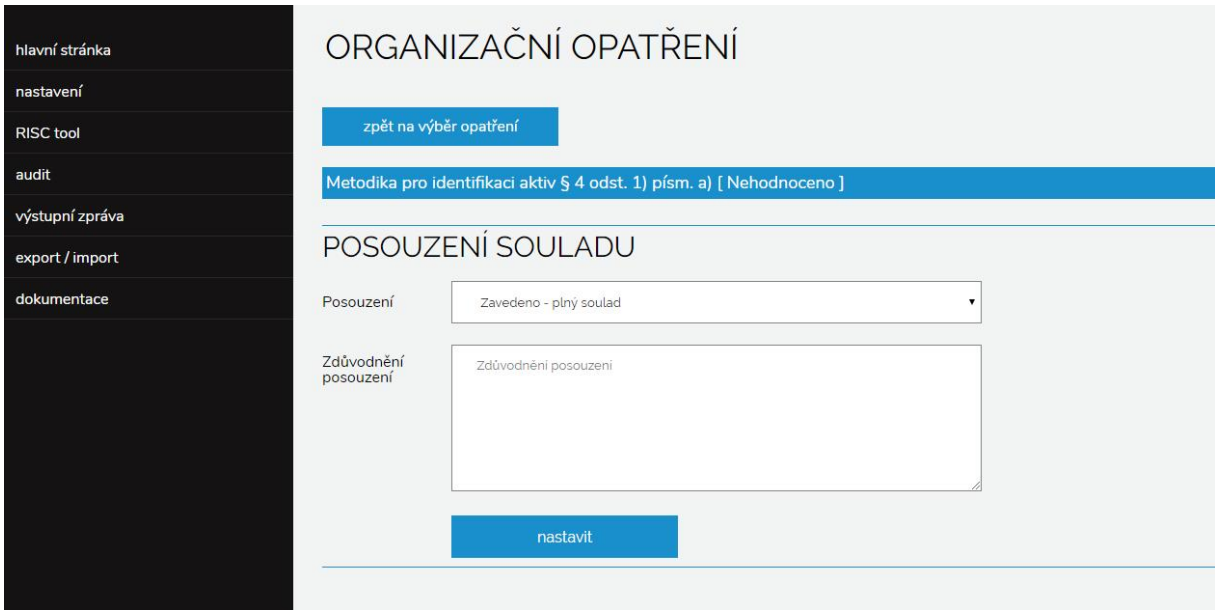
- organizační opatření,
- technická opatření,
- bezpečnostní politika a
- bezpečnostní dokumentace.

V případě organizačních a technických opatření je před hodnocením nutné zvolit konkrétní oblast opatření. Výběr opatření je uveden na Obrázku č. 34.

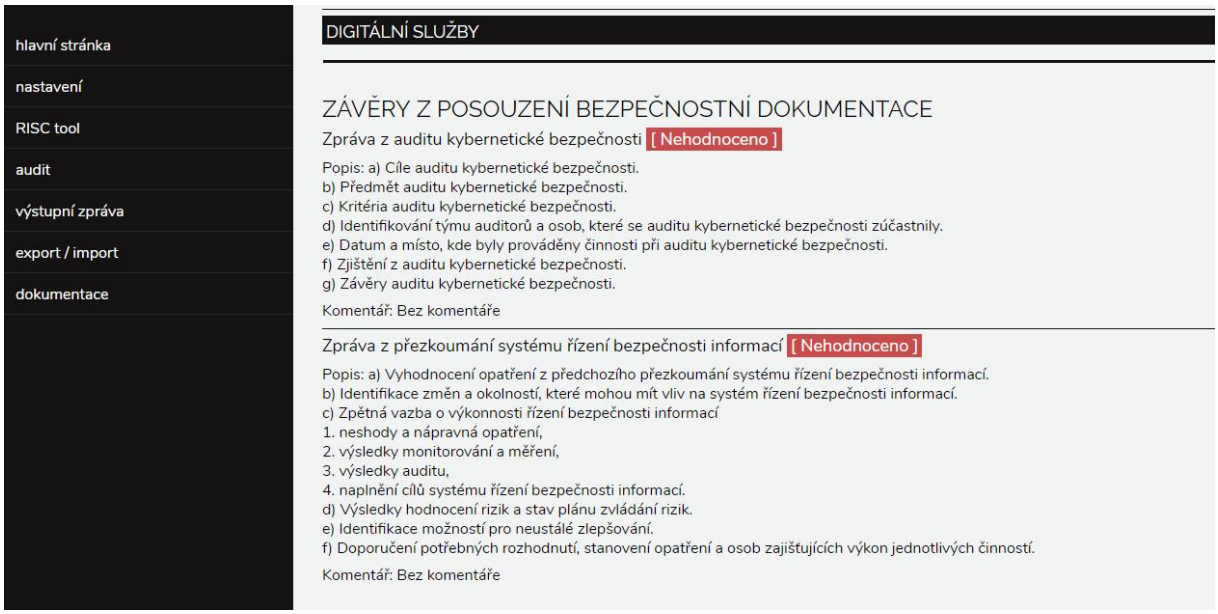


Obrázek 34: Výběr opatření. Zdroj: Autor

Výběrem oblasti hodnocení se dále pracuje s nastavenými kritérii a uživateli jen provádí nastavení stupně souladu. K tomu může uživatel svoje rozhodnutí zdůvodnit. Náhled na posouzení souladu je uveden na Obrázku č. 35. Stupeň souladu se vybírá z přednastavených hodnot, které byly definovány v rámci nastavení nástroje. Hodnocení uživatele nástroje je vhodné doplnit o zdůvodnění. Posouzení shody a jeho zdůvodnění je hlavním výstupem nástroje. Ukázka výstupu je uvedena na Obrázku č. 36. Výstup nástroje je kompletním výpisem z programu auditu podle zvolené osoby a provedených hodnocení. Pro každé opatření je ve výstupu uveden výsledek hodnocení a komentář podle Obrázku č. 35.



Obrázek 35: Posouzení. Zdroj: Autor



Obrázek 36: Ukázka výstupu. Zdroj: Autor

Nástroj pro podporu auditu i nástroj řízení aktiv a rizik v sobě obsahují také stručnou dokumentaci, ve které jsou popsány všechny podstatné informace pro používání nástroje. Dokumentace nástroje je uvedena v Příloze č. 2 a Příloze č. 3. Nástroj i jeho doplněk jsou součástí elektronické přílohy.

7.2.1 Doplněk nástroje

Základní ovládání doplňku je shodné jako pro nástroj pro podporu auditu. Výchozím krokem je opět základní nastavení. Pro použití musí uživatel provést nastavení způsobu hodnocení aktiv a způsob výpočtu rizika.

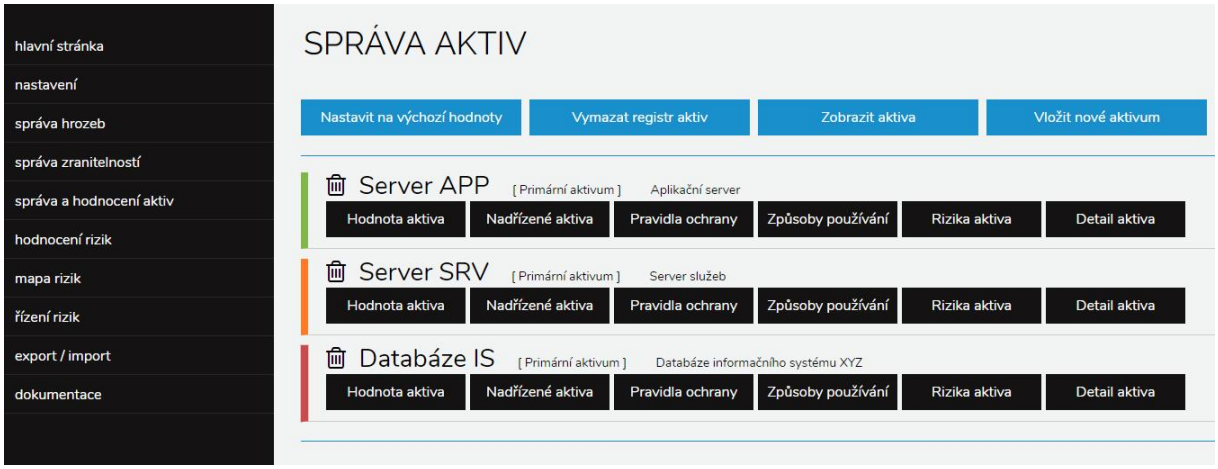
Způsob hodnocení aktiv musí podle vyhlášky vycházet z posouzení dopadů hrozeb na dostupnost (A), důvěrnost (C) a integritu (I). Proto může uživatel volit nastavení výpočtu několika způsoby:

- Hodnota bude stanovena bez použití stupňů
- Hodnota aktiva určena nejvyšší hodnotou z CIA
- Hodnota aktiva určena součtem hodnot z CIA
- Hodnota aktiva určena součinem hodnot z CIA
- Hodnota aktiva určena průměrem z hodnot CIA

Další nastavení udává, jakým způsobem se budou vypočítávat rizika. Uživatel má na výběr:

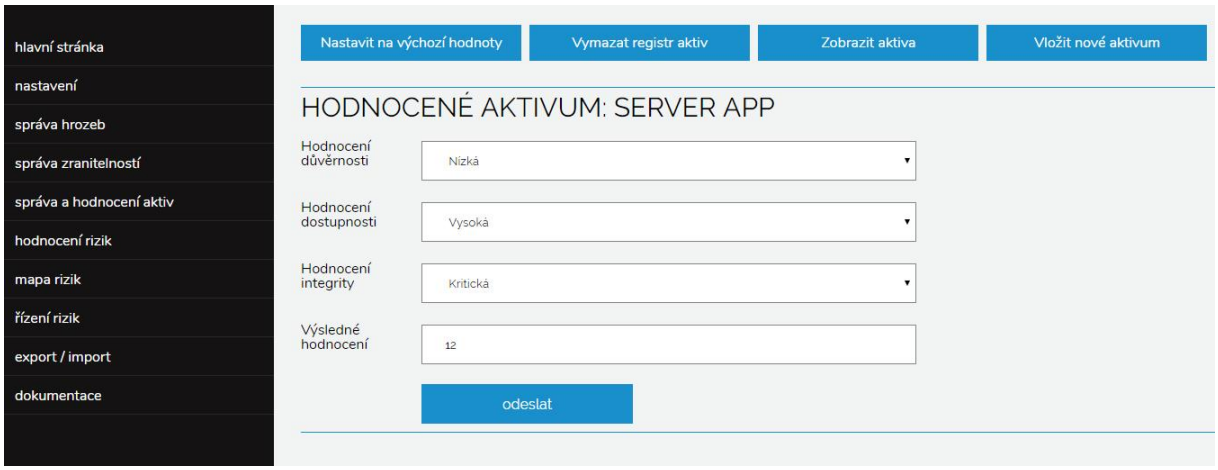
- Riziko = dopad × hrozba × zranitelnost
- Riziko = dopad (odvozený z hodnocení aktiv) × hrozba × zranitelnost

Nastavení způsobu výpočtu rizika je (podle vyhlášky č. 316/2014 Sb. i její novely) možné zvolit. Toto nastavení má vliv i na správu stupnic. Podle první možnosti výpočtu bude nutné v rámci nastavení definovat stupnici dopadu, podle druhé možnosti je pro hodnotu dopadu použita hodnota aktiva.

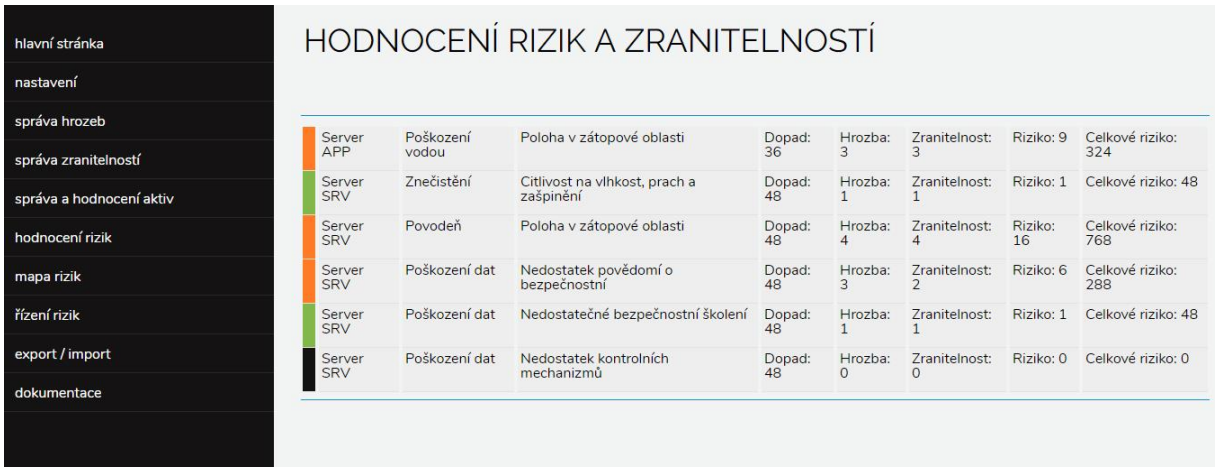


Obrázek 37: Správa aktiv. Zdroj: Autor

Správa aktiv uvedená na Obrázku č. 37 umožňuje evidovat všechny požadované údaje o aktivech. Předpokladem pro řízení rizik pro dané aktivum, je nutnost vyplnění všech povinných informací. Uživatel může prostřednictvím barevné indikace rychle a přehledně zjistit, která aktiva mají neúplně evidované informace. Pokud nebude mít aktivum vyplněny všechny podstatné informace, budou vyloučeny z řízení rizik. Ukázka hodnocení aktiva je na Obrázku č. 38. Na Obrázku č. 39 je zobrazeno hodnocení rizik. Hodnocení zobrazené na Obrázku č. 39 je interaktivní. Pro hodnocení nástroj využívá předdefinované hodnoty ze sekce Nastavení.



Obrázek 38: Hodnocení aktiv. Zdroj: Autor



Obrázek 39:Hodnocení rizik. Zdroj: Autor

Výstup z doplňku nástroje má dvě podoby. První je výpis zvládání rizik, který zobrazuje důležité informace z procesů řízení rizik dává uživatelům kompletní přehled o stavu řízení rizik. Na problémové oblasti je uživatel upozorněn. V rámci výpisu jsou uvedeny i aktiva, která byla kvůli nekompletnosti informací z hodnocení vynechána. Druhý způsob výpisu je zaměřen na aktiva. Tento výpis z evidence aktiv je souhrnný přehled inventáře a obsahuje kontroly úplnosti všech informací, které je nutné pro každé aktivum evidovat. Oba výpisy je možné připojit k závěrečné výstupní zprávě z auditu.

8 Závěr

Tato část práce shrne výsledky a zhodnotí naplnění stanovených cílů. V rámci teoretické části byla provedena rešerše zdrojů, které se zabývaly podobnými tématy a dále byly vysvětleny významné definice a termíny týkající se informační a kybernetické bezpečnosti, řízení rizik a auditu.

Třetí kapitola se věnovala informační a kybernetické bezpečnosti. V kapitole jsou podrobně rozebrány normy, zákony a vyhlášky, které se zabývají informační bezpečností. Jsou zde detailně popsány role působící v rámci řízení informační bezpečnosti a jsou identifikovány povinnosti osob a orgánů, které nařizuje zákon o kybernetické bezpečnosti. Kapitola dále popisuje vývoj regulací v oblasti kybernetické bezpečnosti. Vývoj regulací má vliv na auditované oblasti bezpečnostní politiky, bezpečnostní dokumentace a bezpečnostních opatření. V práci jsou porovnány rozdíly mezi doporučeními podle platné vyhlášky ve srovnání s návrhem její novely. Výstupem je komparace doporučení pro obsah bezpečnostní politiky a bezpečnostní dokumentace. Toto srovnání zachycuje, jaké změny s sebou přináší novela vyhlášky. Prostor je věnován i ochraně osobních údajů ve vztahu ke kybernetické bezpečnosti. Kapitola se také zabývá výkladem kybernetické bezpečnosti podle britského National Cyber Security Centre. Dokumenty popisují deset kroků, ve kterých jsou uvedeny doporučení pro zajištění bezpečnosti. V rámci třetí kapitoly jsou obsaženy i související témata, jako je význam lidského faktoru v souvislosti se zajišťováním bezpečnosti, výkladu problematických aspektů kybernetické bezpečnosti i fenoménu, kterým je kybernetická a informační válka.

Ve čtvrté kapitole je hlavním tématem řízení rizik. Jsou zde popsány vlivy rizik, které působí na organizaci a jejich aktiva, a jaké přístupy mohou organizace zaujmout při řízení rizik. Procesy řízení rizik jsou popsány podle ISO norem, které v této oblasti poskytují doporučení s ohledem na systém řízení bezpečnosti informací. V rámci kapitoly jsou diskutována témata řízení rizik, hodnocení a zvládání rizik, správy a hodnocení aktiv a identifikace hrozeb a zranitelností. Tato kapitola se stala podkladem pro vytvoření doplňkového modulu pro nástroj na podporu auditu, který je významným výstupem práce.

Pátá kapitola se věnuje výkladu důležitých pojmů a vysvětlením principů auditu. Tato kapitola dále popisuje přístup k auditu podle toho, kterou stranou je audit proveden, zabývá se rolí auditora v procesech auditu, popisem průběhu jednotlivých fází a také specifikuje výstup z auditu, kterým je auditorská zpráva. Závěr kapitoly se zabývá auditem podle novely vyhlášky o kybernetické bezpečnosti.

Na poznatky a zjištění z teoretické části navazuje praktická část práce. Hlavním cílem práce je návrh auditu a nástroje pro podporu průběhu auditu. Praktická část zahrnuje analýzu vyhlášky o kybernetické bezpečnosti, respektive její připravované novely. Výsledek analýzy je podkladem pro návrh provedení auditu. V rámci analýzy byly také identifikovány procesy pro určení povinných subjektů jako východisko pro audit. Určení subjektu významně ovlivňuje rozsah auditu. Dále je výstupem kapitoly podrobná analýza opatření, která jsou kritérii auditu. Pro každé opatření jsou identifikovány povinné subjekty, kterých se opatření týká. Rovněž jsou identifikovány významné dokumenty a normy, které poskytují podrobné informace ke každému opatření.

Na kapitolu, která se věnovala analýzám navazuje sedmá kapitola zabývající se návrhem auditu. V kapitole jsou představeny fáze auditu, a každá fáze je podrobněji popsána. Dále se kapitola věnuje popisu nástroje pro podporu průběhu auditu, včetně jeho funkcí a vlastností.

Přínosy práce jsou především výstupy analýz novely vyhlášky. Tyto informace jsou využitelné především pro všechny subjekty, kterých se týkají povinnosti uložené podle zákona a vyhlášky o kybernetické bezpečnosti. Práce poskytuje informace o změnách, které přináší novela vyhlášky. Významným přínosem je také nástroj, který je navržen podle novely vyhlášky, a je určen pro podporu průběhu auditu. Použití tohoto nástroje umožňuje ověřit soulad s novelizovanou vyhláškou. Nástroj je rozšířen o doplněk, který lze využít pro správu a řízení aktiv a rizik podle novely vyhlášky. Jeho důležitou funkcí je export podkladů pro výstup z auditu. Tyto podklady nástroj analyzuje a ověřuje soulad s vyhláškou o kybernetické bezpečnosti v oblastech řízení aktiv a řízení rizik.

Tato práce se věnovala auditu kybernetické bezpečnosti. V rámci zajištění kybernetické bezpečnosti jsou významné také další role, především role manažera a architekta. Také role garantů aktiv a všech uživatelů jsou neodmyslitelnou součástí informační bezpečnosti v organizaci. Rozvoj nástroje, který by zohlednil všechny role, by mohl být pro organizace komplexním nástrojem řízení informační bezpečnosti i zdrojem důležitých informací. Námětem na rozšíření nástroje mohou být i doplňky, které pokryjí správu a řízení podle všech opatření vyhlášky. Manažer a architekt významně ovlivňují kybernetickou bezpečnost a řízení informační bezpečnosti. Audit systému řízení bezpečnosti informací poskytuje zpětnou vazbu a hodnotí naplnění cílů, a výsledky auditu jsou podkladem pro další zlepšování. Pohledy manažera a architekta na oblast kybernetické bezpečnosti by rozšířily výklad tohoto tématu do komplexní podoby.

Terminologický slovník

Termín	Zkratka	Význam (zdroj)
akceptovatelné riziko		riziko zbývající po uplatnění bezpečnostních opatření, jehož úroveň je pro orgán nebo osobu, které jsou povinny zavést bezpečnostní opatření podle zákona, přijatelná (Příloha č. 1, 2018)
aktivum	A	aktivem je vše, co má pro organizaci nějakou hodnotu (Čermák, 2009)
audit		systematický, nezávislý a dokumentovaný proces pro získávání důkazů z auditu a pro jeho objektivní hodnocení s cílem stanovit rozsah, v němž jsou splněna kritéria auditu (ISO 9000, 2005)
bezpečností informací		zajištění důvěrnosti, integrity a dostupnosti informací a dat (Zákon č. 181/2014 Sb., 2018)
bezpečnostní politika		soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv (Příloha č. 1, 2018)
digitální služba		služba informační společnosti podle zákona upravujícího některé služby informační společnost), která spočívá v provozování on-line tržiště, internetového vyhledávače nebo cloud computingu (Zákon č. 181/2014 Sb., 2018)
dostupnost	A	informace jsou k dispozici podle potřeby (COBIT 4.1 Excerpt, 2007)
důvěrnost	C	ochrana citlivých informací před zneužitím (COBIT 4.1 Excerpt, 2007)
hrozba		potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu (Příloha č. 1, 2018)
informační systém základní služby		informační systém, na jehož fungování je závislé poskytování základní služby (Zákon č. 181/2014 Sb., 2018)
integrita	I	týká se platnosti, přesnosti a úplnosti informací (COBIT 4.1 Excerpt, 2007)
kritická informační infrastruktura	KII	prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti (Zákon č. 181/2014 Sb., 2018)
kybernetická bezpečnost	KB	souhrn právních, organizačních, technických, fyzických a vzdělávacích opatření namířených na zajištění nerušeného a bezvadného fungování kybernetického prostoru. (Věcný záměr zákona o kybernetické bezpečnosti, 2012, s. 56)
podpůrné aktivum		se rozumí technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému (Příloha č. 1, 2018)
primárním aktivum		se rozumí informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém (Příloha č. 1, 2018)
riziko		ochrana něčeho před zničením, poškozením nebo ztrátou (Čermák, 2009)
systém řízení bezpečnosti informací	ISMS	část systému řízení orgánu nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona, založená na přístupu k rizikům informačního a komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat, po vzoru normy ISO/IEC 27001 (Příloha č. 1, 2018)
technické aktivum		se rozumí technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, přičemž selhání technického aktiva může mít dopad na informační a komunikační systém (Příloha č. 1, 2018)
ujištění		obecné komplexní nezávislé prověření kontrol, které jsou delegovány na jiné subjekty vzhledem k cílům řízení. (Svatá, 2016, s.18)
Úřad		Národním úřadem pro kybernetickou a informační bezpečnost (Zákon č. 181/2014 Sb., 2018)
vyhláška o kybernetické bezpečnosti	VoKB	vyhláška, která provádí nařízení zákona (Zákon č. 181/2014 Sb., 2018)
významná sít		síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře (Zákon č. 181/2014 Sb., 2018)
významná změna		změna, která má nebo může mít vliv na bezpečnost informací a představuje vysoké riziko (Příloha č. 1, 2018)

významný informační systém	VIS	informační systém, na jehož fungování je závislé poskytování základní služby (Zákon č. 181/2014 Sb., 2018)
základní služba		služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví (Zákon č. 181/2014 Sb., 2018)
zákon o kybernetické bezpečnosti	ZoKB	zákon, který upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti (Zákon č. 181/2014 Sb., 2018)
zranitelnost		slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami (Příloha č. 1, 2018)

Seznam literatury a použitých zdrojů

10 Steps: Home and Mobile Working [online]. 2016, 2016 [cit. 2018-02-16]. Dostupné z: https://www.csc.gov.uk/guidance/10-steps-home-and-mobile-working

10 Steps: Incident Management [online]. 2016, 2016 [cit. 2018-02-16]. Dostupné z: https://www.ncsc.gov.uk/guidance/10-steps-incident-management

10 Steps: Malware Prevention [online]. 2016, 2016 [cit. 2018-02-16]. Dostupné z: https://www.ncsc.gov.uk/guidance/10-steps-malware-prevention

10 Steps: Managing User Privileges [online]. 2016, 2016 [cit. 2018-02-16]. Dostupné z: https://www.ncsc.gov.uk/guidance/10-steps-managing-user-privileges

10 Steps: Monitoring [online]. 2016, 2016 [cit. 2018-02-16]. Dostupné z: https://www.ncsc.gov.uk/guidance/10-steps-monitoring

10 Steps: Network Security [online]. 2016, 2016 [cit. 2018-02-16]. Dostupné z: https://www.ncsc.gov.uk/guidance/10-steps-network-security

10 Steps: Removable Media Controls [online]. 2016, 2016 [cit. 2018-02-16]. Dostupné z: https://www.ncsc.gov.uk/guidance/10-steps-removable-media-controls

10 Steps: Risk Management Regime [online]. 2016, 2016 [cit. 2018-02-16]. Dostupné z: https://www.ncsc.gov.uk/guidance/10-steps-information-risk-management-regime

10 Steps: Secure Configuration [online]. 2016, 2016 [cit. 2018-02-16]. Dostupné z: https://www.ncsc.gov.uk/guidance/10-steps-secure-configuration

10 Steps: User Education and Awareness [online]. 2016, 2016 [cit. 2018-02-16]. Dostupné z: https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness

Akční plán k Národní strategii kybernetické bezpečnosti. 2015. [online]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-967/akc48dnc3adplc3a1n-rkb-final-150408.pdf

BERLINGER, J. a M. VAZQUEZ. US military reviewing security practices after fitness app reveals sensitive info [online]. [cit. 2018-02-25]. Dostupné z: https://edition.cnn.com/2018/01/28/politics/strava-military-bases-location/index.html

Bezpečnostní dokumentace [online]. [cit. 2018-02-24]. Dostupné z: http://www.it-security.cz/sluzby/bezpecnostni-dokumentace.html

BÍNA, Lukáš. Zavedení systému řízení bezpečnosti informací v praxi. Praha, 2014 [cit. 2018-04-14]. Diplomová práce. Česká zemědělská univerzita v Praze.

BRECHLEROVÁ, Dagmar. Řešení informační bezpečnosti (1. část) [online]. [cit. 2018-02-18]. Dostupné z: https://www.systemonline.cz/clanky/reseni-informacni-bezpecnosti-1-cast.htm

Co přináší GDPR a jak je možné využít ISO 27001 a ZKB [online]. [cit. 2018-02-16]. Dostupné z: http://www.krucek.cz/cz/article/co-prinasi-gdpr-a-jak-je-mozne-vyuzit-iso-27001-a-zkb-87800/

COBIT 4.1 Excerpt. IT Governance Institute, 2007. [online]. [cit. 2018-03-16]. Dostupné z: https://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

Common threats to be aware of [online]. [cit. 2018-02-21]. Dostupné z: https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx

ČERMÁK, Miroslav. Řízení informačních rizik v praxi: vysokoškolská učebnice. Brno: Tribun EU, 2009. Knihovnicka.cz. ISBN 978-80-7399-731-1.

ČSN EN ISO 19011 - Směrnice pro auditování systémů managementu. Úřad pro technickou normalizaci, metodologii a státní zkušebnictví, 2012.

ČSN EN ISO 9000 Systémy managementu kvality: Základní principy a slovník. Český normalizační institut., 2005.

ČSN EN ISO/IEC 27001 Bezpečnostní techniky – Systémy řízení bezpečnosti informací: Požadavky. 2014.

ČSN ISO 31000 Management rizik: Principy a směrnice. 2010.

ČSN EN ISO/IEC 17021-1 Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu: Část 1: Požadavky. 2016.

ČSN ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací: - Přehled a slovník. 2009.

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

ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky: Řízení rizik bezpečnosti informací. 2013.

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

ČSN ISO/IEC 27007 Informační technologie – Bezpečnostní techniky: Směrnice pro audit systémů řízení bezpečnosti informací. 2016.

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

ČTK. Jako země i vzduch. NATO: Kyberprostor je novou dimenzí obrany [online]. [cit. 2018-02-24]. Dostupné z: https://www.tyden.cz/rubriky/zahranici/evropa/jako-zeme-i-vzduch-nato-kyberprostor-je-novou-dimenzi-obrany_390236.html

Directive on Security of Network and Information Systems [online]. [cit. 2018-02-22]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205

DOČEKAL, Daniel. Zaměstnanci zatajují kybernetické incidenty, bojí se potrestání. Přitom ohrožují firmu [online]. 2017 [cit. 2018-02-25]. Dostupné z: https://feedit.cz/2017/07/13/zamestnanci-zatajuji-kyberneticke-incidenty-boji-se-potrestani-pritom-ohrozuji-firmu/

DOUCEK, Petr. Bezpečnost informačních systémů a mezinárodní standardy. SYSTEMS INTEGRATION 2004. 2004.

DOUCEK, Petr. Dokumentace, kontrola a audit bezpečnosti IS/CT Jak bezpečnost kontrolovat? (1). AT&P journal, 2005, (3/2005).

DRAGANOV, Vojtěch. Zákon o kybernetické bezpečnosti a jeho dopady na povinné subjekty. Praha, 2016 [cit. 2018-04-14]. Diplomová práce. Vysoká škola ekonomická v Praze.

DURAČINSKÁ, Zuzana. Co přineslo a přinese schválení směrnice NIS? [online]. 2016 [cit. 2018-02-22]. Dostupné z: https://blog.nic.cz/2016/07/22/co-prineslo-a-prinese-schvaleni-smernice-nis/

EU General Data Protection Regulation – A Compliance Guide. IT governance, 2016.

FLEISCHMANNOVÁ, Veronika. Kybernetická bezpečnost. Praha, 2015 [cit. 2018-04-14]. Diplomová práce. Vysoká škola ekonomická v Praze.

FTOREK, Jozef. Manipulace a propaganda: na pozadí současné informační války. Praha: Grada, 2017. Právo (ANAG). ISBN 978-80-271-0605-9.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika: na pozadí současné informační války. 2., přeprac. a aktualiz. vyd. Praha: Grada, 2009. Expert (Grada). ISBN 978-80-247-2615-1.

Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016 [online]. Gartner [cit. 2018-02-25]. Dostupné z: https://www.gartner.com/newsroom/id/3598917

Global Cybersecurity Index 2017. International Telecommunication Union, 2017.

Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy. Praha, 2016. Dostupné z: http://data.idnes.cz/soubory/na_knihovna/59A151006_M02_016_20151005-HYBRIDNI-.PDF

Information security audit (IS audit): A guideline for IS audits based on IT-Grundschutz [online]. 2008 [cit. 2018-04-08]. Dostupné z: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ISRevision/guideline-isrevision_pdf.pdf?__blob=publicationFile

Information Systems Auditing: Tools and Techniques [online]. ISACA, 2016(3) [cit. 2018-04-08].

JEZIORSKÝ, Tomáš. Nový úřad pro kybernetickou bezpečnost. [online]. 2017 [cit. 2018-02-18]. Dostupné z: https://www.s3c.cz/blog/posts/novy-urad-pro-kybernetickou-bezpecnost

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

KAMENÍČEK, Lukáš. Kybernetická bezpečnost z pohledu podnikové informatiky. Praha, 2016 [cit. 2018-04-14]. Diplomová práce. Vysoká škola ekonomická v Praze.

KOHOUT, Jiří. Návrh bezpečnostní politiky informačních technologií v prostředí středně velké společnosti. Praha, 2013 [cit. 2018-04-14]. Bakalářská práce. Unicorn college.

KONEČNÝ, Martin. Nová vyhláška o kybernetické bezpečnosti [online]. 2017 [cit. 2018-02-20]. Dostupné z: https://www.govcert.cz/download/kii-vis/CyberCon2017/Martin_Konecny_Nova_VKB.pdf

KOSUTIC, Dejan. 9 Steps to Cybersecurity. The Manager's Information Security Strategy Manual [online]. [cit. 2018-03-26]. ISBN 978-953-57452-0-4.

KRATOCHVÍL, David. Kybernetická bezpečnost a legislativa ČR. Praha, 2013 [cit. 2018-04-14]. Diplomová práce. Vysoká škola ekonomická v Praze.

KRUČINSKÝ, Adam. Zákon o kybernetické bezpečnosti a směrnice NIS. Interní auditor, 2016, (3/2016).

LIDINSKÝ, Vít. EGovernment bezpečně: technické, forenzní a kybernetické aspekty. Praha: Grada, 2008. Expert (Grada). ISBN 978-80-247-2462-1.

MAISNER, Martin. Zákon o kybernetické bezpečnosti: komentář. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.

NÁDENÍČEK, Petr. Finance a bezpečnost, aneb peníze až na prvním místě [online]. 2006 [cit. 2018-02-25]. Dostupné z: https://firmy.finance.cz/zpravy/finance/66819-finance-a-bezpecnost-aneb-penize-az-na-prvnim-miste/

Národní úřad pro kybernetickou a informační bezpečnost [NÚKIB], nedatováno a IN Co je NÚKIB [online]. [cit. 2018-03-03]. Dostupné z: https://www.govcert.cz/

Národní úřad pro kybernetickou a informační bezpečnost [NÚKIB], nedatováno b IN Vyhláška o kybernetické bezpečnosti [online]. [cit. 2018-02-18]. Dostupné z: https://www.govcert.cz/cs/247-zakon-o-kb/legislativa-zkb/nova-vyhlaska-o-kb/

Národní úřad pro kybernetickou a informační bezpečnost [NÚKIB], nedatováno c IN NOVÁ VYHLÁŠKA O KYBERNETICKÉ BEZPEČNOSTI [online]. [cit. 2018-02-22]. Dostupné z: https://www.govcert.cz/cs/nova-vkb/

NCSI: National Cyber Security Index [online]. [cit. 2018-03-03]. Dostupné z: http://ncsi.ega.ee/ncsi-index/

NIS Network Information Security [online]. [cit. 2018-02-22]. Dostupné z: https://www.kr-vysocina.cz/assets/File.ashx?id_org=450008&id_dokumenty=4079266

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice: na pozadí současné informační války. Brno: Akademické nakladatelství CERM, 2013. Expert (Grada). ISBN 978-80-7204-872-4.

PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. Expert (Grada). ISBN 978-80-7380-589-0.

Poslání a smysl auditu [online]. [cit. 2018-03-22]. Dostupné z: http://www.kacr.cz/poslani-a-smysl-auditu

Projekt Kybernetický polygon [online]. [cit. 2018-02-18]. Dostupné z: https://www.kypo.cz/

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2018/151 [online]. [cit. 2018-02-22]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32018R0151&from=CS

PRŮŠA, Jiří. Česká republika dosáhla významného zlepšení v mezinárodním srovnání připravenosti na kybernetické útoky [online]. 2017 [cit. 2018-02-218]. Dostupné z: https://blog.nic.cz/2017/07/31/ceska-republika-dosahla-vyznamneho-zlepseni-v-mezinarodnim-srovnani-pripravenosti-na-kyberneticke-utoky/

ROHÁČEK, Martin. Nový základ internetové sítě i virtuální kolegové. Cisco předpovídá 6 technologických trendů příštích let [online]. 2017 [cit. 2018-02-21]. Dostupné z: https://blog.nic.cz/2017/07/31/ceska-republika-dosahla-vyznamneho-zlepseni-v-mezinarodnim-srovnani-pripravenosti-na-kyberneticke-utoky/

ŘEHKA, Karel. Informační válka. Praha: Academia, 2017. XXI. století. ISBN 978-80-200-2770-2.

SLÁMEČKA, Vladimír. Manažerská etika: vysokoškolská učebnice. Praha: České vysoké učení technické v Praze, 2012. XXI. století. ISBN 978-80-01-05005-7.

SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích: vysokoškolská učebnice. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.

SMEJKAL, Vladimír. Kybernetická kriminalita: vysokoškolská učebnice. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.

SVATÁ, Vlasta. Audit informačního systému: vysokoškolská učebnice. 2. vyd. Praha: Professional Publishing, 2012. Expert (Grada). ISBN 978-80-7431-106-2.

SVATÁ, Vlasta. Audit informačního systému: vysokoškolská učebnice. V Praze: Oeconomica, nakladatelství VŠE, 2016. Expert (Grada). ISBN 978-80-245-2168-8.

ŠEDIVÁ, Zuzana, GŘIVNA, Tomáš a Radim POLČÁK, ed. Kyberkriminalita a právo: na pozadí současné informační války. Praha: Auditorium, 2008. Expert (Grada). ISBN 978-80-903786-7-4.

ŠKORNIČKOVÁ, Eva. nedatováno a IN Jaké povinnosti ukládá GDPR institucím a firmám [online]. [cit. 2018-02-15]. Dostupné z: https://www.gdpr.cz/gdpr/povinnosti/

ŠKORNIČKOVÁ, Eva. nedatováno b IN Co považuje GDPR za osobní údaje [online]. [cit. 2018-02-15]. Dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

ŠKORNIČKOVÁ, Eva. nedatováno IN Jaké sankce hrozí firmám, které budou GDPR ignorovat [online]. [cit. 2018-02-16]. Dostupné z: https://www.gdpr.cz/gdpr/sankce/

ŠMÍD, Jaroslav. Implementace ZKB. Kritická informační infrastruktura a Významné informační systémy. Jaroslav Šmíd náměstek ředitele NBÚ [online]. [cit. 2018-04-03]. Dostupné z: http://docplayer.cz/33289496-Implementace-zkb-kriticka-informacni-infrastruktura-a-vyznamne-informacni-systemy-jaroslav-smid-namestek-reditele-nbu.html

TOBOLKA, Martin. ISMS, ITSM, BCMS – kdy se zabývat certifikací organizace a jaký to má přínos? [online]. 2012 [cit. 2018-02-25]. Dostupné z: https://www.cqs.cz/Novinky/ISMS-ITSM-BCMS-kdy-se-zabyvat-certifikaci-organizace-a-jaky-to-ma-prinos.html

Věcný záměr zákona o kybernetické bezpečnosti. 2012. [online]. Dostupné z: https://www.govcert.cz/download/legislativa/container-nodeid-926/vecny-zamer-final-vlada.pdf

Vyhláška č. 205/2016 Sb. Vyhláška, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. [online]. [cit. 2018-02-22]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-205

Vyhláška č. 316/2014 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. [online]. [cit. 2018-02-22]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-316/zneni-20150101#p15

Vyhláška č. 437/2017 Sb. Vyhláška o kritériích pro určení provozovatele základní služby. [online]. [cit. 2018-02-22]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-437

VYORAL, Tomáš. ČEŠI JSOU ONLINE NEOPATRNÍ, INDEX BEZPEČNOSTI JE NA MINIMU [online]. 2012 [cit. 2018-02-25]. Dostupné z: https://www.ekonomickymagazin.cz/2017/11/cesi-jsou-online-neopatrni-index-bezpecnosti-je-na-minimu/

Zákon č. 104/2017 Sb. Zákon, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony. [online]. [cit. 2018-02-22]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-104

Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů. [online]. [cit. 2018-02-17]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

Zákon č. 183/2017 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích. [online]. [cit. 2018-02-22]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-183

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. [online]. [cit. 2018-02-22]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205

Zásady tvorby bezpečnostní dokumentace informačních systémů určených k nakládání s utajovanými informacemi. Národní bezpečnostní úřad, 2017.

ŽŮREK, Jiří. Praktický průvodce GDPR: vysokoškolská učebnice. Olomouc: ANAG, 2017. Právo (ANAG). ISBN 978-80-7554-097-3.

Seznam obrázků

Obrázek 1: Vztah kybernetické a informační bezpečnosti. Zdroj: vlastní úprava podle (Kosutic, 2012) 10
Obrázek 2: Hodnotící kritéria srovnávání kybernetické bezpečnosti Global Cybersecurity Index 2017. Zdroj: (Global Cybersecurity Index 2017, 2017) 11
Obrázek 3: Srovnání výsledků kybernetické bezpečnosti podle NCSI z 3. března 2018. Zdroj: (National Cyber Security Index, 2018) 12
Obrázek 4: Srovnání výsledků kybernetické bezpečnosti podle Global Cybersecurity Index 2017. Zdroj: (Global Cybersecurity Index 2017, 2017) 12
Obrázek 5: Schematické znázornění vztahů k zákonu o kybernetické bezpečnosti: Zdroj: (Konečný, 2017) 16
Obrázek 6: Proces určení subjektů kritické infrastruktury. Zdroj: (Šmíd, nedatováno) 20
Obrázek 7: Proces určení subjektů VIS. Zdroj: (Šmíd, nedatováno) 20
Obrázek 8: RACI matice odpovědností za procesy řízení kybernetické bezpečnosti. Zdroj: (NUKIB, nedatováno d) 21
Obrázek 9: PDCA cyklus podle ISO 27000. 28
Obrázek 10:Sada norem ISO 27000 a provázanost jednotlivých norem. Zdroj: (ISO 27000, 2009)31
Obrázek 11: Deset kroků kybernetické bezpečnosti. Zdroj: (10 Steps: Risk Management Regime, 2016) 41
Obrázek 12: Úrovně typů válek. Zdroj: Autor 46
Obrázek 13: Mechanismus uplatnění rizika. Zdroj (Čermák, 2009) 48
Obrázek 14: Optimum investic do bezpečnosti. Zdroj: (Čermák, 2009) 49
Obrázek 15: Řízení rizik podle ISO 31000 a ISO 27005. Zdroj: (ISO 31000, 2010) 50
Obrázek 16: PDCA cyklus řízení rizik podle ISO 27005. Zdroj (ISO 27005, 2013) 51
Obrázek 17: Mapa rizik. Zdroj: (Smejkal, Rais, 2013; Svatá, 2016) 56
Obrázek 18: Vztahy a pojmy týkající se auditu. Zdroj: (ISO 9000, 2005) 59
Obrázek 19: Odkazování v normách. Zdroj: Autor 61
Obrázek 20: ISO 27007 v procesech řízení bezpečnosti informací. Zdroj: Autor 61
Obrázek 21: Typický vývojový diagram procesu auditu a certifikace. Zdroj: (ISO 17021-1, 2016) 65
Obrázek 22: PDCA cyklus programu auditu. Zdroj: (ISO 19011, 2011) 68
Obrázek 23: Typické činnosti při auditu. Zdroj: (ISO 19011, 2011) 69
Obrázek 24: Přehled procesu shromažďování a ověřování informací. Zdroj: (ISO 19011, 2011) .. 70
Obrázek 25: Zjednodušený proces určení povinného subjektu podle ZoKB. Zdroj: Autor 74

Obrázek 26: Vazby mezi opatřeními. Zdroj: Autor 75
Obrázek 27: Fáze plánování. Zdroj: (Information Systems Auditing: Tools and Techniques, 2016) 83
Obrázek 28: Fáze provádění a dokumentace. Zdroj:(Information Systems Auditing: Tools and Techniques, 2016)..... 84
Obrázek 29: Fáze reportování. Zdroj:(Information Systems Auditing: Tools and Techniques, 2016) 85
Obrázek 30: Základní nastavení. Zdroj: Autor 87
Obrázek 31: Práce s kritérii v nástroji. Zdroj: Autor..... 88
Obrázek 32: Nové kritérium. Zdroj: Autor 89
Obrázek 33: Vytvoření a výběr instance programu auditu. Zdroj: Autor 89
Obrázek 34: Výběr opatření. Zdroj: Autor 90
Obrázek 35: Posouzení. Zdroj: Autor 91
Obrázek 36: Ukázka výstupu. Zdroj: Autor 91
Obrázek 37: Správa aktiv. Zdroj: Autor 92
Obrázek 38: Hodnocení aktiv. Zdroj: Autor 93
Obrázek 39:Hodnocení rizik. Zdroj: Autor..... 93

Seznam tabulek

Tabulka 1: Průběh a výhled významných událostí spojených se směrnicí NIS. Zdroj: (Directive on Security of Network and Information Systems, 2018) 18
Tabulka 2: Povinnosti osob a orgánů podle § 3 ZoKB. Zdroj: (Zákon č. 181/2014 Sb., 2014) 23
Tabulka 3: Opatření ve vyhlášce 316/2014 Sb. a její chystané aktualizace. Zdroj: Příloha č. 1 a (Vyhláška č. 316/2014 Sb., 2014) 27
Tabulka 4: Doporučení struktura bezpečnostní dokumentace a bezpečnostní politika podle doporučení z vyhlášky 316/2014 ver srovnání s připravovanou novou podobou vyhlášky.Zdroj: Příloha č. 1 a (Vyhláška č. 316/2014 Sb., 2014) 35
Tabulka 5: Vyjádření hrozeb a zranitelností. Zdroj: Autor 55
Tabulka 6: Srovnání charakteristik interní a externí analýzy rizik. Zdroj: (Čermák, 2009) 57
Tabulka 7: Důležité termíny. Zdroj: (ISO 9000, 2005) 60
Tabulka 8: Výrok auditora. Zdroj: (Poslání a smysl auditu, 2018; Svatá, 2016) 72
Tabulka 9: Základní kritéria auditu kybernetické bezpečnosti a jejich platnost pro orgán nebo osobu. Zdroj: Příloha č. 1 76
Tabulka 10: Související dokumenty 81
Tabulka 11: Relativní časová náročnost auditu. Zdroj: (Information security audit, 2008) 84

Seznam příloh

Příloha 1: Návrh vyhlášky o kybernetické bezpečnosti 111
Příloha 2: Dokumentace nástroje pro podporu průběhu 159
Příloha 3: Dokumentace doplňku nástroje pro podporu průběhu 161

Příloha 1

Návrh vyhlášky o kybernetické bezpečnosti

o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 28 odst. 2 písm. a) až d) a f) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb. a zákona č. 205/2017 Sb. (dále jen „zákon“):

ČÁST PRVNÍ

ÚVODNÍ USTANOVENÍ

§ 1

Předmět úpravy

Tato vyhláška zapracovává příslušný předpis Evropské unie[18]) a pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém, informační systém základní služby anebo informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb, upravuje

a) obsah a strukturu bezpečnostní dokumentace,
b) obsah bezpečnostních opatření, rozsah jejich zavedení,
c) typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
d) náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
e) náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
f) vzor oznámení kontaktních údajů a jeho formu a
g) způsob likvidace dat, provozních údajů, informací a jejich kopií.

Celex 32016L1148

[18]) 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.

§ 2

Vymezení pojmů

V této vyhlášce se rozumí

a) administrátorem role zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva,
b) akceptovatelným rizikem riziko zbývající po uplatnění bezpečnostních opatření, jehož úroveň je pro orgán nebo osobu, které jsou povinny zavést bezpečnostní opatření podle zákona, přijatelná,
c) aktivem primární aktivum a podpůrné aktivum; aktivem
    1. primárním se rozumí informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém,
    2. podpůrným se rozumí technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému,
    3. technickým se rozumí technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, přičemž selhání technického aktiva může mít dopad na informační a komunikační systém,
d) bezpečnostní politikou soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv,
e) hodnocením rizik celkový proces identifikace, analýzy a vyhodnocení rizik,
f) hrozbou potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu,
g) informačním a komunikačním systémem informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém, informační systém základní služby anebo informační systém nebo síť elektronických komunikací, kterou využívá poskytovatel digitálních služeb,
h) rizikem možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu,
i) řízením rizik činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik,
j) systémem řízení bezpečnosti informací část systému řízení orgánu nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona, založená na přístupu k rizikům informačního a komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat, po vzoru normy ISO/IEC 27001,
k) uživatelem fyzická nebo právnická osoba anebo orgán veřejné moci, který využívá aktiva,
l) významným dodavatelem provozovatel a každý, kdo s orgánem nebo osobou, které jsou povinny zavést bezpečnostní opatření podle zákona, vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému,
m) významnou změnou změna, která má nebo může mít vliv na bezpečnost informací a představuje vysoké riziko,
n) zranitelností slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

ČÁST DRUHÁ

BEZPEČNOSTNÍ OPATŘENÍ

HLAVA I

ORGANIZAČNÍ OPATŘENÍ

§ 3

Systém řízení bezpečnosti informací

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v rámci systému řízení bezpečnosti informací

a) deklarují vůdčí roli a závazek vrcholového vedení tohoto orgánu nebo osoby (dále jen „vrcholové vedení"), k podpoře kybernetické bezpečnosti,
b) stanoví s ohledem na požadavky dotčených stran a organizační bezpečnost rozsah a hranice systému řízení bezpečnosti informací, ve kterých určí, kterých organizačních částí a aktiv se systém řízení bezpečnosti informací týká,
c) stanoví cíle systému řízení bezpečnosti informací,
d) pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik zavedou přiměřená bezpečnostní opatření,
e) řídí rizika podle § 5,
f) vytvoří a schválí bezpečnostní politiku v oblasti systému řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku v dalších oblastech podle § 28 a zavedou příslušná bezpečnostní opatření,
g) zajistí provedení auditu kybernetické bezpečnosti u informačního a komunikačního systému (dále jen „audit kybernetické bezpečnosti") podle § 15,
h) zajistí pravidelné vyhodnocování účinnosti systému řízení bezpečnosti informací, které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací, a to nejméně jednou ročně nebo při významné změně anebo v závislosti na kybernetickém bezpečnostním incidentu,
i) průběžně identifikují a následně podle § 11 řídí významné změny, které patří do rozsahu systému řízení bezpečnosti informací,
j) aktualizují systém řízení bezpečnosti informací a příslušnou dokumentaci na základě zjištění auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými významnými změnami a
k) řídí provoz a zdroje systému řízení bezpečnosti informací, zaznamenávají činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik.

(2) Pokud jsou orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, certifikovány podle příslušné technické normy[19]) akreditovaným certifikačním orgánem a zároveň je v

[19]) ISO/IEC 27001.

rozsahu certifikace zahrnut informační a komunikační systém, pak se předpokládá soulad s požadavky této vyhlášky.

Celex 32016L1148

§ 4

Řízení aktiv

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v rámci řízení aktiv

a) stanoví metodiku pro identifikaci aktiv,
b) stanoví metodiku pro hodnocení aktiv alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce,
c) identifikují a evidují aktiva,
d) určí a evidují garanty aktiv,
e) hodnotí a evidují primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní podle písmene b),
f) určí a evidují vazby mezi primárními a podpůrnými aktivy a hodnotí důsledky závislostí mezi primárními a podpůrnými aktivy,
g) hodnotí podpůrná aktiva a zohledňují přitom zejména vzájemné závislosti podle písmene f),
h) na základě hodnocení aktiv stanovují a zavádí pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv,
i) stanoví přípustné způsoby používání aktiv a pravidla pro manipulaci s aktivy s ohledem na úroveň aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv,
j) určí způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv, přičemž zohledňují přílohu č. 4 k této vyhlášce.

(2) Při hodnocení důležitosti primárních aktiv je třeba především posoudit

a) rozsah a důležitost osobních údajů nebo obchodního tajemství,
b) rozsah dotčených právních povinností nebo jiných závazků,
c) rozsah narušení vnitřních řídících a kontrolních činností,
d) poškození veřejných, obchodních nebo ekonomických zájmů, možné finanční ztráty,
e) dopady na poskytování důležitých služeb,
f) rozsah narušení běžných činností,
g) dopady na zachování dobrého jména nebo ochranu dobré pověsti,
h) dopady na bezpečnost a zdraví osob,
i) dopady na mezinárodní vztahy a
j) dopady na uživatele informačního a komunikačního systému.

Celex 32016L1148

§ 5

Řízení rizik

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v rámci řízení rizik v návaznosti na § 4

a) stanoví metodiku pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik,
b) s ohledem na aktiva identifikují relevantní hrozby a zranitelnosti; přitom zvažují zejména kategorie hrozeb a zranitelností uvedených v příloze č. 3 k této vyhlášce,
c) provádí hodnocení rizik v pravidelných intervalech podle odstavce 2 a při významných změnách,
d) při hodnocení rizik zohlední relevantní hrozby a zranitelnosti, posoudí možné dopady na aktiva; tato rizika hodnotí minimálně v rozsahu podle přílohy č. 2 k této vyhlášce,
e) zpracují zprávu o hodnocení rizik,
f) zpracují na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled bezpečnostních opatření požadovaných touto vyhláškou, která
   1. nebyla aplikována, včetně odůvodnění,
   2. byla aplikována, včetně způsobu plnění,
g) zpracují a zavedou plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a způsob realizace bezpečnostních opatření,
h) při hodnocení rizik a v plánu zvládání rizik zohlední
   1. významné změny,
   2. změny rozsahu a hranic systému řízení bezpečnosti informací,
   3. opatření podle § 11 zákona,
   4. kybernetické bezpečnostní incidenty, včetně dříve řešených,
i) v souladu s plánem zvládání rizik zavádí bezpečnostní opatření.

(2) Orgány a osoby uvedené v § 3 písm. e) zákona provádí hodnocení rizik alespoň jednou za tři roky a orgány a osoby uvedené v § 3 písm. c), d) a f) zákona alespoň jednou ročně.

(3) Řízení rizik může být zajištěno i jinými způsoby, než jak je stanoveno v odstavci 1 písm. d), pokud orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, zabezpečí, že použitá opatření zajistí stejnou nebo vyšší úroveň procesu řízení rizik.

(4) S výstupy podle odstavce 1 musí být seznámeno vrcholové vedení.

Celex 32016L1148

§ 6

Organizační bezpečnost

(1) Vrcholové vedení s ohledem na systém řízení bezpečnosti informací

a) zajistí stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací podle § 3 slučitelných se strategickým směřováním orgánu nebo osoby,
b) zajistí integraci systému řízení bezpečnosti informací do procesů orgánu nebo osoby,
c) zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací,
d) komunikuje význam systému řízení bezpečnosti informací a význam dosažení shody s jeho požadavky se všemi dotčenými stranami,
e) zajistí podporu k dosažení zamýšlených výstupů systému řízení bezpečnosti informací orgánu nebo osoby,
f) vede a podporuje zaměstnance k rozvíjení efektivity systému řízení bezpečnosti informací,
g) prosazuje neustálé zlepšování systému řízení bezpečnosti informací,
h) podporuje bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,
i) stanoví pravidla pro určení osob, které budou zastávat bezpečnostní role nebo role administrátorů,
j) zajistí, aby smlouvy s fyzickými osobami zastávajícími bezpečnostní role a role administrátorů obsahovaly ustanovení o bezpečnosti informací,
k) pro bezpečnostní role zajistí příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů,
l) účastní se testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

(2) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, zavedou organizaci řízení bezpečnosti informací, v rámci které určí

a) výbor pro řízení kybernetické bezpečnosti, který je organizovanou skupinu tvořenou osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení bezpečnosti informací a osobami významně se podílejícími na řízení a koordinaci činností spojených s kybernetickou bezpečností a který musí být složen alespoň z jednoho zástupce vrcholového vedení a z manažera kybernetické bezpečnosti,
b) bezpečnostní role a
c) jejich práva a povinnosti související se systémem řízení bezpečnosti informací.

(3) Orgán nebo osoba uvedené v § 3 písm. c), d) a f) zákona určí bezpečnostní roli

a) manažera kybernetické bezpečnosti
b) architekta kybernetické bezpečnosti,
c) garanta aktiva a
d) auditora kybernetické bezpečnosti.

4) Orgán nebo osoba uvedené v § 3 písm. e) zákona určí roli manažera kybernetické bezpečnosti. Ostatní bezpečnostní role podle odstavce 3 určí přiměřeně vzhledem k rozsahu a potřebám systému řízení bezpečnosti informací.

(5) Orgán nebo osoba uvedené v § 3 písm. c), d) a f) zákona zajistí zastupitelnost bezpečnostních rolí uvedených v odstavci 3 písm. a) a b).

(6) Orgán nebo osoba uvedené v § 3 písm. e) zákona zajistí zastupitelnost bezpečnostní role manažera kybernetické bezpečnosti.

(7) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, u výboru pro řízení kybernetické bezpečnosti podle odstavce 2 písm. a) dále zohledňují doporučení uvedená v příloze č. 6 k této vyhlášce.

Celex 32016L1148

§ 7

Bezpečnostní role

(1) Manažer kybernetické bezpečnosti

a) je bezpečnostní role odpovědná za systém řízení bezpečnosti informací, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s řízením kybernetické bezpečnosti, nebo s řízením bezpečnosti informací
   1. po dobu nejméně tří let, nebo
   2. po dobu jednoho roku, pokud úspěšně ukončila vysokoškolské vzdělání,
b) pravidelně informuje vrcholové vedení o
   1. činnostech vyplývajících z rozsahu jeho odpovědnosti a
   2. stavu systému řízení bezpečnosti informací a
c) nesmí vykonávat role odpovědné za provoz informačních a komunikačních systémů.

(2) Architekt kybernetické bezpečnosti

a) je bezpečnostní role zajišťující návrh implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému,
b) je pro činnost podle písmene a) vyškolen a prokáže odbornou způsobilost praxí s navrhováním implementace bezpečnostních opatření a zajišťováním architektury bezpečnosti
   1. po dobu nejméně tří let, nebo
   2. po dobu jednoho roku, pokud úspěšně ukončila vysokoškolské vzdělání, a
c) nesmí vykonávat role odpovědné za provoz informačních a komunikačních systémů.

(3) Garant aktiva je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva.

(4) Auditor kybernetické bezpečnosti

a) je bezpečnostní role odpovědná za provádění auditu kybernetické bezpečnosti, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti, popř. auditů systému řízení bezpečnosti informací
   1. po dobu nejméně tří let, nebo
   2. po dobu jednoho roku, pokud úspěšně ukončila vysokoškolské vzdělání a
b) provádí audit kybernetické bezpečnosti nestranně a výkon jeho role je oddělen od výkonu bezpečnostních rolí uvedených v § 6 odst. 3 písm. a) až c).

(5) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, u bezpečnostních rolí dále zohledňují doporučení uvedená v příloze č. 6 k této vyhlášce.

Celex 32016L1148

§ 8

Řízení dodavatelů

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona,

a) stanoví pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací,
b) evidují své významné dodavatele,
c) prokazatelně informují své významné dodavatele o jejich evidenci podle písmene b),
d) seznamují své dodavatele s pravidly podle písmene a) a vyžadují plnění těchto pravidel,
e) řídí rizika spojená s dodavateli,
f) v souvislosti s řízením rizik spojených s významnými dodavateli zajistí, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti uvedené v příloze č. 7 k této vyhlášce,
g) pravidelně přezkoumávají plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací.

(2) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, u významných dodavatelů dále

a) v rámci výběrového řízení a před uzavřením smlouvy provádí hodnocení rizik souvisejících s plněním předmětu výběrového řízení přiměřeně podle přílohy č. 2 k této vyhlášce,
b) v rámci uzavíraných smluvních vztahů stanoví způsoby a úrovně realizace bezpečnostních opatření a určí obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření,
c) provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany a
d) v reakci na rizika a zjištěné nedostatky zajistí jejich řešení.

(3) Náležitosti prokazatelného informování podle odstavce 1 písm. c) jsou

a) identifikace správce nebo provozovatele,
b) identifikace informačního a komunikačního systému,
c) identifikace významného dodavatele,
d) vyrozumění o skutečnosti, že dodavatel je pro správce významným dodavatelem, a popřípadě také o tom, že významný dodavatel je zároveň provozovatelem podle § 2 písm. g) zákona, a
e) obsah pravidel podle odstavce 1 písm. a).

(4) Orgán nebo osoba uvedená v § 3 písm. c) až f) zákona, která je provozovatelem a byla prokazatelně informována podle odstavce 1 písm. c), hlásí kontaktní údaje formou uvedenou v § 34.

Celex 32016L1148

§ 9

Bezpečnost lidských zdrojů

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v rámci řízení bezpečnosti lidských zdrojů

a) s ohledem na stav a potřeby systému řízení bezpečnosti informací stanoví plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah
   1. poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice a
   2. potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role,
b) určí osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny,
c) v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení,
d) pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajistí pravidelná odborná školení, přičemž vychází z aktuálních potřeb orgánu nebo osoby v oblasti kybernetické bezpečnosti,
e) v souladu s plánem rozvoje bezpečnostního povědomí zajistí pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní,
f) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role,
g) v případě ukončení smluvního vztahu s uživateli, administrátory a osobami zastávajícími bezpečnostní role zajistí předání odpovědností,
h) hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí a
i) určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.

(2) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, vedou o školení podle odstavce 1 přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

§ 10

Řízení provozu a komunikací

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v rámci řízení provozu a komunikací zajišťují bezpečný provoz informačního a komunikačního systému a stanoví provozní pravidla a postupy, které obsahují zejména

a) práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role,
b) postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů,
c) postupy pro sledování kybernetických bezpečnostních událostí a opatření pro ochranu přístupu k záznamům o těchto událostech,
d) pravidla a postupy pro ochranu před škodlivým kódem,
e) řízení technických zranitelností,
f) spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory,
g) postupy řízení a schvalování provozních změn,
h) postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů,
i) pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu,
j) pravidla a postupy pro instalaci technických aktiv,
k) provádění pravidelného zálohování a kontroly použitelnosti provedených záloh a
l) pravidla a postupy pro zajištění bezpečnosti síťových služeb.

(2) Orgán nebo osoba, která jsou povinny zavést bezpečnostní opatření podle zákona, v rámci řízení provozu a komunikací dodržují pravidla a postupy stanovené podle odstavce 1. Tato pravidla a postupy aktualizují v souvislosti s prováděnými nebo plánovanými změnami.

(3) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, zajistí oddělení vývojového, testovacího a provozního prostředí.

Celex 32016L1148

§ 11

Řízení změn

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v rámci řízení změn u informačního a komunikačního systému

a) přezkoumávají možné dopady změn a
b) určují významné změny.

(2) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, u významných změn

a) dokumentují jejich řízení,

b) provádí analýzu rizik,
c) přijímají opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami,
d) aktualizují bezpečnostní politiky a bezpečnostní dokumentaci,
e) zajistí jejich testování a
f) zajistí případné navrácení změn do původního stavu.

(3) Orgán nebo osoba uvedené v § 3 písm. c), d) a f) zákona na základě výsledků analýzy rizik podle odstavce 2 písm. b) rozhodnou o provedení penetračního testování nebo testování zranitelností; pokud rozhodnou o provedení penetračního testování nebo testování zranitelností, postupují podle § 25 odst. 1 a reagují na zjištěné nedostatky.

(4) Orgán nebo osoba uvedená v § 3 písm. e) zákona se řídí požadavky podle odstavce 3 přiměřeně.

Celex 32016L1148

§ 12

Řízení přístupu

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, na základě provozních a bezpečnostních potřeb řídí přístup k informačnímu a komunikačnímu systému a přijímají opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení podle § 19 a 20, a která brání ve zneužití těchto údajů neoprávněnou osobou.

(2) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, dále v rámci řízení přístupu k informačnímu a komunikačnímu systému

a) řídí přístup na základě skupin a rolí,
b) přidělí každému uživateli a administrátorovi přistupujícímu k informačnímu a komunikačnímu systému přístupová práva a oprávnění a jedinečný identifikátor,
c) řídí identifikátory, přístupová práva a oprávnění aplikací a technických účtů,
d) zavádějí bezpečnostní opatření pro řízení přístupu zařízení k prostředkům informačního a komunikačního systému,
e) zavádějí bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných technických zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, která orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, nemají ve své správě,
f) omezí přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce,
g) omezí a kontrolují používání programových nástrojů, které mohou být schopné překonat systémové nebo aplikační kontroly,
h) přidělují a odebírají přístupová oprávnění v souladu s politikou řízení přístupu,
i) provádí pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí,

j) využívají nástroj pro správu a ověřování identity uživatelů podle § 19 a nástroj pro řízení přístupových oprávnění podle § 20,
k) prosazují, aby uživatelé při používání privátních autentizačních informací dodržovali stanovené postupy,
l) zajistí odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role,
m) zajistí odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu a
n) dokumentují přidělování a odebírání přístupových oprávnění.

Celex 32016L1148

§ 13

Akvizice, vývoj a údržba

Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému

a) řídí rizika podle § 5,
b) řídí významné změny podle § 11,
c) stanoví bezpečnostní požadavky,
d) zahrnou bezpečnostní požadavky do projektu akvizice, vývoje a údržby,
e) zajistí bezpečnost vývojového a testovacího prostředí a zajistí ochranu používaných testovacích dat,
f) provádí bezpečnostní testování významných změn před jejich zavedením do provozu a
g) plní požadavek podle § 19 odst. 3, je-li cílem provedení akvizice nebo vývoje nástroj pro správu a ověřování identity.

Celex 32016L1148

§ 14

Zvládání kybernetických bezpečnostních událostí a incidentů

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v rámci zvládání kybernetických bezpečnostních událostí a incidentů

a) zavedou proces detekce a vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů,
b) přidělí odpovědnosti a stanoví postupy pro
   1. průběžnou detekci a vyhodnocování kybernetických bezpečnostních událostí a incidentů a
   2. pro koordinaci a zvládání kybernetických bezpečnostních incidentů,
c) definují a aplikují postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu,
d) zajistí detekci kybernetických bezpečnostních událostí,
e) při detekci kybernetických bezpečnostních událostí se dále řídí podle § 22 a 23,
f) zajistí, že uživatelé, administrátoři, bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti bezpečnosti informací,

g) zajistí posuzování kybernetických bezpečnostních událostí, v rámci kterého musí být rozhodnuto, zda mají být klasifikovány jako kybernetické bezpečnostní incidenty podle § 31,
h) zajistí zvládání kybernetických bezpečnostních incidentů podle stanovených postupů,
i) přijímají opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,
j) hlásí kybernetické bezpečnostní incidenty podle § 32,
k) vedou záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání,
l) prošetří a určí příčiny kybernetického bezpečnostního incidentu a
m) vyhodnotí účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanoví nutná bezpečnostní opatření, popřípadě aktualizují stávající bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.

(2) Orgán nebo osoba uvedené v § 3 písm. c), d), f) a g) zákona při detekci kybernetických bezpečnostních událostí dále používají nástroje podle § 24.

Celex 32016L1148

§ 15

Řízení kontinuity činností

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v rámci řízení kontinuity činností

a) stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,
b) pomocí hodnocení rizik a analýzy dopadů vyhodnotí a dokumentují možné dopady kybernetických bezpečnostních incidentů a posoudí možná rizika související s ohrožením kontinuity činností,
c) na základě výstupů hodnocení rizik a analýzy dopadů podle písmene b) stanoví cíle řízení kontinuity činností formou určení
   1. minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému,
   2. doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému, a
   3. doby obnovení dat jako časového okamžiku, ke kterému musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,
d) stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c),
e) vypracují, aktualizují a pravidelně testují plány kontinuity činností související s provozováním informačního a komunikačního systému a souvisejících služeb a
f) realizují opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti a vychází při tom z požadavků podle § 27.

Celex 32016L1148

§ 16

Audit kybernetické bezpečnosti

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v rámci auditu kybernetické bezpečnosti

a) provádí a dokumentují audit dodržování bezpečnostní politiky, včetně přezkoumání technické shody, a výsledky auditu zohlední v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik a
b) posuzují soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému a určí případná nápravná opatření pro zajištění souladu.

(2) Audit podle odstavce 1 je prováděn

a) přiměřeně při významných změnách,
b) v pravidelných intervalech alespoň po 3 letech v případě orgánu nebo osoby uvedených v § 3 písm. e) zákona a
c) v pravidelných intervalech alespoň po 2 letech v případě orgánu nebo osoby, které nejsou uvedeny v písmenu b).

(3) Není-li v odůvodněných případech možné provést audit v intervalech podle odstavce 2 písm. b) a c) v celém rozsahu, je možné audit provádět průběžně po systematických celcích.

(4) Audit kybernetické bezpečnosti musí být prováděn osobou vyhovující podmínkám stanoveným v § 7 odst. 4, která nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření.

(5) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona a jsou současně provozovatelem informačního a komunikačního systému, předkládají výsledky auditu kybernetické bezpečnosti správci daného informačního a komunikačního systému.
Celex 32016L1148

HLAVA II
TECHNICKÁ OPATŘENÍ

§ 17
Fyzická bezpečnost

Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v rámci fyzické bezpečnosti

a) předchází poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního a komunikačního systému,
b) stanoví fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému, a
c) u fyzického bezpečnostního perimetru stanoveného podle písmene b) přijmou nezbytná opatření a uplatňují prostředky fyzické bezpečnosti
   1. k zamezení neoprávněnému vstupu,
   2. k zamezení poškození a neoprávněným zásahům a
   3. pro zajištění ochrany na úrovni objektů a v rámci objektů.

Celex 32016L1148

§ 18

Bezpečnost komunikačních sítí

Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, pro ochranu bezpečnosti komunikační sítě zahrnuté v rozsahu systému řízení bezpečnosti informací podle § 3 odst. 1 písm. d)

a) zajistí segmentaci komunikační sítě,
b) zajistí řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě,
c) pomocí kryptografie zajistí důvěrnost a integritu pro vzdálený přístup, vzdálenou správu nebo pro přístup do komunikační sítě pomocí bezdrátových technologií,
d) aktivně blokují nežádoucí komunikaci a
e) pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty využívají nástroj, který zajistí ochranu integrity komunikační sítě.

Celex 32016L1148

§ 19

Správa a ověřování identit

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, používají nástroje pro správu a ověření identity uživatelů, administrátorů a aplikací informačního a komunikačního systému.

(2) Nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací zajišťuje

a) ověření identity před zahájením aktivit v informačním a komunikačním systému,
b) řízení počtu možných neúspěšných pokusů o přihlášení,
c) odolnost uložených nebo přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití,
d) ukládání autentizačních údajů ve formě odolné proti offline útokům,
e) opětovné ověření identity po určené době nečinnosti,
f) dodržení důvěrnosti autentizačních údajů při obnově přístupu a
g) centralizovanou správu identit.

(3) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, pro ověření identity uživatelů, administrátorů a aplikací využívají autentizační mechanizmus, který není založený pouze na použití identifikátoru účtu a hesla, nýbrž na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů.

(4) V případě, kdy není možné splnit požadavek podle odstavce 3, musí nástroj pro ověření identity uživatelů, administrátorů a aplikací, který používá autentizaci pomocí kryptografických klíčů, zaručit obdobnou úroveň bezpečnosti.

(5) V případě, kdy není možné splnit požadavek podle odstavců 3 nebo 4, musí nástroj pro ověřování identity uživatelů, administrátorů a aplikací, který používá k autentizaci identifikátor účtu a heslo, vynucovat pravidla

a) minimální délky hesla
   1. 14 znaků u uživatelů a
   2. 17 znaků u administrátorů a aplikací,
b) umožňující zadat heslo o délce alespoň 64 znaků,
c) která neomezují použití malých a velkých písmen, číslic a speciálních znaků,
d) umožňující uživatelům změnu hesla, přičemž nesmí být povoleno více změn hesla během stanoveného období,
e) neumožňující uživatelům a administrátorům
   1. zvolit si nejčastěji používaná hesla,
   2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem a
   3. opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel s ohledem na písmeno d),
f) kontroly vzorů hesel při tvorbě nových nebo při změně hesel a
g) pro povinnou změnu hesla v intervalu maximálně po 18 měsících, přičemž toto pravidlo se nevztahuje na účty sloužící k obnově systému v případě havárie.

(6) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v případě používání autentizace pouze účtem a heslem dále

a) vynutí bezodkladnou změnu výchozího hesla po jeho prvním použití,
b) vynutí bezodkladné zneplatnění hesla sloužícího k obnovení přístupu po jeho prvním použití nebo uplynutím nejvýše 60 minut od jeho vytvoření a
c) povinně zahrnou pravidla tvorby bezpečných hesel do plánu rozvoje bezpečnostního povědomí podle § 6.

Celex 32016L1148

§ 20

Řízení přístupových oprávnění

Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, používají centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění

a) pro přístup k jednotlivým aktivům informačního a komunikačního systému a
b) pro čtení dat, zápis dat a změnu oprávnění.

Celex 32016L1148

§ 21

Ochrana před škodlivým kódem

(1) Orgán nebo osoba uvedené v § 3 písm. c), d) a f) zákona v rámci ochrany před škodlivým kódem

a) zajišťují použití nástroje pro nepřetržitou automatickou ochranu
   1. koncových stanic,
   2. mobilních zařízení,
   3. serverů,
   4. datových úložišť a výměnných datových nosičů,
   5. komunikační sítě a prvků komunikační sítě a
   6. obdobných zařízení,
b) monitorují a řídí používání výměnných zařízení a datových nosičů,
c) řídí automatické spouštění obsahu výměnných zařízení a datových nosičů,
d) řídí oprávnění ke spouštění kódu a
e) provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem.

(2) Orgán nebo osoba uvedené v § 3 písm. e) zákona použijí odstavec 1 přiměřeně.

Celex 32016L1148

§ 22

Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona,

a) zaznamenávají bezpečnostní a provozní události důležitých aktiv informačního a komunikačního systému a
b) na základě hodnocení důležitosti aktiv aktualizují rozsah aktiv, u kterých je zaznamenávání bezpečnostních a provozních událostí prováděno.

(2) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, pro zaznamenávání bezpečnostních a provozních událostí podle odstavce 1 zajišťují

a) sběr informací o bezpečnostních a provozních událostech; zejména zaznamenává
   1. datum a čas včetně specifikace časového pásma,
   2. typ činnosti,
   3. identifikaci technického aktiva, které činnost zaznamenalo,
   4. jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,
   5. jednoznačnou síťovou identifikaci zařízení původce a
   6. úspěšnost nebo neúspěšnost činnosti,
b) jednoznačnou síťovou identifikaci původce, je-li v komunikační síti použit nástroj, který mění jeho síťovou identifikaci,
c) ochranu informací získaných podle písmen a) a b) před neoprávněným čtením a jakoukoli změnou,
d) zaznamenávání
   1. přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,

2. činností provedených administrátory,
3. úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
4. neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
5. činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,
6. zahájení a ukončení činností technických aktiv,
7. kritických i chybových hlášení technických aktiv a
8. přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí,

e) synchronizaci jednotného času technických aktiv patřících do informačního a komunikačního systému nejméně jednou za 24 hodin.

(3) Orgán nebo osoba uvedené v § 3 písm. c), d) a f) zákona uchovávají záznamy událostí podle odstavce 2 nejméně po dobu 24 měsíců.

(4) Orgán nebo osoba uvedené v § 3 písm. e) zákona uchovávají záznamy událostí zaznamenané podle odstavce 2 nejméně po dobu 12 měsíců.

Celex 32016L1148

§ 23

Detekce kybernetických bezpečnostních událostí

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, v rámci komunikační sítě, jejíž součástí je informační a komunikační systém, používají nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí

a) ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi,
b) ověření a kontrolu přenášených dat na perimetru komunikační sítě a
c) blokování nežádoucí komunikace.

(2) Orgán nebo osoba uvedené v § 3 písm. c), d) a f) zákona zajistí detekci kybernetických bezpečnostních událostí v rámci

a) koncových stanic,
b) mobilních zařízení,
c) serverů,
d) datových úložišť a výměnných datových nosičů,
e) síťových aktivních prvků a
f) obdobných aktiv.

Celex 32016L1148

§ 24

Sběr a vyhodnocování kybernetických bezpečnostních událostí

Orgán nebo osoba uvedené v § 3 písm. c), d) a f) zákona používají nástroj pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí, který umožní

a) sběr a vyhodnocování událostí zaznamenaných podle § 22 a 23,
b) vyhledávání a seskupování souvisejících záznamů,
c) poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech,
d) nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí,
e) omezení případů nesprávného vyhodnocení událostí pravidelnou aktualizací nastavení pravidel pro
   1. vyhodnocování kybernetických bezpečnostních událostí a
   2. včasné varování,
f) využívání informací získaných nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.

Celex 32016L1148

§ 25

Aplikační bezpečnost

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, provádí penetrační testy informačního a komunikačního systému se zaměřením na důležitá aktiva, a to

a) před jejich uvedením do provozu a
b) v souvislosti s významnou změnou podle § 11 odst. 3.

(2) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, dále v rámci aplikační bezpečnosti zajistí trvalou ochranu aplikací, informací a transakcí před

a) neoprávněnou činností a
b) popřením provedených činností.

Celex 32016L1148

§ 26

Kryptografické prostředky

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, pro ochranu aktiv informačního a komunikačního systému

a) používají aktuálně odolné kryptografické algoritmy a kryptografické klíče,
b) používají systém správy klíčů a certifikátů, který
   1. zajistí generování, distribuci, ukládání, archivaci, změny, omezení platnosti, revokaci certifikátů a likvidaci klíčů a
   2. umožní kontrolu a audit,
c) prosazují bezpečné nakládání s kryptografickými prostředky,
d) zohledňují doporučení v oblasti kryptografických prostředků vydaná Úřadem, zveřejněná na jeho internetových stránkách.

Celex 32016L1148

§ 27

Zajišťování úrovně dostupnosti informací

Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, zavedou opatření pro zajišťování úrovně dostupnosti, kterými zajistí

a) dostupnost informačního a komunikačního systému pro splnění cílů podle § 15,
b) odolnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost,
c) dostupnost důležitých technických aktiv informačního a komunikačního systému a
d) redundanci aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému.

Celex 32016L1148

§ 28

Průmyslové, řídící a obdobné specifické systémy

Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, pro bezpečnost průmyslových a řídících systémů dále používají nástroje a opatření, které zajistí

a) použití technických a programových prostředků, které jsou určeny do specifického prostředí,
b) omezení fyzického přístupu k zařízením průmyslových a řídících systémů a ke komunikační síti,
c) vyčlenění komunikační sítě určené pro průmyslové a řídící systémy od ostatní infrastruktury,
d) omezení a řízení vzdáleného přístupu k průmyslovým a řídícím systémům,
e) ochranu jednotlivých technických aktiv průmyslových a řídících systémů před využitím známých zranitelností a
f) obnovení chodu průmyslových a řídících systémů po kybernetickém bezpečnostním incidentu.

Celex 32016L1148

§ 29

Digitální služby

(1) Orgán nebo osoba uvedené v § 3 písm. h) zákona zavedou bezpečnostní opatření podle prováděcího nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný.

(2) Orgán nebo osoba uvedené v § 3 písm. h) zákona hlásí kontaktní údaje podle § 34 odst. 2.

(3) Orgán nebo osoba uvedené v § 3 písm. h) zákona hlásí kybernetické bezpečnostní incidenty podle § 32 odst. 2 a 3.

Celex 32016L1148

HLAVA III

BEZPEČNOSTNÍ POLITIKA A BEZPEČNOSTNÍ DOKUMENTACE

§ 30

Bezpečnostní politika a bezpečnostní dokumentace

(1) Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona,

a) stanoví bezpečnostní politiku a vedou bezpečnostní dokumentaci, které obsahově pokryjí oblasti upravené touto vyhláškou,
b) pravidelně přezkoumávají bezpečnostní politiku a bezpečnostní dokumentaci a
c) zajistí, aby byla bezpečnostní politika a bezpečnostní dokumentace aktuální.

(2) Bezpečnostní politika a bezpečnostní dokumentace musí být

a) dostupné v listinné nebo elektronické podobě,
b) komunikovány v rámci orgánu nebo osoby,
c) přiměřeně dostupné dotčeným stranám,
d) řízeny,
e) chráněny z pohledu důvěrnosti, integrity a dostupnosti a
f) vedeny tak, aby informace v nich obsažené byly úplné, čitelné, snadno identifikovatelné a snadno vyhledatelné.

(3) Doporučený obsah bezpečnostní politiky a bezpečnostní dokumentace je uveden v příloze č. 5.

ČÁST TŘETÍ
KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT

§ 31

Kategorizace kybernetických bezpečnostních incidentů

(1) Kategorizace jednotlivých kybernetických bezpečnostních incidentů zohlední

a) způsobené škody,
b) důležitost dotčených aktiv informačního a komunikačního systému,
c) dopady na poskytované služby informačního a komunikačního systému,
d) dopady na služby poskytované jinými informačními a komunikačními systémy a
e) předpokládané škody a další dopady.

(2) Pro potřeby hlášení a zvládání kybernetických bezpečnostních incidentů se na základě zohlednění podle odstavce 1 kybernetické bezpečnostní incidenty zařadí do následujících kategorií

a) Kategorie III – velmi závažný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod,
b) Kategorie II – závažný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí

být vhodnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod, nebo

c) Kategorie I – méně závažný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

(3) Typy kybernetických bezpečnostních incidentů podle dopadu jsou

a) kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv,
b) kybernetický bezpečnostní incident způsobující narušení integrity aktiv,
c) kybernetický bezpečnostní incident způsobující narušení dostupnosti aktiv, nebo
d) kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených v písmenech a) až c).

Celex 32016L1148

§ 32

Forma a náležitosti hlášení kybernetických bezpečnostních incidentů

(1) Kybernetický bezpečnostní incident se Úřadu v elektronické podobě hlásí prostřednictvím

a) elektronického formuláře zveřejněného na internetových stránkách Úřadu,
b) e-mailu na adresu elektronické pošty Úřadu určené pro příjem hlášení kybernetických bezpečnostních incidentů, zveřejněného na internetových stránkách Úřadu,
c) datové zprávy do datové schránky Úřadu, nebo
d) určeného datového rozhraní (pokud je používáno), jehož popis je zveřejněn na internetových stránkách Úřadu.

(2) Kybernetický bezpečnostní incident se provozovateli národního CERT v elektronické podobě hlásí formou uvedenou na internetových stránkách provozovatele národního CERT.

(3) Hlášení kybernetického bezpečnostního incidentu je možné zaslat i v listinné podobě, avšak pouze v případech, kdy nelze využít žádný ze způsobů uvedených v odstavcích 1 a 2.

(4) Náležitosti hlášení kybernetického bezpečnostního incidentu jsou v aktuální podobě uvedeny na internetových stránkách Úřadu.

Celex 32016L1148

ČÁST ČTVRTÁ
REAKTIVNÍ OPATŘENÍ A KONTAKTNÍ ÚDAJE

§ 33

Reaktivní opatření

(1) Orgán nebo osoba, kterým Úřad uložil provést reaktivní opatření,

a) posoudí očekávané dopady reaktivního opatření na informační a komunikační systém a na zavedená bezpečnostní opatření a vyhodnotí možné negativní účinky a
b) stanoví způsob rychlého provedení tohoto opatření, který minimalizuje jeho možné negativní účinky, a určí časový plán jeho provedení.

(2) Orgán nebo osoba, kterým Úřad uložil provést reaktivní opatření, oznámí s ohledem na odstavec 1 způsob provedení reaktivního opatření a jeho výsledek ve formě uvedené na internetových stránkách Úřadu.

§ 34

Kontaktní údaje

(1) Kontaktní údaje se Úřadu v elektronické podobě hlásí prostřednictvím

a) elektronického formuláře zveřejněného na internetových stránkách Úřadu,
b) e-mailu na adresu elektronické pošty Úřadu určenou pro příjem hlášení kybernetických bezpečnostních incidentů, zveřejněnou na internetových stránkách Úřadu,
c) datové zprávy do datové schránky Úřadu, nebo
d) určeného datového rozhraní (pokud je používáno), jehož popis je zveřejněn na internetových stránkách Úřadu.

(2) Kontaktní údaje se provozovateli národního CERT hlásí formou uvedenou na internetových stránkách provozovatele národního CERT.

(3) Hlášení kontaktních údajů je možné zaslat i v listinné podobě, avšak pouze v případech, kdy nelze využít žádný ze způsobů uvedených v odstavci 1 a 2.

(4) Náležitosti hlášení kontaktních údajů jsou v aktuální podobě uvedeny na internetových stránkách Úřadu.

(5) Orgán nebo osoba uvedené v § 3 písm. c) až f) zákona, které jsou provozovatelem, dále k hlášení kontaktních údajů podle odstavce 1 přikládají dokument, kterým je správce prokazatelně informuje podle § 8 odst. 1 písm. c).

ČÁST PÁTÁ
ZÁVĚREČNÁ USTANOVENÍ

§ 35

Zrušovací ustanovení

Zrušuje se vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

§ 36

Účinnost

Tato vyhláška nabývá účinnosti dnem 10. května 2018.

Celex 32016L1148

Příloha č. 1 k vyhlášce č. .../2018 Sb.

Hodnocení aktiv

Pro hodnocení důležitosti aktiv jsou v tomto případě použity stupnice o čtyřech úrovních a posuzuje se, jaký dopad by mělo narušení bezpečnosti informací u jednotlivých aktiv. Orgán nebo osoba uvedené v § 3 písm. c) až g) zákona mohou používat odlišný počet úrovní pro hodnocení důležitosti aktiv, než jaký je uveden v této příloze, dodrží-li jednoznačné vazby mezi jimi používaným způsobem hodnocení důležitosti aktiv a stupnicemi a úrovněmi pro hodnocení důležitosti aktiv, které jsou uvedeny v této příloze.

Je doporučeno, aby si každý orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, tyto dopadové matice přizpůsobily svým potřebám.

Stupnice pro hodnocení důvěrnosti

Úroveň	**Popis**	**Příklady požadavků na ochranu aktiva**
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy orgánu nebo osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:WHITE.	Není vyžadována žádná ochrana. Likvidace/mazání aktiva na úrovni Nízká - viz příloha č. 4.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how orgánu nebo osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. Likvidace/mazání aktiva na úrovni Střední- viz příloha č. 4.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství, citlivé osobní údaje).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Vysoká - viz příloha č. 4.

	V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER.	
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. strategické obchodní tajemství, citlivé osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Kritická - viz příloha č. 4.

Stupnice pro hodnocení integrity

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy orgánu nebo osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů orgánu nebo osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (např. omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů orgánu nebo osoby s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů orgánu nebo osoby s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. pomocí technologie digitálního podpisu).

Stupnice pro hodnocení dostupnosti

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů orgánu nebo osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů orgánu nebo osoby. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů orgánu nebo osoby. Aktiva jsou považována jako kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Příloha č. 2 k vyhlášce č. .../2018 Sb.

Hodnocení rizik

Jednoznačné stanovení funkce pro určení rizika je nezbytnou součástí metodiky pro hodnocení rizik podle § 5.

Hodnota rizika je nejčastěji vyjádřena jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost.

Pro hodnocení rizik lze použít například tuto funkci:

Riziko = dopad (odvozený z hodnocení aktiv podle přílohy č. 1) × hrozba × zranitelnost.

Dopad je v tomto případě odvozen z hodnocení aktiv podle přílohy č. 1.

V případě, že orgán nebo osoba uvedené v § 3 písm. c) až g) zákona využívají metodu pro hodnocení rizik, která nerozlišuje hodnocení hrozby a zranitelnosti, je možné stupnice pro hodnocení hrozeb a zranitelností sloučit. Sloučení stupnic by nemělo vést ke ztrátě schopnosti rozlišení úrovně hrozby a zranitelnosti. Za tímto účelem lze použít například komentář, který zřetelně vyjádří jak úroveň hrozby, tak i úroveň zranitelnosti. Obdobně se postupuje i v případech, kdy orgán nebo osoba používá jiný počet úrovní pro hodnocení dopadů, hrozeb, zranitelností a rizik.

Stupnice pro hodnocení hrozeb

Úroveň	**Popis**
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Stupnice pro hodnocení zranitelností

Úroveň	Popis
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Stupnice pro hodnocení rizik

Úroveň	Popis
Nízké	Riziko je považováno za akceptovatelné.
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
Vysoké	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritické	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

Příloha č. 3 k vyhlášce č. .../2018 Sb.

Zranitelnosti a hrozby

Upozornění: Tato příloha obsahuje jen vybrané kategorie zranitelností a hrozeb. Identifikace konkrétních zranitelností a hrozeb je v odpovědnosti orgánů a osob uvedených v § 3 písm. c) až g) zákona.

Zranitelnosti

1. nedostatečná údržba informačního a komunikačního systému,
2. zastaralost informačního a komunikačního systému,
3. nedostatečná ochrana vnějšího perimetru,
4. nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
5. nedostatečná údržba informačního a komunikačního systému,
6. nevhodné nastavení přístupových oprávnění,
7. nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
8. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
9. nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
10. nedostatečná ochrana aktiv,
11. nevhodná bezpečnostní architektura,
12. nedostatečná míra nezávislé kontroly, nebo
13. neschopnost včasného odhalení pochybení ze strany zaměstnanců.

Hrozby

1. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
2. poškození nebo selhání technického anebo programového vybavení,
3. zneužití identity,
4. užívání programového vybavení v rozporu s licenčními podmínkami,
5. škodlivý kód (například viry, spyware, trojské koně),
6. narušení fyzické bezpečnosti,
7. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
8. zneužití nebo neoprávněná modifikace údajů,
9. ztráta, odcizení nebo poškození aktiva,
10. nedodržení smluvního závazku ze strany dodavatele,
11. pochybení ze strany zaměstnanců,
12. zneužití vnitřních prostředků, sabotáž,
13. dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,
14. nedostatek zaměstnanců s potřebnou odbornou úrovní,
15. cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
16. zneužití vyměnitelných technických nosičů dat,
17. napadení elektronické komunikace (odposlech, modifikace).

Příloha č. 4 k vyhlášce č. .../2018 Sb.

Likvidace dat

Tato příloha popisuje možné způsoby mazání dat a likvidace technických nosičů informace, provozních údajů, informací a jejich kopií.

Jednotliví správci informačního a komunikačního systému si stanoví pravidla pro mazání dat a likvidaci technických nosičů dat. **Tím nesmí být dotčeny povinnosti podle jiných právních předpisů.**

Pozn.: Například u cloudových služeb je nutné zvolit adekvátní úroveň služby nabízející přiměřená bezpečnostní opatření, včetně adekvátních pravidel pro mazání dat a likvidaci technických nosičů dat, vzhledem k hodnotě a důležitosti aktiv.

Stanovená pravidla pro likvidaci dat by měla být stanovena přiměřeně hodnotě a důležitosti aktiv **a měla by zohledňovat:**

- **hodnotu aktiva (zejména z pohledu důvěrnosti),**
- **technologii (typy a velikost nosičů informace),**
- **zda se nosič informace nachází pod kontrolou organizace či nikoliv,**
- **zda jsou data součástí dedikovaného nebo multitenantního prostředí,**
- **kdo bude likvidaci dat provádět (interní zaměstnanec, nebo dodavatel),**
- **dostupnost vybavení a nástrojů pro likvidaci,**
- **kapacitu likvidovaných nosičů,**
- **zda je k dispozici vyškolený personál,**
- **časovou náročnost likvidace,**
- **cenu likvidace s ohledem na nástroje, školení, validaci, opětovné využití nosiče informace**
- **možné způsoby likvidace dat (například zničením nosiče, několikanásobným přepsáním nosiče dat, znečitelněním dat jejich šifrováním apod.).**
- **použitelné způsoby likvidace dat vzhledem ke stavu nosiče informace (např. při poškození zařízení nebude možné použít variantu přepisu informace, ale některý ze způsobu fyzické likvidace).**
- **apod.**

Způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií:

1) Odstranění

- Způsob likvidace spočívá v odstranění dat tak, aby byla pro systém nedostupná (například odstranění datového souboru, vyhození tištěného dokumentu do odpadu).
- Jde o nejméně bezpečný způsob likvidace dat. V případě získání nosiče informace je možné s vynaložením určitého úsilí informace obnovit.
- Tato metoda není použitelná pro nosiče digitálních dat neumožňující opětovný zápis.
- Použitelný způsob pro úroveň důvěrnosti aktiva: nízká.

2) Přepsání

- Způsob likvidace spočívá v přepsání chráněné informace nahodilými hodnotami.
- Jde o středně bezpečný způsob likvidace dat. Volně dostupné nástroje neumožňují obnovení přepsaných informací.
- Přepsání může být nahrazeno nebo kombinováno bezpečnou likvidací kryptografických klíčů k zašifrované informaci.
- Tato metoda není vhodná pro poškozená média, média neumožňující opětovný zápis, případně pro média s velkou kapacitou.
- Použitelný způsob pro úroveň důvěrnosti aktiva: nízká až kritická.

3) Fyzická likvidace nosiče informace

- Způsob likvidace spočívající ve zničení nosiče informace, popřípadě v rozebrání zařízení a následném zničení nosiče informace (mechanickým, chemickým či tepelným působením).
- Jde o nejbezpečnější metodu likvidace dat. Nosič informace po fyzické likvidaci nelze znovu použít pro původní účel. Původní informace není možné obnovit ani při vynaložení velkého množství prostředků a úsilí.
- Použitelný způsob likvidace pro úroveň důvěrnosti aktiva: střední až kritická.

Příklad možných způsobů likvidace podle úrovně důležitosti aktiva:

	Přípustný způsob likvidace podle úrovně důležitosti aktiva			
Nosič informace	**1. Nízká**	**2. Střední**	**3. Vysoká**	**4. Kritická**
Informace na lidsky čitelném nosiči (tištěné dokumenty, poznámky, vyřezávané vzkazy a podobně)	Odstranění: Vyhození do odpadu.	Přepsání: Začernění. ---------- Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje.	Fyzická likvidace: Znehodnocení nosiče informací použitím skartovacího stroje s podélným i příčným řezem, spálením nebo rozložením.	
Mobilní zařízení (mobilní telefony, PDA, tablety)	Odstranění: Vymazání informací, reset zařízení do továrního nastavení.	Přepsání: Pro zařízení s šifrovaným úložištěm - odstranění informací a reset do továrního nastavení.	Fyzická likvidace: Rozebrání zařízení a zničení nosiče informací.	
Síťová zařízení (router, switch, modem, apod.)	Odstranění: Vymazání informací, reset do továrního nastavení.	Přepsání: Odstranění + zahlcení umělými událostmi (umělý síťový provoz, testovací tiskové úlohy apod.).		
Kancelářské vybavení (scanery, tiskárny, fax)				
Magnetická média (magnetické pásky, disky, HDD)	Odstranění: Smazání dat na úrovni souborového systému.	Přepsání: Přepsání dat. V případě šifrovaného média je alternativou bezpečná likvidace		
Optická média (CD, DVD, HD-			Fyzická likvidace:	

DVD, BLU-RAY) **Elektronická média (flash paměti)**		kryptografických klíčů --- Fyzická likvidace.	Zničení nosiče informací.	
Outsourcing a cloud	Přípustný způsob likvidace dat by měl být stanoven smluvním ujednáním.			
	Odstranění: Odstranění všech souborů včetně předchozích verzí.	Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů. --- -- Alternativně v případě dedikovaného paměťového média je možné data po ukončení služby přepsat.	Přepsání: Použití šifrování datových úložišť na úrovni paměťového média a bezpečná likvidace kryptografických klíčů uložených v certifikovaném HSM (např. podle FIPS 140-2 Level 2) řízená zákazníkem. Při ukončení služby bude zlikvidován vrchní přístupový klíč a data jsou přepsána.	Přepsání/fyzická likvidace: Použit způsob viz úroveň “3. Vysoká” nebo použita dedikovaná paměťová kapacita úložiště. Při ukončení služby provedena celková sanitizace všech použitých paměťových médií dle výše uvedených řádků pro úroveň kritická.

Příloha č. 5 k vyhlášce č. ……. Sb.

Obsah bezpečnostních politik a bezpečnostní dokumentace

1. Bezpečnostní politiky

1.1. Politika systému řízení bezpečnosti informací

a) Cíle, principy a potřeby řízení bezpečnosti informací.
b) Deklarace vrcholového vedení o vůdčí roli a závazku k řešení systému řízení bezpečnosti informací.
c) Rozsah a hranice systému řízení bezpečnosti informací.
d) Pravidla a postupy pro řízení dokumentace.
e) Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací.
f) Pravidla a postupy pro provádění auditů kybernetické bezpečnosti.
g) Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací.
h) Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.

1.2. Politika řízení aktiv

a) Identifikace, hodnocení a evidence primárních aktiv
    1. určení a evidence jednotlivých primárních aktiv včetně určení jejich garanta,
    2. hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti.
b) Identifikace, hodnocení a evidence podpůrných aktiv
    1. určení a evidence jednotlivých podpůrných aktiv včetně určení jejich garanta,
    2. určení vazeb mezi primárními a podpůrnými aktivy.
c) Pravidla ochrany jednotlivých úrovní aktiv
    1. způsoby rozlišování jednotlivých úrovní aktiv,
    2. pravidla pro manipulaci a evidenci aktiv podle úrovní aktiv,
    3. přípustné způsoby používání aktiv.
d) Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií.

1.3. Politika organizační bezpečnosti

a) Určení bezpečnostních rolí a jejich práv a povinností.
b) Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí.
c) Požadavky na oddělení výkonu bezpečnostních a provozních rolí.

1.4. Politika řízení dodavatelů

a) Pravidla a principy pro výběr dodavatelů.
b) Pravidla pro hodnocení rizik souvisejících s dodavateli.
c) Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.
d) Pravidla pro provádění kontroly zavedení bezpečnostních opatření.
e) Pravidla pro hodnocení dodavatelů.

1.5. Politika bezpečnosti lidských zdrojů

a) Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení
    1. způsoby a formy poučení uživatelů,
    2. způsoby a formy poučení garantů aktiv,
    3. způsoby a formy poučení administrátorů,

4. způsoby a formy poučení dalších osob zastávajících bezpečnostní role.

a) Bezpečnostní školení nových zaměstnanců.
b) Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací.
c) Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice
    1. vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu,
    2. změna přístupových oprávnění při změně pracovní pozice.

1.6 Politika řízení provozu a komunikací

a) Pravomoci a odpovědnosti spojené s bezpečným provozem.
b) Postupy bezpečného provozu.
c) Požadavky a standardy bezpečného provozu.
d) Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů.

1.7. Politika řízení přístupu

a) Princip minimálních oprávnění/potřeba znát (need to know).
b) Požadavky na řízení přístupu.
c) Životní cyklus řízení přístupu.
d) Řízení privilegovaných oprávnění.
e) Řízení přístupu pro mimořádné situace.
f) Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.

1.8. Politika bezpečného chování uživatelů

a) Pravidla pro bezpečné nakládání s aktivy.
b) Bezpečné použití přístupového hesla.
c) Bezpečné použití elektronické pošty a přístupu na internet.
d) Bezpečný vzdálený přístup.
e) Bezpečné chování na sociálních sítích.
f) Bezpečnost ve vztahu k mobilním zařízením.

1.9. Politika zálohování a obnovy

a) Požadavky na zálohování a obnovu.
b) Pravidla a postupy zálohování.
c) Pravidla bezpečného uložení záloh.
d) Pravidla a postupy obnovy.
e) Pravidla a postupy testování zálohování a obnovy.

1.10. Politika bezpečného předávání a výměny informací

a) Pravidla a postupy pro ochranu předávaných informací.
b) Způsoby ochrany elektronické výměny informací.
c) Pravidla pro využívání kryptografické ochrany.

1.11. Politika řízení technických zranitelností

a) Pravidla pro omezení instalace programového vybavení.
b) Pravidla a postupy vyhledávání opravných programových balíčků.
c) Pravidla a postupy testování oprav programového vybavení.
d) Pravidla a postupy nasazení oprav programového vybavení.

1.12. Politika bezpečného používání mobilních zařízení

a) Pravidla a postupy pro bezpečné používání mobilních zařízení.
b) Pravidla a postupy pro zajištění bezpečnosti zařízení, která orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, nemají ve své správě.

1.13. Politika akvizice, vývoje a údržby

a) Bezpečnostní požadavky pro akvizici, vývoj a údržbu.
b) Řízení zranitelností.
c) Politika poskytování a nabývání licencí programového vybavení a informací
    1. Pravidla a postupy nasazení programového vybavení a jeho evidence.
    2. Pravidla a postupy pro kontrolu dodržování licenčních podmínek.

1.14. Politika dlouhodobého ukládání a archivace informací

a) Pravidla a postupy archivace dokumentů a záznamů.
b) Ochrana archivovaných dokumentů a záznamů.
c) Politika přístupu k archivovaným dokumentům a záznamům.

1.15. Politika ochrany osobních údajů

a) Charakteristika zpracovávaných osobních údajů.
b) Popis přijatých a provedených organizačních opatření pro ochranu osobních údajů.
c) Popis přijatých a provedených technických opatření pro ochranu osobních údajů.

1.16. Politika fyzické bezpečnosti

a) Pravidla pro ochranu objektů.
b) Pravidla pro kontrolu vstupu osob.
c) Pravidla pro ochranu zařízení.
d) Detekce narušení fyzické bezpečnosti.

1.17. Politika bezpečnosti komunikační sítě

a) Pravidla a postupy pro zajištění bezpečnosti sítě.
b) Určení práv a povinností za bezpečný provoz sítě.
c) Pravidla a postupy pro řízení přístupů v rámci sítě.
d) Pravidla a postupy pro ochranu vzdáleného přístupu k síti.
e) Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů.

1.18. Politika ochrany před škodlivým kódem

a) Pravidla a postupy pro ochranu síťové komunikace.
b) Pravidla a postupy pro ochranu serverů a sdílených datových úložišť.
c) Pravidla a postupy pro ochranu pracovních stanic.

1.19. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

a) Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí.
b) Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události.
c) Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí.

1.20. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

a) Pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí.

b) Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí.
c) Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

1.21. Politika bezpečného používání kryptografické ochrany

a) Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu.
b) Pravidla kryptografické ochrany informací
    1. při přenosu po komunikačních sítích,
    2. při uložení na mobilní zařízení nebo vyměnitelný technický nosič dat.
c) Systém správy klíčů.

1.22. Politika řízení změn

a) Způsob a principy řízení významných změn v rámci orgánu nebo osoby, jejich procesech, informačních a komunikačních systémech.
b) Přezkoumávání dopadů významných změn.
c) Způsob vedení evidence a testování významných změn.

1.23. Politika zvládání kybernetických bezpečnostních incidentů

a) Definování kategorií kybernetického bezpečnostního incidentu.
b) Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů.
c) Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů.
d) Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti.
e) Evidence incidentů.

1.24. Politika řízení kontinuity činností

a) Práva a povinnosti zúčastněných osob.
b) Cíle řízení kontinuity činností
    1. minimální úroveň poskytovaných služeb,
    2. doba obnovení chodu,
    3. doba obnovení dat.
c) Politika řízení kontinuity činností pro naplnění cílů kontinuity.
d) Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik.
e) Určení a obsah potřebných plánů kontinuity a havarijních plánů.
f) Postupy pro realizaci opatření vydaných Úřadem.

2. Obsah bezpečnostní dokumentace

2.1. Zpráva z auditu kybernetické bezpečnosti

a) Cíle auditu kybernetické bezpečnosti.
b) Předmět auditu kybernetické bezpečnosti.
c) Kritéria auditu kybernetické bezpečnosti.
d) Identifikování týmu auditorů a osob, které se auditu kybernetické bezpečnosti zúčastnily.
e) Datum a místo, kde byly prováděny činnosti při auditu kybernetické bezpečnosti.
f) Zjištění z auditu kybernetické bezpečnosti.
g) Závěry auditu kybernetické bezpečnosti.

2.2. Zpráva z přezkoumání systému řízení bezpečnosti informací

a) Vyhodnocení opatření z předchozího přezkoumání systému řízení bezpečnosti informací.
b) Identifikace změn a okolností, které mohou mít vliv na systém řízení bezpečnosti informací.
c) Zpětná vazba o výkonnosti řízení bezpečnosti informací
    1. neshody a nápravná opatření,
    2. výsledky monitorování a měření,
    3. výsledky auditu,
    4. naplnění cílů systému řízení bezpečnosti informací.
d) Výsledky hodnocení rizik a stav plánu zvládání rizik.
e) Identifikace možností pro neustálé zlepšování.
f) Doporučení potřebných rozhodnutí, stanovení opatření a osob zajišťujících výkon jednotlivých činností.

2.3. Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik

a) Určení stupnice pro hodnocení primárních aktiv
    1. určení stupnice pro hodnocení úrovní důvěrnosti aktiv,
    2. určení stupnice pro hodnocení úrovní integrity aktiv,
    3. určení stupnice pro hodnocení úrovní dostupnosti aktiv.
b) Určení stupnice pro hodnocení rizik
    1. určení stupnice pro hodnocení úrovní dopadu,
    2. určení stupnice pro hodnocení úrovní hrozby,
    3. určení stupnice pro hodnocení úrovní zranitelnosti,
    4. určení stupnice pro hodnocení úrovní rizik,
c) Metody a přístupy pro zvládání rizik.
d) Způsoby schvalování akceptovatelných rizik.

2.4. Zpráva o hodnocení aktiv a rizik

a) Přehled primárních aktiv
    1. identifikace a popis primárních aktiv,
    2. určení garantů primárních aktiv,
    3. hodnocení primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti.
b) Přehled podpůrných aktiv
    1. identifikace a popis podpůrných aktiv,
    2. určení garantů podpůrných aktiv,
    3. určení vazeb mezi primárními a podpůrnými aktivy.
c) Hodnocení rizik
    1. posouzení možných dopadů na aktiva,
    2. hodnocení existujících hrozeb,
    3. hodnocení existujících zranitelností, hodnocení existujících opatření,
    4. stanovení úrovně rizika, porovnání této úrovně s kritérii pro akceptovatelnost rizik,
    5. určení a schválení akceptovatelných rizik.
d) Zvládání rizik
    1. návrh způsobu zvládání rizik,
    2. návrh opatření a jejich realizace.

2.5. Prohlášení o aplikovatelnosti

a) Přehled vyloučených bezpečnostních opatření požadovaných touto vyhláškou včetně zdůvodnění, proč nebyla aplikována.
b) Přehled zavedených bezpečnostních opatření včetně způsobu jejich implementace.

2.6. Plán zvládání rizik

a) Obsah a cíle vybraných bezpečnostních opatření pro zvládání rizik včetně vazby na konkrétní rizika.
b) Potřebné zdroje pro jednotlivá bezpečnostní opatření pro zvládání rizik.
c) Osoby zajišťující jednotlivá bezpečnostní opatření pro zvládání rizik.
d) Termíny zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.
e) Způsob realizace bezpečnostních opatření.
f) Způsoby hodnocení úspěšnosti zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.

2.7. Plán rozvoje bezpečnostního povědomí

a) Obsah a termíny poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role.
b) Obsah a termíny poučení nových zaměstnanců.
c) Přehledy, které obsahují předmět jednotlivých školení a seznam osob, které školení absolvovaly.
d) Formy a způsoby hodnocení plánu.

2.8. Evidence změn

a) Evidence životního cyklu významných změn.
b) Záznamy o změnách konfigurace podpůrných aktiv

2.9. Hlášené kontaktní údaje

a) Přehled hlášených kontaktních údajů.

2.10. Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků

a) Přehled obecně závazných právních předpisů.
b) Přehled vnitřních předpisů a jiných předpisů.
c) Přehled smluvních závazků.

2.11. Další doporučená dokumentace

a) Topologie infrastruktury.
b) Přehled síťových zařízení.

Příloha č. 6 k vyhlášce č. .../2018 Sb.

Výbor pro řízení kybernetické bezpečnosti a bezpečnostní role

Tato příloha obsahuje popis doporučených požadavků pro výbor pro řízení kybernetické bezpečnosti a bezpečnostní role uvedené v § 6 a 7.

Role:	**Výbor pro řízení kybernetické bezpečnosti**
Klíčové činnosti:	● Odpovědnost za celkové řízení a rozvoj kybernetické bezpečnosti v rámci orgánu nebo osoby ● Tvorba rámce kybernetické bezpečnosti, směrování a zásad kybernetické bezpečnosti orgánu nebo osoby (definování strategických cílů a směrování rozvoje v oblasti kybernetické bezpečnosti) ● Definice rolí a odpovědností v rámci systému řízení bezpečnosti informací ● Definice požadavků na podávání zpráv a kontrolu systému řízení bezpečnosti informací ● Kontrola aktuálního stavu kybernetické bezpečnosti v rámci orgánu nebo osoby a zjišťování, zda dochází k naplňování plánovaných cílů
Další podmínky:	● Člen výboru pro řízení kybernetické bezpečnosti by měl být alespoň: ○ Statutární zástupce orgánu nebo osoby nebo jeho zástupce ○ Manažer kybernetické bezpečnosti ● Členové výboru pro řízení kybernetické bezpečnosti se pravidelně scházejí, přičemž průběh a výstupy z jednání jsou uchovávány v listinné nebo elektronické podobě.

Role:	**Manažer kybernetické bezpečnosti**
Klíčové činnosti:	• Odpovědnost za řízení systému řízení bezpečnosti informací • Pravidelný reporting pro vrcholové vedení orgánu nebo osoby • Pravidelná komunikace s vrcholovým vedením orgánu nebo osoby • Předkládá výboru pro řízení kybernetické bezpečnosti Zprávu o hodnocení aktiv a rizik, Plán zvládání rizik a Prohlášení o aplikovatelnosti. • Poskytuje pokyny pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT • Komunikuje s GovCERT/CSIRT • Podílí se na procesu řízení rizik • Koordinuje řízení incidentů • Vyhodnocuje vhodnost a účinnost bezpečnostních opatření
Znalosti:	• Znalost norem řady ISO/IEC 27000 a obdobných norem z oblasti bezpečnosti a ICT • Znalosti v oblasti ICT (operační systémy, databáze, aplikace, datové sítě) s důrazem na jejich bezpečnost • Řízení rizik • Řízení kontinuity činností • Znalost relevantních právních a regulatorních požadavků, zejména zákona • Znalost kontextu orgánu nebo osoby
Zkušenosti:	• Zkušenost s prosazováním systému řízení bezpečnosti informací • Porozumění definicím rizik a rizikovým scénářům • Zkušenost s řízením rizik v rámci orgánu nebo osoby • Schopnost interpretovat výsledky řízení rizik a koordinovat zvládání rizik
Vzdělání a praxe:	• Alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo • úspěšně ukončené vysokoškolské vzdělání a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti
Relevantní certifikace:	Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP).
Další podmínky:	• Role není slučitelná s rolemi odpovědnými za provoz informačního a komunikačního systému a s dalšími provozními či řídícími rolemi. • Pro správný výkon této role je zapotřebí zajistit potřebné pravomoci, odpovědnost a rozpočet.

Role:	**Architekt kybernetické bezpečnosti**
Klíčové činnosti:	• Odpovědnost za návrh implementace bezpečnostních opatření • Zajišťování architektury bezpečnosti
Znalosti:	• Architektura informačních a komunikačních systémů a její navrhování • Hardwarové komponenty, nástroje a architektury • Operační systémy a software • Podnikové procesy a jejich integrace a závislost na ICT • Řízení bezpečnosti a rizik • Bezpečnost komunikací a sítí • Řízení identit a přístupů • Hodnocení a testování bezpečnosti • Bezpečnost provozu • Základní principy bezpečného vývoje softwaru • Integrace a závislosti ICT a obchodních procesů
Zkušenosti:	• Navrhování implementace bezpečnostních opatření • Navrhování architektury bezpečnosti se zaměřením na cíle a bezpečnost • Bezpečnost vývoje softwaru
Vzdělání a praxe:	• Alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo • úspěšně ukončené vysokoškolské vzdělání a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti
Relevantní certifikace:	Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified in Risk and Information Systems Control (CRISC), CompTIA Security +, Certified Information Security Manager (CISM).
Další podmínky:	• Role není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů

Role:	**Auditor kybernetické bezpečnosti**
Klíčové činnosti:	Provádění auditu kybernetické bezpečnosti
Znalosti:	• Metodologie a rámce auditu informační bezpečnosti • Procesy a postupy interního auditu • Role a funkce interního auditu • Proces auditování ICT bezpečnosti • Strategické a taktické řízení ICT • Akvizice, vývoj a nasazení ICT • Řízení provozu, údržby a služeb ICT • Ochrana aktiv • Hodnocení kybernetické bezpečnosti, metody testování a vzorkování • Relevantní právní předpisy • ICT bezpečnost
Zkušenosti:	• Plánování auditů informační nebo kybernetické bezpečnosti • Provádění auditů systému řízení kybernetické bezpečnosti/systému řízení bezpečnosti informací • Analyzování výsledků auditů • Psaní auditních závěrů, jejich prezentace a navrhování doporučení vedoucích k nápravě nálezů • Reporting stavu plnění zákonných požadavků • Provádění auditů se zaměřením na ICT a informační nebo kybernetickou bezpečnost
Vzdělání a praxe:	• Alespoň 3 roky praxe v oblasti auditu informační nebo kybernetické bezpečnosti, nebo • Úspěšně ukončené vysokoškolské vzdělání a alespoň 1 rok praxe v oblasti auditu informační nebo kybernetické bezpečnosti
Relevantní certifikace:	Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified in Risk and Information Systems Control (CRISC), Lead Auditor Information Security Management System (Lead Auditor ISMS).
Další podmínky:	• Role není slučitelná s rolemi: ○ výboru pro řízení kybernetické bezpečnosti ○ manažera kybernetické bezpečnosti, ○ architekta kybernetické bezpečnosti, ○ garanta aktiva • Role není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů

Role:	**Garant aktiva**
Klíčové činnosti:	• Odpovědnost za zajištění rozvoje, použití a bezpečnosti aktiva • Spolupráce s ostatními bezpečnostními rolemi
Znalosti:	• Dobrá znalost aktiva, jehož je garantem • Dobrá znalost interních bezpečnostních politik a metodik (např. Metodika pro hodnocení aktiv a rizik)

Příloha č. 7 k vyhlášce č. .../2018 Sb.

Řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy

Obsah smlouvy uzavírané s významnými dodavateli:

a) ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),
b) ustanovení o oprávnění užívat data,
c) ustanovení o autorství programového kódu, popřípadě o programových licencích,
d) ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),
e) ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi orgánem nebo osobou, které jsou povinny zavést bezpečnostní opatření podle zákona, a dodavatelem a nebudou v rozporu s požadavky orgánu nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona, na dodavatele,
f) povinnost dodavatele dodržovat bezpečnostní politiky v rámci systému řízení bezpečnosti informací orgánu nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona,
g) řízení změn,
h) přezkum smluv v pravidelné periodě,
i) soulad smluv s aktuálně účinnou legislativou,
j) povinnost dodavatele informovat orgán nebo osobu, které jsou povinny zavést bezpečnostní opatření podle zákona, o
    1. kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,
    2. bezpečnostních rizicích souvisejících s plněním smlouvy,
    3. významné změně kontroly nad tímto dodavatelem nebo změně kontroly nad zásadními aktivy využívanými tímto dodavatelem k plnění podle smlouvy se správcem,
k) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (např. přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat apod.),
l) řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci BCM),
m) formát předání dat, provozních údajů a informací po vyžádání správcem,
n) pravidla pro likvidaci dat,
o) právo orgánu nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona, jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy a
p) ustanovení o sankcích za porušení povinností.

Příloha 2

Dokumentace nástroje pro podporu průběhu auditu

Tento nástroj je prototypem aplikace na podporu auditu kybernetické bezpečnosti. Nástroj obsahuje demo data pro audit podle novely vyhlášky č. 316/2014 Sb. (VoKB) a zákona o kybernetické bezpečnosti č. 181/2014 Sb. (ZoKB)

Prvotní použití vyžaduje nastavení aplikace (menu nastavení). Základním krokem je nastavení všech potřebných kritérií. Změny v nastavení během používání nástroje může mít negativní dopad na další používání a funkce hodnocení.

OVLÁDACÍ PRVKY

Téměř v celé sekci nastavení se používají stejné ovládací prvky. Použita je následující sada ovládacích prvků:

- Nastavení výchozích hodnot (uložených demo dat)
- Vymazání registrů
- Zobrazení registru
- Vložení nového záznamu

Dále se používá tento grafický objekt:

- Odstranění záznamu

EXPORT / IMPORT

Exportovat lze všechna uložená dat. Před importem je vhodné zálohovat svá data. Nástroj Zničit všechna data odstraní všechna data v úložišti a nelze je obnovit. Vytvoření prázdných objektů připraví úložiště pro případ importu všech dat například při přemisťování či sdílení dat.

LICENCE

V nástroji se využívají následující rozšíření s vlastními licenčními podmínkami:

- Font Awesome 4.7
- jQuery 2.1.4. a jeho doplněk Accordion
- Google Fonts Nunito a Raleway

VERZE

Aktuální verze nástroje je 0.2.2.

KOMPATIBILITA, TESTOVÁNÍ A OMEZENÍ

Nástroj je vyvíjen a testován pro webový prohlížeč Google Chrome.

Omezením je nemožnost sdílení dat s více uživateli. Data se ukládají lokálně pomocí javascriptové funkce localStorage, která umožňuje uložení maximálně 10 MB dat.

Příloha 3

Dokumentace doplňku nástroje pro podporu průběhu auditu

Tento nástroj je prototypem aplikace na podporu řízení aktiv a rizik. Nástroj vychází z vyhlášky o kybernetické bezpečnosti (Vyhláška č. 316/2014 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti) a normy ISO 27005.

Prvotní použití vyžaduje nastavení aplikace (menu nastavení). Základním krokem je nastavení všech stupnic. Požadavkem správy stupnic v sekci nastavení vyžaduje postupné vkládání hodnot vždy od nejnižší po nejvyšší úroveň. Změny v nastavení během používání nástroje může mít negativní dopad na další používání a funkcí hodnocení. Doporučení k používání je vhodně stanovit stupnice v sekci nastavení a provést ověření.

Zásadní je nastavení metody výpočtu rizika. Na výběr jsou dvě možnosti. První možnost vychází z doporučení vyhlášky o kybernetické bezpečnosti (316/2014 Sb.) a druhá možnost je výpočet podle doporučení podle novelizované vyhlášky. Obě vyhlášky ponechávají uživatelům možnost volby, pro kterou rovnici výpočtu rizika se hodnotitelé rozhodnou.

OVLÁDACÍ PRVKY

Téměř v celé sekci nastavení, dále v sekcích správy hrozeb a správy zranitelností se používají stejné ovládací prvky nebo se nijak zásadně nemění. Použita je následující sada ovládacích prvků (v kontextových obměnách):

- Nastavení výchozích hodnot (uložených demo dat)
- Vymazání registrů
- Zobrazení uloženého číselníku
- Vložení nového záznamu

Dále se používají tyto grafické objekty:

- Editace položek a přidávání nových záznamů
- Odstranění záznamu

Barevnost, která určuje úplnost hodnocení nebo míru rizika:

- Neznámé hodnocení / riziko
- Záznam je kompletní; nízká úroveň rizika
- Záznam je částečně kompletní; střední úroveň rizika
- Záznam není kompletní; vysoká úroveň rizika

OVLÁDÁNÍ

Princip používání nástroje je založen na definování číselníků a používání jejich hodnot prostřednictvím formulářů. Nástroj při každé interakci načítá aktuální dostupnou kolekci dat. Díle umožňuje souběžné procházení obsahu z celého menu bez přerušení rozpracovaných činností, a to až do chvíle znovunačtení stránky nebo jiné akce. Nástroj nevyužívá funkce prohlížeče "Zpět" a "Další".

HODNOCENÍ

Správa a hodnocení aktiv zajišťuje celou agendu evidence aktiv a zároveň lze aktivum ohodnotit. Hodnocení aktiv využívá data z menu nastavení. Aktivum je hodnoceno z pohledu důvěrnosti, dostupnosti a integrity. Význam tohoto hodnocení se liší podle zvoleného způsobu výpočtu rizika. Tato odlišnost má původ v interpretaci výpočtu rizika v obou vyhláškách o kybernetické bezpečnosti, podle kterých je tento nástroj navržen. Nástroj pracuje s hodnotou rizika podle zvoleného způsobu výpočtu stejně. Rozdílná je skutečná hodnota rizika.

Kontrolu splnění všech podmínek a náležitostí správy aktiv a jejich hodnocení, pro potřeby řízení rizik, lze ověřit tlačítkem Kontrola stavu. Tímto krokem se ověří poslední uložené sestavy hodnocení aktiv. Každé hodnocení je nutné pojmenovat. Zároveň se opatří datumem pro možnost pozdějšího srovnání. Z nabídky Uložená hodnocení lze zvolit, se kterým hodnocením bude nástroj dále pracovat. Zvolená sada dat hodnocení se zobrazí formou tabulky. Zobrazená tabulka se řídí nastavenou hodnotou výpočtu rizika.

Pro hodnocení rizika podle rovnice výpočtu Riziko = dopad × hrozba × zranitelnost je výsledným rizikem hodnota ve sloupci Riziko a hodnota sloupce Celkové riziko jen promítá hodnotu aktiva v souvislosti s rizikem. Podle rovnice výpočtu Riziko = dopad (odvozený z hodnocení aktiv) × hrozba × zranitelnost se ve sloupci Riziko zobrazí pomocný výpočet rizika (v tomto pojetí se jedná více o míru pravděpodobnosti), ale skutečná hodnota rizika je zobrazena ve sloupci Celkové riziko. Uvedené odlišnosti hodnocení rizika se projevují také v Mapě rizik.

V sekci hodnocení rizik se určuje míra rizika prostřednictvím nastavených hodnot ze sekce správy a hodnocení aktiv. Hodnocení rizik využívá jako vstup proces hodnocení aktiv a číselníky ze sekce nastavení. Výběr hodnoty pro ohodnocení rizika se provádí kliknutím na položku v tabulce. Zobrazení mapy rizik pro konkrétní zranitelnost lze zobrazit kliknutím na buňku v tabulky s názvem zranitelnosti. Srovnání jednotlivých hodnocení lze zobrazit klinutím na název aktiva. V rámci srovnávací tabulky lze skrýt nepotřebné řádky klinutím na libovolnou buňku řádku. Pro snazší orientaci lze na jakékoliv buňce Celkového rizika setřídit data od nejvyšší hodnoty k nejnižší.

Kliknutím na sloupec riziko v základním přehledu (tabulky aktiv a jejich hodnocení) lze přidat odůvodnění výsledného rizika.

ŘÍZENÍ RIZIK

V rámci řízení rizik umožňuje nástroj pro každou položku spravovat plány zvládání rizik, bezpečnostní opatření včetně prohlášení o aplikovatelnosti, stavu přijetí/nepřijetí opatření a jeho odůvodnění. Kompletní výsledky řízení rizik zobrazuje Výpis zvládání rizik. Řízení rizik pracuje s posledním dostupným hodnocením rizik. Starší záznamy lze využít jen ve srovnávání v rámci hodnocení rizik.

MAPA RIZIK

Nástroj je Mapa rizik slouží jako grafická prezentace výsledků hodnocených rizik.

EXPORT / IMPORT

Exportovat lze všechna uložená dat. Před importem je vhodné zálohovat svá data. Nástroj Zničit všechna data odstraní všechna data v úložišti. Zničená data nelze obnovit. Vytvoření prázdných objektů připraví úložiště pro případ importu všech potřebných dat například při přemisťování či sdílení dat, ale v případě, že některé objekty obsahují data, pak budou tato data přepsána. Rozdíl mezi zničením dat a vytvořením prázdných objektů je v tom, že zničení dat odstraní i objekty v úložišti.

LICENCE

V nástroji se využívají následující rozšíření s vlastními licenčními podmínkami:

- Font Awesome 4.7

- jQuery 2.1.4. a jeho doplněk Accordion
- Google Fonts Nunito a Raleway

VERZE

Aktuální verze nástroje je 0.5.0.

KOMPATIBILITA, TESTOVÁNÍ A OMEZENÍ

Nástroj je vyvíjen a testován pro webový prohlížeč Google Chrome.

Omezením je nemožnost sdílení dat s více uživateli. Data se ukládají lokálně prostřednictvím javascriptu (localStorage). Toto úložiště umožňuje uložit maximálně 10 MB dat.