VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

ORGANIZAČNÍ OPATŘENÍ PRO ZAJIŠTĚNÍ INFORMAČNÍ BEZPEČNOSTI NA PODNIKATELSKÉ FAKULTĚ

ORGANIZATIONAL MEASURES TO ENSURE INFORMATION SECURITY AT FACULTY OF BUSINESS AND MANAGEMENT

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Tomáš Mráz

AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák

SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

ZADÁNÍ DIPLOMOVÉ PRÁCE

Ústav:	Ústav informatiky
Student:	**Bc. Tomáš Mráz**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2021/22
Studijní program:	Informační management

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

Organizační opatření pro zajištění informační bezpečnosti na podnikatelské fakultě

Charakteristika problematiky úkolu:

Úvod

Teoretická východiska práce

Analýza problému a současné situace

Vlastní návrh řešení a přínos práce

Závěr

Cíle, kterých má být dosaženo:

Vymezení a návrh organizačních opatření pro podnikatelskou fakultu VUT v Brně.

Základní literární prameny:

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

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

DOUCEK Petr, Martin KONEČNÝ a Luděk NOVÁK. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2020. ISBN 978-80-88260-39-4.

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

SEDLÁK Petr, Martin KONEČNÝ a kolektiv. Kybernetická (ne)bezpečnost. Brno: CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2021/22

V Brně dne 28.2.2022

L.S.

_____	_____
doc. Ing. Miloš Koch, CSc.	doc. Ing. Vojtěch Bartoš, Ph.D.
garant	děkan

Abstrakt

Tato diplomová práce se věnuje analýze současného stavu a návrhu bezpečnostních opatření v rámci systému řízení bezpečnosti informací na fakultě podnikatelské, VUT v Brně. Navrhovaná bezpečnostní opatření berou v úvahu zejména požadavky stanovené Zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů a Vyhláškou č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

Klíčová slova

systém řízení bezpečnosti informací, informační bezpečnost, zákon o kybernetické bezpečnosti, vyhláška o kybernetické bezpečnosti, řízení aktiv, řízení rizik, organizační bezpečnost, bezpečnostní role, řízení dodavatelů, bezpečnost lidských zdrojů, řízení provozu a komunikací, řízení změn, řízení přístupů, akvizice, vývoj a údržba, kybernetický bezpečnostní incident a událost, řízení kontinuity činností, audit kybernetické bezpečnosti

Abstract

This diploma thesis deals with the analysis of the current state and the design of security measures within the information security management system at the Faculty of Business, Brno University of Technology. The proposed security measures take into account in particular the requirements set by Act No. 181/2014 Coll. on Cyber Security and on Amendments to Related Acts and Decree No. 82/2018 Coll. on security measures, cyber security incidents, reactive measures, filing requirements in the field of cyber security and data disposal.

Key words

information security management system, information security, cyber security law, cyber security decree, asset management, risk management, organizational security, security roles, supplier management, human resources security, traffic and communications management, change management, access control, acquisition development and maintenance, cyber security incident and event, business continuity management, cyber security audit

Bibliografická citace

MRÁZ, Tomáš. *Organizační opatření pro zajištění informační bezpečnosti na podnikatelské fakultě* [online]. Brno, 2022 [cit. 2022-04-03]. Dostupné z https://www.vutbr.cz/studenti/zav-prace/detail/143231. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce: Petr Sedlák.

Čestné prohlášení

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

V Brně dne 9. května 2022 ……

podpis autora

Poděkování

Chtěl bych poděkovat vedoucímu mé práce, panu Ing. Petru Sedlákovi za odborné vedení této diplomové práce.

OBSAH

ÚVOD

Každodenní využívání informačních a komunikačních technologií v osobním i profesním životě je pro většinu z nás dnes již naprostá samozřejmost. Přirozeným zájmem všech fyzických i právnických osob je svá data chránit, zvláště pak ta osobní a citlivá, která mohou být vyzrazena, zneužita nebo poškozena či ztracena a způsobit nám škodu v podobě např. finančních ztrát, krádeže identity nebo reputační újmy.

V roce 2021 bylo celosvětově připojeno odhadem na 46 miliard IoT zařízení, tedy zařízení, která jsou schopna přijímat a odesílat data. V roce 2030 je předběžný odhad IoT zařízení stanoven na 125 miliard. Snaha o zmapování toho, kde všude jsou naše osobní nebo obchodní data uložena a kudy proudí, je naprosto nemyslitelná. Hlavní problém je totiž fakt, že tato data nejsou ve většina případů ani vygenerována námi. Běžná obchodní transakce, fotografie, na které nás někdo označil na sociálních sítích nebo každodenní administrativní úkon ve státní správě, kde se objevilo naše jméno. To je jen pár příkladů, kdy jsou naše osobní nebo obchodní údaje zpracovány třetí stranou a rozeslány pro nás neznámo kam.

Ačkoliv jsou bezpečnost osobních údajů a v širším měřítku informační a kybernetická bezpečnost aktuálním tématem, jedná se stále o oblasti, v nichž byly standardy vytvořeny teprve nedávno a tempo s jakými se aktualizují jen sotva stíhá technologické pokroky, které v dnešní době zažíváme.

Česká republika se obranou kybernetického prostoru zabývá od roku 2010, ale teprve v roce 2015 byly snahy zákonodárců a odborníků reflektovány v právním řádu, který je platný zejména pro právní subjekty, které jsou definovány jako součást tzv. kritické informační infrastruktury. S rostoucí potřebou chránit více a více odvětví a zároveň s rostoucím rizikem kybernetických útoků probíhá úměrně na úrovni Evropské unie i České republiky evoluce právního řádu a z původních desítek určených subjektů jsou dnes na našem území již stovky.

1 CÍLE PRÁCE A VYMEZENÍ POJMŮ

Hlavním cílem této diplomové práce je poskytnout vrcholovému vedení a osobám odpovědným za kybernetickou bezpečnost na straně Vysokého učení technického v Brně, Fakultě podnikatelské (dále jen „VUT FP“) jeden z prvotních podnětů pro implementaci systému řízení bezpečnosti informací, za účelem zajištění souladu s legislativními požadavky České republiky v oblasti kybernetické bezpečnosti.

1.1 Dílčí cíle

Dílčími cíli této diplomové práce je odpovědět na následující otázky:

1. Proč je téma kybernetické bezpečnosti relevantní pro VUT FP?
2. V jakém stavu se nachází kybernetická bezpečnost na VUT FP?
3. Jaké kroky je potřeba vykonat pro zajištění souladu s legislativními požadavky, za účelem zajištění kybernetické bezpečnosti na VUT FP?

1.2 Vymezení pojmů

Účelem této diplomové práce je seznámit osoby na straně VUT FP s problematikou řízení kybernetické bezpečnosti - a to nejen ty, které se již v oblasti bezpečnosti informací a informačních technologií orientují, ale i další osoby, které umožňují činnosti a projekty v této oblasti zprostředkovávat napříč celou organizační strukturou VUT FP. V tomto smyslu je potřeba nejprve vymezit několik základních pojmů, které se budou v této práci opakovat.

Aktivum – je vše, co má pro jeho vlastníka nějakou hodnotu. Nejedná se pouze o hmotné statky, ale i předmět duševního vlastnictví, tedy nehmotné statky.

V kontextu systému řízení bezpečnosti informací tak, jak s ním pracuje česká legislativa, rozlišujeme aktiva na primární a podpůrná.

Primární aktiva – jedná se o taková aktiva, jejichž ztráta nebo narušení má dopad na chod, funkčnost, bezpečnost a účel organizace.

Jako primární aktiva jsou vnímány zejména informace a služby.

Informace – digitální i nedigitální (materiální) aktivum, které je vytvářeno a zpracováváno v rámci výkonu agendy jeho vlastníka, např. záznamy o provozu,

uživatelská data, přístupové údaje, konfigurační soubory, zdrojové kódy, zálohy, certifikáty, logy a metadata.

Služby – chápeme jako výkon jednotlivých činností organizace, kterými je myšleno např. získávání, poskytování, zpracování, shromažďování, vyhodnocování, ukládání, předávání, likvidování, zobrazování informací a umožnění komunikace v rámci těchto činností.

Podpůrná aktiva – aktiva, která jsou potřebná pro správnou funkčnost, zpracování a uchování primárních aktiv.

Mezi podpůrná aktiva řadíme technické vybavení, programové vybavení, komunikační prostředky, objekty, zaměstnance a dodavatele, kteří se podílejí na provozu, rozvoji, správě a zabezpečení informačního systému.

Bezpečnost informací – řeší ochranu a dostupnost informací. Zabývá se nejen bezpečností informačních a komunikačních technologií, ale i bezpečností informací v nedigitální formě (1).

Informační systém – lze chápat jako systematické propojení informací a procesů, které tyto informace zpracovávají (1).

Kybernetický prostor – je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací (2).

Kybernetická bezpečnost – lze chápat jako souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany kybernetického prostoru (2).

Důvěrnost – vlastnost nedostupnosti informace vůči neoprávněným jednotlivcům, entitám nebo procesům (3).

Dostupnost – vlastnost přístupnosti a použitelnosti informace pro autorizované entity (3).

Integrita – vlastnost přesnosti a úplnosti informace (3).

Dopad – škoda způsobená v důsledku hrozby (1).

Hrozba – událost, která ohrožuje bezpečnost (1).

Zranitelnost – slabé místo aktiva, které může být napadnutelné hrozbou (1).

Riziko – kombinace hrozby, zranitelnosti a dopadu na aktivum (1).

Bezpečnostní opatření – souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru (4).

Nejlepší praxe – (Best practice) – jedná se o osvědčené postupy a metody řízení, pomocí kterých bylo v organizacích prokazatelně dosáhnuto dobrých výsledku (5).

CERT / CSIRT – (Computer Emergency Response Team / Computer Security Incident Response Team) – je skupina odborníků na informační bezpečnost odpovědná za ochranu, detekci a reakci na kybernetické bezpečnostní incidenty. Tyto skupiny mohou existovat jak v rámci soukromých subjektů, tak na národních i mezinárodních úrovních.

Kritická informační infrastruktura (KII) – je prvek nebo systém prvků kritické infrastruktury (4).

Významný informační systém (VIS) – je informační systém, který je spravován orgánem veřejné moci, který není zároveň součástí kritické informační infrastruktury ani součástí základní služby (4).

Správce informačního systému – je orgán nebo osoba, která definuje účel zpracování informací a podmínky pro provoz informačního systému (4).

Správce komunikačního systému – je orgán nebo osoba, která definuje účel komunikačního systému a podmínky pro jeho provoz (4).

Provozovatel informačního nebo komunikačního systému – je orgán nebo osoba, která zajišťuje funkčnost technických a programových prostředků, jež tvoří informační nebo komunikační systém (4).

2 TEORETICKÁ VÝCHODISKA PRÁCE

Tato kapitola diplomové práce pomůže čtenáři pochopit základní principy systému řízení bezpečnosti informací **zejména v souladu s požadavky české legislativy.** V první části bude popsán legislativní rámec zastřešující kybernetickou bezpečnost, který je platný pro jasně definované právní subjekty, mezi které se VUT FP řadí. V další části budou popsány obecné principy systému řízení bezpečnosti informací. V poslední části budou přiblíženy metodiky, které lze v jeho řízení využít.

2.1 Legislativní rámec kybernetické bezpečnosti České republiky

Přestože počátky kybernetické kriminality můžeme datovat již do 70. let 20. století, teprve s přechodem do druhého milénia nastal skutečně masový růst internetového pokrytí po celém světě. Co spotřebitelům naskytlo dosud nevídané možnosti v oblastech usnadnění práce a výměny informací, zároveň otevřelo brány jednotlivcům a skupinám, jejichž cílem bylo pomocí internetu páchat škody a obohacovat se. Bohužel adaptace veřejného i soukromého sektoru na tyto nové hrozby neprobíhala dostatečně rychle a nebyla jednotná. Za účelem nastavení harmonizovaného bezpečnostního rámce se proto do této problematiky vložil stát.

Kybernetická bezpečnost v České republice byla od počátku založena na efektivní spolupráci všech relevantních aktérů na národní i mezinárodní úrovni. Tato podkapitola bude však věnovaná hlavně kybernetické bezpečnosti na našem území.

2.2 Vývoj kybernetické bezpečnosti v ČR

Dne 15. března 2010 bylo schváleno usnesení č. 205 o řešení problematiky kybernetické bezpečnosti a gestorem problematiky kybernetické bezpečnosti bylo ustanoveno Ministerstvo vnitra České republiky, přičemž se stalo národní autoritou této oblasti (7).

Dne 24. května 2010 bylo přijato usnesení č. 380, kterým byla zřízena Meziresortní koordinační rada pro oblast kybernetické bezpečnosti (7).

Dne 9. prosince 2010 bylo Ministerstvem vnitra České republiky ve sdružení s CZ.NIC podepsáno Memorandum, kterým byl zřízen Národní CSIRT (7).

Dne 20. července 2011 bylo Vládou České republiky přijato usnesení č. 564, kterým byla mimo jiné schválena Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011–2015 (7).

Dne 19. října 2011 bylo Vládou České republiky přijato usnesení č. 781 jímž byl ustaven Národní bezpečnostní úřad jako gestor problematiky kybernetické bezpečnosti, přičemž se stal národní autoritou této oblasti (7).

Dne 13. května 2014 bylo Národním bezpečnostním úřadem (NBÚ ČR) otevřeno Národní centrum kybernetické bezpečnosti (Vládní CERT) (7).

Dne 13. srpna 2014 byl prezidentem České republiky podepsán zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti – dále jen ZKB), který nabyl účinnosti 1. ledna 2015 (7).

Současně s tímto zákonem přešla v platnost 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 – dále jen VKB) (2).

Dne 12. března 2015 byla schválena strategie Národní strategie kybernetické bezpečnosti České republiky na období 2015–2020.

Dne 1. srpna 2017 nabyla účinnosti novela zákona o kybernetické bezpečnosti č. 205/2017 Sb., z důvodu nutné harmonizace s evropským právem v podobě směrnice Evropského parlamentu a Rady EU 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii – směrnice NIS (2).

Na základě stejného zákona byl současně zřízen Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), přičemž se stal národní autoritou v oblasti kybernetické bezpečnosti.

Dne 28. května 2018 byla novelizována vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti – VKB) (2).

Dne 25. května 2018 nabylo účinnosti Obecné nařízení na ochranu osobních údajů neboli GDPR (General Data Protection Regulation), kterým byl nahrazen zákon č. 101/2000 Sb., o ochraně osobních údajů (2).

Dne 2. prosince 2020 byla schválena strategie Národní strategie kybernetické bezpečnosti České republiky na období 2021–2025.

2.3 Instituce na poli kybernetické a informační bezpečnosti v ČR

Na poli kybernetické a informační bezpečnosti v České republice působí řada institucí v rámci veřejného sektoru. Podkapitoly níže stručně představují ty nejvýznamnější z nich.

2.3.1 Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB

Jak již bylo zmíněno v předchozí kapitole, aktuálně je NÚKIB národní autoritou v oblasti kybernetické bezpečnosti. To znamená, že NÚKIB je správním úřadem pro kybernetickou bezpečnost, ochranu utajovaných informací pro oblast informačních a komunikačních systémů, kryptografickou ochranu a problematiku veřejně regulované služby navigačního systému Galileo (8).

Mezi další odpovědnosti a role úřadu patří například:

- spolupráce s CERT a CSIRT bezpečnostními týmy po celém světě,
- příprava národních bezpečnostních politik v oblasti kybernetické bezpečnosti,
- definování bezpečnostních standardů pro informační systémy kritické informační infrastruktury,
- stanovení pravidel pro ochranu utajovaných informací v oblasti informačních a komunikačních systémů,
- příprava a koordinace kybernetických cvičení jak v ČR, tak v zahraničí,
- hájení zájmů ČR na poli kybernetické bezpečnosti,
- příprava zákonů a podzákonných norem, které se týkají kybernetické bezpečnosti,
- vytyčování národní strategie kybernetické bezpečnosti,
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti (8).

Kromě výše uvedeného je NÚKIB odpovědný za **kontrolu dodržování zákona a vyhlášky o kybernetické bezpečnosti**, poskytování metodických podpor a posuzování stavu kybernetické bezpečnosti v organizacích.

2.3.2 Vládní CERT – GovCERT

Při ochraně kritické informační infrastruktury a významných informačních systémů hraje Vládní CERT klíčovou roli. Úkolem této organizační složky NÚKIB je čelit bezpečnostním výzvám, reakce na incidenty, koordinace činností při jejich řešení a jejich předcházení ve formě vydávání reaktivních a ochranných opatření. Vládní CERT zároveň působí jako prvotní zdroj bezpečnostních informací pro organizace v rámci státní správy, ale i soukromou sféru a občany (10).

2.3.3 Národní CERT – CSIRT.CZ

Hlavními odpovědnostmi národního CERT je přijímání hlášení o kybernetických bezpečnostních incidentech od osob uvedených v § 3 ZKB, jejich uchovávání, ochrana a vyhodnocování. Pro tyto osoby působí jako kontaktní místo a poskytuje jim metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu. Činnost národního CERT je úzce spjata s činnostmi NÚKIB, konkrétně vládního CERT, jemuž předává údaje o kybernetických bezpečnostních incidentech, bez uvedení ohlašovatele.

Provozovatelem této instituce je od jejího založení v ČR sdružení CZ.NIC. Jedná se o zájmové sdružení právnických osob, jehož hlavním posláním je provoz a rozvoj důvěryhodné, bezpečné a stabilní infrastruktury a dalších obecně prospěšných internetových služeb. Toto sdružení je zároveň provozovatelem domény .cz (10).

2.3.4 Národní bezpečnostní úřad – NBÚ

NBÚ je ústřední správní úřad v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti. Mezi hlavní odpovědnosti NBÚ patří vydávání osvědčení pro fyzické osoby i podnikatele. Tato osvědčení garantují, že osoby byly prověřeny a nebyly odhaleny žádné skutečnosti, které by je mohly kompromitovat při přístupu k utajovaným informacím nebo při výkonu citlivých činností. Jedná se o efektivní způsob, jak zajistit ochranu citlivých informací, ať už jde o obranné, vojenské, bezpečnostní, ekonomické nebo politické záměry České republiky (11).

2.3.5 Bezpečnostní informační služba České republiky – BIS

BIS je hlavní zpravodajskou institucí českého státu, jejímž cílem je ochrana území českého státu. Jiným označením hovoříme o civilní kontrarozvědce. Tohoto dosahuje získáváním, shromažďováním a vyhodnocováním informací, které se týkají:

- hrozeb terorismu,
- aktivit ohrožující bezpečnost státu nebo její významné ekonomické zájmy,
- činností cizích zpravodajských služeb na území ČR,
- záměrů nebo činů, které směřují proti demokratickým základům, svrchovanosti a územní celistvosti ČR,
- aktivit organizovaného zločinu,
- činností ohrožujících utajované informace (12).

2.3.6 Úřad pro zahraniční styky a informace – ÚZSI

Hlavním cílem ÚZSI je pro orgány a činitele státní správy českého státu zabezpečovat přesné, objektivní a včasné zpravodajské informace, které jsou původem ze zahraničí a mohou mít vliv na bezpečnost a ochranu politických a ekonomických zájmů ČR v zahraničí. Jedná se tedy o civilní rozvědku. Činnost ÚZSI nemá represivní charakter a nejedná se o orgán činný v trestním řízení, ani z jeho činnosti nevyplývá ohrožení práv a svobod občanů ČR (13).

2.3.7 Vojenské zpravodajství – VZ

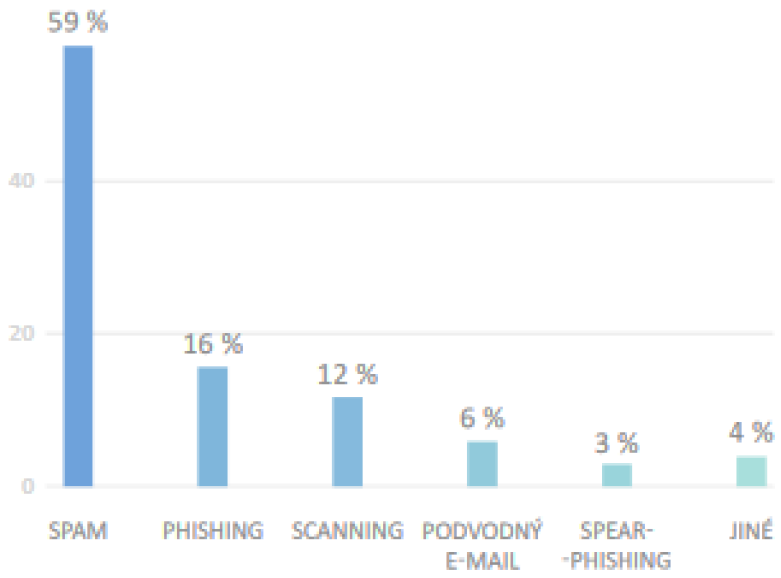
VZ je ozbrojená zpravodajská služba ČR. Součástí této služby je rozvědná i kontrarozvědná činnost. Hlavním úkolem VZ je získávání, shromažďování a vyhodnocování informací, které mohou ovlivňovat schopnost obrany ČR. Zdroje těchto informací mohou pocházet jak z vlastního území, tak ze zahraničí (14).

2.4 Aktuální vývoj kybernetických hrozeb v ČR

Z posledního zveřejněného hlášení o vývoji kybernetické bezpečnosti, které vydává NÚKIB, vyplývá, že v roce 2020 bylo proti českým institucím, organizacím a firmám napříč všemi sektory nahlášeno 468 incidentů. Oproti tomu bylo v roce 2019 nahlášeno pouze 217 incidentů. Toto navýšení nelze jednoznačně přisoudit k tomu, že by těchto

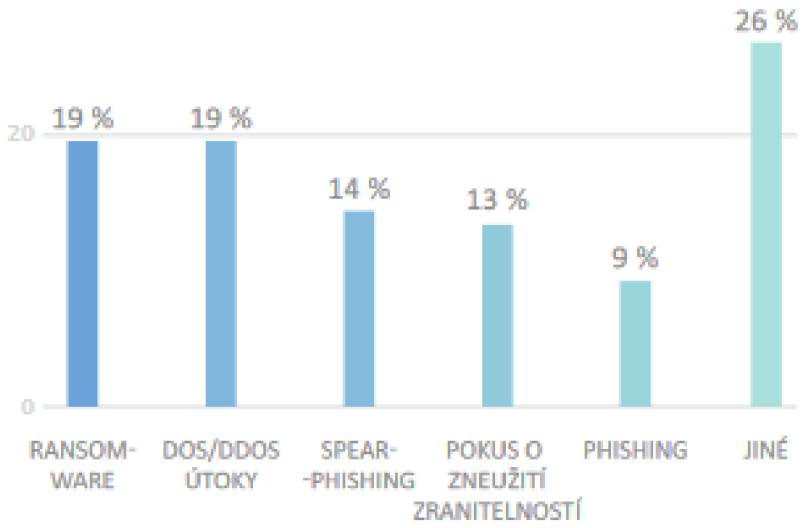
incidentů proběhlo víc, ale dalším z faktorů může být to, že o existenci a činnosti NÚKIB panuje na úrovni veřejnosti vyšší povědomí. O čem nicméně pochyb být nemůže, je fakt, že vzrostla závažnost těchto incidentů s odkazem na kybernetické útoky na Nemocnici Rudolfa a Stefanie Benešov v roce 2019 a Fakultní nemocnici Brno v roce 2020, které měly zásadní dopad na schopnost nemocnic poskytovat zdravotní péči během a bezprostředně po útoku.

Mezi nejrozšířenější útoky v roce 2020 patřily spam, phishing a skenování vnějších sítí organizací. Data byla získána z dotazníků, které rozeslal NÚKIB v roce 2020. Na dotazníky odpovědělo celkem 222 subjektů, mezi kterými bylo 63 institucí z veřejného sektoru, 24 finančních institucí, 77 zdravotnických zařízení, 14 organizací v oblasti poskytování digitálních služeb, 12 subjektů patřících do energetického sektoru, 12 subjektů z průmyslu a 20 institucí v oblasti vzdělávání (15).



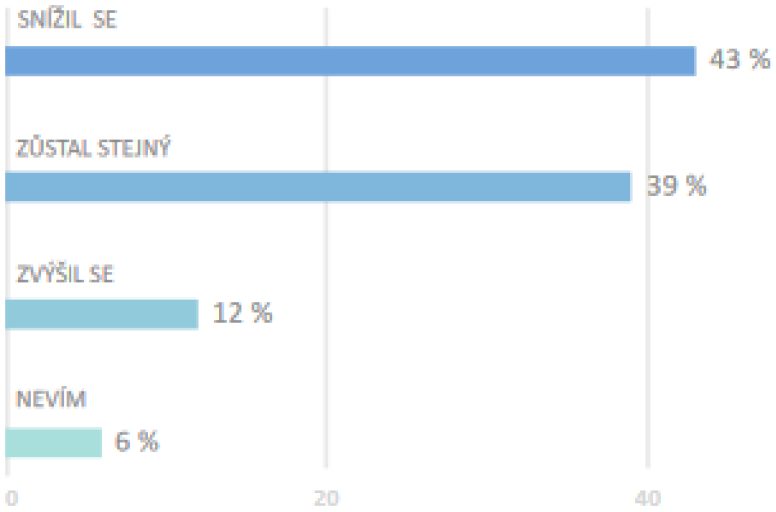
Obrázek 1: Nejčastější typy kybernetických útoků v roce 2020 (Zdroj: [15, str. 9])

Dalším dotazem, na který respondenti odpovídali, bylo hodnocení závažnosti útoků. Mezi nejzávažnější typy útoků respondenti uváděli ransomware útoky, DoS/DDoS útoky, phishingové útoky a pokusy o zneužití zranitelností (15).

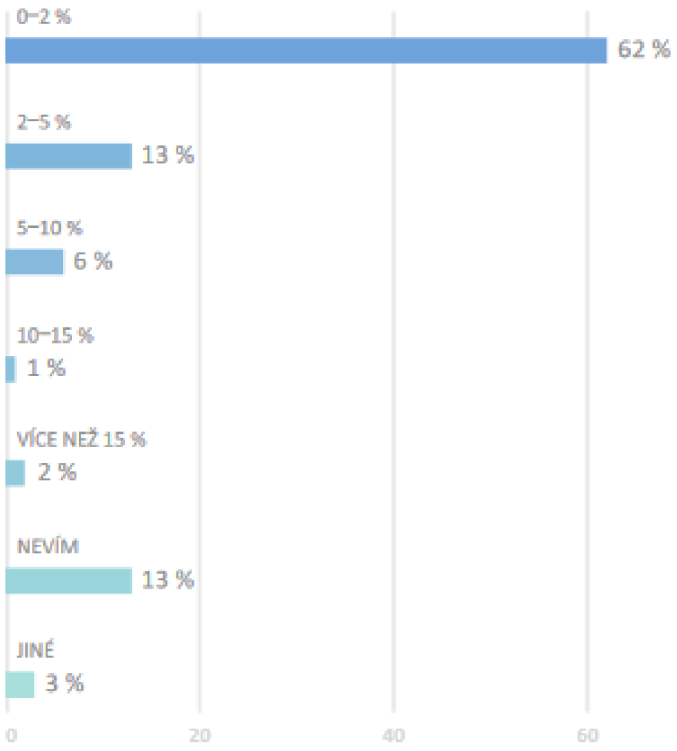


Obrázek 2: Kategorie nejzávažnějších typů kybernetických útoků v roce 2020 (Zdroj: [15, str. 9])

Jedním z přetrvávajících problémů patří nedostatek finančních prostředků vynaložených organizacemi na zajištění kybernetické bezpečnosti. Ten v drtivé většině dle vyjádření respondentů zůstal stejný nebo se snižoval. A to přesto, že dotazované organizace investují do kybernetické bezpečnosti pouze 0-5 % z jejich celkového rozpočtu (15).



Obrázek 3: Vývoj rozpočtu na kybernetickou bezpečnost oproti roku 2019 (Zdroj: [15, str. 10])



Obrázek 4: Podíl rozpočtu v kybernetické bezpečnosti na celkovém rozpočtu (Zdroj: [15, str. 10])

Dopady podfinancování můžeme hledat na více místech. Tím nejcitelnějším je určitě to, že na trhu práce není dostatek odborníků v oblasti kybernetické bezpečnosti, kteří by byly schopni zastávat bezpečnostní role v organizacích. Poptávka tak značně převládá nad nabídkou. To má přirozeně vliv na to, že pouze organizace, které dokážou tyto odborníky adekvátně ohodnotit, si mohou dovolit tyto odborníky získat a udržet.

Avšak i řadoví zaměstnanci, kteří jsou každý den vystaveni nebezpečí kybernetických útoků, tyto dopady pociťují, ať už si je uvědomují nebo ne. Neadekvátní alokace finančních zdrojů se také podepisuje na obecné osvětě o kybernetické bezpečnosti a kontinuálním zlepšování bezpečnostního povědomí zaměstnanců. Ti tak často ani nemají šanci rozpoznat podezřelé chování pracovní stanice, informačního a komunikačního systému nebo rozeznat podvodné a phishingové emaily.

2.5 Zákon o kybernetické bezpečnosti

Jak již bylo zmíněno v krátkém shrnutí vývoje kybernetické bezpečnosti v ČR, zákon o kybernetické bezpečnosti č. 181/2014 Sb. byl přijat v roce 2014 s cílem upravovat práva a povinnosti osob a působnost a pravomoci orgánu veřejné moci v oblasti kybernetické

bezpečnosti. Hlavními důvody pro přijetí tohoto zákona byl nárůst kyberkriminality, kyberterorismu a rostoucí závislost společnosti na fungování informačních technologií (6).

§ 1 ZKB udává, že předmětem úpravy jsou následující oblasti:

„*(1) Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánu veřejné moci v oblasti kybernetické bezpečnosti.*

(2) Tento zákon zapracovává příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.

(3) Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.“

Ideou tohoto zákona je tedy nastavit podmínky spolupráce mezi subjekty tohoto zákona ze soukromého i veřejného sektoru a veřejnou správou. Účelem je zajištění oprávnění a povinností s cílem zvýšení bezpečnosti kybernetického prostoru a efektivní zvládání kybernetických bezpečnostních incidentů (6).

Podle § 2 písm. a) ZKB „*se kybernetickým prostorem rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.*“

Záměrem ZKB je tedy chránit alespoň tu část infrastruktury, která je významná pro fungování státu a jejíž narušení by mohlo vést k poškození nebo ohrožení zájmů České republiky v oblastech kritické informační infrastruktury, významných informačních systémů, významných sítí elektronických komunikací a základních služeb.

Věcnou působnost ZKB lze shrnout následovně:

- Práva a povinnosti orgánu státu, jemuž byla svěřena pravomoc v oblasti zajišťování kybernetické bezpečnosti. Tímto ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany je od 1. srpna 2017 NÚKIB.
- Zřízení vládního CERT, jako součást NÚKIB, jež působí jako pracoviště provozované za účelem ochrany služeb a sítí elektronických komunikací a informačních systému před kybernetickými bezpečnostními událostmi.

- Mechanismus přenosu informací, které jsou nezbytné pro prevenci před kybernetickými hrozbami, které dále slouží pro analýzu možných kybernetických útoků a pro způsoby jejich včasného rozpoznání.
- Sestavení systému včasného varování a dále prevence a osvěty včetně poskytování pomoci v rámci zavádění preventivních opatření a protiopatření pro případy hrozících útoků.
- Nastavení bezpečnostních systémů nezbytných pro chod státu.
- Pravidla pro koordinaci činností pro odvrácení a během odvrácení útoků na prvky kritické informační infrastruktury a k řešení situací, kdy je potřeba přijímat bezpečnostní opatření před možnými následky těchto útoků (6).

Grafické zobrazení povinností orgánu a osob podle zákona č. 181/2014 Sb., které publikoval NÚKIB, lze nalézt v příloze I.

2.6 Vyhláška o kybernetické bezpečnosti

Vyhláška o kybernetické bezpečnosti č. 82/2018 Sb., byla přijata 28. května 2018 se záměrem nahrazení původní vyhlášky č. 316/2014 Sb. Jejím hlavním úkolem bylo zapracování Směrnice Evropského parlamentu a Rady EU 2016/1448 (Směrnice NIS) pro informační systémy kritické informační infrastruktury, komunikační systémy kritické informační infrastruktury, významné informační systémy, informační systémy základní služby a informační systémy nebo sítě elektronických komunikací, které využívá poskytovatel digitálních služeb.

Vyhláška upravuje následující oblasti:

- strukturu a obsah bezpečnostní dokumentace.
- rozsah a obsah bezpečnostních opatření,
- typy a kategorie kybernetických bezpečnostních incidentů, včetně jejich hodnocení,
- náležitosti a způsob ohlašování kybernetických bezpečnostních incidentů,
- náležitosti a způsob provedení reaktivního opatření a jeho výsledku,
- vzor oznámení kontaktních údajů, včetně jeho formy,
- způsoby likvidace dat, provozních údajů, informací a jejich kopií.

Ve vztahu k ZKB je účelem VKB podrobněji specifikovat obecně formulovaná ustanovení ve formě detailně popsaných vyžadovaných bezpečnostních opatření a doprovázejících příloh. Obecnou zásadou zůstává, že subjekty zákona by měly všechna tato opatření aplikovat přiměřeně a všechny informace v předpisech obsažené přizpůsobit vlastním potřebám v oblasti řízení kybernetické bezpečnosti (6).

2.7 Systém řízení bezpečnosti informací

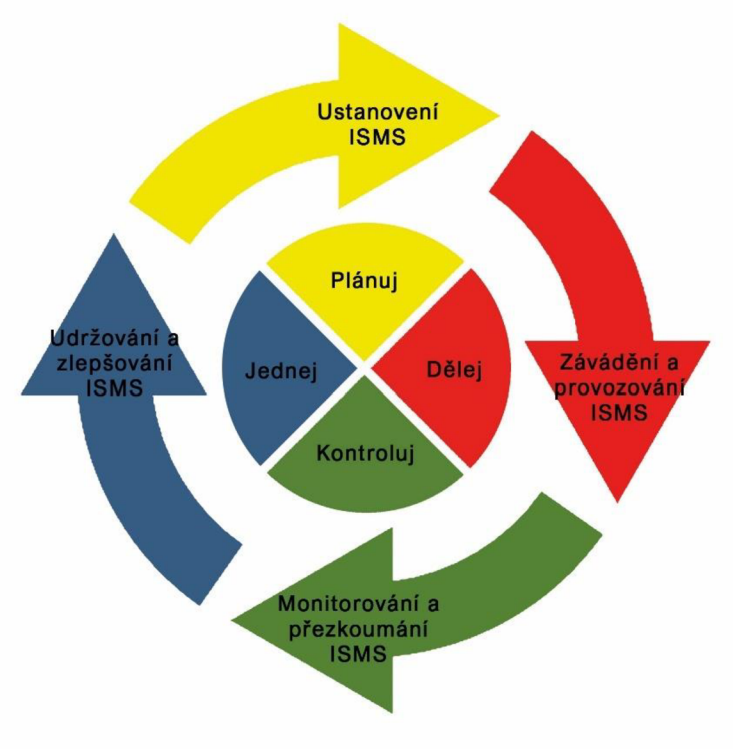
Systém řízení bezpečnosti informací (dále jen „ISMS“) je zdokumentovaný systém, skládající se z bezpečnostních zásad, které chrání důvěrnost, dostupnost a integritu aktiv před hrozbami a zranitelnostmi a pomáhají tak snižovat rizika, kterým se organizace vystavuje. Riziko v tomto kontextu představuje možnost ztráty, poškození nebo zničení informačního aktiva v důsledku hrozby využívající zranitelnosti.

Norma ČSN ISO/IEC 27001 popisuje ISMS jako systematický přístup k vytvoření, implementaci, provozu, monitorování, kontrole, údržbě a zlepšování bezpečnosti informací organizace a jejich zabezpečení k dosažení obchodních cílů. Skládá se ze zásad, pokynů, postupů a souvisejících zdrojů a činností. ISMS musí být založen na posouzení rizik, při kterých se rozhoduje o tom, jaká bezpečnostní opatření aktiva potřebují k dosažení přijatelné úrovně rizika.

Aby byl systém řízení bezpečnosti informací úspěšný, musí být neustále kontrolován a zlepšován. Pomocí cyklu Plan-Do-Check-Act (PDCA) toho lze snadněji dosáhnout.

2.7.1 PDCA model

Jedním z best practice přístupů v oblasti řízení nejen kybernetické bezpečnosti je model PDCA cyklu, který se sestává z následujících činností. Obrázek č. 5 tento model graficky znázorňuje.



Obrázek 5: Grafické zobrazení PDCA cyklu (Zdroj: Vlastní zpracování)

Plánuj

V této fázi jsou plánovány činnosti. V závislosti na velikosti projektu může plánování zabrat hlavní část úsilí celého projektového týmu. Obvykle se skládá z menších kroků, aby byl sestaven plán na míru s menším prostorem pro selhání.

Otázky, které je třeba si položit během plánování:

- Co je jádrem problematiky, kterou je potřeba vyřešit?
- Jaké zdroje jsou k tomu potřeba?
- Jaké zdroje jsou k tomu k dispozici?
- Jaké je nejlepší řešení problematiky za využití zdrojů, které jsou k dispozici?
- Jaké jsou měřitelné podmínky úspěchu plánu a jaké jsou jeho cíle?

V kontextu kybernetické bezpečnosti je zde třeba ustanovit politiky ISMS, vytyčit cíle, určit procesy a postupy, které souvisí s řízením rizik a zlepšováním bezpečnosti informací (6).

Dělej

Jakmile je odsouhlasen plán, je čas jednat. V této fázi bude využito vše, co bylo zvažováno v plánovací fázi. Standardizace je v této fázi jednoznačným klíčem k tomu, aby by plán implementován úspěšně.

V kontextu kybernetické bezpečnosti se jedná o zavedení a využívání politiky ISMS, opatření, procesů a postupů (6).

Kontroluj

Jedná se pravděpodobně o nejdůležitější část PDCA cyklu. Pokud je potřeba usměrnit plán, vyhnout se opakujícím se chybám a aplikovat postupy pro neustále zlepšování úspěšně, je potřeba se této fázi důkladně věnovat.

V kontextu kybernetické bezpečnosti je toto fáze, ve které je nutné posuzovat fungování ISMS a měřit výkon v dosahování definovaných cílů a tyto výsledky hlásit vrcholovému vedení k přezkoumání (6).

Jednej

Pokud je v kontrolní fázi vyhodnoceno, že došlo k naplnění cílů, může být celý plán přijat a aplikován. Tím se celá tato iterace PDCA cyklu stane standardem pro řešení dané problematiky do budoucna.

V kontextu kybernetické bezpečnosti je na základě výstupů z kontrolní fáze potřeba přijmout opatření k nápravě a preventivní opatření, která jsou založená na výsledcích interního auditu ISMS a přezkoumání ISMS ze strany vrcholového vedení (6).

3 ANALÝZA SOUČASNÉHO STAVU

V této části diplomové práce bude cílem odpovědět na dvě dílčí otázky, které byly položeny v první kapitole, tedy:

1. Proč je téma kybernetické bezpečnosti relevantní pro VUT FP?
2. V jakém stavu se nachází kybernetická bezpečnost na VUT FP?

Přestože byla významnost kybernetické bezpečnosti popsána v teoretických východiscích této práce, zatím nebyl zodpovězena otázka, proč by se mělo VUT FP zabývat kybernetickou bezpečností dle ZKB a VKB.

Jakmile je toto jasné, je provedena GAP analýza současného stavu kybernetické bezpečnosti a souladu VUT FP s požadavky VKB.

3.1 Kontext organizace

Vysoké učení technické v Brně patří mezi nejstarší veřejné vysoké školy na území dnešní České republiky a byla vůbec první dvojjazyčnou školou na Moravě, když byla založena ještě za Rakouska-Uherska v roce 1899.

Dnes je VUT mezinárodně uznávanou vzdělávací institucí, která se může pyšnit špičkovými odbornými a vědeckými znalostmi na osmi fakultách a třech vysokoškolských ústavech.

Těmito fakultami jsou:

- Fakulta stavební,
- Fakulta strojního inženýrství,
- Fakulta elektrotechniky a komunikačních technologií
- Fakulta architektury,
- Fakulta chemická,
- Fakulta podnikatelská,
- Fakulta výtvarných umění,
- Fakulta informačních technologií.

Mezi zmíněné vysokoškolské ústavy patří:

- Centrum sportovních aktivit,
- Středoevropský technologický institut,
- Ústav soudního inženýrství.

Studenti zde mohou získávat kvalitní vzdělání napříč technickými, přírodovědnými, ekonomickými a uměleckými obory. VUT se dále intenzivně věnuje aktivitám v oblasti výzkumu a vývoje, probíhajícím na půdě výzkumných center (16).

Praktická část diplomové práce se však zaměřuje pouze na prostředí kybernetické bezpečnosti Fakulty podnikatelské. Jedná se o strategické rozhodnutí, které bylo přijato z důvodu enormního rozsahu organizačního, personálního a technického charakteru v rámci celého VUT. Takovýto rozsah by zkrátka nebylo možné pokrýt v jedné diplomové práci. Společným přáním autora a vedoucího diplomové práce je, aby byly výstupy využity v budoucích projektech v oblasti kybernetické bezpečnosti.

3.2 Legislativní požadavky kladené na VUT FP

Dle § 3 zákona o kybernetické bezpečnosti jsou „*orgány a osobami, kterým se ukládají povinnost v oblasti kybernetické bezpečnosti:*

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem 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.“

Z uvedené citace vyplývá, že pouze uvedené osoby jsou povinny dodržovat povinnosti v oblasti kybernetické bezpečnosti. VUT FP spadá mezi uvedenými orgány a osobami pod písmeno e), tedy je správcem a provozovatelem významného informačního systému.

Významným informačním systémem se dle § 2 písm. d) zákona o kybernetické bezpečnosti rozumí „*informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit* ***výkon působnosti orgánu veřejné moci.***“

Z této definice je zřejmé, že jako významné informační systémy mohou být identifikovány pouze ty, kterými VUT FP vykonává svoji působnost jakožto orgán veřejné moci.

K výkonu působnosti orgánu veřejné moci školy dochází zejména pokud je rozhodováno o právech a povinnostech žáků, studentů, akademických pracovníků a dalších osob, na základě školského zákona nebo zákona o vysokých školách, případně dalších vnitřních předpisů vysokých škol. U VUT FP a dalších vysokých škol se může jednat o širší množinu činností s ohledem na míru jejich samosprávy.

V praxi se jedná o systémy, jejichž pomocí je podpořeno autoritativní rozhodování ze strany školy, např. rozhodnutí o přijetí nebo nepřijetí studentů, přerušení studia, uznání studia, přiznání stipendia, ukončení studia apod.

Systémy, které autoritativní rozhodování ze strany školy nepodporují, mezi významné informační systémy nepatří. Takovéto systémy typicky slouží k zajištění provozu školy, výuky, docházky apod.

Pokud jsou tedy významné informační systémy identifikovány, musí ve všech relevantních oblastech být splněny požadavky ZKB a VKB (17).

3.3 GAP analýza

GAP analýza byla provedena s pomocí formuláře prohlášení o aplikovatelnosti, který je volně dostupný na webových stránkách NÚKIB. Přestože formulář slouží primárně jako vzor zpracování požadavku § 5 odst. 1 písm. a) VKB, byl v rámci této diplomové práce využit jako vzor pro dotazník. Tento dotazník byl vyplněn s pomocí vedoucího

diplomové práce, který se významným způsobem podílí na zájmech VUT FP v oblasti kybernetické bezpečnosti.

V nadcházejících podkapitolách bude GAP analýza zpracována v její zjednodušené verzi, dle následující šablony:

zjednodušený popis požadavků	
soulad	komentář

- Název oblasti – číslo § VKB a název kapitoly.
- Zjednodušený popis požadavků – zkrácený výpis nebo parafráze požadavku VKB.
- Soulad:
  - ANO – požadavek je plněn,
  - NE – požadavek není plněn,
  - A/N – požadavek je plněn částečně,
  - NON – není relevantní / nelze určit míru souladu.
- Komentář – způsob plnění požadavku nebo důvod jeho neplnění.

Plné znění všech požadavků dle VKB lze nalézt v příloze I.

Je podstatné zdůraznit, že zkoumaným rozsahem této diplomové práce jsou požadavky, které se týkají pouze následujících částí VKB:

- Část druhá – bezpečnostní opatření,
  - Hlava I – organizační opatření,
  - Hlava III – bezpečnostní politika a bezpečnostní dokumentace,
- Část třetí – kybernetický bezpečnostní incident,
- Část čtvrtá – reaktivní opatření.

Tedy pro upřesnění, Hlava II – technická opatření a přílohy VKB nejsou v rozsahu analytické části této diplomové práce.

3.3.1 Systém řízení bezpečnosti informací

P1: Je stanoven rozsah systému řízení bezpečnosti informací s ohledem na požadavky dotčených stran a jsou určeny organizační části a aktiva, jichž se ISMS týká.	
NE	-

P1: Jsou stanoveny cíle ISMS.	
NE	-

P1: Pro stanovený rozsah jsou na základě cílů ISMS, bezpečnostních potřeb a hodnocení rizik zavedena přiměřená bezpečnostní opatření.	
NE	-

P1: Účinnost ISMS je pravidelně vyhodnocována. Jejím obsahem je hodnocení stavu ISMS, revize hodnocení rizik, posouzení výsledků provedených auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na ISMS.	
NE	-

P1: ISMS a související dokumentace je aktualizována na základě zjištění auditů kybernetické bezpečnosti, výsledků hodnocení ISMS a v souvislosti s prováděnými významnými změnami.	
NE	-

P1: Provoz ISMS a jeho zdroje jsou řízeny a činnosti s nimi spojené jsou zaznamenávány.	
NE	-

Požadavky na systém řízení bezpečnosti informací dle § 3 VKB nejsou implementovány.

3.3.2 Řízení aktiv

P2: Je stanovena metodika pro identifikaci a hodnocení aktiv.	
NE	-

P2: Aktiva jsou identifikována, hodnocena, evidována a jsou určeni jejich garanti.	
NE	-

P2: Primární aktiva jsou hodnocena z hlediska důvěrnosti, integrity a dostupnosti.	
NE	-

P2: Mezi primárními a podpůrnými aktivy jsou určeny vazby a důsledky těchto závislostí jsou vyhodnocovány.	
NE	-

P2: Jsou stanoveny přípustné způsoby používání aktiv a pravidla pro manipulaci s nimi s ohledem na jejich úroveň.	
NE	-

P2: Jsou stanoveny způsoby likvidace dat, provozních údajů, informací a jejich kopií s ohledem na úroveň aktiv.	
NE	-

P2: Důležitost primárních aktiv je posouzena alespoň z následujících hledisek: • rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství, • rozsah dotčených právních povinností nebo jiných závazků, • rozsah narušení vnitřních řídících a kontrolních činností, • poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty, • dopady na poskytování důležitých služeb, • rozsah narušení běžných činností, • dopady na zachování dobrého jména nebo ochranu dobré pověsti, • dopady na bezpečnost a zdraví osob, • dopady na mezinárodní vztahy a dopady na uživatele informačního a komunikačního systému.	
NE	-

Požadavky na řízení aktiv dle § 4 VKB nejsou implementovány.

3.3.3 Řízení rizik

P3: Je stanovena metodika pro identifikaci a hodnocení rizik, včetně kritérií pro jejich akceptovatelnost.	
NE	-

P3: S návazností na aktiva jsou identifikovány relevantní hrozby a zranitelnosti, které jsou následně vyhodnoceny s ohledem na možné dopady na aktiva.	
NE	-

P3: Hodnocení rizik je prováděno alespoň jednou za tři roky.	
NE	-

P3: Je zpracována zpráva o hodnocení rizik.	
NE	-

P3: Je zpracováno prohlášení o aplikovatelnosti, které obsahuje přehled bezpečnostních opatření, která: • nebyla aplikována, včetně zdůvodnění, • byla aplikována, včetně způsobu plnění.	
NE	-

P3: Je zpracován plán zvládání rizik, který obsahuje cíle, přínosy, odpovědné osoby, potřebné zdroje, termín zavedení, popis vazeb mezi riziky a bezpečnostními opatřeními a způsob jejich realizace. V tomto plánu jsou zohledněny zejména významné změny, změny rozsahu ISMS a kybernetické bezpečnostní incidenty, včetně těch již řešených.	
NE	-

P3: V souladu s plánem zvládání rizik jsou zaváděna bezpečnostní opatření.	
NE	-

Požadavky na řízení rizik dle § 5 VKB nejsou implementovány.

3.3.4 Organizační bezpečnost

P4: Zaměstnanci jsou informování o významu ISMS a o důležitosti dosažení shody s jeho požadavky se všemi dotčenými stranami.	
NE	-

P4: Vrcholové vedení zajišťuje podporu k dosažení zamýšlených výstupů ISMS ve formě potřebných zdrojů a vede zaměstnance k rozvíjení efektivity ISMS.	
NE	-

P4: Jsou stanovena pravidla pro určování administrátorů a osob zastávající bezpečnostní role, včetně příslušných pravomocí.	
NE	-

P4: Je zajištěno testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.	
NE	-

P4: Je určeno složení výboru pro řízení kybernetické bezpečnosti, bezpečnostní role a jejich práva a povinnosti související s ISMS.	
NE	-

Požadavky na organizační bezpečnost dle § 6 VKB nejsou implementovány.

3.3.5 Bezpečnostní role

P5: Role Manažera kybernetické bezpečnosti je obsazena osobou, která je pro tuto činnost vyškolena a prokázala svou odbornou způsobilost praxí s řízením kybernetické bezpečnosti nebo s řízením bezpečnosti informací.	
NE	-

P5: Role garantů aktiv je obsazena.	
NE	-

Požadavky na bezpečnostní role dle § 7 VKB nejsou implementovány.

3.3.6 Řízení dodavatelů

P6: Jsou stanovena pravidla pro dodavatele, která zohledňují požadavky ISMS, dodavatelé jsou s nimi prokazatelně seznámeni a tyto pravidla plní.	
NE	-

P6: Je vedena evidence významných dodavatelů a ti jsou o této skutečnosti prokazatelně informovaní.	
NE	-

P6: Smlouvy obsahují způsoby a úrovně realizace bezpečnostních opatření a jsou určeny vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.	
NE	-

P6: Jsou přiměřeně řízena rizika v souvislosti s výběrovým řízením a před uzavřením smlouvy, která souvisí s předmětem výběrového řízení.	
NE	-

P6: Rizika spojená s předmětem plnění smlouvy jsou pravidelně vyhodnocována a bezpečnostní opatření s nimi spojená jsou pravidelně kontrolována.	
soulad	-

Požadavky na řízení dodavatelů dle § 8 VKB nejsou implementovány.

3.3.7 Bezpečnost lidských zdrojů

P7: S ohledem na stav a potřeby ISMS je stanoven plán rozvoje bezpečnostního povědomí, který zajistí odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje konkrétní formu, obsah a rozsah: • poučení uživatelů, administrátorů, osob zastávající bezpečnostní role a dodavatelů o jejich povinnostech a bezpečnostní politice organizace, • potřebných teoretických a praktických školení uživatelů, administrátorů a osob zastávající bezpečnostní role.	
NE	-

P7: Jsou určeny osoby odpovědné za jednotlivé činnosti uvedené v plánu rozvoje bezpečnostního povědomí	
NE	-

P7: Uživatelé, administrátoři, osoby zastávající bezpečnostní role a dodavatelé jsou o svých povinnostech a bezpečnostní politice seznamováni formou vstupních a pravidelných školení.	
NE	-

P7: Bezpečnostní povědomí zaměstnanců v souladu s jejich pracovní náplní je pravidelně ověřováno.	
NE	-

P7: Dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role je pravidelně kontrolováno.	
NE	-

P7: Je zajištěno předání odpovědností v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role.	
A/N	Předání odpovědností je zajištěno standardně v rámci pracovních smluv zaměstnanců, nicméně konkrétní náležitosti týkající se administrátorů a osob zastávajících bezpečnostní role nejsou nikde kodifikovány.

P7: Účinnost plánu rozvoje bezpečnostního povědomí je vyhodnocována, včetně provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí.	
NE	-

P7: Jsou určena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.	
A/N	Podmínky disciplinárního řízení v případě závažného porušení pracovní kázně, etického kodexu a dalších vnitřních předpisů VUT FP jsou řešeny, nicméně při jejich vzniku nebyly brány v potaz případné okolnosti spojené s kybernetickou bezpečností, zejména na straně administrátorů a osob zastávajících bezpečnostní role.

P7: Jsou vedeny záznamy a přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.	
ANO	Organizace vede a uchovává tyto záznamy.

Požadavky na bezpečnost lidských zdrojů dle § 9 VKB jsou implementovány jen částečně, a to pouze v oblastech, ve kterých se VKB protíná s běžnou praxí v oblasti řízení lidských zdrojů.

3.3.8 Řízení provozu a komunikací

P8: Jsou stanoveny pravidla a postupy, které zohledňují práva a povinnosti uživatelů, administrátorů a osob zastávajících bezpečnostní role.	
A/N	Práva a povinnosti uživatelů a administrátorů jsou na obecné úrovni kodifikována, nicméně je potřeba provést revizi zejména s ohledem na fakt, že zde nejsou zastoupeny bezpečnostní role.

P8: Jsou stanoveny pravidla a postupy, které zohledňují postupy pro spuštění a ukončení chodu systémů, restart nebo jejich obnovení po selhání a pro ošetření chybových stavů nebo mimořádných jevů.	
NE	-

P8: Jsou stanoveny pravidla a postupy, které zohledňují postupy pro sledování kybernetických bezpečnostních událostí a opatření pro ochranu přístupu k jejich záznamům.	
NE	-

P8: Jsou stanoveny pravidla a postupy, které zohledňují pravidla a postupy pro ochranu před škodlivým kódem a technických zranitelností.	
A/N	Oddělení IT se zabývá ochranou před škodlivým kódem a technickými zranitelnostmi, nicméně celý proces není řízen na strategické úrovni.

P8: Jsou stanoveny pravidla a postupy, které zohledňují zejména spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory.	
NE	-

P8: Jsou stanoveny pravidla a postupy, které zohledňují postupy řízení a schvalování provozních změn.	
NE	-

P8: Jsou stanoveny pravidla a postupy, které zohledňují postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.

NE	-

P8: Jsou stanoveny pravidla a postupy, které zohledňují pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu.
NE -

P8: Jsou stanoveny pravidla a postupy, které zohledňují pravidla a postupy pro instalaci technických aktiv.	
A/N	Pravidla a postupy existují, nicméně nepracují např. s požadavky na určení pravidel rozdílných pro jednotlivé úrovně těchto aktiv.

P8: Jsou stanoveny pravidla a postupy, které zohledňují provádění pravidelného zálohování a kontroly použitelnosti provedených záloh.	
A/N	Zálohování a kontrola použitelnosti provedených záloh probíhá, nicméně vzhledem k chybějícímu procesu řízení aktiv nelze jednoznačně určit, zda jsou takto pokryta všechna primární aktiva v určeném rozsahu ISMS.

P8: Jsou stanoveny pravidla a postupy, které zohledňují pravidla a postupy pro zajištění bezpečnosti síťových služeb.	
NE	-

Požadavky na řízení provozu a komunikací dle § 10 VKB jsou implementovány jen částečně, zejména v oblastech, kde jsou příslušné dokumentace a postupy potřebné, bez ohledu na zákonné požadavky. Bez návaznosti na ISMS, které na VUT FP není řízeno, je však nelze považovat za dostatečné.

3.3.9 Řízení změn

P9: V rámci řízení změn informačního a komunikačního systému jsou přezkoumávány jejich možné dopady a jsou určovány významné změny.	
NE	-

P9: Řízení významných změn je dokumentováno.	
NE	-

P9: V rámci významných změn jsou řízena rizika spojená se změnami.	
NE	-

P9: Jsou přijímána opatření pro snížení dopadů spojených s významnými změnami.	
NE	-

P9: Je zajištěno testování významných změn.	
NE	-

P9: Je zajištěno možné navrácení do původního stavu.	
NE	-

Požadavky na řízení změn dle § 11 VKB nejsou implementovány.

3.3.10 Řízení přístupů

P10: VUT FP řídí přístupy na základě provozních a bezpečnostních potřeb k informačnímu a komunikačnímu systému a přijímá opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení.	
NON	-

P10: Přístupy jsou řízeny na základě skupin a rolí.	
NON	-

P10: Přidělovaná přístupová práva a oprávnění, které uživatelé a administrátoři využívají k přístupu do informačního a komunikačního systému mají jedinečný identifikátor.	
NON	-

P10: Jsou přijímaná bezpečnostní opatření pro řízení přístupu k aplikacím a technickým účtům.	
NON	-

P10: Bezpečnostní opatření jsou zřízena pro mobilní zařízení, případně jiná technická zařízení, která nejsou ve správě VUT FP.	
NON	-

P10: VUT FP pravidelně přezkoumává nastavení přístupových oprávnění a jejich rozdělení do přístupových skupin a rolí.	
NON	-

P10: Jsou zajištěny postupy a prostředky pro změnu a odebrání přístupových oprávnění v případě ukončení pracovního poměru nebo změny pracovní pozice.	
NON	-

Požadavky na řízení přístupů dle § 12 VKB nelze ověřit, jelikož jsou centrálně řízeny CVIS (Centrum výpočetních a informačních služeb VUT) a nepodařilo se za tuto oblast zajistit respondenty.

3.3.11 Akvizice, vývoj a údržba

P11: V souvislosti s akvizicí, vývojem a údržbou informačního a komunikačního systému jsou řízena rizika.	
NE	-

P11: V souvislosti s akvizicí, vývojem a údržbou informačního a komunikačního systému jsou řízeny významné změny a jsou testovány před jejich zavedením do provozu.	
NE	-

P11: V souvislosti s akvizicí, vývojem a údržbou informačního a komunikačního systému jsou stanoveny bezpečnostní požadavky.	
NE	-

P11: V souvislosti s akvizicí, vývojem a údržbou informačního a komunikačního systému je zajištěna bezpečnost vývojového a testovacího prostředí.	
NE	-

Požadavky na akvizici, vývoj a údržbu informačních a komunikačních systémů dle § 13 VKB nejsou implementovány.

3.3.12 Zvládání kybernetických bezpečnostních událostí a incidentů

P12: Je zaveden proces detekce a vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů a jsou přiděleny odpovědnosti v rámci těchto činností.

NE	-

P12: Jsou definovány postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu.
NE -

P12: Je zajištěna detekce kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů.
NE -

P12: Je zajištěno, že zaměstnanci i dodavatelé budou oznamovat neobvyklé chování informačního a komunikačního systému a podezření na zranitelnosti.
NE -

P12: Jsou přijímána opatření pro odvrácení a zmírnění dopadu kybernetických bezpečnostních incidentů.
NE -

Požadavky na zvládání kybernetických bezpečnostních událostí a incidentů dle § 14 nejsou implementovány.

3.3.13 Řízení kontinuity činností

P13: V rámci řízení kontinuity činností jsou stanoveny práva a povinnosti administrátorů a osob zastávající bezpečnostní role.
NE -

P13: Jsou vyhodnocovány možné dopady kybernetických bezpečnostních incidentů a v souvislosti s nimi jsou posuzována možná rizika související s ohrožením kontinuity činností.
NE -

P13: Jsou stanoveny cíle řízení kontinuity činností určením: • minimální úrovně poskytovaných služeb, • doby obnovení chodu, • bodu obnovení dat.
NE -

P13: Je stanovena politika řízení kontinuity činností.

NE	-

P13: Jsou zpracovány, aktualizovány a testovány plány kontinuity činností a havarijní plány v souvislosti s provozem informačního a komunikačního systému.	
A/N	Existují dílčí havarijní plány v oblasti obnovy chodu serverů podporujících provoz informačního komunikačního systému. Avšak tyto plány existují samostatně, bez další návaznosti na obecnější proces řízení kontinuity činností.

P13: Jsou realizována opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti.	
NE	-

Požadavky na řízení kontinuity činností dle § 15 VKB nejsou implementovány. Existují jen dílčí havarijní plány, které však nejsou v plném souladu s definovanými požadavky.

3.3.14 Audit kybernetické bezpečnosti

P14: Je prováděn a dokumentován audit kybernetické bezpečnosti: • v rámci rozsahu významných změn, • v pravidelných intervalech alespoň každé 3 roky.	
NE	-

P14: V rámci auditu je sledováno dodržování bezpečnostní politiky, včetně přezkoumání technické shody a výsledky auditu jsou zohledněny v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.	
NE	-

Požadavky na audit kybernetické bezpečnosti dle § 16 VKB nejsou implementovány.

3.3.15 Bezpečnostní politika a bezpečnostní dokumentace

P15: Bezpečnostní politika a bezpečnostní dokumentace jsou pravidelně přezkoumávány a je zajištěno, aby byly aktuální.	
A/N	-

P15: Bezpečnostní politika a bezpečnostní dokumentace je dostupná v listinné nebo elektronické podobě, je komunikována v rámci organizace dotčeným stranám.	
A/N	-

P15: Bezpečnostní politika a bezpečnostní dokumentace je řízena, chráněna z pohledu důvěrnosti, integrity a dostupnosti a je vedena tak, aby informace v ní obsažené byly úplné, čitelné, snadno identifikovatelné a snadno vyhledatelné.	
A/N	-

Požadavky na bezpečnostní politiky a bezpečnostní dokumentace dle § 30 jsou implementovány jen částečně.

Požadavky na související obsah bezpečnostní politiky a bezpečnostní dokumentace dle přílohy č. 5 VKB implementovány nejsou.

3.3.16 Kategorizace kybernetických bezpečnostních incidentů

P16: Kybernetické bezpečnostní incidenty jsou kategorizovány podle významnosti s ohledem na: • dopady obsažené v dopadových určujících kritériích, • počet dotčených uživatelů, • způsobené nebo předpokládané škody, • důležitost dotčených aktiv informačního a komunikačního systému, • dopady na poskytované služby informačního a komunikačního systému, • dopady na služby poskytované jinými informačními a komunikačními systémy, • délku trvání incidentu, • zeměpisný rozsahu dotčené oblasti, • případné další dopady.	
NE	-

Požadavky na kategorizaci kybernetických bezpečnostních incidentů dle § 31 VKB nejsou implementovány.

3.3.17 Reaktivní opatření

P17: VUT FP posuzuje očekávané dopady reaktivního opatření na informační a komunikační systém a na zavedená bezpečnostní opatření a vyhodnotí možné negativní účinky.	
NE	-

P17: VUT FP stanovuje způsoby rychlého provedení tohoto opatření, které minimalizuje možné negativní účinky a určí časový plán jeho provedení.	
NE	-

Požadavky na reaktivní opatření dle § 33 VKB nejsou implementovány.

3.3.18 Kontaktní údaje

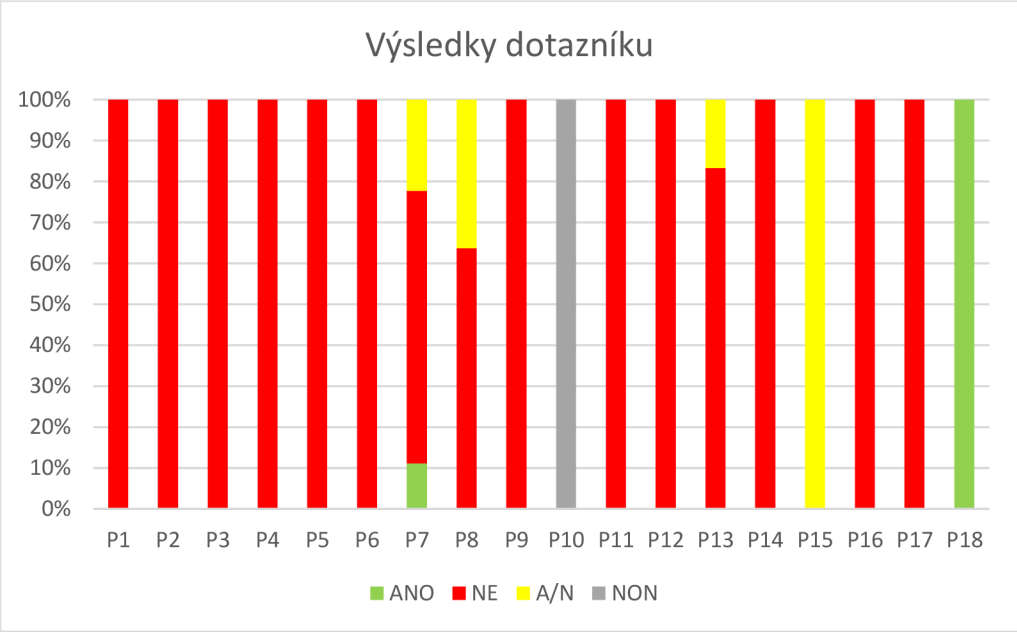
P18: Kontaktní údaje na VUT FP byly oznámeny NÚKIB	
ANO	-

Požadavky na hlášení kontaktních údajů na NÚKIB dle § 34 VKB byly implementovány.

3.4 Vyhodnocení GAP analýzy

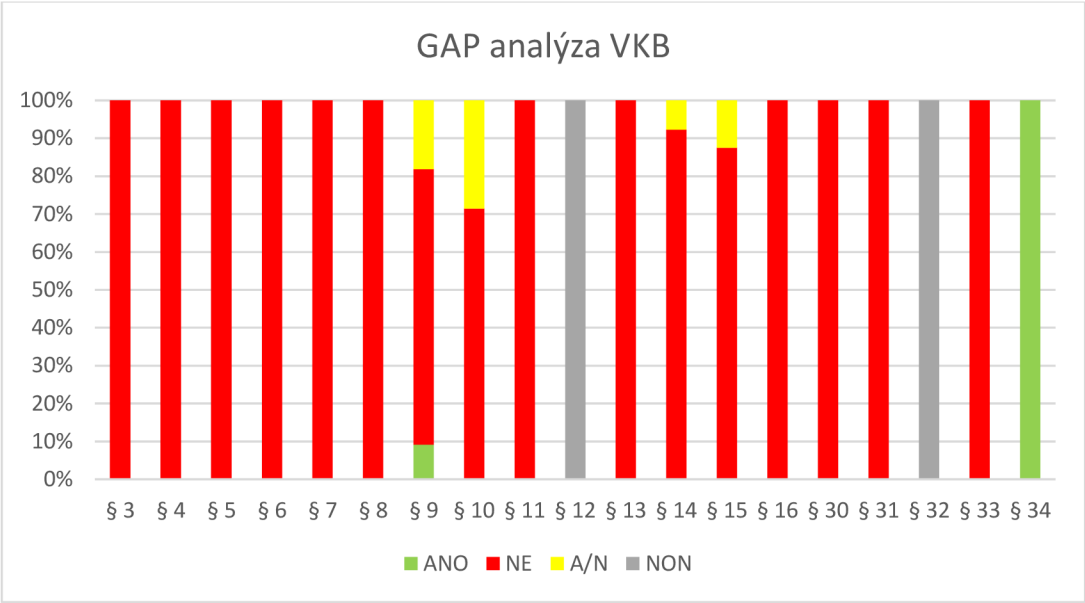
Dotazník byl sestaven agregací požadavků VKB do logických celků tak, aby umožnil snazší formulaci jednotlivých paragrafů, odstavců a písmen.

Z obrázku č. 5 vyplývá, že se podařilo zajistit odpověď na všechna témata P1 až P18, mimo P10, pro které se nepodařilo zajistit adekvátního respondenta.



Obrázek 6: Sloupcový graf shody s VKB na základě zjednodušeného dotazníku (Zdroj: Vlastní zpracování)

Zaznačené odpovědi v dotazníku byly následně interpretovány do prohlášení o aplikovatelnosti, které je obsaženo v příloze II, ze které byla následně analýza výsledků provedena znovu, viz obrázek č. 6.



Obrázek 7: Sloupcový graf interpretace v prohlášení o aplikovatelnosti (Zdroj: Vlastní zpracování)

Porovnáním grafů lze potvrdit, že data byla interpretována správně, jelikož nevznikly výrazné odchylky. § 32, který se týkal hlášení kybernetických bezpečnostních incidentů byl z dotazníku vyřazen poté, co vyšlo najevo, že neexistuje proces pro identifikování a vyhodnocování těchto incidentů. Tím nelze objektivně ohodnotit, zda VUT FP tento požadavek plní nebo ne, a tím byl vyřazen jako nerelevantní.

3.4.1 Shrnutí analýzy

Z výsledků analýzy vyplývá, že VUT FP je z převážné části v nesouladu s legislativními požadavky plynoucí ze ZKB a VKB. Většina oblastí VKB není vůbec řešena, nebo je řešena jen částečně. Oblasti, které jsou řešeny, však nejsou dostatečně zdokumentovány a nepanuje v souvislosti s nimi všeobecné povědomí v tom, jak zapadají do rozsahu ISMS.

To však neznamená, že by se organizace doposud kybernetickou bezpečnostní nijak nezabývala. Chybí jí nicméně řízení na strategické i procesní úrovni. U již implementovaných bezpečnostních opatření tak nebyl brán ohled na to, zda jsou nebo budou v souladu s legislativními požadavky.

Určením VUT FP jako správce významného informačního systému, započala časově omezená lhůta pro uvedení stavu kybernetické bezpečnosti do souladu se ZKB a VKB. Po jejím skončení může být kdykoliv na VUT FP dodáno oznámení o započetí kontroly

ze strany NÚKIB. V nejhorším případě, při zjištění závažných nedostatků, může být vedeno správní řízení za nedodržení zákonných požadavků a při nedodržení nápravných opatření může být za každý jeden bod nesouladu udělena pokuta až ve výši 1 000 000 Kč.

4 VLASTNÍ NÁVRH ŘEŠENÍ A PŘÍNOS PRÁCE

Cílem této kapitoly bude odpovědět na poslední dílčí otázku z úvodu této diplomové práce, tedy:

3. Jaké kroky je potřeba vykonat pro zajištění souladu s legislativními požadavky, za účelem zajištění kybernetické bezpečnosti na VUT FP?

Toho bude dosaženo doporučeními v podobě metodických pokynů, včetně praktických příkladů pro vybrané oblasti, kde byly v během GAP analýzy zjištěny nedostatky.

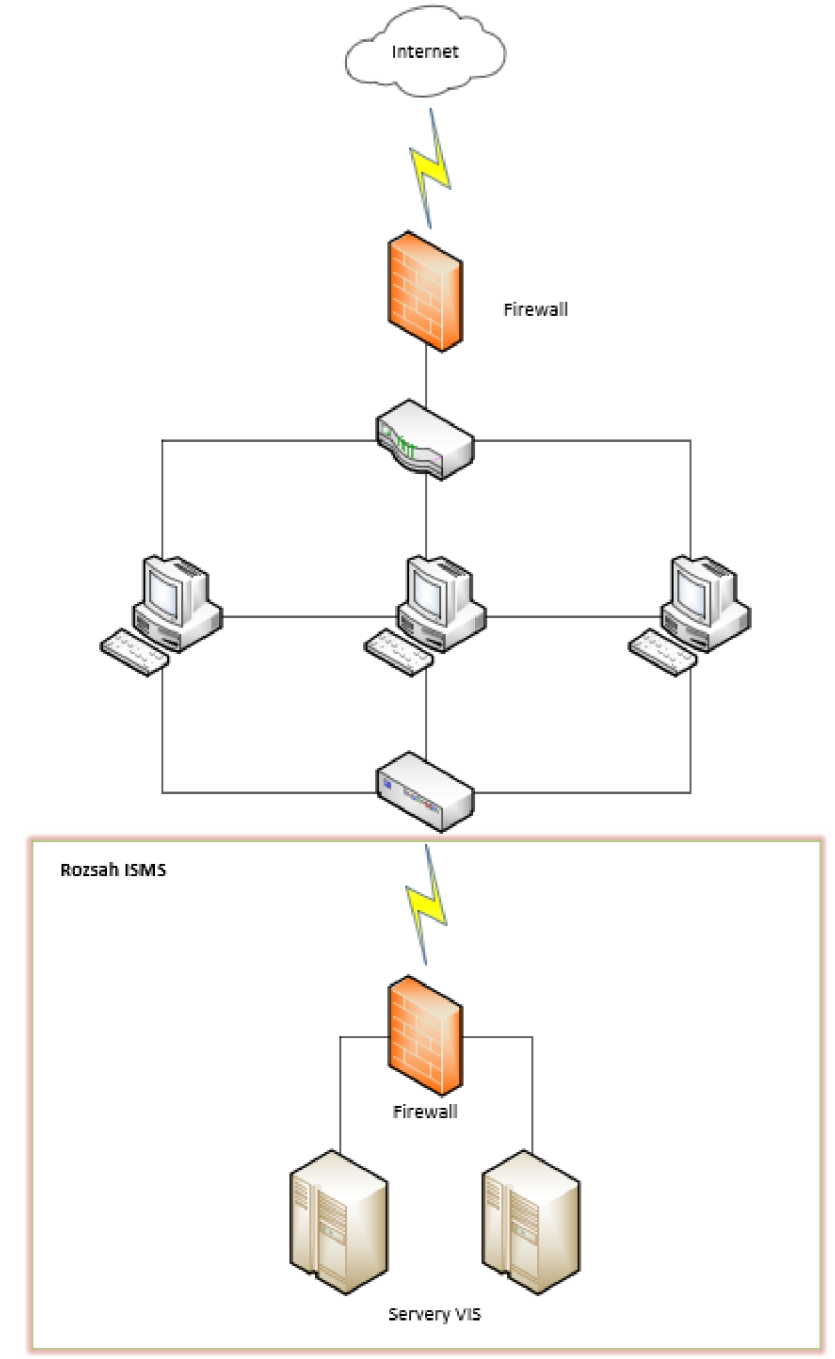
4.1 Určení rozsahu

Do rozsahu ISMS je vždy nutné zahrnout určené systémy dle ZKB, a aktiva a organizační části, které na ně mají vliv z hlediska kybernetické bezpečnosti. To znamená, že mají přímý vliv na výkon jejich služeb v požadovaném rozsahu a kvalitě.

Rozsah ISMS je potřeba vymezit zejména s ohledem na informace a služby, které je nutné zabezpečit. Může být vymezen buď jako rozsah primárních a podpůrných aktiv nebo může být rozsah stanoven na celou organizaci.

Účelem definice rozsahu ISMS je určit ta aktiva a organizační celky, na která musí být aplikována přiměřená bezpečnostní opatření, díky kterým bude zajištěno, že informační a kybernetická bezpečnost bude na takové úrovni, aby je dokázala chránit během celého jejich životního cyklu i s ohledem na externí vazby. Je nezbytné, aby byl rozsah ISMS dokumentovanou informací.

Velmi zjednodušené schéma rozsahu ISMS z hlediska síťové topologie je znázorněno v obrázku č. 7.



Obrázek 8: Příklad rozsahu ISMS pouze na systémy dle ZKB (Zdroj: Vlastní zpracování)

Při určování rozsahu ISMS je však třeba dbát i na další aspekty, které na tomto obrázku nejsou znázorněny.

Fyzický aspekt rozsahu

Fyzickým aspektem rozsahu je myšlen fyzický perimetr, kterým jsou pokryty všechny objekty a prostory, ve kterých je využíván a provozován agendový systém. Nemusí jít

pouze o objekty a prostory, které má ve vlastnictví přímo VUT FP, ale i pronajaté prostory, které vlastní dodavatelé.

Organizační a personální aspekt rozsahu

Organizačními a personálními aspekty rozsahu jsou myšleni:

- Zaměstnanci organizace a další osoby, které VIS využívají k výkonu agendy VUT FP.
- Dodavatelé, kteří se podílejí na dodávkách nejen primárních a podpůrných aktiv, ale i služeb s nimi spojených.

Technologický aspekt rozsahu

Technologickými aspekty rozsahu jsou myšleny:

- Primární aktiva a podpůrná aktiva, která jsou provozována VUT FP a podporují službu určeného VIS.
- Primární aktiva a podpůrná aktiva, která jsou provozována dodavateli a podporují službu určeného VIS.

4.2 Strategické cíle ISMS

Strategické cíle by měly být celkové záměry v oblasti systému řízení bezpečnosti, které vychází z obecné strategie VUT FP, které si organizace sama stanoví a které jsou, pokud možno, specifické, měřitelné, dosažitelné, relevantní a časově vymezené. Tyto cíle by měly být pravidelně vyhodnocovány, aktualizovány a měly by být dokumentovány, včetně způsobů a důkazů jejich naplňování.

Tabulka 1: Příklad stanovených cílů ISMS (Zdroj: Vlastní zpracování)

	Cíl	Cílová hodnota	Měřitelnost	Termín dosažení	Odpovědnost
1	Sestavení výboru pro řízení kybernetické bezpečnosti	Jmenování členů výboru a ustanovení pravidelných schůzí	Zápisy ze zasedání výboru, plnění stanovených cílů	30. 06. 2022	Vrcholové vedení
2	Zmapování aktiv a rizik	Vytvoření konkrétního registru aktiv a rizik, včetně identifikace, ohodnocení a propojení aktiv a rizik	Pravidelné revize a vyhodnocování aktiv a rizik	31. 08. 2022	MKB
3	Zajištění souladu s legislativou	Minimalizovat riziko vyplývající ze vzniku trestněprávní odpovědnosti VUT FP	Ročně: interní audit Kvartálně: Schůze výboru pro KB	31. 12. 2022	Výbor pro KB

4.3 Osoby podílející se na rozvoji kybernetické bezpečnosti a bezpečnostní role

Jedním z prvních kroků, které VUT FP musí v rámci řízení kybernetické bezpečnosti udělat, je stanovit osoby podílející se na rozvoji kybernetické bezpečnosti a bezpečnostní role.

Správce nebo provozovatel významného informačního systému má povinnost ustanovit výbor pro řízení kybernetické bezpečnosti a bezpečnostní role manažera kybernetické bezpečnosti a garantů aktiv. Potřeba podpory vrcholového vedení nicméně přetrvává. Bezpečnostní role architekta kybernetické bezpečnosti a auditora kybernetické bezpečnosti nejsou v tomto případě vyžadovány, nicméně v rámci přístupu dobré praxe zde budou přesto uvedeni jako bezpečnostní role vhodné k obsazení.

Vrcholové vedení

Konečnou odpovědnost za ISMS ve společnosti nese vrcholové vedení. Je nezbytné, aby vrcholové vedení demonstrovalo aktivní podporu ISMS, zabývalo se problematikou kybernetické bezpečnosti a zajistilo adekvátní podmínky bezpečnostním rolím i dalším osobám, které se na rozvoji kybernetické bezpečnosti podílejí.

Příkladem vrcholového vedení VUT FP by mohl být rektor, případně vrcholový orgán či osoby rektorem pověřené se srovnatelnými pravomocemi a odpovědnostmi, které ho však budou pravidelně informovat o stavu kybernetické bezpečnosti.

Výbor pro řízení kybernetické bezpečnosti

Hlavním úkolem výboru pro řízení kybernetické bezpečnosti je implementace a údržba ISMS v působnosti VUT FP. Výbor je odpovědný za řízení a rozvoj kybernetické bezpečnosti. Mezi členy musí být alespoň jeden zástupce vrcholového vedení, nebo jím pověřená osoba a manažer kybernetické bezpečnosti.

Klíčovými činnostmi výboru jsou:

- Tvorba rámce kybernetické bezpečnosti, jeho zásad a směřování (určování cílů ISMS a rozvoj ISMS).
- Určování rolí a odpovědností v ISMS.
- Určování metrik a kontrola dodržování cílů ISMS.
- Pravidelné schůze výboru, přičemž jejich průběh a výstupy z jednání jsou dokumentovány a uchovávány.

Doporučené složení výboru:

- zástupce vrcholového vedení organizace,
- vedoucí úseku bezpečnosti,
- vedoucí úseku ICT,
- vedoucí legislativního úseku,
- vedoucí ekonomického úseku,
- vedoucí personálního úseku,
- manažer kybernetické bezpečnosti a
- architekt kybernetické bezpečnosti.

Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnosti je bezpečnostní role, která je zodpovědná za funkční a procesní řízení celého ISMS. Jedná se o pojící článek mezi vrcholovým vedením VUT FP a zaměstnanci VUT FP, kteří se věnují operativě organizace, a to nejen v oblasti kybernetické bezpečnosti. Je tedy jednotným kontaktním místem v rámci organizace.

Manažer kybernetické bezpečnosti je v tomto ohledu ústřední osobou a měl by mít adekvátní zázemí, potřebné pravomoci, dostatečné zdroje a odpovídající schopnosti a praxi. **Manažer kybernetické bezpečnosti nesmí být odpovědný za výkon rolí v provozu ICT a jeho role musí být striktně oddělena**. To znamená, že manažer kybernetické bezpečnosti nesmí zároveň zastávat tuto bezpečnostní roli a roli např. vedoucího ICT úseku.

Klíčovými odpovědnostmi manažera kybernetické bezpečnosti jsou:

- Odpovědnost za řízení ISMS.
- Podávání pravidelných hlášení pro vrcholové vedení.
- Udržování pravidelné komunikace s vrcholovým vedením.
- Předávání zpráv o hodnocení aktiv a rizik, plánu zvládání rizik a prohlášení o aplikovatelnosti na výboru kybernetické bezpečnosti.
- Účast na vytváření, hodnocení, výběru, řízení a ukončování dodavatelských vztahů v oblasti ICT.
- Komunikace s národním CERT.
- Odpovědnost za proces řízení aktiv a rizik.
- Koordinace v oblasti řízení kybernetických bezpečnostních incidentů.
- Určování vhodnosti bezpečnostních opatření a jejich vyhodnocování.

Mezi znalosti, které by manažer kybernetické bezpečnosti měl mít, patří:

- Normy řady ISO/IEC 2700 a další normy v oblasti bezpečnosti a ICT.
- Přehled o operačních systémech, databázích, aplikacích, datových sítích s důrazem na bezpečnost.
- Proces řízení rizik.
- Proces řízení kontinuity činností.
- Přehled o relevantních regulatorních požadavcích, zejména ZKB a VKB.
- Dobrý přehled a znalost prostředí VUT FP.

Manažer kybernetické bezpečnosti by dále měl splňovat podmínku 3 let praxe v oboru informační nebo kybernetické bezpečnosti, nebo absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti.

Garant aktiva

Garant aktiva je bezpečnostní role, která je zodpovědná za rozvoj a monitorování aktiva, ke kterému je přiřazena. Garantem by měly být osoby, které mají detailní znalost daného aktiva a v praxi s ním pracují nebo ho spravují. Jedná se také o klíčovou bezpečnostní roli z hlediska řízení aktiv a rizik, jelikož se přímo podílí na jejich hodnocení ve spolupráci s manažerem kybernetické bezpečnosti.

V praxi se nejčastěji jedná o administrátory, vedoucí pracovníky útvarů, či experty na konkrétní HW, SW.

Architekt kybernetické bezpečnosti

Hlavním úkolem architekta kybernetické bezpečnosti je zajištění bezpečné architektury informačních systémů s ohledem na potřeby v oblasti ISMS. Tato bezpečnostní role by neměla být zaměňována s architektem ICT, jehož úkolem je návrh konfigurací HW a SW v rámci optimalizace provozu informačních systémů. Nicméně sloučení těchto rolí není v rozporu s VKB, které se vyjadřuje k oddělení těchto rolí jen v rámci dobrovolného doporučení.

Klíčovými odpovědnostmi architekta kybernetické bezpečnosti jsou:

- Odpovědnost za návrhy implementací bezpečnostních opatření.
- Zajištění bezpečné architektury.

Mezi znalosti, které by architekt kybernetické bezpečnosti měl mít, patří:

- Architektura a její návrh v oblasti informačních a komunikačních systémů.
- Znalost HW, SW, operačních systémů a jeho komponentů, nástrojů a související architektury.
- Bezpečnost komunikací a sítí.
- Řízení identit, přístupů a souvisejících nástrojů.
- Testování bezpečnosti.
- Provozní bezpečnost.
- Integrace ICT do agendy VUT FP.
- Dobrý přehled a znalost prostředí VUT FP.

Architekt kybernetické bezpečnosti by dále měl splňovat podmínku 3 let praxe v oboru informační nebo kybernetické bezpečnosti, nebo absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti.

Auditor kybernetické bezpečnosti

Auditor kybernetické bezpečnosti je bezpečnostní role, která je zodpovědná za provádění auditu kybernetické bezpečnosti. Základní podmínkou je, aby byl auditor nestranný a nezávislý, což znamená, že je to bezpečnostní role neslučitelná s rolí manažera kybernetické bezpečnosti a rolí architekta kybernetické bezpečnosti. Zároveň by tato role neměla být v organizační struktuře zařazena do oddělení, které jsou odpovědné za provoz ICT. Hlavní pracovní náplní auditora by mělo být zkoumání míry souladu ISMS s definovanými požadavky VKB, případně zkoumání míry souladu s jinými normami, které jsou ve strategii VUT FP.

Vzhledem k tomu, že audity jsou spíše nárazová činnost, bývá tato role často outsourcována dodavatelsky, případně jsou osoby v oddělení interního auditu organizace proškolovány pro výkon této činnosti, pokud takové oddělení existuje.

Klíčovými odpovědnostmi auditora kybernetické bezpečnosti jsou:

- Plánování auditů kybernetické bezpečnosti.
- Provádění plánovaných auditů, včetně vedení související dokumentace.
- Sdělování výsledků auditů a návrhy doporučení pro jejich řešení.
- Zpracování závěrečných zpráv a prezentace zjištění.
- Následná kontrola bezpečnostních opatření.
- Příprava a realizace opakovaných auditů.

4.4 Řízení aktiv

Z definice slova aktivum vyplývá, že to je vše, co má pro jeho vlastníka nějakou hodnotu. Z hlediska kybernetické bezpečnosti odlišujeme aktiva na primární a podpůrná. V rámci ISMS se řídí ta aktiva, která se nachází v jeho rozsahu. Proto je v této fázi nutné již mít jasně definovaný rozsah.

Aktiva je možno seskupovat do tzv. typových aktiv, což jsou skupiny aktiv s podobnými vlastnostmi, které nemůžeme nebo nechceme jednotlivě vyjmenovávat. Je důležité si

uvědomit, že takto sloučená aktiva si musí být natolik podobná, abychom mohli jednoznačně dokázat, že na ně působí stejné hrozby, zranitelnosti a platí pro ně stejná bezpečnostní opatření. Tato aktiva se musí hodnotit stejně z pohledu důvěrnosti, dostupnosti a integrity. U podpůrných aktiv je třeba také zohledňovat jejich vazby na primární aktiva. Vytvoření typového aktiva nesmí vést k tomu, že výsledné hodnocení bude netransparentní nebo zkreslené.

Řízení aktiv je kontinuální proces, který je nutné neustále zlepšovat. Vzhledem k tomu, že VUT FP se doposud mapováním aktiv nezabývalo, je doporučeno postupovat v tomto ohledu po iteracích. Tedy začít větším množstvím typových aktiv a pravidelnými revizemi jít do co největšího detailu. Je potřeba ale dbát na to, aby celý proces byl stále řiditelný, tedy aby osoby odpovědné za řízení aktiv byly schopny prokazatelně aktiva identifikovat, evidovat, hodnotit a aktualizovat. Všechny tyto kroky musí být také dokumentovány ve formě metodiky pro identifikaci a hodnocení aktiv a jejich garantů. Tato metodika by měla být návodná, srozumitelná a jednoznačná tak, aby bylo proces opakovatelný, přezkoumatelný a vedl za stejných podmínek ke stejným výsledkům bez závislosti na tom, kdo tento proces provádí.

4.4.1 Identifikace primárních aktiv

Za primárními aktivy v organizaci můžeme vidět informace, procesy a služby.

Informace:

- Vitální pro plnění poslání společnosti.
- Strategické údaje.
- Osobní údaje.
- Informace, které jsou zpracovávány v rámci agendy určeného VIS.

Procesy a služby:

- Jejichž ztráta nebo omezení může znemožnit výkon agendy VUT FP.
- Nutné pro to, aby VUT FP mohlo naplňovat smluvní, právní a regulační požadavky.

Při identifikaci primárních aktiv lze vycházet kromě určeného VIS, například z prozkoumání hlavní činnosti organizace. Klíčovým krokem jsou tedy rozhovory

s vedoucími pracovníky jednotlivých úseků VUT FP. Je vhodné začít u účelu VIS, např. evidování a zpracování požadavků související s přijímáním studentů. Z účelu tedy lze odvodit první primární aktivum, kterým může být přijímací řízení. V souvislosti s touto službou lze hledat informace, které daná služba zpracovává, např. formuláře, dopisy, osobní údaje, výsledky řízení atd.

V případech, kdy nelze jednoznačně identifikovat primární aktiva z informací, které služba zpracovává, je možné pracovat i s primárním aktivem typu služba. Za zpracování informací, tedy poskytnutí služby, se v tomto případě počítá i prosté zobrazení, např. vizualizace v uživatelském rozhraní, nebo přehrání zvuku.

Otázky, které mohou pomoci VUT FP v identifikaci primárních aktiv:

- Je služba určena podle ZKB?
- Jaký je účel agendy nebo informačního systému?
- Jaké jsou klíčové procesy, agendy nebo informační systémy organizace?
- Jací jsou klíčoví zákazníci či uživatelé organizace?
- Bez jakých informací nebo procesů nelze vykonávat agendu organizace?
- S jakými osobními údaji, citlivými daty nebo obchodními tajemstvími organizace nakládá?
- Jsou s existencí organizace spojeny nějaké zákonné nebo smluvní požadavky?
- Může mít narušení bezpečnosti aktiv vliv na bezpečnost či zdraví osob?
- Hrozí v případě narušení bezpečnosti aktiv možnost finanční ztráty či pokuty a sankce?

4.4.2 Evidence primárních aktiv

Všechna primární aktiva, která se nacházejí v rozsahu ISMS, musí být odpovědnou osobou zaznamenávána v dokumentované podobě. Konkrétní podoba evidence aktiv není definována a je na vlastním zvážení každé organizace.

Příklad atributů, které by mohlo VUT FP evidovat:

- ID aktiva,
- název,
- garant aktiva,

- hodnocení aktiva z hlediska důvěrnosti, dostupnosti a integrity,
- detailní popis a další informace o aktivu jako uživatelé, relevantní legislativa či normy atd.

Tabulka 2: Jednoduchý příklad evidence primárních aktiv (Zdroj: Vlastní zpracování)

ID	Primární aktivum	Kategorie	Specifikace	Garant aktiva
S1	Přijímání přihlášek ke studiu	Služba	Zajišťování procesu přijímání přihlášek ke studiu	Administrátor systému
I1	Seznam přihlášek ke studiu	Informace	Evidence přihlášek	Vedoucí studijního oddělení
I2	Rozhodnutí o nepřijetí	Informace	Evidence rozhodnutí	Vedoucí studijního oddělení

4.4.3 Určení garantů primárních aktiv

Primární aktiva musí mít určeny své garanty a tyto garanty evidovat. Manažerovi kybernetické bezpečnosti by v této činnosti mohl pomoci např. organizační řád. Stanovení těchto garantů by mělo být formalizováno, např. jmenováním či dodatkem ve smlouvě a mělo by být schváleno vrcholovým vedením nebo výborem kybernetické bezpečnosti.

Garanti jsou vybíráni na základě jejich pracovního zařazení, odborných a procesních znalostí přiřazeného aktiva. Garant musí být schopen na základě svých zkušeností a na základě možných dopadů ohodnotit aktivum tak, aby byla osoba odpovědná za hodnocení rizik schopna tato rizika vyhodnotit a řídit.

4.4.4 Hodnocení primárních aktiv

Při hodnocení primárního aktiva v kategorii služba nelze provést hodnocení bez toho, aby byla zvážena hodnota informací, se kterými tato služba pracuje. Proto je potřeba nejdříve hodnotit primární aktiva v kategorii informace, které služba poté zpracovává. Služba poté přebere nejvyšší hodnoty jednotlivých atributů, mezi které patří dostupnost, důvěrnost a integrita, z navázaných primárních aktiv typu informace.

Výslednou hodnotou procesu hodnocení primárních aktiv by měl být dopad na aktivum v případě realizace hrozby. Pokud bude využit v rámci VKB doporučený vzorec pro

výpočet dopadu, kombinací hodnot důvěrnosti, dostupnosti a integrity, pak musíme daná aktiva ohodnotit právě z hlediska těchto aspektů.

$$Dopad = důvěrnost \times dostupnost \times integrita$$

VKB dále doporučuje, aby byla využita stupnice o čtyřech stupních. Při posuzování aktiv je nutné uvažovat o nejhorším možném scénáři a nebrat v úvahu jakákoliv doposud aplikovaná bezpečnostní opatření.

Důvěrnost

Opatření v oblasti důvěrnosti chrání informace před neoprávněným přístupem a zneužitím. Většina informačních systémů obsahuje informace, které mají určitý stupeň citlivosti. Mohou to být obchodní informace, které by konkurenti mohli využít ve svůj prospěch, nebo osobní informace týkající se zaměstnanců, zákazníků nebo klientů organizace.

Důvěrné informace mají často hodnotu, a proto jsou systémy často vystaveny útokům, když zločinci hledají zranitelnosti, které by mohli zneužít. Mezi vektory hrozeb patří přímé útoky, jako je krádež hesel a zachycení síťového provozu a vícevrstvé útoky, jako je sociální inženýrství a phishing. Ne všechna porušení důvěrnosti jsou úmyslná. Mezi několik typů běžných náhodných porušení patří zasílání citlivých informací e-mailem nesprávnému příjemci, publikování soukromých dat na veřejné webové servery a ponechání důvěrných informací zobrazených na bezobslužném počítačovém monitoru.

Existuje mnoho protiopatření, která organizace zavádějí, aby byla zajištěna důvěrnost. Hesla, seznamy řízených přístupů a postupy ověřování pomocí softwaru pro řízení přístupu k informacím. Tyto metody řízení přístupu jsou doplněny používáním šifrování k ochraně informací, ke kterým lze přistupovat navzdory kontrolním prvkům, jako jsou například e-maily. Mezi další protiopatření na ochranu důvěrnosti patří organizační opatření, jako jsou zásady a školení, stejně jako fyzické kontroly, které lidem brání v přístupu k zařízením a vybavení.

Tabulka č. 3 znázorňuje příklad toho, jak by mohla vypadat stupnice hodnocení důvěrnosti pro sledovaná aktiva.

Tabulka 3: Stupnice pro hodnocení důvěrnosti (Zdroj: Vlastní zpracování)

Hodnocení důvěrnosti		
Úroveň		Popis
Nízká	1	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:WHITE.
Střední	2	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.
Vysoká	3	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER.
Kritická	4	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED nebo TLP:AMBER.

Dostupnost

Aby byl informační systém užitečný, musí být dostupný oprávněným uživatelům. Opatření dostupnosti chrání včasný a nepřerušovaný přístup do systému. Některé z nejzásadnějších hrozeb pro dostupnost nemají škodlivý charakter a zahrnují selhání hardwaru, neplánované výpadky softwaru a problémy s šířkou pásma sítě. Škodlivé útoky zahrnují různé formy sabotáže, které mají způsobit škodu organizaci tím, že uživatelům odepře přístup k informačnímu systému.

Dostupnost a odezva webových stránek je pro mnoho organizací vysokou prioritou. Narušení dostupnosti poskytovaných služeb i na krátkou dobu může vést ke ztrátě příjmů, nespokojenosti uživatelů a poškození pověsti. Jedním z nejběžnějších způsobů externího narušení dostupnosti patří tzv. Denial of Service (DoS) útok. Je to metoda, kterou hackeři často používají k narušení webové služby. Při útoku DoS hackeři zaplaví server nadbytečnými požadavky, čímž server zahltí a znehodnotí službu pro legitimní uživatele. V průběhu let poskytovatelé služeb vyvinuli sofistikovaná protiopatření pro detekci a ochranu před DoS útoky, ale hackeři také stále získávají na sofistikovanosti, a tak tyto typy útoků zůstávají trvalým problémem.

Protiopatření týkající se dostupnosti k ochraně dostupnosti systému jsou stejně četné jako způsoby ohrožení dostupnosti. Systémy, které mají vysoké požadavky na nepřetržitou dobu dostupnosti, by měly mít značnou hardwarovou redundanci s okamžitě dostupnými záložními servery a datovým úložištěm. U velkých podnikových systémů je běžné mít redundantní systémy na samostatných fyzických lokalitách. Měly by být k dispozici softwarové nástroje pro sledování výkonu systému a síťového provozu. Protiopatření na ochranu před útoky DoS zahrnují firewally a směrovače.

Tabulka č. 4 znázorňuje příklad toho, jak by mohla vypadat stupnice hodnocení dostupnosti pro sledovaná aktiva.

Tabulka 4: Stupnice pro hodnocení dostupnosti (Zdroj: Vlastní zpracování)

Hodnocení dostupnosti		
Úroveň		Popis
Nízká	1	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
Střední	2	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.
Vysoká	3	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.
Kritická	4	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.

Integrita

Opatření v oblast integrity aktiv chrání informace před neoprávněnou změnou. Tato opatření poskytují záruku přesnosti a úplnosti údajů. Potřeba chránit informace zahrnuje jak data, která jsou uložena v systémech, tak data, která jsou přenášena mezi systémy, jako je e-mail. Při zachování integrity je nejen nutné řídit přístup na úrovni systému, ale dále zajistit, aby uživatelé systému mohli měnit pouze informace, které jsou oprávněni měnit.

Existuje mnoho protiopatření, která lze zavést na ochranu integrity. Kontrola přístupu a přísné podmínky autentizace mohou pomoci zabránit autorizovaným uživatelům v provádění neoprávněných změn. Ověření hash a digitální podpisy mohou pomoci zajistit, že transakce jsou autentické a že soubory nebyly změněny nebo poškozeny. Pro ochranu

integrity dat jsou stejně důležité administrativní kontroly, jako je oddělení odpovědností a školení.

Tabulka č. 5 znázorňuje příklad toho, jak by mohla vypadat stupnice hodnocení integrity pro sledovaná aktiva.

Tabulka 5: Stupnice pro hodnocení integrity (Zdroj: Vlastní zpracování)

Hodnocení integrity		
Úroveň		Popis
Nízká	1	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.
Střední	2	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.
Vysoká	3	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.
Kritická	4	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.

Dopad

Dopad vyjadřuje škodu, která v případě narušení bezpečnosti informací (důvěrnost, dostupnost, integrita) vznikne na daném aktivu.

Tabulka č. 6 znázorňuje příklad toho, jak by mohla vypadat interpretace výsledné hodnoty dopadu pro sledovaná aktiva. Kvalitativní i kvantitativní kritéria pro jednotlivé úrovně dopadů by si mělo VUT FP vyhodnotit na základě vlastních potřeb ochrany bezpečnosti informací.

Tabulka 6: Stupnice interpretace výsledné hodnoty dopadu (Zdroj: Vlastní zpracování)

Hodnocení dopadu		
Úroveň		Popis
Nízká	1	Dopad je v omezeném časovém období a malého rozsahu, nesmí být katastrofický. Rozsah případných škod nepřesahuje (alespoň jedno kritérium): a) 10 zraněných osob s následnou hospitalizací po dobu delší než 24 hodin. b) Finanční nebo materiální ztráty do 5 000 000 Kč. c) Představuje dopad na uživatele s rozsáhlým omezením služeb postihující nejvýše 250 osob.
Střední	2	Dopad je omezeného rozsahu a v omezeném časovém období. Rozsah případných škod se pohybuje v rozmezí: a) Do 10 mrtvých nebo od 11 do 100 osob s následnou hospitalizací po dobu delší než 24 hodin. b) Finanční nebo mateirální zráty od 5 000 000 kč do 50 000 000 Kč. c) Představuje dopad na veřejnost s rozsáhlým omezením služeb postihující od 251 do 2 500 osob.
Vysoká	3	Dopad je omezeného rozsahu, ale trvalý nebo katastrofický. Rozsah případných škod se pohybuje v rozmezí: a) Od 11 do 100 mrtvých nebo od 101 do 100 osob s následnou hospitalizací po dobu dělší než 24 hodin. b) Finanční nebo materiální ztráty od 50 000 000 Kč do 500 000 000 Kč. c) Představuje dopad na veřejnost s rozsáhlým omezením služeb postihující od 2 501 do 25 000 osob.
Kritická	4	Dopad je ložného rozsahu, je trvalý a katastrofický. Rozsah případných škod se pohybuje v rozmezí: a) 101 a více mrtvých a 1001 a více osob s následnou hospitalizací po dobu delší než 24 hodin. b) Finanční nebo materiální ztráty převyšující 500 000 000 Kč. c) Představuje dopad na veřejnost s rozsáhlým omezením služeb postihující více než 25 000 osob.

Dle VKB vyžaduje, aby byly během hodnocení primárních aktiv posouzeny minimálně vybrané oblasti, které jsou definovány ve VKB § 6 odst. 2 písm. a) až j).

§ 4, odstavec 2 vyhlášky o kybernetické bezpečnosti vyžaduje: *„při hodnocení důležitosti primárních aktiv je třeba posoudit alespoň:*

a) rozsah a důležitost osobních údajů, zvláštních kategorií 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 a 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.“

Hodnocení aktiv probíhá na společném jednání MKB a garanta aktiva. Před tímto jednáním je vhodné, seznámit garanty s metodikou identifikace a hodnocení aktiv, pokud tak již nebylo učiněno v rámci rozvoje bezpečnostního povědomí bezpečnostních rolí. Za finální hodnocení by měl být odpovědný MKB, jelikož na rozdíl od garanta disponuje holistickým pohledem na oblast řízení aktiv a může tak korigovat případné nadhodnocování nebo podhodnocování jednotlivých hodnot aktiva. Z této schůzky by měl být evidován alespoň stručný záznam o jednání, díky kterému bude možná zpětná dohledatelnost.

V průběhu schůzky může MKB využít tyto příklady otázek:

- Jaký bude dopad na aktivum v případě narušení dostupnosti? Představte si, že vaše aktivum nebude dostupné v rámci týdnů až měsíců, co tím pádem hrozí?
- Může mít narušení integrity vliv na ochranu osobních údajů? Představte si, že neznámý útočník pozmění osobní údaje všech studentů v databázi.

Tyto otázky je potřeba položit u všech atributů, tedy důvěrnost, dostupnost a integrita, a pro všechny oblasti dopadů, které jsou uvedené ve VKB § 6 odst. 2.

4.4.5 Identifikace podpůrných aktiv

Podpůrná aktiva jsou aktiva, která jsou potřebná pro správnou funkčnost, zpracování a uchování primárních aktiv. Sama o sobě hodnotu pro organizaci netvoří.

Možné kategorie podpůrných aktiv jsou:

- technické vybavení,
- programové vybavení,
- komunikační prostředky,
- objekty,
- lidské zdroje,
- dodavatelé a externí systémy a služby.

Technické vybavení

Do kategorie technického vybavení můžeme zařadit fyzické komponenty informačních systémů nebo jejich částí. Mezi typické příklady patří pracovní stanice, datová úložiště, servery nebo mobilní zařízení.

Programové vybavení

Do kategorie programového vybavení můžeme zařadit veškeré programy a aplikace, které jsou spustitelné na technickém vybavení a komunikačních prostředcích. Díky programovému vybavení lze technické vybavení a komunikační prostředky ovládat a s jejich pomocí tak vykonávat agendu organizace. Mezi typické příklady patří operační systémy, firmware, kancelářské balíky atd.

Komunikační prostředky

Do kategorie komunikačních prostředků můžeme zařadit zařízení a komponenty, které umožňují spojení jednotlivých prvků technického vybavení a díky tomu tak vytváří síť. Mezi typické příklady patří drátové i bezdrátové připojení a veškeré komponenty, které jsou potřebné pro jejich funkčnost. Nepatří sem však aktivní prvky, jako např. směrovače a přepínače.

Objekty

Do kategorie objektů řadíme jednoduše všechny fyzické prostory, ve kterých se informační systémy nebo jejich součástí nachází. Mezi typické příklady patří areály, objekty, inženýrské sítě atd.

Lidské zdroje

Do kategorie lidských zdrojů řadíme všechny zaměstnance a externí pracovníky, kteří mají vliv na informační systém nebo jeho částí. Mezi typické příklady patří uživatel, administrátoři, vývojáři, bezpečnostní role, vedení organizace i personál dodavatele.

Externí systémy a služby

Do kategorie externích systémů a služeb spadají všechny externí systémy a služby, které jsou kritické pro zajištění funkčnosti informačního systému nebo jeho součástí. Mezi typické příklady patří dodávky elektřiny nebo certifikační služby.

Při identifikaci podpůrných aktiv je potřeba zkoumat potřeby funkčnosti primárního aktiva.

Otázky, které mohou pomoci VUT FP v identifikaci podpůrných aktiv:

- Co všechno je nezbytné pro to, aby bylo primární aktivum dostupné?
- Kde jsou podpůrná aktiva umístěna?
- Kdo je odpovědný za technickou správu aktiva?
- Kdo jsou dodavatelé jednotlivých kategorií podpůrných aktiv?

Hlavním problémem při identifikaci podpůrných aktiv je zvolení správného měřítka detailu. Pokud je detail příliš malý, tedy pokud jsou skupinová aktiva příliš rozsáhlá, může organizace ztrácet dostatečnou míru detailu, a tím kompromitovat celkovou bezpečnost aktiv. Pokud je detail příliš velký, organizace nemusí být schopna aktiva adekvátně řídit v důsledku nedostatečných kapacit.

4.4.6 Evidence podpůrných aktiv

Podobně jako je tomu u primárních aktiv, je nezbytné vést evidenci podpůrných aktiv.

Příklad atributů, které by mohlo VUT FP evidovat:

- ID aktiva,
- název,
- garant aktiva,
- hodnocení aktiva z hlediska důvěrnosti, dostupnosti a integrity,
- detailní popis a další informace o aktivu jako uživatelé, které agendy je využívají, jejich dodavatel atd.

Tabulka 7: Jednoduchý příklad evidence podpůrných aktiv (Zdroj: Vlastní zpracování)

ID	Podpůrné aktivum	Kategorie	Popis	Garant aktiva
P1	Operační systém Windows 10	Programové vybavení	-	Administrátor
P2	Aplikační server	Technické vybavení	Standalone server	Administrátor
P3	Office 365	Externí služby	Licence	Dodavatel

4.4.7 Určení garantů podpůrných aktiv

Stejně jako u primárních aktiv, musí mít podpůrná aktiva přiřazeny a evidovány své garanty. Jejich určování také probíhá ve spolupráci s výborem kybernetické bezpečnosti nebo vrcholovým vedením a formalizace jmenování probíhá také stejným způsobem.

Garanty podpůrných aktiv jsou často zaměstnanci ICT, kteří jsou zodpovědní za daný prvek. U podpůrných aktiv v kategorii dodavatelů a externích služeb to jsou zaměstnanci odpovědní za smluvní vztah.

4.4.8 Hodnocení podpůrných aktiv a určení jejich vazeb na primární aktiva

Proces hodnocení podpůrných aktiv musí být identický jako v případě primárních aktiv. Nejprve je tedy nutno posoudit jejich hodnocení a určit dopad narušení bezpečnosti informací. Opět tedy platí, že podpůrná aktiva by měla být ohodnocena z hlediska důvěrnosti, dostupnosti a integrity, za využití stejného vzorce pro výpočet dopadu v případě realizace hrozby, stejně jako u primárních aktiv. Také zde platí stejné doporučení pro jejich ohodnocení do čtyř úrovní.

Při hodnocení podpůrných aktiv je nezbytné zohlednit jejich vazby na primární aktiva. S ohledem na aktuální stav VUT FP v oblasti řízení aktiv bude nejefektivnější zvolit metodu, kdy podpůrná aktiva přebírají automaticky nejvyšší hodnoty důvěrnosti, dostupnosti a integrity z primárních aktiv, na které jsou vázána. To znamená, že pokud má jedno podpůrné aktivum více primárních aktiv, které jsou závislé na jeho chodu, přebere v každém tomto aspektu právě nejvyšší hodnotu, které tato primární aktiva dosahují. Nevýhodou tohoto přístupu je nicméně skutečnost, že hodnoty podpůrných aktiv mohou být zkreslené a může docházet k jejich nadhodnocení a případným neúměrným nákladům na zajišťování jejich bezpečnosti.

4.5 Řízení rizik

Řízení rizik bezpečnosti informací je strukturovaný přístup, který je založen na neustále se opakujícím procesu zlepšování. Cílem je snížit jednotlivá rizika na takové úrovně, které jsou pro VUT FP akceptovatelné a mít i nadále přiměřenou jistotu, že v dynamicky se měnícím světě zůstávají rizika bezpečnosti informací trvale na akceptovatelné úrovni.

Všechny postupy a výstupy, které se týkají procesu řízení rizik musí být v dokumentované podobě, tedy v metodice pro hodnocení rizik, včetně stanovení kritérií pro jejich akceptovatelnost. Stejně jako v případě řízení rizik by měla být metodika dostatečně návodná, srozumitelná a jednoznačná tak, aby byl celý proces opakovatelný, přezkoumatelný a aby vedl za stejných podmínek ke stejným výsledkům bez závislosti na konkrétní osobě.

4.5.1 Katalog zranitelností

Zranitelnost je vlastnost aktiva, jeho nedostatek nebo slabina, která může být zneužita hrozbami a generovat tak nežádoucí vliv. Zranitelnost představuje citlivost aktiva vzhledem ke konkrétní hrozbě.

VKB vyžaduje, aby byl vytvořen katalog zranitelností, který je minimálně v rozsahu přílohy č. 3 VKB, která obsahuje jednotlivé kategorie zranitelností. Je doporučeno, aby VUT FP zvážilo existenci i dalších zranitelností, které v katalogu nejsou uvedeny, ale jsou pro jeho prostředí relevantní.

Příloha č. 3 vyhlášky o kybernetické bezpečnosti udává následující výčet zranitelností:

„*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,

13. neschopnost včasného odhalení pochybení ze strany zaměstnanců.“

Praktický příklad katalogu zranitelností lze nalézt v příloze III.

4.5.2 Katalog hrozeb

Hrozba je událost nebo aktivita, která ovlivňuje bezpečnost a má potenciál způsobit škodu. Může být úmyslná, neúmyslná, nebo vzniknout vyšší mocí.

VKB vyžaduje, aby byl vytvořen katalog hrozeb, který je minimálně v rozsahu přílohy č. 3 VKB, která obsahuje jednotlivé kategorie hrozeb. Je doporučeno, aby VUT FP zvážilo existenci i dalších hrozeb, které v katalogu nejsou uvedeny, ale jsou pro jeho prostředí relevantní.

Příloha č. 3 vyhlášky o kybernetické bezpečnosti udává následující výčet hrozeb:

„*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).“

Praktický příklad katalogu hrozeb lze nalézt v příloze IV.

4.5.3 Vzorec pro výpočet rizika

Existuje více způsobů, kterými lze získat hodnotu rizika, nicméně VKB doporučuje využít níže popsanou metodu, která je v souladu s metodikou řízení aktiv.

$$Riziko = dopad \times hrozba \times zranitelnost$$

Dopad

Jak již byl popsán v předchozích kapitolách, včetně způsobu jeho výpočtu, hodnota dopadu vyjadřuje škodu, která v případě narušení bezpečnosti informací (důvěrnost, dostupnost, integrita), vznikne na daném aktivu.

Hrozba

Dnešní kybernetické prostředí se zmítá nekonečným proudem potenciálních hrozeb – od malwaru, který do vašeho softwaru zasazuje nebezpečné spustitelné soubory, a ransomwaru, který uzamkne systémy, až po speciálně cílené útoky hackerů. Všechny tyto hrozby hledají cestu dovnitř, zranitelnost ve vašem prostředí, kterou mohou zneužít. Některé hrozby však mají větší potenciál pro zneužití než jiné.

Dle tabulky č. 8, u hrozeb hodnotíme pravděpodobnost, s jakou nastane.

Tabulka 8: Hodnocení hrozeb (Zdroj: Vlastní zpracování)

Hodnocení hrozeb		
Úroveň		Popis
Nízká	1	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	2	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	3	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	4	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Zranitelnost

Zranitelnosti jsou slabá místa v aktivech – slabiny, které je otevírají potenciálním hrozbám a zvýšenému riziku.

Dle tabulky č. 9, u zranitelností hodnotíme pravděpodobnost, s jakou bude zneužita.

Tabulka 9: Hodnocení zranitelností (Zdroj: Vlastní zpracování)

Hodnocení zranitelností		
Úroveň		Popis
Nízká	1	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	2	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	3	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	4	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.

4.5.4 Kritéria pro akceptovatelnost rizik

Kritéria pro akceptovatelnost znamenají tzv. „risk appetite“ organizace. Ten stanovuje vrcholové vedení a mělo by představovat hranici mezi riziky, které je organizace schopna přijmout a riziky, které musí být ošetřeny bezpečnostními opatřeními, jelikož je jejich realizace příliš pravděpodobná nebo jsou dopady příliš závažné.

Tabulka 10: Kritéria pro akceptovatelnost rizik (Zdroj: Vlastní zpracování)

Hodnocení rizik			
Úroveň		Popis	Proces zvládání rizika
Nízká	< 16	Riziko je považováno za akceptovatelné.	Riziko je akceptováno MKB po konzultaci s garantem aktiva. Riziko je pravidelně monitorováno.
Střední	16 <= HR < 32	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.	Riziko je akceptováno MKB po konzultaci s garantem aktiva. V případě akceptace je riziko pravidelně monitorováno. V případě potřeby snížení rizika navrhne architekt KB ve spolupráci s MKB bezpečnostní opatření.
Vysoká	32 <= HR < 48	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.	Riziko není akceptováno. Po konzultaci s garantem aktiva navrhuje MKB bezpečnostní opatření ve spolupráci s architektem KB.
Kritická	>= 48	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	Riziko není akceptováno. Po konzultaci s garantem aktiva navrhuje MKB bezpečnostní opatření ve spolupráci s architektem KB. Tato rizika mají nejvyšší prioritu v jejich řešení a měla by být zvládána přednostně.

Tabulka 11: Maticové zobrazení možných hodnot rizika (Zdroj: Vlastní zpracování)

Úrovně rizika									
	Hrozba x Zranitelnost								
Dopad		1	2	3	4	6	8	9	12	16
	1	1	2	3	4	6	8	9	12	16
	2	2	4	6	8	12	16	18	24	32
	3	3	6	9	12	18	24	27	36	48
	4	4	8	12	16	24	32	36	48	64

4.5.5 Identifikace rizik

Rizika jsou identifikována zvolením vhodných kombinací aktivum-zranitelnost-hrozba. Účelem tohoto procesu není vytvořit kombinace všeho se vším. Např. u aktiva zaměstnanci není relevantní kombinací zranitelnost typu nedostatečná údržba a hrozba typu poškození nebo selhání technického nebo programového vybavení. Je potřeba volit takové varianty, které jsou reálné a relevantní. Kombinace, které nejsou, by do procesu řízení rizik neměly být zahrnuty. Je ovšem důležité všechny tyto kombinace předem zvážit.

4.5.6 Hodnocení rizik

Hodnocení rizik v souladu s VKB znamená ohodnocení relevantních kombinací hodnot aktivum-zranitelnost-hrozba dle již výše zmíněného vzorce. Výsledkem je hodnota rizika, která musí být porovnána s kritérii pro akceptovatelnost, načež by mělo být vydáno rozhodnutí, zda bude riziko akceptováno nebo zvládnuto jiným způsobem.

4.5.7 Zvládání rizik

Po identifikaci a ohodnocení rizik je nutné rizika vhodným způsobem dále zvládat tak, aby na ně organizace byla připravena. V tomto ohledu zde platí několik obecných zásad.

Pokud je riziko ošetřeno preventivním řešením, náklady na toto řešení by neměly přesahovat potencionální hodnotu rizika.

Pokud je riziko ošetřeno reaktivním bezpečnostním opatřením, měly by dodatečné náklady být investovány až v momentě, kdy se scénář realizuje. Jedná se nejčastěji o rizika, které nebyly nijak ošetřeny, nebo zvolená bezpečnostní opatření nebyla účinná.

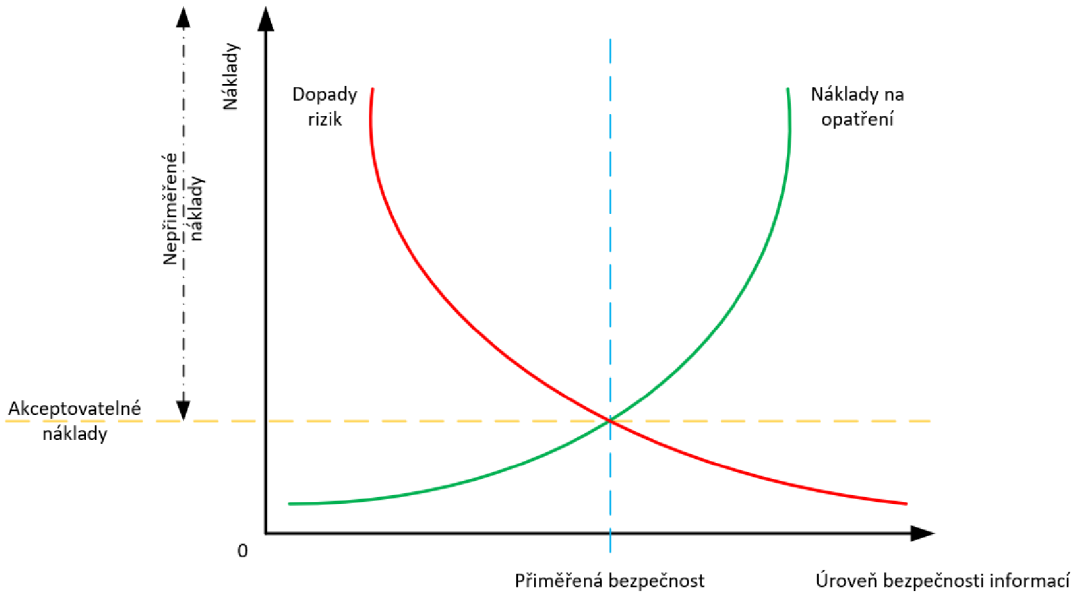
Je vhodné mít připraveny krizové plány i pro případy, kdy byla bezpečnostní opatření aplikována a rizika tak byla snížena nebo přenesena.

Všechna rizika je nutné monitorovat a pravidelně přezkoumávat metody jejich zvládání. Pravděpodobnost jejich výskytu a jejich dopad se totiž může v čase měnit. Může se také měnit schopnost organizace tato rizika zvládat, ať už směrem k lepšímu či horšímu. Monitorování rizik by mělo být prováděno s ohledem na typ rizika a jeho závažnost. Vážnější rizika je potřeba monitorovat neustále, zatímco méně závažná lze monitorovat periodicky.

Všechna rizika by měla mít určené osoby za jejich zvládání, monitorování a přezkoumávání.

Pokud výsledná hodnota rizika překračuje hranici akceptovatelnosti, musí být vybrána vhodná bezpečnostní opatření pro snížení hodnoty rizika nebo pro jeho eliminaci, aby byla zajištěna požadovaná úroveň bezpečnosti informací. V případě, kdy je finanční náročnost opatření neúměrná vůči riziku, které má ošetřit, je nutné zvolit jiné, méně účinné opatření nebo pokrýt toto riziko dílčími opatřeními i za předpokladu, že toto ošetření rizik nebude dlouhodobě účinné nebo dostatečné.

Obrázek č. 9 zobrazuje vztah přiměřenosti mezi náklady a bezpečností.



Obrázek 9: Graf posouzení přiměřených nákladů a přiměřené bezpečnosti (Zdroj: Vlastní zpracování)

Akceptace rizika

Riziko lze akceptovat pasivně, pokud nebyla např. nalezena vhodná nebo smysluplná opatření. Pasivní akceptace znamená, že nejsou zavedena žádná bezpečnostní opatření, kromě záznamu o tomto riziku v evidenci rizik.

Riziko lze akceptovat pasivně zejména u středních hodnot rizik. U těchto rizik by měly být vytvořeny jisté rezervy, např. ve formě lidských nebo finančních zdrojů, které by měly případný výskyt rizika pokrýt.

Redukce a eliminace rizika

Tato metoda je nejběžnějším způsobem zvládání rizik. Jde o aktivní přístup, kde je cílem výběr vhodného bezpečnostního opatření tak, aby byla rizika snížena na přijatelnou úroveň.

Vhodná bezpečnostní opatření jsou uvedena ve VKB, nicméně nejde o jejich konečný výčet. Cílem zavádění bezpečnostních opatření je provádět je na základě hodnocení rizik a v takovém rozsahu, aby byla zajištěna kybernetická bezpečnost v organizaci. Hodnota rizika, kterou získáme při jeho výpočtu udává, jak důležité a v jakém rozsahu je potřeba bezpečnostní opatření implementovat. Je pravidlem, že zaváděním bezpečnostních opatření se snižuje hodnota zranitelnosti, kdežto hodnota hrozeb zůstává v daném čase, v daném místě a pro dané aktivum stejná, bez ohledu na opatření.

Vyhnutí se riziku

Metodou vyhnutí se riziku rozumíme utlumení rizika, např. významně omezit využívání aktiva, nebo vypnutí, např. nepoužívání daného aktiva. Tento způsob zvládání rizik se využívá v případech, kdy je výskyt jistý a dopad kritický.

Přenesení nebo sdílení rizika

Pokud organizace nedisponuje kapacitami na zavedení bezpečnostních opatření, musí být odpovědnost přenesena na třetí stranu. Riziko je tedy přesměrováno na externí společnost s jejím vědomým souhlasem. Typickým příkladem je pojištění, kde bezpečnostní opatření má sice dopad na náklady organizace, ale případná škoda bude uhrazena někým jiným.

4.5.8 Výběr opatření pro zvládání rizik

Bezpečnostní opatření je forma zavádění a prosazování konkrétních bezpečnostních postupů organizačního charakteru, implementaci technických nastavení, konfigurací a nasazování bezpečnostních technologií.

Mezi bezpečnostní opatření organizačního charakteru patří zajištění personální bezpečnosti, organizace řízení kybernetické bezpečnosti, požadavky na chování uživatelů, administrátorů a osob zastávajících bezpečnostní role, souhrn zákonných a smluvních požadavků, předpisy, metodiky a politiky. Jednou z forem těchto opatření je např. interní nebo provozní směrnice, která obsahuje detailní popis toho, co je opatřením zamýšleno, jakým způsobem by mělo být realizováno, koho se týká, jak by mělo být implementováno a prosazováno. Organizační opatření popisují ve VKB § 3 až § 16.

Bezpečnostními opatřeními technického charakteru jsou myšleny oblasti fyzické ochrany, HW, SW atd. Konkrétně se jedná o nasazení bezpečnostních technologií, jejich konfigurace v přímé souvislosti s ochranou bezpečnosti informační a komunikační sítě, prvků této sítě a technických a programových prostředků. Mezi tato bezpečnostní opatření patří např. technické řízení přístupových oprávnění, nástroj ke správě a ověřování identit, nástroje pro ochranu před škodlivým kódem, nástroje pro sběr a vyhodnocování provozních a bezpečnostních událostí atd. Technická opatření popisují ve VKB § 17 až § 29.

Bezpečnostní opatření se zavádí za účelem skutečného a účinného snižování identifikovaného rizika (hrozba a zranitelnost), aby bylo dosáhnuto efektivní ochrany

informací z hlediska důvěrnosti, dostupnosti a integrity. V praxi se může stát, že přestože jsou rizika snížena implementací bezpečnostních opatření, výsledná hodnota rizika po revizi stále není akceptovatelná. V tomto případě je nutné zavádět další bezpečnostní opatření, dokud hodnota rizika nebude akceptovatelná. Při implementaci bezpečnostních opatření je třeba dbát na kontext ostatních rizik a souvisejících bezpečnostních opatření.

Pokud nelze bezpečnostní opatření zavést ihned, např. z důvodu administrativních, finančních nebo technologických překážek, je nutné toto zdržení dokumentačně zdůvodnit a v mezičase riziko snižovat dílčími bezpečnostními opatřeními.

Při výběru bezpečnostních opatření je vhodné zvážit následující:

- cílení opatření na zjištěná rizika (hrozby, zranitelnosti ve vazbě na důvěrnost, dostupnost a integritu aktiv),
- postupovat v souladu s požadavky VKB,
- využívat odborných znalostí a zkušeností garantů aktiv a dalších kvalifikovaných osob,
- zohledňovat přiměřenost opatření vzhledem k nákladům a dopadům na existující procesy, které jsou s implementací opatření spojeny,
- řídit proces implementace a zavedení bezpečnostního opatření,
- popsat zamýšlené cíle a přínosy zavedeného bezpečnostního opatření,
- postupovat v souladu s interními předpisy VUT FP,
- informovat zainteresované osoby o návrhu, průběhu a výsledku implementace bezpečnostního opatření,
- stanovit odpovědnosti za jednotlivé činnosti.

4.5.9 Plán zvládání rizik

RTP (Risk Treatment Plan), neboli plán zvládání rizik, je jedním z klíčových dokumentů, který vychází z procesu hodnocení rizik.

Při jeho vytváření se musí vycházet kromě hodnocení rizik i z dalších souvisejících procesů, jako je např. audit kybernetické bezpečnosti, již proběhlé bezpečnostní incidenty, varování nebo reaktivní opatření vydané NÚKIB atd.

Cílem plánu zvládání rizik je systematickým přístupem zavádět bezpečnostní opatření, stanovovat priority v rámci eliminace rizik a efektivní plánování zdrojů potřebných pro zajištění kybernetické bezpečnosti.

Plán zvládání rizik by měl obsahovat následující údaje:

- cíle a přínosy bezpečnostních opatření,
- určení osob, které prosazují bezpečnostní opatření,
- potřebné finanční, technické, lidské a informační zdroje,
- termíny implementace opatření,
- popis vazby mezi riziky a souvisejícími bezpečnostními opatřeními,
- způsob realizace bezpečnostního opatření.

Plán zvládání rizik by se měl řídit obecnými pokyny řízené dokumentace. Měl by tedy být aktualizován nejen pravidelně v rámci revizí dokumentace, ale i při jakékoliv změně výše vyjmenovaných okolností.

4.5.10 Zpráva o hodnocení rizik

Zpráva o hodnocení rizik uvádí stručný souhrn výsledků hodnocení rizik pro relevantní zainteresované strany. Slouží jako stručný přehled identifikovaných rizik, míry jejich akceptovatelnost či neakceptovatelnosti a bezpečnostní opatření navržená pro jejich zvládání. Zpráva by měla být předkládána výboru KB, který by ji měl schválit.

4.5.11 Prohlášení o aplikovatelnosti

SoA (Statement of Applicability), neboli prohlášení o aplikovatelnosti je dokument, který popisuje zavedená bezpečnostní opatření včetně způsobu jejich implementace, a současně nezavedená opatření včetně odůvodnění, z jakého důvodu se tak stalo. Tento dokument by měl být taktéž předkládán výboru KB, který by jej měl schválit.

Prohlášení o aplikovatelnosti a plán zvládání rizik jsou klíčové dokumenty v oblasti řízení ISMS a měly by vyjadřovat přesné a aktuální informace o stavu kybernetické bezpečnosti uvnitř VUT FP.

4.6 Přínos práce

Hlavním cílem praktické části této diplomové práce bylo najít způsoby, jakými by mohlo VUT FP napravit nesoulady s VKB, které byly identifikovány v analytické části práce. Vzhledem k množství nálezů a rozsahu potřebných nápravných opatření byl však v praktické části zúžen počet těchto oblastí na ty nejkritičtější. Jedná se tedy konkrétně o oblasti:

- určení rozsahu ISMS,
- určení strategických cílů ISMS,
- jmenování osob podílejících se na rozvoji kybernetické bezpečnosti,
- řízení aktiv,
- řízení rizik.

Jedná se o oblasti, které jsou v procesu implementace a řízení ISMS naprosto klíčové a měly by být zvládnuty před pokračováním na návazných bezpečnostních opatřeních. V těchto kritických oblastech byla pro VUT FP vypracována metodická příručka, včetně názorných příkladů, jak by mohla být zajištěna akceptovatelná úroveň kybernetické bezpečnosti. Jak již bylo zdůrazněno, VUT FP by mělo k těmto příručkám pouze přihlédnout a uzpůsobit je vlastním potřebám v oblasti kybernetické bezpečnosti. Nejedná se tedy o jediný možný a správný způsob, jak problematiku ISMS uchopit.

Tím byl splněn třetí a zároveň poslední dílčí cíl této diplomové práce.

ZÁVĚR

Cílem diplomové práce bylo s pomocí GAP analýzy identifikovat oblasti kybernetické bezpečnosti, ve kterých byla Fakulta podnikatelská, Vysokého učení technického v Brně, v nesouladu s požadavky zákona o kybernetické bezpečnosti č. 181/2014 Sb. a vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.

V první kapitole bylo vytyčeno několik dílčích cílů, které pomohly tuto diplomovou práci strukturovat do lépe uchopitelných logických celků a zároveň poskytnout jakýsi měřitelný prvek, a to ve formě schopnosti na tyto cíle v průběhu diplomové práce odpovídat.

Další kapitola obsahovala zejména teoretický základ a nastínění aktuální reality kybernetické bezpečnosti na území České republiky. Byly popsány správní orgány, které se zabývají různými agendami v této oblasti a byly také v základu objasněny předměty právní úpravy zákona a vyhlášky o kybernetické bezpečnosti.

Úkolem analytické části bylo odpovědět na první dva dílčí cíle této diplomové práce, tedy proč je téma kybernetické bezpečnosti relevantní pro Vysoké učení technické v Brně a v jakém stavu se na Podnikatelské fakultě nachází. Struktura této kapitoly tedy následovala právě tyto dva cíle. Nejprve bylo vyjasněno, jakým způsobem naplňuje organizace definici správce významného informačního systému a následně byla zpracována GAP analýza, která následovala bezpečnostní opatření vyžadované vyhláškou o kybernetické bezpečnosti. Výsledky vypovídají samy o sobě, nicméně je třeba vzít v potaz fakt, že k nahlášení kontaktních údajů ze strany Vysokého učení technického v Brně, jakožto správce významného informačního systému, došlo teprve v roce 2022, což znamená, že je organizace v oblasti implementace ISMS teprve na začátku.

S vědomím těchto skutečností se autor této diplomové práce v její praktické části soustředil na to, jak Fakultě podnikatelské pomoci v počátečních fázích řešení problematiky ISMS. Bylo vyhodnoceno, že nejúčinnějším řešením bude nabídnout v rámci této práce metodickou podporu v oblastech určení rozsahu ISMS, určení strategických cílů ISMS, jmenování osob podílejících se na rozvoji kybernetické bezpečnosti, řízení aktiv a řízení rizik, včetně praktických ukázek řešení.

SEZNAM POUŽITÝCH ZDROJŮ

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

(2) SEDLÁK, Petr, Martin KONEČNÝ a kolektiv. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-068-2.

(3) JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0.

(4) ČESKO. Zákon č. 181/2014 Sb. ze dne 29. srpna 2014 *o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. 2014 [cit. 2022-2-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

(5) ŠIKÝŘ, Martin. *Nejlepší praxe v řízení lidských zdrojů*. Praha: Grada, 2014. Manažer. ISBN 978-80-247-5212-9.

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

(7) CyberSecurity.CZ. *Kybernetická bezpečnost (Cyber Security)* [online]. [cit. 2022-2-20]. Dostupné z: https://cybersecurity.cz/basic.html

(8) Národní úřad pro kybernetickou a informační bezpečnost. *O úřadu* [online]. [cit. 2022-2-25]. Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu/

(9) Národní úřad pro kybernetickou a informační bezpečnost. *Vládní CERT* [online]. [cit. 2022-2-25]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/

(10) CZ.NIC. *KONCEPCE SDRUŽENÍ CZ.NIC PRO OBDOBÍ 2020-2024* [online]. [cit. 2022-2-25]. Dostupné z: https://www.nic.cz/files/nic/doc/Koncepce_CZNIC_2020-2024.pdf

(11) Národní bezpečnostní úřad. *O nás* [online]. [cit. 2022-2-25]. Dostupné z: https://www.nbu.cz/cs/o-nas/955-o-nas/

(12) Bezpečnostní informační služba. *O nás* [online]. [cit. 2022-2-25]. Dostupné z: https://www.bis.cz/o-nas/

(13) Úřad pro zahraniční styky a informace. *Kdo jsme* [online]. [cit. 2022-2-25]. Dostupné z: https://www.uzsi.cz/kdo-jsme

(14) Vojenské zpravodajství. *Kdo jsme* [online]. [cit. 2022-2-25]. Dostupné z: https://www.vzcr.cz/kdo-jsme-35

(15) Národní úřad pro kybernetickou a informační bezpečnost. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* [online]. [cit. 2022-3-1]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

(16) Vysoké učení technické v Brně. *Profil univerzity* [online]. [cit. 2022-3-30]. Dostupné z: https://www.vut.cz/vut/profil

(17) Národní úřad pro kybernetickou a informační bezpečnost. *Významné informační systémy ve školství* [online]. [cit. 2022-3-30]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/2021-02-22_VIS-skoly_FAQ_v.0.1.pdf

(18) ČESKO. Vyhláška č. 82/2018 Sb. ze dne 25. května 2018 *o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)* [online]. 2018 [cit. 2022-2-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

(19) Národní úřad pro kybernetickou a informační bezpečnost. *Povinnosti orgánů a osob podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti* [online]. [cit. 5-3-2022]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

SEZNAM POUŽITÝCH ZKRATEK

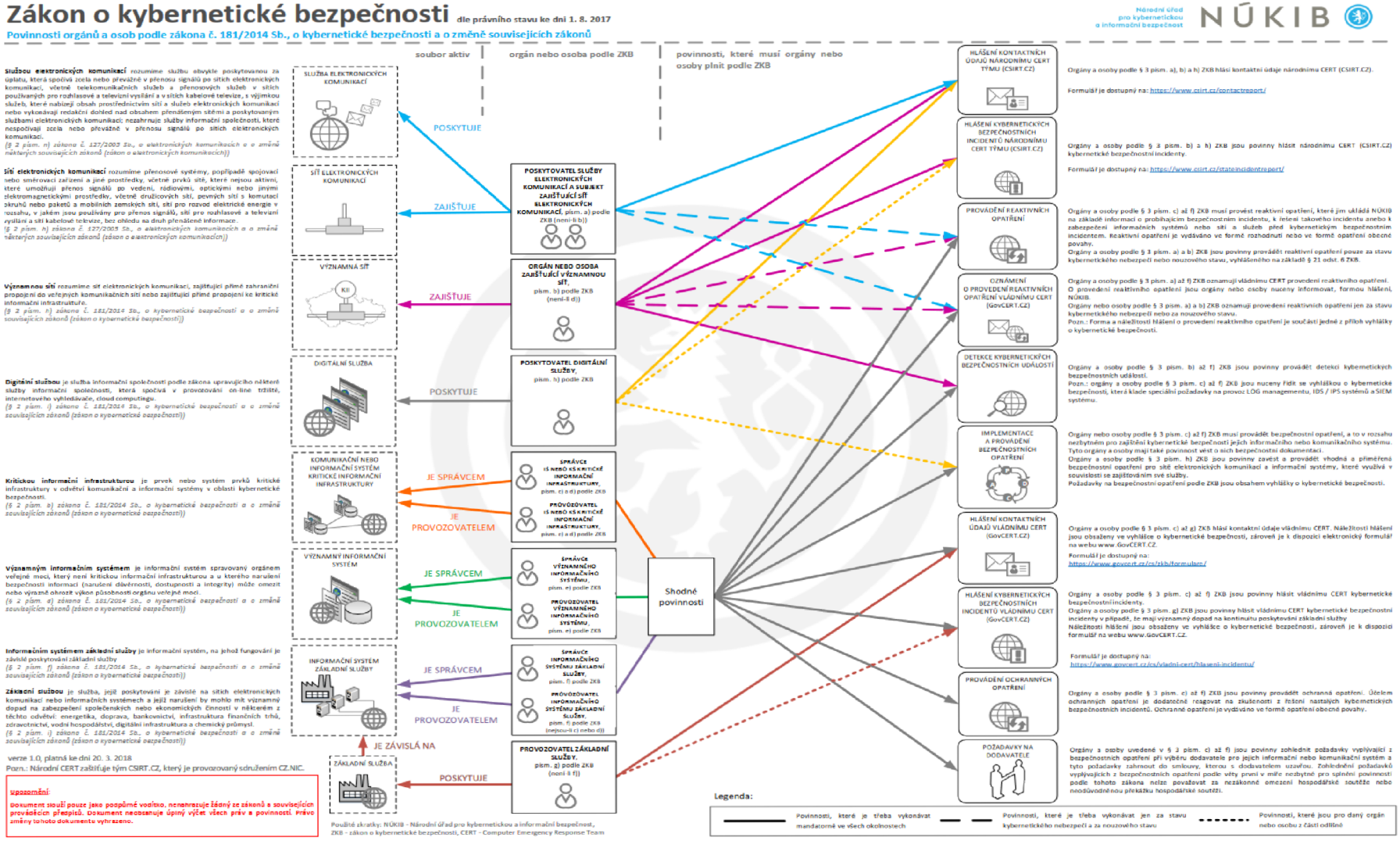
BIS	Bezpečnostní informační služba České republiky
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ČR	Česká republika
DoS	Denial of Service
DDoS	Distributed Denial of Service
EU	Evropská unie
GDPR	General Data Protection Regulation
HW	Hardware
ICT	Information and Communication Technologies
ID	Identity
IoT	Internet of Things
ISMS	Information and Security Management System
KB	Kybernetická bezpečnost
KII	Kritická informační infrastruktura
MKB	Manažer kybernetické bezpečnosti
NBÚ	Národní bezpečnostní úřad
NIS	The Network and Information Security Directive
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PDCA	Plan, Do, Control, Act
SW	Software
ÚZSI	Úřad pro zahraniční styky a informace
VIS	Významný informační systém
VKB	Vyhláška o kybernetické bezpečnosti
VUT FP	Vysoké učení technické v Brně, Fakulta podnikatelská
VZ	Vojenské zpravodajství
ZKB	Zákon o kybernetické bezpečnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha I: Povinnosti orgánů a osob podle zákona č. 181/2014 Sb. (Zdroj: [19])



Příloha II: Interpretace dotazníku GAP analýzy v prohlášení o aplikovatelnosti (Zdroj: Vlastní zpracování)

#	Zdroj	§	Název §	úroveň členění				Text §	relevan		jak/čím plněno	kde kodifikováno/popsáno
				1	2	3	4		VIS	a / n		
87	VKB	§ 3	Systém řízení bezpečnosti informací					Povinná osoba v rámci systému řízení bezpečnosti informací	-		nařešeno	
88	VKB	§ 3	Systém řízení bezpečnosti informací	a				stanoví s ohledem na požadavky dotčených stran a organizační bezpečnost rozsah systému řízení bezpečnosti informací, ve kterém určí organizační části a aktiva, jichž se systém řízení bezpečnosti informací týká,	v	NE		
89	VKB	§ 3	Systém řízení bezpečnosti informací	b				stanoví cíle systému řízení bezpečnosti informací,	v	NE		
90	VKB	§ 3	Systém řízení bezpečnosti informací	c				pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik zavede přiměřená bezpečnostní opatření,	v	NE		
91	VKB	§ 3	Systém řízení bezpečnosti informací	d				řídí rizika podle § 5,	v	NE		
92	VKB	§ 3	Systém řízení bezpečnosti informací	e				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 § 30 a zavede přiměřená bezpečnostní opatření,	v	NE		
93	VKB	§ 3	Systém řízení bezpečnosti informací	f				zajistí provedení auditu kybernetické bezpečnosti u informačního a komunikačního systému (dále jen „audit kybernetické bezpečnosti") podle § 16,	v	NE		
94	VKB	§ 3	Systém řízení bezpečnosti informací	g				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,	v	NE		
95	VKB	§ 3	Systém řízení bezpečnosti informací	h				průběžně identifikuje a následně podle § 11 řídí významné změny, které patří do rozsahu systému řízení bezpečnosti informací,	v	NE		
96	VKB	§ 3	Systém řízení bezpečnosti informací	i				aktualizuje 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	v	NE		
97	VKB	§ 3	Systém řízení bezpečnosti informací	j				řídí provoz a zdroje systému řízení bezpečnosti informací a zaznamenává činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik.	v	NE		
98	VKB	§ 4	Řízení aktiv	1				Povinná osoba v rámci řízení aktiv	-		nařešeno	
99	VKB	§ 4	Řízení aktiv	1	a			stanoví metodiku pro identifikaci aktiv,	v	NE		
100	VKB	§ 4	Řízení aktiv	1	b			stanoví metodiku pro hodnocení aktiv alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce,	v	NE		
101	VKB	§ 4	Řízení aktiv	1	c			identifikuje a eviduje aktiva,	v	NE		
102	VKB	§ 4	Řízení aktiv	1	d			určí a eviduje garanty aktiv,	v	NE		
103	VKB	§ 4	Řízení aktiv	1	e			hodnotí a eviduje primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní podle písmene b),	v	NE		
104	VKB	§ 4	Řízení aktiv	1	f			určí a eviduje vazby mezi primárními a podpůrnými aktivy a hodnotí důsledky závislostí mezi primárními a podpůrnými aktivy,	v	NE		
105	VKB	§ 4	Řízení aktiv	1	g			hodnotí podpůrná aktiva a zohledňuje přitom zejména vzájemné závislosti podle písmene f),	v	NE		
106	VKB	§ 4	Řízení aktiv	1	h			na základě hodnocení aktiv stanovuje a zavádí pravidla ochrany nutná pro zabezpečení jednotlivých úrovní aktiv,	v	NE		
107	VKB	§ 4	Řízení aktiv	1	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,	v	NE		
108	VKB	§ 4	Řízení aktiv	1	j			určí způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv v souladu s přílohou č. 4 k této vyhlášce.	v	NE		
109	VKB	§ 4	Řízení aktiv	2				Při hodnocení důležitosti primárních aktiv je třeba posoudit alespoň	-		nařešeno	
110	VKB	§ 4	Řízení aktiv	2	a			rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství,	v	NE		
111	VKB	§ 4	Řízení aktiv	2	b			rozsah dotčených právních povinností nebo jiných závazků,	v	NE		
112	VKB	§ 4	Řízení aktiv	2	c			rozsah narušení vnitřních řídicích a kontrolních činností,	v	NE		
113	VKB	§ 4	Řízení aktiv	2	d			poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty,	v	NE		
114	VKB	§ 4	Řízení aktiv	2	e			dopady na poskytování důležitých služeb,	v	NE		
115	VKB	§ 4	Řízení aktiv	2	f			rozsah narušení běžných činností,	v	NE		
116	VKB	§ 4	Řízení aktiv	2	g			dopady na zachování dobrého jména nebo ochranu dobré pověsti,	v	NE		
117	VKB	§ 4	Řízení aktiv	2	h			dopady na bezpečnost a zdraví osob,	v	NE		
118	VKB	§ 4	Řízení aktiv	2	i			dopady na mezinárodní vztahy a	v	NE		
119	VKB	§ 4	Řízení aktiv	2	j			dopady na uživatele informačního a komunikačního systému.	v	NE		
140	VKB	§ 5	Řízení rizik	1				Povinná osoba v rámci řízení rizik v návaznosti na § 4	-		nařešeno	
141	VKB	§ 5	Řízení rizik	1	a			stanoví metodiku pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik,	v	NE		
142	VKB	§ 5	Řízení rizik	1	b			s ohledem na aktiva identifikuje relevantní hrozby a zranitelnosti; přitom zvažuje zejména kategorie hrozeb a zranitelností uvedených v příloze č. 3 k této vyhlášce,	v	NE		
143	VKB	§ 5	Řízení rizik	1	c			provádí hodnocení rizik v pravidelných intervalech podle odstavce 2 a při významných změnách,	v	NE		
144	VKB	§ 5	Řízení rizik	1	d			při hodnocení rizik zohlední relevantní hrozby a zranitelnosti a posoudí možné dopady na aktiva; tato rizika hodnotí alespoň v rozsahu přílohy č. 2 k této vyhlášce,	v	NE		
145	VKB	§ 5	Řízení rizik	1	e			zpracuje zprávu o hodnocení rizik,	v	NE		
146	VKB	§ 5	Řízení rizik	1	f			zpracuje na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled bezpečnostních opatření požadovaných touto vyhláškou, která	v	NE		
147	VKB	§ 5	Řízení rizik	1	f	1		nebyla aplikována, včetně odůvodnění,	v	NE		
148	VKB	§ 5	Řízení rizik	1	f	2		byla aplikována, včetně způsobu plnění,	v	NE		
149	VKB	§ 5	Řízení rizik	1	g			zpracuje a zavede 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, popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a způsob realizace bezpečnostních opatření,	v	NE		
150	VKB	§ 5	Řízení rizik	1	h			při hodnocení rizik a v plánu zvládání rizik zohlední	-		nařešeno	

#	Zdroj	§	Název §	1	2	3	4	Text §	VIS	a / n	jak/čím plněno	kde kodifikováno/popsáno
151	VKB	§ 5	Řízení rizik	1	h	1		významné změny,	v	NE		
152	VKB	§ 5	Řízení rizik	1	h	2		změny rozsahu systému řízení bezpečnosti informací,	v	NE		
153	VKB	§ 5	Řízení rizik	1	h	3		opatření podle § 11 zákona a	v	NE		
154	VKB	§ 5	Řízení rizik	1	h	4		kybernetické bezpečnostní incidenty, včetně dříve řešených, a	v	NE		
155	VKB	§ 5	Řízení rizik	1	i			v souladu s plánem zvládání rizik zavádí bezpečnostní opatření.	v	NE		
157	VKB	§ 5	Řízení rizik	2				povinná osoba uvedená v § 3 písm. e) zákona alespoň jednou za tři roky.	v	NE		
158	VKB	§ 5	Řízení rizik	3				Řízení rizik může být zajištěno i jinými způsoby, než jak je stanoveno v odstavci 1 písm. d), pokud povinná osoba zabezpečí, že použitá opatření zajistí stejnou nebo vyšší úroveň procesu řízení rizik.	v	NE		
198	VKB	§ 6	Organizační bezpečnost	1				Povinná osoba s ohledem na systém řízení bezpečnosti informací	-		neřešeno	
199	VKB	§ 6	Organizační bezpečnost	1	a			zajistí stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací podle § 3 slučitelných se strategickým směřováním povinné osoby,	v	NE		
200	VKB	§ 6	Organizační bezpečnost	1	b			zajistí integraci systému řízení bezpečnosti informací do procesů povinné osoby,	v	NE		
201	VKB	§ 6	Organizační bezpečnost	1	c			zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací,	v	NE		
202	VKB	§ 6	Organizační bezpečnost	1	d			informuje zaměstnance o významu systému řízení bezpečnosti informací a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,	v	NE		
203	VKB	§ 6	Organizační bezpečnost	1	e			zajistí podporu k dosažení zamýšlených výstupů systému řízení bezpečnosti informací,	v	NE		
204	VKB	§ 6	Organizační bezpečnost	1	f			vede zaměstnance k rozvíjení efektivity systému řízení bezpečnosti informací a podporuje je při tomto rozvíjení,	v	NE		
205	VKB	§ 6	Organizační bezpečnost	1	g			prosazuje neustálé zlepšování systému řízení bezpečnosti informací,	v	NE		
206	VKB	§ 6	Organizační bezpečnost	1	h			podporuje osoby zastávající bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,	v	NE		
207	VKB	§ 6	Organizační bezpečnost	1	i			zajistí stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role,	v	NE		
208	VKB	§ 6	Organizační bezpečnost	1	j			zajistí, aby byla zachována mlčenlivost administrátorů a osob zastávajících bezpečnostní role,	v	NE		
209	VKB	§ 6	Organizační bezpečnost	1	k			pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů a	v	NE		
210	VKB	§ 6	Organizační bezpečnost	1	l			zajistí testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.	v	NE		
211	VKB	§ 6	Organizační bezpečnost	2				Povinná osoba v rámci systému řízení bezpečnosti informací určí složení výboru pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související se systémem řízení bezpečnosti informací.	v	NE		
217	VKB	§ 6	Organizační bezpečnost	4				Povinná osoba uvedená v § 3 písm. e) zákona určí role manažera kybernetické bezpečnosti a garanta aktiva. Ostatní bezpečnostní role podle odstavce 3 určí přiměřeně vzhledem k rozsahu a potřebám systému řízení bezpečnosti informací.	v	NE		
219	VKB	§ 6	Organizační bezpečnost	6				Povinná osoba uvedená v § 3 písm. e) zákona zajistí zastupitelnost bezpečnostní role manažera kybernetické bezpečnosti.	v	NE		
220	VKB	§ 6	Organizační bezpečnost	7				Výbor pro řízení kybernetické bezpečnosti je tvořen 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, jehož členem musí být alespoň jeden zástupce vrcholového vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti. Povinná osoba u výboru pro řízení kybernetické bezpečnosti přihlédne k doporučením uvedeným v příloze č. 6 k této vyhlášce.	v	NE		
221	VKB	§ 7	Bezpečnostní role	1				Manažer kybernetické bezpečnosti	-		neřešeno	
222	VKB	§ 7	Bezpečnostní role	1	a			je bezpečnostní role odpovědná za systém řízení bezpečnosti informací, přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s řízením kybernetické bezpečnosti nebo s řízením bezpečnosti informací	v	NE		
223	VKB	§ 7	Bezpečnostní role	1	a	1		po dobu nejméně tří let, nebo	v	NE		
224	VKB	§ 7	Bezpečnostní role	1	a	2		po dobu jednoho roku, pokud absolvovala studium na vysoké škole,	v	NE		
225	VKB	§ 7	Bezpečnostní role	1	b			odpovídá za pravidelné informování vrcholového vedení o	v	NE		
226	VKB	§ 7	Bezpečnostní role	1	b	1		činnostech vyplývajících z rozsahu jeho odpovědnosti a	v	NE		
227	VKB	§ 7	Bezpečnostní role	1	b	2		stavu systému řízení bezpečnosti informací a	v	NE		
228	VKB	§ 7	Bezpečnostní role	1	c			nesmí být pověřen výkonem rolí odpovědných za provoz informačního a komunikačního systému.	v	NE		
282	VKB	§ 7	Bezpečnostní role	3				Garant aktiva je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva.	v	NE		
239	VKB	§ 7	Bezpečnostní role	5				Povinná osoba při určování osob zastávajících bezpečnostní role přihlédne k doporučením uvedeným v příloze č. 6 k této vyhlášce.	v	NE		
349	VKB	§ 8	Řízení dodavatelů	1				Povinná osoba	-		neřešeno	
350	VKB	§ 8	Řízení dodavatelů	1	a			stanoví pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací,	v	NE		
351	VKB	§ 8	Řízení dodavatelů	1	b			vede evidenci svých významných dodavatelů,	v	NE		
352	VKB	§ 8	Řízení dodavatelů	1	c			prokazatelně písemně informuje své významné dodavatele o jejich evidenci podle písmene b),	v	NE		
353	VKB	§ 8	Řízení dodavatelů	1	d			seznamuje své dodavatele s pravidly podle písmene a) a vyžaduje plnění těchto pravidel,	v	NE		
354	VKB	§ 8	Řízení dodavatelů	1	e			řídí rizika spojená s dodavateli,	v	NE		
355	VKB	§ 8	Řízení dodavatelů	1	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, a	v	NE		
356	VKB	§ 8	Řízení dodavatelů	1	g			pravidelně přezkoumává plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací.	v	NE		
357	VKB	§ 8	Řízení dodavatelů	2				Povinná osoba u významných dodavatelů dále	-		neřešeno	
358	VKB	§ 8	Řízení dodavatelů	2	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,	v	NE		
359	VKB	§ 8	Řízení dodavatelů	2	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,	v	NE		
360	VKB	§ 8	Řízení dodavatelů	2	c			provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany a	v	NE		
361	VKB	§ 8	Řízení dodavatelů	2	d			v reakci na rizika a zjištěné nedostatky zajistí jejich řešení.	v	NE		
362	VKB	§ 8	Řízení dodavatelů	3				Náležitosti prokazatelného informování podle odstavce 1 písm. c) jsou	-		neřešeno	
363	VKB	§ 8	Řízení dodavatelů	3	a			identifikace správce nebo provozovatele,	v	NE		

#	Zdroj	§	Název §	1	2	3	4	Text §	VIS	a / n	jak/čím plněno	kde kodifikováno/popsáno
364	VKB	§ 8	Řízení dodavatelů	3	b			identifikace informačního a komunikačního systému,	v	NE		
365	VKB	§ 8	Řízení dodavatelů	3	c			identifikace významného dodavatele,	v	NE		
366	VKB	§ 8	Řízení dodavatelů	3	d			vyrozumění o skutečnosti, že dodavatel je pro správce významným dodavatelem, a popřípadě také o tom, že významný dodavatel je zároveň provozovatelem, a	v	NE		
367	VKB	§ 8	Řízení dodavatelů	3	e			obsah pravidel podle odstavce 1 písm. a).	v	NE		
368	VKB	§ 8	Řízení dodavatelů	4				Povinná 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.	v	NE		
388	VKB	§ 9	Bezpečnost lidských zdrojů	1				Povinná osoba v rámci řízení bezpečnosti lidských zdrojů	-		neřešeno	
389	VKB	§ 9	Bezpečnost lidských zdrojů	1	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	-			
390	VKB	§ 9	Bezpečnost lidských zdrojů	1	a	1		poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice a	v	NE		
391	VKB	§ 9	Bezpečnost lidských zdrojů	1	a	2		potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role,	v	NE		
392	VKB	§ 9	Bezpečnost lidských zdrojů	1	b			určí osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny,	v	NE		
393	VKB	§ 9	Bezpečnost lidských zdrojů	1	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,	v	NE		
394	VKB	§ 9	Bezpečnost lidských zdrojů	1	d			pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajistí pravidelná odborná školení, přičemž vychází z aktuálních potřeb povinné osoby v oblasti kybernetické bezpečnosti,	v	NE		
395	VKB	§ 9	Bezpečnost lidských zdrojů	1	e			v souladu s plánem rozvoje bezpečnostního povědomí zajistí pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní,	v	NE		
396	VKB	§ 9	Bezpečnost lidských zdrojů	1	f			zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role,	v	NE		
397	VKB	§ 9	Bezpečnost lidských zdrojů	1	g			v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajistí předání odpovědnosti,	v	A/N		
398	VKB	§ 9	Bezpečnost lidských zdrojů	1	h			hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí a	v	NE		
399	VKB	§ 9	Bezpečnost lidských zdrojů	1	i			určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.	v	A/N		
400	VKB	§ 9	Bezpečnost lidských zdrojů	2				Povinná osoba vede o školení podle odstavce 1 přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.	v	ANO		
401	VKB	§ 10	Řízení provozu a komunikací	1				Povinná osoba v rámci řízení provozu a komunikací zajišťuje bezpečný provoz informačního a komunikačního systému a stanoví provozní pravidla a postupy, které obsahují zejména	-		částečně řešeno	
402	VKB	§ 10	Řízení provozu a komunikací	1	a			práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role,	v	A/N	částečně řešeno	útvar IS
403	VKB	§ 10	Řízení provozu a komunikací	1	b			postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů,	v	NE		
404	VKB	§ 10	Řízení provozu a komunikací	1	c			postupy pro sledování kybernetických bezpečnostních událostí a opatření pro ochranu přístupu k záznamům o těchto událostech,	v	NE		
405	VKB	§ 10	Řízení provozu a komunikací	1	d			pravidla a postupy pro ochranu před škodlivým kódem,	v	A/N	částečně řešeno	útvar IS
406	VKB	§ 10	Řízení provozu a komunikací	1	e			řízení technických zranitelností,	v	NE		
407	VKB	§ 10	Řízení provozu a komunikací	1	f			spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory,	v	NE		
408	VKB	§ 10	Řízení provozu a komunikací	1	g			postupy řízení a schvalování provozních změn,	v	NE		
409	VKB	§ 10	Řízení provozu a komunikací	1	h			postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů,	v	NE		
410	VKB	§ 10	Řízení provozu a komunikací	1	i			pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu,	v	NE		
411	VKB	§ 10	Řízení provozu a komunikací	1	j			pravidla a postupy pro instalaci technických aktiv,	v	A/N	částečně řešeno	útvar IS
412	VKB	§ 10	Řízení provozu a komunikací	1	k			provádění pravidelného zálohování a kontroly použitelnosti provedených záloh a	v	A/N	částečně řešeno	útvar IS
413	VKB	§ 10	Řízení provozu a komunikací	1	l			pravidla a postupy pro zajištění bezpečnosti síťových služeb.	v	NE		
414	VKB	§ 10	Řízení provozu a komunikací	2				Povinná osoba v rámci řízení provozu a komunikací dodržuje pravidla a postupy stanovené podle odstavce 1 a tato pravidla a postupy aktualizuje v souvislosti s prováděnými nebo plánovanými změnami.	v	NE		
415	VKB	§ 10	Řízení provozu a komunikací	3				Povinná osoba zajistí oddělení vývojového, testovacího a provozního prostředí.	v	NE		
416	VKB	§ 11	Řízení změn	1				Povinná osoba v rámci řízení změn u informačního a komunikačního systému	-		neřešeno	
417	VKB	§ 11	Řízení změn	1	a			přezkoumává možné dopady změn a	v	NE		
418	VKB	§ 11	Řízení změn	1	b			určuje významné změny.	v	NE		
419	VKB	§ 11	Řízení změn	2				Povinná osoba u významných změn	-		neřešeno	
420	VKB	§ 11	Řízení změn	2	a			dokumentuje jejich řízení,	v	NE		
421	VKB	§ 11	Řízení změn	2	b			provádí analýzu rizik,	v	NE		
422	VKB	§ 11	Řízení změn	2	c			přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami,	v	NE		
423	VKB	§ 11	Řízení změn	2	d			aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci,	v	NE		
424	VKB	§ 11	Řízení změn	2	e			zajistí jejich testování a	v	NE		
425	VKB	§ 11	Řízení změn	2	f			zajistí možnost navrácení do původního stavu.	v	NE		
428	VKB	§ 12	Řízení přístupu	1				Povinná osoba na základě provozních a bezpečnostních potřeb řídí přístup k informačnímu a komunikačnímu systému a přijímá 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.	v	NON		
429	VKB	§ 12	Řízení přístupu	2				Povinná osoba dále v rámci řízení přístupu k informačnímu a komunikačnímu systému	-		částečně řešeno	
430	VKB	§ 12	Řízení přístupu	2	a			řídí přístup na základě skupin a rolí,	v	NON	řešeno dodávkou CVIS	
431	VKB	§ 12	Řízení přístupu	2	b			přidělí každému uživateli a administrátorovi přistupujícímu k informačnímu a komunikačnímu systému přístupová práva a oprávnění a jedinečný identifikátor,	v	NON	řešeno dodávkou CVIS	
432	VKB	§ 12	Řízení přístupu	2	c			řídí identifikátory, přístupová práva a oprávnění aplikací a technických účtů,	v	NON	řešeno dodávkou CVIS	

#	Zdroj	§	Název §	1	2	3	4	Text §	VIS	a / n	jak/čím plněno	kde kodifikováno/popsáno
433	VKB	§ 12	Řízení přístupu	2	d			zavádí bezpečnostní opatření pro řízení přístupu zařízení k prostředkům informačního a komunikačního systému,	√	NON	řešeno dodávkou CVIS	
434	VKB	§ 12	Řízení přístupu	2	e			zavádí bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných technických zařízení, popřípadě i bezpečnostní opatření spojená s využitím technických zařízení, která povinná osoba nemá ve své správě,	√	NON	řešeno dodávkou CVIS	
435	VKB	§ 12	Řízení přístupu	2	f			omezí přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce,	√	NON	řešeno dodávkou CVIS	
436	VKB	§ 12	Řízení přístupu	2	g			omezí a kontroluje používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly,	√	NON	řešeno dodávkou CVIS	
437	VKB	§ 12	Řízení přístupu	2	h			přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu,	√	NON	řešeno dodávkou CVIS	
438	VKB	§ 12	Řízení přístupu	2	i			provádí pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí,	√	NON	řešeno dodávkou CVIS	
439	VKB	§ 12	Řízení přístupu	2	j			využívá nástroj pro správu a ověřování identity podle § 19 a nástroj pro řízení přístupových oprávnění podle § 20,	√	NON	řešeno dodávkou CVIS	
440	VKB	§ 12	Řízení přístupu	2	k			prosazuje, aby uživatelé při používání privátních autentizačních informací dodržovali stanovené postupy,	√	NON	řešeno dodávkou CVIS	
441	VKB	§ 12	Řízení přístupu	2	l			zajistí odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role,	√	NON	řešeno dodávkou CVIS	
442	VKB	§ 12	Řízení přístupu	2	m			zajistí odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu a	√	NON	řešeno dodávkou CVIS	
443	VKB	§ 12	Řízení přístupu	2	n			dokumentuje přidělování a odebírání přístupových oprávnění.	√	NON	řešeno dodávkou CVIS	
444	VKB	§ 13	Akvizice, vývoj a údržba					Povinná osoba v souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému	-		neřešeno	
445	VKB	§ 13	Akvizice, vývoj a údržba	a				řídí rizika podle § 5,	√	NE		
446	VKB	§ 13	Akvizice, vývoj a údržba	b				řídí významné změny podle § 11,	√	NE		
447	VKB	§ 13	Akvizice, vývoj a údržba	c				stanoví bezpečnostní požadavky,	√	NE		
448	VKB	§ 13	Akvizice, vývoj a údržba	d				zahrne bezpečnostní požadavky do projektu akvizice, vývoje a údržby,	√	NE		
449	VKB	§ 13	Akvizice, vývoj a údržba	e				zajistí bezpečnost vývojového a testovacího prostředí a zajistí ochranu používaných testovacích dat,	√	NE		
450	VKB	§ 13	Akvizice, vývoj a údržba	f				provádí bezpečnostní testování významných změn před jejich zavedením do provozu a	√	NE		
451	VKB	§ 13	Akvizice, vývoj a údržba	g				plní požadavek podle § 19 odst. 3, je-li cílem provedení akvizice nebo vývoje nástroj pro správu a ověřování identity.	√	NE		
452	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů					Povinná osoba v rámci zvládání kybernetických bezpečnostních událostí a incidentů	-		neřešeno	
453	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	a			zavede proces detekce a vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů,	√	NE		
454	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	b			přidělí odpovědnosti a stanoví postupy pro	-		neřešeno	
455	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	b	1		detekci a vyhodnocování kybernetických bezpečnostních událostí a incidentů a	√	NE		
456	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	b	2		koordinaci a zvládání kybernetických bezpečnostních incidentů,	√	NE		
457	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	c			definuje a aplikuje postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu,	√	NE		
458	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	d			zajistí detekci kybernetických bezpečnostních událostí,	√	NE		
459	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	e			při detekci kybernetických bezpečnostních události se dále řídí § 22 a 23,	√	NE		
460	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	f			zajistí, že uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti,	√	A/N		
461	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	g			zajistí posuzování kybernetických bezpečnostních událostí, při kterém musí být rozhodnuto, zda mají být klasifikovány jako kybernetické bezpečnostní incidenty podle § 31,	√	NE		
462	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	h			zajistí zvládání kybernetických bezpečnostních incidentů podle stanovených postupů,	√	NE		
463	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	i			přijímá opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,	√	NE		
464	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	j			hlásí kybernetické bezpečnostní incidenty podle § 32,	√	NE		
465	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	k			vede záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání,	√	NE		
466	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	l			prošetří a určí příčiny kybernetického bezpečnostního incidentu a	√	NE		
467	VKB	§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů	1	m			vyhodnotí účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanoví nutná bezpečnostní opatření, popřípadě aktualizuje stávající bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.	√	NE		
469	VKB	§ 15	Řízení kontinuity činností					Povinná osoba v rámci řízení kontinuity činností	-		částečně řešeno	
470	VKB	§ 15	Řízení kontinuity činností	a				stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,	√	NE		
471	VKB	§ 15	Řízení kontinuity činností	b				pomocí hodnocení rizik a analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a posoudí možná rizika související s ohrožením kontinuity činností,	√	NE		
472	VKB	§ 15	Řízení kontinuity činností	c				na základě výstupů hodnocení rizik a analýzy dopadů podle písmene b) stanoví cíle řízení kontinuity činností formou určení	-		neřešeno	
473	VKB	§ 15	Řízení kontinuity činností	c	1			minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému,	√	NE		
474	VKB	§ 15	Řízení kontinuity činností	c	2			doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému, a	√	NE		

#	Zdroj	§	Název §	1	2	3	4	Text §	VIS	a / n	jak/čím plněno	kde kodifikováno/popsáno
475	VKB	§ 15	Řízení kontinuity činností	c	3			bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,	v	NE		
476	VKB	§ 15	Řízení kontinuity činností	d				stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c),	v	NE		
477	VKB	§ 15	Řízení kontinuity činností	e				vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a havarijní plány související s provozováním informačního a komunikačního systému a souvisejících služeb a	v	A/N	částečně řešeno	DR plán pro serverovnu
478	VKB	§ 15	Řízení kontinuity činností	f				realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti a vychází při tom z požadavků podle § 27.	v	NE		
479	VKB	§ 16	Audit kybernetické bezpečnosti	1				Povinná osoba v rámci auditu kybernetické bezpečnosti	-		neřešeno	
480	VKB	§ 16	Audit kybernetické bezpečnosti	1	a			provádí a dokumentuje audit dodržování bezpečnostní politiky, včetně přezkoumání technické shody, a výsledky auditu zohlední v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik a	v	NE		
481	VKB	§ 16	Audit kybernetické bezpečnosti	1	b			posuzuje 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.	v	NE		
482	VKB	§ 16	Audit kybernetické bezpečnosti	2				Audit podle odstavce 1 je prováděn	-		neřešeno	
483	VKB	§ 16	Audit kybernetické bezpečnosti	2	a			při významných změnách, v rámci jejich rozsahu,	v	NE		
484	VKB	§ 16	Audit kybernetické bezpečnosti	2	b			v pravidelných intervalech alespoň po 3 letech v případě povinné osoby uvedené v § 3 písm. e) zákona a	v	NE		
486	VKB	§ 16	Audit kybernetické bezpečnosti	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. V takovém případě je nutno audit v celém rozsahu provést nejpozději do 5 let.	v	NE		
487	VKB	§ 16	Audit kybernetické bezpečnosti	4				Audit kybernetické bezpečnosti musí být prováděn osobou vyhovující podmínkám stanoveným v § 7 odst. 4, která nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření.	v	NE		
488	VKB	§ 16	Audit kybernetické bezpečnosti	5				Povinná osoba, která je současně provozovatelem, předkládá výsledky auditu kybernetické bezpečnosti správci daného informačního a komunikačního systému.	v	NE		
618	VKB	§ 30	Bezpečnostní politika a bezpečnostní dokumentace	1				Povinná osoba	-			
619	VKB	§ 30	Bezpečnostní politika a bezpečnostní dokumentace	1	a			stanoví bezpečnostní politiku a vede bezpečnostní dokumentaci zahrnující oblasti uvedené v příloze č. 5,	v	NE		
620	VKB	§ 30	Bezpečnostní politika a bezpečnostní dokumentace	1	b			pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci a	v	NE		
621	VKB	§ 30	Bezpečnostní politika a bezpečnostní dokumentace	1	c			zajistí, aby byla bezpečnostní politika a bezpečnostní dokumentace aktuální.	v	NE		
622	VKB	§ 30	Bezpečnostní politika a bezpečnostní dokumentace	2				Bezpečnostní politika a bezpečnostní dokumentace musí být	-			
623	VKB	§ 30	Bezpečnostní politika a bezpečnostní dokumentace	2	a			dostupné v listinné nebo elektronické podobě,	v	NE		
624	VKB	§ 30	Bezpečnostní politika a bezpečnostní dokumentace	2	b			komunikovány v rámci povinné osoby,	v	NE		
625	VKB	§ 30	Bezpečnostní politika a bezpečnostní dokumentace	2	c			přiměřené dostupné dotčeným stranám,	v	NE		
626	VKB	§ 30	Bezpečnostní politika a bezpečnostní dokumentace	2	d			řízeny,	v	NE		
627	VKB	§ 30	Bezpečnostní politika a bezpečnostní dokumentace	2	e			chráněny z pohledu důvěrnosti, integrity a dostupnosti a	v	NE		
628	VKB	§ 30	Bezpečnostní politika a bezpečnostní dokumentace	2	f			vedeny tak, aby informace v nich obsažené byly úplné, čitelné, snadno identifikovatelné a snadno vyhledatelné.	v	NE		
846	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	1				Jednotlivé kybernetické bezpečnostní incidenty se kategorizují podle významnosti při zohlednění	-			
847	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	1	a			dopadů obsažených v dopadových určujících kritériích, podle kterých byly povinné osoby určeny,	v	NE		
848	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	1	b			počtu dotčených uživatelů,	v	NE		
849	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	1	c			způsobené nebo předpokládané škody,	v	NE		
850	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	1	d			důležitosti dotčených aktiv informačního a komunikačního systému,	v	NE		
851	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	1	e			dopadů na poskytované služby informačního a komunikačního systému,	v	NE		
852	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	1	f			dopadů na služby poskytované jinými informačními a komunikačními systémy,	v	NE		
853	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	1	g			délky trvání incidentu,	v	NE		
854	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	1	h			zeměpisného rozsahu dotčené oblasti a	v	NE		
855	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	1	i			dalších dopadů.	v	NE		
856	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	2				Pro potřeby hlášení a zvládání kybernetických bezpečnostních incidentů se na základě zohlednění podle odstavce 1 kybernetické bezpečnostní incidenty zařadí do následujících kategorií	-			

#	Zdroj	§	Název §	1	2	3	4	Text §	VIS	a / n	jak/čím plněno	kde kodifikováno/popsáno
857	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	2	a			Kategorie III - velmi významný 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,	v	NE		
858	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	2	b			Kategorie II - významný 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	v	NE		
859	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	2	c			Kategorie I - méně významný 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.	v	NE		
860	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	3				Typy kybernetických bezpečnostních incidentů podle dopadu jsou	-			
861	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	3	a			kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv,	v	NE		
862	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	3	b			kybernetický bezpečnostní incident způsobující narušení integrity aktiv,	v	NE		
863	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	3	c			kybernetický bezpečnostní incident způsobující narušení dostupnosti aktiv, nebo	v	NE		
864	VKB	§ 31	Kategorizace kybernetických bezpečnostních incidentů	3	d			kybernetický bezpečnostní incident způsobující kombinaci dopadů uvedených v písmenech a) až c).	v	NE		
865	VKB	§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	1				Kybernetický bezpečnostní incident se Úřadu hlásí na elektronickém formuláři zveřejněném na internetových stránkách Úřadu zaslaném	-			
866	VKB	§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	1	a			na adresu elektronické pošty Úřadu určenou pro příjem hlášení kybernetických bezpečnostních incidentů, zveřejněnou na internetových stránkách Úřadu,	v	NON		
867	VKB	§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	1	b			do datové schránky Úřadu, nebo	v	NON		
868	VKB	§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	1	c			prostřednictvím datového rozhraní, pokud je používáno, jehož popis je zveřejněn na internetových stránkách Úřadu.	v	NON		
869	VKB	§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	2				Kybernetický bezpečnostní incident se provozovateli národního CERT hlásí na elektronickém formuláři zveřejněném na internetových stránkách provozovatele národního CERT zaslaném	-			
873	VKB	§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	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.	v	NON		
874	VKB	§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	4				Náležitosti hlášení kybernetického bezpečnostního incidentu jsou	-			
875	VKB	§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	4	a			identifikace odesílatele,	v	NON		
876	VKB	§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	4	b			identifikace informačního a komunikačního systému,	v	NON		
877	VKB	§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	4	c			datum a čas zjištění incidentu a	v	NON		
878	VKB	§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů	4	d			popis incidentu.	v	NON		
879	VKB	§ 33	Reaktivní opatření	1				Povinná osoba, které Úřad uložil provést reaktivní opatření,	-			
880	VKB	§ 33	Reaktivní opatření	1	a			posoudí očekávané dopady reaktivního opatření na informační a komunikační systém a na zavedená bezpečnostní opatření a vyhodnotí možné negativní účinky a	v	NE		
881	VKB	§ 33	Reaktivní opatření	1	b			stanoví způsob rychlého provedení tohoto opatření, který minimalizuje jeho možné negativní účinky, a určí časový plán jeho provedení.	v	NE		
882	VKB	§ 33	Reaktivní opatření	2				Povinná osoba, které Úřad uložil provést reaktivní opatření, oznámí způsob provedení reaktivního opatření a jeho výsledek ve formě uvedené na internetových stránkách Úřadu.	v	NE		
883	VKB	§ 34	Kontaktní údaje	1				Kontaktní údaje se Úřadu oznamují na elektronickém formuláři zveřejněném na internetových stránkách Úřadu zaslaném	-			
884	VKB	§ 34	Kontaktní údaje	1	a			na adresu elektronické pošty Úřadu určenou pro příjem oznámení kontaktních údajů, zveřejněnou na internetových stránkách Úřadu,	v	ANO		
885	VKB	§ 34	Kontaktní údaje	1	b			do datové schránky Úřadu, nebo	v	ANO		
886	VKB	§ 34	Kontaktní údaje	1	c			prostřednictvím datového rozhraní, pokud je používáno, jehož popis je zveřejněn na internetových stránkách Úřadu.	v	ANO		
887	VKB	§ 34	Kontaktní údaje	2				Kontaktní údaje se provozovateli národního CERT oznamují na elektronickém formuláři zveřejněném na internetových stránkách provozovatele národního CERT zaslaném	-			

#	Zdroj	§	Název §	1	2	3	4	Text §	VIS	a / n	jak/čím plněno	kde kodifikováno/popsáno
891	VKB	§ 34	Kontaktní údaje	3				Hlášení kontaktních údajů je možné zaslat i v listinné podobě, avšak pouze v případech, kdy nelze využít žádný ze způsobů uvedených v odstavcích 1 a 2.	v	ANO		
892	VKB	§ 34	Kontaktní údaje	4				Vzor oznámení kontaktních údajů je uveden v příloze č. 8 k této vyhlášce.	v	ANO		
893	VKB	§ 34	Kontaktní údaje	5				Povinná osoba uvedená v § 3 písm. c) až f) zákona, která je provozovatelem, dále k hlášení kontaktních údajů podle odstavce 1 přikládá dokument, kterým ji správce prokazatelně informuje podle § 8 odst. 1 písm. c).	v	ANO		

Příloha III: Ukázka evidence zranitelností (Zdroj: Vlastní zpracování)

ID	Popis zranitelnosti	Komentář
Z01	Nedostatečná údržba informačního a komunikačního systému	
Z02	Zastaralost informačního a komunikačního systému	
Z03	Nedostatečná ochrana vnějšího perimetru	
Z04	Nedostatečné bezpečnostní povědomí uživatelů a administrátorů	
Z05	Špatné nebo neexistující nastavení smluvních závazků, špatné řízení dodavatelů	Špatné nebo neexistující nastavení smluvních závazků, SLA,pokuty a sankce apod.
Z06	Nevhodné nastavení přístupových oprávnění	
Z07	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	
Z08	Nedostatečné monitorování a logování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	
Z09	Nedostatečné nebo žádné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí, jejich nedodržení	
Z10	Nedostatečná ochrana aktiv (např. serevrů, koncových zařízení, síťových prvků)	
Z11	Nevhodná bezpečnostní architektura	
Z12	Nedostatečná míra nezávislé kontroly	
Z13	Neschopnost včasného odhalení pochybení	
Z14	Nechráněné komunikační přenos (absence šifrování)	Chybějící šifrování, linky přístupné ve veřejném prostoru mimo kontrolu MZe
Z15	Modifikace či odposlech elektronické komunikace	Modifikace či odposlech elektronické komunikace (např. man-in-the-middle)
Z16	Nechráněná hesla	Hesla uložená v čitelném textu v IS, nosičích, fyzicky napsané, v tabulkách, skriptech apod.
Z17	Neoprávěné použití software	Užití SW mimo licenční ujednání, použití mimo určený účel apod.
Z18	Chybějící podpora ze strany výrobce	Žádné či velmi špatné poskytování podpory výrobce
Z19	Nedostatečná kontrola přístupů dodavatelů	Žádné či nedostatečná kontrola přístupů, auditovaný záznam, ukládání záznamů po krátký čas
Z20	Nedostatečně zajištěná fyzická bezpečnost	Nedostatečně zajištěná fyzická bezpečnost, neexistence režimových zón, chráněných DC apod.
Z21	Nedostatečné řízení přístupu	Žádné či nedostatečné řízení přístupů
Z22	SW zranitelnost zařízení	Zranitelnost či chyba v kódu
Z23	Zero-day zranitelnosti	Zranitelnost používaného software, která není ještě obecně známá, resp. pro ni neexistuje obrana
Z24	Backdoor, úmyslný nebezpečný kód	HW a SW výrobce může obsahovat nežádoucí funkce, úmyslný backdor, škodlivý kód výrobce, které běžnými prostředky nelze odhalit, Úmyslný backdoor, či jiné nežádoucí funkce
Z25	Nedostatečné monitorování a logování	Žádné či chybějící logování a monitoring, ukládání záznamů po krátký čas
Z26	Nedostatečné řízení bezpečnostních incidentů	
Z27	Nedostatečná správa a řízení technických zranitelností	
Z28	Podvržení sítě	
Z29	Nedostatečná ochrana před škodlivým kódem (viry, malware, červy, sopustitelné řetězce a příkazy apod.)	Např. chybějící či nektualizovaný antivir, sandbox, antimalvare apod.
Z30	Nevhodné umístění aktiv	
Z31	Chybějící záložní zdroje energie	
Z32	Skrytý privilegovaný přístup	Neznámé servisní účičty, které jsou skryté a která zná pouze výrobce (např. spustitelné v CMD apod.)
Z33	Špionážní zařízení	Primárně HW výrobce, který může obsahovat nežádoucí funkce, např. umožní vypnutí zařízení, odesílání dat ze zařízením prostřednictvím radiokomunikace či jinak, které běžnými prostředky nelze odhalit. Zařízení může být součástí desky nebo chipu dodávaného zařízení a je běžnými prostředky neodhalitelné.

Příloha IV: Ukázka evidence hrozeb (Zdroj: Vlastní zpracování)

ID	Popis hrozby	Komentář
H01	Porušení bezpečnostní politiky a stanovených pravidel, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	Zaměstnanec nebo dodavatel jedná v nesouladu s pravidly a postupy bezp. politiky.
H02	Poškození nebo selhání technického anebo programového vybavení	Technické selhání hostitelského počítače, serveru, úložiště nebo síťové infrastruktury nebo selhání (výpadek, nesprávná funkce) operačního systému, síťového operačního systému nebo aplikace. Zahrnuje i nedostatečnou kontrolu vstupních dat.
H03	Zneužití či podvrhnutí identity	
H04	Užívání programového vybavení v rozporu s licenčními podmínkami	
H05	Škodlivý kód (nap. viry, spyware, trojské koně, kryptoviry)	Zavedení počítačových virů, červů a jiného malware do IS (např. při instalaci, ze záložního média, z přílohy e-mailu, webové stránky atd.). Zahrnuje i trvale působící hrozby (APT).
H06	Narušení fyzické bezpečnosti	
H07	Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie	Selhání nebo úmyslné přerušení komunikačních linek a sítí (např. změna směrovacích tabulek nebo výpadek služeb poskytovaných třetí stranou). Zahrnuje také všechny případy selhání dodávky elektřiny (výpadek, ...).
H08	Zneužití nebo neoprávněná modifikace údajů, informací	
H09	Ztráta, odcizení nebo poškození aktiva, informace, dat	Ztráta, odcizení nebo poškození zařízení, média, informace, dokumentu apod.
H10	Nedodržení smluvního závazku ze strany dodavatele	Narušení atributů informační bezpečnosti ze strany dodavatele
H11	Pochybení ze strany zaměstnanců, uživatelů, administrátorů	Omyly při údržbě hardware a software, např. chyby administrátorů při úpravách konfigurací nebo instalaci software.
H12	Zneužití vnitřních prostředků, systémových zdrojů, sabotáž	Použití HW či SW a jejich služeb pro jiné, než určené účely (např. stahování videa, používání aplikací pro osobní potřebu atd.), které může snižovat jejich výkon nebo dostupnost. Hrozbu způsobí vnitřní zaměstnanec.
H13	Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	
H14	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Absence klíčového personálu, nedostatek zaměstnanců s potřebnou odbornou úrovní
H15	Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	Pokus o zneužití zranitelnosti podpůrného aktiva. Může mít za následek odepření služby, získání přístupu k datům, modifikaci dat, spuštění cizího kódu atd. Zahrnuje útok přes klasickou i bezdrátovou síť (Wi-Fi, BT) a USB aj. Zahrnuje i DOS a DDOS útoky. Případy manipulace lidí za účelem provedení určité akce nebo získání určité
H16	Zneužití vyměnitelných technických nosičů dat	
H17	Trvale působící a pokročilé technické hrozby, technické špionáže	
H18	Odepření/odmítnutí služby	
H19	Neoprávněný přístup a manipulace s aktivem nebo daty	Kontrola nad obsahem informací a dat. Používání účtů, které nejsou jejich vlastní, pracovníky organizace nebo pracovníky dodavatelských organizací. Zahrnuje např. přímé zneužití přihlašovacích údajů, hádání hesel a další útoky na autentizační mechanismus, použití počítače po přihlášení oprávněného uživatele apod. Zahrnuje také eskalaci práv a odcizení autentizačních údajů.
H20	Lokalizace uživatelů	Lokalizace uživatele podle IP adresy v komunikaci přenášené v síti, nebo ukládané v informačním systému.
H21	Napadení elektronické komunikace (odposlech, modifikace)	Infiltrace komunikace – tedy manipulace s normálním tokem dat při přenosu (např. replay attack, změna dat). Odposlouchávání komunikací – tedy pokusy o narušení důvěrnosti elektronicky přenášených dat jejich zachycením.
H22	Pořizování záznamu (audio, video)	
H23	Zaznamenávání hovorů	Zaznamenávání hovorů, odposlech v telefonní síti
H24	Nesprávné řízení bezpečnosti	Selhání business procesů. Hrozba zahrnuje situace, ve kterých dochází k chybám při řízení bezpečnosti (např. nedodržení zákonných a smluvních požadavků atd.).