Technická opatření kybernetické bezpečnosti

Bc. Martin Hořický

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Martin Hořický**
Osobní číslo:	**A17460**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Technická opatření kybernetické bezpečnosti**
Téma práce anglicky:	**Technical Measures of Cybersecurity**

Zásady pro vypracování

1. Proveďte literární rešerší na dané téma.
2. Shromážděte požadavky na řešení.
3. Navrhněte technické řešení ve formě doporučení na zlepšení bezpečnosti.
4. Zdůvodněte volbu jednotlivých doporučení technického řešení.
5. Realizujte a otestujte odpovídající část technického řešení ve spolupráci s uživatelem.
6. Věnujte pozornost zabezpečení.

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

Seznam doporučené literatury:

1. ČESKO. Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti. In: Sbírka zákonů České republiky. 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181
2. ČSN EN ISO/IEC 27000. Informační technologie –Bezpečnostní techniky –Systémy řízení bezpečnosti informací – Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2020.
3. JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 9788074543128. Dostupné také z: http://hdl.handle.net/10563/25821
4. POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice. ISBN 8086898385.
5. ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 147 s. ISBN 9788073807375.
6. GUPTA, Manish, Raj SHARMAN a John WALP. Information technology risk management and compliance in modern organizations. Hershey: Business Science Reference, [2017], 1 online zdroj. ISBN 9781522526056. Dostupné také z: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1540761&authtype=ip,shib&custid=s3936755
7. STALLINGS, William a Lawrie BROWN. Computer security: principles and practice. Fourth edition. Chennai: Pearson, [2020], 800 atrn. ISBN 978-93-534-3886-9.

Vedoucí diplomové práce: **Ing. Tomáš Kadavý**
Ústav informatiky a umělé inteligence

Konzultant diplomové práce: **Ing. Ivan Masár**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. prosince 2021**
Termín odevzdání diplomové práce: **23. května 2022**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 7. února 2022

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 24.5.2022 Martin Hořický, v.r.

podpis studenta

ABSTRAKT

Diplomová práce se zabývá nutnými opatření pro zavedení požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti pro modelovou univerzitu v České republice. V první části práce je uveden rozsah zákona a také další povinnosti subjektů řídících se tímto zákonem. Společně s tím byla realizována analýza organizačních a technických opatření a identifikovány neshody. V druhé části jsou popsány nutné body pro implementaci požadavků zákona a také nezbytné technické opatření s ohledem na rozsah identifikovaných systémů.

Klíčová slova: zákon o kybernetické bezpečnosti, kybernetická bezpečnost, kybernetický bezpečnostní incident

ABSTRACT

This diploma thesis deal with necessary measurements in the case of the implementation of the requirements of Cybersecurity law no. 181/2014 for the model university in the Czech Republic. First part includes analysis of mentioned law above, including other obligations of the organization operates under it. Together with-it vulnerability scan of the applications and analysis of the law impact was performed. In the second part required steps are described for the implementation of the requirements of the law. Technical measurements are described too.

Keywords: cyber security law, cyber security, cyber security incident, information lifecycle

Děkuji touto cestou Ing. Tomáši Kadavému za pomoc, cenné rady a čas, který mi věnoval při tvorbě této diplomové práce.

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

OBSAH

ÚVOD

Kybernetická bezpečnost je zcela zásadní oblast a potřeba všech společností. Rizika spojená s výsledkem úspěšného útoku mají nemalý dopad na provozuschopnost celé společnosti. Nejen v rámci zemí Evropské unie je zavedena regulace pro subjekty veřejné moci, což jsou mimo jiné poskytovatelé kritické infrastruktury. Omezení poskytování jejich služeb by mělo zásadní dopad nejen na větší množství obyvatel.

V území České republiky je právní regulace zajištěna Zákonem o kybernetické bezpečnosti č. 181/2014 Sb. a také doprovodnou vyhláškou. Zavedení legislativních požadavků je následně povinen každý subjekt, který je identifikován. Když opomeneme legislativní povinnost, tak samotné zavedení opatření je vzhledem k vývoji kybernetických hrozeb vhodné pro všechny společnosti na území každého státu. Kybernetické útoky nejsou výjimkou a ojedinělým jevem, který se stane jenom občas.

Tato práce se zaměřuje na zavedení požadavků Zákona kybernetické bezpečnosti u subjektu provozujícího významný systém. V první části je proveden rozbor legislativních požadavků, společně se stručným rozborem připravované legislativy Evropské unie NIS2. V analytické části je provedena identifikace požadavků a následně navržena opatření pro zajištění souladu.

Jako předměty této práce jsem definoval:

- Analýza provedení literární rešerše legislativních požadavků
- Analýza prostředí společnosti a identifikace nezbytných bodů pro zajištění souladu
- Návrh opatření pro samotné zajištění souladu

I. TEORETICKÁ ČÁST

1 ZAVEDENÍ POŽADAVKŮ ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

Kybernetická kriminalita a s ní spojená odpovídající rizika je velmi skloňované téma**.**

Kybernetická bezpečnost byla dříve chápana jako oblast, která má dopad jenom na vybrané společnosti a není z ní problém, který může mít dopad. Společně s rostoucí digitalizací i služeb státu byl tento problém stále více skloňován a také legislativně ukotven v Zákoně č. 181/2014 Sb. o kybernetické bezpečnosti (dále jen ZOKB)

Jako základ výše uvedeného zákona jsou standardy ISO/IEC skupiny 27000. Praxi z těchto ze standardů je samozřejmě také možné nalézt ve velkém množství i jiných ověřovacích standardů pro prostředí IT. Zákon č. 181/2014 Sb. je reakcí na rizika v oblasti informační infrastruktury formou zajištění bezpečnosti odvětví, kde narušení bezpečnosti může mít zásadní význam na poskytování služeb státu, či života jeho občanů. Do jeho subjektů, které mu podléhají nepatří tedy jenom služby státu, ale také subjekty, které jsou pro ně potřebné. Mohu zde například zmínit energetiku, telekomunikace, produkce potravin, logistiku, zdravotnictví, či definované subjekty veřejné moci. Kde je ještě stále je mírně opomenut, je také jeho vliv na dodavatelský řetězec poskytující služby subjektům spadajícím pod působnost zákona. Postupem času jsou do jeho působnosti zařazováni vybraní dodavatelé.

Zajištění informační bezpečnosti se také intenzivně věnuje bankovní sektor, kde je tato oblast již dlouhodobě řešena. Rostoucí digitalizace i v průmyslu zcela jistě rozšíří v dalších letech jeho působnost také na klíčové průmyslové podniky.

Tato diplomová práce má za cíl realizaci analýzy prostředí modelové univerzity, identifikaci souladu s požadavky zákona na základě provedení analýzy dle ISO/IEC 27001, provedení technických testů vybraných systémů a návrhu opatření pro implementaci požadavků zákona.

Pro účinné zavedení opatření v kybernetické bezpečnosti je důležité se zaměřit na tři otázky [7]:

1. Jaká aktiva musíme chránit?
2. Jak jsou aktiva ohrožena?
3. Co můžeme udělat, abychom těmto hrozbám čelili?

1.1 Legislativní požadavky

V kapitolách jsou uvedeny legislativní požadavky ve vztahu na ZOKB.

1.1.1 Zákon o kybernetické bezpečnosti

Vzhledem k tomu, že cíle této práce není podrobný rozbor Zákona č. 181/2018 Sb., ale jeho implementace, v této práci nejsou rozebrány detailně veškeré jeho části. Pro zajištění alespoň úvodní míry detailu níže uvádím jeho zásadní body.

Hlavním gestorem zákona je Národní úřad pro kybernetickou bezpečnost.

Z pohledu evropského práva tento zákon odkazuje na následující evropskou regulaci:

- **32016R0679** – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Text s významem pro EHP)
- **32016L1148** – Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a in-formačních systémů v Unii
- **31995L0046** – Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti vešel v platnost dne 1. ledna 2015 a společně s ním také následující prováděcí vyhlášky:

- č. 316/2014 Sb. o kybernetické bezpečnosti
- č. 317/2014 Sb. o významných informačních systémech
- č. 437/2017 Sb. o kritériích pro určení provozovatele základní služby
- č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- č. 315/2021 Sb. o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci

Novelizace zákona byla provedena na základě následujících zákonů:

- 261/2021 Sb. Zákon, kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci
- 12/2020 Sb. Zákon o právu na digitální služby
- 111/2019 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů
- 35/2018 Sb. Zákon o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny
- 205/2017 Sb. Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony
- 183/2017 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích
- 104/2017 Sb. Zákon, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony

Obsah tohoto zákona také mění velkou řadu dalších zákonů v České republice. Mezi ty patří následující:

- 418/2021 Sb. Zákon, kterým se mění zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, zákon č. 17/2012 Sb., o Celní správě České re-publiky, ve znění pozdějších předpisů, zákon č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů, a další související zákony
- 374/2021 Sb. Zákon, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony
- 315/2021 Sb. Vyhláška o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci
- 284/2021 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím stavebního zákona

- 283/2021 Sb. Zákon stavební zákon
- 270/2021 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o občanských průkazech
- 261/2021 Sb. Zákon, kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci
- 150/2021 Sb. Zákon, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony
- 36/2021 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o Sbírce právních předpisů územních samosprávných celků a některých správních úřadů
- 34/2021 Sb. Zákon o prověřování zahraničních investic
- 573/2020 Sb. Vyhláška, kterou se mění vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby
- 360/2020 Sb. Vyhláška, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb.
- 254/2020 Sb. Nález ÚS ČR o zrušení ustanovení, zamítnutí, zastavení a odmítnutí návrhu na zrušení ustanovení zákona č. 395/2009 Sb., o významné tržní síle při prodeji zemědělských a potravinářských produktů a jejím zneužití
- 12/2020 Sb. Zákon o právu na digitální služby
- 311/2019 Sb. Zákon, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů
- 277/2019 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o Sbírce zákonů a mezinárodních smluv
- 111/2019 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů
- 82/2018 Sb. Vyhláška o kybernetické bezpečnosti
- 35/2018 Sb. Zákon o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny

- 252/2017 Sb. Zákon, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a zákon č. 483/1991 Sb., o České televizi, ve znění pozdějších předpisů
- 205/2017 Sb. Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony
- 194/2017 Sb. Zákon o opatřeních ke snížení nákladů na zavádění vysokorychlostních sítí elektronických komunikací a o změně některých souvisejících zákonů
- 183/2017 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích
- 104/2017 Sb. Zákon, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony
- 426/2016 Sb. Nařízení vlády o posuzování shody rádiových zařízení při jejich dodávání na trh
- 298/2016 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů
- 205/2016 Sb. Vyhláška, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- 378/2015 Sb. Zákon, kterým se mění zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů, a některé další zákony
- 318/2015 Sb. Zákon, kterým se mění zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů, zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, zákon

č. 329/1999 Sb., o cestovních dokladech, ve znění pozdějších předpisů, a další související zákony

- 222/2015 Sb. Zákon, kterým se mění zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
- 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích
- 316/2014 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- 250/2014 Sb. Zákon o změně zákonů souvisejících s přijetím zákona o státní službě
- 181/2014 Sb. Zákon o kybernetické bezpečnosti
- 273/2008 Sb. Zákon o Policii ČR
- 289/2005 Sb. Zákon o Vojenském zpravodajství
- 127/2005 Sb. Zákon o elektronických komunikacích

1.1.2 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Podstatnou částí zákona je vymezení oblasti jeho působení a definice pojmů. Pro účely této práce je klíčové definovat osoby a orgány, kterých se týká. Z pohledu zákona se jedná zejména o následující osoby a orgány:

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),

b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d),

c) správce informačního systému kritické informační infrastruktury,

d) správce komunikačního systému kritické informační infrastruktury

e) správce významného informačního systému. [1]

Zákon pak následně v dalších paragrafech vymezuje bezpečnostní opatření, kterou jsou oso-by povinny ze zákona zabezpečit. Bezpečnostní opatření jsou vždy rozdělena na organizační a

technická. S ohledem na dobrou praxi je samozřejmě kladen větší důraz na technická, organizační představují jenom rámec povinností daného subjektu.

V oblasti kybernetické bezpečnosti jsou dlouhodobě upřednostňována technická opatření, zejména z důvodu že mají mnohem větší vliv na potenciální rizika. Z mého pohledu vyjma nezbytných opatření je zcela klíčové mít korektně zavedený systém řízení rizik a dle jeho výstupů komplexně řídit celou oblasti informační bezpečnosti. Bez znalosti rizik není totiž možné zcela korektně realizovat opatření na jejich zmírnění a může se stát, že jsou nasazena opatření, které v lepším případě jenom částečně vyřeší rizika.

Z pohledu zákona je také důležitou části povinnost subjektů hlásit kybernetické události a incidenty. Na veškeré incidenty následně i reaguje NUKIB a mj. i formou podpory na místě incidentu.

V dalších částech zákon definuje opatření, které je nutné provést k ochraně před hrozbami v kyberprostory. Obecně je vždy jedná o varování, reaktivní a ochranná opatření

1.1.3 Vyhláška č. 316/2014 Sb. o kybernetické bezpečnosti

Je velice podstatným dokumentem pro zavedení požadavků zákon č. 181/2014 Sb. a stanovuje obsah a strukturu bezpečnostní dokumentace pro systémy spadající pod tento zákon.

Tato vyhláška také obsahuje výčet bezpečnostních opatření a rozsah jejich zavedení, typy kybernetických incidentů, náležitosti jejich hlášení. Je také předmětem pro zavedení systému informační bezpečnosti. Jejím obsahem je také rozpracování do podrobností technických opatření.

Mezi ty se dle této vyhlášky řadí:

- fyzická bezpečnost,
- nástroj pro ochranu integrity komunikačních sítí,
- nástroj pro ověřování identity uživatelů,
- nástroj pro řízení přístupových oprávnění,
- nástroj pro ochranu před škodlivým kódem,
- nástroj pro zaznamenávání činnosti kritické informační infrastruktury

a významných informačních systémů, jejich uživatelů a administrátorů,

- nástroj pro detekci kybernetických bezpečnostních událostí,
- nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
- aplikační bezpečnost,
- kryptografické prostředky,
- nástroj pro zajišťování úrovně dostupnosti informací,
- bezpečnost průmyslových a řídících systémů [2]

1.1.4 Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích

Obsahem této vyhlášky je určení kritérií, které je nutné splnit, aby byl systém označen jako významný. Určující kritéria jsou rozdělena na dopadová a oblastní.

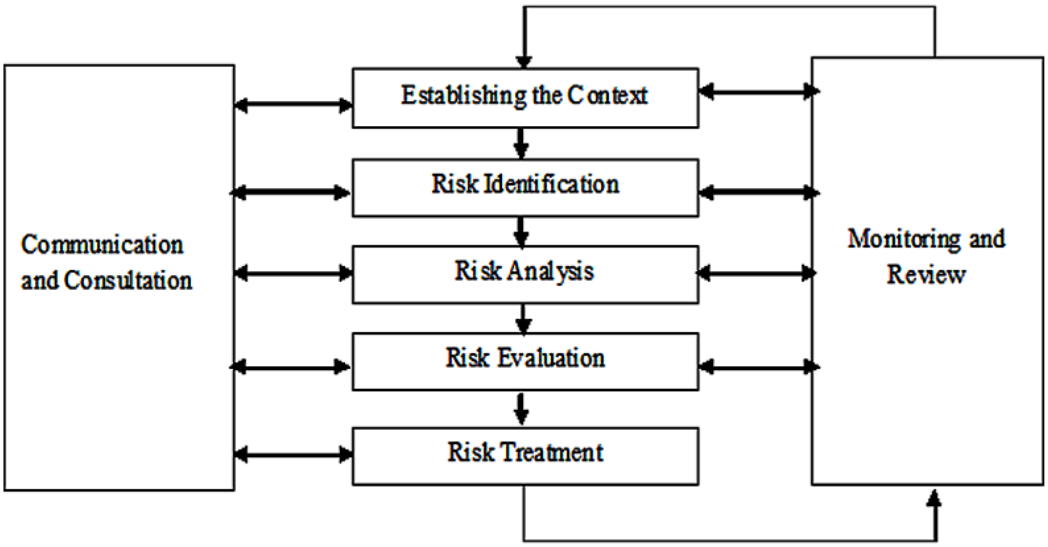
Dopadová vyhodnocují dopady napadení informačního systému s ohledem na fungování a hospodaření orgánů veřejné moci, vliv na poskytování služeb a informační bezpečnost, či zásah do osobního života.

Oblastní určující kritéria jsou rozdělena na orgány veřejné moci a kraje v rámci přenesené působnosti, ovšem u obou jsou téměř hodné oblasti, kterými jsou: vedení správního řízení, databáze obsahující osobní údaje, hospodaření orgánu veřejné moci, výkon spisové služby, státní dozor, kontrolní a inspekční činnost, příprava na krizové situace a jejich řešení, tvor-ba právních předpisů, elektronická pošta, vedení internetových stránek, mezirezortní spolu-práce, mezinárodní spolupráce, zadávání veřejných zakázek, státní statistická služba. [3]

Při přihlédnutí ke všem kritériím je zcela patrné, že vliv zákona se projevuje v rámci celé nejen veřejné správy, ale také subjektů na ně na navázaných.

1.2 Řízení rizik

Níže uvedená kapitola obsahuje metodiku řízení rizik a opatření nezbytné pro jejich zavedení. Samotné řízení rizik představuje ucelený proces a jeho postup je vyobrazen na obrázku níže.



Obrázek č. 1 - Proces managementu řízení rizik [4]

1.2.1 Identifikace aktiv

Primárním cílem vyhodnocení aktiv je jejich rozlišení, identifikace vlastníka a jejich významu pro společnosti.

V rámci identifikace budeme rozlišovat dva hlavní druhy:

1. Primární aktiva – informace nebo služby zpracovávané, nebo poskytované společností nebo její informační systémy

2. Sekundární aktiva – aktiva zajišťující podmínky pro provoz primárních aktiv (technické vybavení – SW, HW, zaměstnance, dodavatele, partnery, budovy atd.)

Správná identifikace aktiv je klíčovou součástí následných kroků, a to zejména s ohledem na korektní zařazení a vyhodnocení. V této oblasti je také zásadní, aby rozlišení nebylo příliš detailní a tím se stalo těžce udržitelné.

1.2.2 Posouzení aktiv

Hodnota každého aktiva bude vyhodnocena na základě jejich důvěrnosti, integrity a dostupnosti dopad vyhodnocen na základě potenciálního dopadu v případě vzniku hrozby. Násled-né vyhodnocení dopadu bude provedeno na základě čtyř stupňové škály.

1.2.3 Posouzení důvěrnosti

Posouzení důvěrnosti bude realizováno na základě evaluace aktiv a zajištění omezení přístupu pouze pro určené osoby. Důvěrnost bude vypočítána na základě aktiva, označeného jako ACx dle následující škály.

Hodnota AC		Popis
1	Nízká	Jedná se o veřejně přístupné informace, anebo informace, které byly určeny k publikaci veřejnosti. Jejich únik nemá žádný dopad na společnost
2	Střední	Jedná se o informace, které nejsou veřejně dostupné a zahrnují interní informace společnosti. Jejich ochrana není vyžadována na základě právní úpravy, či smluvního vztahu.
3	Vysoká	Jedná se o informace, které nejsou veřejně dostupné a zahrnují interní informace společnosti. Jejich ochrana je vyžadována na základě právní úpravy, či smluvního vztahu (obchodní tajemství, osobní údaje)
4	Kritická	Jedná se o informace, které nejsou veřejně dostupné a zahrnují interní informace společnosti. Jejich ochrana je vyžadována na základě právní úpravy, či smluvního vztahu (strategické informace, citlivá osobní data). Jejich únik by měl zásadní dopad na společnost

Tabulka č. 1 - Stupně důvěrnosti aktiv

1.2.4 Posouzení integrity

Integrita aktiv bude vyhodnocena na základě vyhodnocení, zdali jsou informace správné, odpovídající a kompletní. Integrita bude vypočítána na základě aktiva, označeného jako AIx dle následující škály.

Hodnota AA		Popis
1	Nízká	Narušení dostupnosti nemá zásadní dopad na společnost.
2	Střední	Narušení dostupnosti by nemělo být delší než jeden týden, v opačném případě to má dopad na společnost.
3	Vysoká	Narušení dostupnosti nesmí být delší než jeden den.
4	Kritická	Kritická aktiva, kde dostupnost musí být zajištěna ve velmi krátkém čase.

Tabulka č. 2 - Stupně dostupnosti aktiv

„V případě integrity je potřeba si uvědomit, že pokud dojde k nežádoucí změně dat (a to ať už úmyslně, náhodou, či technickým selháním v důsledku působení vyšší moci), nemusí být tato nežádoucí změna vůbec odhalena a může uplynout dlouhá doba, než si někdo něčeho všimne. Čím později se na tento bezpečnostní incident přijde, tím vážnější bude jeho dopad. Problém spočívá v tom, že je velice obtížné dohledat, jaká byla ona původní hodnota, protože nebudeme vědět, kdy přesně ke změně došlo.“ [5]

1.2.5 Průměrné vyhodnocení aktiv

Hodnota aktiv bude vypočtena na základě následujícího vzorce.

$$A_X = \mathbf{Round}\left(\frac{AC_X + AI_X + AA_X}{3}\right)$$

Následné rozlišení aktiv bude realizováno dle následujícího rozlišení:

Hodnota A_x	Popis
1	Aktivum má nízkou významnost pro společnost
2	Aktivum má střední významnost pro společnost
3	Aktivum má vysokou významnost pro společnost
4	Aktivum má kritickou významnost pro společnost

Tabulka č. 3 - Hodnocení významnosti aktiv

1.2.6 Identifikace rizik

Identifikace rizik představuje pravidelné a kontinuální monitorování všech probíhajících interních a externích událostí, které ovlivňují naplňování cílů. U těchto událostí pak rozlišujeme pozitivní nebo negativní dopad. Události, které mají negativní dopad, jsou rizika. Identifikace rizik spočívá ve zjištění a strukturované evidenci významných potenciálních rizik. Seznam potenciálních rizik je zpracováván formou tzv. databáze rizik. Registr rizik pak obsahuje seznam řízených, nejvýznamnějších rizik.

1.2.7 Rizika v informační bezpečnosti

Identifikace rizik a jejich vyhodnocení je klíčovou částí systému informační bezpečnosti, které zahrnuje opatření pro zajištění bezpečnosti informací s důrazem na zajištění dostupnosti, integrity a důvěrnosti zpracovávaných informací.

Primární cílem bude identifikace primárních a sekundárních aktiv, identifikace potenciálních hrozeb a zranitelností k nim a také definice odpovídajících bezpečnostních opatření. Implementace bezpečnostních opatření bude provedena v rámci mitigace identifikované výše rizika.

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

Tabulka č. 4 - Stupnice pro hodnocení hrozeb v informační bezpečnosti

Stupnice pro hodnocení zranitelností - V_{xy}	
Úroveň	Popis
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, které jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
Střední	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání

	opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Tabulka č. 5 - Stupnice pro hodnocení zranitelností v informační bezpečnosti

1.2.8 Zpracování analýzy rizik

Riziko většinou neexistuje izolovaně, ale obvykle se jedná o určité kombinace rizik, které mohou ve svém dopadu představovat hrozbu pro obchodní cíle společnosti. Vzhledem k množství rizik je třeba určit priority z pohledu dopadu a pravděpodobnosti jejich výskytu a zaměřit se na klíčové rizikové oblasti.

Analýza rizik se zabývá odhalováním a pochopením rizik. Poskytuje podklady pro rozhodnutí o nutnosti zabývat se určenými riziky a doporučuje nejvhodnější a nákladově efektivní strategii zvládání rizik. Analýza rizik obsahuje odhalení zdrojů rizik, jejich příznivých a nepříznivých následků a možností, že se tyto následky přihodí. Mohou být identifikovány faktory, které ovlivňují následky a jejich pravděpodobnosti. Rizika se analyzují spojením následků a jejich pravděpodobností. Ve většině případů se berou v úvahu už existující opatření.

Při vypracování analýzy rizik aplikujeme následující postupy a to i v jejich kombinaci:

- postup založený na systematické kontrole plnění předem stanovených podmínek a opatření (směrnice, procesy),
- postup hledající rizikové situace a navržení opatření pro zvýšení spolehlivosti a efektivity systému, hledání možného selhání,
- postup hledání možných dopadů konkrétních situací (co se stane, když),
- postup založený na vyhledávání nebezpečných stavů, nouzových situací, jejich příčin a dopadů a na jejich zařazení do kategorií dle předem stanovených kritérií,

- systematický a komplexní přístup pro predikci odhadu, četnosti a dopadů rizikových situací při provádění provozních činností,
- identifikace scénářů potenciálního rizika na základě brainstormingu,
- postup, který sleduje průběh procesu od počátku prostřednictvím konstruování jeho průběhu, vždy na základě dvou možností: příznivé a nepříznivé,
- postup založený na rozboru způsobů selhání a jejich důsledků, který umožňuje hledání dopadů a příčin na základě systematicky a strukturovaně vymezených selhání systému,
- postup založený na systematickém zpětném rozboru události za využití řetězce příčin, které mohou vést k vybrané vrcholové události,
- postup posouzení vlivu lidského činitele.

1.2.9 Vyhodnocení rizik

Vyhodnocení významnosti (resp. důležitosti) identifikovaných rizik provádí odborně vybavený expert, nebo skupina expertů. Skupinové hodnocení základního souboru rizik respondenty probíhá zpravidla formou řízené skupinové diskuse a jeho výstupem je jednak posouzení a popř. modifikace základního souboru potenciálních rizik, jednak jejich počáteční vyhodnocení z hlediska jejich významnosti. Předmětem hodnocení je u každého rizika velikost jeho dopadu D a pravděpodobnost výskytu P. Dopad i pravděpodobnost jsou hodnoceny v kvantitativních škálách s definovaným významem jednotlivých stupňů škály.

Stupeň dopadu rizika „D“ je hodnocen dle následující stupnice:

ÚROVEŇ	OZNAČENÍ DOPADU	ZÁVAŽNOST DOPADU
1	téměř neznatelný	neovlivňuje znatelně fungování, neřeší se na úrovni managementu
2	drobný	ovlivňuje pouze dílčí aktivity, řeší většinou vedoucí zaměstnanec útvaru
3	významný	vyžaduje okamžité řešení situace, vyžaduje se řešení od střední úrovně vedení
4	velmi významný	významná ztráta, soudní spor, významné poškození majetku, vyžaduje se řešení od vrcholového vedení společnosti

5	katastrofický	ztráta majetku, podnikání/významná ztráta, vyžaduje se řešení od vrcholového vedení společnosti

Tabulka č. 6 - Stupně dopadu rizika

Velikost pravděpodobnosti výskytu rizika „P“ je hodnocena dle následující stupnice:

ÚROVEŇ	OZNAČENÍ	INTERVAL PRAVDĚPODOBNOSTI
1	téměř vyloučené	vyskytuje se pouze ve výjimečných případech
2	nepravděpodobné	vyskytnout se může, ale nemusí také vůbec
3	možné	někdy se může vyskytnout
4	pravděpodobné	pravděpodobně se vyskytne
5	téměř jisté	vyskytne se skoro vždy

Tabulka č. 7 - Pravděpodobnost výskytu rizika

Parametr míra rizika „V“ je dán součinem bodového ohodnocení dopadu rizika „D“ (dopad) a pravděpodobnosti výskytu rizika „P“. V = D x P

Výpočet výše rizika v informační bezpečnosti

Finální riziko bude vypočteno na základě následujícího vzorce.

Samotný výpočet bude proveden podle vyhodnocení jednotlivých oblastí,

kde:

1. TP_x – hrozba
2. V_{xy} – zranitelnost
3. A_y – průměrná hodnota aktiva

$$\boldsymbol{R_{XY} = A_Y * V_{XY} * TP_X}$$

Veškeré hodnoty jsou vždy dle obdobné škály, jako v případě aktiv (4 bodové).

Vypočtená výše rizika může dosahovat následující stupnice:

Hodnota rizika		Popis
1–15	Nízké	Riziko je akceptovatelné

Hodnota rizika		Popis
16–31	Střední	Riziko může být sníženo, jeho hodnota může být přenesena, či mitigována
32–47	Vysoké	Riziko je neakceptované po delší období, jeho hodnota musí být snížena
48–64	Kritické	Riziko není akceptovatelné v daném čase a musí být okamžitě řešeno

Tabulka č. 8 - Vyhodnocení výše rizika v informační bezpečnosti

Výsledky identifikace rizik je potřeba analyzovat a určit priority jejich řešení. Pokud máme známá rizika, která nám vyšla z předchozí identifikace, již můžeme tato rizika hodnotit a přisuzovat jim patřičný význam.

1.2.10 Registr rizik

Výsledek analýzy rizik je zaznamenám prostřednictvím databáze rizik a dále pak registru rizik, který obsahuje seznam potenciálních rizik a údaje o nich:

- Skupina rizikových oblastí
- Riziková oblast
- Riziko
- Popis rizika
- Pravděpodobnost - P
- Dopad - D
- Míra rizika – V = D x P
- Stupeň významnosti – nízká/střední/vysoká

Databáze rizik a registr rizik jsou vedeny v elektronické formě. Každé riziko má uveden podrobnější popis a další atributy. V registru rizik jsou rizika standardně tříděna dle dalších hledisek do vhodných kategorií a skupin. Databáze rizik a registr rizik se jsou základní nástroje pro evidenci rizik a pro jejich další řízení.

1.2.11 Popis metodiky hodnocení vyzrálosti ISMS

Model procesní vyspělosti (CMM - Capability Maturity Model neboli model vyspělosti řízení procesů, jenž je přímým předchůdcem modelu CMMI)) vyjadřuje stav, ve kterém se organizace (informační systém) nachází, číslem od 0 do 5. Model vyspělosti způsobilosti dovoluje relativně jednoduše definovat cíle pro řízení bezpečnosti informací s možností stanovit měřitelné a vyhodnotitelné úkoly pro příslušné vedoucí pracovníky.

U každé hodnocené oblasti jsou posuzovány následující čtyři aspekty:

pochopení a komunikace problematiky;

definice pravidel;

související procesy a příprava na implementaci pravidel;

sledování účinnosti zásad a souvisejících procesů a postupy pro zlepšování.

Hodnotící stupně jsou následující:

0	**Neexistence**	Organizace si neuvědomuje potřebu bezpečnosti IT. Zodpovědnost a jednotlivé úlohy pro zajištění bezpečnosti nejsou nikomu přiděleny. Nejsou opatření podporující management bezpečnosti IT. Neexistuje žádný způsob informování o bezpečnosti IT, ani žádný proces reagující na porušení bezpečnosti IT. Zcela chybí jakýkoli rozpoznatelný systém administrace bezpečnostního procesu.
1	**Náhodně (výchozí/ad hoc)**	Organizace si uvědomuje potřebu bezpečnosti IT. Povědomí o potřebě bezpečnosti vychází výhradně z individuální iniciativy. Bezpečnosti IT se řeší nárazově a není nijak měřena. Pokud dojde k porušení bezpečnosti IT, reakce jsou nekonkrétní, protože není jasné, kdo je za co zodpovědný. Reakce na porušení bezpečnosti jsou nepředvídatelné.
2	**Opakovaně (ale intuitivně)**	Zodpovědnost za bezpečnost IT spočívá na koordinátorovi bezpečnosti IT, ačkoli jeho pravomoci jsou omezeny. Povědomí o potřebě bezpečnosti je neurčité a omezené. Přestože ze systému přicházejí informace týkající se bezpečnosti, neanalyzují se. Služby třetích stran nemusí vyhovovat potřebám bezpečnosti,

		specifickým pro organizaci. Bezpečnostní postupy se vytvářejí, ale odborné schopnosti a nástroje nejsou adekvátní. Způsob informování o bezpečnosti IT je nekompletní, zavádějící anebo irelevantní. Školení o bezpečnosti se provádí výhradně na základě iniciativy jedince. Bezpečnost IT se chápe výhradně jako doména a zodpovědnost IT a organizace si neuvědomuje, že bezpečnost IT je její součástí.
3	**Definovaně (definovaný proces managementu)**	Existuje povědomí o bezpečnosti a je podporováno ze strany vedení společnosti. Jsou definovány bezpečnostní procedury IT a dodržují se. Jsou určeny osoby zodpovědné za bezpečnost IT, ale neděje se tak permanentně. Bezpečnostní plán IT a bezpečnostní řešení jsou tvořeny na základě současné analýzy rizik. Podávání zpráv o bezpečnosti nezahrnuje jasně stanovené obchodní cíle. Testování se provádí náhodně, např. intrusivní testování. Pro potřeby organizace a IT se provádí bezpečnostní školení, které ale není pravidelné a jeho organizace zůstává neformální.
4	**Měřitelně (řízená a měřitelná)**	Zodpovědnost a úkoly spojené s bezpečností IT jsou jasně stanoveny, řízeny a uplatňovány. Jsou prováděny důsledné analýzy bezpečnostních rizik IT a analýzy dopadu na bezpečnost IT. Jsou kompletně zpracovány bezpečnostní postupy, včetně bližších specifik spojených s bezpečností. Aktivity spojené s udržením povědomí o bezpečnosti jsou vedeny závaznou formou. Identifikace, autentizace a autorizace uživatelů podléhají standardizaci. Pro personál zodpovídající za audit a řízení bezpečnosti je vyžadována bezpečnostní certifikace. Bezpečnostní testování probíhá s využitím standardních a formalizovaných procesů, které vedou ke zlepšení úrovně bezpečnosti. Bezpečnostní procesy IT jsou koordinovány s bezpečnostními funkcemi organizace. Způsob informování o bezpečnosti IT je propojen s obchodními záměry organizace. Školení o bezpečnosti IT se týká jak IT, tak i obchodní části organizace. Školení o bezpečnosti IT je plánováno a řízeno způsobem, který odpovídá potřebám organizace a definovaným profilům

		bezpečnostních rizik. KGI a KPI pro bezpečnostní management jsou již definována, ale nejsou ještě měřena.
5	**Optimalizovaně**	Bezpečnost IT je předmětem společné zodpovědnosti IT a obchodního managementu a je zařazena v cílech bezpečnosti organizace. Bezpečnostní požadavky IT jsou jasně definovány, optimalizovány a jsou součástí schváleného bezpečnostního plánu. Uživatelé a zákazníci se mohou lépe podílet na definování bezpečnostních požadavků a bezpečnostní funkce jsou začleněny do aplikací již během jejich vývoje. Bezpečnostní incidenty jsou bez prodlení řešeny prostřednictvím oficiálních procedur reagujících na incidenty, které jsou podporovány automatickými nástroji. Bezpečnost podléhá pravidelnému posuzování, čímž dochází k vyhodnocování efektivnosti implementace bezpečnostního plánu. Informace o hrozbách a slabinách jsou systematicky shromažďovány a analyzovány. Pro potřeby neustálého zdokonalování procesu je využíváno bezpečnostního testování, analýzy pravé příčiny chyb a proaktivní identifikaci rizik. Bezpečnostní procesy a technologie jsou integrovány v rámci celé organizace. Klíčové indikátory výkonu a cílů pro bezpečnostní management jsou zkompletovány a komunikovány. Management využívá Klíčové indikátory výkonu a cílů k neustálému zdokonalování bezpečnostního plánu.

Tabulka č. 9 - Hodnotící stupně

1.2.12 Míra prosazení daného stupně

Pro přesnější rozlišení míry prosazení procesů podle jednotlivých stupňů jsou definovány následující možné tři úrovně shody, které jsou určeny pro všech pět stupňů podle výše definovaných pravidel:

Plně zavedeno (P) – toto hodnocení je možné aplikovat v případě, kdy je převážná většina požadovaných parametrů definovaných pro jednotlivé sledované oblasti naplněna. Případné odchylky se mohou objevit pouze v omezeném rozsahu u nevýznamných parametrů.

Částečně zavedeno (C) – toto hodnocení je aplikováno v případech, kdy je možné vysledovat částečné naplnění uvedených parametrů alespoň u některé ze sledovaných oblastí.

Není zavedeno – toto hodnocení je aplikováno v případech, kdy nelze u žádného ze čtyř sledovaných oblastí identifikovat stav, který by vypovídal o naplnění některého z uvedených parametrů.

Jednotlivé stupně hodnocení jsou konstruovány tak, že vyšší stupeň v sobě zahrnuje vždy prosazení nižších stupňů minimálně na úrovni, na jaké je prosazen pro daný proces sám. Obecně tedy pro korektní hodnocení musí být vždy nižší stupeň prosazen stejně nebo více než stupeň vyšší. Tedy například:

Příklady hodnocení	**Stupeň**				
	1	**2**	**3**	**4**	**5**
Korektní hodnocení	C	C			
Korektní hodnocení	P	P	C	C	
Nekorektní hodnocení (stupeň 1 musí být prosazen minimálně na úrovni C)		C	C		
Nekorektní hodnocení (stupně 1 a 2 musí být prosazeny na úrovni P)	C	C	P	C	
Nekorektní hodnocení (stupeň 1 musí být prosazen na úrovni P)		P	P	C	

Tabulka č. 10 - Příklady hodnocení

Hodnocení každé činnosti nebo opatření může být (a v případě, že není zcela naplněn každý stupeň 1 až 5, musí být) doplněno komentářem.

1.2.13 Budoucí požadavky NIS2

NIS2[1] je nově připravovaná evropská regulace, je pokračování evropské směrnice NIS[2], která byla přijata v roce v roce 2016. Její přijetí si vyžádalo doposud největší a nejvíce rozsáhlou změnu zákona o kybernetické bezpečnosti. V tento moment je připravována revize nařízení a očekává se další rozsáhlá změna Zákona o kybernetické bezpečnosti. Důležité je podotknout, že zatím není schválené finální znění. Z pohledu právního, bude po jejím přijetí následovat

[1] V případě Evropského parlamentu - https://www.europarl.europa.eu/meet-docs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2021/10-28/NIS2_COMPROMISE_amendment_EN.pdf ,v případě Evropské rady https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/en/pdf

[2] https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52020PC0823

dvouleté období pro transpozici do českého práva. Jako podstatnou část lze očekávat rozšíření seznamu povinných osob dle velikosti organizace.

2 IDENTIFIKACE POŽADAVKŮ NA ŘEŠENÍ

2.1 Formální požadavky

Dle vyhlášky č. 317/2014 Sb. o významných informačních systémech § 3 není možné vyloučit, že identifikované systémy budou identifikovány jako významné systémy dle výše uvedené vyhlášky. Na danou organizaci se tedy budou vztahovat požadavky kybernetického zákona č. 181/2014 Sb. v platném znění. S tím jsou spojeny legislativní povinnosti, jako například hlášení bezpečnostních incidentů, řízení rizik, opatření v oblasti prevence a také detekce kybernetických událostí.

Pro vyhodnocení srovnání požadavků zákona je dále v následující kapitola zpracována srovnávací analýza.

2.2 Srovnání nastavených postupů a identifikace potenciálních slabých míst

Samotné provedení zavedení legislativních požadavků je nezbytné provést v několika etapách, kde první části je vyhodnocení stavu již zavedených opatření. Tato oblast se nejlépe realizuje přes srovnávací analýzu a s tím spojené vyhodnocení již existujících procesních opatření. V další kapitole je provedena komplexní analýza prostředí a vzhledem k tomu, že Zákon o kybernetické bezpečnosti je založen mj. na normě ISO 27001 a s tím spojenými opatřeními.

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
ČSN ISO/IEC 27001 kapitola 4					
4. Kontext organizace	**C**				
4.1 Porozumění organizaci a jejímu kontextu	C				
4.2 Porozumění potřebám a očekáváním zainteresovaných stran	C				
4.3 Stanovení rozsahu systému řízení bezpečnosti informací	C				
4.4 Systém řízení bezpečnosti informací	C				
4.1 Porozumění organizaci a jejímu kontextu					
Organizace musí určit vnější a vnitřní oblasti, které jsou relevantní pro její činnost a mají vliv na schopnost dosahovat zamýšlených cílů systému řízení bezpečnosti informací.					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast kontextu organizace není zavedena. Doporučení: Zavést 4.1 porozumění organizace a jejímu kontextu. Tato část by měla zahrnovat analýzu vnější a vnitřní oblasti podniku (např. SWOT, PESTEL).					
4.2 Porozumění potřebám a očekáváním zainteresovaných stran	***C***				
Organizace musí určit: *a) Zainteresované strany, které mají vztah k systému řízení bezpečnosti informací* *b) požadavky těchto zainteresovaných stran, které jsou relevantní k bezpečnosti Informací.*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda:					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Oblast „Porozumění potřebám a očekáváním zainteresovaných stran“ není zavedena. Doporučení: Definovat zájmové skupiny podstatné pro ISMS a jejich požadavky na ISMS (zákazník, dodavatel, vlastník, regulátor (stát)).					
4.3 Stanovení rozsahu systému řízení bezpečnosti informací	***C***				
Organizace musí při stanovení rozsahu vzít v potaz: *a) externí a interní aspekt uvedený v 4.1* *b) Požadavky uvedené v bodě 4.2* *c) Propojení a závislosti mezi činnostmi prováděnými organizací a těmi činnostmi, které jsou prováděné jinými organizacemi.* *Rozsah musí být písemně zdokumentován*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast „Stanovení rozsahu systému řízení bezpečnosti informací“ není zavedena. Doporučení: Zohlednit závislosti mezi 4.1 a 4.2 a činnostmi prováděné organizací a činnostmi prováděné jinými organizacemi.					
4.4 Systém řízení bezpečnosti informací	***C***				
Organizace musí ustavit, implementovat, udržovat a neustále zlepšovat systém řízení bezpečnosti informací v souladu s požadavky této mezinárodní normy.					
Zjištěný stav: Oblast není zavedena. Systémová neshoda:					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Oblast „Systém řízení bezpečnosti informací“ není zavedena. Doporučení: Implementovat cyklus neustálého zlepšování (Demingův cyklus) do systému řízení bezpečnosti informací.					
ČSN ISO/IEC 27001 kapitola 5					
5. Vůdčí role	**C**				
5.1 Vůdčí role a závazek	C				
5.2 Politika	C				
5.3 Role, odpovědnosti a pravomoci organizace	C				
5.1 Vůdčí role a závazek					
Vrcholové vedení organizace musí s ohledem na systém řízení bezpečnosti informací demonstrovat vůdčí roli a závazek tím, že: *a) zajistí stanovení politiky bezpečnosti informací a cílů bezpečnosti informací slučitelných se strategickým směřováním organizace;* *b) zajistí integraci požadavků systému řízení bezpečnosti informací do procesů organizace;* *c) zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací;* *d) komunikuje význam efektivního řízení bezpečnosti informací a význam dosažení shody s požadavky systému řízení bezpečnosti informací;* *e) zajistí dosažení zamýšleného výstupu (výstupů) systému řízení bezpečnosti Informací organizace;* *f) směřuje a podporuje osoby k přispívání efektivnosti systému řízení bezpečnosti informací;*					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
g) prosazuje neustále zlepšování; *h) podporuje ostatní relevantní řídicí role k prokázání jejich vůdčí role v oblastech jejich odpovědnosti.*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Nejsou definovány cíle pro bezpečnosti informací. Nejsou popsány procesy ve společnosti; alokování zdrojů potřebných pro ISMS. Doporučení: Definovat cíle bezpečnosti informací; integrovat požadavky ISMS do procesů organizace; zajistit potřebné zdroje potřebné pro ISMS; komunikovat význam efektivního řízení bezpečnosti informací napříč organizací; zajistit dosažení zamýšleného výstupu ISMS; zavést proces neustálého zlepšování ISMS					
5.2 Politika	***C***				
Vrcholové vedení organizace musí stanovit politiku bezpečnosti informací, která: *a) je přiměřená záměrům organizace;* *b) zahrnuje cíle bezpečnosti informaci (viz 6.2) nebo poskytuje rámec pro nastavení cílů bezpečnosti informací;* *c) zahrnuje závazek ke splnění aplikovatelných požadavků týkajících se bezpečnosti* *d) zahrnuje závazek k neustálému zlepšování systému řízení bezpečnosti informací;* *Politika bezpečnosti informací musí:* *e) být dostupná v písemné podobě*					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
f) být komunikována v rámci organizace; *g) být přiměřeně dostupná zainteresovaným stranám.*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast není zavedena. Doporučení: Zavést politiku bezpečnosti informací, která bude přiměřená záměrům organizace, zahrnout cíle z bezpečnosti informací z části 6.2; zpřístupnit politiku v písemné podobě; komunikovat politiku v rámci organizace; zajisti jejich přiměřenou dostupnost relevantním stranám.					
5.3 Role, odpovědnosti a pravomoci organizace	***P***	***C***			
Vrcholové vedení organizace musí zajistit, že odpovědnosti a pravomoci pro role relevantní bezpečnosti informací jsou přiřazeny a komunikovány. *Vrcholové vedení organizace musí přiřadit odpovědnosti a pravomoci pro:* *a) zajištění, že systém řízení bezpečnosti informací je ve shodě s požadavky této mezinárodni normy;* *b) podávání zpráv o výkonnosti systému řízení bezpečnosti informací vrcholovému vedení organizace.*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast „Role, odpovědnosti a pravomoci organizace„ není zavedena. Doporučení:					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Zajistit odpovědnosti a pravomoci pro zajištění, že ISMS je ve shodě s požadavky normy; podávat zprávy o výkonnosti ISMS vrcholovému vedení organizace.					
ČSN ISO/IEC 27001 kapitola 6					
6. Plánování	**C**				
6.1 Opatření zaměřená na rizika a příležitosti	C				
6.1.1 Obecně	C				
6.1.2 Posuzování rizik bezpečnosti informací	C				
6.1.3 Ošetření rizik bezpečnosti informací	C				
6.2 Cíle bezpečnosti informací a plánování jejich dosažení	C				
6.1.1 Obecně					
Při plánování systému řízení bezpečnosti informací musí organizace zvážit aspekt uvedený v 4.1 a požadavky uvedené v 4.2 a určit rizika a příležitosti, na které se potřebuje zaměřit pro: *a) zajištění, že systém řízení bezpečnosti informací organizace může dosáhnout zamýšleného výstupu (výstupů);* *b) předcházení nebo snížení nežádoucích následků;* *c) dosažení neustálého zlepšování.* *Organizace musí plánovat:* *d) opatření zaměřená na tato rizika a příležitosti;* *e) jak:* *1) integrovat a implementovat tato opatření do procesů systému řízení bezpečnosti informací;* *2) vyhodnocovat efektivnost těchto opatření.*					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Nejsou zavedeny cíle bezpečnosti informací; nelze zajistit bod a) Snížení nežádoucích následků je zavedeno, ale ne pro celý katalog rizik (katalog rizik rozpracovat). Není zaveden proces neustálého zlepšování Chybí vyhodnocení efektivnosti opatření. Doporučení: Identifikovat cíle bezpečnosti informací a zajistit, že ISMS lze dosáhnout zamýšleného cíle Rozpracovat katalog rizik pro celou společnost a zahrnout vlastníka rizika, zavést proces pro neustálé zlepšování, hodnocení efektivnosti opatření.					
6.1.2 Posuzování rizik bezpečnosti informací	***C***				
Organizace musí definovat a aplikovat proces posuzování rizik bezpečnosti informací, který: *a) stanoví a udržuje kritéria rizik bezpečnosti informací, která zahrnují:* *1) kritéria akceptace rizik* *2) kritéria pro provádění posouzení rizik bezpečnosti informací* *b) zajistí, že opakovaná posouzení rizik bezpečnosti informací produkují konzistentní, opodstatněné a porovnatelné výsledky;* *c) identifikuje rizika bezpečnosti informací:* *1) používá proces posuzování rizik bezpečnosti informací k identifikaci rizik spojených se ztrátou důvěrnosti, integrity a dostupnosti informací v rozsahu systému řízení bezpečnosti informací;*					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
2) identifikuje vlastníky rizik *d) analyzuje rizika bezpečnosti informací* *1) posuzuje potenciální následky, které by nastaly, pokud by se realizovala rizika identifikovaná v 6.1.2 c) 1)* *2) posuzuje reálnou pravděpodobnost výskytu rizik identifikovaných v 6.1.2 c) 1)* *3) určuje úroveň rizik.* *e) hodnotí rizika bezpečnosti informací* *1) porovnává výsledky analýzy rizik s kritérii hodnocení rizik v 6.1.2 a)* *2) stanovuje priority analyzovaných rizik pro ošetření rizika.* *Organizace musí uchovávat dokumentované informace o procesu posuzování rizik bezpečnosti informací.*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Nejsou stanoveny kritéria pro vyhodnocení rizika. Nejsou zavedena kritéria pro provádění posouzení rizik bezpečnosti informací. Doporučení: Stanovit metodiku řízení rizik bezpečnosti informací, které budou zahrnovat kritéria akceptace rizik; kritéria pro provádění posouzení rizik bezpečnosti informací. Zajistit, že opakovaná posouzení rizik bezpečnosti informací produkují konzistentní, opodstatněné a porovnatelné výsledky. Identifikovat rizika bezpečnosti informací (proces posouzení rizik bezpečnosti informací je spojený se ztrátou důvěrnosti, integrity a dostupnosti informací); Identifikovat vlastníka rizik.					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Posoudit potenciální následky, které by nastaly, pokud by se realizovala identifikovaná rizika; Posoudit reálnou pravděpodobnost výskytu identifikovaných rizik; určit úroveň rizik. Porovnávat výsledky analýzy rizik s kritérii hodnocení rizik; stanovit priority analyzovaných rizik pro ošetření rizik; dokumentovat.					
6.1.3 Ošetření rizik bezpečnosti informací	***C***				
Organizace musí definovat a používat proces ošetření rizik bezpečnosti informací pro: *a) výběr vhodných variant pro ošetření rizika bezpečnosti informací s ohledem na výsledky posuzování rizik;* *b) určení všech opatření nezbytných k implementaci vybrané varianty (variant) pro ošetření rizika bezpečnosti informací;* *c) porovnání opatření určených výše v 6.1.3 b) s opatřeními v příloze A a pro verifikaci, že žádné nezbytné opatření nabylo vynecháno;* *d) vytvoření Prohlášení o aplikovatelnosti, které obsahuje nezbytná opatření (viz 6.1.3 b) a c)) a zdůvodnění pro jejich zahrnutí, ať už jsou nebo nejsou implementována, a zdůvodnění pro vyloučení opatření z přílohy A;* *e) formulaci plánu ošetření rizik bezpečnosti informací;* *f) získání souhlasu vlastníků rizik ohledně plánu ošetření rizik bezpečnosti informací a přijetí zbytkových rizik bezpečnosti informací.* *Organizace musí uchovávat dokumentované informace o procesu ošetření rizik bezpečnosti informací.*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast „Ošetření rizik bezpečnosti informací“ není zavedena.					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Doporučení: Zavést proces pro zvládání rizik. Určit všechna opatření pro zvládání rizik. Formulovat plán ošetření rizik bezpečnosti informací. Získat souhlas vlastníka rizik se zvládáním rizik a přijetím zbytkových rizik. Dokumentovat informace o procesu zvládání rizik.					
6.2 Cíle bezpečnosti informací a plánování jejich dosažení	***C***				
Organizace musí stanovit cíle bezpečnosti informací relevantní jednotlivým funkcím a úrovním řízení. Cíle bezpečnosti informací musí: *a) být konzistentní s politikou bezpečnosti informací* *b) být měřitelné (pokud je to proveditelné)* *c) vzít v úvahu aplikovatelné požadavky bezpečnosti informací a výsledky z posuzování rizik a ošetření rizik;* *d) být komunikovány* *e) být dle potřeby aktualizovány.* *Při plánování, jak dosáhnout cílů bezpečnosti informací musí organizace určit:* *f) co bude vykonáno;* *g) jaké zdroje budou vyžadovány;* *h) kdo bude odpovědný;* *i) kdy to bude dokončeno;* *j) jak budou výsledky vyhodnoceny.*					
Zjištěný stav: Oblast není zavedena.					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Systémová neshoda: Oblast „Cíle bezpečnosti informací a plánování jejich dosažení“ není zavedena. Doporučení: Stanovit cíle bezpečnosti informací relevantní jednotlivým funkcím a úrovním řízení.					
ČSN ISO/IEC 27001 kapitola 7					
7. Podpora	**C**				
7.1 Zdroje	C				
7.2 Kompetence	C				
7.3 Povědomí	C				
7.4 Komunikace	C				
7.5 Dokumentované informace	C				
7.1 Zdroje					
Organizace musí určit a zajistit zdroje potřebné pro ustavení, implementování, udržování a neustále zlepšování systému řízení bezpečnosti informací.					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast „Zdroje“ není zavedena. Doporučení: Zavést zdroje pro ustanovení, implementování, udržování a neustálé zlepšování ISMS.					
7.2 Kompetence	***C***				
Organizace musí: *a) určit nezbytné kompetence osoby (osob) vykonávajících pro organizaci práci, která má vliv na výkonnost bezpečnosti informací;*					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
b) zajistit, že tyto osoby jsou kompetentní na základě odpovídajícího vzdělání, školení nebo zkušeností; *c) tam, kde je to aplikovatelné, přijmout opatření k získání nezbytné kompetence a vyhodnocovat efektivnost těchto přijatých opatření;* *d) uchovávat odpovídající dokumentované informace jako důkazy o kompetenci.*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast „Kompetence“ není zavedena. Doporučení: Určit potřebnou kompetenci osob, které vykonávají práci, která má vliv na výkonnost bezpečnosti informací; Zajistit, že mají odpovídající vzdělání a průběžná školení; Hodnotit efektivitu činností; dokumentovat.					
7.3 Povědomí	***P***	***C***			
Osoby pracující pro organizaci si musí být vědomé: *a) politiky bezpečnosti informací* *b) svého přínosu k efektivnosti systému řízení bezpečnosti informací, včetně výhod zlepšené výkonnosti bezpečností informací;* *c) důsledků nepřizpůsobení se požadavkům systému řízení bezpečnosti informací.*					
Zjištěný stav: Oblast není zavedena ve formální rovině, samotné povědomí je ale z povahy činnosti univerzity již zavedeno. Systémová neshoda: Oblast „Povědomí“ není zavedena. Doporučení: Zajistit, aby pracovníci měli povědomí o politikách bezpečnosti informací; byli si vědomí svého přínosu k efektivnosti ISMS; dopadů nesouladu s požadavky ISMS.					
7.4 Komunikace	***C***				

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Organizace musí ve vztahu k systému řízení bezpečnosti informací určit potřebu pro interní a externí komunikaci, která zahrnuje: *a) o čem komunikovat;* *b) kdy komunikovat;* *c) s kým komunikovat;* *d) kdo musí komunikovat;* *e) procesy, kterými musí být komunikace realizována.*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast „Komunikace“ není zavedena. Doporučení: určit, potřebu pro interní a externí komunikaci ve vztahu k systému řízení bezpečnosti informací, která musí zahrnout, o čem, kdy, s kým a kdo musí komunikovat, procesy, kterými musí být komunikace realizována.					
7.5 Dokumentované informace	***C***				
Systém řízení bezpečnosti informací musí zahrnovat: *a) dokumentované informace požadované touto mezinárodní normou;* *b) dokumentované informace určené organizací za nezbytné pro efektivnost systému řízení bezpečnosti informací.* *Při vytváření a aktualizaci dokumentovaných informací musí organizace zajistit odpovídající:* *a) identifikaci a popis (např. název, datum, autor, číslo jednací)* *b) formát (např. jazyk, verze softwaru, grafika) a médium (např. papír, elektronická média)* *c) přezkoumání a schvalování vhodnosti a přiměřenosti.*					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Dokumentované informace vyžadované systémem řízení bezpečnosti informací a touto mezinárodní normou musí být řízeny, aby bylo zajištěno následující: *a) dokumentované informace jsou dostupné a vhodné pro použití, a to kdekoli a kdykoli je to potřebné;* *b) dokumentované informace jsou odpovídajícím způsobem chráněny (například před prozrazením, nevhodným použitím nebo ztrátou integrity).* *Pro řízení dokumentovaných informací musí organizace věnovat pozornost následujícím činnostem, pokud jsou aplikovatelné:* *c) distribuci, přístupu, vyhledání a použití;* *d) ukládání a zachování, včetně zachování čitelnosti;* *e) řízení změn (například řízení verzí);* *f) uchovávání a likvidace.* *Dokumentované informace externího původu, které organizace určí jako nezbytné pro plánování a provozování systému řízení bezpečnosti informací, musí být dle potřeby identifikovány a řízeny.*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast „Dokumentované informace“ není zavedena. Doporučení: Dokumentovat informace řízené normou ISO 27001. Dokumentovat informace identifikované jako nezbytné pro efektivnost ISMS. Zajistit pravidelné aktualizování dokumentovaných informací zahrnující? Identifikaci a popis, formát + přezkoumání vhodnosti a dostatečnosti. Zajistit dostupnost dokumentovaných informací a vhodnost pro použití, kde je potřeba.					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Další činnosti, kterým je nutno se věnovat jsou: a) distribuce, přístup, vyhledání a použití; b) ukládání a zachování, včetně zachování čitelnosti; c) řízení změn (například řízení verzí); d) uchovávání a likvidace. Doporučený seznam dokumentace je následující: Politika bezpečnosti informací Analýza rizik Prohlášení o aplikovatelnosti Plán zvládání rizik Cíle ISMS Kompetence, výcvik Program interního auditu a výsledek hodnocení interního auditu Řízení neshod Nápravná opatření					
ČSN ISO/IEC 27001 kapitola 8					
8. Provoz	**C**				
8.1 Plánování a řízení provozu	C				
8.2 Posuzování rizik bezpečnosti informací	C				
8.3 Ošetření rizik bezpečnosti informací	C				
8.1 Plánování a řízení provozu					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Organizace musí plánovat, implementovat a řídit procesy potřebné ke splnění požadavků bezpečnosti informací a implementovat opatření určená v 6.1. Organizace musí také implementovat plány k dosažení cílů bezpečnosti informací určených v 6.2.					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast „Plánování a řízení provozu“ není zavedena. Doporučení: Zavést řízení změn a přezkoumat dopady nechtěných změn.					
8.2 Posuzování rizik bezpečnosti informací	***C***				
Organizace musí posuzovat rizika bezpečnosti informací v pravidelných intervalech, nebo pokud jsou plánovány nebo nastanou významné změny, a to s ohledem na kritéria stanovená v 6.1.2 a). *Organizace musí uchovávat dokumentované informace o výsledcích posuzování rizik bezpečnosti informací.*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast „Posuzování rizik bezpečnosti informací“ není zavedena. Doporučení: Zavést hodnocení rizik a dokumentovat informace o výsledcích hodnocení rizik.					
8.3 Zvládání rizik bezpečnosti informací	***C***	***C***			
Organizace musí implementovat plán ošetření rizik bezpečnosti informací. *Organizace musí uchovávat dokumentované informace o výsledcích ošetření rizik bezpečnosti informací.*					
Zjištěný stav: Oblast není zavedena. Systémová neshoda: Oblast „zvládání rizik bezpečnosti informací“ není zavedena. Doporučení: Zavést plán zvládání rizik a dokumentovat výsledky o zvládání rizik.					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
ČSN ISO/IEC 27001 kapitola 9					
9. Hodnocení výkonnosti	**C**				
9.1 Monitorování, měření, analýza a hodnocení	C				
9.2 Interní audit	C				
9.3 Přezkoumání vedením organizace	C				
9.1 Monitorování, měření, analýza a hodnocení					
Organizace musí vyhodnocovat výkonnost bezpečnosti informací a efektivnost systému řízení bezpečnosti informací. Organizace musí určit: *a) co je třeba monitorovat a měřit, včetně procesů a opatření bezpečnosti informací;* *b) použitelné metody monitorování, měření, analýzy a hodnocení k zajištění platných výsledků;* *c) kdy musí monitorování a měření prováděno;* *d) kdo monitorovat a měřit;* *e) kdy budou výsledky z monitorování a měření analyzovány a vyhodnoceny;* *f) kdo bude analyzovat a vyhodnocovat tyto výsledky.*					
Zjištěný stav: Oblast není zavedena. Dílčí neshoda: Oblast „Monitorování, měření, analýza a hodnocení“ není zavedena. Doporučení: Zavést hodnocení výkonnosti bezpečnosti informací a účinnost ISMS; stanovit KPI, metodiku, odpovědnosti za měření, vyhodnocení, dokumentování.					
9.2 Interní audit	***C***				
Organizace musí v plánovaných intervalech provádět interní audity k získání informací o tom, zda systém řízení bezpečnosti informací:					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
a) vyhovuje: *1. vlastním požadavkům organizace na systém řízení bezpečnosti informací* *2. požadavkům normy ISO/IEC 27001* *b) je efektivně implementován a udržován.* *Organizace musí:* *a) plánovat, ustavit, implementovat a udržovat auditní program (programy), včetně četnosti, metod, odpovědností, plánování požadavků a podávání zpráv. Auditní program (programy) musí vzít v úvahu význam příslušných procesů a výsledky předchozích auditů;* *b) definovat kritéria auditu a rozsah každého auditu;* *c) vybrat auditory a provádět audity při zajištění objektivity a nestrannosti procesu auditu;* *d) zajistit, aby byly výsledky auditů předkládány relevantním vedoucím pracovníkům;* *e) uchovávat dokumentované informace jako důkazy o programu (programech) a výsledcích auditů;* *f) zajistit, aby byly výsledky auditů předkládány relevantním vedoucím pracovníkům;* *g) uchovávat dokumentované informace jako důkazy o programu (programech) a výsledcích auditů.*					
Zjištěný stav: Oblast není zavedena. Dílčí neshoda: Oblast „Interní audit“ není zavedena. Doporučení: Zavést interní audit.					
9.3 Přezkoumání vedením organizace	***C***				

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Vrcholové vedení organizace musí v plánovaných intervalech přezkoumávat systém řízení bezpečnosti informací organizace pro zajištění jeho neustálé vhodnosti, přiměřenosti a efektivnosti. *Přezkoumání vedením organizace musí zvážit:* *a) stav opatření z předešlých přezkoumání vedením organizace;* *b) změny v externím a interním aspektu, které jsou relevantní pro systém řízení bezpečnosti informací;* *c) zpětnou vazbu na výkonnost bezpečnosti informací, včetně trendů ohledně:* *1) neshod a nápravných opatření;* *2) výsledků monitorování a měření;* *3) výsledků auditů;* *4) plnění cílů bezpečnosti informací* *d) zpětnou vazbu od zainteresovaných stran;* *e) výsledky posuzování rizik a stav plánu ošetření rizika;* *f) příležitosti pro neustálé zlepšování.* *Výstupy z přezkoumání vedením organizace musí zahrnovat rozhodnutí vztahující se k příležitostem neustálého zlepšování a k jakýmkoliv potřebám pro změny v systému řízení bezpečností informací.* *Organizace musí uchovávat dokumentované informace jako důkazy o výsledcích přezkoumání vedením organizace.*					
Zjištěný stav: Oblast není zavedena. Dílčí neshoda: Oblast „Přezkoumání vedením organizace“ není zavedena. Doporučení: Zavést přezkoumání ISMS (po zavedení).					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
ČSN ISO/IEC 27001 kapitola 10					
10. Zlepšování	**C**				
10.1 Neshody a nápravná opatření	C				
10.2 Neustálé zlepšování	C				
10.1 Neshody a nápravná opatření					
V případě výskytu neshody, musí organizace: *a) reagovat na neshodu, a pokud je to aplikovatelné:* *1) přijmout opaření k řízení a nápravě neshody;* *2) zabývat se následky;* *b) vyhodnotit potřebu pro opatření k odstranění příčin neshody, aby se neshoda znovu nevyskytla, prostřednictvím:* *1) přezkoumání neshody;* *2) určení příčin neshody;* *3) určení, zda existují podobné neshody nebo by se mohly potenciálně vyskytnout;* *c) implementovat jakákoliv potřebná opatření;* *d) přezkoumat efektivnost každého přijatého nápravného opatření;* *e) provést změny v systému řízení bezpečnosti informací, pokud je to nezbytné.* *Nápravná opatření musí být přiměřená dopadům neshod, kterým čelí.* *Organizace musí uchovávat dokumentované informace jako důkazy o:* *f) podstatě neshod a každého následného přijatého opatření;* *g) výsledcích každého nápravného opatření.*					

	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Zjištěný stav: Oblast není zavedena. Dílčí neshoda: Oblast „Neshody a nápravná opatření“ není zavedena. Doporučení: Zavést proces reakce na neshodu; přijmout opatření k řízení a nápravě neshody; zabývat se následky. Zavést potřebná opatření. Přezkoumat účinnost nápravných opatření. Provést změny ISMS, když je potřeba. Dokumentovat informace o příčinách neshod a výsledcích nápravných opatření.					
10.2 Neustálé zlepšování	***C***				
Organizace musí neustále zlepšovat vhodnost, přiměřenost a efektivnost systému řízení bezpečnosti informaci.					
Zjištěný stav: Oblast není zavedena. Dílčí neshoda: Proces „Neustálé zlepšování“ není zaveden. Doporučení: Zavést proces neustálého zlepšování ISMS.					

Tabulka č. 11 - Srovnávací analýza [9]

2.2.1 Bezpečnostní cíle informační bezpečnosti

Bezpečnostní politika představuje základní politiku organizace. Hlavní cílem bezpečnostní politiky je:

- Definovat hlavní cíle při ochraně informací.
- Stanovit způsob jak bezpečnost řešit.
- Určit pravomoci a zoodpovědnosti. [6]

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
ČSN ISO/IEC 27001 příloha A, kapitola 5					
A.5 Politiky bezpečnosti informací	**C**				
A.5.1 Směřování bezpečnosti informací vedením organizace	C				
A.5.1 Směřování bezpečnosti informací vedením organizace	***C***				
Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkající se činnosti organizace, příslušnými zákony a směrnicemi.					
Zjištěný stav: Oblast není zavedena. Dílčí neshoda: není zavedena politika bezpečnosti informací. Doporučení: V rámci implementace systému bezpečnosti informací zavést politiku pro řízení bezpečnosti informací; schválení vedením, dát na vědomí zaměstnancům, relevantním stranám a pravidelně aktualizovat.					
ČSN ISO/IEC 27001 příloha A, kapitola 6					
A.6 Organizace bezpečnosti informací	**C**				
A.6.1 Interní organizace	C				
A.6.2 Mobilní zařízení a práce na dálku	C				
A.6.1 Interní organizace	***C***				
Cíl: Nastavit řídící rámec pro nastartování a kontrolu implementace a provozování informační bezpečnosti v organizaci.					
Zjištěný stav: Existuje Org. Chart. Kontakt s příslušnými autoritami (zákon o KB se nevztahuje), Kontakt se zájmovými skupinami – ne Dílčí neshoda: nejsou definovány a přiděleny odpovědnosti v oblasti bezpečnosti informací Kontakt se zájmovými skupinami neprobíhá.					

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
Doporučení: V rámci implementace systému bezpečnosti informací přidělit a definovat odpovědnosti v oblasti bezpečnosti informací.					
A.6.2 Mobilní zařízení a práce na dálku	***C***	***C***			
Cíl: Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku.					
Zjištěný stav: Práce na dálku je umožněna pouze přes vpn klienta. U mobilních zařízení je komunikace uživatelů využívající VPN připojení pro přístup do externích sítí směrována přes podnikový firewall. Dále je zajištěna ochrana proti škodlivým programům pomocí antivirového programu. V případě krádeže mobilního zařízení musí uživatel nahlásit tuto událost správci sytému.					
ČSN ISO/IEC 27001 příloha A, kapitola 7					
A.7 Bezpečnost lidských zdrojů					
A.7.1 Před uzavřením pracovního poměru	C	C	C		
A.7.2 Během pracovního vztahu	C	C	C		
A.7.3. Ukončení a změna pracovního poměru	C	C	C		
A.7.1 Před uzavřením pracovního poměru	***C***	***C***	***C***		
Cíl: Zajistit, aby zaměstnanci a smluvní strany byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybráni vhodní kandidáti.					
Zjištěný stav: Prověření informací poskytnutých uchazečem o zaměstnání v životopisu není prováděno. Zaměstnanci jsou seznámeni se svými povinnostmi při nástupu. Dílčí neshoda: Background check není prováděn. Doporučení: V rámci implementace systému bezpečnosti informací provádět pro klíčové pozice background check.					
A.7.2 Během pracovního vztahu	***C***	***C***			

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
Cíl: Zajistit, aby zaměstnanci a smluvní partneři si byli vědomi a naplňovali odpovědnosti za bezpečnost informací.					
Zjištěný stav: Při nastoupení nového zaměstnance je nový zaměstnanec proškolen o zásadách bezpečnosti informací, BOZP a následně je školen vedoucím pracovníkem jednotlivých oddělení (obchodní, technické, management). Proces disciplinárního řízení je zaveden. V případě porušení pracovní kázně je zaměstnanci poslán vytýkací dopis a následně je situace řešena operativně. Uchování informací je v souladu s GDPR. Ukončení – protokol o předání hmotných věcí, dohoda, v rámci GDPR					
A.7.3. Ukončení a změna pracovního poměru	***C***	***C***			
Cíl: Chránit zájmy organizace v rámci procesu změny nebo ukončení pracovního vztahu.					
Zjištěný stav: Ukončení, či změna pracovního poměru je prováděno ústní formou. V případě ukončení je vyplněn protokol o předání hmotných věcí a následně jsou ukončeny přístupy. Uchování informací je v souladu s GDPR. Dílčí neshoda: Postup není formálně popsán. Doporučení: V rámci implementace systému bezpečnosti informací formálně popsat postup pro ukončení, či změnu pracovního poměru.					
ČSN ISO/IEC 27001 příloha A, kapitola 8					
A.8 Řízení aktiv	**C**	**C**			
A.8.1 Odpovědnost za aktiva	C	C			
A.8.2 Klasifikace informací	C	C			
A.8.3 Manipulace s médii	C	C			
A.8.1 Odpovědnost za aktiva					

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
Cíl: Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně.					
Zjištěný stav V rámci řízení aktiv není popsán postup pro akceptaci rizika, kritičnost, vlastník rizika ani pravidla pro přípustné použití informací a aktiv souvisejících s informacemi a vybavením pro zpracování informací. Služební auto je používáno i k soukromým účelům. V případě vrácení je sepsán protokol o navrácení prostředků, který je evidován v rámci osobních karet. Dílčí zjištění: Není sepsán postup pro akceptaci rizika, kritičnost, vlastník rizika ani pravidla pro přípustné použití informací a aktiv souvisejících s informacemi a vybavením pro zpracování informací. Doporučení: V rámci implementace systému bezpečnosti informací definovat odpovědnosti za aktiva.					
A.8.2 Klasifikace informací	***X***				
Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci.					
Zjištěný stav: Oblast není zavedena. Dílčí neshoda: Není zavedena klasifikace informací. Doporučení: Zavést klasifikaci informací.					
A.8.3 Manipulace s médii	***C***	***C***			
Cíl: Předcházet neoprávněnému vyzrazení, modifikaci, odstranění nebo zničení informací uložených na médiích.					
Přenosná media ošetřena na úrovni neoprávněné manipulace dat Provozní řád – systém přístupu na úrovni klíčů – nikdo se nedostane k datovému poli- fyz. bezpečnost Dílčí neshoda: Nejsou definovány postupy pro nakládání s médii na základě jejich klasifikace.					

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
Doporučení: V rámci implementace systému bezpečnosti informací definovat postupy pro nakládání s vyměnitelnými médii.					
ČSN ISO/IEC 27001 příloha A, kapitola 9					
A.9 Řízení přístupu	**C**	**C**			
A.9.1 Požadavky organizace na řízení přístupu	C	C			
A.9.2 Řízení přístupu uživatelů	C	C			
A.9.3 Odpovědnost uživatelů	C	C			
A.9.4 Řízení přístupu k systémům a aplikacím	C	C			
A.9.1 Požadavky organizace na řízení přístupu					
Cíl: Omezit přístupu k informacím a vybavení pro zpracování informací					
Zjištěný stav: Oblast není zavedena. Dílčí neshoda: Není zavedena politika řízení přístupu. Doporučení: V rámci implementace systému bezpečnosti informací zavést politiku pro řízení přístupu.					
A.9.2 Řízení přístupu uživatelů	***C***	***C***			
Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k systémům a službám.					
Zjištěný stav: Využíváno Active Directory; definovány skupinové politiky dle pracovní pozice a povinností; AD DC zajišťuje autentizaci a autorizace uživatelů, počítačů a dalších služeb na základě předdefinovaných politik. Zavedena unikátní uživatelská jména a hesla s vynucenými požadavky na komplexitu. Registrace a management uživatelských účtů provádí technický ředitel. Dílčí neshoda: Proces zřízení uživatelského oprávnění a ukončení je veden neformálně.					

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
Doporučení: Zavést formální proces pro řízení přístupových oprávnění; zavést change management.					
A.9.3 Odpovědnost uživatelů	***C***	***C***			
Cíl: Učinit uživatele odpovědné za ochranu jejich autentizačních informací.					
Zjištěný stav: Uživatelé jsou v procesu přijímaní dle organizační směrnic proškoleni na ochranu přístupových hesel. Je tak zakázáno: -Sdělovat přístupové informace ke svému účtu dalším osobám. -Zaznamenávat heslo na papír nebo obdobnou podobu a nalepovat na zařízení či jiné viditelné místo. -Pracovat pod cizí identitou, používat prostředky k jejímu získání nebo zneužít v tomto pochybení či nedbalosti jiného uživatele. Uživatel je povinen udržovat své přístupové informace v tajnosti, aby nemohlo dojít k jejich zneužití.					
A.9.4 Řízení přístupu k systémům a aplikacím	***C***	***C***			
Cíl: Předcházet neautorizovanému přístupu k systémům a aplikacím.					
Zjištěný stav: Po ukončení práce musí uživatel zajistit pracovní stanici proti neoprávněnému přístupu vypnutím, odhlášením, nebo uzamknutím. Pokud zaměstnanec odchází od počítače pouze dočasně, je nutné se od svého uživatelského účtu buď odhlásit, nebo uzamknou relace.					
ČSN ISO/IEC 27001 příloha A, kapitola 10					
A.10 Kryptografie	**C**	**C**			
A.10.1 Kryptografická opatření	C	C			
A.10.1 Kryptografická opatření	***C***	***C***			

		Stupně hodnocení			
		1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
Cíl: Zajistit řádné a efektivní používání kryptografie k ochraně důvěrnosti, autentičnosti a / nebo integrity informací.						
Zjištěný stav: Není interně zavedeno, mobilní koncové stanice mají mít šifrované, ale není řízeno, disky v diskovém poli nejsou šifrované. Není zavedena politika pro uložení dekryptovacích klíčů. Certifikační klíče pro přístup ke klientům jsou v odpovědnosti klienta, společnost s nimi nakládá dle svojí politiky. Dílčí neshoda: Mobilní koncové stanice mají být šifrované, ale není řízeno, disky v diskovém poli nejsou šifrované. Není zavedena politika pro uložení dekryptovacích klíčů. Doporučení: V rámci implementace systému bezpečnosti informací zavést šifrování pevných disků; politiku pro uložení dešifrovacích klíčů.						
ČSN ISO/IEC 27001 příloha A, kapitola 11						
A.11 Fyzická bezpečnost a bezpečnost prostředí	**C**					
A.11.1 Bezpečné oblasti	C					
A.11.2 Zařízení	C					
A.11.1 Bezpečné oblasti	***C***					
Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace.						
Zjištěný stav: viz neshoda. Dílčí neshoda: vnější perimetr není dostatečně chráněn kamerovým systémem; chybí označení, že je prostor monitorován.						

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
Nejsou definovány bezpečnostní zóny. Doporučení: V rámci implementace systému bezpečnosti informací zavést postupy pro ochranu fyz. perimetr kamerovým systémem; zavést značení, že je prostor monitorován. Definovat stupně bezpečnostních zón v organizaci.					
A.11.2 Zařízení	***C***				
Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činnosti organizace.					
Prostředí je provozováno na několika fyzických serverech. Zálohování je nastaveno v plánovaném intervalu, včetně zálohování na páskovou knihovnu. Servery, diskové pole jsou připojeny na UPS. Síťový perimetr je zabezpečen přes FW. Dílčí neshoda: Dané postupy nejsou formalizovány. Nejsou definovány odpovědnosti. Doporučení: V rámci implementace systému bezpečnosti informací zavést postupy, plány obnovy činnosti, včetně definované odpovědnosti.					
ČSN ISO/IEC 27001 příloha A, kapitola 12					
A.12 Bezpečnost provozu	**C**				
A.12.1 Provozní postupy a odpovědnosti	C				
A.12.2 Ochrana proti malwaru	C				
A.12.3 Zálohování	C				
A.12.4 Zaznamenávání formou logů a monitorování	C				
A.12.5 Správa provozního softwaru	C				

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
A.12.6 Řízení technických zranitelností	C				
A.12.7 Hlediska auditu informačních systémů	C				
A.12.1 Provozní postupy a odpovědnosti	***C***				
Cíl: Zajistit správný a bezpečný provoz vybavení pro zpracování informací.					
Zjištěný stav: Testovací prostředí je odděleno od produkčního. Dílčí neshoda: Proces řízení změn není zaveden. Řízení kapacit není zavedeno. Provozní postupy nejsou zavedeny Doporučení: V rámci implementace systému bezpečnosti informací zavést postupy pro řízení změn, řízení kapacit a provozní postupy.					
A.12.2 Ochrana proti malwaru	***C***				
Cíl: Zajistit, aby informace a vybavení pro zpracovávání informaci byly chráněny proti malwaru.					
Zjištěný stav: Ochrana před malwarem je zajištěna na úrovni síťových opatření a softwarových řešení.					
A.12.3 Zálohování	***C***				
Cíl: Chránit proti ztrátě dat.					
Zjištěný stav: Zálohování je řešeno pouze v jedné lokalitě. Zálohovací pásky nejsou umístěny tak, aby byly zabezpečeny proti externími vlivům. Dílčí neshoda: Zálohy nejsou umístěny mimo lokalitu. Doporučení: V rámci implementace systému bezpečnosti informací zavést postupy pro kopírování záloh mimo primární lokalitu.					
A.12.4 Zaznamenávání formou logů a monitorování	***C***				
Cíl: Zaznamenat události a vytvářet záznamy.					

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
Zjištěný stav: Všechny důležité systémy pro zpracování informací jsou synchronizovány s jediným referenčním zdrojem času. Dílčí neshoda: Logy události jsou zaznamenávány, ale nedokumentovány. Administrátorský deník není veden. Logy nejsou chráněny proti neoprávněnému přístupu. Doporučení: V rámci implementace systému bezpečnosti informací zavést postupy dokumentování logů událostí, administrátorský deník, ochranu proti neoprávněnému přístupu a zfalšování.					
A.12.6 Řízení technických zranitelností	***C***	***C***			
Cíl: Zabránit využívání technických zranitelností.					
Zjištěný stav: Síťový perimetr je zabezpečen přes NG FW s konfigurovanými pravidly, včetně detekce potenciálně nežádoucí aktivity. Dílčí neshoda: Nejsou realizovány testy zranitelností v pravidelném intervalu, opatření pro oblast kybernetické bezpečnosti (penetrační testy). Doporučení: V rámci implementace systému bezpečnosti informací zavést testy zranitelností v pravidelném intervalu.					
A. 12.7 Hlediska auditu informačních systémů	***C***				
Cíl: Minimalizovat dopady auditních činností na provozní systémy.					
Zjištěný stav: Oblasti není zavedena. Dílčí neshoda: Oblast „Hlediska auditu informačních systémů“ není zavedena. Doporučení: V rámci implementace systému bezpečnosti informací zavést postupy pro minimalizování dopadu auditních činností na provozní systémy.					
ČSN ISO/IEC 27001 příloha A, kapitola 13					
A.13 Bezpečnost komunikací	**C**				

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
A.13.1 Správa bezpečnosti sítě	C				
A.13.2 Přenos informací	C				
A.13.1 Správa bezpečnosti sítě	***C***				
Cíl: Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací.					
Zjištěný stav: Síťový perimetr je chráněn na úrovni jeho hranice přes firewall s aplikovanými pravidly. Jistá úroveň bezpečnosti je také zajištěna přes poskytovatele konektivity**.**					
A.13.2 Přenos informací	C				
A.13.2 Přenos informací	***C***				
Cíl: Zajistit bezpečnost informací při jejich přenosu v rámci organizace a s externími subjekty.					
Zjištěný stav: Dohody o mlčenlivosti nejsou podepisovány s relevantními osobami. Dílčí neshoda: Není zavedena politika pro přenos informací a pravidla pro třetí strany. Doporučení: V rámci implementace systému bezpečnosti informací zavést politiku pro přenos informací a pravidla pro přístup k informacím třetích stran.					
ČSN ISO/IEC 27001 příloha A, kapitola 14 NR					
A.14 Akvizice, vývoj a údržba systémů	**C**				
A.14.1 Bezpečnostní požadavky informačních systémů	C				
A.14.2 Bezpečnost v procesech vývoje a podpory	C				
A.14.3 Data pro testování	C				
A.14.1 Bezpečnostní požadavky informačních systémů	***C***				

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
Cíl: Zajistit, aby se bezpečnost informací stala nedílnou součástí informačních systémů v jejich celém životním cyklu. To zahrnuje i požadavky na informační systémy, které poskytují služby ve veřejných sítích.					
A.14.2 Bezpečnost v procesech vývoje a podpory	***C***				
Cíl: Zajistit, aby bezpečnost informací byla navrhována a implementována v životním cyklu vývoje informačních systémů.					
A.14.3 Data pro testování	***C***				
Cíl: Zajistit ochranu dat používaných pro testování.					
ČSN ISO/IEC 27001 příloha A, kapitola 15					
A.15 Dodavatelské vztahy	**C**				
A.15.1 Bezpečnost informací v dodavatelských vztazích	C				
A.15.2 Řízení dodávek služeb dodavatelů	C				
A.15.1 Bezpečnost informací v dodavatelských vztazích	***C***				
Cíl: Zajistit ochranu aktiv organizace, ke kterým mají dodavatelé přístup.					
Zjištěný stav: Přístup externích subjektů je řešen na základě postupů pro vznik dodavatelského vztahu. Přístupy a informace jsou omezeny na principu minimálnosti. Dílčí neshoda: Není explicitně vyžadována dohoda o mlčenlivosti a přenášeny požadavky v oblasti kybernetické bezpečnosti přímo na dodavatele. Doporučení: V rámci implementace systému bezpečnosti informací zavést proces pro řízení dodavatelských vztahů a vyžadovat mj. podpis dohody o mlčenlivosti.					
A.15.2 Řízení dodávek služeb dodavatelů	***C***				

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
Cíl: Udržovat dohodnutou úroveň bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami.					
Zjištěný stav: Dané postupy jsou řešeny dle požadavků organizace a odpovídající závazky jsou přeneseny na dodavatele.					
ČSN ISO/IEC 27001 příloha A, kapitola 16					
A.16 Řízení incidentů bezpečnosti informací	**C**				
A.16.1 Řízení incidentů bezpečnosti informací a zlepšování	C				
A.16.1 Řízení incidentů bezpečnosti informací a zlepšování	***C***				
Cíl: Zajistit odpovídající a efektivní přístup ke zvládání incidentů bezpečnosti informací zahrnujícímu komunikaci ohledně bezpečnostních událostí a slabých míst.					
Zjištěný stav: V případě identifikace bezpečnostního incidentu je uživatel povinen tuto skutečnost okamžitě hlásit. Incidenty nejsou evidovány; pouze incidenty s nízkou hodnotou. Cloudové prostředí – office 365 Dílčí neshoda: Není zaveden formální proces pro řízení bezpečnostních incidentů. Doporučení: V rámci implementace systému bezpečnosti informací zavést proces pro řízení bezpečnostních incidentů.					
ČSN ISO/IEC 27001 příloha A, kapitola 17					
A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	**C**				
A.17.1 Kontinuita bezpečnosti informací	C				
A.17.2 Redundance	C				
A.17.1 Kontinuita bezpečnosti informací	***C***				

	Stupně hodnocení				
	1. Náhodně	**2. Opakovatelně**	**3. Definovaně**	**4. Měřitelně**	**5. Optimalizovaně**
Cíl: Kontinuita bezpečnosti informací musí být součástí systémů řízení kontinuity činností organizace.					
Zjištěný stav: Nebyly identifikovány formalizovaní postupy pro řízení kontinuity informací a jejich pravidelné testování. Dílčí neshoda: DR plány nejsou formálně popsány, nebylo identifikováno průběžné přezkoumávání planu o obnovy. Doporučení: V rámci implementace systému bezpečnosti informací zavést postup DR, periodicky testovat zálohy.					
A.17.2 Redundance	***C***				
Cíl: Zajistit dostupnost vybavení pro zpracování informací.					
Zjištěný stav: Infrastruktura je redundantní výkonově i prostorově.					
ČSN ISO/IEC 27001 příloha A, kapitola 18					
A.18 Soulad s požadavky	**C**				
A.18.1 Soulad s právními a smluvními požadavky	C				
A.18.2 Přezkoumání bezpečnosti informací	C				
A.18.1 Soulad s právními a smluvními požadavky	***C***				
Cíl: Vyvarovat se porušení zákonných, předpisových nebo smluvních povinností týkající se bezpečnosti informací a jakýchkoliv bezpečnostních požadavků.					
Zjištěný stav: Byly identifikovány postupy pro zajištění souladu v oblasti GDPR. Dílčí neshoda: Nebyly identifikovány postupy pro zajištění souladu s ZOKB. Doporučení: V rámci implementace systému bezpečnosti informací zavést postupy pro soulad se ZOKB a odpovídající vyhlášky.					

	Stupně hodnocení				
	1. Náhodně	2. Opakovatelně	3. Definovaně	4. Měřitelně	5. Optimalizovaně
A.18.2 Přezkoumání bezpečnosti informací	***C***				
Cíl: Zajistit, že bezpečnost informací je implementována a provozována v souladu s politikami a postupy organizace.					
Zjištěný stav: Oblast není zavedena. Dílčí neshoda: Oblast „*Přezkoumání bezpečnosti informací" není zavedena.* Doporučení: Zavést „Přezkoumání bezpečnosti informací".					

Tabulka č. 12 - Bezpečnostní cíle informační bezpečnosti [9]

2.3 Procesní opatření

V rámci srovnávací analýzy nebyly identifikovány žádné interní postupy ve vztahu k systémům, které jsou v rozsahu této práce. Postupy pro jejich zavedení jsou součástí praktické části.

2.4 Identifikace systémů

V rámci analytické práce jsem provedl identifikaci systémů, včetně jejich správné implementace. Vzhledem k tomu, že tato práce je veřejně publikována, jsou jednotlivé názvy aplikací anonymizovány a není uveden jejich, popis, technologie, či jakýkoliv identifikující popis.

Testované služby
Služba 1
Služba 2
Služba 3
Služba 4

Služba 5
Služba 6
Služba 7
Služba 8
Služba 9
Služba 10
Služba 11
Služba 12
Služba 13
Služba 14
Služba 15
Služba 16
Služba 17
Služba 18
Služba 19
Služba 20
Služba 21
Služba 22
Služba 23
Služba 24
Služba 25
Služba 26

Služba 27
Služba 28

Tabulka č. 13 - Identifikované systémy

2.5 Technická opatření

Pro identifikaci nastavených opatření bylo provedeno testování jednak externího a interního síťového perimetru, a to definovaného rozsahu. Společně s tím byly provedeny testy aplikací na základě OWASP. Identifikované analýza dostupných aplikací. Detailní výpis těchto testů není v této práci uveden, a to zejména s ohledem na potenciální rizika. Nebyla také provedena identifikace potenciálních falešně pozitivních nálezů.

Identifikované zranitelnosti jsou uvedeny níže v dalších kapitolách. Vzhledem k tomu, že byly identifikovány také zranitelnosti, které mohou mít zcela zásadní vliv na provoz daného serveru, mitigační opatření byla již realizována v době zpracování této práce.

Součástí testů bylo provedení veškerých dodaných služeb, s tím že pro výstupy byly předány v rámci mitigačních prací. Níže jsou uvedeny pouze nejvíce rizikové služby.

2.5.1 Služba 15

ID	Zranitelnost	CVSS	Potenciální hrozba a řešení
1	**Cross-Site Scripting**	**3**	**Hrozba** Tato aplikace je potenciálně zranitelná vůči XSS- **Řešení** Ověřit, že dané znaky jsou správně zpracovány a je s nimi korektně nakládáno. Například znak " pokud je zobrazen, tak je nahrazen znakem %22.
2	Web shell	**3**	**Hrozba** Byl identifikován webový shell na server. Může obsahovat zranitelný soubor, který umožňuje útočníkovi předávat kódy na webový server. **Řešení**

			Odstranit veškeré instance webového shellu a zjistit, jestli na serveru nebyly provedeny žádné autorizované změny.

2.5.2 Služba 10

ID	Zranitelnost	CVSS	Potenciální hrozba a řešení
1	Reflected Cross-Site Scripting (XSS) Vulnera-bilities	**5**	**Hrozba** Byla identifikována hrozba ve formuláři XSS umožňující provést cross-site scripting útok. **Řešení** Filtrovat veškerá data data a zajistit, že data jsou správně předávána a zpracovávána.

2.5.3 Služba 25

V případě této aplikace nebyly identifikovány žádné zranitelnosti vyšší než CVSS 3.

2.5.4 Služba 12

ID	Zranitelnost	CVSS	Potenciální hrozba a řešení
1	Web shell	5	**Hrozba** Byl identifikován webový shell na server. Může obsahovat zranitelný soubor, který umožňuje útočníkovi předávat kódy na webový server. **Řešení** Odstranit veškeré instance webového shellu a zjistit, jestli na serveru nebyly provedeny žádné autorizované změny.
2	WordPress XML-RPC	4	**Hrozba**

	Pingback Vulnerability		Bylo identifikováno API řešení WordPress na kterém je daný projekt provozován. Pingback může umožnit útočníkovi realizovat útoky přes DDOS a také SSRF. **Řešení** Odstranit soubor "pingback.ping" z XML-RPC.
3	Clickjacking - Framable Page	3	**Hrozba** Chybí definovaná hlavička: X-Frame-Options. Pokud to není uvedeno, může útočník přes metodu clickjacking nasadit další frame webové stránky. **Řešení** Doplnit: - X-Frame-Options: Tato HTTP odpověď minimalizuje hrozbu - Content-Security-Policy: Tento 'frame-ancestors' proměnná bývá použita na potlačení metod.

2.5.5 Služba 23

ID	Zranitelnost	CVSS	Potenciální dopad a řešení
1	SQL Injection	5	**Hrozba** Bylo identifikováno potenciální využití SQL injection na dané stránce. Tato hrozba může mít zcela zásadní dopad na provoz daného řešení, včetně potenciální kompromitace dat. **Řešení** Provést revizi celého řešení a zajistit nemožnost využití této hrozby, zpravidla je to řešení na úrovni databázového serveru, či frameworku na kterém je provozováno.
2	Command Injection	5	**Hrozba**

			Byla detekována možnost spuštění kódu přímo na webovém serveru. Útočník může spustit vzdáleně příkaz na úrovni systému. **Řešení** Omezit spuštění systémových příkazů, pokud je nezbytné jejich využití, tak omezit jejich oprávnění a zajistit správnost vstupních dat do nich.
3	Apache Log4j Remote Code Execution	5	**Hrozba** Byla identifikována zranitelnost Apache Log4j v aplikaci. V případě úspěšného využití umožní útočníkovi provést vzdálené spuštění kódu na cíli. **Řešení** Provést aktualizaci dané knihovny, či provést opatření pro mitigaci.

2.5.6 Služba 3

ID	Zranitelnost	CVSS	Potenciální hrozba a řešení
1	SQL Injection	5	**Hrozba** Bylo identifikováno potenciální využití SQL injection na dané stránce. Tato hrozba může mít zcela zásadní dopad na provoz daného řešení, včetně potenciální kompromitace dat. **Řešení** Provést revizi celého řešení a zajistit nemožnost využití této hrozby, zpravidla je to řešení na úrovni databázového serveru, či frameworku na kterém je provozováno.
2	Přihlašovací stránka není	4	**Hrozba** Přihlašovací stránka není předávána přes šifrované spojení.

	řešena přes HTTPS		**Řešení** Upravit přihlašovací stránku na šifrované spojení.

2.5.7 Služba 24

ID	Zranitelnost	CVSS	Potenciální hrozba a řešení
1	WordPress XML-RPC Pingback Vulnerability	4	**Hrozba** Bylo identifikováno API řešení WordPress na kterém je daný projekt provozován. Pingback může umožnit útočníkovi realizovat útoky přes DDOS a také SSRF. **Řešení** Odstranit soubor "pingback.ping" z XML-RPC.

2.5.8 Služba 16

ID	Zranitelnost	CVSS	Potenciální hrozba a řešení
1	WordPress XML-RPC Pingback	4	**Hrozba** Bylo identifikováno API řešení WordPress na kterém je daný projekt provozován. Pingback může umožnit útočníkovi realizovat útoky přes DDOS a také SSRF. **Řešení** Odstranit soubor "pingback.ping" z XML-RPC.
2	HTML form containing password	3	**Hrozba** Přihlašovací stránka není předávána přes šifrované spojení. **Řešení** Upravit přihlašovací stránku na šifrované spojení.

2.5.9 Služba 1

ID	Zranitelnost	CVSS	Potenciální dopad a řešení

1	WordPress REST API User Enumeration Vulnerability	4	**Hrozba** Bylo identifikováno API řešení WordPress na kterém je daný projekt provozován. Pingback může umožnit útočníkovi realizovat útoky přes DDOS a také SSRF. **Řešení** Odstranit soubor "pingback.ping" z XML-RPC.
2	Web Server Uses Plain-Text Form Based Authentication	3	**Hrozba** Přihlašovací stránka není předávána přes šifrované spojení. **Řešení** Upravit přihlašovací stránku na šifrované spojení.
3	PHP Multiple Denial of Service Vulnerabilities	3	**Hrozba** Byly identifikovány zranitelnosti ve verzi používaného PHP. **Řešení** Provést aktualizace verze jazyka PHP, případně provést izolaci serveru.

II. PRAKTICKÁ ČÁST

3 NÁVRH OPATŘENÍ

V kapitolách níže jsou uvedena opatření pro implementaci požadavků, a to jak organizační, tak technická.

3.1 Návrh formálních požadavků

Z hlediska formálních požadavků je nezbytné zavést alespoň minimum pro zajištění souladu s legislativou. Jedním z pilířů implementace je bezpečnostní řád, který ukotvuje celé prostředí ISMS organizace. Další nezbytné body jsou uvedeny níže. Uvedené formální předpoklady představují obecný rámec dle požadavků ZOKB.

Každá z níže uvedených politik a směrnice musí odpovídat odpovídající struktuře interní dokumentace společnosti.

Z hlediska nezbytných opatření je vhodné využít odpovídající standard, který je možné identifikovat v ZOKB, což je ISO 27001. V tomto případě je dobré zvážit, že pokud je realizována i certifikace dle ISO normy, každý subjekt definuje dokument prohlášení o aplikovatelnosti.

Nezbytná dokumentace je uvedena v dalších kapitolách níže.

3.1.1 Politika ISMS

Je určujícím dokumentem, který zajišťuje ukotvení politiky ISMS v prostředí organizace. Organizace se v této politice zavazuje nejen k definování odpovědností.

Nezbytné je definovat závazek vedení organizace, nejlépe v následujících bodech:

- ustanovením této politiky ISMS
- stanovením cílů ISMS a plánu pro jejich dosažení
- stanovením rolí, povinností a odpovědností v oblasti bezpečnosti informací
- zajištěním dostatečných zdrojů pro procesy ISMS
- rozhodováním o přijatelné míře rizika
- zajištěním interních auditů
- prováděním přezkoumání ISMS

Organizace by také musí zajistit určení odpovědností za jednotlivé oblasti, a to dle organizační struktury. Minimálně by to mělo být provedeno v následujícím rozsahu:

Kvestor univerzity v konečném důsledku odpovídá a svou osobou zaštiťuje:

a) úroveň celkové bezpečnosti informací společnosti, vyhodnocování a sledování bezpečnostních rizik a přijímání strategických rozhodnutí k jejich minimalizaci, prostřednictvím manažera bezpečnosti informací,

b) účinnou implementaci bezpečnostní politiky ve všech oblastech působnosti společnosti,

c) neustálé zvyšování bezpečnostního povědomí zaměstnanců společnosti.

Jelikož další odpovědnosti jsou ryze technického charakteru, bude nezbytné určit tuto odpovědnost na kompetentní osobu. V rámci této práci tuto roli budu dále nazývat Manažer bezpečnosti informací. Je to osoba odpovědná za koordinaci veškerých aktivit spojených s bezpečností informací ve společnosti. Odpovídá za návrh, kontrolu a zlepšování opatření oblasti ICT, fyzické, personální a administrativní bezpečnosti informací a za realizaci bezpečnostních opatření.

V rámci společnosti a své odpovědnosti odpovídá za:

a) prosazování pravidel stanovených v této směrnici v projektech, smlouvách a komplexních řešeních bezpečnosti informací,

b) metodické řízení bezpečnosti informací a dat, hodnocení a řízení bezpečnostních rizik,

c) tvorbu, publikaci, evidenci a aktualizaci bezpečnostní dokumentace, včetně údržby klasifikačního schéma dle požadavků legislativy a garantů informací a dat,

d) zajištění bezpečnosti v souladu s platnou národní i nadnárodní legislativou, která se týká činnosti společnosti,

e) vyhodnocování a řešení bezpečnostních incidentů a celkového stavu bezpečnosti,

f) návrh efektivních bezpečnostních opatření s ohledem na priority a míru rizik a minimalizaci nákladů na bezpečnost,

g) sestavení celkového rozpočtu na informační bezpečnost a efektivní vynakládání finančních prostředků v rámci schváleného rozpočtu na informační bezpečnost,

h) schvalování specifických metodik a postupů v oblasti bezpečnosti informací, např. hodnocení informačních rizik, systém klasifikace informací,

i) přijímání a podporu iniciativ v oblasti bezpečnosti informací dotýkajících se celé organizace, např. program zvyšování bezpečnostního vědomí,

j) prosazování, aby podpora organizace bezpečnosti informací byla viditelná v celé společnosti,

k) spolupráci s administrátorem sítě, kterému pomáhá řešit na strategické úrovni problematiku bezpečnosti ICT,

l) v oblasti fyzické bezpečnosti spolupracuje se správou objektu, případně s externími subjekty,

m) v případě potřeby za spolupráci s orgány veřejné správy (Policie ČR, hasiči), pohotovostní služby), zájmovými skupinami, kterými jsou ve smyslu ISO/IEC 27002 míněna oborová sdružení nebo specializovaná fóra zabývající se bezpečností informací,

n) reporting vedení společnosti v oblasti bezpečnosti informací,

o) stanovení a delegování specifických rolí a odpovědnosti za bezpečnost informací v rámci ICT,

p) průběžné sledování bezpečnosti ICT a správnosti nastavení,

q) kontrolu správnosti nastavení doménových politik a uživatelských účtů,

r) kontrolu bezpečnostních logů aplikací a vyhodnocování bezpečnostních incidentů,

s) návrh bezpečnostních opatření a přístupových práv,

t) kontrolu monitoringu odchozích dat a jeho vyhodnocení.

u) instalaci, konfiguraci prostředků ICT, s ohledem na zajištění bezpečnosti a kontinuity činností,

v) udržování provozní dokumentace obsahující popis klíčových parametrů,

w) udržování helpdesku a provozní dokumentace obsahujících hlášené provozní chyby, změny konfigurace, instalace a aktualizace,

x) hlášení podezřelých událostí a bezpečnostních incidentů v rámci ICT systémů a technologií ISMS,

y) kontrolu správnosti nastavení doménových politik a uživatelských účtů,

z) kontrolu nastavení uživatelských účtů.

aa) dodržování klíčového režimu.

V oblastech ve vztahu k dceřiným společnost může být tato role, či některé z jejich odpovědností delegovány na odpovědnou osobu v dané lokalitě. Delegování může být provedeno jen v případě schválení Kvestora. Deleguje své odpovědnosti v rámci svého týmu na provozního administrátora a administrátora bezpečnosti.

Tato politika také musí ustanovit kontrolní orgán, kde je zpravidla určena odpovědnost na interní audit.

3.1.2 Směrnice – Pravidla ISMS

Hlavním cílem této směrnice je zavedení a provozování systému řízení bezpečnosti informací (ISMS) je zavedení komplexního, systematického, dokumentovaného, trvalého procesu průběžného hodnocení informačních rizik, výběru, implementace, dokumentace a údržby adekvátních bezpečnostních opatření, kontroly jejich funkčnosti a efektivnosti a neustálého zlepšování celkového stavu bezpečnosti informací v společnosti.

3.1.2.1 Základní pravidla ISMS

Tento dokument představuje formální potvrzení procesu ISMS ve společnosti a definuje jeho hlavní poslání, cíle, náplň a odpovědnosti.

Působnost systému řízení ISMS se vztahuje na zpracování, uchovávání a distribuci informací v rámci všech procesů ve společnosti.

Minimálně 1x ročně CTO provede přezkoumání působnosti procesu ISMS tak, aby zahrnoval především všechny klíčové procesy a činnosti společnosti a všechna informační aktiva, která tyto procesy zajišťují a využívají.

Vedení na základě svých pravomocí a odpovědností definovaných v „Politice ISMS“ zajistí koordinaci realizace procesu ISMS ve společnosti a jeho rozpracování do konkrétních opatření a dokumentace.

Dále zajistit naplňování a zajištění třech základních atributů bezpečnosti informací:

1. důvěrnosti – ochrana aktiv proti neautorizovanému přístupu a úniku,

2. integrity – ochrana aktiv před jejich neautorizovanou modifikací a zajistit jejich úplnost a správnost,

3. dostupnosti – je nutné zabezpečit jejich dostupnost v souladu s požadavky organizace.

Pro dosažení těchto cílů je třeba periodicky procházet základní PDCA fáze (Plan-Do-Check-Act) procesu ISMS, stanovit odpovědnosti za realizaci jednotlivých kroků těchto fází i za realizaci bezpečnostních opatření, které jsou procesem ISMS vybírána, implementována, provozována, kontrolována a zlepšována.

Etapy ISMS	**Základní kroky v rámci etap ISMS**	**Realizace kroků ISMS**
Plánuj	ustavení ISMS	tato směrnice
	působnost ISMS	Projekt bezpečnosti informací – etapa 2
	bezpečnostní politika informací	Bezpečnostní řád společnosti
	hodnocení rizik	Projekt bezpečnosti informací – etapa 2
Dělej	zvládání rizik	Projekt bezpečnosti informací – etapa 2 + 3
	zavedení vybraných opatření ISMS	Projekt bezpečnosti informací – etapa 3
	dokumentace opatření a procesu ISMS	Projekt bezpečnosti informací – etapa 3
	prohlášení o aplikovatelnosti opatření	Projekt bezpečnosti informací – etapa 3
Kontroluj	přezkoumání ISMS na úrovni vedení CTO	Projekt bezpečnosti informací – etapa 4
	zajištění, že opatření ISMS fungují efektivně	dodržování vybraných opatření a postupů
	interní audity ISMS	kontrola dodržování vybraných opatření a postupů
Jednej	analýza nalezených neshod a problémů	přezkoumání výsledků auditů a kontrol a návrh opatření

	šetření bezpečnostních incidentů	šetření bezpečnostních incidentů a návrh opatření
	realizace preventivních a nápravných opatření	výběr konkrétních opatření, jejich implementace a dokumentace

Tabulka č. 14 - Etapy ISMS

V uvedených krocích a fázích ISMS procesu jsou vybírány, implementovány, provozovány, dokumentovány a zlepšovány adekvátní opatření z normy ISO/IEC 27002:2005, která představuje souhrn doporučených praktik a opatření pro zajištění bezpečnosti informací.

Opatření z této normy jsou vybírána na základě hodnocení rizik, požadavků relevantní národní a nadnárodní legislativy, smluvních požadavků, ke kterým je společnost zavázán a na základě požadavků poslání, procesů, principů a cílů společnosti.

3.1.3 Směrnice pro realizaci analýzy rizik

Systém řízení rizik zavedený ve společnosti vychází z metodiky uvedené ve VKB a navazuje na systém řízení aktiv zavedený dokumentem „Identifikace a správa informačních aktiv“. Z tohoto dokumentu využívá zejména rozdělení aktiv, jejich identifikaci a určení vazeb mezi nimi, a dále zavádí pravidla pro určení rizik na základě významu primárních aktiv, působících hrozeb a zranitelností podpůrných a technických aktiv určených jako VIS, vyplývajících z narušení jejich důvěrnosti, integrity a dostupnosti.

Životní cyklus řízení rizik ve společnosti se skládá z následujících částí:

- stanovení kontextu (definice prostředí –oblast působnosti SŘBI),
- stanovení akceptovatelné úrovně rizik,
- analýzy rizik,
- zvládání rizik,
- monitorování a přehodnocování rizik.

Pro zajištění objektivního hodnocení aktiv i rizik a srovnatelnosti výsledků jednotlivých analýz rizik, jsou v prostředí společnosti veškeré analýzy rizik realizovány dle této metodiky.

Analýza rizik je realizována v následujících krocích:

- identifikace a hodnocení primárních aktiv,

- identifikace podpůrných aktiv,
- určení vazeb mezi primárními a podpůrnými aktivy,
- identifikace a hodnocení hrozeb,
- identifikace a hodnocení zranitelností podpůrných aktiv,
- hodnocení rizik,
- návrh způsobu zvládání rizik,
- návrh opatření pro zvládání rizik.

3.1.4 Směrnice pro řízení přístupů a lidských zdrojů

Uvedená směrnice má za cíl nastavit politiky pro řízení lidských zdrojů, od vzniku oprávnění, přes pravidla pro jeho změnu a také postupy v případě ukončení.

Přístupová práva jsou rozdělena na základě zařazení uživatele do role podle její specifikace.

Při vzniku pracovního poměru jsou založena odpovědnou osobou na základě schváleného požadavku nadřízeným pracovníka.

V případě změny přidělených přístupových práv je jejich nastavení provedeno na základě schváleného požadavku nadřízeného pracovníka odpovědnou osobou.

Ukončení je opět provedeno v rámci řízeného postupu odpovědnou osobou, ukončení musí být realizováno v rámci všech aktivních přístupů, které uživatel měl aktivní.

Další důležitou politikou je správa uživatelských hesel, kde musí být nastaveny politika pro nakládání s nimi, opatření pro privilegované uživatele a postupy pro nakládání s nimi v případě výchozí instalace.

Přístupová práva musí být také pravidelně přezkoumávána a případné rozdíly vyhodnoceny.

Pro nakládání s hesly musí být nastaveny přesné postupy a to mj. v následujícím rozsahu:

- po prvním přihlášení je uživatel nucen změnit výchozí heslo,
- uživatelé musí být seznámeni s pravidly používání hesel, uživatelé musí mít možnost z vlastní iniciativy si změnit heslo do aplikací,
- obměna hesel musí být vyžadována,

- heslo nesmí být čitelné při zadávání,
- hesla musí být ukládána nevratným šifrováním,
- implicitní hesla musí být změněna bezprostředně po instalaci,
- měla by být preferována jednotná politika hesel ve všech aplikacích.
- hesla nesmí být zaznamenávána, s výjimkou schváleného uložení vedení společnosti,
- hesla musí být pravidelně měněna,
- délka hesla a pravidla se liší podle druhu uživatelského účtu,
- hesla nesmí obsahovat žádné údaje ve spojení s uživatelem, jeho pracovním zařazení a ostatní snadno určené údaje.

3.1.5 Směrnice pro - Mobilní zařízení a Práce na dálku

Vzhledem k tomu, že mobilní zařízení poskytuje také přístup k aktivům organizace, je nutné pro práci s ním mít nastavené odpovídající postupy. Zejména s ohledem na minimalizaci rizik a potenciální ztrátu, či únik dat.

Opatření je také nutné nastavit pro práci na dálku, na vzdáleném pracovišti musí existovat opatření zajišťující dodržování bezpečnostní politiky informací společnosti.

A to zejména:

- podle klasifikace dat musí být zavedeny příslušná opatření pro zajištění jejich bezpečnosti,

- bezdrátové sítě musí být nastaveny tak, aby nebylo do nich možný přístup neoprávněnými osobami,

- přenosný počítač, či zařízení musí mít nastavenou bezpečnostní bránu, tak aby nebyla možná připojení do zařízení z ostatních v síti,

- pro přístup do společnosti musí být umožněno pouze na základě připojení k VPN serveru.

3.1.6 Směrnice pro klasifikaci informací a dat

Data představují klíčové aktivum každé organizace a postupy pro nakládání s nimi jsou stanoveny na základě jejich klasifikace.

3.1.6.1 Klasifikace informací

a) *Chráněné* – informace, se kterými pracují pouze pověření zaměstnanci v souladu s interními postupy a přidělenými přístupovými právy do zabezpečených IS:

- *osobní údaje* ve smyslu Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR) a zákona č. 110/2019 Sb., o zpracování osobních údajů (obsahují kromě údajů o zdravotním stavu osoby také rodné číslo, jméno a příjmení, adresu bydliště nebo název obce pod 10 000 obyvatel) a dále vnitřní pokyny a personální předpisy (dle § 11 zákona č. 106/1999 Sb.) a personální údaje, krizové plány apod. (zák. č. 240/2000 Sb.) a dále všechna data (informace), jejichž zveřejnění by mohlo vést k poškození duševního vlastnictví společnost,
- *anonymizované osobní údaje* ve smyslu Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR) a zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (neobsahují rodné číslo, jméno a příjmení, adresu bydliště nebo název obce pod 10 000 obyvatel),
- *jiné chráněné informace*

Do stupně 3 – CHRÁNĚNÉ se klasifikuje informace v případě, že její vyzrazení, chybné použití nebo přístup neoprávněné osoby k ní a to i uvnitř společnosti, mohou ohrozit či ztížit činnost společnosti nebo způsobit újmu fyzické nebo právnické osobě, která informaci poskytla, nebo které se informace týká. Tyto jsou určeny pouze pověřeným zaměstnancům společnosti a smluvním třetím stranám. Podrobně v kapitole Označování informací a manipulace s nimi.

b) *Pro vnitřní potřebu* – běžná agenda nepodléhající vyššímu stupni ochrany, informace vystavené na intranetu:

Do stupně 2 – INTERNÍ tj. PRO VNITŘNÍ POTŘEBU se informace klasifikuje v případě, že svým obsahem nespadá do stupně CHRÁNĚNÉ a nespadá do stupně EXTERNÍ. Jde o interní materiály zveřejňované prostřednictvím intranetu (vnitřní sítě)

c) *Informace určené pro zveřejnění* – doporučeno k vystavení na internetu společnosti nebo určeno ke zveřejnění útvarem zodpovědným za komunikaci s veřejností):

Do stupně 1 – EXTERNÍ tj. URČENÉ PRO ZVEŘEJNĚNÍ se informace klasifikuje v případě, kdy se jedná o informaci, kterou je společnost povinná zveřejnit podle zvláštního zákona, například zákona č. 106/1999 Sb., o svobodném přístupu k informacím, nebo o informace poskytované na veřejných internetových stránkách ministerstva, publikace určené veřejnosti, různé formy agregace dat, a data získaná z veřejných zdrojů.

3.1.7 Směrnice fyzické bezpečnosti

Fyzická bezpečnost se řeší na úrovni každého pracoviště a nejvíce vhodným způsobem je vytvoření bezpečnostních zón dle povahy informací a dat v nich zpracovávaných. S ohledem na činnost univerzity je dostatečné nastavit čtyř stupňový systém, který je shrnut v tabulce níže:

Název zóny	Popis
Bezpečnostní zóna 1	Prostory se zvýšenými nároky na bezpečnost (místnosti, kde se zpracovávají a uchovávají zejména osobní data ve fyzické podobě, či slouží jako úložiště fakticky citlivých dat).
Kancelář se zvýšenými nároky na bezpečnost	Kanceláře se zvýšenými nároky na bezpečnost (rektorát, personální oddělení, IT)
Kancelář	Ostatní kancelářské prostory
Veřejný prostor	Veřejně přístupné prostory (chodba, učebny).

Tabulka č. 15 - Návrh bezpečnostních zón

Způsob zabezpečení objektů/pracovišť se stanovuje v souladu s obecně závaznými právními předpisy a interními normami společnosti. Informace týkající se projekce, montáže, provozu a údržby zabezpečení objektu je nutné považovat za interní.

Před stanovením rozsahu zabezpečení je proveden bezpečnostní průzkum určeny a oceněny aktiva, vyhledány zranitelná místa a hrozby a navrženo bezpečnostní opatření s přihlédnutím na jejich hodnotu.

Při návrhu bezpečnostních opatření je nutné postupovat od perimetru až po jednotlivá aktiva, přičemž je kladen důraz na zabezpečení perimetru. Pro pracoviště platí, že perimetr je na hranici objektu.

3.1.8 Směrnice zálohování a obnovy dat

Zálohování, obnova a dlouhodobé ukládání jsou součástí procesů ISMS a zahrnují veškeré vytváření záložních kopií dat, softwaru a kopií systému, jejich obnovu a archivaci dat. V rámci provozovaných informačních systémů společnosti jsou zálohována a dlouhodobě ukládána data systémů a aplikací.

Zálohování důležitých technických aktiv je v prostředí společnost zajišťováno:

• využitím redundance v návrhu řešení informačních systémů,

• zajištěním náhradních technických aktiv.

Za účelem efektivního využití prostředků a řízení záloh jsou rozlišovány tři oblasti podle požadavků kladených na jejich zálohování:

• Data s maximální přípustnou ztrátou méně než 24 hodin, tzn. RPO < 24 hodin

• Data s maximální přípustnou ztrátou 24 hodin a více, tzn. RPO >= 24 hodin

• Operační systém, aplikace a konfigurace (zálohy IS bez dat).

3.1.8.1 Požadavky na zálohování a obnovu

Zálohování a obnova informačních systémů, aplikací a dat musí být prováděna pracovníky s dostatečnou a odpovídající znalostí systémového prostředí organizace a s patřičnou odbornou způsobilostí. Pro realizaci zálohování, testování a obnovy dat je ve společnosti určena role Administrátor, které jsou přidělena patřičná systémová a aplikační oprávnění. Vhodnou technologii pro zálohování, obnovu a dlouhodobé ukládání navrhuje Architekt kybernetické bezpečnosti. Požadavky na četnost (frekvenci), dostupnost záloh a dobu jejich uchování stanovují vlastníci informačních aktiv (vlastníci informací) v závislosti na dopadech způsobených nedostupností či ztrátou dat identifikovaných na základě analýzy rizik bezpečnosti informací, popřípadě výstupů analýzy dopadů, a s ohledem na možnosti zálohovací infrastruktury. Doba uchování záloh musí reflektovat legislativní požadavky a provozní podmínky. Požadavky na zálohování schvaluje manažer kybernetické bezpečnosti.

3.1.9 Směrnice řízení změn

Veškeré změny systémů pro zpracování prostředků informací musí být řízeny.

Odpovědnosti za řízení změn se liší podle zařazení aktiv a kategorizace zpracovávaných dat.

Veškeré programové vybavení musí být před uvedení do produktivního provozu otestováno.

Před finálním schválením je vyhodnocena existence bezpečnostního rizika. Pokud existuje, podléhá navrhovaná změna schválení odpovědné osoby za řízení IT.

Aktiva	Navrhuje	Schvaluje
Informační	Manažer provozu	Určená osoba
Programová	Manažer provozu	Určená osoba
Fyzická	Manažer provozu	Určená osoba
Služby	Manažer provozu	Určená osoba

Tabulka č. 16 - Schvalovací postupy pro řízení změn

3.1.10 Směrnice řízení dodavatelů

Externími subjekty jsou všichni dodavatelé, kteří poskytují nebo dodávají do organizace zboží, služby na základě smluvního vztahu.

U zpracovávaných informací externími subjekty musí být zejména zachována jejich důvěrnost a zajištěna bezpečnost.

Pro dodržení a zachování jednotné úrovně ochrany informací je nutné, aby:

a) ve smlouvě s externím subjektem byly definovány podmínky přístupu a přístup byl řízen,

b) byla na základě vyhodnocených rizik stanovena odpovídající bezpečnostní opatření, externí subjekt se musí zejm. zavázat dodržovat pravidla stanovená touto směrnicí,

c) smlouvy musí obsahovat ujednání zajišťující zejména:

- ochranu informací, duševního vlastnictví, know-how, obchodního tajemství a osobních údajů, a definovány odpovědnosti za případné porušení, či nedostatečnou ochranu těchto informací,
- dodržování ujednaných bezpečnostních opatření,
- postupy pro prevenci, zjišťování a prošetřování bezpečnostních incidentů,
- další náležitosti podle příslušných právních předpisů, pokud je dodavatel v pozici zpracovatele osobních údajů.

Smlouva musí být za obě strany podepsána osobou, která je za společnost oprávněna jednat navenek.

Pro prostory společnosti, do kterých má přístup třetí strana, musí být zachována bezpečnost a přístup třetích stran řízen.

Do smluv musí být zařazeny požadavky z následujícího seznamu, které jsou pro daný případ relevantní:

a) obecná pravidla bezpečnosti informací (netechnické standardy),

b) ochrana aktiv zahrnující:

- postupy sloužící k ochraně aktiv organizace včetně informací a programového vybavení,

- postup sloužící ke zjištění, zda nedošlo ke kompromitaci aktiv, například ztrátě nebo modifikaci dat,

- opatření zajišťující vrácení či zničení informací/aktiv po ukončení smluvního vztahu nebo v jeho průběhu,

- integritu a dostupnost aktiv,

- omezení kopírování a šíření informací.

c) popis každé služby, která je třetí straně zpřístupněna,

d) cílová úroveň služby a neakceptovatelné úrovně služby,

e) tam, kde je to vhodné, podmínky přechodu personálu mezi smluvními stranami,

f) konkrétní smluvní závazky třetí strany,

g) odpovědnosti a náležitosti vyplývající z právních norem, např. z legislativy na ochranu osobních údajů – zvláště v případech uzavírání smluv mezi stranami z různých států je nutné vzít v úvahu národní legislativu,

h) ochrana duševního vlastnictví a autorských práv,

i) ujednání o řízení přístupu zahrnující:

- povolené metody přístupu a jeho kontrolu, použití jedinečných identifikátorů, jako jsou uživatelské identifikátory a hesla,

- autorizační proces pro přístup uživatele a jeho oprávnění,

- požadavky na vedení a dostupnost seznamu jednotlivců, kteří jsou vzhledem ke svým předdefinovaným právům a privilegiím oprávněni využívat nabízené služby,

j) popis ověřitelných kritérií výkonnosti, způsob jejich sledování a hlášení,

k) ve smlouvě mají být stanoveny procedury pro monitorování činností uživatelů, administrátorů a bezpečnostních činností a událostí; mají být vymezeny odpovědnosti za zaznamenávání a ošetřování bezpečnostních incidentů,

l) právo auditovat dodržování smluvních povinností a právo nechat provést tyto audity třetí stranou,

m) popis eskalace problému v případech řešení havárie, pokud je to potřebné, měla by být zvážena pravidla pro řešení havarijních situací,

n) odpovědnost za instalaci a údržbu technického a programového vybavení,

o) jasná pravidla hlášení a schválený formát těchto hlášení,

p) jasný a specifikovaný proces řízení změn,

q) jakákoliv opatření fyzické ochrany a mechanizmy, které zajišťují jejich plnění,

r) školení externích uživatelů a správců v metodách, postupech a v bezpečnosti,

s) opatření k zajištění ochrany před škodlivým programovým vybavením,

t) systém zjišťování, hlášení, upozorňování a vyšetřování bezpečnostních incidentů a případů prolomení bezpečnosti,

u) podmínky spolupráce třetích stran se subdodavateli,

v) povinnost zachovávat mlčenlivost a důvěrnost o informacích, včetně osobních údajů.

3.1.11 Směrnice vyhodnocování indicidentů

Zaměstnanci a externí pracovníci jsou seznámeni s postupy hlášení před zahájením pracovní činnosti podle typu incidentů.

Typy incidentů:

1) porušení bezpečnosti,

2) možné hrozby,

3) slabiny,

4) bezpečnostní rizika.

Reakce na bezpečnostní incidenty musí být provedena v co nejkratší lhůtě.

Součástí postupů musí být nastavené postupy pro hlášení bezpečnostních událostí a incidentů, a to s ohledem na povahu událostí, která nastala.

3.1.12 Směrnice řízení kontinuity činností

Pro správné postupů pro řízení kontinuity činností, prostředky je nutné rozdělit dle jejich účelu a přiřadit jim dle jejich rizikovosti odpovídající dobu obnovy a také maximálně tolerovanou dobu odstávky.

Prostředek	**Rizikovost**
Servery	5
Internetové připojení	4
Tiskárny	1
EZS	2
Kamerový systém	2
Kancelářské počítače	4

Tabulka č. 17 - Typy prostředků a jejich klasifikace

Rizikovost je označena známkami od 1-5, kde 1 je nejméně riziková a 5 nejvíce.

3.1.12.1 Požadavky na obnovu funkčnosti

Doby obnovy se mohou operativně upravovat podle druhu vzniku krizové situace.

Prostředek	**Priorita**	**Doba obnovy pracovní dny**
Servery	1	2h
Internetové připojení	1	2h
Tiskárny administrativa	4	2d
EZS	5	24h
Kamerový systém	5	48h
Kancelářské počítače	2	2h

Tabulka č. 18 - Požadavky na obnovu funkčnosti

3.2 Identifikace prostředí a zdůvodnění

Požadavky Zákona č. 181/2014 Sb. se vztahují jenom na identifikované systémy v prostředí organizace. Dané systémy musí naplňovat požadavky daného zákona. S ohledem ale na to, že rizika jsou také ve vztahu k dalším systémům.

Identifikace prostředí je provedena s ohledem na činnost organizace. Univerzita je vždy orgánem veřejné moci, dle Zákona č. 111/1998 Sb. o vysokých školách

V tabulce níže jsou uvedeny systémy, které byly zařazeny do rozsahu této práce a identifikovány jako systém pro ZOKB. Je důležité zmínit, že se nejedná o jediné systémy univerzity. Kupříkladu univerzitní systém pro řízení studia nebyl předmětem této práce. S ohledem na jeho povahu, je možné předpokládat, že bude také identifikován jako významný systém.

Systém	[redacted]
Služba 6	

Tabulka č. 19 - Identifikované významné systémy

3.3 Návrh technických opatření

Technická opatření se věnují zejména síťové vrstvě, tato vrstva je totiž z pohledu kybernetické bezpečnosti nejvíce zásadní. Síťová opatření a návrhy na jejich realizaci jsou uvedeny v bodech níže:

3.3.1 VLAN

Jednotlivé systémy musí být odděleny do jednotlivých virtuálních sítí s omezenou komunikací do vnitřního perimetru sítě. Je také vhodné realizovat opatření zajišťující izolaci jednotlivých systémů mezi sebou. Tj. pokud například existuje skupina systémů na jednom frameworku, je vhodné je provozovat v jedné VLAN.

3.3.2 WAF – Web Application Firewall

Je více než vhodným řešením pro zajištění ochrany před hrozbami z vnějšího perimetru. V případě výběru vhodného řešení zajistí ochranu před jednotlivými útoky a proaktivně na ně reagovat, ještě než se nejlépe dostanou do perimetru organizace. Využití WAF je také vhodné jako ochrana proti DDOS útokům, kde jsou na trhu řešení, které dokáží tuto formu účinně odfiltrovat, ještě než se dostanou do prostředí společnosti.

3.3.3 XDR – Extended Detection and Response

Hrozby je nutné filtrovat na úrovni síťového prostředí, a to nejlépe přes nástroje, které zajistí na základě kolekce informací a behaviorální analýzu dat. Dané řešení musí být v nejlepší případě v proaktivním režimu, tj. řešit případné incidenty do úrovně eliminace potenciálního dopadu. Například přes izolaci dané stanice, či přes ošetření rizikových toků dat.

Nezbytnou částí je testování zranitelností síťového prostředí a aplikací. Bez znalosti zranitelnosti není možné aplikovat odpovídající opatření a také odpovídajícím způsobem zabezpečit prostředí. Tak aby bylo testování účinné, musí probíhat pravidelně a mít na definované kroky pro řešení zjištěných nedostatků.

Obecný proces při zjištění zranitelností zahrnuje následující kroky:

1. Identifikace zranitelnosti a provedení analýzy, jestli není identifikována mylně.
2. Identifikace opatření pro rychlou nápravu, zde je nezbytné zvažovat také možný. dopad identifikované zranitelnosti na prostředí a podle možného dopadu.
3. Identifikovat možné dopady aplikace nápravného opatření.

4. Provést odpovídající testování.
5. Nasazení nápravy řešení.
6. Provedení opětovného testu zranitelností.

Výše uvedený cyklus je nutné opakovat v pravidelných intervalech a také na základě monitoringu nových zranitelností mít možnost jej nasadit operativně. Pro tuto aplikaci je nutné mít provedenou analýzu o tom jaké řešení jsou v organizaci využívané a také jaké jsou jejich zranitelnosti a případně také kde jsou identifikovány zranitelnosti nultého dne.

ZÁVĚR

Samotný Zákon č. 181/2014 Sb. zahrnuje opatření, které mohou při správné implementaci vést ke snížení potenciálních dopadů kybernetických incidentů, či událostí. Pro zajištění efektivního vynaložení zdrojů a také pro implementaci adekvátních opatření je při jeho implementaci důležité každé opatření nasazovat korektně a také zvážit veškerá potenciální rizika. Bez této úvahy může dojít k neúplné implementaci opatření, či jejich zavedení pouze ve formální rovině.

V rámci této práce jsem se zaměřil na analýzu legislativních požadavků, společně s tím byly provedeny testy zranitelností vybraných aplikací a identifikace hrozeb, včetně definice nápravných opatření. Následně byla provedena srovnávací analýza pro posouzení shody s požadavky Zákona č. 181/2014 Sb., kde byla využita ISO 27001 norma. Následně byla navržena nápravná opatření, jak organizačního, tak technického charakteru.

Velmi častou chybou implementace opatření je jejich zavedení bez hlubšího kontextu. Zákon sice ukládá legislativní povinnost pro zavedení opatření, ale i bez něj je v době přesunu nejen organizovaného zločinu do kyberprostoru zcela zásadní implementovat odpovídající opatření pro mitigaci potenciálních dopadů.

Závěrem této práce bych také rád doplnil, že i když formální postupy působí jako „papírová“ bezpečnost, jejich význam je hlavně ve formě ukotvení postupů ve formě nutných pracovních, či smluvních povinností a tím také její lepší vynutitelnost. Důležitá je také minimalizace výjimek z definovaných opatření a tím zajištění jednotného prostředí.

SEZNAM POUŽITÉ LITERATURY

[1] ČESKO. Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti. In: Sbírka zákonů České republiky. 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

[2] ČESKO. Vyhláška č. 316/2014 Sb.: Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-316

[3] ČESKO. Vyhláška č. 317/2014 Sb.: Vyhláška o významných informačních systémech a jejich určujících kritériích. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-317

[4] GUPTA, Manish, Raj SHARMAN a John WALP. Information technology risk management and compliance in modern organizations. Hershey: Business Science Reference,

[5] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 147 s. ISBN 9788073807375.

[6] JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 9788074543128. Dostupné také z: http://hdl.handle.net/10563/25821

[2017], 1 online zdroj. ISBN 9781522526056. Dostupné také z: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1540761&authtype=ip,shib&custid=s3936755

[7] STALLINGS, William a Lawrie BROWN. Computer security: principles and practice. Fourth edition. Chennai: Pearson, [2020], 800 atrn. ISBN 978-93-534-3886-9.

[8] POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice. ISBN 8086898385.

[9] ČSN EN ISO/IEC 27000. Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2020.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ZOKB	Zákona č. 181/2018 Sb.
SW	Software
HW	Hardware
AC	Průměrná důvěrnost
AI	Průměrná integrita
AA	Průměrná dostupnost
TP	Hrozba
ISMS	Information Security Management System
CVSS	Common Vulnerability Scoring System
VKB	Vyhláška č. 316/2014 Sb.
SŘBI	Systém řízení bezpečnosti informací (nebo ISMS)
VPN	Virtual Private Network
RPO	Recovery Point Objective

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA PI: VÝBĚR OPATŘENÍ PRO IMPLEMENTACI

Skupina / cíl / opatření		Vyb.	Důvod nevybrání opatření	Zav.	Mitigace rizika
A.5	**Politiky bezpečnosti informací**				
A.5.1	**Směřování bezpečnosti informací vedením organizace**				
A.5.1.1	Politiky pro bezpečnost informací	ano		ano	
A.5.1.2	Přezkoumání politik pro bezpečnost informací	ano		ano	
A.6	**Organizace bezpečnosti informací**				
A.6.1	**Interní organizace**				
A.6.1.1	Role a odpovědnosti bezpečnosti informací	ano		ano	
A.6.1.2	Princip oddělení povinností	ano		ano	
A.6.1.3	Kontakt s příslušnými orgány a autoritami	ano		ano	
A.6.1.4	Kontakt se zájmovými skupinami	ano		ano	
A.6.1.5	Bezpečnost informací v řízení projektů	ano		ano	
A.6.2	**Mobilní zařízení a práce na dálku**				
A.6.2.1	Politika mobilních zařízení	ano		ano	
A.6.2.2	Práce na dálku	ano		ano	
A.7	**Bezpečnost lidských zdrojů**				
A.7.1	**Před vznikem pracovního vztahu**				
A.7.1.1	Prověřování	ano		ano	

Skupina / cíl / opatření		**Vyb.**	**Důvod nevybrání opatření**	**Zav.**	**Mitigace rizika**
A.7.1.2	Podmínky pracovního vztahu	ano		ano	
A.7.2	**Během pracovního vztahu**				
A.7.2.1	Odpovědnost vedení organizace	ano		ano	
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	ano		ano	
A.7.2.3	Disciplinární řízení	ano		ano	
A.7.3	**Ukončení a změna pracovního vztahu**				
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	ano		ano	
A.8	**Řízení aktiv**				
A.8.1	**Odpovědnost za aktiva**				
A.8.1.1	Seznam aktiv	ano		ano	
A.8.1.2	Vlastnictví aktiv	ano		ano	
A.8.1.3	Přípustné použití aktiv	ano		ano	
A.8.1.4	Navrácení aktiv	ano		ano	
A.8.2	**Klasifikace informací**				
A.8.2.1	Klasifikace informací	ano		ano	
A.8.2.2	Označování informací	ano		ano	
A.8.2.3	Manipulace s aktivy	ano		ano	
A.8.3	**Manipulace s médii**				
A.8.3.1	Správa výměnných médií	ano		ano	
A.8.3.2	Likvidace médií	ano		ano	
A.8.3.3	Přeprava fyzických médií	ano		ano	

Skupina / cíl / opatření		Vyb.	Důvod nevybrání opatření	Zav.	Mitigace rizika
A.9	**Řízení přístupu**				
A.9.1	**Požadavky organizace na řízení přístupu**				
A.9.1.1	Politika řízení přístupu	ano		ano	
A.9.1.2	Přístup k sítím a síťovým službám	ano		ano	
A.9.2	**Řízení přístupu uživatelů**				
A.9.2.1	Registrace a zrušení registrace uživatele	ano		ano	
A.9.2.2	Správa uživatelských přístupů	ano		ano	
A.9.2.3	Správa privilegovaných přístupových práv	ano		ano	
A.9.2.4	Správa tajných autentizačních informací uživatelů	ano		ano	
A.9.2.5	Přezkoumání přístupových práv uživatelů	ano		ano	
A.9.2.6	Odebrání nebo úprava přístupových práv	ano		ano	
A.9.3	**Odpovědnost uživatelů**				
A.9.3.1	Používání tajných autentizačních informací	ano		ano	
A.9.4	**Řízení přístupu k systémům a aplikacím**				
A.9.4.1	Omezení přístupu k informacím	ano		ano	
A.9.4.2	Bezpečné postupy přihlášení	ano		ano	
A.9.4.3	Systém správy hesel	ano		ano	

Skupina / cíl / opatření		**Vyb.**	**Důvod nevybrání opatření**	**Zav.**	**Mitigace rizika**
A.9.4.4	Použití privilegovaných programových nástrojů	ano		ano	
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	ano		ano	
A.10	**Kryptografie**				
A.10.1	**Kryptografická opatření**				
A.10.1.1	Politika pro použití kryptografických opatření	ano		ano	
A.10.1.2	Správa klíčů	ano		ano	
A.11	**Fyzická bezpečnost a bezpečnost prostředí**				
A.11.1	**Bezpečné oblasti**				
A.11.1.1	Fyzický bezpečnostní perimetr	ano		ano	
A.11.1.2	Fyzické kontroly vstupu	ano		ano	
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	ano		ano	
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	ano		ano	
A.11.1.5	Práce v bezpečných oblastech	ano		ano	
A.11.1.6	Oblasti pro nakládku a vykládku	ano		ano	
A.11.2	**Zařízení**				
A.11.2.1	Umístění zařízení a jeho ochrana	ano		ano	
A.11.2.2	Podpůrné služby	ano		ano	

Skupina / cíl / opatření		**Vyb.**	**Důvod nevybrání opatření**	**Zav.**	**Mitigace rizika**
A.11.2.3	Bezpečnost kabelových rozvodů	ano		ano	
A.11.2.4	Údržba zařízení	ano		ano	
A.11.2.5	Přemístění aktiv	ano		ano	
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	ano		ano	
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	ano		ano	
A.11.2.8	Uživatelská zařízení bez obsluhy	ano		ano	
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	ano		ano	
A.12	**Bezpečnost provozu**				
A.12.1	**Provozní postupy a odpovědnosti**				
A.12.1.1	Dokumentované provozní postupy	ano		ano	
A.12.1.2	Řízení změn	ano		ano	
A.12.1.3	Řízení kapacit	ano		ano	
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	ano		ano	
A.12.2	**Ochrana proti malwaru**				
A.12.2.1	Opatření proti malwaru	ano		ano	
A.12.3	**Zálohování**				
A.12.3.1	Zálohování informací	ano		ano	
A.12.4	**Zaznamenávání formou logů a monitorování**				

Skupina / cíl / opatření		**Vyb.**	**Důvod nevybrání opatření**	**Zav.**	**Mitigace rizika**
A.12.4.1	Zaznamenávání událostí formou logů	ano		ano	
A.12.4.2	Ochrana logů	ano		ano	
A.12.4.3	Logy o činnosti administrátorů a operátorů	ano		ano	
A.12.4.4	Synchronizace hodin	ano		ano	
A.12.5	**Správa provozního softwaru**				
A.12.5.1	Instalace softwaru na provozní systémy	ano		ano	
A.12.6	**Řízení technických zranitelností**				
A.12.6.1	Řízení technických zranitelností	ano		ano	
A.12.6.2	Omezení instalace softwaru	ano		ano	
A.12.7	**Hlediska auditu informačních systémů**				
A.12.7.1	Opatření k auditu informačních systémů	ano		ano	
A.13	**Bezpečnost komunikací**				
A.13.1	**Správa bezpečnosti sítě**				
A.13.1.1	Opatření v sítích	ano		ano	
A.13.1.2	Bezpečnost síťových služeb	ano		ano	
A.13.1.3	Princip oddělení v sítích	ano		ano	
A.13.2	**Přenos informací**				
A.13.2.1	Politiky a postupy při přenosu informací	ano		ano	

Skupina / cíl / opatření		**Vyb.**	**Důvod nevybrání opatření**	**Zav.**	**Mitigace rizika**
A.13.2.2	Dohody o přenosu informací	ano		ano	
A.13.2.3	Elektronické předávání zpráv	ano		ano	
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	ano		ano	
A.14	**Akvizice, vývoj a údržba systémů**				
A.14.1	**Bezpečnostní požadavky informačních systémů**				
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	ano		ano	
A.14.1.2	Zabezpečení aplikačních služeb na veřejných sítích	ano		ano	
A.14.1.3	Ochrana transakcí aplikačních služeb	ano		ano	
A.14.2	**Bezpečnost v procesech vývoje a podpory**				
A.14.2.1	Politika bezpečného vývoje	ano		ano	
A.14.2.2	Postupy řízení změn systémů	ano		ano	
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	ano		ano	
A.14.2.4	Omezení změn softwarových balíků	ano		ano	
A.14.2.5	Principy budování bezpečných systémů	ano		ano	
A.14.2.6	Prostředí bezpečného vývoje	ano		ano	
A.14.2.7	Outsourcovaný vývoj	ano		ano	
A.14.2.8	Testování bezpečnosti systémů	ano		ano	

Skupina / cíl / opatření		**Vyb.**	**Důvod nevybrání opatření**	**Zav.**	**Mitigace rizika**
A.14.2.9	Testování akceptace systémů	ano		ano	
A.14.3	**Data pro testování**				
A.14.3.1	Ochrana dat pro testování	ano		ano	
A.15	**Dodavatelské vztahy**				
A.15.1	**Bezpečnost informací v dodavatelských vztazích**				
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	ano		ne	
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	ano		ano	
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	ano		ano	
A.15.2	**Řízení dodávek služeb dodavatelů**				
A.15.2.1	Monitorování a přezkoumání služeb dodavatelů	ano		ano	
A.15.2.2	Řízení změn ve službách dodavatelů	ano		ano	
A.16	**Řízení incidentů bezpečnosti informací**				
A.16.1	**Řízení incidentů bezpečnosti informací a zlepšování**				
A.16.1.1	Odpovědnosti a postupy	ano		ano	
A.16.1.2	Hlášení událostí bezpečnosti informací	ano		ano	
A.16.1.3	Hlášení slabých míst bezpečnosti informací	ano		ano	

Skupina / cíl / opatření		**Vyb.**	**Důvod nevybrání opatření**	**Zav.**	**Mitigace rizika**
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	ano		ano	
A.16.1.5	Reakce na incidenty bezpečnosti informací	ano		ano	
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	ano		ano	
A.16.1.7	Shromažďování důkazů	ano		ano	
A.17	**Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací**				
A.17.1	**Kontinuita bezpečnosti informací**				
A.17.1.1	Plánování kontinuity bezpečnosti informací	ano		ano	
A.17.1.2	Implementace kontinuity bezpečnosti informací	ano		ano	
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	ano		ano	
A.17.2	**Redundance**				
A.17.2.1	Zajistit dostupnost vybavení pro zpracování informací	ano		ano	
A.18	**Soulad s požadavky**				
A.18.1	**Soulad s právními a smluvními požadavky**				
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	ano		ano	
A.18.1.2	Ochrana duševního vlastnictví	ano		ano	

Skupina / cíl / opatření		**Vyb.**	**Důvod nevybrání opatření**	**Zav.**	**Mitigace rizika**
A.18.1.3	Ochrana záznamů	ano		ano	
A.18.1.4	Soukromí a ochrana osobních údajů	ano		ano	
A.18.1.5	Regulace kryptografických opatření	ano		ano	
A.18.2	**Přezkoumání bezpečnosti informací**				
A.18.2.1	Nezávislé přezkoumání bezpečnosti informací	ano		ano	
A.18.2.2	Shoda s bezpečnostními politikami a normami	ano		ano	
A.18.2.3	Přezkoumání technické shody	ano		ano	

PŘÍLOHA PII: MAPOVÁNÍ SYSTÉMŮ

Název v práci	Systém	Role	URL
Služba 1	[redacted]		
Služba 2			
Služba 3			
Služba 4			
Služba 5			
Služba 6			
Služba 7			
Služba 8			
Služba 9			
Služba 10			
Služba 11			
Služba 12			
Služba 13			
Služba 14			
Služba 15			
Služba 16			
Služba 17			
Služba 18			
Služba 19			
Služba 20			

Služba 21	[redacted]
Služba 22	
Služba 23	
Služba 24	
Služba 25	
Služba 26	
Služba 27	
Služba 28	