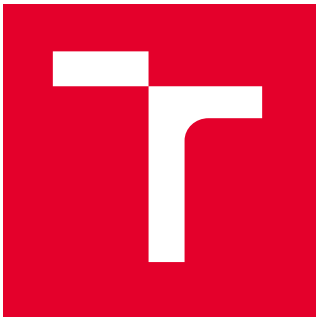


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

APLIKACE PRO ZOBRAZENÍ ANALÝZY RIZIK

APPLICATIONS FOR DISPLAYING RISK ANALYSIS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Anna Voskárová**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Zdeněk Martinásek, Ph.D.**
SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Bc. Anna Voskárová ***ID:*** 211326

Ročník: 2 ***Akademický rok:*** 2022/23

NÁZEV TÉMATU:

Aplikace pro zobrazení analýzy rizik

POKYNY PRO VYPRACOVÁNÍ:

Hlavním cílem práce je návrh a implementace nástroje, který organizaci umožní v rámci vlastního systému řízení informační bezpečnosti (ISMS) provádět analýzu rizik a využívat její výsledky pro návrh nápravných opatření. V teoretické části práce prostudujte současný stav problematiky (ISO27XXX, Kybernetický zákon a doporučení NÚKIB). Na základě výsledků navrhněte komplexní metodiku analýzy rizik, která bude v souladu s obecně používanými standardy pro řízení informační bezpečnosti. Metodika bude zahrnovat postupy a podklady pro: identifikaci a ohodnocení aktiv, katalog zranitelností s ohodnocením (míra zranitelnosti), katalog hrozeb s jejich ohodnocením (pravděpodobnost hrozby a dopad hrozby), určení vzájemných vazeb mezi aktivy, hrozbami a zranitelnostmi, výpočet rizik pro aktuální stav organizace, návrh opatření pro další zvládání rizik v souladu s definovanými pravidly pro akceptaci rizik (plán zvládání rizik), evidenci rizik a jejich atributů, včetně sledování trendů rizik. V praktické části navrhněte a implementujte program umožňující prezentaci výsledků analýzy rizik dle Vámi navržené metodologie (formou dashboardu). Poslední části praktického výstupu bude implementace kontrolního seznamu vlastní metodologie do platformy Penterep včetně využití vhodné komponenty na zobrazení výsledků. V rámci semestrálního projektu realizujte vlastní návrh metodologie analýzy rizik a implementujte jednoduchý nástroj pro zobrazení výsledků formou dashboardu.

DOPORUČENÁ LITERATURA:

[1] DISTERER, Georg. ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 2013, 4.2.

[2] COHRSSEN, John J.; COVELLO, Vincent T. Risk analysis: a guide to principles and methods for analyzing health and environmental risks. DIANE Publishing, 1999.

Termín zadání: 6.2.2023 ***Termín odevzdání:*** 19.5.2023

Vedoucí práce: doc. Ing. Zdeněk Martinásek, Ph.D.

Konzultant: Josef Novotný

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Diplomová práca sa zameriava na problematiku posúdenia rizík bezpečnosti informácií. Práca sa v teoretickej časti venuje popisu problematiky informačnej bezpečnosti, existujúcich štandardov v tejto oblasti a tiež právnej úprave kybernetickej bezpečnosti platnej a účinnej na území Českej republiky. V rámci praktickej časti je najprv predstavená vlastná metodika pre vykonanie analýzy rizík bezpečnosti informácií, ktorá bola následne prakticky aplikovaná za účelom realizácie posúdenia rizík informačnej bezpečnosti vo firme pôsobiacej najmä v oblasti informačných a komunikačných technológií, ktorej činnosťami sú vývoj, výroba, inštalácia a servis priemyslových riadiacich a informačných systémov. Pre potreby prezentácie výsledkov zistených vykonanou analýzou bol realizovaný návrh a následná implementácia webovej aplikácie, ktorá slúži ako praktický nástroj umožňujúci prehľadným a názorným spôsobom zobraziť a prezentovať výstupy analýzy rizík. Poslednou súčasťou praktickej časti tejto práce je vytvorenie kontrolného zoznamu vhodného pre vykonanie auditu kybernetickej bezpečnosti a jeho implementácia v podobe nasadenia vlastného modulu do existujúcej platformy Penterep, ktorý vytvára ideálny nástroj umožňujúci posúdiť mieru plnenia jednotlivých bezpečnostných opatrení v rámci kybernetickej bezpečnosti.

KĽÚČOVÉ SLOVÁ

informačná a kybernetická bezpečnosť, systém riadenia bezpečnosti informácií, analýza rizík bezpečnosti informácií, webová aplikácia, bezpečnostný audit

ABSTRACT

The diploma thesis deals with the information security risk assessment. The theoretical part of the thesis is devoted to the description of information security basics, existing standards in the area of information security, and also the current cybersecurity legislation applicable in Czech Republic. In the practical part, an own information security risk analysis methodology is first presented, which was then practically applied for the purpose of assessing information security risks in a company operating in the field of information and communication technologies, whose main activities are the development, production, installation and service of industrial controllers and information systems. Furthermore, for presentation of the results of the performed analysis, the design and implementation of web application takes place, which can be used as a useful tool that allows displaying and presenting the outputs of the risk analysis in a clear and illustrative way. The last part of this thesis includes the creation of a checklist for performing a cybersecurity audit and its subsequent implementation as a custom module into the existing Penterep platform, which creates an ideal tool for the needs of assessing the degree of fulfillment of individual security measures within the area of cybersecurity.

KEYWORDS

information security and cybersecurity, information security management system, information security risk analysis, web application, security audit

Vysadené pomocou balíčku `thesis` verzie 4.07; `http://latex.feec.vutbr.cz`

VOSKÁROVÁ, Anna. *Aplikace pro zobrazení analýzy rizik*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2023, 119 s. Diplomová práca. Vedúci práce: doc. Ing. Zdeněk Martinásek, PhD.

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora:	Bc. Anna Voskárová
VUT ID autora:	211326
Typ práce:	Diplomová práca
Akademický rok:	2022/23
Téma závěrečnej práce:	Aplikace pro zobrazení analýzy rizik

Vyhlasujem, že svoju záverečnú prácu som vypracovala samostatne pod vedením vedúcej/cého záverečnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autorka uvedenej záverečnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto záverečnej práce som neporušila autorské práva tretích osôb, najmä som nezasiahla nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomá následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autorky*

*Autor podpisuje iba v tlačenej verzii.

POĎAKOVANIE

Rada by som vyjadrila svoje poďakovanie vedúcemu tejto diplomovej práce pánovi doc. Ing. Zdeňkovi Martináskovi, Ph.D. za odbornú pomoc a usmernenie pri písaní mojej práce, za cenné rady a poznatky, užitočné pripomienky, inšpiratívne nápady a predovšetkým za čas, ktorý mi pri príprave tejto práce venoval. Ďalej by som sa chcela poďakovať odbornému konzultantovi tejto záverečnej práce a tiež ďalším pracovníkom Spoločnosti za ich pomoc, usmernenie a odborné vedenie, vďaka čomu som mohla viac preniknúť do problematiky zadanej záverečnej práce, a všetky znalosti nadobudnuté pod odborným vedením prakticky aplikovať. A v neposlednom rade by som sa chcela poďakovať svojej mamine za veľkú podporu v priebehu celého môjho štúdia.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

V dnešnej modernej dobe, kedy informačné a komunikačné technológie zažívajú čoraz väčší a väčší rozmach, sa stáva kvalitné zabezpečenie dát a kľúčových aktív pre organizácie s akýmkoľvek zameraním absolútnou nutnosťou. Aby bolo možné všetkým dátam a informáciám poskytnúť dostatočnú úroveň zabezpečenia, je žiadúce v prvom rade identifikovať, pred akými nežiadúcimi hrozbami je potrebné tieto dáta a informácie zabezpečiť. Organizácie za týmto účelom implementujú systém riadenia bezpečnosti informácií[1], v rámci ktorého realizujú proces riadenia rizík. Práve ten im umožní včas identifikovať všetky hrozby a nežiadúce riziká, ktoré tieto hrozby môžu generovať, následne na zistené riziká reagovať, a tým zvýšiť úroveň zabezpečenia aktív a prevádzkovaných činností.

Teoretická časť tejto práce je v úvode venovaná problematike informačnej bezpečnosti vo všeobecnosti, následne prináša pohľad na rodinu noriem ISO/IEC 27xxx, pričom sa bližšie zameriava na najdôležitejší spomedzi týchto štandardov – konkrétne na normu ISO/IEC 27001, ktorá predstavuje základný rámec celého ISMS.

V súvislosti s diskutovaním problematiky informačnej bezpečnosti nemôže byť opomenutá ani oblasť kybernetickej bezpečnosti. Ďalšia kapitola tejto práce je preto venovaná predstaveniu základných právnych predpisov, ktoré na národnej úrovni upravujú práve problematiku kybernetickej bezpečnosti. Jedná sa o zákon o kybernetickej bezpečnosti[2] a jeho prevádzaciu vyhlášku[3].

Hlavnou časťou tejto práce je návrh vlastnej metodiky pre vykonanie analýzy rizík, ktorej cieľom je priniesť možnosť identifikácie a ohodnotenia možných nežiadúcich rizík s následným prínosom v podobe zvládania, resp. ošetrenia týchto rizík. Vlastná metodika je vytváraná za účelom vykonania podrobnej analýzy rizík bezpečnosti informácií v spolupráci s firmou[4], kde má autorka tejto práce pracovne-právny vzťah. Jedná sa o firmu pôsobiacu v oblasti informačných a komunikačných technológií, ktorej hlavnými činnosťami sú vývoj, výroba, inštalácia a servis priemyslových riadiacich a informačných systémov. Metodika je navrhovaná „na mieru“, s prihliadnutím na špecifický kontext činností Spoločnosti.

Praktický výstup práce spočíva v implementácii nástroja v podobe jednoduchej webovej aplikácie, ktorá umožní prehľadným spôsobom zobraziť výsledky analýzy

[1] Skrátene ISMS, z angl. *Information Security Management System*.

[2] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů, ďalej len „ZoKB“.

[3] Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ďalej len „VoKB“.

[4] Pre účely tejto práce sú všetky súvislosti spojené s danou firmou anonymizované, skutočný názov firmy je v textovej časti práce nahradený názvom „Spoločnosť“.

rizík realizovanej v súlade s metodikou pre analýzu rizík, ktorej návrh taktiež spadá pod vlastný prínos praktickej časti tejto práce. Tento nástroj môže byť analytikmi informačnej a kybernetickej bezpečnosti využitý pre prezentáciu získaných výsledkov vykonanej analýzy rizík za účelom predloženia a názorného vysvetlenia skutočností zistených analýzou vedeniu Spoločnosti. Tento vytvorený nástroj bude umožňovať prehľadné zobrazenie identifikovaných rizík spoločne s ich ohodnotením a taktiež identifikáciou nápravných opatrení zavedených za účelom minimalizácie pravdepodobnosti vzniku a/alebo miery dopadu týchto identifikovaných rizík.

Poslednou súčasťou praktickej časti bude vlastný návrh a následná implementácia kompletného kontrolného zoznamu zostaveného na základe ustanovení vyhlášky o kybernetickej bezpečnosti, ktorý možno využiť pri vykonávaní auditu kybernetickej bezpečnosti pre potreby overenia miery plnenia požiadaviek na oblasť kybernetickej bezpečnosti. Vytvorený kontrolný zoznam bude za účelom jeho praktického využitia nasadený do prostredia platformy Penterep.

1 Teória informačnej bezpečnosti

1.1 Základné pojmy a definície

Úvodná kapitola tejto práce prináša výklad základných pojmov, ktorých vysvetlenie a pochopenie je pre riešenie problematiky informačnej a kybernetickej bezpečnosti nevyhnutné. Uvedené pojmy sú v súlade s terminológiou použitou v medzinárodných normách rodiny 27xxx a taktiež s terminológiou použitou v ZoKB [1] a VoKB [2].

Informačná bezpečnosť

Definícií pojmu „informačná bezpečnosť“ existuje niekoľko. Vo všeobecnosti možno samotnú bezpečnosť definovať ako schopnosť určitého systému alebo jeho častí odolávať vonkajším aj vnútorným hrozbám, ktoré na tento systém môžu nepriaznivo pôsobiť, tak, aby mohla byť zachovaná štruktúra tohto systému, jeho stabilita, spoľahlivosť a prejavy [3]. Pokiaľ hovoríme konkrétne o bezpečnosti informácií, jedná sa o schopnosť systému zachovať si požadovanú úroveň atribútov bezpečnostnej triády, medzi ktoré radíme vlastnosti ako dôvernosť, integritu a dostupnosť tohto systému [4].

Informačná bezpečnosť zahŕňa ochranu informácií počas celého ich životného cyklu. V súčasnej dobe je spájaná predovšetkým s informáciami komunikovanými prostredníctvom informačných technológií. Informačnú bezpečnosť je teda možné charakterizovať ako praktický odbor, ktorý vznikol predovšetkým za účelom ochrany informácií. Primárnym cieľom informačnej bezpečnosti je poskytnúť informáciám patričnú ochranu pred narušením ich dôvernosti, integrity a/alebo dostupnosti [5].

Aktívum

Pod pojmom aktívum si možno predstaviť čokoľvek, čo má pre konkrétneho vlastníka daného aktíva určitú hodnotu. Môže sa jednať o hmotné či nehmotné objekty, ako sú napríklad informácie, dáta, software, hardwarové vybavenie, technológie, budovy a priestory. Aktívom môže byť pre organizáciu aj vlastnosť, ako príklad možno uviesť dostupnosť dát či funkčnosť prevádzkovaného systému. Za aktívum možno označiť taktiež know-how, dobré meno organizácie, jej zamestnancov, konkrétne ich znalosti a skúsenosti apod.

Hrozba

Hrozbou môže byť akákoľvek vlastnosť, sila, udalosť, aktivita alebo osoba, ktorá pôsobí buď priamo na aktívum alebo na bezpečnostné opatrenie nasadené za účelom ochrany daného aktíva s cieľom získať prístup k aktívu a nežiadúcim spôsobom

toto aktívum ovplyvniť. Hrozbou teda rozumieme akékoľvek nežiadúce pôsobenie na aktívum, ktoré zapríčiní poškodenie, zneužitie alebo nedostupnosť aktíva.

Základnou charakteristikou hrozby je jej úroveň, ktorá je hodnotená v závislosti na troch základných faktoroch, ktorými sú nebezpečnosť, prístup a motivácia danej hrozby. S prihliadnutím k uvedeným dielčím charakteristikám možno tieto hrozby kategorizovať, a to konkrétne v závislosti na zdroji, ktorý danú hrozbu môže vyvolať, na hrozby vonkajšie a vnútorné, a ďalej v závislosti na motivácii zdroja danú hrozbu realizovať na hrozby náhodné a úmyselné.

Zraniteľnosť

Zraniteľnosť predstavuje slabé miesto aktíva alebo bezpečnostného opatrenia nasadeného za účelom ochrany tohto aktíva, ktoré môže hrozba zneužiť k uplatneniu svojho nežiadúceho vplyvu.

Bezpečnostné opatrenie

Bezpečnostným opatrením môže byť prakticky čokoľvek, čo prispieva k zníženiu pravdepodobnosti a/alebo dopadu určitého rizika. Cieľom bezpečnostného opatrenia je poskytovať ochranu aktívu, resp. eliminovať jeho zraniteľnosti, aby nemohli byť hrozbou zneužité, a/alebo znižovať negatívne dopady v prípade, že hrozba určitú zraniteľnosť nepriaznivým spôsobom zneužije.

Riziko

Vo všeobecnom poňatí si pod pojmom riziko možno predstaviť akékoľvek vystavenie nepriaznivým okolnostiam, ktoré bude mať za následok odchýlenie od očakávaného priebehu činností. Jedná sa o určitý odhad pravdepodobnosti výskytu nebezpečenstva alebo udalosti, ktorá vyvolá nežiadúce následky.

Popis významu slova riziko poskytuje tiež norma ISO/IEC 27005, ktorá riziko definuje ako „*účinok neistoty na dosiahnutie cieľov*“ [6]. Vznik rizika je teda spojený s istou mierou neistoty, pri ktorej nie je možné jasne predpovedať, kedy a či vôbec riziková udalosť nastane. Takáto udalosť nastáva len s určitou pravdepodobnosťou a spôsobuje odchýlenie sa od očakávaného výsledku, vývoja či stavu. Ak sa riziko vo forme určitej neistoty vyskytne, môže mať pozitívny a/alebo negatívny dopad na dosiahnutie jedného či viacerých vytýčených cieľov.

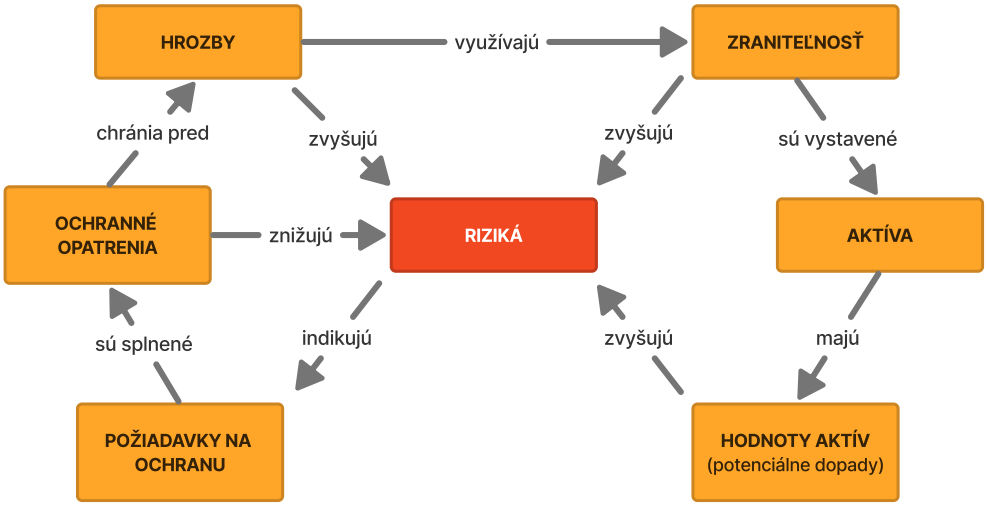
Pojem rizika je vymedzený aj v samotnej VoKB, a to konkrétne ako *„možnosť, že určitá hrozba využije zraniteľnosť aktíva a spôsobí tým škodu“*[1]. Z tejto definície je zrejmé, že nie každá hrozba musí zákonite predstavovať riziko. Je tomu tak len

[1] Viď § 2 písm. h) VoKB.

v prípade, že existuje určitá zraniteľnosť na sledovanom aktíve, ktorú môže táto hrozba využiť k uplatneniu svojho nežiadúceho vplyvu.

Nakoľko výskyt rizika nie je možné vopred jednoznačne predpokladať, je teda zrejmé, že miera rizika, ktorá popisuje celkový dopad jeho nepriaznivého pôsobenia, bude určená tým, či vôbec môže nastať taká udalosť, ktorá by spôsobila odklon od očakávaného priebehu činnosti, a taktiež tým, čo by táto udalosť, v prípade jej realizácie, spôsobila. Na základe tejto úvahy je možné odvodiť tiež vyjadrenie rizika z matematického hľadiska, kedy riziko chápeme ako súčin dvoch parametrov, a to pravdepodobnosti výskytu nežiadúceho javu, resp. pravdepodobnosť toho, že konkrétna hrozba zneužije niektorú zo zraniteľností daného aktíva, a dopadu, ktorý realizácia tejto hrozby vyvolá.

Vzájomné vzťahy medzi vyššie uvedenými a popísanými pojmami sú schematicky znázornené na obr. 1.1



Obr. 1.1: Vzťahy medzi základnými pojmami informačnej bezpečnosti [7].

Bezpečnostná triáda CIA

Pojem „bezpečnostná triáda“ pokrýva celkom tri atribúty bezpečnosti informácií, a to konkrétne dôvernosť (C – z angl. *confidentiality*), integritu (I – z angl. *integrity*) a dostupnosť (A – z angl. *availability*). Zachovanie **dôvernosti** informácií spočíva v tom, že tieto informácie by mali byť prístupné len tým entitám, ktoré sú oprávnené poznať ich obsah, a preto je potrebné zabrániť prístupu neautorizovaným entitám. Pre zachovanie **integrity** je nutné, aby nedochádzalo k neautorizovanej modifikácii systému a informácií. A nakoniec, aby mohla byť zachovaná **dostupnosť**, musia byť informácie, služby a systémy chránené pred nežiadúcimi prejavmi, ktoré by mohli ich dostupnosť narušiť. [8]

1.2 Štandardy informačnej bezpečnosti

Zaistenie dostatočnej úrovne bezpečnosti informácií je v dnešnej modernej dobe, kedy informačné a komunikačné prostriedky a s nimi súvisiace technológie zažívajú čoraz väčší a intenzívnejší rozvoj, nepochybne veľmi potrebné a žiadúce. Informačná bezpečnosť predstavuje disciplínu, ktorá napomáha riešiť existujúce problémy súvisiace s bezpečnosťou činností, ktoré sú denno-denne realizované práve prostredníctvom informačných a komunikačných technológií. Či už sa jedná o prenos dát medzi užívateľmi naprieč celým svetom alebo len o spracovanie údajov, ktorého rozsah má prevažne lokálny charakter, či akúkoľvek inú činnosť spojenú s využitím komunikačných prostriedkov, bezpečnosť dát a informácií by mala byť v dostatočnej miere zaistená pri vykonávaní obdobných činností za každých okolností.

Aby bolo pre jednotlivcov (užívateľov) či celé organizácie možné adekvátnym spôsobom zaistiť bezpečnosť informácii, je potrebné stanoviť určitý rámec, ktorý bude predstavovať akýsi návod, ktorý napomôže správne implementovať a následne udržiavať bezpečnosť informácií na požadovanej úrovni a v požadovanom rozsahu. Za týmto účelom vznikli a stále ešte vznikajú mnohé štandardy a doporučenia pre riadenie bezpečnosti informácií. To, ktoré riešenie je ideálne a ktoré najvhodnejším spôsobom pokryje všetky potreby konkrétnej organizácie, vždy závisí na špecifickom kontexte determinujúcom mnohé faktory, ktoré konečnú voľbu ovplyvňujú.

V tejto práci bude bližšie popísaný prístup riadenia bezpečnosti informácií podľa medzinárodných noriem rodiny ISO/IEC 27xxx, ktorý je pre potreby tejto diplomovej práce kľúčový, no za zmienku určite stoja i mnohé iné, celosvetovo využívané štandardy, ako napr. COBIT[2] či framework ITIL[3].

1.2.1 Rodina medzinárodných noriem ISO/IEC 27xxx

Ako už odznelo v úvode tejto kapitoly, informácie predstavujú pre organizácie najdôležitejšiu skupinu aktív, a preto je potrebné všetky informácie (resp. informačné aktíva) chrániť pred nežiadúcim pôsobením rozličných hrozieb. Za účelom ochrany informácií vzniká v súčasnej dobe veľké množstvo štandardov, ktoré definujú požiadavky na implementáciu a prevádzku činností a procesov s cieľom zaistiť dostatočnú úroveň bezpečnosti informačných systémov a sietí a v nich prevádzkovaných aktív.

Jednou veľkou skupinou týchto štandardov je rodina noriem ISO/IEC 27xxx[4], ktorá predstavuje sadu medzinárodných noriem definujúcich tzv. Systém riadenia bezpečnosti informácií, skrátene ISMS[5]. Ich tvorcom je Medzinárodná organizácia

[2] Z angl. *Control Objectives for Information and Related Technology.*

[3] Z angl. *Information Technology Infrastructure Library.*

[4] Táto rodina noriem je tiež známa pod označením ISO/IEC 27000 alebo ISO-27K.

[5] Z angl. *Information Security Management System.*

pre normalizáciu (*International Organization for Standardization*), ktorá v roku 2005 vydala prvú z celej tejto rodiny noriem, a to konkrétne normu ISO/IEC 27001. Táto norma predstavuje základný rámec ISMS a pomocou nej sa tiež celý systém ISMS pre jednotlivé organizácie certifikuje.

Hlavným cieľom a prínosom ISMS je poskytnúť organizáciám všeobecný návod, akým spôsobom môžu svoje informácie vhodným spôsobom chrániť. Z tohto pohľadu sú najdôležitejšími dva štandardy, a to okrem spomínanej normy ISO/IEC 27001, ktorá definuje požiadavky na riadenie bezpečnosti informácií a slúži k udeľovaniu certifikácií pre organizácie, ktoré sa rozhodnú ISMS realizovať, tiež norma ISO/IEC 27002, ktorá poskytuje „návod“ popisujúci to, akým spôsobom môžu organizácie jednotlivé opatrenia normy ISO/IEC 27001 vhodne implementovať.

Predstavená rodina noriem obsahuje v súčasnosti celkom viac než 50 štandardov. Tabuľka 1.1 uvádza prehľad vybraných noriem z tejto rodiny, ktoré sú pre účely tejto práce relevantné, spoločne s ich stručným popisom [9].

Tab. 1.1: Prehľad noriem rodiny ISO/IEC 27xxx.

Terminológia	
ISO/IEC 27000	**Informačné technológie – Bezpečnostné metódy – Systémy riadenia bezpečnosti informácií – Prehľad a slovník:** Terminologický slovník obsahujúci základné pojmy a definície používané v štandardoch rodiny 27000.
Všeobecné požiadavky	
ISO/IEC 27001	**Informačné technológie – Bezpečnostné metódy – Systémy riadenia bezpečnosti informácií – Požiadavky:** Hlavná norma systému riadenia bezpečnosti informácií (ISMS), ktorá špecifikuje požiadavky na vytvorenie, implementáciu, udržiavanie a zlepšovanie ISMS v kontexte organizácie. Predstavuje návod pre organizácie, ako postupovať pri implementácií bezpečnostnej politiky.
ISO/IEC 27006	**Informačné technológie – Bezpečnostné metódy – Systémy riadenia bezpečnosti informácií – Požiadavky na orgány poskytujúce audit a certifikáciu systémov riadenia bezpečnosti informácií:** Špecifikuje požiadavky a poskytuje návod pre organizácie poskytujúce audit a certifikácie ISMS. Štandard je primárne zameraný na podporu akreditácie organizácií poskytujúcich certifikáciu ISMS.

ISO/IEC 27009	**Informačné technológie – Bezpečnostné metódy – Aplikácia normy ISO/IEC 27001 špecifická pre daný sektor – Požiadavky:** Definuje požiadavky na používanie normy ISO/IEC 27001 v každom špecifickom sektore. Vysvetľuje, ako zahrnúť dodatočné požiadavky k požiadavkám v ISO/IEC 27001, ako zdokonaliť niektorú z požiadaviek a ako zahrnúť opatrenia alebo súbory opatrení navyše k ISO/IEC 27001. Táto medzinárodná norma zabezpečuje, že dodatočné alebo vylepšené požiadavky nie sú v rozpore s požiadavkami normy ISO/IEC 27001.
ISO/IEC 270021	**Techniky – Požiadavky na spôsobilosť odborníkov na systémy manažérstva bezpečnosti informácií:** Uvádza spôsobilosti požadované alebo očakávané od odborníkov, ktorí riadia ISMS v súlade s normami ISO/IEC 27001, 27002, 27005 a 27007. Norma nešpecifikuje systém osobnej certifikácie alebo kvalifikácie ako taký, ale v skutočnosti slúži ako referencia pre orgány, ktoré takéto systémy prevádzkujú.
Všeobecné postupy	
ISO/IEC 27002	**Informačné technológie – Bezpečnostné metódy – Kontroly bezpečnosti informácií:** Táto norma definuje ciele, resp. požadované kontrolné opatrenie pre ochranu informačných aktív proti narušeniu ich dôvernosti, dostupnosti a integrity. Poskytuje návodné praktiky a postupy pre riadenie informačnej bezpečnosti vrátane výberu, implementácie a riadenia opatrení berúc do úvahy rizikové prostredia informačnej bezpečnosti organizácie. Norma môže byť tiež využitá certifikačnými autoritami, ktoré podľa nej postupujú pri udeľovaní certifikácie.
ISO/IEC 27003	**Informačné technológie – Bezpečnostné metódy – Systémy riadenia bezpečnosti informácií – Pokyny:** Táto norma sa zameriava na kritické aspekty úspešného návrhu a implementácie ISMS v súlade s ISO/IEC 27001. Popisuje proces špecifikácie a návrhu ISMS od počiatku až po vytvorenie plánu implementácie

ISO/IEC 27004	**Informačné technológie – Bezpečnostné metódy – Systémy riadenia bezpečnosti informácií – Monitorovanie, meranie, analýza a hodnotenie:** Táto norma poskytuje návod pre vývoj a používanie metrík a merania pre posúdenie efektivity implementovaného systému ISMS a jednotlivých opatrení.
ISO/IEC 27005	**Informačné technológie – Bezpečnostné metódy – Riadenie rizík bezpečnosti informácií:** Táto norma poskytuje doporučenia a techniky pre realizáciu procesu riadenia rizík bezpečnosti informácií v organizáciách. Všetky tieto doporučenia definuje s ohľadom na požiadavky na ISMS podľa normy ISO/IEC 27001.
ISO/IEC 27007	**Informačné technológie – Bezpečnostné metódy – Smernice pre audit systémov riadenia bezpečnosti informácií:** Sada niekoľkých doporučení k vykonávaniu auditov systému ISMS pre zaistenie súladu s normou ISO/IEC 19011 (smernica pre audity systému managementu kvality a systému environmentálneho managementu).
ISO/IEC 27008	**Informačné technológie – Bezpečnostné metódy – Pokyny na hodnotenie kontrolných mechanizmov bezpečnosti informácií:** Obsahuje doporučenia a postupy pre audítorov kontrolujúcich implementáciu ISMS v súlade s normou ISO/IEC 27002. Zároveň táto norma tiež dopĺňa normu ISO/IEC 27007.
ISO/IEC 27013	**Informačné technológie – Bezpečnostné metódy – Návod na integrovanú implementáciu ISO/IEC 27001 a ISO/IEC 20000-1:** PNorma poskytuje návod pre integrovanú implementáciu ISO/IEC 27001 a ISO/IEC 20000-1 pre organizácie, ktoré zamýšľajú tieto dva existujúce manažérske systémy integrovať.
ISO/IEC 27014	**Informačné technológie – Bezpečnostné metódy – Riadenie bezpečnosti informácií:** Poskytuje koncepty a princípy strategického riadenia informačnej bezpečnosti, pomocou ktorých môžu organizácie vyhodnocovať, koordinovať, monitorovať a komunikovať aktivity súvisiace s informačnou bezpečnosťou.

ISO/IEC 27016	**Informačné technológie – Bezpečnostné metódy – Riadenie informačnej bezpečnosti – Organizačná ekonomika:** Norma je publikovaná vo forme technickej správy (TR – z angl. *Technical Report*), poskytuje návod pre organizácie pre tvorbu rozhodnutí v súvislosti s ochranou informácií a pre pochopenie ekonomických dôsledkov týchto rozhodnutí v kontexte konkurenčných požiadaviek na využívané zdroje.
Postupy so špecifickým sektorovým zameraním	
ISO/IEC 27010	**Informačné technológie – Bezpečnostné metódy – Riadenie informačnej bezpečnosti pre medzisektorovú a medziorganizačnú komunikáciu:** Norma poskytuje návod pre implementáciu riadenia informačnej bezpečnosti v rámci organizácií zdieľajúcich informácie.
ISO/IEC 27011	**Informačné technológie – Bezpečnostné metódy – Súbor postupov na opatrenia v informačnej bezpečnosti založený na ISO/IEC 27002 pre telekomunikačné organizácie:** Norma poskytuje návod na implementáciu systému riadenia informačnej bezpečnosti v telekomunikačných organizáciách, aby tieto organizácie boli schopné splniť základné požiadavky kladené na dostupnosť, dôvernosť a integritu.
ISO/IEC 27017	**Informačné technológie – Bezpečnostné metódy – Súbor postupov na opatrenia v informačnej bezpečnosti založený na ISO/IEC 27002 pre cloudové služby:** Obsahuje sadu postupov, ktorá poskytuje dodatočné odporúčania na implementáciu opatrení informačnej bezpečnosti nad rámec súboru opatrení uvedeného v norme ISO/IEC 27002, v kontexte cloud computingu.
ISO/IEC 27018	**Informačné technológie – Bezpečnostné metódy – Súbor postupov na ochranu osobných údajov (OÚ) pre verejné cloudy v pozícií spracovateľov osobných údajov:** Odporúčania pre prevádzkovateľov cloudových služieb týkajúce sa ochrany osobných údajov ich klientov.

ISO/IEC 27019	**Informačné technológie – Bezpečnostné metódy – Riadenie informačnej bezpečnosti v energetickom priemysle – Kontroly informačnej bezpečnosti pre odvetvie dodávok energie:** Poskytuje návod založený na ISO/IEC 27002 na aplikáciu riadenia informačnej bezpečnosti na riadiace a kontrolné systémy používané v energetickom priemysle.

1.3 Systém riadenia bezpečnosti informácií (ISMS)

Medzinárodná norma ISO/IEC 27001 za účelom ochrany informácií a prevádzkovaných informačných systémov zakladá a definuje tzv. **Systém riadenia bezpečnosti informácií**, skrátene ISMS[6]. Ako už z názvu vyplýva, jedná sa o systém zaoberajúci sa primárne riadením bezpečnosti informácií, konkrétne riadením a správou informačných aktív s cieľom eliminovať výskyt nepriaznivých rizík, ktoré by mohli spôsobiť ich stratu, poškodenie alebo nedostupnosť. Tento dokumentovaný systém pozostáva zo súborov interných smerníc, politík a postupov, ktoré sú definované organizáciou za účelom nastavenia vhodných pravidiel a zásad s cieľom zaistiť adekvátnu ochranu jej informačných aktív.

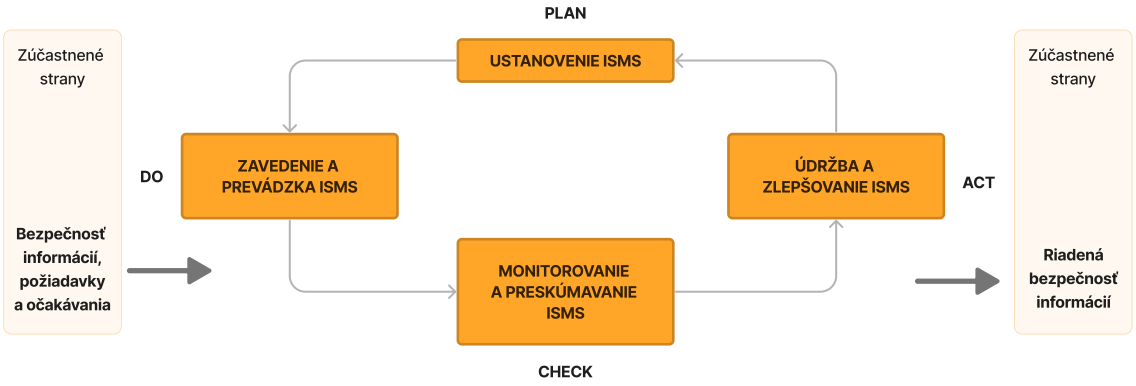
ISMS tak predstavuje systematický prístup k riadeniu bezpečnosti informácií a pozostáva z niekoľkých dielčích krokov, ktorými sú ustanovenie, implementácia, resp. zavedenie, prevádzka, monitorovanie a preskúmavanie, údržba a zlepšovanie úrovne informačnej bezpečnosti organizácie. Systém riadenia bezpečnosti informácií je, podobne ako ostatné systémy riadenia, založený na modeli tzv. PDCA cyklu[7]. Jedná sa o metódu postupného zlepšovania napríklad kvality výrobkov, služieb, procesov, aplikácií či dát prebiehajúcu formou opakovaného vykonávania štyroch základných etáp, ktoré možno úzko prepojiť s činnosťami súvisiacimi s implementáciou a následným fungovaním systému ISMS, a to nasledovne:

- **PLAN** (Naplánuj) – ustanovenie ISMS,
- **DO** (Vykonaj) – zavedenie a prevádzka ISMS,
- **CHECK** (Kontroluj) – monitorovanie a preskúmavanie ISMS,
- **ACT** (Jednaj) – údržba a zlepšovanie ISMS .

[6] Z angl. *Information Security Management System.*

[7] Tiež známy pod pojmom Demingov model.

Aplikácia PDCA cyklu na činnosti realizované v súvislosti so systémom ISMS je schematicky znázornená na obr. 1.2, popis jednotlivých krokov nasleduje.



Obr. 1.2: Previazanosť PDCA modelu s ISMS [10].

Ustanovenie ISMS

V rámci prvej etapy celého procesu ISMS je dôležité upresniť rozsah a vymedziť hranice, ktorých sa riadenie informačnej bezpečnosti týka. Na základe výsledkov vykonaného ohodnotenia rizík je stanovené manažérske zadanie a tiež je realizovaný návrh nevyhnutných bezpečnostných opatrení, ktorých cieľom má byť zvýšenie úrovne bezpečnosti informácií v nadväznosti na implementáciu systému ISMS. [11]

Zavedenie a prevádzka ISMS

Súčasťou druhej etapy ISMS je systematická a efektívna implementácia vybraných bezpečnostných opatrení. [11]

Monitorovanie a preskúmavanie ISMS

Zavedený systém ISMS, plnenie jednotlivých úloh v rámci vykonávaných činností a dosahovanie stanovených cieľov musí byť pravidelne sledované a následne vyhodnocované. Za účelom následného zlepšenia systému ISMS je dôležitá spätná väzba vyhodnotenia prebiehajúcich procesov a činností. Hlavným cieľom tejto etapy je teda sledovanie a ohodnocovanie dostatočných i neuspokojivých prvkov riadenia bezpečnosti informácií. [11]

Údržba a zlepšovanie ISMS

Na základe výstupov predchádzajúceho kroku v podobe zistení a možných nálezov z prebiehajúceho monitorovania ISMS sú realizované činnosti za účelom zlepšovania

systému ISMS. V rámci záverečnej etapy PDCA cyklu sú zavádzané dodatočné opatrenia a/alebo zjednané iné nápravy s cieľom celkového zlepšenia efektivity a účinnosti zavedeného systému a odstránenia zistených slabín a nedostatkov. [11]

V aktuálne platnej verzii normy[8] ČSN ISO/IEC 27001 z r. 2014, ktorá predstavuje hlavný východiskový podklad pri písaní tejto práce, síce nie je obsiahnutá výslovná definícia samotného PDCA cyklus, ako tomu bolo v predošlých verziách tejto normy, no i napriek tomu je možno definíciu a popis všetkých častí procesu ISMS (v náväznosti na PDCA cyklus) nájsť aj v samotnej štruktúre normy 27001. Mapovanie jednotlivých kapitol tejto normy na vyššie uvedené procesy PDCA cyklu uvádza tab. 1.2

Tab. 1.2: Mapovanie normy ISO/IEC 27001 na PDCA cyklus.

PLAN	**4. Súvislosti v organizácii**	Kontext organizácie
		Rozsah ISMS
	5. Vedúce postavenie	Vedúce postavenie a záväzok
		Politika
		Organizačné roly, zodpovednosť a právomoci
	6. Plánovanie	Posúdenie rizík informačnej bezpečnosti
		Ošetrenie rizík informačnej bezpečnosti
		Ciele informačnej bezpečnosti a plány ich dosiahnutia
	7. Podpora	Kompetencie a povedomie
		Komunikácia
		Dokumentované informácie
DO	**8. Prevádzka**	Plánovanie a riadenie prevádzky
CHECK	**9. Vyhodnotenie výkonnosti**	Monitorovanie, meranie, analýza a vyhodnotenie
		Interný audit
		Preskúmavanie managementom
ACT	**10. Zlepšovanie**	Nezhoda a nápravné činnosti

Podrobný rozbor a popis jednotlivých kapitol normy ISO/IEC 27001, ich obsah a požiadavky z nich vyplývajúce budú súčasťou následujúcej kap. 1.4.

[8] V čase písania tejto záverečnej práce je známa už aj norma ISO/IEC 27001:2022, ktorá bola k obdobiu 10/2022 vydaná v anglickom jazyku, a ktorá sa v priebehu nastávajúceho obdobia stane nástupcom ešte stále aktuálne platnej normy ISO/IEC 27001:2013.

1.4 Štruktúra požiadaviek normy ISO/IEC 27001

Táto kapitola prináša bližší popis a rozbor jednotlivých kapitol normy ISO/IEC 27001. Informácie, ktoré sú obsahom tejto kapitoly, autorka práce nadobudla praxou a tiež vďaka účasti na certifikovaných školeniach[9] zameraných na problematiku ISMS a súvisiacich oblastí. Z tohto dôvodu nie sú pri popise niektorých faktov uvádzané zdroje literatúry, nakoľko autorka čerpala pri písaní kapitoly primárne zo svojich vlastných znalostí a vedomostí.

Prvé tri časti normy (a to konkrétne časti postupne s názvom „predmet normy“, „normatívne odkazy“, „termíny a definície“) neobsahujú konkrétne požiadavky na implementáciu systému ISMS, ale poskytujú úvodné slovo k ďalším kapitolám, ktoré jednotlivé požiadavky ďalej popisujú. Z tohto dôvodu je pre účely tejto práce norma 27001 [12] podrobne rozoberaná až od svojej štvrtej časti.

1.4.1 Kapitola 4 – Súvislosti v organizácii

Kontext organizácie

Každá organizácia musí identifikovať všetky vnútorné a tiež vonkajšie faktory, ktoré sú relevantné z pohľadu ISMS, a ktoré tak môžu určitým spôsobom ovplyvniť očakávané výstupy implementovaného systému ISMS. Externé faktory prichádzajú z vonkajšieho okolia organizácie, sú to napr. platná legislatíva, právne predpisy, sociálne a kultúrne aspekty spoločnosti, ekonomická a politická situácia štátu apod. Medzi interné faktory možno radiť organizačnú štruktúru ako celok, jednotlivých zamestnancov, nastavené rozhodovacie procesy v spoločnosti, projektové riadenie, zavedené kultúry a princípy a mnohé iné.

Pri skúmaní kontextu organizácie nesmú byť opomenuté ani všetky relevantné zainteresované strany, ktoré sú v určitom postavení voči organizácií a na ktorých potreby a očakávania musí organizácia prihliadať pri svojich činnostiach. Sú to napr. klienti, koncoví užívatelia poskytovaných služieb, zamestnanci, dodávatelia, obchodní partneri, konzultanti či ďalšie autority. Všetky tieto zainteresované strany majú svoje určité požiadavky voči organizácií, a to samozrejme aj v kontexte zaistenia požadovanej úrovne bezpečnosti informácií.

Rozsah ISMS

Ďalšou požiadavkou štvrtej kapitoly normy ISO/IEC 27001 je definovanie rozsahu, v akom bude celý systém ISMS implementovaný a udržiavaný. Pred zavedením

[9] Napr. úspešne absolvované školenie od spoločnosti Tayllorcox s názvom *ISO 27000 Foundation* zakončené certifikačnou skúškou.

ISMS musí organizácia tento rozsah definovať a patričným spôsobom dokumentovať. Definovaný rozsah určuje, na aké všetky činnosti sa implementovaný systém ISMS bude vzťahovať – môže sa jednať o celú organizáciu a všetky jej činnosti alebo môže pokrývať len určitú časť organizácie a jej konkrétne špecifické činnosti.

Pri definovaní rozsahu ISMS je potrebné prihliadať na všetky skutočnosti relevantné pre vymedzený kontext organizácie, konkrétne je nutné brať do úvahy:

- všetky interné a externé faktory tvoriace kontext organizácie,
- požiadavky a očakávania všetkých zainteresovaných strán,
- vzájomné závislosti a vzťahy medzi činnosťami organizácie a aktivitami, resp. činnosťami ďalších relevantných strán (napr. dodávatelia, zákazníci, ...).

1.4.2 Kapitola 5 – Vedúce postavenie

Vedúce postavenie a záväzok

Top management organizácie musí preukázať podporu pri budovaní ISMS, vo svojej vodcovskej pozícií musí byť príkladom pre ostatných členov/zamestnancov organizácie pri dodržiavaní zásad a princípov implementovaného ISMS. Norma definuje niekoľko zásad, pomocou ktorých, pokiaľ budú dodržané, môže top management organizácie preukázať plnú podporu systému ISMS. Top management by predovšetkým mal:

- zaistiť, aby boli zavedené politiky ISMS spoločne s očakávanými cieľmi,
- zaistiť, aby bol ISMS integrovaný spoločne s ďalšími procesmi (napr. BCMS[10]),
- poskytnúť zdroje, ktoré sú potrebné pre zavedenie a udržiavanie ISMS,
- informovať o dôležitosti bezpečnosti informácií,
- monitorovať, či zavedený systém dosahuje požadované výsledky,
- zabezpečiť kontinuálne zlepšovanie procesov a
- podporovať ďalšie riadiace role v organizácii.

Politika

Ako bolo uvedené už v predošlej požiadavke, vedenie organizácie musí zaistiť, aby bola v organizácií zavedená politika informačnej bezpečnosti. Jedná sa o dokument (resp. súbor viacerých dokumentov), ktorý bližšie špecifikuje požiadavky a zásady na riadenie bezpečnosti informácií v rámci organizácie. Politika informačnej bezpečnosti musí byť v súlade so zameraním činností organizácie a musí definovať ciele, ktoré majú byť v oblasti bezpečnosti informácií dosiahnuté. Jedná sa o primárny dokument, ktorý môže byť ďalej rozvíjaný ďalšími podrobnejšími, špecificky zameranými politikami (napr. smernicami, pracovnými postupmi apod.).

[10]Systém riadenia kontinuity prevádzky, z angl. *Business Continuity Management System.*

Medzi požiadavkami prílohy A normy ISO/IEC 27001 je definovaných celkom 15 dokumentov rozvíjajúcich politiku informačnej bezpečnosti, ktoré ale môžu byť, s prihliadnutím na špecifické potreby konkrétnej organizácie, doplnené o ďalšie relevantné podklady.

Organizačné roly, zodpovednosť a právomoci

Vedenie spoločnosti musí ďalej zaistiť, aby boli stanovené zodpovednosti a právomoci v oblasti bezpečnosti informácií a aby boli určené osoby, ktoré budú zastávať špecifické role a plniť dôležité úlohy v kontexte bezpečnosti informácií v zavedenom systéme ISMS.

1.4.3 Kapitola 6 – Plánovanie

Posúdenie rizík informačnej bezpečnosti

Každá organizácia by mala navrhnúť, implementovať a realizovať proces posúdenia rizík za účelom identifikácie možných nežiadúcich rizík, ktoré by sa mohli vyskytnúť na aktívach organizácie pri vykonávaní prevádzkovaných činností. Za týmto účelom je potrebné, aby organizácia navrhla metodiku posúdenia rizík a následne realizovala posúdenie v súlade s touto metodikou. Problematike posúdenia rizík sa podrobnejšie venuje kap. 1.5 tejto práce.

Ošetrenie rizík informačnej bezpečnosti

Jedným z krokov posúdenia rizík je stanovenie hranice akceptovateľnosti jednotlivých rizík, ktorá určuje, aké z identifikovaných rizík môžu byť prijaté a naopak pre ktoré z nich musia byť navrhnuté a následne zavedené nápravné opatrenia, aby bola ich hodnota znížená aspoň na úroveň prijateľnosti.

Neodmysliteľnou súčasťou fázy ošetrenia rizík je návrh plánu pre zvládanie rizík, ktorý musí obsahovať:

- identifikované riziká a ich hodnotu (mieru rizika) stanovenú podľa aplikovanej metodiky pre posudzovanie rizík,
- opatrenia, ktoré je potrebné zaviesť za účelom zníženia miery rizika, pokiaľ tieto riziká nespĺňajú podmienku pre akceptovanie,
- osobu zodpovednú za implementáciu navrhovaných ošetrujúcich opatrení,
- zdroje, ktoré sú potrebné pre zavedenie a následné udržiavanie ošetrujúcich opatrení a
- časový rámec pre zavedenie týchto opatrení.

Pri navrhovaní a následnom zavádzaní ošetrujúcich opatrení je cieľom znížiť riziko na čo najmenšiu možnú úroveň, ideálne eliminovať dané riziko úplne. V praxi sa

ale častokrát stretávame so situáciou, kedy úplná eliminácia určitého rizika nie je možná, a hovoríme vtedy o tzv. reziduálnom (zostatkovom) riziku. Jedná sa o riziko, ktoré vznikne z pôvodne identifikovaného rizika po zavedení nápravných opatrení. Za predpokladu, že opatrenia pre ošetrenie daného rizika boli navrhnuté správne, je miera reziduálneho rizika nižšia než miera rizika pôvodného. Miera reziduálneho rizika sa následne opäť porovná s nastavenou hranicou pre akceptovateľnosť rizika a posúdi sa, či už je možné takéto riziko prijať, alebo je potrebné navrhnúť a zaviesť ďalšie opatrenia pre zníženie tohto rizika.

Celý proces ošetrenia rizík identifikovaných v rámci posúdenia rizík musí byť dostatočne a vhodným spôsobom dokumentovaný, spoločne s navrhovanými a zavádzanými opatreniami, ktoré musia byť súčasťou prehlásenia o aplikovateľnosti.

Ciele informačnej bezpečnosti a plány ich dosiahnutia

Proces riadenia bezpečnosti informácií vyžaduje jasne definované ciele, ktoré chce organizácia zavedením systému ISMS dosiahnuť. Tieto ciele by mali byť:

- navrhnuté v súlade s definovanou politikou bezpečnosti informácií,
- merateľné, aby bolo možné posúdiť (s)plnenie týchto cieľov,
- v súlade s požiadavkami organizácie na bezpečnosť informácií a tiež s výstupmi posúdenia a následného ošetrenia rizík,
- komunikované zamestnancom organizácie,
- pravidelne aktualizované
- a dokumentované.

Pri definovaní cieľov je potrebné prihliadať na konkrétny kontext ISMS, ktorý bude pre každú organizáciu jedinečný. Aby bolo možné ciele definovať čo najvhodnejším spôsobom, je nutné brať do úvahy špecifické činnosti organizácie, jej aktivity, požiadavky na ochranu a bezpečnosť informácií proti ich zničeniu, krádeži, zneužitiu atď. Tieto ciele môžu byť navrhnuté za účelom:

- zvýšenia miery súladu s právnymi a legislatívnymi požiadavkami,
- eliminácie výskytu bezpečnostných udalostí a incidentov,
- zamedzenia narušenia bezpečnosti informácií a prevádzkovaných informačných systémov a sietí, atď.

Za účelom efektívneho dosahovania definovaných cieľov je žiadúce, aby organizácia navrhla plán pre ich dosahovanie. Tento plán by mal obsahovať nielen samotné ciele, ktoré majú byť dosiahnuté, ale tiež jednotlivé kroky, ktoré je potrebné podniknúť pre dosiahnutie špecifikovaných cieľov. Okrem uvedeného by mal plán ďalej obsahovať:

- definíciu zdrojov potrebných pre vykonanie jednotlivých krokov,
- osoby zodpovedné za vykonanie jednotlivých krokov,
- časový rámec na dosiahnutie definovaného cieľa,

- postupy, na základe ktorých bude možné výsledky ohodnotiť a tým tiež posúdiť dosiahnutie daného cieľa.

1.4.4 Kapitola 7 – Podpora

Kompetencie a povedomie

Organizácia musí určiť osoby a ich kompetencie, ktoré budú mať vplyv na úroveň bezpečnosti informácií. Je žiadúce, aby boli týmto osobám priradené kompetencie a povinnosti s prihliadnutím k ich vzdelanosti a aby bola úroveň ich vedomostí ďalej rozvíjaná. Tieto osoby, ktoré sú pri výkone svojich činností akýmkoľvek zapojené do procesov navrhovania, zavádzania či udržiavania ISMS, by mali vo všeobecnosti:

- mať povedomie o požiadavkách normy ISO/IEC 27001,
- porozumieť základným konceptom, technikám a procedúram pre zvyšovanie bezpečnosti informácií,
- byť schopné identifikovať a analyzovať možné riziká bezpečnosti informácií a následne navrhnúť proces ošetrenia týchto rizík v súlade s bezpečnostnými požiadavkami definovanými prílohou A normy ISO/IEC 27001 a postupmi, ktoré definuje norma ISO/IEC 27002,
- mať dostatočné povedomie o používaných technológiách a tiež vedieť správne vyhodnotiť požiadavky na ich primerané zabezpečenie.

Aby bolo možné v rámci interného prostredia organizácie zaistiť potrebnú mieru bezpečnosti informácií, je dôležité, aby mali jednotliví zamestnanci, resp. užívatelia dostatočné povedomie a dôležitosti bezpečnosti informácií a všetkých súvisiacich aspektoch, a to aj vedomosť o možných nepriaznivých následkoch, ktoré môžu nastať v prípade, že bezpečnosť informácií nebude dosahovať požadovanú úroveň. Organizácia by preto mala navrhnúť program pre zvyšovanie bezpečnostného povedomia zamestnancov a vytvárať im vhodné podmienky pre ďalšie rozširovanie ich vedomostí v oblasti bezpečnosti informácií, napr. realizáciou školení zamestnancov, podporou ich samovzdelávania, informovaním o dôležitosti bezpečnosti informácií. Zvyšovanie bezpečnostného povedomia by malo predstavovať neustály proces, a preto by tieto aktivity mali byť realizované opakovane, v pravidelných časových intervaloch.

Komunikácia

Organizácia musí zaistiť, aby boli všetky relevantné zainteresované strany dostatočne informované o zavedení a realizovaní ISMS organizáciou. Pre splnenie tejto požiadavky musí preto organizácia vhodným spôsobom komunikovať, a to jednak interne (zamestnanci), a taktiež i navonok (zákazníci, dodávatelia, partneri, autority atď.) so všetkými zainteresovanými stranami.

Dokumentované informácie

Ako už bolo popísané v predchádzajúcich častiach, pre účely zavedenia a prevádzkovania systému ISMS je nevyhnutné taktiež založiť a viesť dokumentáciu, ktorá bude systém ISMS vhodným spôsobom zaznamenávať a podporovať. Rozsah a forma tejto dokumentácie bude závisieť vždy na špecifickom kontexte aktivít vykonávaných v rámci pôsobenia konkrétnej organizácie. Avšak norma ISO/IEC 27001 definuje niekoľko povinných dokumentov, ktoré musia byť súčasťou bezpečnostnej dokumentácie každej organizácie. Medzi tieto dokumenty patria konkrétne:

- dokumentácia rozsahu ISMS,
- metodika pre posudzovanie rizík a ich následné zvládanie,
- ciele informačnej bezpečnosti,
- prehlásenie o aplikovateľnosti,
- dokumentované informácie o výsledkoch monitorovania hodnotenia výkonnosti a efektívnosti zavedeného ISMS,
- správy z vykonaného interného auditu a preskúmania vedením organizácie, spoločne s dokumentáciou plánov a navrhovaných opatrení pre odstránenie zistených nedostatkov.

Tieto povinné dokumenty môže ďalej organizácia doplniť o niekoľko ďalších dokumentov, akými môžu byť napr. rôzne pravidlá a pracovné postupy, príručky, návody či manuály, ktoré budú vhodným spôsobom podporovať povedomie jednotlivých zamestnancov a celý proces riadenia bezpečnosti informácií v organizácii.

Organizácia musí následne zabezpečiť, aby bola všetka vytvorená dokumentácia udržiavaná vždy v aktuálnom stave a aby vhodne a dostatočne reflektovala všetky aspekty významné pre systém ISMS danej organizácie. Všetka vytvorená dokumentácia musí byť vo vhodnom formáte dostupná všetkým zainteresovaným osobám, ktoré akýmkoľvek spôsobom zasahujú do kontextu ISMS organizácie. Musí byť tiež zaistená integrita a dôvernosť vytvorenej a udržiavanej dokumentácie, čo znamená, že organizácia musí zabezpečiť, aby bola dokumentácia chránená proti neoprávneným modifikáciám a zneužitiu zo strany neoprávnených subjektov.

1.4.5 Kapitola 8 – Prevádzka

Plánovanie a riadenie prevádzky

Organizácia by mala dostatočným a vhodným spôsobom plánovať, implementovať a kontrolovať procesy súvisiace s riadením bezpečnosti informácií, aby bolo možné dosiahnuť všetky ciele stanovené v tejto oblasti. Za týmto účelom musí organizácia navrhnúť a realizovať vhodné aktivity, aby bolo možné predchádzať, ideálne úplne zamedziť, vzniku možných nežiadúcich rizík bezpečnosti informácií, alebo v prípade

výskytu týchto rizík následne znížiť ich nepriaznivé dopady na aktíva alebo činnosti organizácie.

Organizácia musí taktiež plánovať zmeny s prihliadnutím na možné riziká, ktoré môžu v dôsledku zavedenia týchto zmien vzniknúť. Po zavedení akejkoľvek zmeny je nutné opakovane realizovať posúdenie rizík a v prípade potreby tiež navrhnúť ďalšie opatrenia za účelom odstránenia nových identifikovaných rizík.

1.4.6 Kapitola 9 – Vyhodnotenie výkonnosti

Monitorovanie, meranie, analýza a vyhodnotenie

Zavedený systém ISMS v rámci organizácie je potrebné monitorovať a následne vyhodnocovať jeho efektívnosť. Za účelom splnenia tejto požiadavky je potrebné stanoviť to, aké podklady, v akom rozsahu, kedy a akým spôsobom budú monitorované a následne analyzované za účelom finálneho vyhodnotenia efektívnosti ISMS. Medzi sledované parametre možno zaradiť napr. výskyt a početnosť bezpečnostných udalostí a incidentov, mieru plnenia stanovených cieľov bezpečnosti informácií, zistené zraniteľnosti aktív organizácie atď. Všetky informácie získané v procese monitorovania organizácia následne analyzuje a vyhodnocuje, aby bolo možné určiť, kde, v akých miestach systému ISMS je nutné realizovať zmeny. Výsledky tejto analýzy spoločne s navrhovanými zmenami musia byť dokumentované.

V súvislosti s diskutovaním problematiky monitorovania a následného vyhodnocovania účinnosti a efektívnosti ISMS je vhodné spomenúť štandard ISO/IEC 27004, ktorý obsahuje návodné postupy práve pre tieto účely (viď tab. 1.1).

Interný audit

Prevádzkovaný systém ISMS by mal byť v pravidelných intervaloch preskúmavaný. Prostredníctvom vykonaného interného auditu môže organizácia získať informácie o tom, do akej miery sú splnené požiadavky normy ISO/IEC 27001, o ktorých plnenie sa organizácia usiluje práve implementáciou systému ISMS. Pre každý interný audit musí byť definovaný rozsah, tj. ktoré aktivity a činnosti budú preskúmavané a hodnotené, a tiež kritériá, pomocou ktorých sa bude vyhodnocovať dodržiavanie súladu s požiadavkami normy ISO/IEC 27001, prípadne s inými požiadavkami (napr. legislatívne požiadavky, zmluvy so zákazníkmi apod.).

Audítor vykonávajúci interný audit bezpečnosti informácií v rámci organizácie musí mať dostatočné znalosti v oblasti riadenia bezpečnosti informácií a jeho činnosť v zmysle vykonávania auditu musí byť nezávislá od činností, ktoré sú týmto auditom preskúmavané. Môže sa jednať o osobu z vnútorného prostredia organizácie alebo sa môže organizácia rozhodnúť využiť služby externých audítorských firiem.

Výsledky vykonaného auditu slúžia organizácií k posúdeniu, či a do akej miery sú dodržiavané požiadavky kladené na systém ISMS. Na základe zistení auditu sa môže organizácia rozhodnúť, aké zmeny za účelom nápravy zistených nedostatkov v rámci systému ISMS je potrebné prijať. Výsledky auditu sú následne vhodným a prehľadným spôsobom prezentované vedeniu organizácie.

Preskúmavanie managementom

Vedenie organizácie by malo v pravidelných intervaloch preverovať zavedený systém ISMS, aby bolo možné overiť jeho vhodnosť a efektívnosť vzhľadom k požiadavkám a cieľom, ktoré majú byť dosiahnuté. Pri preskúmavaní musí brať vedenie spoločnosti do úvahy:

- činnosti a kroky, ktoré boli vykonané od posledného realizovaného preskúmania systému ISMS,
- zmeny, ktoré sa vyskytli v prostredí (internom aj externom) organizácie,
- hodnotenie výkonnosti informačnej bezpečnosti (napr. vo forme reportovacej správy z vykonaného auditu),
- spätnú väzbu od zainteresovaných strán,
- výsledky posúdenia rizík s prihliadnutím na mieru dodržania navrhnutého plánu pre ošetrenie identifikovaných rizík,
- možnosti ďalšieho zlepšovania.

Výstupom preskúmania vedením organizácie sú zistenia ohľadom potrebných zmien a nápravných opatrení, ktoré by bolo vhodné prijať a zaviesť za účelom zvýšenia výkonnosti a efektívnosti zavedeného systému ISMS.

1.4.7 Kapitola 10 – Zlepšovanie

Nezhoda a nápravné činnosti

V prípade zistenia, že s pomocou zavedeného systému ISMS organizácia nedosahuje a v dostatočnej miere neplní všetky relevantné požiadavky, je nevyhnutné podniknúť kroky vedúce k odstráneniu zistených nedostatkov. V niektorých prípadoch však nie je možné v plnom rozsahu všetky zistené nedostatky odstrániť úplne. Je ale potrebné navrhnúť také nápravné opatrenia, pomocou ktorých bude možné zmierniť nežiadúce následky plynúce z nedostatočného súladu so stanovenými požiadavkami.

Všetky zavedené nápravné opatrenia musia byť riadne a vhodným spôsobom dokumentované a musia byť hodnotené vzhľadom k cieľu, ktorým je zaistenie dostatočného súladu so všetkými stanovenými požiadavkami.

1.5 Riadenie rizík bezpečnosti informácií

Všetky organizácie si v rámci vykonávania svojich pravidelných činností stanovujú a definujú vlastné jedinečné ciele, ktoré sa snažia správnou a dôslednou realizáciou týchto činností dosiahnuť. Pri vykonávaní akejkoľvek z týchto plánovaných činností sa môže v zamýšľanom fungovaní organizácie vyskytnúť neočakávaný priebeh, ktorý sa prejavuje ako určité riziko. Aby bolo možné predchádzať vzniku takýchto neistých, neočakávaných situácií, je žiadúce, aby organizácia priebežne kontrolovala, zaisťovala a minimalizovala výskyt takýchto nežiadúcich udalostí. Kompletný proces, ktorého cieľom je zistenie, kontrola a následná minimalizácia či ideálne eliminácia udalostí, ktoré môžu ovplyvňovať určitý subjekt, sa nazýva riadenie rizík [13].

Riadenie rizík predstavuje proces systematického vyhľadávania, posudzovania, hodnotenia a odstraňovania neistôt [14]. Riadenie rizík by malo byť nepretržitým procesom, počas ktorého je nutné:

- stanoviť kontext činností organizácie, ktoré sú hlavným záujmom posúdenia,
- ďalej identifikovať a vyhodnotiť riziká,
- následne vytvoriť plán pre zvládanie identifikovaných rizík
- a nakoniec ošetriť riziká predstavujúce najväčšiu hrozbu pre činnosti organizácie v podobe nežiadúceho pôsobenia a najzávažnejšieho dopadu na chránené aktíva a procesy.

Riadenie rizík ako systematický proces teda umožňuje analyzovať, čo nepriaznivé sa môže vyskytnúť a aké môžu byť prípadné nežiadúce dôsledky, pred rozhodnutím, čo (aké kroky) a kedy (v akom časovom období) by sa malo uskutočniť za účelom redukcie rizika na prijateľnú úroveň [6].

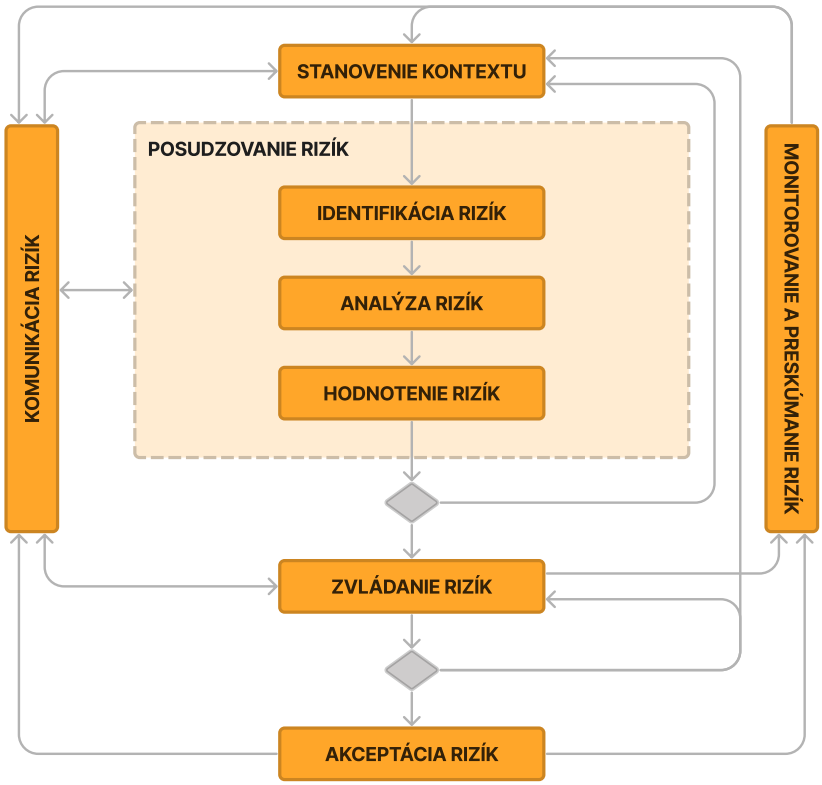
1.5.1 Proces riadenia rizík

Proces riadenia rizík sa skladá z niekoľkých dielčích častí, krokov, ktoré je potrebné vykonať v presne definovanom slede. Riadenie rizík zahŕňa nasledujúce procesy [14]:

- stanovenie kontextu,
- posudzovanie rizík, ktoré zahŕňa (pod)kroky identifikácie, analýzy a následného hodnotenia rizík,
- a ošetrenie, resp. zvládanie zistených rizík.

Po vykonaní vyššie uvedených základných krokov je následne do celého procesu zavedené monitorovanie a preskúmanie rizík, komunikácia rizík a nakoniec prípadná akceptácia tých rizík, ktoré vyhovujú kritériám prijateľnosti. Celý priebeh procesu riadenia rizík, tak ako ho popisuje norma ISO/IEC 31000, je zobrazený na obr. 1.3.

Cieľový koncept metodiky hodnotenia rizík, ktorej návrh je súčasťou tejto práce (viď ďalej v kap. 2.1), sa zameriava na dve najdôležitejšie časti, a to posúdenie rizík



Obr. 1.3: Proces managementu rizík podľa normy ISO/IEC 31000 [14].

a ich následné ošetrenie. Tieto hlavné časti je možné ďalej rozdeliť na štyri fázy, ktorými sú postupne identifikácia, analýza, hodnotenie a nakoniec zvládanie takto identifikovaných a ohodnotených rizík. Podrobnejšie členenie a vzájomnú nadväznosť týchto krokov tiež zachytáva obr. 1.3.

Problematike riadenia rizík sa autorka tejto práce venovala už v rámci svojej záverečnej bakalárskej práce, kde sa konkrétne v prvej kapitole tejto práce zamerala na podrobný popis jednotlivých krokov posudzovania a následného zvládania rizík. Z tohto dôvodu preto čitateľov odkazujeme na spomínanú záverečnú prácu [15].

1.6 Právna úprava kybernetickej bezpečnosti

1.6.1 Pojem kybernetickej bezpečnosti

V kap. 1.1 bol bližšie vysvetlený pojem informačnej bezpečnosti. V poslednej dobe sa však často stretávame tiež s pojmom „kybernetická bezpečnosť“ a mnohí ľudia žijú v mylnej domnienke, že oba tieto pojmy za sebou ukrývajú to isté. V skutočnosti však možno pojem „kybernetická bezpečnosť“ chápať ako podmnožinu informačnej bezpečnosti, ako je znázornené na obr. 1.4, a to na základe skutočnosti, že informačná bezpečnosť si kladie za cieľ ochraňovať informácie v akejkoľvek podobe, zatiaľ čo primárnym cieľom kybernetickej bezpečnosti je ochrana informácií len v podobe digitálnej [16].

Obr. 1.4: Vzájomný vzťah informačnej a kybernetickej bezpečnosti.

Kybernetická bezpečnosť je v dnešnej modernej dobe diskutovaná v mnohých oblastiach ľudského života, nakoľko sa samotný pojem kybernetickej bezpečnosti stal tzv. multi-odborovým fenoménom, ktorý je vo veľkom rozsahu používaný nielen naprieč technickými, ale rovnako tak aj humanitnými odbormi [17]. Dôsledkom tejto skutočnosti je, že existuje veľké množstvo častokrát rozličných definícií pojmu „kybernetická bezpečnosť“. Jednou z nich môže byť definícia, kedy je kybernetická bezpečnosť chápaná ako *„súhrn právnych, organizačných, technických a vzdelávacích prostriedkov smerujúcich k zaisteniu ochrany kybernetického priestoru“* [18], pričom pod pojmom „kybernetický priestor“ ďalej rozumieme *„digitálne prostredie umožňujúce vznik, spracovanie a výmenu informácií, tvorené informačnými systémami, službami a sieťami elektronických komunikácií“*[11].

[11] Viď § 2 písm. a) ZoKB [1].

1.6.2 Relevantné právne predpisy

V právnom prostredí Českej republiky je právna úprava kybernetickej bezpečnosti zakotvená v dvoch hlavných právnych predpisoch, ktorými sú:

- **zákon o kybernetické bezpečnosti**[12] ako primárny predpis národného práva Českej republiky a
- prevádzacia vyhláška, konkrétne **vyhláška o kybernetické bezpečnosti**[13], ktorá ako sekundárny právny predpis samotný zákon ďalej rozvádza, dopĺňa a bližšie špecifikuje.

Zákon o kybernetickej bezpečnosti upravuje práva a povinnosti osôb, ďalej tiež právomoci a pôsobnosť orgánov verejnej moci v oblasti kybernetickej bezpečnosti a upravuje zaisťovanie bezpečnosti sietí elektronických komunikácií a informačných systémov. Medzi jeho hlavné ciele patrí:

- stanoviť základnú úroveň bezpečnostných opatrení,
- zlepšiť detekciu kybernetických bezpečnostných incidentov,
- zaviesť hlásenie kybernetických bezpečnostných incidentov,
- zaviesť systém opatrení k reakcii na kybernetické bezpečnostné incidenty,
- upraviť činnosť dohľadových pracovísk. [19]

Zákon o kybernetickej bezpečnosti spracováva tiež príslušné predpisy Európskej únie – konkrétne sa jedná o transpozíciu medzinárodnej **smernice NIS**[14] do národného práva. Táto smernica tvorí základný rámec právnej úpravy kybernetickej bezpečnosti na úrovni medzinárodného európskeho práva a jej primárnym cieľom je prostredníctvom vysokej úrovne bezpečnosti sietí a informačných systémov zlepšiť fungovanie vnútorného medzinárodného trhu.

V období, odkedy ZoKB vstúpil do platnosti a stal sa účinným, bol tento zákon už niekoľkokrát novelizovaný[15]. V roku 2017 boli vydané a schválené dve obsahovo významné novely ZoKB, a to prostredníctvom:

- zákona č. 104/2017 Sb. s účinnosťou od 1. júla 2017 a
- zákona č. 205/2017 Sb. s účinnosťou od 1. augusta 2017.

Až do súčasnej doby prebehlo ešte niekoľko ďalších novelizácií ZoKB, konkrétne novelizácia zákonom č. 183/2017 Sb., zákonom 35/2018 Sb., zákonom č. 111/2019 Sb.,

[12] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů [1].

[13] Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat [2].

[14] Smernica Európskeho parlamentu a Rady (EÚ) č. 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii [20].

[15] Novelizácia je proces, v rámci ktorého je novým právnym predpisom doplnený či (po)zmenený starší, skôr vydaný, schválený, platný a účinný právny predpis. Tento novší právny predpis, ktorým je upravený právny predpis pôvodný, sa nazýva novela.

zákonom č. 12/2020 Sb., zákonom č. 261/2021 Sb., a aktuálne posledná novelizácia zákonom č. 226/2022 Sb. [19]

Mimo vyššie uvedených právnych predpisov možno v súvislosti s problematikou kybernetickej bezpečnosti spomenúť aj ďalšie zákony, vyhlášky a nariadenia, ktoré ich dopĺňajú. Medzi tieto partia konkrétne:

- **vyhláška č. 317/2014 Sb.** o významných informačních systémech a jejich určujících kritériích,
- **nařízení vlády č. 432/2010 Sb.** o kritériích pro určení prvku kritické infrastruktury,
- **zákon č. 127/2005 Sb.** o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích),
- **zákon č. 240/2000 Sb.** o krizovém řízení a o změně některých zákonů (krizový zákon).

1.6.3 Štruktúra opatrení podľa vyhlášky č. 82/2018 o kybernetickej bezpečnosti

Zákon č. 181/2014 o kybernetickej bezpečnosti (ZoKB) stanovuje povinnosti osôb a orgánov verejnej moci v oblasti kybernetickej bezpečnosti. Vyhláška č. 82/2018 o kybernetickej bezpečnosti (VoKB) predstavuje prevádzací predpis k uvedenému zákonu, ktorý tento primárny právny predpis dopĺňa a ďalej rozvíja. VoKB stanovuje spôsoby a postupy pre zaistenie bezpečného prostredia pre informačné systémy, siete a služby v rámci územia Českej republiky. Táto vyhláška má za cieľ minimalizovať riziká spojené so zneužitím informácií a ohrozením dostupnosti poskytovaných informačných služieb. VoKB konkrétne pojednáva o:

- povinnostiach subjektov, ktorí disponujú prístupom k informačným systémom a sieťam, a ktorí sú povinní zaistiť odpovedajúcu úroveň bezpečnosti týchto systémov a sietí,
- tvorbe bezpečnostných opatrení pre ochranu informačných systémov a sietí,
- povinnostiach v prípade výskytu nepriaznivých incidentov v oblasti kybernetickej bezpečnosti, akými sú nahlásenie vzniknutého incidentu príslušným úradom[16] a spolupráca pri jeho následnom riešení,
- základných požiadavkách na kybernetickú bezpečnosť v oblasti správy informačných systémov a sietí. [19]

Ustanovenia tejto vyhlášky sú rozhodujúce pre každú organizáciu či subjekt, ktorý v rámci svojich činností spracováva citlivé informácie a/alebo poskytuje služby iným subjektom prostredníctvom internetu či iných sietí.

[16] Takýmto úradom je na území Českej republiky hlavný regulačný orgán v oblasti kybernetickej bezpečnosti – Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Ako bolo uvedené vyššie, VoKB, okrem iného, špecifikuje tiež základnú štruktúru bezpečnostných opatrení, ktoré by mali všetky povinné subjekty[17] pri zavádzaní a prevádzke systému ISMS implementovať, aby bola dosiahnutá dostatočná úroveň bezpečnosti informácií v prevádzkovaných sieťach a informačných systémoch.

Pod pojmom bezpečnostné opatrenie rozumieme „*ochranné opatrenie pre zaistenie bezpečnostných požiadaviek kladených na systém*“[22]. VoKB delí bezpečnostné opatrenia na dve základné kategórie, a to opatrenia organizačné a technické, ktoré vo svojich jednotlivých ustanoveniach bližšie špecifikuje a podrobne vysvetľuje. Medzi **organizačné opatrenia**[18]patrí:

- systém riadenia bezpečnosti informácií,
- riadenie aktív,
- riadenie rizík,
- organizačná bezpečnosť,
- bezpečnostné role,
- riadenie dodávateľov,
- bezpečnosť ľudských zdrojov,
- riadenie prevádzky a komunikácií,
- riadenie zmien,
- riadenie prístupu,
- akvizícia, vývoj a údržba,
- zvládanie kybernetických bezpečnostných incidentov a udalostí,
- riadenie kontinuity činností
- a audit kybernetickej bezpečnosti.

Ďalšie ustanovenia[19] vyhlášky špecifikujú **opatrenia technického charakteru**, konkrétne sa jedná o opatrenia v nasledujúcich oblastiach:

- fyzická bezpečnosť,
- bezpečnosť komunikačných sietí,
- správa a overovanie identít,
- riadenie prístupových oprávnení,
- ochrana pred škodlivým kódom,
- zaznamenávanie udalostí informačného a komunikačného systému, jeho užívateľov a administrátorov,
- detekcia kybernetických bezpečnostných udalostí,

[17]Povinné subjekty sú všetky subjekty, na ktoré sa vzťahujú ustanovenia ZoKB a ktoré sú povinné pri svojich činnostiach dodržiavať požiadavky definované v tomto zákone a tiež v jeho prevádzacej vyhláške (VoKB). Zákon je záväzný pre všetky subjekty stanovené v § 3 ZoKB. Stanovenie konkrétnych orgánov alebo osôb, na ktoré sa ustanovenia ZoKB vzťahujú, závisí na splnení charakteristík alebo kritérií pre určenie jednotlivých povinných osôb. [21]

[18]Viď § 3 až § 16 VoKB [2].

[19]Viď § 17 až § 29 VoKB [2].

- aplikačná bezpečnosť,
- kryptografické prostriedky,
- zaisťovanie úrovne dostupnosti informácií,
- priemyselné, riadiace a obdobné špecifické systémy
- a digitálne služby.

Jednotlivé opatrenia VoKB bližšie špecifikuje, čím poskytuje povinným subjektom spadajúcim pod pôsobnosť ZoKB návodný postup, akým spôsobom môžu vhodne zabezpečiť svoje informačné systémy a siete tak, aby vzniknuté riešenie bolo v súlade s požiadavkami ZoKB a jeho prevádzacej vyhlášky.

1.6.4 Minimálne požiadavky na riadenie bezpečnosti informácií

Na území Českej republiky pôsobí a zastáva rozhodujúcu úlohu v oblasti kybernetickej bezpečnosti regulačný orgán, ktorým je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Ten v rámci vykonávanie svojich kompetencií vydáva aj niekoľko návodných postupov a odporučení[20] pre povinné subjekty podľa ZoKB, ale tiež pre subjekty, ktoré pod pôsobnosť ZoKB nespadajú.

Pre mnohé subjekty je postačujúce aplikovať zjednodušené princípy, postupy a doporučenia v oblasti kybernetickej bezpečnosti. NÚKIB tieto svoje doporučenia v publikovaných návodných materiáloch [23] delí na dve časti:

- manažérska časť – obsahuje popis procesne orientovaných oblastí, ktoré spravidla zahŕňajú popisy postupov, ktoré je v rámci organizácie potrebné zaviesť a dodržiavať,
- technická časť – obsahuje konkrétne návody pre zaistenie minimálnej úrovne zabezpečenia.

Pre bližší popis jednotlivých oblastí, konkrétnych cieľov a doporučení pre implementáciu opatrení zaisťujúcich požadovanú úroveň bezpečnosti informácií viď [23].

[20] Viď napr. „Minimální bezpečnostní standard“[23].

1.7 Zhodnotenie súčasného stavu existujúcich riešení v oblasti riadenia rizík informačnej bezpečnosti

V predchádzajúcich kapitolách bolo predstavených a bližšie popísaných niekoľko existujúcich štandardov a doporučení v oblasti informačnej a kybernetickej bezpečnosti. Veľká pozornosť bola venovaná najmä medzinárodnej norme ISO/IEC 27001, ktorá predstavuje základný rámec pre systém ISMS v oblasti riadenia bezpečnosti informácií. Ďalej boli tiež diskutované právne aspekty kybernetickej bezpečnosti, kde bol predstavený ZoKB spoločne s jeho prevádzacou vyhláškou. Tá špecifikuje niekoľko bezpečnostných (organizačných a technických) opatrení, ktoré sú subjekty spadajúce pod pôsobnosť ZoKB povinné implementovať, aby bolo možné dosiahnuť požadovanú úroveň bezpečnosti informácií.

Tieto, ale aj mnohé iné existujúce riešenia majú jednu hlavnú nevýhodu, ktorou je ich všeobecnosť. Predstavujú len akýsi rámec, podľa ktorého by mal subjekt postupovať, avšak bez prihliadnutia na špecifický kontext, v rámci ktorého je bezpečnosť informácií určitého subjektu (napr. organizácie) riešená. Aplikácia všeobecného postupu nie je nesprávna, avšak častokrát môže byť za účelom naplnenia potrieb konkrétneho subjektu nedostatočná. Preto je vhodnejšou alternatívou pri riešení otázok v oblasti informačnej a kybernetickej bezpečnosti postupovať na základe vlastných postupov a riešení vytvorených „na mieru“, ktoré budú špecificky zamerané na jedinečný kontext činností danej organizácie.

Práve z tohto dôvodu bude v ďalšej časti tejto práce predstavený a podrobne popísaný vlastný návrh metodiky pre posudzovanie rizík informačnej bezpečnosti. Navrhnutá metodika bola vytvorená s prihliadnutím na špecifický kontext procesov Spoločnosti, pre ktorú v čase písania tejto práce autorka vykonáva pracovnú činnosť. Ďalšou súčasťou praktickej časti tejto práce je následná implementácia aplikácie, pomocou ktorej je možné prehľadne zobraziť výsledky vykonanej analýzy podľa postupu uvedeného v navrhnutej metodike. Aj pre tento účel existuje dnes už niekoľko rôznych tzv. GRC[21] riešení, ako príklad možno uviesť nástroje Archer IRM[22], Eramba[23] či ServiceNow[24].

[21] GRC – z angl. *Governance, Risk and Compliance* – jedná sa o softwarové aplikácie či nástroje, ktoré môžu byť využívané napr. k hodnoteniu rizík, kontrole užívateľských oprávnení a riadeniu prístupov a tiež k zefektívneniu dodržiavania legislatívnych a ďalších požiadaviek.

[22] Pre viac informácií viď [24].

[23] Pre viac informácií viď [25].

[24] Pre viac informácií viď [26].

2 Praktická časť

2.1 Vlastný návrh metodiky pre analýzu rizík bezpečnosti informácií

Jednou z hlavných častí tejto diplomovej práce je návrh a popis vlastnej metodiky pre riadenie rizík, ktorá bola vytvorená za účelom vykonania procesu riadenia rizík informačnej bezpečnosti v Spoločnosti. Metodika bola navrhnutá s prihliadnutím na existujúce štandardy a odporúčania v tejto oblasti, ktoré boli vydané regulačným orgánom pôsobiacom na území Českej republiky (NÚKIB), viď napr. [27]. Navrhnutá metodika zároveň preberá niekoľko častí a krokov z prístupu pre posudzovanie rizík stanovenom normou ISO/IEC 27005 [6], ktoré ale vhodným spôsobom rozširuje pre špecifický kontext riadenia rizík v Spoločnosti. V rámci tejto kapitoly budú postupne vysvetlené jednotlivé fázy riadenia rizík, ktoré boli zo všeobecného pohľadu popísané v kap. 1.5.

2.1.1 Identifikácia a rozdelenie aktív

Prvou fázou procesu riadenia rizík informačnej bezpečnosti je posudzovanie rizík, ktoré zahŕňa postupne identifikáciu a ohodnotenie kontextu riadenia informačnej bezpečnosti relevantného pre organizáciu, ktorá sa rozhodne posúdenie rizík pre svoje potreby vykonať.

Prvým a základným krokom komplexného procesu riadenia rizík je identifikácia aktív, ktoré spadajú do hodnoteného rozsahu informačnej bezpečnosti. Základom metodiky je preto rozdelenie aktív na aktíva primárne a podporné, pričom je vhodné podporné aktíva združovať do logických celkov. Pre potreby Spoločnosti bolo v rámci metodiky navrhnuté nasledovné rozdelenie aktív:

- **primárne aktíva:**
  - informačné aktíva – dáta a informácie,
  - služby poskytované zákazníkom – služby poskytované Spoločnosťou,
- **podporné aktíva:**
  - priestory – lokality, budovy, miestnosti a ich vybavenie,
  - fyzické aktíva – technické vybavenie vrátane systémového, programového vybavenia, sieťová infraštruktúra a jej súčasti,
  - aplikačné programové aktíva – systémy a aplikácie,
  - personál – zamestnanci podieľajúci sa na činnostiach Spoločnosti,
  - služby prijímané od externých dodávateľov – predstavujú služby, ktoré sú nevyhnutné k vykonávaniu činností Spoločnosti,
  - podporné služby prebiehajúce interne v rámci Spoločnosti.

Kompletný zoznam[1] identifikovaných aktív Spoločnosti, vrátane ich rozdelenia na primárne a podporné, je súčasťou prílohy A.1.

Hodnotenie aktív

Hodnotenie aktív spočíva v stanovení ich hodnoty, ktorá sa odvíja od **hodnotenia atribútov bezpečnostnej triády** (ktorými sú dôvernosť, integrita a dostupnosť) a z **významnosti** daného aktíva, ktorá reflektuje finančnú hodnotu, resp. ekonomický význam aktíva z pohľadu Spoločnosti. Hodnotenie jednotlivých parametrov bezpečnostnej triády (dôvernosť, integrita a dostupnosť) sa odvíja od hodnotenia dopadov na aktíva, ktoré spočíva v posúdení dopadu na Spoločnosť v prípade, pokiaľ budú dané aktíva v dôsledku realizácie hrozby nedostupné, prístupné neoprávneným osobám a/alebo neoprávneným spôsobom modifikované.

Každý z parametrov bezpečnostnej triády je hodnotený s využitím škály 1 až 4, kde nízka hodnota (1) predstavuje nízky dopad na Spoločnosť v prípade, že dôjde k narušeniu bezpečnostného parametra, naopak vyššia hodnota (4) predstavuje vysoký dopad. Nasledujúce tabuľky 2.1, 2.2 a 2.3 uvádzajú hodnotenie jednotlivých atribútov spoločne s popisom jednotlivých kategórií.

Tab. 2.1: Stupnica pre hodnotenie dôvernosti aktív.

1	Nízka	Narušenie a/alebo strata dôvernosti aktíva nemá žiadny alebo má len minimálny dopad na činnosti Spoločnosti.
2	Stredná	Narušenie a/alebo strata dôvernosti aktíva má určitý (znateľný) dopad na činnosti Spoločnosti.
3	Vysoká	Narušenie a/alebo strata dôvernosti aktíva má významný dopad na činnosti Spoločnosti.
4	Kritická	Narušenie a/alebo strata dôvernosti aktíva má veľmi významný (až likvidačný) dopad na činnosti Spoločnosti.

Pre každé identifikované aktívum Spoločnosti sú tak určené celkom 3 hodnoty, pre každý z parametrov dôvernosť (C), integrita (I) a dostupnosť (A) jedna hodnota zvlášť. Výsledná hodnota odpovedajúca hodnoteniu dopadov pre konkrétne aktívum sa stanoví ako aritmetický priemer z týchto 3 hodnôt, a to nasledovne:

$$\text{hodnotenie dopadu} = \frac{C + I + A}{3}. \tag{2.1}$$

[1]Neodmysliteľnou súčasťou výtvarného katalógu aktív by mala byť informácia o vlastníkovi každého aktíva. Jedná sa o osobu, ktorá je zodpovedná za zaobstaranie aktíva, jeho prevádzku a tiež za udržiavanie patričnej úrovne jeho bezpečnosti. Z dôvodu zachovania požadovanej úrovne súkromia Spoločnosti však táto informácia nie je v prílohe A.1 uvádzaná.

Tab. 2.2: Stupnica pre hodnotenie integrity aktív.

1	Nízka	Narušenie integrity (akékoľvek poškodenie informácií, chyby v software, chyby personálu apod.) nemá žiadny alebo má len minimálny dopad na procesy a činnosti Spoločnosti, vrátane bezpečnosti.
2	Stredná	Narušenie integrity (akékoľvek poškodenie informácií, chyby v software, chyby personálu apod.) má určitý (obmedzený) dopad na procesy a činnosti Spoločnosti, vrátane bezpečnosti. Narušenie integrity nebude mať bezprostredný vplyv na služby poskytované zákazníkom.
3	Vysoká	Narušenie integrity (akékoľvek poškodenie informácií, chyby v software, chyby personálu apod.) má významný dopad na procesy a činnosti Spoločnosti, vrátane bezpečnosti. Narušenie integrity bude mať vplyv na služby poskytované zákazníkom.
4	Kritická	Narušenie integrity (akékoľvek poškodenie informácií, chyby v software, chyby personálu apod.) má veľmi závažný (až likvidačný) dopad na procesy a činnosti Spoločnosti, vrátane bezpečnosti. Narušenie integrity bude mať významný vplyv na služby poskytované zákazníkom.

Tab. 2.3: Stupnica pre hodnotenie dostupnosti aktív.

1	Nízka	Narušenie a/alebo strata dostupnosti aktíva nemá žiadny alebo má len zanedbateľný dopad na procesy a služby poskytované Spoločnosťou. Nehrozí finančná strata.
2	Stredná	Narušenie a/alebo strata dostupnosti aktíva môže mať určitý dopad na procesy a služby poskytované Spoločnosťou. Hrozí nízka finančná strata. Výpadok pravdepodobne nebude mať bezprostredný vplyv na služby poskytované zákazníkom.
3	Vysoká	Narušenie a/alebo strata dostupnosti aktíva pravdepodobne bude mať dopad na procesy a služby poskytované Spoločnosťou. Hrozí vysoká finančná strata. Výpadok bude mať pravdepodobne priamy vplyv na služby poskytované zákazníkom.
4	Kritická	Narušenie a/alebo strata dostupnosti aktíva bude mať s vysokou pravdepodobnosťou dopad na procesy a poskytované služby. Hrozia veľmi vysoké finančné straty. Výpadok bude mať takmer určite priamy vplyv na služby poskytované zákazníkom.

Ďalším krokom v priebehu hodnotenia aktív je určenie významnosti daného aktíva. Táto hodnota vyjadruje finančnú hodnotu, resp. význam daného aktíva pre Spoločnosť. Hodnotenie vyjadruje napr. náklady vynaložené v prípade zničenia alebo straty aktíva a jeho následnej obnovy (resp. následného znovuzaobstarania daného aktíva), alebo zahŕňa okrem samotnej hodnoty aktíva aj možné nadväzujúce škody, ktoré sa môžu sekundárne vyskytnúť (napr. pokuty v dôsledku nefunkčnosti daného aktíva). Významnosť aktíva je hodnotená s využitím škály 1 až 4, popis týchto štyroch úrovní prehľadne zobrazuje tab. 2.4.

Tab. 2.4: Stupnica pre hodnotenie významnosti aktív.

1	Nízka	desiatky až stovky tisíc Kč
2	Stredná	jednotky miliónov Kč
3	Vysoká	nižšie desiatky miliónov Kč
4	Kritická	vyššie desiatky miliónov Kč a viac (likvidačné škody)

Výsledná hodnota aktíva reflektuje všetky vyššie popísané parametre, zahŕňa teda hodnotenie dopadov a tiež hodnotu významnosti daného aktíva. Hodnota aktíva sa stanoví podľa vzorca:

$$\text{hodnota aktíva} = \text{hodnotenie dopadu} * \text{významnosť aktíva}, \tag{2.2}$$

kde veličina *„hodnotenie dopadu“* je stanovená aritmetickým priemerom hodnôt pre dôvernosť, integritu a dostupnosť daného aktíva (viď vzťah 2.1).

Väzby medzi primárnymi a podpornými aktívami

Pre potreby správneho identifikovania možných nežiadúcich rizík, ktoré môžu na aktíva pôsobiť, nie je postačujúce uvažovať len tie riziká, ktoré vznikajú (môžu sa prejaviť) priamo na konkrétnych aktívach. Je potrebné uvažovať aj riziká prenesené, tzv. sekundárne riziká majúce pôvod na niektorom z podporných aktív, ktoré je nevyhnutné ďalej pre činnosť aktíva primárneho. Takto vzniknuté riziko sa prejaví následne aj prenesene na primárnom aktíve. Z tohto dôvodu je potrebné identifikovať väzby medzi aktívami reprezentujúce skutočnosť, ktoré podporné (príp. ostatné primárne) aktíva sa podieľajú na činnosti ktorých primárnych aktív.

Takto určené väzby sú hodnotené pomocou štyroch parametrov vyjadrujúcich váhu vplyvu podporného aktíva postupne na všetky parametre primárneho aktíva, a to konkrétne na jeho dôvernosť, dostupnosť, integritu a významnosť. Váha vplyvu je hodnotená na škále 1 až 4, kde nízka hodnota (1) vyjadruje nízky vplyv hodnoteného aktíva na dôvernosť, dostupnosť, integritu alebo významnosť konkrétneho

primárneho aktíva a naopak vysoká hodnota (4) vyjadruje vysoký vplyv hodnoteného aktíva na dôvernosť, dostupnosť, integritu alebo významnosť konkrétneho primárneho aktíva. Príklad mapovania väzieb medzi podpornými a primárnymi aktívami v zjednodušenej podobe zobrazuje tab. 2.5.

Tab. 2.5: Príklad mapovania väzieb medzi primárnymi a podpornými aktívami.

	primárne aktívum 1				primárne aktívum 2			
	C	I	A	V	C	I	A	V
podporné aktívum 1	1	1	1	1	1	1	1	1
podporné aktívum 2	1	1	1	1	1	1	1	1
podporné aktívum 3	2	2	2	2	2	2	2	2
primárne aktívum 1	–	–	–	–	1	1	1	1
primárne aktívum 2	1	1	1	1	–	–	–	–
podporné aktívum 4	2	3	4	3	1	2	2	2

2.1.2 Identifikácia a hodnotenie hrozieb

Ďalším krokom fázy identifikácie rizík je identifikácia možných hrozieb, ktoré môžu nepriaznivým spôsobom ovplyvniť aktíva Spoločnosti. Pre účely identifikácie hrozieb je vytvorený katalóg hrozieb, ktorých pôsobenie je nutné uvažovať, nakoľko ich výskyt je relevantný vzhľadom k prevádzkovaným činnostiam v rámci Spoločnosti. Pri vytváraní katalógu hrozieb (a tiež katalógu zraniteľností, viz kap. 2.1.3) boli vzaté do úvahy už existujúce zdroje, a to konkrétne zoznam hrozieb (a zraniteľností) uvedený vo VoKB [2] a zoznam hrozieb (a zraniteľností) uvedený v norme ISO/IEC 27005 [6], pričom boli vhodne doplnené ďalšími zdrojmi, ktoré reflektujú špecifický kontext činností Spoločnosti, ako je napr. evidencia incidentov Spoločnosti, praktické skúsenosti zamestnancov Spoločnosti, požiadavky a praktické skúsenosti zákazníkov a dodávateľov Spoločnosti atď. Vytvorený katalóg hrozieb je súčasťou prílohy A.2 tejto práce. Identifikované hrozby sú v rámci tohto katalógu rozdelené do niekoľkých kategórií v závislosti na pôvode danej hrozby.

Jednotlivým hrozbám z katalógu hrozieb je pridelená hodnota na základe dvoch parametrov – **pravdepodobnosti výskytu** danej hrozby a **dopadu**, ktorý realizácia danej hrozby pravdepodobne spôsobí. Oba tieto parametre sú hodnotené pomocou 4stupňovej škály. Kategorizácia hodnôt pre parameter pravdepodobnosti vý-

skytu je bližšie popísaná v tab. 2.6 a pre dopad spôsobený danou hrozbou v tab. 2.7. Nízka hodnota (1) predstavuje malú pravdepodobnosť, že sa hodnotená hrozba vyskytne, resp. nízky dopad, ktorý realizácia hrozby spôsobí. Naopak vysoká hodnota (4) predznamenáva veľkú pravdepodobnosť výskytu hrozby, resp. veľký dopad v prípade realizácie danej hrozby. Výsledná hodnota hrozby sa z uvedených dvoch parametrov stanoví podľa vzorca:

$$\text{úroveň hrozby} = \text{pravdepodobnosť hrozby} * \text{dopad hrozby}. \tag{2.3}$$

Tab. 2.6: Stupnica pre hodnotenie pravdepodobnosti hrozby.

1	Nízka	Pravdepodobnosť realizácie hrozby je zanedbateľná, jej výskyt nie je častejší než jedenkrát v priebehu 5 rokov.
2	Stredná	Pravdepodobnosť realizácie hrozby je malá, jej výskyt sa pohybuje v rozpätí od 1 roku do 5 rokov.
3	Vysoká	Pravdepodobnosť realizácie hrozby je vysoká, jej výskyt sa pohybuje v rozpätí od 1 mesiaca do 1 roku.
4	Kritická	Pravdepodobnosť realizácie hrozby je veľmi vysoká až takmer istá, jej výskyt je častejší než jedenkrát v priebehu mesiaca.

Tab. 2.7: Stupnica pre hodnotenie dopadu hrozby.

1	Nízky	Škody v prípade realizácie hrozby sú relatívne nízke a nemajú vplyv na činnosti Spoločnosti.
2	Stredný	Škody v prípade realizácie hrozby sú citeľné, majú istý vplyv na činnosti Spoločnosti, ale môžu byť s vynaložením určitého úsilia a prostriedkov v akceptovateľnom čase odstránené.
3	Vysoký	Škody v prípade realizácie hrozby sú veľké, vo veľkej miere ovplyvňujú činnosti Spoločnosti, ale môžu byť s vynaložením veľkého úsilia a prostriedkov odstránené.
4	Kritický	Škody v prípade realizácie hrozby sú kritické, môžu mať kritický dopad na činnosti Spoločnosti a môžu napr. viesť až k likvidácii Spoločnosti.

Pre každú hrozbu z katalógu hrozieb je tiež určený zdroj hrozby, ktorý danú hrozbu realizuje – udáva informáciu o tom, či má hrozba pôvod v internom prostredí Spoločnosti (tj. vnútorný zdroj) alebo pôsobí z jej vonkajšieho okolia (tj. vonkajší zdroj), príp. môže pôsobiť z oboch oblastí. Ďalej je pre každú hrozbu určený úmysel,

s ktorým zdroj hrozby túto hrozbu realizuje – úmysel poskytuje informáciu o tom, či zdroj hrozby realizuje hrozbu náhodne (tj. náhodný úmysel) alebo naopak zámerne (tj. zámerný úmysel), príp. je prípustná tiež kombinácia.

2.1.3 Identifikácia a hodnotenie zraniteľností

Obdobne ako aj v prípade identifikácie a hodnotenia hrozieb, aj pri tvorbe katalógu zraniteľností boli vzaté do úvahy existujúce štandardy a odporúčania. Vytvorený katalóg zraniteľností je súčasťou prílohy A.3.

Každej zraniteľnosti z katalógu zraniteľností je priradená **úroveň zraniteľnosti**. Táto hodnota reflektuje významnosť danej zraniteľnosti v závislosti na pravdepodobnosti zneužitia tejto zraniteľnosti niektorou z hrozieb. Úroveň zraniteľnosti sa stanovuje podľa 4stupňovej škály, ktorá je bližšie popísaná v tab. 2.8. Nízka hodnota (1) predstavuje malú pravdepodobnosť, že hodnotená hrozba spôsobí v dôsledku zneužitia danej zraniteľnosti vysoký dopad. Naopak vysoká hodnota (4) označuje veľkú pravdepodobnosť úspešnosti hrozby pri zneužití tejto zraniteľnosti.

Tab. 2.8: Stupnica pre hodnotenie úrovne zraniteľnosti.

1	Nízka	Zraniteľnosť vôbec neexistuje nebo nie je podstatná, jej zneužitie niektorou z hrozieb nie je pravdepodobné. Sú zavedené bezpečnostné opatrenia, ktoré sú schopné včas detegovať možné zraniteľnosti alebo prípadné pokusy o ich zneužitie.
2	Stredná	Zraniteľnosť je relatívne podstatná, môže byť zneužitá niektorou z hrozieb, jej zneužitie je málo pravdepodobné až pravdepodobné.
3	Vysoká	Zraniteľnosť je veľmi podstatná, môže byť jednoducho zneužitá niektorou z hrozieb, jej zneužitie je pravdepodobné až veľmi pravdepodobné.
4	Kritická	Zraniteľnosť je kritická, môže byť s vysokou pravdepodobnosťou jednoducho zneužitá niektorou z hrozieb, jej zneužitie je takmer isté.

2.1.4 Väzby hrozby-zraniteľnosti

Pre účely finálneho stanovenia miery rizika je potrebné definovať špecifický kontext, v ktorom je dané riziko hodnotené. Tento kontext zahŕňa nielen jednotlivé identifikované aktíva, hrozby a zraniteľnosti, ale skúma a hodnotí tiež ich vzájomné väzby a relevancie.

Každá zraniteľnosť prispieva svojou prítomnosťou k zvýšeniu pravdepodobnosti výskytu jednej či viacerých hrozieb. Prítomnosť jednotlivých zraniteľností je potrebné vždy hodnotiť vzhľadom ku konkrétnemu kontextu *hrozba-aktívum*, pre ktorý sa miera zraniteľnosti stanovuje. To, ktoré identifikované zraniteľnosti môžu svojou prítomnosťou prispieť k realizácii ktorých hrozieb, je súhrnne zachytené v matici *„Hrozby vs. zraniteľnosti“*, ktorá je súčasťou prílohy A.4. Jej zjednodušená podoba, slúžiaca pre názorné vysvetlenie, je zobrazená v tab. 2.9. Relácie, ktoré sa medzi jednotlivými hrozbami a zraniteľnosťami môžu vyskytnúť, sú nasledujúce:

- „0“ – zraniteľnosť neprispieva k realizácii danej hrozby, alebo
- „1“ – zraniteľnosť prispieva k realizácii danej hrozby.

Tab. 2.9: Matica väzieb hrozby-zraniteľnosti.

	Hrozby:	1. hrozba	2. hrozba	3. hrozba	4. hrozba
Zraniteľnosti:	ID	1	2	3	4
1. zraniteľnosť	1	$V_1H_1 = 1$	$V_1H_2 = 1$	$V_1H_3 = 0$	$V_1H_4 = 1$
2. zraniteľnosť	2	$V_2H_1 = 0$	$V_2H_2 = 1$	$V_2H_3 = 0$	$V_2H_4 = 1$
3. zraniteľnosť	3	$V_3H_1 = 0$	$V_3H_2 = 0$	$V_3H_3 = 0$	$V_3H_4 = 0$
4. zraniteľnosť	4	$V_4H_1 = 1$	$V_4H_2 = 1$	$V_4H_3 = 1$	$V_4H_4 = 0$
	AP:	0,5	0,75	0,25	0,5

2.1.5 Väzby hrozby-aktíva

Každá hrozba, ktorá je súčasťou vytvoreného katalógu hrozieb, môže nežiadúcim spôsobom pôsobiť na jedno alebo viac aktív Spoločnosti. Táto skutočnosť je zachytená v matici *„Hrozby vs. aktíva“*, ktorá je súčasťou prílohy A.5. Jej zjednodušená podoba, slúžiaca pre názorné vysvetlenie, je zobrazená v tab. 2.10. Relácie, ktoré sa medzi jednotlivými hrozbami a aktívami môžu vyskytnúť, sú nasledujúce:

- „0“ – hrozba nemôže nežiadúcim spôsobom pôsobiť na dané aktívum, alebo
- „1“ – hrozba môže nežiadúcim spôsobom pôsobiť na dané aktívum.

2.1.6 Väzby aktíva-zraniteľnosti

Zraniteľnosť predstavuje slabé miesto (vlastnosť) aktíva, ktoré môže byť zneužité hrozbou k uplatneniu jej nežiadúceho vplyvu, tj. k realizácii rizika. Všetky možné zraniteľnosti jednotlivých aktív, ktoré sú zahrnuté vo vytvorenom katalógu zraniteľností, nemusia byť vždy zákonite relevantné pre všetky aktíva Spoločnosti. To, ktoré

Tab. 2.10: Matica väzieb hrozby-aktíva.

	Hrozby:	1. hrozba	2. hrozba	3. hrozba	4. hrozba
Aktíva:	ID	1	2	3	4
1. aktívum	1	$A_1H_1 = 1$	$A_1H_2 = 1$	$A_1H_3 = 1$	$A_1H_4 = 0$
2. aktívum	2	$A_2H_1 = 0$	$A_2H_2 = 1$	$A_2H_3 = 0$	$A_2H_4 = 1$
3. aktívum	3	$A_3H_1 = 1$	$A_3H_2 = 1$	$A_3H_3 = 0$	$A_3H_4 = 0$
4. aktívum	4	$A_4H_1 = 0$	$A_4H_2 = 1$	$A_4H_3 = 1$	$A_4H_4 = 0$

spomedzi uvedených zraniteľností sú relevantné pre konkrétne hodnotené aktívum Spoločnosti (resp. ktoré z nich sa môžu vyskytnúť na určitom aktíve), je zachytené v matici *„Aktíva vs. zraniteľnosti“*, ktorá je súčasťou prílohy A.6. Jej zjednodušená podoba, slúžiaca pre názorné vysvetlenie, je zobrazená v tab. 2.11. Relácie, ktoré sa medzi jednotlivými aktívami a zraniteľnosťami môžu vyskytnúť, sú nasledujúce:

- „0“ – zraniteľnosť nie je relevantná (nemôže sa objaviť) pre dané aktívum, alebo
- „1“ – zraniteľnosť je relevantná (môže sa objaviť) pre dané aktívum.

Tab. 2.11: Matica väzieb aktíva-zraniteľnosti.

	Zraniteľnosti:	1. zraniteľnosť	2. zraniteľnosť	3. zraniteľnosť	4. zraniteľnosť
Aktíva:	ID	1	2	3	4
1. aktívum	1	$A_1V_1 = 0$	$A_1V_2 = 1$	$A_1V_3 = 0$	$A_1V_4 = 0$
2. aktívum	2	$A_2V_1 = 0$	$A_2V_2 = 0$	$A_2V_3 = 1$	$A_2V_4 = 0$
3. aktívum	3	$A_3V_1 = 1$	$A_3V_2 = 1$	$A_3V_3 = 0$	$A_3V_4 = 1$
4. aktívum	4	$A_4V_1 = 0$	$A_4V_2 = 1$	$A_4V_3 = 1$	$A_4V_4 = 1$

2.1.7 Stanovenie miery rizika

Ďalším krokom analýzy rizík je určenie hodnoty identifikovaných rizík – hovoríme preto o stanovení hodnoty tzv. **miery rizika**, ktorá udáva veľkosť identifikovaného rizika. Miera rizika sa vždy určuje pre špecifický hodnotený kontext *hrozba-aktívum*, pričom táto veličina reflektuje:

- **hodnotu aktíva** (stanovenú v závislosti na parametroch hodnotenia dopadov a významnosti daného aktíva pre Spoločnosť),
- **úroveň hrozby**, v dôsledku pôsobenia ktorej sa riziko prejaví,
- **väzby medzi hrozbou a zraniteľnosťami**, tj. aké zraniteľnosti môžu byť zneužité danou hrozbou k uplatneniu jej nežiadúceho vplyvu, a tým prispieť ku zvýšeniu pravdepodobnosti realizácie tejto hrozby,
- **väzby medzi aktívom a zraniteľnosťami**, tj. aké zraniteľnosti sú relevantné (môžu sa objaviť) pre konkrétne hodnotené aktívum,
- **úroveň každej zraniteľnosti**, ktorá je pre hodnotený kontext *hrozba-aktívum* relevantná, a tak sa určitým spôsobom podieľa na zvyšovaní výslednej miery rizika.

Miera zraniteľnosti

Ďalšou z veličín, ktorú je potrebné pre stanovenie výslednej miery rizika určiť, je **miera zraniteľnosti**. Táto veličina určuje pre každý hodnotený kontext *hrozba-aktívum* pôsobenie všetkých zraniteľností, ktoré sú pre daný kontext relevantné. Miera zraniteľnosti v sebe zahŕňa:

- **väzby** konkrétneho hodnoteného **aktíva so všetkými zraniteľnosťami** uvedenými v katalógu zraniteľností, tj. ktoré z týchto zraniteľností sú pre dané posudzované aktívum relevantné a môžu sa teda na ňom objaviť,
- a tiež **väzby** konkrétnej hodnotenej **hrozby so všetkými zraniteľnosťami** z katalógu zraniteľností, tj. aké zraniteľnosti môžu byť danou hrozbou zneužité k realizácii rizika.

Miera zraniteľnosti sa vypočíta ako skalárny súčin:

- všetkých hodnôt z matice *„Hrozby vs. zraniteľnosti“* relevantných pre danú hrozbu v hodnotenom kontexte,
- a súčinu všetkých hodnôt z matice *„Aktíva vs. zraniteľnosti“* relevantných pre dané aktívum v hodnotenom kontexte a hodnôt úrovne zraniteľnosti pre všetky relevantné zraniteľnosti.

Výsledok skalárneho súčinu je následne násobený hodnotou udávajúcou aritmetický priemer výskytov hodnôt „1“ z matice *„Hrozby vs. zraniteľnosti“* v príslušnom stĺpci pre danú hodnotenú hrozbu.

Pre kontext napr. *druhá hrozba-prvé aktívum* by bola miera zraniteľnosti vypočítaná nasledovne:

$$\begin{aligned}\text{miera zraniteľnosti } H_2A_1 = [&V_1H_2 * (A_1V_1 * \text{úroveň zraniteľnosti } V_1)+\\ &+ V_2H_2 * (A_1V_2 * \text{úroveň zraniteľnosti } V_2)+\\ &+ V_3H_2 * (A_1V_3 * \text{úroveň zraniteľnosti } V_3)+\\ &+ V_4H_2 * (A_1V_4 * \text{úroveň zraniteľnosti } V_4)] * 0,75 \end{aligned} \quad (2.4)$$

Spôsob kalkulácie miery rizika

Miera rizika sa vypočíta pre každý hodnotený kontext *hrozba-aktívum* zvlášť, pričom táto hodnota v sebe zahŕňa:

- **mieru zraniteľnosti** pre konkrétny kontext *hrozba-aktívum* stanovenú podľa postupu popísanom v kap. 2.1.7,
- **hodnotu aktíva** stanovenú podľa postupu popísanom v kap. 2.1.1,
- **úroveň hrozby** stanovenú podľa postupu popísanom v kap. 2.1.2,
- **hodnotu parametru** A_xH_y, ktorý je relevantný pre hodnotený kontext *hrozba-aktívum*.

Miera rizika sa potom stanoví ako súčin vyššie uvedených veličín, a to nasledovne (pre príklad hodnotenia kontextu *druhá hrozba-prvé aktívum*):

$$\begin{aligned}\text{miera rizika } H_2A_1 = \text{miera zraniteľnosti } H_2A_1 * \text{hodnota aktíva } A_1 *\\ * \text{úroveň hrozby } H_2 * A_1H_2 \end{aligned} \quad (2.5)$$

Pre účely následnej kategorizácie ohodnoteného rizika do jednotlivých úrovní závažnosti v závislosti na miere rizika (stanovenej podľa vzťahu 2.5) je vypočítaná hodnota vo výsledku dodatočne podelená hodnotou 16, a to aj vzhľadom k skutočnosti, že vstupné parametre *„hodnota aktíva“* a *„úroveň hrozby“* môžu dosahovať maximálne možné ohodnotenie 16, zatiaľ čo *„úroveň zraniteľnosti“* je hodnotená iba na škále v rozmedzí 1 až 4.

2.1.8 Kategorizácia rizík

Výsledné riziko je v závislosti na dosiahnutej hodnote určujúceho parametra *„miera rizika“* zaradené do jednej z kategórií, ktoré vyjadrujú mieru rizika v 4stupňovej škále. Tieto úrovne odpovedajú slovnému popisu nízke, stredné, vysoké a kritické riziko. Mapovanie hodnôt miery rizika do príslušných úrovní (kategórií), spoločne s popisom navrhovaného postupu s prihliadnutím na akceptovateľnosť daného rizika, je prehľadne zobrazené v tab. 2.12.

Tab. 2.12: Výsledná kategorizácia rizík v závislosti na miere rizika.

Kategória rizika		Akceptovateľnosť rizika	Miera rizika
1	Nízke	Riziko je považované za akceptovateľné.	< 15
2	Stredné	Riziko môže byť znížené menej náročnými opatreniami alebo v prípade vyššej náročnosti opatrení je riziko akceptovateľné.	15 – 70
3	Vysoké	Riziko je dlhodobo neprípustné a musia byť zahájené systematické kroky k jeho odstráneniu.	70 – 375
4	Kritické	Riziko je neprípustné a musia byť okamžite zahájené kroky k jeho odstráneniu.	> 375

V priebehu analýzy rizík vykonanej za účelom ohodnotenia stavu bezpečnosti informácií v prostredí Spoločnosti bolo identifikovaných celkom 35 rizík. Všetky tieto riziká boli ohodnotené podľa postupu, ktorý bol podrobne popísaný v tejto kapitole. Kompletný prehľad identifikovaných rizík, spoločne s ich ohodnotením (stanovenou max. hodnotou – mierou rizika) a následnou kategorizáciou do príslušnej úrovne závažnosti, je súčasťou prílohy A.7.

2.1.9 Ošetrenie rizík

Neodmysliteľnou súčasťou riadenia rizík informačnej bezpečnosti je návrh opatrení za účelom odstránenia nedostatkov zistených vykonanou analýzou, ktorý je realizovaný ako ďalší krok procesu po ukončení komplexného posúdenia a vyhodnotenia rizík. S cieľom eliminovať, či aspoň minimalizovať jednotlivé riziká je vypracovaný **Plán zvládania rizík** obsahujúci zoznam navrhovaných bezpečnostných opatrení, ktorých zavedenie a následné udržiavanie by malo viesť k zmierneniu, v ideálnom prípade až k odstráneniu nežiadúcich dopadov identifikovaných rizík.

Kompletný Plán zvládania rizík, ktorý bol vytvorený za účelom poskytnutia výstupov z vykonanej analýzy rizík pre potreby v rámci Spoločnosti, je súčasťou prílohy A.8.

2.2 Aplikácia pre zobrazenie výsledkov analýzy rizík

Ďalšou hlavnou súčasťou praktickej časti tejto záverečnej práce je návrh a následná implementácia aplikácie umožňujúcej prehľadným spôsobom zobraziť a prezentovať výsledky analýzy rizík informačnej bezpečnosti realizovanej podľa navrhnutej metodiky, ktorá bola predstavená a podrobne popísaná v kap. 2.1.

Aplikácia je realizovaná v podobe webovej aplikácie[2] a v čase písania tejto práce je dostupná na adrese: `https://xvoska00.github.io/sp-analyza-rizik`.

2.2.1 Vlastný návrh webovej aplikácie

Spôsob implementácie aplikácie ako nástroja pre prezentáciu výstupov z analýzy rizík v podobe práve webovej aplikácie bol zvolený z dôvodu osobných skúseností autorky s implementáciou tohto typu aplikácií a taktiež z dôvodu, že pre účely prezentácie výsledkov sa jedná o efektívny nástroj, ktorý umožňuje jednoduchým spôsobom pracovať s dátami analýzy a ktorý spĺňa všetky požiadavky potrebné pre ich následnú prezentáciu.

Pred zahájením samotnej implementácie aplikácie bolo potrebné najskôr vytvoriť ideový návrh funkčnosti vyvíjanej aplikácie, ktorého hlavnou podstatou je uchopenie základnej predstavy o tom:

- akým spôsobom bude aplikácia získavať potrebné dáta,
- akým spôsobom prebehne spracovanie týchto dát a
- akým spôsobom bude aplikácia tieto dáta zobrazovať.

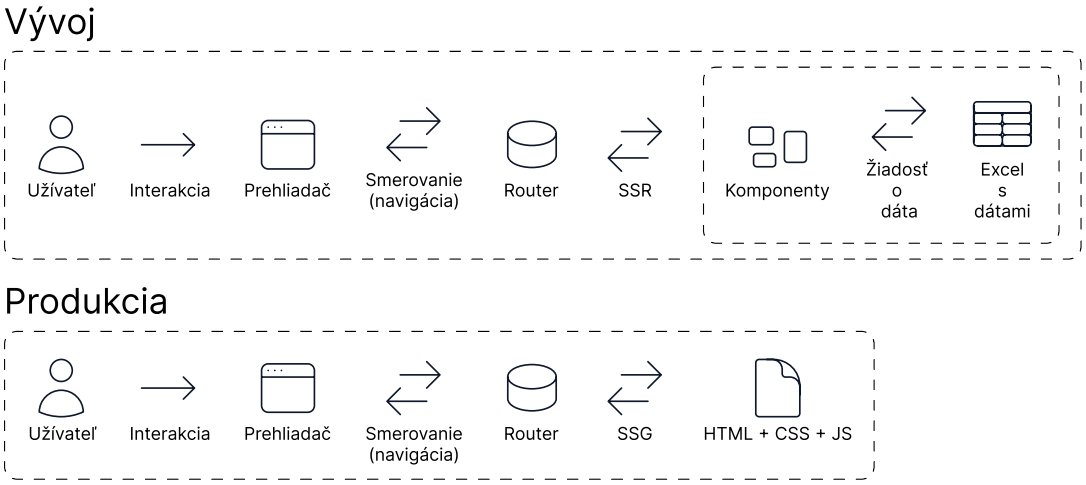
Výstupy z vykonanej analýzy rizík, ktoré majú byť s využitím aplikácie prehľadným spôsobom prezentované, sú spracované v excelovskom formáte `.xlsx`, vďaka čomu nebolo potrebné do funkčného modelu zakomponovať pripojenie k databáze údajov. Pre účely zobrazenia výsledkov je teda postačujúce načítať vopred spracované dáta z už existujúceho súboru.

Ďalším parametrom, ktorý bolo potrebné zvážiť, bol vhodný spôsob zobrazenia zaznamenaných dát. Nakoľko sa nejedná o dynamické dáta, ale o dáta statické, ktorých obsah počas ich spracovania aplikáciou nemôže byť na základe interakcie s užívateľom aplikácie zmenený, bolo možné vygenerovať statické stránky[3], k čomu musel byť zvolený vhodný framework. Vybrané nástroje a použité knižnice potrebné

[2]Webová aplikácia je vytvorená v českom jazyku z dôvodu, že bola vyvíjaná pre interné potreby Spoločnosti, pre ktorú autorka v čase písania tejto práce vykonávala pracovnú činnosť.

[3]Statická webová stránka sa skladá z pevného nemenného obsahu, ktorý nie je možné zmeniť vplyvom užívateľskej interakcie. Všetky dáta, ktoré statická webová stránka využíva, resp. zobrazuje, sú pevné a nemenné v čase. V porovnaní s dynamickými webovými stránkami sú statické stránky jednouchšie na implementáciu, ich načítanie prebieha v znateľne kratšom čase, ale ich nevýhodou je obmedzená možnosť interaktivity a personalizácie pre užívateľa.

pre dosiahnutie tejto funkcionality, spoločne s odôvodnením ich výberu, budú bližšie popísané v nasledujúcej kap. 2.2.2. Vlastný návrh funkčnosti webovej aplikácie je schematicky zobrazený na obr. 2.1, popis nasleduje.



Obr. 2.1: Návrh implementácie webovej aplikácie.

Nakoľko bol pre implementáciu aplikácie zvolený framework Next.js umožňujúci generovať statické stránky, je možné definovať rozdiel v prejavoch aplikácie počas jej vývoja a následne jej finálnou verziou nasadenou do produkčného prostredia. Rozdiel medzi vývojom a finálnou verziou je následujúci:

- **Vývoj** – počas vývoja aplikácie nie sú externé dáta (prijímané `.xlsx` dáta) súčasťou aplikácie, ale sú získavané dynamicky, a to po zadaní požiadavky na ich zobrazenie, ktorá vzniká pri navigácií na konkrétnu stránku webovej aplikácie[4]. Využíva sa SSR (*Server-Side Rendering*), čo znamená, že k získaniu dát a ich zobrazeniu dochádza na strane serveru a následne je na stranu klienta posielaný kompletný HTML kód obsahujúci dáta potrebné k zobrazeniu na aktuálnej stránke.
- **Finálna verzia** – v produkčnej fáze využíva vytvorená webová aplikácia plne nasadená do bežiaceho prostredia staticky generované stránky, ktoré vznikajú vďaka použitiu SSG (*Static-Site Generation*). Jedná sa o proces, v priebehu ktorého sú webové stránky pomocou build procesu[5] dopredu vygenerované so všetkými potrebnými dátami vo forme statických HTML súborov (je vytvorený

[4]V rámci webovej aplikácie existuje niekoľko rôznych stránok, medzi ktorými je užívateľovi umožnená navigácia. Každá z týchto stránok si pre svoje potreby (tj. na základe toho, čo má byť zobrazeným obsahom na konkrétnej stránke) získava z Excelu pre seba relevantné dáta.

[5]Build proces vo frameworku Next.js je proces, počas ktorého dochádza ku kompletnému „zostaveniu“ jednotlivých stránok webovej aplikácie. Pre každú takúto stránku sa vopred vytvárajú statické súbory. Počas build procesu sa každá stránka vyplní potrebnými dátami z `.xlsx` súboru s dátami z vykonanej analýzy.

kompletný HTML kód), čím sa stávajú „predpripravenými“ k zobrazeniu. Keď užívateľ pristúpi na konkrétnu stránku, obdrží kompletný HTML kód, ktorý obsahuje všetky potrebné dáta k zobrazeniu už takto vopred vygenerovanej stránky, žiadne dáta nie je potrebné dodatočne rendrovať[6] za behu aplikácie. Tento prístup prináša rýchlejšiu odozvu celej aplikácie.

2.2.2 Použité nástroje

Táto podkapitola obsahuje predstavenie nástrojov, ktoré boli použité pri implementácii webovej aplikácie, spoločne s odôvodnením výberu jednotlivých nástrojov.

Next.js

Pre vytvorenie základnej podoby a štruktúry webovej stránky bol využitý framework Next.js [28], ktorý využíva javascriptovú knižnicu React [29]. Autorka sa rozhodla pre využitie tohto frameworku na základe skúseností s Reactom, pomocou ktorého sa rozhodla už v minulosti realizovať taktiež implementáciu praktického výstupu k svojej záverečnej bakalárskej práci, a tiež z dôvodu, že tento framework umožňuje jednoduché vytváranie viacstránkovej aplikácie a ďalej umožňuje jednotlivé stránky generovať staticky alebo tiež dynamicky, v prípade potreby, pričom je tieto prístupy možné kombinovať.

Vytvorená webová aplikácia aktuálne využíva staticky generované stránky, avšak do budúcnosti sa otvárajú možnosti rozšírenia funkcionality o dynamické stránky (napr. vloženie vlastného súboru s vytvorenou analýzou užívateľom).

Tailwind CSS

Tailwind CSS [30] predstavuje open source framework, ktorý umožňuje jednoduchým spôsobom dotvárať vizuálnu stránku vytváranej webovej aplikácie pomocou vopred preddefinovaných CSS[7] tried. Výber tohto frameworku bol založený na skutočnosti, že jeho použitie umožňuje rýchlejší vývoj aplikácie a tiež lepšiu prehľadnosť.

XLSX

Balíček XLSX [31] je nástroj umožňujúci pracovať so súbormi (tabuľkami) vytvorenými v programe Microsoft Excel. Pre potreby vytvorenia webovej aplikácie bolo nutné nájsť použiteľný balíček, ktorý umožní čítať súbory s príponou `.xlsx`.

[6] „Rendrovanie“ je pojem označujúci proces, v rámci ktorého dochádza k načítaniu a spusteniu napísaného HTML kódu aplikácie, jeho následnej kompilácií a finálnemu zobrazeniu v takej podobe, ktorá je vo výsledku zobrazená užívateľovi webovej stránky na obrazovke a s ktorou môže tento užívateľ určitým spôsobom interagovať.

[7] Z angl. *Cascading Style Sheet*.

Chart.js

Chart.js [32] je javascriptová knižnica, pomocou ktorej je možné vytvárať grafické zobrazenia rôznych druhov a typov. Súčasťou vytvorenej webovej aplikácie je tiež graf zobrazujúci kategorizáciu identifikovaných rizík, a tak bolo potrebné pre tieto účely nájsť vhodný nástroj, ktorý uľahčí pri programovaní prácu s grafmi.

2.2.3 Štruktúra webovej stránky

Implementovaná webová aplikácia bola vytvorená s využitím knižnice React, ktorej jednou zo základných charakteristík je možnosť práce s tzv. **komponentami**. Jedná sa o určitú nezávislú, samostatnú časť kódu aplikácie, ktorú možno v rámci celého kódu opakovane využívať, a ktorá rozdeľuje výsledné užívateľské rozhranie na menšie dielčie súčasti.

Využitie komponent pri implementácii webovej aplikácie ako praktického výstupu k tejto záverečnej práci sa javilo ako veľmi výhodné, a to najmä z toho dôvodu, že jednotlivé stránky, ktoré webová aplikácia obsahuje a následne užívateľovi zobrazuje, obsahujú častokrát rovnaké, resp. veľmi podobné prvky, ktoré môžu byť v rámci kódu implementované rovnakým spôsobom. Pokiaľ by komponenty využité neboli, vo výslednom kóde aplikácie by vzniklo veľké množstvo zbytočných duplicitných riadkov, ktoré prakticky nie sú potrebné. Hlavnou výhodou použitia komponent je teda to, že je postačujúce definovať ich základnú štruktúru v rámci kódu iba jedenkrát. Následne môžu byť takto preddefinované komponenty opakovane využité v rôznych miestach aplikácie, príp. ďalej rozvíjané či doplnené o ďalšie potrebné prvky, podľa aktuálnych potrieb a konkrétneho spôsobu ich využitia v danom mieste aplikácie.

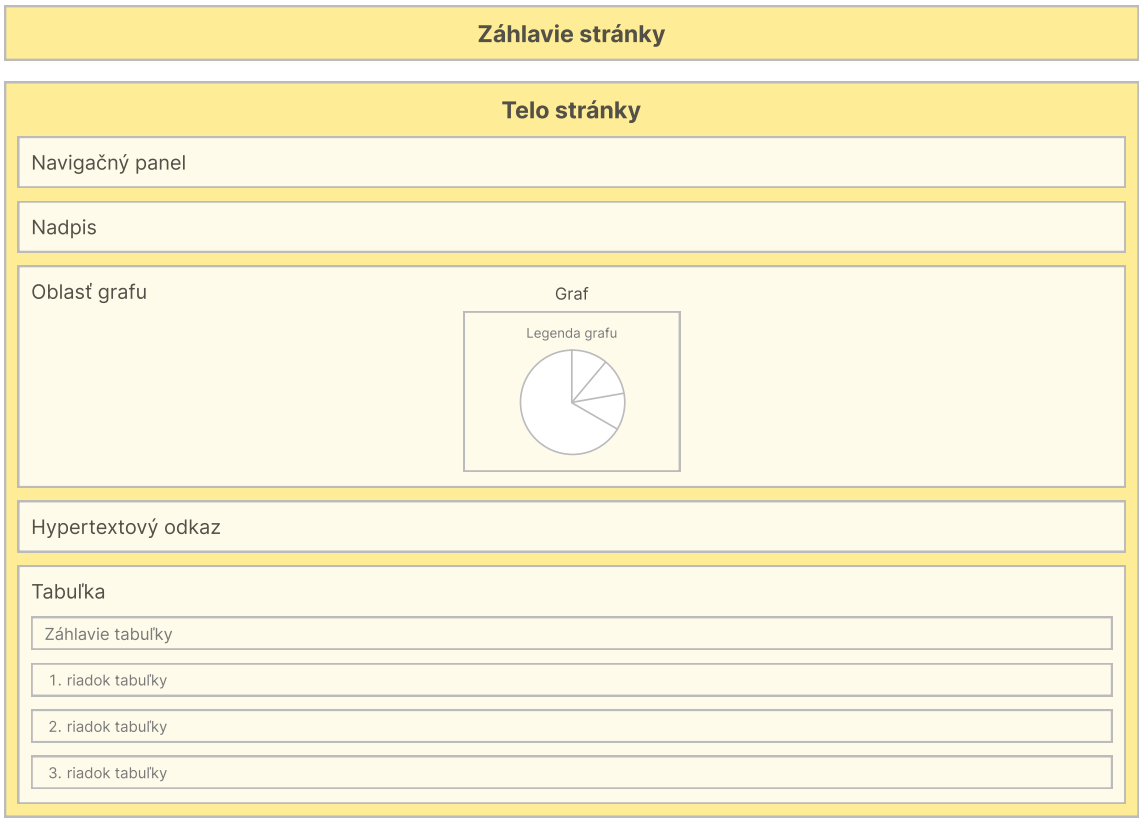
Pre implementáciu aplikácie bol zvolený spôsob členenia kódu a s tým súvisiaceho delenia použitých komponent na:

- **atómy** – predstavujú „najmenšie“, ďalej už nedeliteľné časti kódu aplikácie,
- **molekuly** – jedná sa o komplexnejšie komponenty, ktoré sú zložené z dielčích menších, už definovaných komponent, konkrétne z viacerých atómov a/alebo iných molekúl.

Jednotlivé webové stránky[8], na ktoré môže užívateľ v prostredí webovej aplikácie pristupovať, sú „zostavené“ z vytvorených komponent. Pri implementácii webovej aplikácie bolo definovaných spolu 29 rôznych komponent. Nie je však pravidlom, že pre zobrazenie každej z webových stránok musia byť zákonite využité všetky komponenty. Vždy sú využité len tie z nich, ktoré sú potrebné s prihliadnutím na obsahovú náplň zobrazovanú konkrétnou stránkou.

[8]Tieto webové stránky, resp. ich ukážky, sú zaznamenané v rámci nasledujúcej kap.2.2.4.

Pre jednu z dostupných webových stránok bol vytvorený zjednodušený diagram usporiadania jednotlivých blokov, v rámci ktorých je udržiavaný zobrazovaný obsah. Tento diagram je znázornený na obr. 2.2.



Obr. 2.2: Rozloženie komponent do základnej štruktúry stránky.

Základnú štruktúru každej stránky je možné rozdeliť na dve základné časti:

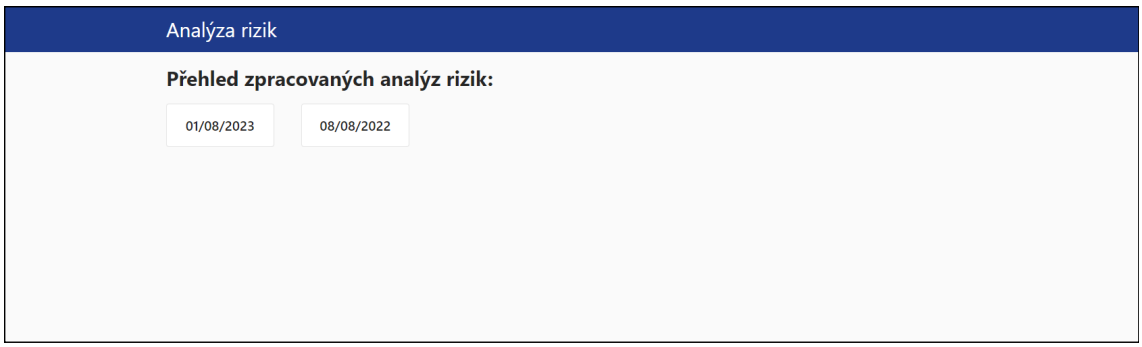
- **záhlavie** stránky a
- **telo** stránky, v rámci ktorého je udržiavaný obsah špecifický pre konkrétnu stránku.

Jedinečnosť obsahu na jednotlivých stránkach determinuje použitie a rozloženie komponent potrebných pre zostavenie konkrétnej stránky. Zobrazený diagram (obr. 2.2) reprezentuje stránku obsahujúcu výpis identifikovaných rizík[9]. Jednotlivé bloky tejto stránky, ktoré sú v uvedenom diagrame znázornené, sú ďalej zložené z jednej či viacerých komponent (či už atómov alebo molekúl) – pre zjednodušenie názornej ukážky však nebola štruktúra stránky zachytená v rámci uvedeného diagramu rozčlenená až do úplných podrobností.

[9]Skutočná podoba tejto stránky je zachytená na obr. 2.4.

2.2.4 Ukážka webovej aplikácie

Na úvodnej stránke vytvorenej webovej aplikácie je zobrazený prehľad spracovaných analýz rizík[10], viď obr. 2.3. Užívateľ si môže kliknutím na príslušný dátum vybrať ľubovoľnú analýzu, ktorej skúmaniu sa chce ďalej venovať.



Obr. 2.3: Úvodná stránka webovej aplikácie.

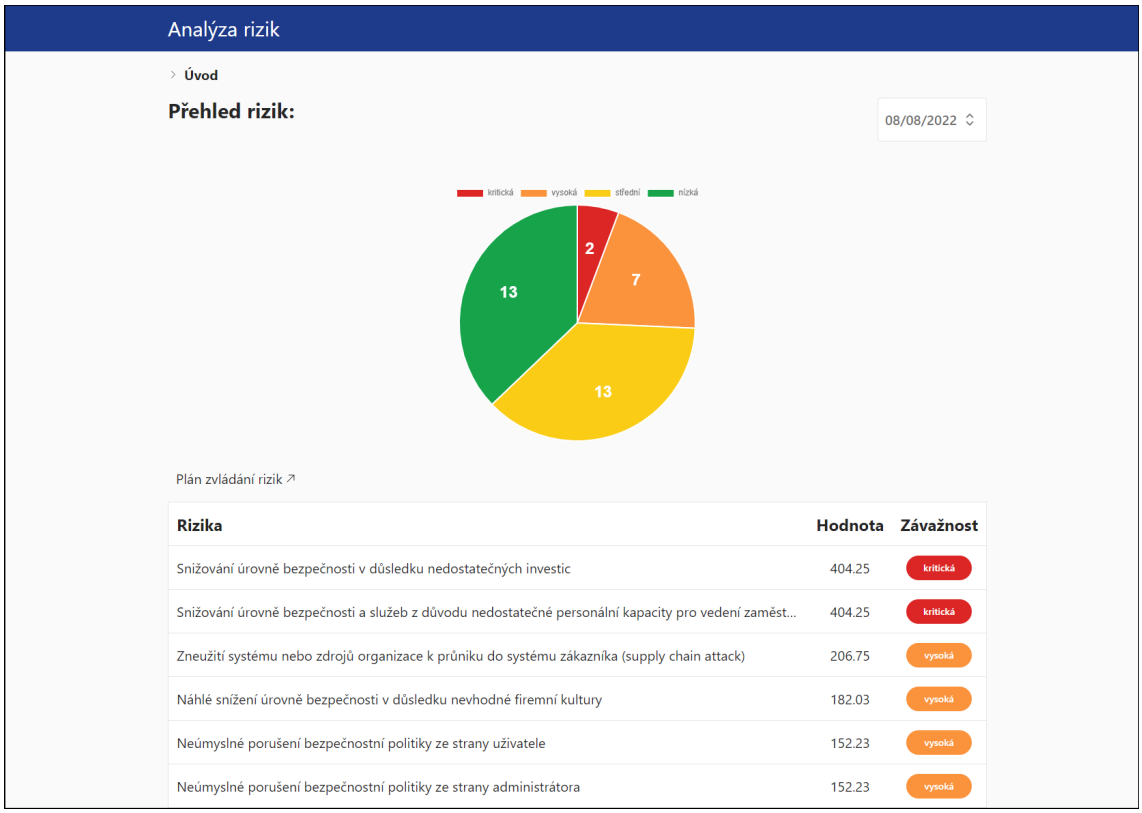
Po kliknutí na niektorý z ponúkaných dátumov vykonaných analýz je užívateľ presmerovaný na ďalšiu stránku, na ktorej je zobrazený výpis identifikovaných rizík usporiadaných zostupne na základe ich hodnoty (miery) a kategórie závažnosti, a to konkrétne od kritickej závažnosti, postupne cez vysokú, strednú, až nakoniec nízku závažnosť rizika. Súčasťou tejto stránky aplikácie je aj graf názorne zobrazujúci rozloženie identifikovaných rizík do jednotlivých kategórií na základe úrovne ich závažnosti[11]. Zobrazený graf zároveň funguje ako filter – po kliknutí do príslušnej časti grafu je možné zobraziť len tie riziká, ktoré spadajú do vybranej kategórie závažnosti. Náhľad stránky je zobrazený na obr. 2.4.

Kliknutím na ľubovoľné riziko zo zoznamu identifikovaných rizík sa užívateľovi zobrazí stránka reprezentujúca „kartu vybraného rizika“ (viď obr. 2.5). Na tejto stránke sú prehľadným spôsobom zobrazené všetky dôležité informácie týkajúce sa daného rizika, a to konkrétne:

- názov rizika,
- popis hrozby, ktorá svojím pôsobením dané riziko generuje,
- dátum vykonania analýzy, v rámci ktorej bolo dané riziko identifikované,

[10] V čase odovzdania tejto práce umožňuje aplikácia užívateľovi výber z dvoch spracovaných analýz, ku ktorým sú všetky príslušné údaje zaznamenané vo východzom `.xlsx` súbore, z ktorého si aplikácia získava potrebné dáta pre zobrazenie. Skutočné a kompletné výstupy z vykonanej analýzy rizík pre potreby Spoločnosti sú obsiahnuté v analýze s označením ‘08-08-2022’. Druhá analýza, tj. analýza s označením ‘01-08-2023’, slúži len ako ukážkový príklad pre demonštráciu možnosti výberu a zobrazenia výstupov z rôznych analýz, hodnoty tejto analýzy nie sú relevantné a nereflektujú skutočné výstupy z vykonanej analýzy rizík.

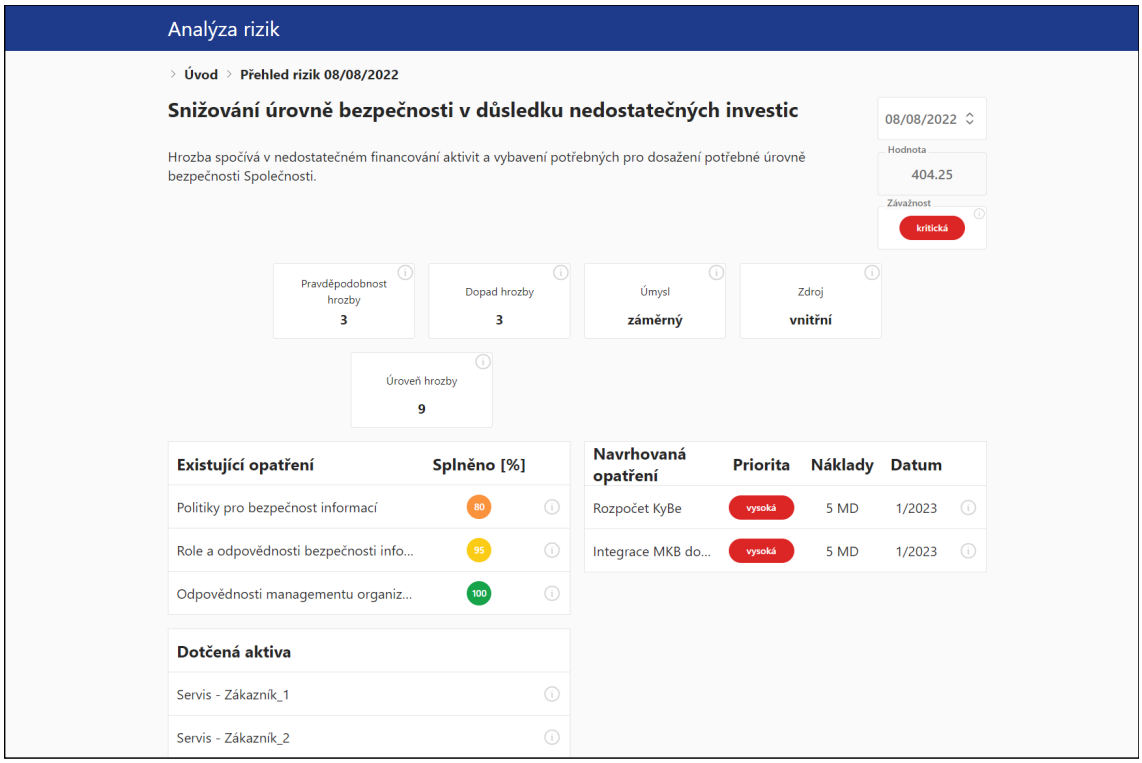
[11] Rozdelenie rizík do príslušných kategórií na základe ich hodnoty (miery rizika) a stanovenej úrovne závažnosti odpovedá kategorizácií uvedenej v tab. 2.12.



Obr. 2.4: Stránka zobrazujúca jednotlivé riziká identifikované v rámci analýzy.

- hodnota identifikovaného rizika zistená vykonanou analýzou,
- kategorizácia rizika do príslušnej úrovne závažnosti na základe hodnoty (miery) tohto rizika,
- hodnoty pravdepodobnosti a miery dopadu hrozby zistené v rámci analýzy,
- úroveň danej hrozby stanovenú z predošlých dvoch parametrov podľa postupu popísanom v kap. 2.1.2,
- zdroj hrozby, tj. či má hrozba pôvod v internom prostredí alebo pôsobí z jej vonkajšieho okolia,
- úmysel danej hrozby, tj. či zdroj hrozby realizuje túto hrozbu náhodne alebo naopak zámerne,
- existujúce opatrenia, ktoré sú implementované proti pôsobeniu danej hrozby, spoločne s percentuálnou hodnotou vyjadrujúcou mieru ich plnenia,
- navrhované opatrenia, ktorých návrh a očakávaná implementácia predstavuje výstup z vykonanej analýzy rizík (tzv. Plán zvládania rizík),
- zoznam dotknutých aktív, ktoré sú v dôsledku nepriaznivého pôsobenia danej hrozby ovplyvnené v najväčšej miere.

Náhľad stránky zobrazujúci detailné informácie o jednom z identifikovaných rizík je zobrazený na obr. 2.5.



Obr. 2.5: Stránka zobrazujúca kartu identifikovaného rizika.

Poslednou dostupnou stránkou vytvorenej webovej aplikácie, ktorá má v rámci prezentácie výsledkov analýzy rizík zásadný význam, je stránka obsahujúca náhľad Plánu pre zvládanie rizík, viď obr. 2.6. Tento Plán obsahuje zoznam opatrení, ktoré je nutné, resp. vhodné implementovať za účelom eliminácie nedostatkov (resp. rizík) zistených vykonanou analýzou. Pre každé z navrhovaných opatrení sú ďalej na tejto stránke webovej aplikácie zobrazené nasledujúce informácie:

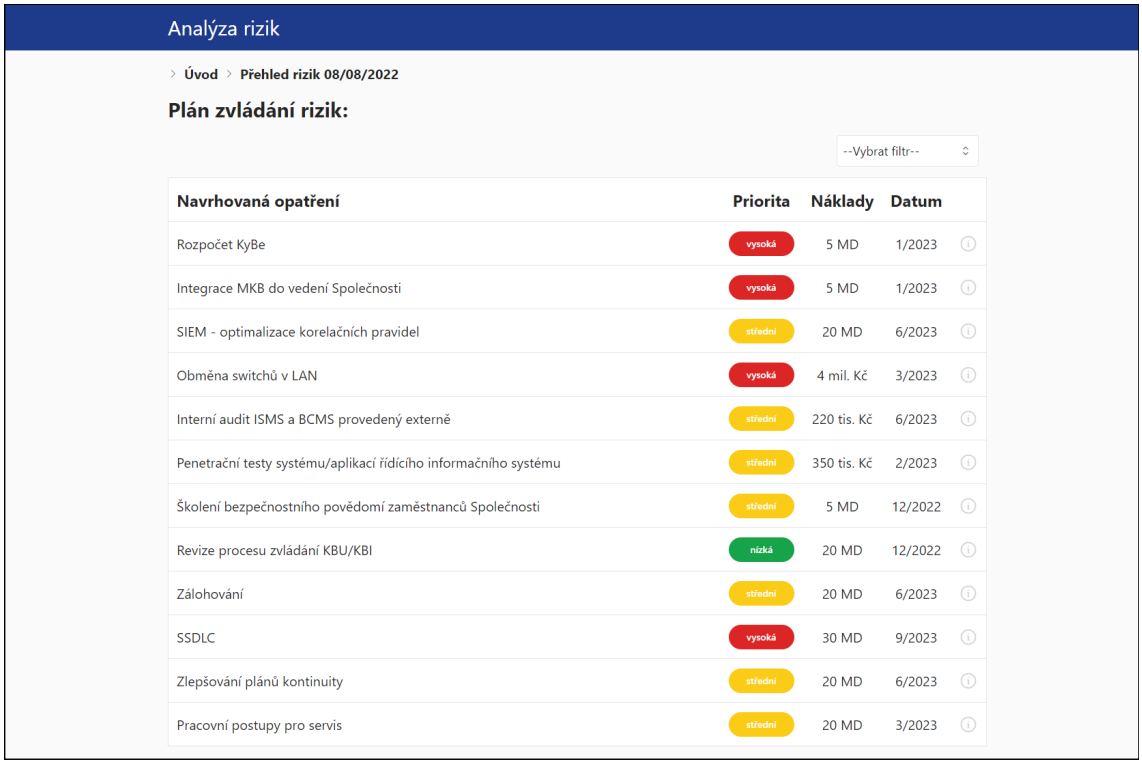
- priorita[12] – definuje nutnosť zavedenia navrhovaného opatrenia s prihliadnutím na závažnosť rizika, ktoré má byť vďaka zavedeniu tohto opatrenia zmiernené, v ideálnom prípade úplne eliminované,
- náklady[13] – definujú náklady spojené so zaobstaraním, príp. návrhom, následným zavedením a udržiavaním navrhovaného opatrenia,

[12]Spravidla platí, že pre riziká spadajúce do kategórie závažnosti „kritické“ sú navrhované opatrenia s prioritou „vysoká“, ďalej pre riziká zaradené do nižšej kategórie závažnosti sú navrhované opatrenia, ktorých zavedenie má nižšiu prioritu atď.

[13]Náklady môžu byť vyčíslené buď v jednotkách Kč, alebo v tzv. „človeko-dňoch“ (skrátene MD – z angl. *Man-day*). Táto jednotka vyjadruje pracovný čas jednej osoby odpovedajúci jednému pracovnému dňu, typicky 8 hodín. Definuje tiež množstvo nákladov potrebných na finančné ohodnotenie jedného zamestnanca vykonávajúceho určitú pracovnú činnosť po dobu jedného pracovného dňa. V rámci Spoločnosti, pre ktorú bol uvedený Plán zvládania rizík ako výstup z analýzy rizík vytvorený, sú definované v rozpočte kybernetickej bezpečnosti pre aktuálny kalendárny rok sadzby interných nákladov za 1 MD, a to konkrétne v hodnote odpovedajúcej približne čiastke 7 000 Kč.

- dátum – definuje časové rozmedzie, v rámci ktorého by malo byť navrhované opatrenie zavedené a účinné.

V uvedenom zozname navrhovaných opatrení je možné taktiež filtrovať tieto opatrenia, a to podľa vyššie uvedených vlastností – ich priority, potrebných nákladov alebo očakávaného dátumu zavedenia. Užívateľ môže vďaka tejto funkcionalite získať názornejšiu predstavu o tom, ktoré opatrenia sú napr. kritické (z pohľadu ich priority) alebo do zavedenia ktorých opatrení bude potrebné investovať najväčšie množstvo finančných prostriedkov (množstvo nákladov) apod.



Obr. 2.6: Stránka zobrazujúca Plán zvládania rizík.

2.3 Kontrolný zoznam pre vykonanie auditu kybernetickej bezpečnosti podľa VoKB

Súčasťou procesov riadenia bezpečnosti informácií sú nepochybne aj činnosti zamerané na overovanie účinnosti a efektívnosti nasadených bezpečnostných opatrení, ktorých hlavnou úlohou je zvyšovať úroveň bezpečnosti prevádzkovaných informačných systémov a sietí. Povinné subjekty podľa ZoKB majú za úlohu implementovať vhodné technické a organizačné opatrenia, aby bolo možné zaistiť dostatočnú úroveň informačnej a kybernetickej bezpečnosti. Za účelom overenia, či sú požadované bezpečnostné opatrenia implementované a či je pomocou týchto opatrení možné zaistiť a udržiavať požadovanú úroveň bezpečnosti, je nutné vykonať audit plnenia a dodržiavania jednotlivých bezpečnostných opatrení.

V rámci tejto kapitoly bude definovaný kompletný zoznam auditných položiek, ktorý môže slúžiť ako podklad pre vykonanie kontrolného auditu bezpečnostných opatrení, ktorých plnenie vyžaduje VoKB [2]. Kontrolný zoznam bol vytvorený na základe jednotlivých ustanovení VoKB, aby bolo možné v rámci auditu kybernetickej bezpečnosti vykonaného s využitím vytvoreného kontrolného zoznamu v plnom rozsahu overiť mieru plnenia súladu s požiadavkami stanovenými VoKB. Jednotlivé auditné položky z vytvoreného zoznamu sú rozdelené do niekoľkých kategórií, a to na základe ich príslušnosti ku konkrétnemu paragrafu VoKB, napr. § 3 VoKB definuje požiadavky na „Systém riadenia bezpečnosti informácií“, § 4 VoKB potom požiadavky na „Riadenie aktív“ atď., viď tab. B.1 a B.2. Kompletný zoznam auditných položiek, kategorizovaných podľa ich relevancie ku konkrétnym ustanoveniam VoKB, je súčasťou prílohy B.

Tab. 2.13: Zoznam auditných položiek k § 3 VoKB.

Odst.	Písm.	Auditná položka
	a)	Je stanovený rozsah ISMS?
	b)	Sú stanovené ciele ISMS?
	c)	Sú zavedené primerané bezpečnostné opatrenia?
	d)	Je zavedený proces riadenia rizík?
	e)	Je vytvorená, zavedená a schválená bezpečnostná politika v oblasti ISMS?
	f)	Je uskutočňovaný audit kybernetickej bezpečnosti v pravidelných intervaloch alebo pri významných zmenách?

	g)	Dochádza k pravidelnému vyhodnocovaniu účinnosti zavedeného ISMS, ktoré obsahuje hodnotenie aktuálneho stavu ISMS vrátane revízie hodnotenia rizík, posúdenia výsledkov vykonaných auditov kybernetickej bezpečnosti a dopadov kybernetických bezpečnostných incidentov na ISMS?
	h)	Sú priebežne identifikované významné zmeny spadajúce do rozsahu ISMS?
	i)	Je vykonávaná aktualizácia ISMS a príslušnej dokumentácie na základe zistení auditov kybernetickej bezpečnosti, výsledkov hodnotenia ISMS a v súvislosti s uskutočnenými zmenami?
	j)	Je riadená prevádzka a zdroje ISMS, sú zaznamenávané činnosti spojené s ISMS a riadením rizík?

Tab. 2.14: Zoznam auditných položiek k § 4 VoKB.

Odst.	Písm.	Auditná položka
1	a), b)	Je stanovená metodika pre identifikáciu a hodnotenie aktív?
1	c)	Je uskutočňovaná identifikácia a evidencia aktív?
1	d)	Sú určení garanti príslušných aktív?
1	e)	Je uskutočňované hodnotenie a evidencia primárnych aktív z hľadiska dôvernosti, integrity a dostupnosti?
1	f)	Sú určené väzby medzi primárnymi a podpornými aktívami?
1	g)	Je uskutočňované hodnotenie podporných aktív?
1	h)	Sú stanovené a zavádzané pravidlá ochrany nutné pre požadované zabezpečenie aktív?
1	i)	Sú stanovené prípustné spôsoby používania aktív a pravidlá pre manipuláciu s aktívami?
1	j)	Je určený spôsob likvidácie dát?

2.3.1 Vlastný modul do platformy Penterep

Vytvorený zoznam auditných položiek predstavený v úvode kap. 2.3, prostredníctvom ktorého je možné overiť mieru súladu plnenia jednotlivých bezpečnostných opatrení pre zaistenie kybernetickej bezpečnosti s požiadavkami VoKB, bol nasadený do existujúceho prostredia platformy Penterep [33]. Zvolená platforma umožňuje, okrem iného, vytvárať kontrolné zoznamy (tzv. checklisty), v rámci ktorých je možné

definovať sady otázok, ktoré by mali byť v priebehu vykonávania auditu overené – z tohto dôvodu bola vybraná práve platforma Penterep ako vhodná alternatíva pre vytváranie rôznych kontrolných zoznamov, práve aj pre potreby vykonania auditu kybernetickej bezpečnosti.

Do platformy Penterep bolo nasadených 25 kontrolných zoznamov obsahujúcich vyššie uvedené auditné otázky. Celkom bolo vytvorených 198 otázok („testov“), ktoré boli následne rozdelené do týchto 25 kategórií, odpovedajúcim jednotlivým vytvoreným kontrolným zoznamom, pre lepšie a jednoznačnejšie vyhodnotenie miery plnenia jednotlivých kategórií bezpečnostných opatrení definovaných VoKB (jeden kontrolný zoznam obsahuje otázky slúžiace k overeniu plnenia požiadaviek vyplývajúcich z ustanovení konkrétneho paragrafu VoKB). Takéto rozdelenie všetkých auditných položiek do týchto kategórií bolo zvolené z dôvodu, že v niektorých prípadoch môže byť žiadúce overiť len niektoré oblasti kybernetickej bezpečnosti (napr. fyzickú bezpečnosť – § 17), pričom nie je potrebné realizovať kompletný audit všetkých požiadaviek VoKB. Vďaka rozdeleniu na jednotlivé kategórie tak nemusia byť počas auditu vyhodnotené všetky definované otázky, ale len tie, ktoré sú pre konkrétnu overovanú oblasť relevantné.

K vytvoreným testom bolo následne definovaných celkom 225 zraniteľností predstavujúcich možné nedostatky, resp. nálezy, ktoré môžu byť v priebehu vykonávania auditu kybernetickej bezpečnosti odhalené. Tieto nedostatky (nálezy) sa môžu objaviť v prípadoch, kedy nebude zaistená dostatočná miera súladu plnenia jednotlivých bezpečnostných požiadaviek, ktoré vo svojich ustanoveniach definuje VoKB.

2.3.2 Praktické využitie nasadených kontrolných zoznamov

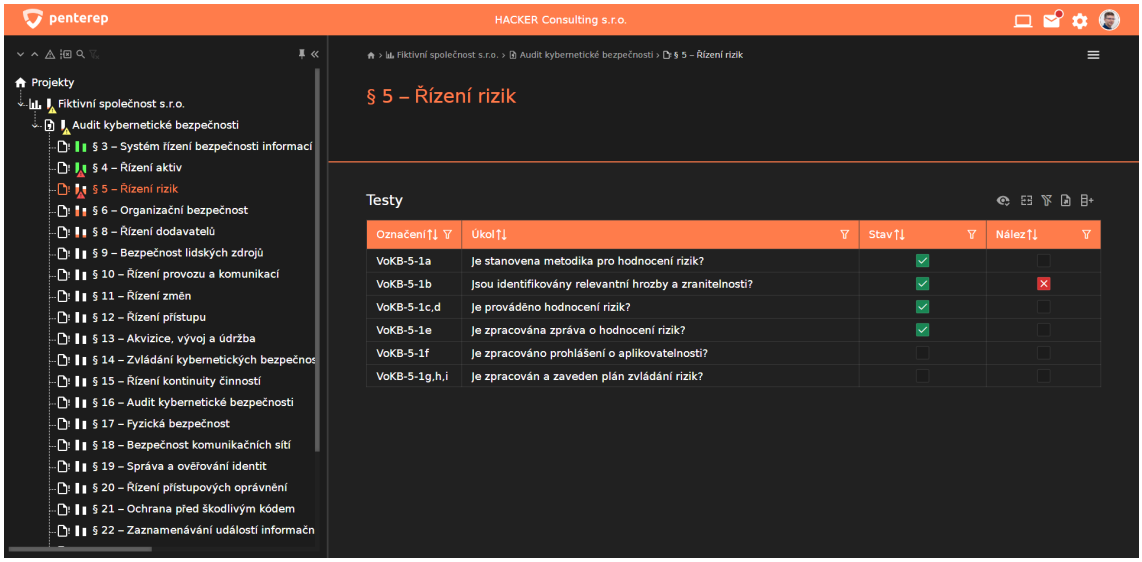
Vytvorené kontrolné zoznamy implementované do platformy Penterep môžu slúžiť ako pomocný nástroj pre rôzne organizácie či samotných audítorov kybernetickej bezpečnosti k vykonaniu bezpečnostného auditu. Táto kapitola obsahuje niekoľko obrazových záznamov z užívateľského rozhrania platformy, na základe ktorých bude tiež uvedený popis postupu pri vykonávaní auditu založenom na využití vytvorených kontrolných zoznamov.

Výber kontrolného zoznamu

Audit kybernetickej bezpečnosti je možné rozdeliť na niekoľko dielčích podčastí – vďaka rozdeleniu sady nadefinovaných auditných položiek (otázok) do niekoľkých kategórií je tak v každej fáze auditu možné overiť a vyhodnotiť plnenie jednotlivých ustanovení vždy konkrétneho paragrafu VoKB.

Audit vykonávaný s využitím platformy Penterep je reprezentovaný vo forme „projektu“, v rámci ktorého je potrebné definovať subjekt (spoločnosť, organizáciu),

pre ktorý je audit kybernetickej bezpečnosti vykonávaný, a tiež vybrať typ realizovaného testovania – v našom prípade sa jedná o „Audit kybernetické bezpečnosti“, ako je zachytené v ľavej časti na obr. 2.7. Samotný audit je potom členený na jednotlivé kategórie.



Obr. 2.7: Ukážka užívateľského rozhrania.

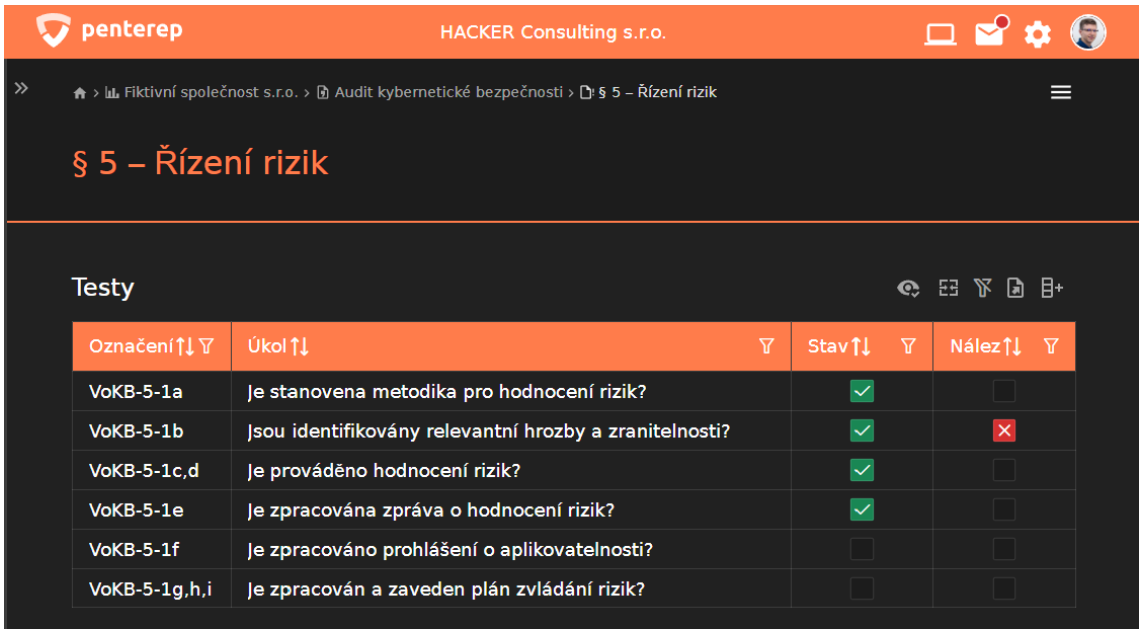
Priebeh auditu – overovanie plnenia auditných položiek

Po uskutočnení výberu kategórie, ktorá má byť predmetom auditu, sa príslušné auditné položky (otázky) spadajúce do tejto kategórie objavia zoradené v tabuľke v hlavnej časti užívateľského rozhrania, kde je následne možné jednotlivé auditné položky vyhodnotiť výberom a zaškrtnutím príslušného políčka v tabuľke. Detail tejto tabuľky je bližšie zobrazený na obr. 2.8. Políčko „stav“ označuje, či bola daná položka už overená, a ďalej políčko „nález“ označuje, že bol pre danú položku zistený určitý nedostatok[14].

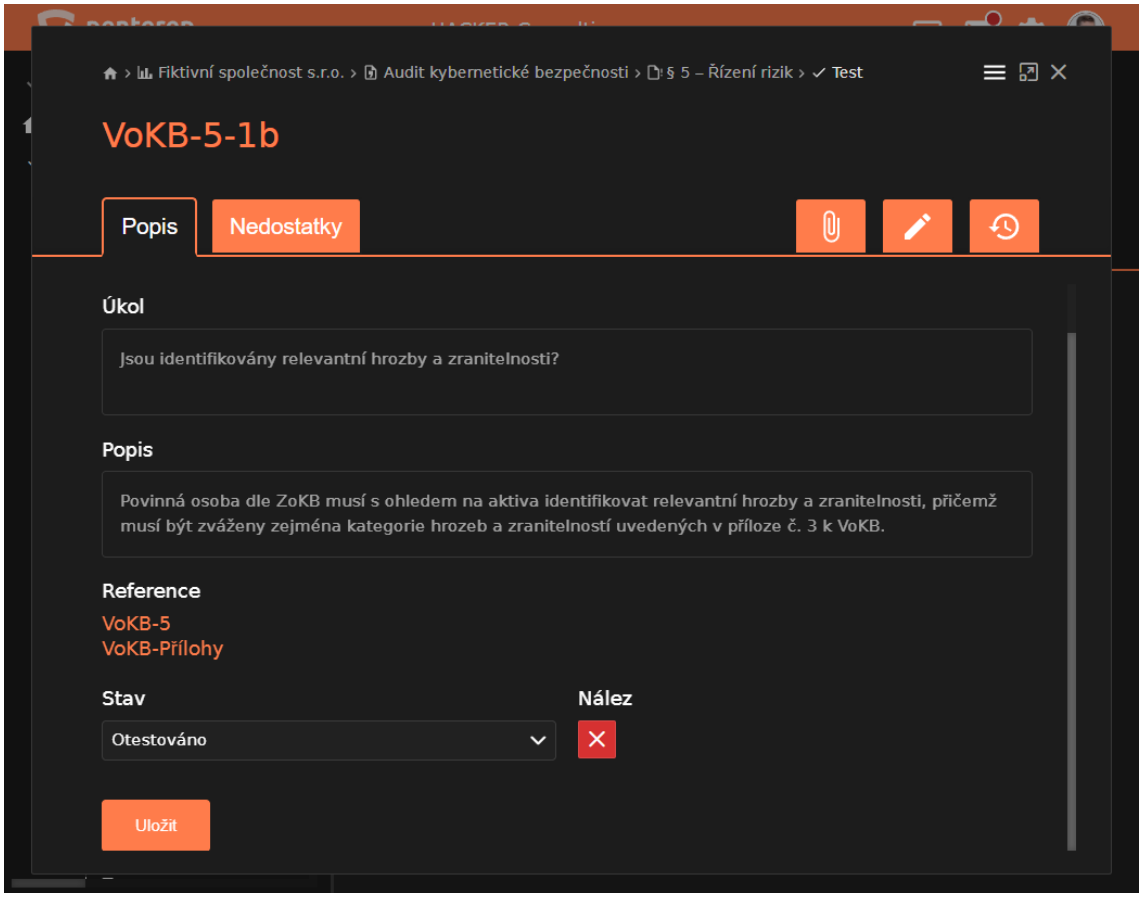
Pre jednotlivé auditné položky, ktoré sú súčasťou vybranej kategórie, je možné kliknutím na príslušnú položku zobraziť jej detail, viď obr. 2.9. Následne je zobrazené dialógové okno, v ktorom sú zaznamenané nasledujúce informácie:

- **úkol** – zadanie auditnej položky (otázky), ktorá je predmetom overovania,
- **popis** – bližšia definícia, ktorá vychádza z konkrétneho ustanovenia VoKB,
- **reference** – hypertextový odkaz (príp. odkazy) na príslušné ustanovenia VoKB,
- **stav** – indikuje, či bola daná auditná položka už overená,
- **nález** – záznam o tom, či bol pre danú položku zistený nedostatok.

[14]V prípade, že je daná auditná položka reprezentujúca konkrétne ustanovenie VoKB splnená, nie je zistený žiadny nález a toto políčko zostane nezaškrtnuté.



Obr. 2.8: Tabuľka pre overovanie auditných položiek.

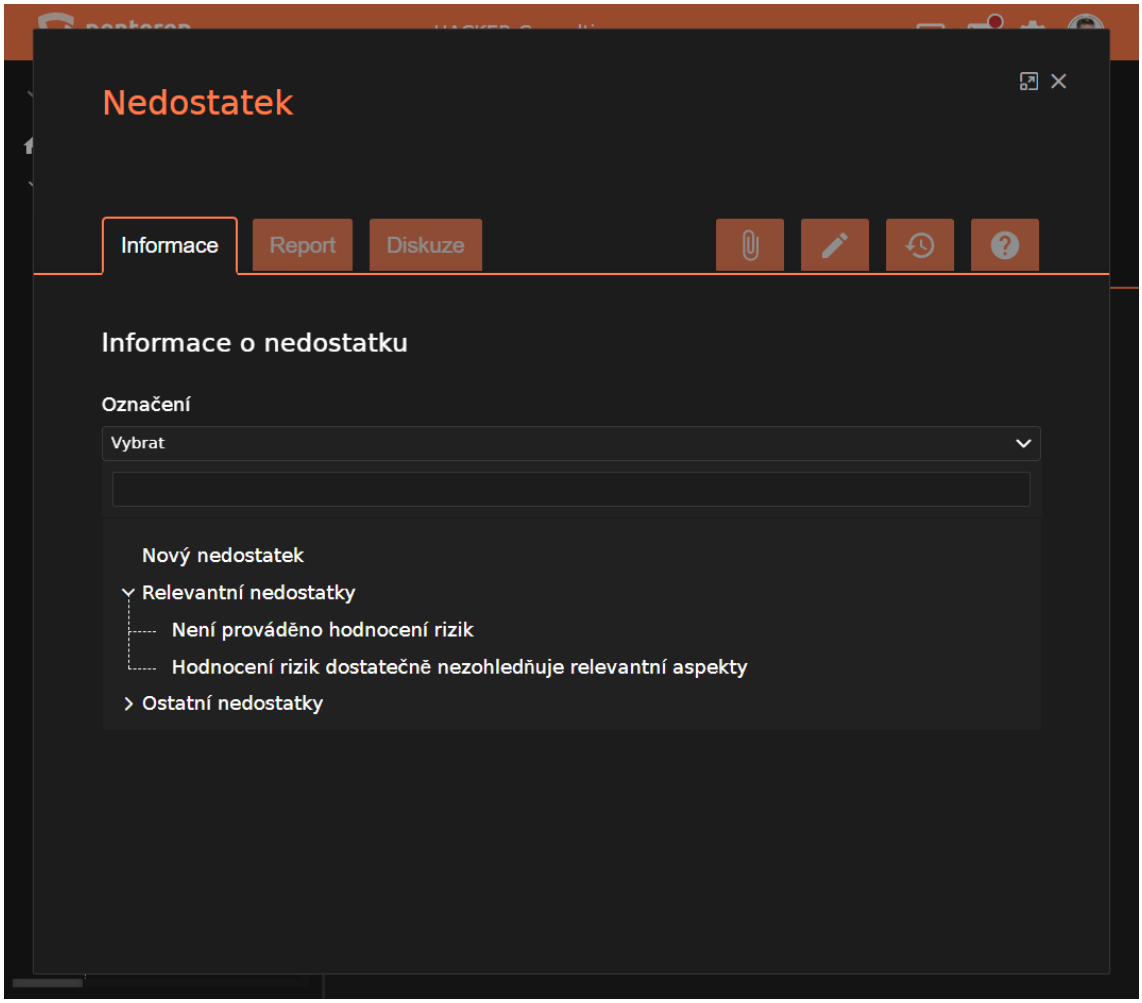


Obr. 2.9: Detail auditnej položky.

Priebeh auditu – nález nedostatku (nezhody)

Pre jednotlivé auditné položky je definovaný vždy jeden či viac možných nedostatkov, ktoré môžu vzniknúť zo situácie, kedy bude v priebehu auditu zistené, že príslušná auditná položka, resp. odpovedajúce ustanovenie VoKB, na základe ktorého bola daná auditná položka vytvorená, nie je splnené. Takýto nález predstavuje určitý nedostatok plnenia požadovaných bezpečnostných opatrení zo strany auditovaného subjektu, a teda reprezentuje dôvod vzniknutého nesúladu s požiadavkami VoKB.

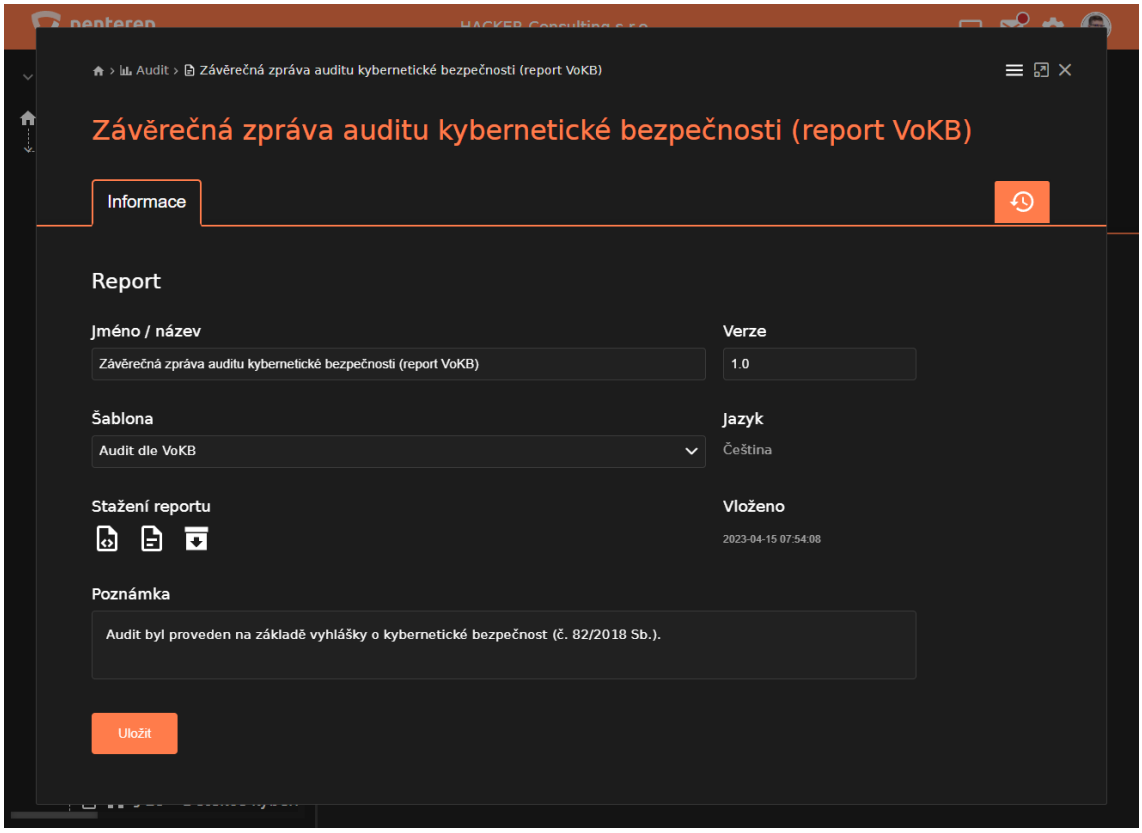
Pokiaľ bude v priebehu auditu odhalené, že subjekt (organizácia) neplní niektoré z ustanovení VoKB dostatočným spôsobom alebo ho plní len čiastočne, je potrebné určiť konkrétny nález, ktorý reprezentuje nedostatok vyplývajúci z tohto zistenia. Pre zvolenú auditnú položku je možné zobraziť zoznam k nej relevantných nedostatkov (táto skutočnosť je zachytená na obr. 2.10), ktoré môžu vzniknúť v dôsledku jej nesplnenia, a z tohto zoznamu následne vybrať konkrétny nedostatok, ktorý je hlavným predmetom zistenia vykonávaného auditu.



Obr. 2.10: Určenie nedostatkov vyplývajúcich zo zistení auditu.

Priebeh auditu – výsledný report

Výhodou využitia platformy Penterep je možnosť automatického vygenerovania reportu (záverečnej správy) ako hlavného výstupu z vykonaného auditu kybernetickej bezpečnosti. Možnosť vygenerovania záverečnej správy (viď obr. 2.11) sa zobrazí po vyhodnotení jednotlivých auditných položiek z aktuálne overovaného kontrolného zoznamu. Pre generovanie je možné zvoliť druh šablóny na základe preferencií konkrétneho audítora, do ktorej sú následne automaticky vložené výsledky zistení z vykonaného auditu.



Obr. 2.11: Ukážka reportu (záverečnej správy) z vykonaného auditu.

Hlavnou obsahovou náplňou reportu sú jednotlivé nálezy (nedostatky), ktoré boli počas auditu odhalené. Účelom tohto reportu je informovať auditovaný subjekt o výsledkoch a zisteniach vykonaného auditu a poskytnúť mu informácie o tom, v akých oblastiach boli jednotlivé nedostatky zistené a o aké konkrétne nedostatky sa jedná. Na základe týchto informácií bude môcť následne subjekt učiniť potrebné kroky vedúce k odstráneniu zistených nedostatkov (napr. dodatočnou implementáciou požadovaných bezpečnostných opatrení alebo vylepšením, posilnením opatrení, pokiaľ ich implementácia doposiaľ nebola dostatočná), čím zaistí, že v daných problematických oblastiach sa nezhody prevedú na zhody, čo sa prejaví ako zvýšenie miery

súladu plnenia jednotlivých požiadaviek na kybernetickú bezpečnosť vyplývajúcich z ustanovení VoKB.

Jednoduchá ukážka takejto záverečnej správy (reportu) je zahrnutá v prílohe C. Táto ukážka nie je skutočným výstupom realizovaného auditu, ale slúži len pre znázornenie obsahu generovaného reportu. Zámerne boli počas „ukážkového auditu“, ktorého výstup je reprezentovaný práve danou prílohou, nájdené mnohé nálezy, aby bolo možné názorne ukázať, aké informácie sú obsahom vygenerovaného reportu. Report vždy obsahuje nasledujúce informácie:

- **názov príslušnej auditnej položky**, pre ktorú bol identifikovaný určitý nález (nedostatok),
- ďalej **popis zisteného nedostatku**, tj. v čom spočíva vzniknutá nezhoda a
- **odôvodnenie**, ktoré vychádza spravidla z definície samotnej auditnej položky, pre ktorú bol konkrétny nález identifikovaný.

Záver

Táto záverečná diplomová práca bola venovaná problematike analýzy rizík v oblasti bezpečnosti informácií. V teoretickej časti práce boli predstavené základné poznatky z oblasti teórie informačnej bezpečnosti a niektoré existujúce štandardy a doporučenia upravujúce požiadavky na systém riadenia bezpečnosti informácií (ISMS), pričom boli podrobne vysvetlené požiadavky normy ISO/IEC 27001. Ďalej bola istá pozornosť venovaná procesu riadenia rizík a taktiež bola diskutovaná problematika právnej úpravy kybernetickej bezpečnosti a predstavené aktuálne existujúce riešenia v tejto oblasti.

Praktická časť tejto záverečnej práce zahŕňa vo svojej prvej časti vlastný návrh metodiky pre analýzu rizík informačnej bezpečnosti. Vytvorená metodika definuje a jednoznačne popisuje postupne všetky kroky posudzovania rizík, a to konkrétne identifikáciu aktív, hrozieb a zraniteľností, ich analýzu a ohodnotenie a výsledné stanovenie miery (hodnoty) identifikovaných rizík s následnou kategorizáciou týchto rizík do príslušných úrovní. V nadväznosti na vykonanú analýzu rizík je realizovaný návrh pre zvládanie nežiadúcich rizík, ktoré boli v priebehu analýzy identifikované, a to v podobe špecifikácie nápravných opatrení, ktorých implementácia by mala byť za účelom minimalizácie, ideálne odstránenia zistených rizík a iných nedostatkov realizovaná v nadchádzajúcom procese ošetrenia rizík.

Navrhnutá metodika pre analýzu rizík bola následne aplikovaná na špecifický kontext činností a aktív Spoločnosti, pre ktorú autorka vykonávala v čase písania tejto práce dlhodobo pracovnú činnosť. Výsledky zistené vykonanou analýzou boli prezentované vedeniu Spoločnosti. Všetky relevantné skutočnosti, potrebné údaje, záznamy a ďalšie dáta, ku ktorým bol udelený súhlas s ich zaradením do tejto práce, sú zaznamenané v prílohách, viď príloha A.

Ďalšou súčasťou praktickej časti je implementácia webovej aplikácie[15], ktorá slúži ako jednoduchý a prehľadný nástroj pre zobrazenie výsledkov vykonanej analýzy rizík a pre prezentovanie zistených poznatkov vedeniu Spoločnosti. Aplikácia bola vyvíjaná primárne za účelom získania možnosti prezentovať výsledky analýzy interne v prostredí Spoločnosti, no je možné diskutovať o jej využití aj pre iné subjekty. Aplikácia umožňuje výber spomedzi viacerých vykonaných analýz, ktorých údaje možno zobraziť a prezentovať, čo môže byť veľkou výhodou v prípade pravidelného preskúmania stavu informačnej bezpečnosti. Pre každú z analýz je možné zobraziť prehľad zistených rizík, spoločne s ich ohodnotením, a tiež grafické rozloženie týchto

[15]V čase odovzdania diplomovej práce sú všetky príslušné zdrojové kódy webovej aplikácie uložené v Git repozitári, vďaka čomu je možné k webovej aplikácii pristúpiť taktiež spôsobom zadania URL adresy `https://xvoska00.github.io/sp-analyza-rizik/` do užívateľom preferovaného webového prehliadača.

rizík do jednotlivých úrovní závažnosti. Ďalšou možnosťou je získanie podrobných informácií o každom riziku. S pomocou vyvinutej aplikácie je tiež možné prezentovať Plán zvládania rizík obsahujúci návrh a plán nasadenia opatrení za účelom ošetrenia jednotlivých rizík s cieľom zlepšenia stavu informačnej bezpečnosti a výsledkov následnej analýzy rizík do budúcnosti.

Posledná časť práce je venovaná praktickému riešeniu problematiky vykonania auditu kybernetickej bezpečnosti a overenia súladu plnenia jednotlivých požiadaviek na kybernetickú bezpečnosť definovaných vyhláškou o kybernetickej bezpečnosti. Pre potreby vykonania auditu bol vytvorený zoznam auditných položiek, ktorý môže slúžiť ako vhodný podklad pre jeho realizáciu. Jeho kompletná podoba je zaznamenaná v prílohách, viď príloha B. Vytvorený kontrolný zoznam bol následne nasadený do prostredia platformy Penterep, ktorá umožňuje zjednodušiť priebeh rozličných typov testovaní, akým môže byť napríklad aj samotný audit kybernetickej bezpečnosti. Pri realizácii auditu pomocou platformy Penterep je možné jeho priebeh rozdeliť do jednotlivých kategórií, identifikovať nedostatky v oblasti kybernetickej bezpečnosti na strane auditovaného subjektu a všetky zistené nálezy prehľadným spôsobom zhrnúť a prezentovať vo forme záverečného reportu ako hlavného výstupu z vykonaného auditu kybernetickej bezpečnosti.

Záverom možno konštatovať, že všetky stanovené ciele tejto diplomovej práce boli splnené. V rámci tejto práce bola naštudovaná problematika informačnej a kybernetickej bezpečnosti. Bola navrhnutá komplexná metodika pre analýzu rizík bezpečnosti informácií, ktorá bola aj prakticky aplikovaná. Ďalej bol tiež realizovaný návrh a vlastná implementácia aplikácie umožňujúcej prezentáciu výsledkov analýzy rizík realizovanej podľa navrhnutej metodiky. Táto aplikácia umožňuje všetky potrebné funkcionality, a z toho dôvodu môže byť považovaná za plne funkčnú. Nakoniec bol do platformy Penterep implementovaný kontrolný zoznam, ktorý možno využiť pre potreby vykonania auditu kybernetickej bezpečnosti za účelom overenia miery plnenia jednotlivých požiadaviek vyhlášky o kybernetickej bezpečnosti.

Literatúra

[1] *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* In: Zákony pro lidi [právny informačný systém]. AION CS, s.r.o. [cit. 2022-09-20]. Dostupné z URL: <https://www.zakonyprolidi.cz/cs/2014-181>

[2] *Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).* In: Zákony pro lidi [právny informačný systém]. AION CS, s.r.o. [cit. 2022-09-20]. Dostupné z URL: <https://www.zakonyprolidi.cz/cs/2018-82>

[3] MINISTERSTVO VNITRA ČR, ODBOR BEZPEČNOSTNÍ POLITIKY A PREVENCE KRIMINALITY. *Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu.* [online]. [cit. 2022-09-21]. Praha, 2016. Dostupné z URL: <https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx>

[4] ČSN ISO/IEC 27000: *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[5] ČANDÍK, Marek. *Informační bezpečnost.* [online]. [cit. 2022-09-21]. Praha, 2010. Dostupné z URL: <http://www.cybersecurity.cz/data/candik2.pdf>

[6] ČSN ISO/IEC 27005: *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[7] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích.* 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 488 s. ISBN 978-80-247-4644-9.

[8] ČERMÁK, Miroslav. Clever and Smart. *CIA: Je důvěrnost, integrita a dostupnost dostačující?* [online]. [cit. 2022-09-21].

Dostupné z URL: <https://www.cleverandsmart.cz/cia-je-duvernost-integrita-a-dostupnost-dostacujici/>

[9] ISO/IEC 27000 series. *ISO/IEC 27001 Information Security Management System Family.* [online]. [cit. 2022-09-21]. Dostupné z URL: <https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iso-27000-series/>

[10] ČSN ISO/IEC 27001: *Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2006.

[11] NOVÁK, Luděk a Josef POŽÁR. *Systém řízení informační bezpečnosti. CyberSecurity.cz - Kybernetická bezpečnost.* [online]. [cit. 2023-02-13]. Dostupné z URL: <www.cybersecurity.cz/data/SRIB.pdf>

[12] ČSN ISO/IEC 27001: *Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[13] HÁLEK, Vítězslav. *Krizový management – teorie a praxe.* Bratislava: Donau-Media, 2008. 322 s. ISBN 978-80-89364-00-8.

[14] ČSN ISO/IEC 31000: *Management rizik – Principy a směrnice.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

[15] VOSKÁROVÁ, Anna. *Hodnocení rizik v ochraně osobních údajů* [online]. Brno, 2021 [cit. 2022-09-21]. Dostupné z URL: <https://www.vutbr.cz/studenti/zav-prace/detail/133532>. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Jakub Míšek.

[16] ČERMÁK, Miroslav. Clever and Smart. *Informační bezpečnost vs. kybernetická bezpečnost.* [online]. [cit. 2022-09-21]. Dostupné z URL: <https://www.cleverandsmart.cz/information-security-vs-cybersecurity/>

[17] HARAŠTA, Jakub. *Právní aspekty kybernetické bezpečnosti ČR. Revue pro právo a technologie.* [online]. Brno, 2013. [cit. 2022-09-21]. Dostupné z URL: <https://journals.muni.cz/revue/article/view/5015/pdf>

[18] JIRÁSEK, P. NOVÁK, L. POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha:Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2013. [cit. 2022-09-21]. ISBN 978-80-7251-397-0. Dostupné z URL: <https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf>

[19] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Legislativa KB.* [online]. [cit. 2023-03-14]. Dostupné z URL: <https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/>

[20] *Smernica Európskeho parlamentu a Rady (EÚ) č. 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.* In: EUR-Lex. [právny informačný systém]. © Úrad pre vydávanie publikácií Európskej únie. [cit. 2022-09-20]. Dostupné z URL: <https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32016L1148&from=cs>

[21] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Pro které instituce je zákon o kybernetické bezpečnosti závazný?* [online]. [cit. 2022-09-29]. Dostupné z URL: <https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/#otazka1>

[22] JIRÁSEK, P., NOVÁK, L., POŽÁR J. *Výkladový slovník kybernetické bezpečnosti.* [online]. [cit. 2022-09-29]. Dostupné z URL: <https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf>

[23] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Minimální bezpečnostní standard.* [online]. [cit. 2022-09-29]. Dostupné z URL: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/>

[24] *Archer IRM.* [online]. [cit. 2022-09-29]. Dostupné z URL: <https://www.archerirm.com/>

[25] *Eramba.* [online]. [cit. 2022-09-29]. Dostupné z URL: <https://www.eramba.org/>

[26] *ServiceNow.* [online]. [cit. 2022-09-29]. Dostupné z URL: <https://www.servicenow.com/products/governance-risk-and-compliance.html>

[27] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti.* [online]. [cit. 2022-10-24]. Dostupné z URL: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/>

[28] *Next.js.* [online]. [cit. 2022-11-05]. Dostupné z URL: <https://nextjs.org/>

[29] *React.* [online]. [cit. 2022-11-05]. Dostupné z URL: <https://reactjs.org/>

[30] *Tailwind CSS.* [online]. [cit. 2022-11-05]. Dostupné z URL: <https://tailwindcss.com/>

[31] *SheetJS.* [online]. [cit. 2022-11-05]. Dostupné z URL: <https://www.npmjs.com/package/xlsx>

[32] *Chart.js.* [online]. [cit. 2022-11-05]. Dostupné z URL: <https://www.chartjs.org/>

[33] LAZAROV, W., MARTINÁSEK, Z. Web Platform for Comprehensive Penetration Testing. In *Proceedings II of the 28th Conference STUDENT EEICT 2022 Selected Papers.* 1. Brno: Brno University of Technology, Faculty of Electrical Engineering and Communication, 2022. s. 88-91. ISBN: 978-80-214-6030-0.

Zoznam symbolov a skratiek

BCMS Business Continuity Management System

COBIT Control Objectives for Information and Related Technology

CSS Cascading Style Sheet

HTML Hypertext Markup Language

ISMS Information Security Management System

ITIL Information Technology Infrastructure Library

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost

SSG Static-Site Generation

SSR Server-Side Rendering

VoKB Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

ZoKB Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Zoznam príloh

A Analýza rizík

A.1 Register aktív

Príloha obsahuje kompletný zoznam identifikovaných aktív, vrátane ich rozdelenia na primárne a podporné aktíva Pre každé aktívum sú určené:

- tri hodnoty reprezentujúce **hodnotenie dopadov** (dopad na dôvernosť aktíva, jeho integritu a dostupnosť)
- a ďalej hodnota **významnosti aktíva**, ktorá vyjadruje finančnú hodnotu, resp. význam aktíva pre Spoločnosť.

Všetky uvedené parametre sú hodnotené na škále v rozmedzí 1 (nízka) až 4 (vysoká). Z týchto celkom štyroch parametrov je nakoniec určená výsledná **hodnota každého aktíva** podľa vzťahov 2.1 a 2.2.

Skupina aktiv	ID aktiva	Aktivum	Popis aktiva	Primární / Podpůrné	Důvěrnost	Dostupnost	Integrita	Významnost aktiva	Hodnota aktiva
Lokality a jejich vybavení, podpůrná infrastruktura	1	Budova a její podpůrná infrastruktura - Pracoviště_1	Budova v lokalitě Pracoviště_1 - včetně veškeré podpůrné infrastruktury, jako je voda, plyn, elektřina	Podpůrné	2	3	3	4	11
	2	Budova a její podpůrná infrastruktura - Pracoviště_2	Budova v lokalitě Pracoviště_2 - včetně veškeré podpůrné infrastruktury, jako je voda, plyn, elektřina	Podpůrné	2	2	2	3	6
	3	Budova a její podpůrná infrastruktura - Pracoviště_3	Budova v lokalitě Pracoviště_3 - včetně veškeré podpůrné infrastruktury, jako je voda, plyn, elektřina	Podpůrné	2	3	3	4	11
	4	Serverovna - Pracoviště_1	Serverovna a její vybavení v budově Pracoviště_1 - přízemí	Podpůrné	2	4	4	4	13
	5	Serverovna - Pracoviště_2	Serverovna a její vybavení v budově Pracoviště_2	Podpůrné	2	3	3	3	8
	6	Serverovna - Pracoviště_3	Serverovna a její vybavení v budově Pracoviště_3 - 1. n.p.	Podpůrné	2	4	4	4	13
	7	Autopark - ČR	Firemní vozidla dislokovaná v lokalitě Pracoviště_1 a Pracoviště_2	Podpůrné	2	2	2	2	4
	8	Autopark - SR	Firemní vozidla dislokovaná v lokalitě Pracoviště_3	Podpůrné	2	2	2	2	4
Hardware	9	LAN - síťová infrastruktura - KII - Pracoviště_1	LAN síťová infrastruktura podporující služby přímo související se zákazníky a dodávanými produkty (KII) - rozvody, switche, firewally, aktivní prvky...	Podpůrné	3	3	3	3	9
	10	LAN - síťová infrastruktura - Společnost - Pracoviště_1	LAN síťová infrastruktura podporující interní služby Společnosti - rozvody, switche, firewally, aktivní prvky...	Podpůrné	2	2	2	2	4
	11	WiFi infrastruktura - Pracoviště_1	APs a další prvky tvořící wifi infrastrukturu v lokalitě	Podpůrné	1	1	1	1	1
	12	Vývojové servery - Pracoviště_1	Servery používáné pro vývoj aplikací	Podpůrné	3	2	3	2	5
	13	Ostatní servery - KII - Pracoviště_1	Ostatní servery používané pro účely související se zákazníky (např. SVN)	Podpůrné	3	3	3	3	9
	14	Ostatní servery - Společnost - Pracoviště_1	Ostatní servery používané pro interní účely Společnosti	Podpůrné	2	2	2	2	4
	15	Docházkový systém a EZS - Pracoviště_1	Vstupní systém budovy a EZS	Podpůrné	1	1	1	1	1
	16	Kamerový systém - Pracoviště_1	IP kamery v rámci budovy a okolí	Podpůrné	1	1	1	1	1
	17	Stanice, notebooky, mobilní telefony - KII - Pracoviště_1	PC stanice a notebooky používané pro účely související se zákazníky a pro přístup do systémů zákazníků	Podpůrné	3	3	3	1	3
	18	Stanice, notebooky, mobilní telefony - Společnost - Pracoviště_1	PC stanice a notebooky používané pro interní účely Společnosti	Podpůrné	2	2	2	1	2
	19	Ostatní HW a periférie - Pracoviště_1	Tiskárny, skenery, čtečky apod.	Podpůrné	1	1	1	1	1
	20	LAN - síťová infrastruktura - KII - Pracoviště_2	LAN síťová infrastruktura podporující služby přímo související se zákazníky a dodávanými produkty (KII) - rozvody, switche, firewally, aktivní prvky...	Podpůrné	3	3	3	3	9
	21	LAN - síťová infrastruktura - Společnost - Pracoviště_2	LAN síťová infrastruktura podporující interní služby Společnosti - rozvody, switche, firewally, aktivní prvky...	Podpůrné	2	2	2	2	4
	22	WiFi infrastruktura - Pracoviště_2	APs a další prvky tvořící wifi infrastrukturu v lokalitě	Podpůrné	1	1	1	1	1
	23	Ostatní servery - KII - Pracoviště_2	Ostatní servery používané pro účely související se zákazníky	Podpůrné	3	3	3	3	9
	24	Ostatní servery - Společnost - Pracoviště_2	Ostatní servery používané pro interní účely Společnosti	Podpůrné	2	2	2	2	4
	25	Docházkový systém a EZS - Pracoviště_2	Vstupní systém budovy a EZS	Podpůrné	1	1	1	1	1
	26	Kamerový systém - Pracoviště_2	IP kamery v rámci budovy a okolí	Podpůrné	1	1	1	1	1
	27	Stanice, notebooky, mobilní telefony - KII - Pracoviště_2	PC stanice a notebooky používané pro účely související se zákazníky a pro přístup do systémů zákazníků	Podpůrné	3	3	3	1	3
	28	Stanice, notebooky, mobilní telefony - Společnost - Pracoviště_2	PC stanice a notebooky používané pro interní účely Společnosti	Podpůrné	2	2	2	1	2
	29	Ostatní HW a periférie - Pracoviště_2	Tiskárny, skenery, čtečky apod.	Podpůrné	1	1	1	1	1
	30	LAN - síťová infrastruktura - KII - Pracoviště_3	LAN síťová infrastruktura podporující služby přímo související se zákazníky a dodávanými produkty (KII) - rozvody, switche, firewally, aktivní prvky...	Podpůrné	3	3	3	3	9
	31	LAN - síťová infrastruktura - Společnost - Pracoviště_3	LAN síťová infrastruktura podporující interní služby Společnosti - rozvody, switche, firewally, aktivní prvky...	Podpůrné	2	2	2	2	4
	32	WiFi infrastruktura - Pracoviště_3	APs a další prvky tvořící wifi infrastrukturu v lokalitě	Podpůrné	1	1	1	1	1
	33	Ostatní servery - KII - Pracoviště_3	Ostatní servery používané pro účely související se zákazníky	Podpůrné	3	3	3	3	9
	34	Ostatní servery - Společnost - Pracoviště_3	Ostatní servery používané pro interní účely Společnosti	Podpůrné	2	2	2	2	4
	35	Docházkový systém a EZS - Pracoviště_3	Vstupní systém budovy a EZS	Podpůrné	1	1	1	1	1
	36	Kamerový systém - Pracoviště_3	IP kamery v rámci budovy a okolí	Podpůrné	1	1	1	1	1
	37	Stanice, notebooky, mobilní telefony - KII - Pracoviště_3	PC stanice a notebooky používané pro účely související se zákazníky a pro přístup do systémů zákazníků	Podpůrné	3	3	3	1	3
	38	Stanice, notebooky, mobilní telefony - Společnost - Pracoviště_3	PC stanice a notebooky používané pro interní účely Společnosti	Podpůrné	2	2	2	1	2
	39	Ostatní HW a periférie - Pracoviště_3	Tiskárny, skenery, čtečky apod.	Podpůrné	1	1	1	1	1
Systémy a aplikace	40	IDM	Identity Management - řízení přístupu v rámci LAN Společnosti	Podpůrné	3	3	3	2	6
	41	Redmine	Tiketovací systém Společnosti	Podpůrné	3	2	3	2	5
	42	Nextcloud	Systém pro uložení a správu dokumentů	Podpůrné	3	2	2	1	2
	43	Antivirový SW	AV včetně centrální správy	Podpůrné	2	2	2	1	2
	44	SIEM	AV OSSIM	Podpůrné	2	2	2	1	2
	45	VPN	VPN používaná pro přístup ke zdrojům Společnosti	Podpůrné	2	3	3	2	5
	46	VPN spojení	IP Sec spojení/linky k zákazníkům	Podpůrné	3	3	3	2	6
	47	Účetní SW	ABRA	Podpůrné	3	2	2	1	2
	48	Virtualizace	KVM	Podpůrné	2	2	2	1	2
	49	Testovací systémy	Vývojová laboratoř a další testovací systémy	Podpůrné	2	2	2	1	2
	50	Operační systémy	Windows, Ubuntu, RedHat	Podpůrné	2	2	2	1	2
	51	Další drobný a kancelářský SW	MS Office, Firefox, ostatní	Podpůrné	2	2	2	1	2
	52	Zaměstnanci - KII - Pracoviště_1, Pracoviště_2	Zaměstnanci spadající pod Společnost ČR, kteří se podílejí přímo na činnostech pro zákazníky nebo pracují s daty souvisejícími se zákaznickými systémy	Podpůrné	3	3	3	3	9
	53	Zaměstnanci - Vývoj - Pracoviště_1, Pracoviště_2	Zaměstnanci spadající pod Společnost ČR, kteří se podílejí na vývoji	Podpůrné	3	2	3	3	8

Personál	54	Zaměstnanci - Společnost - Pracoviště_1, Pracoviště_2	Zaměstnanci spadající pod Společnost ČR, kteří nepřicházejí do styku s KII/zákazníky	Podpůrné	2	2	2	2	4
	55	Zaměstnanci - KII - Pracoviště_3	Zaměstnanci spadající pod Společnost SK, kteří se podílejí přímo na činnostech pro zákazníky nebo pracují s daty souvisejícími se zákaznickými systémy	Podpůrné	3	3	3	3	9
	56	Zaměstnanci - Vývoj - Pracoviště_3	Zaměstnanci spadající pod Společnost SK, kteří se podílejí na vývoji	Podpůrné	3	2	3	3	8
	57	Zaměstnanci - Společnost - Pracoviště_3	Zaměstnanci spadající pod Společnost SK, kteří nepřicházejí do styku s KII/zákazníky	Podpůrné	2	2	2	2	4
Informační aktiva	58	Data - Systém	Data získaná, uložená a zpracovávaná Systémem (vč. systém. modulu) - uložená u Společnosti	Primární	3	2	2	2	5
	59	Data - vývoj SW	Zdrojové kódy a skripty vyvíjených aplikací, modulů	Primární	3	2	4	4	12
	60	Data - vývoj HW	Komunikační moduly pro přenos dat do řídícího inf. systému, schemata, PCB	Primární	2	2	4	2	5
	61	Data - účetnictví a ekonomika	Fakturace, mzdy, apod.	Primární	2	1	3	3	6
	62	Data - personalistika	Osobní spisy (karta zaměstnance, prac. smlouva, záznamy o školení, zdravotní prohlídky)	Primární	3	1	2	2	4
	63	Data - provoz - ČR	Data související s provozem firmy, budov, zaměstnanci apod. neuvedená v jiných položkách	Primární	2	1	2	1	2
	64	Data - provoz - SR	Data související s provozem firmy, budov, zaměstnanci apod. neuvedená v jiných položkách	Primární	2	1	2	1	2
	65	Data - nabídky - ČR	Nabídky zákazníkům, vyjednávání se zákazníky	Primární	3	2	3	3	8
	66	Data - nabídky- SR	Nabídky zákazníkům, vyjednávání se zákazníky	Primární	3	2	3	3	8
	67	Data - smlouvy - ČR	Smlouvy se zákazníky a dodavateli	Primární	3	1	3	3	7
	68	Data - smlouvy - SR	Smlouvy se zákazníky a dodavateli	Primární	3	1	3	3	7
	69	Data - archiv - Pracoviště_1	Fyzické dokumenty uložené v archivu	Primární	3	1	3	2	5
	70	Data - archiv - Pracoviště_3	Fyzické dokumenty uložené v archivu	Primární	3	1	3	2	5
	71	Data - ISMS a BCMS	Data systému řízení	Primární	3	2	3	3	8
	72	Data - QMS	Data systému řízení	Primární	2	1	2	1	2
	73	Data - BOZP	Data systému řízení	Primární	2	1	2	1	2
	74	Data - EMS	Data systému řízení	Primární	2	1	2	1	2
	75	Data - Gsuite	Data v GSuite (e-maily, dokumenty, kalendáře...)	Primární	3	3	3	2	6
	76	Data - Datové schránky	Data v datových schránkách	Primární	3	3	3	2	6
Služby - poskytované	77	Servis - Zákazník_1	Servisní služby poskytované pro Zákazníka_1	Primární	3	4	4	4	15
	78	Servis - Zákazník_2	Servisní služby poskytované pro Zákazníka_2	Primární	3	4	4	4	15
	79	Servis - Zákazník_3	Servisní služby poskytované pro Zákazníka_3	Primární	3	4	4	4	15
	80	Servis - Zákazník_4	Servisní služby poskytované pro Zákazníka_4	Primární	3	4	4	4	15
	81	Servis - Zákazník_5	Servisní služby poskytované pro Zákazníka_5	Primární	3	4	4	4	15
	82	Servis - Zákazník_6	Servisní služby poskytované pro Zákazníka_6	Primární	3	2	4	3	9
	83	Hotline - Pracoviště_1	Zákaznická linka 24x7	Primární	2	4	4	4	13
	84	Hotline - Pracoviště_3	Zákaznická linka 24x7	Primární	2	4	4	4	13
	85	Dodávka řídícího informačního systému	Realizace zakázek - implementace řídícího inf. systému, HMI... (SW+HW)	Primární	2	2	4	4	11
Služby - přijímané	86	ISP - Pracoviště_1	Primární internetová konektivita - Pracoviště_1	Podpůrné	2	3	3	2	5
	87	Záložní ISP - Pracoviště_1	Záložní internetová konektivita - Pracoviště_1	Podpůrné	2	2	2	1	2
	88	ISP - Pracoviště_2	Internetová konektivita - Pracoviště_2	Podpůrné	2	2	2	1	2
	89	Mobilní a datové služby - ČR	Služby mobilního operátora	Podpůrné	2	2	2	1	2
	90	Utility služby - Pracoviště_1	Dodávky - voda, plyn, elektřina, PCO	Podpůrné	2	2	2	1	2
	91	Utility služby - Pracoviště_2	Dodávky - voda, plyn, elektřina	Podpůrné	2	2	2	1	2
	92	ISP - Pracoviště_3	Internetová konektivita - Pracoviště_3	Podpůrné	2	3	3	2	5
	93	Mobilní a datové služby - SR	Služby mobilního operátora	Podpůrné	2	2	2	1	2
	94	Utility služby - Pracoviště_3	Dodávky - voda, plyn, elektřina	Podpůrné	2	2	2	1	2
	95	Gsuite	Cloud služby Google - mail, disk, kalendář	Podpůrné	3	3	3	1	3
	96	vpsFree cloud hosting	Cloud služba pro hosting Redmine u Zákazníka	Podpůrné	3	3	3	2	6
	97	Hosting web stránek	Hosting pro umístění webových stránek firmy	Podpůrné	1	1	2	1	1
Služby - interní	98	Vývoj SW	Realizace vývojových činností	Podpůrné	3	3	4	4	13
	99	Interní IT podpora	Uživatelská podpora Společnosti, provoz interních systémů a aplikací	Podpůrné	3	3	3	3	9
	100	Office služby - Pracoviště_1	Backoffice a provoz budovy	Podpůrné	2	2	2	2	4
	101	Office služby - Pracoviště_2	Backoffice a provoz budovy	Podpůrné	2	2	2	2	4
	102	Office služby - Pracoviště_3	Backoffice a provoz budovy	Podpůrné	2	2	2	2	4

A.2 Katalóg hrozieb

Príloha obsahuje kompletný katalóg hrozieb spoločne s popisom identifikovaných hrozieb. Pre každú hrozbu je určená:

- hodnota **pravdepodobnosti** realizácie hrozby (na škále v rozmedzí 1 až 4)
- a tiež hodnota **dopadu** nepriaznivého pôsobenia danej hrozby (opäť na škále v rozmedzí 1 až 4).

Z týchto dvoch parametrov je následne určená **úroveň hrozby** podľa vzťahu 2.3. Ďalej je pre každú z hrozieb určený:

- **zdroj hrozby**, ktorý danú hrozbu realizuje,
- a **úmysel**, ktorý poskytuje informáciu o tom, či identifikovaný zdroj hrozby realizuje hrozbu náhodne alebo naopak zámerne.

Kategorie	ID	Hrozba	Pravděpodobnost	Dopad	Úroveň hrozby	Popis hrozby	Úmysl (náhodný/záměrný)	Zdroj (vnitřní/vnější)
Uživatelé	1	neúmyslné porušení bezpečnostní politiky ze strany uživatele	3	2	6	Hrozba spočívá ve vykonání neúmyslné chyby v důsledku nedbalosti nebo nedostatečné znalosti běžného uživatele, která bude mít dopad na aktiva.	náhodný	vnitřní
	2	neúmyslné porušení bezpečnostní politiky ze strany administrátora	2	3	6	Hrozba spočívá ve vykonání neúmyslné chyby v důsledku nedbalosti nebo nedostatečné znalosti administrátora, která bude mít dopad na aktiva.	náhodný	vnitřní
	3	úmyslné porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatele	1	2	2	Hrozba spočívá v úmyslném konání ze strany běžného uživatele způsobeném v důsledku jeho vnitřní motivace (nespokojenost, konflikt apod.), které je v rozporu s definovánou bezpečnostní politikou, s následným dopadem na aktiva.	záměrný	vnitřní
	4	úmyslné porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátora	1	4	4	Hrozba spočívá v úmyslném konání ze strany administrátora způsobeném v důsledku jeho vnitřní motivace (nespokojenost, konflikt apod.), které je v rozporu s definovánou bezpečnostní politikou, s následným dopadem na aktiva.	záměrný	vnitřní
Organizace	5	ztráta jednoho nebo více klíčových zaměstnanců	2	3	6	Hrozba spočívá v nedostatečné zastupitelnosti zaměstnanců Společnosti na klíčových pracovních pozicích v důsledku náhlé a neočekávané nedostupnosti/ztráty (úraz, pracovní neschopnost). Riziko se může dále zvyšovat s absencí/nedostatečností dokumentace klíčových provozních procesů a jejich neaktuálností.	náhodný	vnější
	6	nedostatek zaměstnanců s potřebnou odbornou úrovní na pracovním trhu	3	2	6	Hrozba spočíva v neschopnosti zajistit potřebné personální kapacity pro organizaci, což bude mít dopad na kvalitu procesů, včetně zajištění bezpečnosti.	náhodný	vnější
	7	náhlá indispozice nebo nedostupnost servisního pracovníka	2	4	8	Hrozba spočívá v neschopnosti organizace poskytovat zákazníkům služby servisu v předem dojednaném čase a kvalitě v důsledku neočekávané nedostupnosti servisního pracovníka. Hrozba je dále posilována nedostatečnou úrovní zastupitelnosti servisních pracovníků.	náhodný	vnější
	8	náhlé snížení úrovně bezpečnosti v důsledku nevhodné firemní kultury	3	3	9	Hrozba spočívá v aktuálním stavu organizace, kdy řada činností a kvalita jejich provedení spočívá zejména na svědomitosti jednotlivých zaměstnanců, jejich zanícení a sounáležitosti s firmou - jednotlivé pracovní činnosti jsou prováděny bez potřeby vyšší úrovně kontroly vedením. Pokud by došlo k nevhodné změně firemní kultury, ať již ze strany vedení (např. změnou pracovních podmínek) nebo ze strany jednotlivých zaměstnanců (např. pokles pracovní morálky), bude to pravděpodobně mít dopad mj. i na dodržování bezpečnostních pravidel a tedy i na celkovou úroveň bezpečnosti Společnosti.	záměrný	vnitřní
	9	snižování úrovně bezpečnosti v důsledku nedostatečných investic	3	3	9	Hrozba spočívá v nedostatečném financování aktivit a vybavení potřebných pro dosažení potřebné úrovně bezpečnosti Společnosti.	záměrný	vnitřní
	10	snižování úrovně bezpečnosti a služeb z důvodu nedostatečné personální kapacity pro vedení zaměstnanců	3	3	9	Hrozba spočívá v neschopnosti vedoucích/odborných zaměstnanců předávat know-how a řídit služebně mladší zaměstnance, což bude mít dopad na jejich odbornou úroveň a schopnost plnit pracovní úkoly, včetně dopadu na úroveň bezpečnosti v poskytovaných službách i interně v rámci Společnosti.	záměrný	vnitřní
	11	pokuta nebo jiný postih Společnosti z důvodu porušení zákonných povinností	1	2	2	Hrozba spočívá v možném nesouladu s některými legislativními ustanoveními, která mohou přímo či nepřímo definovat požadavky na zajištění ochrany některých informací a dosažení požadované úrovně bezpečnosti při výkonu činností Společnosti V případě porušení, resp. nedodržení těchto požadavků může být Společnosti sankcionována.	náhodný	vnější
Technické selhání	12	poškození nebo selhání technického anebo programového vybavení organizace (včetně chybné funkčnosti)	3	2	6	Hrozba je způsobena neočekávanou technickou poruchou nebo nesprávnou funkcí HW nebo SW. Hrozba se zvyšuje v důsledku nedostatečné pravidelné údržby a kontroly.	náhodný/záměrný	vnitřní/vnější
	13	porušení dostupnosti nebo integrity zdrojových kódu vyvíjeného SW	1	2	2	Hrozba se pravděpodobně projeví v rámci servisu zákazníků, kdy dojde k nemožnosti stažení zdrojových kódů řídícího informačního systému nebo poškození zdrojových kódů. Toto může nastat v důsledku řady příčin, např. výpadek SVN, výpadek spojení, porucha HW, síťový útok apod. Tuto hrozbu hodnotíme v rámci rozsahu našeho ISMS	náhodný/záměrný	vnitřní/vnější
	14	omezení, nedostupnost monitoringu systému	1	1	1	Hrozba spočívá v neznalosti aktuálního stavu systému, což znemožňuje dostatečně rychle reagovat na výskyt nežádoucích jevů/stavů v systému.	náhodný/záměrný	vnitřní
	15	zneužití vyměnitelných technických nosičů dat	1	3	3	Hrozba spočívá zejména ve zneužití přenosného paměťového média interním útočníkem ke krádeži a/nebo zneužití většího objemu interních informací Společnosti.	záměrný	vnitřní
	16	ztráta, odcizení nebo poškození technického aktiva uživatelů (NTB, PC, mobily)	3	1	3	Hrozba spočívá v činnosti interního nebo i externího útočníka směřované vůči jakémukoliv aktivu Společnosti, které může být v důsledku těchto úmyslných činností poškozeno, kompromitováno nebo zničeno.	záměrný	vnitřní/vnější
	17	ztráta, odcizení nebo poškození klíčových technických aktiv firmy (servery, infrastruktura)	1	3	3	Hrozba spočívá v činnosti interního nebo i externího útočníka směřované vůči některému z kritických aktiv Společnosti, které může být v důsledku těchto úmyslných činností poškozeno, kompromitováno nebo zničeno.	záměrný	vnitřní/vnější
	18	přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	2	1	2	Hrozba spočívá v selhání podpůrných služeb, na kterých jsou závislé klíčové procesy Společnosti (zejména dodávka a servis řídícího informačního systému), např. krátkodobý nebo dlouhodobý výpadek dodávky energie, selhání telekomunikačních služeb způsobené problémy poskytovatele těchto služeb nebo kybernetickým útokem vedeným na telekomunikační infrastrukturu apod.	náhodný	vnější
	19	okamžitá nedostupnost prostředků pro zajištění služeb (auto, autopark, vybavení servisního pracovníka)	2	1	2	Hrozba může být způsobena náhlou poruchou nebo ztrátou vybavení, které servisní pracovník nezbytně potřebuje pro zajištění servisních služeb v odpovídající kvalitě a v požadovaném čase (SLA).	náhodný	vnější
	20	nefunkčnost spojení mezi servisním pracovištěm a systémem zákazníka	1	4	4	Hrozba spočívá v okamžité nedostupnosti spojení (nefunkční jump server, S2S VPN, výpadek linky …) do systému zákazníka, což znemožní poskytnutí servisních služeb v požadovaném čase (SLA).	náhodný	vnitřní/vnější
Dodavatelé, zákazníci	21	nedodržení smluvního závazku ze strany dodavatele	1	2	2	Hrozba se může projevit v rámci dodávky nebo v rámci servisu, většinou formou neplnění zasmluvněných lhůt plnění v požadovaném rozsahu a kvalitě, což může mít dopad na poskytování dílčích dodávek nebo servisních služeb zákazníkům.	náhodný	vnější
	22	selhání služeb dodavatele, narušení dodávky	1	3	3	Hrozba spočívá v nerealizaci předpokládaných dodávek nebo služeb ze strany dodavatele, je nutné hledat náhradního dodavatele. Míra dopadu této hrozby se zvyšuje s předpokládaným objemem plnění dodavatele.	náhodný/záměrný	vnější
	23	neúmyslná chyba pracovníka dodavatele	1	3	3	Hrozba vychází z neúmyslně způsobeného bezpečnostního incidentu pracovníkem dodavatele, který se projeví na aktivu zákazníka.	náhodný	vnější
	24	úmyslné odcizení nebo poškození aktiva Společnosti pracovníkem dodavatele	1	2	2	Hrozba vychází z úmyslného odcizení nebo poškození aktiva Společnosti pracovníkem dodavatele.	záměrný	vnější
	25	narušení služeb (SLA) Společnosti z důvodu nesouladu nebo nespolupráce na straně zákazníka	2	4	8	Hrozba spočívá v tom, že zákazník vědomě a přes upozornění Společnosti na své straně nevytvoří podmínky nutné pro realizaci služeb v souladu s SLA - např. nespolupracuje v domluvených lhůtách (odsouhlasování činností), nemá k dispozici dostatečné úložiště pro offline zálohy nebo nemá k dispozici dostatečný HW potřebný pro obnovu systému apod.	náhodný/záměrný	vnější
	26	narušení bezpečnosti Společnosti porušením bezpečnostní politiky na straně zákazníka	2	3	6	Hrozba může být způsobena např. vědomým používáním zastaralých SW nástrojů v systému zákazníka, což může mít dopad v systému Společnosti (výskyt zranitelností - nedostatečná úroveň bezpečnosti). Příp. může dojít k rozšíření incidentu ze systému zákazníka do systému Společnosti.	náhodný/záměrný	vnější
Fyzická bezpečnost	27	narušení fyzické bezpečnosti	1	1	1	Hrozba spočívá v narušení perimetru fyzické bezpečnosti v důsledku úmyslného narušení prvků fyzické ochrany. Realizací hrozby může dojít k poškození aktiva v závislosti na umístnění daného aktiva a úrovni zajištění jeho fyzické bezpečnosti.	záměrný	vnější
	28	živelní pohromy a neočekávané události (záplava, vítr, oheň, blesk, zemětřesení atp.)	1	1	1	Hrozba spočívá v působení přírodních živlů na aktiva organizace, které můžou mít za následek omezení dostupnosti služby v důsledku výskytu sekundárních dopadů výskytu těchto nežádoucích živelních pohrom a jiných neočekávaných událostí.	náhodný	vnější
	29	přinucení pracovníka k činnosti porušující bezpečnostní politiku (fyzický nebo psychický nátlak, vydírání)	1	4	4	Hrozba může být realizována buď přímo (fyzicky) nebo prostředky vzdálené komunikace, kdy útočník působí na pracovníka Společnosti (fyzický/psychický nátlak, vydírání apod.) s cílem přinutit ho provést podvratnou činnost v systému Společnosti nebo v systému zákazníka.	záměrný	vnější
Externí hrozby (útoky)	30	cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	3	2	6	Hrozba spočívá v narušení nebo úplném znemožnění poskytování služby v důsledku realizace kybernetického útoku, ke kterému může dojít v důsledku nedostatečné ochrany na vnějším perimetru sítě a/nebo nedostatečné edukace zainteresovaných osob (zaměstnanci, dodavatelé) v oblasti kybernetické bezpečnosti.	záměrný	vnější
	31	napadení elektronické komunikace (odposlech, modifikace)	2	2	4	Hrozba spočívá v neoprávněném proniknutí do síťové infrastruktury, odposlechu komunikace s dopadem na narušení důvěrnosti a/nebo její modifikaci s dopadem na zachování integrity a případně i dostupnosti komunikace.	záměrný	vnější
	32	síťové DoS, DDoS útoky, SPAM	1	1	1	Hrozba spočívá v zablokování komunikace zahlcením komunikačních linek, síťových prvků nebo jiných aktiv dostupných po síti nebo vzdáleně.	záměrný	vnější
	33	škodlivý kód, počítačové viry	2	2	4	Hrozba spočívá v zavedení škodlivých kódů/programů do provozovaných systémů nebo do vytvářených zdrojových kódů/aplikací v důsledku porušení definovaných bezpečnostních politik, neoprávněného nakládání s používaným HW a SW a/nebo nedostatočného bezpečnostního povědomí uživatelů.	záměrný	vnější
	34	externí průnik do vnitřního systému organizace po síti	2	2	4	Hrozba spočívá v provedení úspěšného hackerského útoku na systém Společnosti.	záměrný	vnější
	35	zneužití systému nebo zdrojů organizace k průniku do systému zákazníka (supply chain attack)	2	4	8	Hrozba spočívá v průniku externího útočníka do systému zákazníka prostřednictvím systému Společnosti, přičemž tohoto může dosáhnout např. úspěšným hackerským útokem na síť Společnosti, úspěšným útokem na jednotlivé uživatele/pracovníky Společnosti (sociální inženýrství), neautorizovaným zásahem do zdojových kódů řídícího informačního systému nebo jiných aplikací poskytovaných zákazníkům.	záměrný	vnější

A.3 Katalóg zraniteľností

Príloha obsahuje kompletný katalóg všetkých identifikovaných zraniteľností spoločne s ich hodnotením. Pre každú zraniteľnosť je stanovená hodnota veličiny **úroveň zraniteľnosti** na škále v rozmedzí 1 (nízka) až 4 (vysoká).

ID	Zranitelnost	Úroveň zranitelnosti
1	nedostatečná analýza a řízení rizik organizace	2
2	nedostatečná bezpečnostní dokumentace	2
3	nedostatočné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	2
4	nedostatečná podpora bezpečnosti ze strany vedení organizace	2
5	nedostatočné vymezení zásad pro bezpečnost informací v řízení projektu	3
6	nedostatečné vymezení zásad pro práci s mobilními zařízeními	1
7	nedostatečné bezpečnostní povědomí uživatelů	1
8	nedostatečná opatření pro ochranu technických a informačních aktiv	1
9	nedostatečná pravidla pro řízení prístupu	2
10	nevhodné nastavení přístupových oprávnění	2
11	kryptografické prostředky za účelem ochrany informací nejsou používány nebo jsou používány zranitelné	2
12	nedostatky v zabezpečení fyzického přístupu	1
13	provozní postupy a odpovědnosti nejsou dostatečně vymezeny a dokumentovány	2
14	nedostatečné oddělení vývojového, testovacího a produkčního prostředí	1
15	nedostatečná ochrana proti škodlivému kódu	2
16	nejsou realizovány pravidelné zálohy informací	2
17	nedostatečné monitorování událostí v systému	2
18	nejsou definovány pravidla a bezpečnostní požadavky pro nasazení softwaru	1
19	technické zranitelnosti nejsou systematicky identifikovány a řízeny	2
20	nedostatečná ochrana dat při přenosu mimo interní síť	1
21	nedostatečná ochrana vnějšího perimetru sítě	1
22	nedostatečne definované bezpečnostní požadavky pro akvizici a vývoj	3
23	nedostatečné řízení změn systémů	2
24	nedostatečné řízení dodavatelských vztahů	1
25	nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	3
26	nejsou ustanoveny plány a postupy pro řízení kontinuity činností	2
27	není zajištěn soulad s právními a smluvními požadavky nebo je soulad nedostatečný	1
28	nedostatečná identifikace zákonných požadavků	1
29	nedostatečná ochrana duševního vlastnictví	1
30	nedostatečná ochrana soukromí a osobních udajů	1
31	nedostatečné přezkoumávání bezpečnosti informací	1

A.4 Väzby hrozby-zraniteľnosti

Príloha obsahuje maticu reprezentujúcu väzby medzi identifikovanými hrozbami a zraniteľnosťami. Tieto väzby vypovedajú o skutočnosti, ktoré z identifikovaných zraniteľností môžu svojou prítomnosťou prispieť k realizácii ktorých hrozieb.
Relácie, ktoré sa medzi jednotlivými hrozbami a zraniteľnosťami môžu vyskytnúť, sú nasledujúce:

- „0“ – zraniteľnosť neprispieva k realizácii danej hrozby,
- „1“ – zraniteľnosť prispieva k realizácii danej hrozby.

Hrozby

		neúmyslné porušení bezpečnostní politiky ze strany uživatele	neúmyslné porušení bezpečnostní politiky ze strany administrátora	úmyslné porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatele	úmyslné porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátora	ztráta jednoho nebo více klíčových zaměstnanců	nedostatek zamestnanců s potřebnou odbornou úrovní na pracovním trhu	náhlá indispozice nebo nedostupnost servisního pracovníka	snížení úrovně bezpečnosti v důsledku nevhodné firemní kultury	snižování úrovně bezpečnosti v důsledku nedostatečných investic	snižování úrovně bezpečnosti a služeb z důvodu nedostatečné personální kapacity pro vedení zaměstnanců	pokuta nebo jiný postih Společnosti z důvodu porušení zákonných povinností	poškození nebo selhání technického anebo programového vybavení organizace	porušení dostupnosti nebo integrity zdrojových kódu vyvíjeného SW	omezení, nedostupnost monitoringu systému	zneužití vyměnitelných technických nosičů dat	ztráta, odcizení nebo poškození technického aktiva uživatelů (NTB, PC, mobily)	ztráta, odcizení nebo poškození klíčových technických aktiv firmy (servery, infrastruktura)	přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	okamžitá nedostupnost prostředků pro zajištění služeb (auto, autopark, vybavení servisního pracovníka)	nefunkčnost spojení mezi servisním pracovištěm a systémem zákazníka	nedodržení smluvního závazku ze strany dodavatele	selhání služeb dodavatele, narušení dodávky	neúmyslná chyba pracovníka dodavatele	úmyslné odcizení nebo poškození aktiva Společnosti pracovníkem dodavatele	narušení služeb (SLA) Společnosti z důvodu nesouladu nebo nespolupráce na straně zákazníka	narušení bezpečnosti Společnosti porušením bezpečnostní politiky na straně zákazníka	narušení fyzické bezpečnosti	živelní pohromy a neočekávané události (záplava, vítr, oheň, blesk, zemětřesení atp.)	přinucení pracovníka k činnosti porušující bezpečnostní politiku (fyzický nebo psychický nátlak, vydírání)	cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	napadení elektronické komunikace (odposlech, modifikace)	síťové DoS, DDoS útoky, SPAM	škodlivý kód, počítačové viry	externí průnik do vnitřního systému organizace po síti	zneužití systému nebo zdrojů organizace k průniku do systému zákazníka
Zranitelnost	ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
nedostatečná analýza a řízení rizik organizace	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
nedostatečná bezpečnostní dokumentace	2	1	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	1	1	1	1
nedostatočné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	3	1	1	0	0	0	0	0	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	1	1
nedostatečná podpora bezpečnosti ze strany vedení organizace	4	1	1	1	1	1	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
nedostatečné vymezení zásad pro bezpečnost informací v řízení projektu	5	1	1	0	0	0	0	1	1	1	1	1	0	0	1	1	0	0	0	1	1	1	0	1	0	1	0	0	0	0	0	0	0	0	1	1
nedostatečné vymezení zásad pro práci s mobilními zařízeními	6	1	1	0	0	0	0	0	0	1	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1
nedostatečné bezpečnostní povědomí uživatelů	7	1	1	0	0	0	0	0	0	1	1	1	0	1	0	1	1	1	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	1	1	1
nedostatečná opatření pro ochranu aktiv	8	1	1	0	0	0	0	0	1	1	1	1	1	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
nedostatečná pravidla pro řízení přístupu	9	1	1	1	1	0	0	0	1	1	1	1	0	1	0	0	1	1	0	0	0	0	0	1	1	0	0	0	0	1	1	1	0	1	1	1
nevhodné nastavení přístupových oprávnění	10	1	1	1	1	0	0	0	1	1	1	1	0	1	0	0	1	1	0	0	1	1	1	1	1	0	0	0	0	1	1	1	0	1	1	1
kryptografické prostředky za účelem ochrany informací nejsou používány nebo jsou používány zranitelné	11	1	1	1	1	0	0	0	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	1	1	0	0	0	0	1	0	1	0	0	1	1
nedostatky v zabezpečení fyzického přístupu	12	1	1	1	1	0	0	0	1	1	1	1	1	1	0	1	1	1	1	1	1	0	0	1	1	0	0	1	0	1	1	0	0	0	0	1
provozní postupy a odpovědnosti nejsou dostatečně vymezeny a dokumentovány	13	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	1
nedostatečné oddělení vývojového, testovacího a produkčního prostředí	14	1	1	1	1	0	0	0	0	1	1	1	1	1	1	0	1	1	0	0	0	0	0	1	1	0	0	0	0	1	1	1	1	1	1	1
nedostatečná ochrana proti škodlivému kódu	15	1	1	0	0	0	0	0	0	1	1	1	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1
nejsou realizovány pravidelné zálohy informací	16	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
nedostatečné monitorování událostí v systému	17	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	1	0	1	0	1	0	0	1	1	0	1	1	0	1	1	1	1	1	1	1
nejsou definovány pravidla a bezpečnostní požadavky pro nasazení softwaru	18	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	1	1	1
technické zranitelnosti nejsou systematicky identifikovány a řízeny	19	0	0	1	1	0	0	0	1	1	1	1	1	1	1	1	n	0	0	0	1	0	0	0	1	0	0	0	0	0	1	1	1	1	1	1
nedostatečná ochrana dat při přenosu mimo interní síť	20	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	1	1	1
nedostatečná ochrana vnějšího perimetru sítě	21	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	1	1	1	1	1
nedostatečne definované bezpečnostní požadavky pro akvizici a vývoj	22	1	1	1	1	0	0	0	1	1	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1
nedostatečné řízení změn systémů	23	1	1	1	1	0	0	0	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1
nedostatečné řízení dodavatelských vztahů	24	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	1	1	1	0	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1
nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	25	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1	1	1
nejsou ustanoveny plány a postupy pro řízení kontinuity činností	26	1	1	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
není zajištěn soulad s právními a smluvními požadavky nebo je soulad nedostatečný	27	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0
nedostatečná identifikace zákonných požadavků	28	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
nedostatečná ochrana duševního vlastnictví	29	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
nedostatečná ochrana soukromí a osobních udajů	30	0	0	0	0	1	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0
nedostatečné přezkoumávání bezpečnosti informací	31	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	1	1	0	1	1	1	1	1	1	1	1

A.5 Väzby hrozby-aktíva

Príloha obsahuje maticu reprezentujúcu väzby medzi identifikovanými hrozbami a jednotlivými aktívami Spoločnosti. Tieto väzby vypovedajú o skutočnosti, ktoré z identifikovaných hrozieb môžu nežiadúcim spôsobom pôsobiť na ktoré aktívum, resp. aktíva. Možné relácie, ktoré sa medzi jednotlivými hrozbami a aktívami môžu vyskytnúť, sú nasledujúce:

- „0“ – hrozba nemôže nežiadúcim spôsobom pôsobiť na dané aktívum,
- „1“ – hrozba môže nežiadúcim spôsobom pôsobiť na dané aktívum.

Hrozby

1. neúmyslné porušení bezpečnostní politiky ze strany uživatele
2. neúmyslné porušení bezpečnostní politiky ze strany administrátora
3. úmyslné porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatele
4. úmyslné porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátora
5. ztráta jednoho nebo více klíčových zaměstnanců
6. nedostatek zaměstnanců s potřebnou odbornou úrovní na pracovním trhu
7. náhlá indispozice nebo nedostupnost servisního pracovníka
8. snížení úrovně bezpečnosti v důsledku nevhodné firemní kultury
9. snižování úrovně bezpečnosti v důsledku nedostatečných investic
10. snižování úrovně bezpečnosti a služeb z důvodu nedostatečné personální kapacity pro vedení zaměstnanců
11. pokuta nebo jiný postih Společnosti z důvodu porušení zákonných povinností
12. poškození nebo selhání technického anebo programového vybavení organizace
13. porušení dostupnosti nebo integrity zdrojových kódu vyvíjeného SW
14. omezení, nedostupnost monitoringu systému
15. zneužití vyměnitelných technických nosičů dat
16. ztráta, odcizení nebo poškození technického aktiva uživatelů (NTB, PC, mobily)
17. ztráta, odcizení nebo poškození klíčových technických aktiv firmy (servery, infrastruktura)
18. přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb
19. okamžitá nedostupnost prostředků pro zajištění služeb (auto, autopark, vybavení servisního pracovníka)
20. nefunkčnost spojení mezi servisním pracovištěm a systémem zákazníka
21. nedodržení smluvního závazku ze strany dodavatele
22. selhání služeb dodavatele, narušení dodávky
23. neúmyslná chyba pracovníka dodavatele
24. úmyslné odcizení nebo poškození aktiva Společnosti pracovníkem dodavatele
25. narušení služeb (SLA) Společnosti z důvodu nesouladu nebo nespolupráce na straně zákazníka
26. narušení bezpečnosti Společnosti porušením bezpečnostní politiky na straně zákazníka
27. narušení fyzické bezpečnosti
28. živelní pohromy a neočekávané události (záplava, vítr, oheň, blesk, zemětřesení atp.)
29. přinucení pracovníka k činnosti porušující bezpečnostní politiku (fyzický nebo psychický nátlak, vydírání)
30. cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik
31. napadení elektronické komunikace (odposlech, modifikace)
32. síťové DoS, DDoS útoky, SPAM
33. škodlivý kód, počítačové viry
34. externí průnik do vnitřního systému organizace po síti
35. zneužití systému nebo zdrojů organizace k průniku do systému zákazníka

Aktiva	ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
Budova a její podpůrná infrastruktura - Pracoviště_1	1	1	1	1	1	0	0	0	1	1	1	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0
Budova a její podpůrná infrastruktura - Pracoviště_2	2	1	1	1	1	0	0	0	1	1	1	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0
Budova a její podpůrná infrastruktura - Pracoviště_3	3	1	1	1	1	0	0	0	1	1	1	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0
Serverovna - Pracoviště_1	4	0	1	0	1	0	0	0	1	1	1	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0
Serverovna - Pracoviště_2	5	0	1	0	1	0	0	0	1	1	1	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0
Serverovna - Pracoviště_3	6	0	1	0	1	0	0	0	1	1	1	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0
Autopark - ČR	7	1	1	1	1	0	0	0	1	1	1	1	1	0	0	0	1	1	0	0	0	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0
Autopark - SR	8	1	1	1	1	0	0	0	1	1	1	1	1	0	0	0	1	1	0	0	0	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0
LAN - síťová infrastruktura - KII - Pracoviště_1	9	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
LAN - síťová infrastruktura - Společnost - Pracoviště_1	10	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
WiFi infrastruktura - Pracoviště_1	11	0	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Vývojové servery - Pracoviště_1	12	1	1	0	1	1	0	0	1	1	1	1	1	1	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Ostatní servery - KII - Pracoviště_1	13	1	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Ostatní servery - Společnost - Pracoviště_1	14	1	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Docházkový systém a EZS - Pracoviště_1	15	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Kamerový systém - Pracoviště_1	16	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Stanice, notebooky, mobilní telefony - KII - Pracoviště_1	17	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Stanice, notebooky, mobilní telefony - Společnost - Pracoviště_1	18	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Ostatní HW a periférie - Pracoviště_1	19	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
LAN - síťová infrastruktura - KII - Pracoviště_2	20	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
LAN - síťová infrastruktura - Společnost - Pracoviště_2	21	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
WiFi infrastruktura - Pracoviště_2	22	0	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Ostatní servery - KII - Pracoviště_2	23	1	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Ostatní servery - Společnost - Pracoviště_2	24	1	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Docházkový systém a EZS - Pracoviště_2	25	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Kamerový systém - Pracoviště_2	26	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Stanice, notebooky, mobilní telefony - KII - Pracoviště_2	27	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Stanice, notebooky, mobilní telefony - Společnost - Pracoviště_2	28	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Ostatní HW a periférie - Pracoviště_2	29	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
LAN - síťová infrastruktura - KII - Pracoviště_3	30	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
LAN - síťová infrastruktura - Společnost - Pracoviště_3	31	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
WiFi infrastruktura - Pracoviště_3	32	0	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Ostatní servery - KII - Pracoviště_3	33	1	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Ostatní servery - Společnost - Pracoviště_3	34	1	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Docházkový systém a EZS - Pracoviště_3	35	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Kamerový systém - Pracoviště_3	36	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Stanice, notebooky, mobilní telefony - KII - Pracoviště_3	37	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Stanice, notebooky, mobilní telefony - Společnost - Pracoviště_3	38	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Ostatní HW a periférie - Pracoviště_3	39	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
IDM	40	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0
Redmine	41	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0
Nextcloud	42	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0
Antivirový SW	43	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1	0
SIEM	44	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0
VPN	45	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	1	0	0	0	0	0	0	0	1	1	0	1	1	1	0
VPN spojení	46	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	1	0	0	0	0	0	0	0	1	1	0	1	1	1	1
Účetní SW	47	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1	0
Virtualizace	48	0	1	0	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1	0
Testovací systémy	49	1	1	1	1	1	0	0	1	1	1	1	1	1	1	0	1	1	1	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1	0
Operační systémy	50	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1	0
Další drobný a kancelářský SW	51	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1	0
Zaměstnanci - KII - Pracoviště_1, Pracoviště_2	52	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0

	Hrozby	neúmyslné porušení bezpečnostní politiky ze strany uživatele	neúmyslné porušení bezpečnostní politiky ze strany administrátora	úmyslné porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatele	úmyslné porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátora	ztráta jednoho nebo více klíčových zaměstnanců	nedostatek zamestnanců s potřebnou odbornou úrovní na pracovním trhu	náhlá indispozice nebo nedostupnost servisního pracovníka	snížení úrovně bezpečnosti v důsledku nevhodné firemní kultury	snižování úrovně bezpečnosti v důsledku nedostatečných investic	snižování úrovně bezpečnosti a služeb z důvodu nedostatečné personální kapacity pro vedení zaměstnanců	pokuta nebo jiný postih Společnosti z důvodu porušení zákonných povinností	poškození nebo selhání technického anebo programového vybavení organizace	porušení dostupnosti nebo integrity zdrojových kódu vyvíjeného SW	omezení , nedostupnost monitoringu systému	zneužití vyměnitelných technických nosičů dat	ztráta, odcizení nebo poškození technického aktiva uživatelů (NTB, PC, mobily)	ztráta, odcizení nebo poškození klíčových technických aktiv firmy (servery, infrastruktura)	přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	okamžitá nedostupnost prostředků pro zajištění služeb (auto, autopark, vybavení servisního pracovníka)	nefunkčnost spojení mezi servisním pracovištěm a systémem zákazníka	nedodržení smluvního závazku ze strany dodavatele	selhání služeb dodavatele, narušení dodávky	neúmyslná chyba pracovníka dodavatele	úmyslné odcizení nebo poškození aktiva Společnosti pracovníkem dodavatele	narušení služeb (SLA) Společnosti z důvodu nesouladu nebo nespolupráce na straně zákazníka	narušení bezpečnosti Společnosti porušením bezpečnostní politiky na straně zákazníka	narušení fyzické bezpečnosti	živelní pohromy a neočekávané události (záplava, vítr, oheň, blesk, zemětřesení atp.)	přinucení pracovníka k činnosti porušující bezpečnostní politiku (fyzický nebo psychický nátlak, vydírání)	cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	napadení elektronické komunikace (odposlech, modifikace)	síťové DoS, DDoS útoky, SPAM	škodlivý kód, počítačové viry	externí průnik do vnitřního systému organizace po síti	zneužití systému nebo zdrojů organizace k průniku do systému zákazníka
Aktiva	ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
Zaměstnanci - Vývoj - Pracoviště_1, Pracoviště_2	53	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Zaměstnanci - Společnost - Pracoviště_1, Pracoviště_2	54	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Zaměstnanci - KII - Pracoviště_3	55	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Zaměstnanci - Vývoj - Pracoviště_3	56	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Zaměstnanci - Společnost - Pracoviště_3	57	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0
Data - Systém	58	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	0	1	1	1
Data - vývoj SW	59	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	1	1	0
Data - vývoj HW	60	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	1	1	0
Data - účetnictví a ekonomika	61	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	0	1	1	1	1	1	1	0	1	1	0
Data - personalistika	62	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	1	1	0
Data - provoz - ČR	63	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0
Data - provoz - SR	64	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0
Data - nabídky - ČR	65	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	1	1	0
Data - nabídky- SR	66	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	1	1	0
Data - smlouvy - ČR	67	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	1	1	0
Data - smlouvy - SR	68	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	1	1	0
Data - archiv - Pracoviště_1	69	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0
Data - archiv - Pracoviště_3	70	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0
Data - ISMS a BCMS	71	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0
Data - QMS	72	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0
Data - BOZP	73	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0
Data - EMS	74	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0
Data - Gsuite	75	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	0	0	1	1	1	1	1	0	1	1	0
Data - Datové schránky	76	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0
Servis - Zákazník_1	77	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Servis - Zákazník_2	78	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Servis - Zákazník_3	79	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Servis - Zákazník_4	80	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Servis - Zákazník_5	81	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Servis - Zákazník_6	82	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
Hotline - Pracoviště_1	83	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	1
Hotline - Pracoviště_3	84	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	1
Dodávka řídícího informačního systému	85	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
ISP - Pracoviště_1	86	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	0	0	0
Záložní ISP - Pracoviště_1	87	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	0	0	0
ISP - Pracoviště_2	88	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	0	0	0
Mobilní a datové služby - ČR	89	0	0	1	1	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	0	0	0
Utility služby - Pracoviště_1	90	0	0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	0	0	0	0
Utility služby - Pracoviště_2	91	0	0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	0	0	0	0
ISP - Pracoviště_3	92	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	0	0	0
Mobilní a datové služby - SR	93	0	0	1	1	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	0	0	0
Utility služby - Pracoviště_3	94	0	0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	0	0	0	0
Gsuite	95	0	0	0	1	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	0	1	0	1	1	1	1	0
vpsFree cloud hosting	96	0	0	0	1	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	0	1	0	1	1	1	1	0
Hosting web stránek	97	0	0	0	1	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	1	0	0	0	0	1	0	1	1	1	1	0
Vývoj SW	98	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	0	1	1	1	1	1	1	1	1	1	0
Interní IT podpora	99	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1	0
Office služby - Pracoviště_1	100	0	0	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1	0
Office služby - Pracoviště_2	101	0	0	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1	0
Office služby - Pracoviště_3	102	0	0	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1	0

A.6 Väzby aktíva-zraniteľnosti

Príloha obsahuje maticu reprezentujúcu väzby medzi identifikovanými zraniteľnosťami a jednotlivými aktívami Spoločnosti. Tieto väzby vypovedajú o skutočnosti, ktoré z identifikovaných zraniteľností sa môžu vyskytnúť na ktorých aktívach, a teda môžu byť zneužité niektorou z hrozieb k uplatneniu jej nežiadúceho vplyvu na dané aktívum. Relácie, ktoré sa medzi jednotlivými aktívami a zraniteľnosťami môžu vyskytnúť, sú nasledujúce:

- „0“ – zraniteľnosť nie je relevantná (nemôže sa objaviť) pre dané aktívum,
- „1“ – zraniteľnosť je relevantná (môže sa objaviť) pre dané aktívum.

Zranitelnosti

		nedostatečná analýza a řízení rizik organizace	nedostatečná bezpečnostní dokumentace	nedostatočné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	nedostatečná podpora bezpečnosti ze strany vedení organizace	nedostatočné vymezení zásad pro bezpečnost informací v řízení projektu	nedostatečné vymezení zásad pro práci s mobilními zařízeními	nedostatečné bezpečnostní povědomí uživatelů	nedostatečná opatření pro ochranu aktiv	nedostatečná pravidla pro řízení přístupu	nevhodné nastavení přístupových oprávnění	kryptografické prostředky za účelem ochrany informací nejsou používány nebo jsou používány zranitelné	nedostatky v zabezpečení fyzického přístupu	provozní postupy a odpovědnosti nejsou dostatečně vymezeny a dokumentovány	nedostatečné oddělení vývojového, testovacího a produkčního prostředí	nedostatečná ochrana proti škodlivému kódu	nejsou realizovány pravidelné zálohy informací	nedostatečné monitorování událostí v systému	nejsou definovány pravidla a bezpečnostní požadavky pro nasazení softwaru	technické zranitelnosti nejsou systematicky identifikovány a řízeny	nedostatečná ochrana dat při přenosu mimo interní síť	nedostatečná ochrana vnějšího perimetru sítě	nedostatečne definované bezpečnostní požadavky pro akvizici a vývoj	nedostatečné řízení změn systémů	nedostatečné řízení dodavatelských vztahů	nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	nejsou ustanoveny plány a postupy pro řízení kontinuity činností	není zajištěn soulad s právními a smluvními požadavky nebo je soulad nedostatečný	nedostatečná identifikace zákonných požadavků	nedostatečná ochrana duševního vlastnictví	nedostatečná ochrana soukromí a osobních údajů	nedostatečné přezkoumávání bezpečnosti informací
Aktiva	ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Budova a její podpůrná infrastruktura - Pracoviště_1	1	1	1	1	1	0	0	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Budova a její podpůrná infrastruktura - Pracoviště_2	2	1	1	1	1	0	0	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Budova a její podpůrná infrastruktura - Pracoviště_3	3	1	1	1	1	0	0	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Serverovna - Pracoviště_1	4	1	1	1	1	0	0	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Serverovna - Pracoviště_2	5	1	1	1	1	0	0	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Serverovna - Pracoviště_3	6	1	1	1	1	0	0	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Autopark - CR	7	1	1	1	1	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Autopark - SR	8	1	1	1	1	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
LAN - síťová infrastruktura - KII - Pracoviště_1	9	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	1	1	0	0	0	0	1
LAN - síťová infrastruktura - Společnost - Pracoviště_1	10	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	1	1	0	0	0	0	1
WiFi infrastruktura - Pracoviště_1	11	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	1	1	0	0	0	0	1
Vývojové servery - Pracoviště_1	12	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Ostatní servery - KII - Pracoviště_1	13	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Ostatní servery - Společnost - Pracoviště_1	14	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Docházkový systém a EZS - Pracoviště_1	15	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Kamerový systém - Pracoviště_1	16	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Stanice, notebooky, mobilní telefony - KII - Pracoviště_1	17	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Stanice, notebooky, mobilní telefony - Společnost - Pracoviště_1	18	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Ostatní HW a periférie - Pracoviště_1	19	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
LAN - síťová infrastruktura - KII - Pracoviště_2	20	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	1	1	0	0	0	0	1
LAN - síťová infrastruktura - Společnost - Pracoviště_2	21	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	1	1	0	0	0	0	1
WiFi infrastruktura - Pracoviště_2	22	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	1	1	0	0	0	0	1
Ostatní servery - KII - Pracoviště_2	23	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Ostatní servery - Společnost - Pracoviště_2	24	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Docházkový systém a EZS - Pracoviště_2	25	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Kamerový systém - Pracoviště_2	26	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Stanice, notebooky, mobilní telefony - KII - Pracoviště_2	27	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Stanice, notebooky, mobilní telefony - Společnost - Pracoviště_2	28	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Ostatní HW a periférie - Pracoviště_2	29	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
LAN - síťová infrastruktura - KII - Pracoviště_3	30	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	1	1	0	0	0	0	1
LAN - síťová infrastruktura - Společnost - Pracoviště_3	31	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	1	1	0	0	0	0	1
WiFi infrastruktura - Pracoviště_3	32	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	1	1	1	0	1	1	0	0	0	0	1
Ostatní servery - KII - Pracoviště_3	33	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Ostatní servery - Společnost - Pracoviště_3	34	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Docházkový systém a EZS - Pracoviště_3	35	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Kamerový systém - Pracoviště_3	36	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Stanice, notebooky, mobilní telefony - KII - Pracoviště_3	37	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Stanice, notebooky, mobilní telefony - Společnost - Pracoviště_3	38	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
Ostatní HW a periférie - Pracoviště_3	39	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1
IDM	40	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
Redmine	41	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
Nextcloud	42	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
Antivirový SW	43	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
SIEM	44	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
VPN	45	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
VPN spojení	46	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
Účetní SW	47	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
Virtualizace	48	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1

Zranitelnosti

Aktiva	ID	1 nedostatečná analýza a řízení rizik organizace	2 nedostatečná bezpečnostní dokumentace	3 nedostatočné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	4 nedostatečná podpora bezpečnosti ze strany vedení organizace	5 nedostatočné vymezení zásad pro bezpečnost informácií v řízení projektu	6 nedostatečné vymezení zásad pro práci s mobilními zařízeními	7 nedostatečné bezpečnostní povědomí uživatelů	8 nedostatečná opatření pro ochranu aktiv	9 nedostatečná pravidla pro řízení přístupu	10 nevhodné nastavení přístupových oprávnění	11 kryptografické prostředky za účelem ochrany informací nejsou používány nebo jsou používány zranitelné	12 nedostatky v zabezpečení fyzického přístupu	13 provozní postupy a odpovědnosti nejsou dostatečně vymezeny a dokumentovány	14 nedostatečné oddělení vývojového, testovacího a produkčního prostředí	15 nedostatečná ochrana proti škodlivému kódu	16 nejsou realizovány pravidelné zálohy informací	17 nedostatečné monitorování událostí v systému	18 nejsou definovány pravidla a bezpečnostní požadavky pro nasazení softwaru	19 technické zranitelnosti nejsou systematicky identifikovány a řízeny	20 nedostatečná ochrana dat při přenosu mimo interní síť	21 nedostatečná ochrana vnějšího perimetru sítě	22 nedostatečne definované bezpečnostní požadavky pro akvizici a vývoj	23 nedostatečné řízení změn systémů	24 nedostatečné řízení dodavatelských vztahů	25 nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	26 nejsou ustanoveny plány a postupy pro řízení kontinuity činností	27 není zajištěn soulad s právními a smluvními požadavky nebo je soulad nedostatečný	28 nedostatečná identifikace zákonných požadavků	29 nedostatečná ochrana duševního vlastnictví	30 nedostatečná ochrana soukromí a osobních údajů	31 nedostatečné přezkoumávání bezpečnosti informací
Testovací systémy	49	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
Operační systémy	50	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
Další drobný a kancelářský SW	51	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
Zaměstnanci - KII - Pracoviště_1, Pracoviště_2	52	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1
Zaměstnanci - Vývoj - Pracoviště_1, Pracoviště_2	53	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1
Zaměstnanci - Společnost - Pracoviště_1, Pracoviště_2	54	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1
Zaměstnanci - KII - Pracoviště_3	55	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1
Zaměstnanci - Vývoj - Pracoviště_3	56	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1
Zaměstnanci - Společnost - Pracoviště_3	57	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1
Data - Systém	58	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	1	0	1	1	1	1	1	0	1
Data - vývoj SW	59	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	1	0	1	1	1	1	1	0	1
Data - vývoj HW	60	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	1	0	1	1	1	1	1	0	1
Data - účetnictví a ekonomika	61	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	1	1
Data - personalistika	62	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	1	1
Data - provoz - ČR	63	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - provoz - SR	64	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - nabídky - ČR	65	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - nabídky- SR	66	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - smlouvy - ČR	67	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - smlouvy - SR	68	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - archiv - Pracoviště_1	69	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - archiv - Pracoviště_3	70	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - ISMS a BCMS	71	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - QMS	72	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - BOZP	73	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - EMS	74	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - Gsuite	75	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Data - Datové schránky	76	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	0	1
Servis - Zákazník_1	77	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1
Servis - Zákazník_2	78	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1
Servis - Zákazník_3	79	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1
Servis - Zákazník_4	80	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1
Servis - Zákazník_5	81	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1
Servis - Zákazník_6	82	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1
Hotline - Pracoviště_1	83	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	1	0	1	1	0	1	1	1	1	1	0	1
Hotline - Pracoviště_3	84	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	1	0	1	1	0	1	1	1	1	1	0	1
Dodávka řídícího informačního systému	85	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	0	1	1	1	1	1	1	1	1	0	1
ISP - Pracoviště_1	86	1	1	0	1	0	0	0	1	0	0	0	0	1	0	1	0	1	0	0	0	0	1	1	1	0	1	0	0	0	0	1
Záložní ISP - Pracoviště_1	87	1	0	0	1	0	0	0	1	0	0	0	0	1	0	1	0	1	0	0	0	0	1	1	1	0	1	0	0	0	0	1
ISP - Pracoviště_2	88	1	0	0	1	0	0	0	1	0	0	0	0	1	0	1	0	1	0	0	0	0	1	1	1	0	1	0	0	0	0	1
Mobilní a datové služby - ČR	89	1	0	0	1	0	0	0	1	0	0	0	0	1	0	1	0	1	0	0	0	0	1	1	1	0	1	0	0	0	0	1
Utility služby - Pracoviště_1	90	1	0	0	1	0	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	1	1	0	1	0	0	0	0	1
Utility služby - Pracoviště_2	91	1	0	0	1	0	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	1	1	0	1	0	0	0	0	1
ISP - Pracoviště_3	92	1	0	0	1	0	0	0	1	0	0	0	0	1	0	1	0	1	0	0	0	0	1	1	1	0	1	0	0	0	0	1
Mobilní a datové služby - SR	93	1	0	0	1	0	0	0	1	0	0	0	0	1	0	1	0	1	0	0	0	0	1	1	1	0	1	0	0	0	0	1
Utility služby - Pracoviště_3	94	1	0	0	1	0	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	1	1	0	1	0	0	0	0	1
Gsuite	95	1	0	0	1	0	0	0	1	1	1	0	0	1	0	1	1	1	0	0	0	0	1	1	1	0	1	0	0	0	0	1
vpsFree cloud hosting	96	1	0	0	1	0	0	0	1	1	1	0	0	1	0	1	1	1	1	0	0	0	1	1	1	0	1	0	0	0	0	1
Hosting web stránek	97	1	0	0	1	0	0	0	1	1	1	0	0	1	0	1	1	1	1	0	0	0	1	1	1	0	1	0	0	0	0	1
Vývoj SW	98	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	1
Interní IT podpora	99	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0	0	1	0	0	0	0	1
Office služby - Pracoviště_1	100	1	1	1	1	0	1	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Office služby - Pracoviště_2	101	1	1	1	1	0	1	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	1
Office služby - Pracoviště_3	102	1	1	1	1	0	1	1	1	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	1

A.7 Prehľad rizík

Príloha obsahuje kompletný zoznam rizík, ktoré boli identifikované analýzou rizík vykonanou za účelom posúdenia úrovne bezpečnosti informácií v rámci Spoločnosti. Tento prehľad obsahuje všetky riziká zoradené zostupne v závislosti na ich hodnote (miere rizika), ktorá bola počas analýzy stanovená pre každé identifikované riziko. V závislosti na hodnote rizika je pre každé riziko stanovená jeho úroveň, tj. riziko je zaradené do príslušnej kategórie – kritické, vysoké, stredné alebo nízke riziko.

ID	Hrozba	Max. riziko	Úroveň rizika
R - H9	snižování úrovně bezpečnosti v důsledku nedostatečných investic	404,25	vysoké
R - H10	snižování úrovně bezpečnosti a služeb z důvodu nedostatečné personální kapacity pro vedení zaměstnanců	404,25	vysoké
R - H35	zneužití systému nebo zdrojů organizace k průniku do systému zákazníka (supply chain attack)	206,75	vysoké
R - H8	náhlé snížení úrovně bezpečnosti v důsledku nevhodné firemní kultury	182,03	vysoké
R - H1	neúmyslné porušení bezpečnostní politiky ze strany uživatele	152,23	střední
R - H2	neúmyslné porušení bezpečnostní politiky ze strany administrátora	152,23	střední
R - H11	pokuta nebo jiný postih Společnosti z důvodu porušení zákonných povinností	89,83	střední
R - H34	externí průnik do vnitřního systému organizace po síti	89,42	střední
R - H12	poškození nebo selhání technického anebo programového vybavení organizace (včetně chybné funkčnosti)	87,47	střední
R - H33	škodlivý kód, počítačové viry	69,67	střední
R - H31	napadení elektronické komunikace (odposlech, modifikace)	63,87	střední
R - H30	cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik	58,55	střední
R - H23	neúmyslná chyba pracovníka dodavatele	49,50	střední
R - H4	úmyslné porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany administrátora	47,90	střední
R - H13	porušení dostupnosti nebo integrity zdrojových kódu vyvíjeného SW	38,20	střední
R - H16	ztráta, odcizení nebo poškození technického aktiva uživatelů (NTB, PC, mobily)	36,19	střední
R - H17	ztráta, odcizení nebo poškození klíčových technických aktiv firmy (servery, infrastruktura)	32,65	střední
R - H20	nefunkčnost spojení mezi servisním pracovištěm a systémem zákazníka	32,65	střední
R - H3	úmyslné porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatele	23,95	střední
R - H29	přinucení pracovníka k činnosti porušující bezpečnostní politiku (fyzický nebo psychický nátlak, vydírání)	23,42	střední
R - H24	úmyslné odcizení nebo poškození aktiva Společnosti pracovníkem dodavatele	19,52	nízké
R - H15	zneužití vyměnitelných technických nosičů dat	18,54	nízké
R - H21	nedodržení smluvního závazku ze strany dodavatele	15,14	nízké
R - H22	selhání služeb dodavatele, narušení dodávky	11,71	nízké
R - H14	omezení, nedostupnost monitoringu systému	10,38	nízké
R - H18	přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb	9,05	nízké
R - H7	náhlá indispozice nebo nedostupnost servisního pracovníka	8,52	nízké
R - H32	síťové DoS, DDoS útoky, SPAM	8,46	nízké
R - H26	narušení bezpečnosti Společnosti porušením bezpečnostní politiky na straně zákazníka	7,10	nízké
R - H25	narušení služeb (SLA) Společnosti z důvodu nesouladu nebo nespolupráce na straně zákazníka	6,62	nízké
R - H19	okamžitá nedostupnost prostředků pro zajištění služeb (auto, autopark, vybavení servisního pracovníka)	4,26	nízké
R - H5	ztráta jednoho nebo více klíčových zaměstnanců	2,66	nízké
R - H6	nedostatek zaměstnanců s potřebnou odbornou úrovní na pracovním trhu	1,42	nízké
R - H27	narušení fyzické bezpečnosti	0,71	nízké
R - H28	živelní pohromy a neočekávané události (záplava, vítr, oheň, blesk, zemětřesení atp.)	0,44	nízké

A.8 Plán zvládania rizík

Príloha obsahuje kompletný Plán zvládania rizík, ktorý definuje zoznam bezpečnostných opatrení navrhnutých za účelom zníženia, resp. eliminácie nežiadúcich rizík identifikovaných vykonanou analýzou rizík bezpečnosti informácií v rámci interného prostredia Spoločnosti.

Pre každé z opatrení je definovaných niekoľko položiek, ktoré upresňujú a bližšie špecifikujú tieto navrhované opatrenia. Význam jednotlivých položiek je následujúci:

- **ID** – identifikačné číslo opatrenia, pod ktorým môže byť vedené aj v ďalších interných dokumentoch Spoločnosti,
- **datum vytvoření** – dátum definície opatrenia na základe výsledkov vykonanej analýzy rizík,
- **ISMS (POA) mapování** – priradenie navrhovaného opatrenia k existujúcemu opatreniu vedenému v rámci Prehlásenia o aplikovateľnosti,
- **rizika mapování** – zoznam rizík, ku ktorým sa navrhované opatrenie vzťahuje, tj. riziká, ktoré môžu byť v dôsledku zavedenia konkrétneho opatrenia ošetrené,
- **název opatření**,
- popis – bližšia charakteristika navrhovaného opatrenia,
- **cíle/přínosy** – aký vplyv na prebiehajúce procesy v rámci Spoločnosti bude mať zavedenie konkrétneho opatrenia,
- **odpovědnost** – definícia (meno) osoby, ktorá je zodpovedná za implementáciu a následné udržiavanie daného opatrenia,
- **spolupracuje** – ďalšia osoby, príp. osoby podieľajúce sa spoločne so zodpovednou osobou na implementácii a udržiavaní daného opatrenia,
- **priorita** – dôležitosť zavedenia navrhovaného opatrenia; typicky sa táto vlastnosť vzťahuje k závažnosti rizika, resp. rizík, ktoré majú byť vďaka zavedeniu opatrenia ošetrené,
- **termín (zavedení opatření/dokončení)** – očakávaný dátum konečného nasadenia opatrenia,
- **odhad nákladů, zdroje** – náklady, ktoré bude potrebné vynaložiť na zaobstaranie, zavedenie a následnú údržbu navrhovaného opatrenia,
- **stav implementace (%)** – miera implementácie daného opatrenia,
- **metrika vyhodnocení účinnosti opatření** – kritérium, na základe ktorého možno vyhodnotiť, či a do akej miery je implementované opatrenie účinné.

ID	Datum vytvoření	ISMS (POA) mapování	Rizika mapování	Název opatření	Popis	Cíle / přínosy	Odpovědnost	Spolupracuje	Priorita	Termín (zavedení opatření/ dokončení)	Odhad nákladů - zdroje (externí/interní, CZK/MDs)	Stav implementace (%)	Metrika vyhodnocení účinnosti opatření
1/2022	18.10.2022	A 5.4	R-H9, R-H10, R-H8	**Rozpočet KyBe**	Počínaje rokem 2023 sestavit na roční bázi rozpočet pro řízení kybernetické bezpečnosti, který bude zahrnovat jak nákladovou část (osobní náklady, náklady na technická opatření…), tak i porovnání s příjmy od zákazníků s novými smlouvami (jak budou postupně uzavírány). Rozpočet bude konzultován/schválen vedením Společnosti.	- Větší angažovanost některých členů vedení v rámci KyBe. - Větší přehled o nákladech na KyBe.	Zaměstnanec_1	Zaměstnanec_2	vysoká	1/2023	5 MD	0%	Existence a plnění rozpočtu na daný rok
2/2022	18.10.2022	A 5.2, A 5.4	R-H9, R-H10, R-H8	**Integrace MKB do vedení Společnosti**	Zajistit větší součinnost vedení Společnosti s řízením KyBe (MKB). Zajistit účast MKB na každém jednání představenstva Společnosti tak, aby mohl informovat jednotlivé členy vedení o aktuálním stavu KyBe a potřebných opatřeních k zajištění odpovídající úrovně KyBe v Společnosti. Reflektuje mj. doporučení z dohledového auditu vykonaného Certifikačním orgánem v r. 2022.	- Lepší operativní řízení bezpečnosti. - Lepší reakce Společnosti na změny v oblasti KyBe.	Zaměstnanec_1	Zaměstnanec_2	vysoká	1/2023	5 MD	0%	Účast MKB na všech jednáních ČR i SK představenstva
3/2022	18.10.2022	A 8.15, A 8.16	R-H35, R-H34, R-H33, R-H30, R-H4, R-H3	**SIEM - optimalizace korelačních pravidel**	Návrh nových pravidel a celkové odladění a ověření účinnosti stávajícího SIEM řešení.	- Větší pravděpodobnost detekce případných útoků - omezení rizika nedetekovaného útoku na Společnosti.	Zaměstnanec_2	Zaměstnanec_1, Zaměstnanec_3	střední	6/2023	20 MD	0%	SIEM je schopen detekovat běžné útoky
4/2022	18.10.2022	A 8.5, A 8.20, A 8.21, A8.22	R-H35, R-H34, R-H33, R-H30, R-H4, R-H3	**Obměna switchů v LAN**	Obnova zařízení infrastruktury LAN.	- Celkové zvýšení úrovně zabezpečení LAN Společnosti.	Zaměstnanec_1	Zaměstnanec_2, Zaměstnanec_3	vysoká	3/2023	4 mil. Kč	0%	Všechny switche v lokalitách Pracoviště_1 a Pracoviště_2 jsou vyměněné
5/2022	18.10.2022	A 5.35, A 5.36	R-H8, R-H11	**Interní audit ISMS a BCMS provedený externě**	Provedení interního auditu ISMS a BCMS externím auditorem.	- Získání vnějšího nezaujatého pohledu. - Úspora interních zdrojů. - Doklad úrovně ISMS a BCMS pro zákazníky.	Zaměstnanec_1	Zaměstnanec_2, Zaměstnanec_4, Zaměstnanec_5	střední	6/2023	220 tis. Kč	0%	Výstupy z interního auditu, zhodnocení stavu ISMS/BCMS, návrh dalšího postupu
6/2022	18.10.2022	A 8.8, A 8.25, A 8.26, A 8.27, A 8.28, A 8.29	R-H31, R-H32, R-H33, R-H34, R-H35	**Penetrační testy systému/aplikací řídicího informačního systému**	Provedení komplexních penetračních testů řídicího infroamčního systému nezávislým dodavatelem, použití výsledků ke zdokonalení SSDLC.	- Nalezení případných bezpečnostních děr/chyb v rámci řešení. - Zlepšení bezpečnosti vývoje řídicího informačního systému.	Zaměstnanec_1	Zaměstnanec_4	střední	2/2023	350 tis. Kč	0%	Výstupy z testů, největší chyby ve vývoji aplikací Společnosti, opatření směrem k vývoji SW
7/2022	18.10.2022	A 6.3	R-H1, R-H2, R-H16, R-H17, R-H29, R-H30	**Školení bezpečnostního povědomí zaměstnanců Společnosti**	Provést periodické školení všech zaměstnanců Společnosti v rozsahu: - seznámení s aktuálními hrozbami - seznámení s identifikovanými riziky z AR Společnosti - opakování nejdůležitějších bezpečnostních opatření a pravidel	- Omezení rizik spojených s uživateli a jejich chováním/chybami. - Zlepšení reakce na incidenty. - Seznámení zaměstnanců s aktuálními riziky.	Zaměstnanec_1	Zaměstnanec_3	střední	12/2022	5 MD	0%	% účasti zaměstnanců na školení
8/2022	18.10.2022	A 5.24, A 5.25, A 5.26, A 5.27	R-H31, R-H32, R-H33, R-H34, R-H35	**Revize procesu zvládání KBU/KBI**	Revidovat a zlepšit proces detekce, vyhodnocování a zvládání kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů - návaznost na sjednocení tiketovacího nástroje, evidenci vazby incidentu/události na KII/konkrétního zákazníka. Souvisí se zjištěním 9.1 auditu Zákazníka z r. 2021.	- Zajištění lepší návaznosti procesu na analýzu rizik a další oblasti KyBe.	Zaměstnanec_1	Zaměstnanec_3	nízká	12/2022	20 MD	0%	Přepracovaný proces zvládání KBU/KBI, aktualizovaná směrnice, existující návaznost na proces analýzy rizik
9/2022	18.10.2022	A 8.13, A 5.30	R-H12, R-H13, R-H16, R-H17	**Zálohování**	Popsat veškeré činnosti spojené se zálohováním do PO34, zejména umístění záloh (registr záloh), frekvenci zálohování, postupy obnovy systémů, testování záloh atd.	- Zlepšení předpokladů úspěšné obnovy po havárii. - Zprůhlednění oblasti zálohování v Společnosti.	Zaměstnanec_1	Zaměstnanec_2, Zaměstnanec_6	střední	6/2023	20 MD	0%	Seznam záloh, postupy pro obnovu nejdůležitějších systémů
10/2022	18.10.2022	A 8.25, A 8.26, A 8.27, A 8.28, A 8.29, A 8.30	R-H13	**SSDLC**	Implementace zásad, činností a postupů bezpečného vývoje do procesu vývoje řídicího informačního systému v rámci Společnosti. Základem bude průběžně rozvíjený a aktualizovaný model hrozeb řídicího informačního systému, ze kterého bude vycházet katalog doporučovaných opatření pro vývojáře jeho jednotlivých částí.	- Omezení rizik souvisejících s bezpečnostními chybami v rámci řídicího informačního systému.	Zaměstnanec_1	Zaměstnanec_2	vysoká	9/2023	30 MD	0%	Existence modelu hrozeb a katalogu opatření pro vývojáře
11/2022	18.10.2022	A 5.29, A 5.30	R-H18, R-H21, R-H22, R-H23	**Zlepšování plánů kontinuity**	Revidovat současné havarijní plány, rozpracovat k nim dílčí plány obnovy pro klíčové systémy.	- Zvýšit praktickou účinnost havarijních plánů a pravděpodobnosti úspěšné obnovy při reálné havárii.	Zaměstnanec_1	Zaměstnanec_3, Zaměstnanec_7	střední	6/2023	20 MD	0%	Zvýšení detailu havarijních plánů
12/2022	18.10.2022	A 5.37	R-H7, R-H19, R-H20	**Pracovní postupy pro servis**	Aktualizovat pracovní postupy (PO) pro Servis, zejména s ohledem na aktualizovaná smluvní pravidla a opatření KyBe.	- Omezit riziko negativních událostí u zákazníků a z toho plynoucích sankcí.	Zaměstnanec_1	Zaměstnanec_3	střední	3/2023	20 MD	0%	Existence pracovních postupů pro všechny zákazníky

B Kontrolný zoznam pre audit kybernetickej bezpečnosti

§ 3 – Systém řízení bezpečnosti informací

Tab. B.1: Zoznam auditných položiek k § 3 VoKB.

Odst.	Písm.	Auditná položka
	a)	Je stanovený rozsah ISMS?
	b)	Sú stanovené ciele ISMS?
	c)	Sú zavedené primerané bezpečnostné opatrenia?
	d)	Je zavedený proces riadenia rizík?
	e)	Je vytvorená, zavedená a schválená bezpečnostná politika v oblasti ISMS?
	f)	Je uskutočňovaný audit kybernetickej bezpečnosti v pravidelných intervaloch alebo pri významných zmenách?
	g)	Dochádza k pravidelnému vyhodnocovaniu účinnosti zavedeného ISMS, ktoré obsahuje hodnotenie aktuálneho stavu ISMS vrátane revízie hodnotenia rizík, posúdenia výsledkov vykonaných auditov kybernetickej bezpečnosti a dopadov kybernetických bezpečnostných incidentov na ISMS?
	h)	Sú priebežne identifikované významné zmeny spadajúce do rozsahu ISMS?
	i)	Je vykonávaná aktualizácia ISMS a príslušnej dokumentácie na základe zistení auditov kybernetickej bezpečnosti, výsledkov hodnotenia ISMS a v súvislosti s uskutočnenými zmenami?
	j)	Je riadená prevádzka a zdroje ISMS, sú zaznamenávané činnosti spojené s ISMS a riadením rizík?

§ 4 – Řízení aktiv

Tab. B.2: Zoznam auditných položiek k § 4 VoKB.

Odst.	Písm.	Auditná položka
1	a), b)	Je stanovená metodika pre identifikáciu a hodnotenie aktív?
1	c)	Je uskutočňovaná identifikácia a evidencia aktív?
1	d)	Sú určení garanti príslušných aktív?
1	e)	Je uskutočňované hodnotenie a evidencia primárnych aktív z hľadiska dôvernosti, integrity a dostupnosti?
1	f)	Sú určené väzby medzi primárnymi a podpornými aktívami?
1	g)	Je uskutočňované hodnotenie podporných aktív?
1	h)	Sú stanovené a zavádzané pravidlá ochrany nutné pre požadované zabezpečenie aktív?
1	i)	Sú stanovené prípustné spôsoby používania aktív a pravidlá pre manipuláciu s aktívami?
1	j)	Je určený spôsob likvidácie dát?

§ 5 – Řízení rizik

Tab. B.3: Zoznam auditných položiek k § 5 VoKB.

Odst.	Písm.	Auditná položka
1	a)	Je stanovená metodika pre hodnotenie rizík, vrátane stanovenia kritérií pre akceptovateľnosť rizík?
1	b)	Sú identifikované relevantné hrozby a zraniteľnosti, pričom sú vzaté do úvahy najmä kategórie hrozieb a zraniteľností uvedené v prílohe č. 3 VoKB?
1	c)	Je uskutočňované hodnotenie rizík v pravidelných intervaloch, a to konkrétne podľa § 5 odst. 2 VoKB, a tiež pri významných zmenách?
1	d), e)	Je uskutočňované hodnotenie rizík, pri ktorom sú zohľadnené relevantné hrozby a zraniteľnosti a posudzované možné dopady na aktíva, a to minimálne v rozsahu podľa prílohy č. 2 VoKB, je spracovaná správa o hodnotení rizík?
1	f)	Je spracované prehlásenie o aplikovateľnosti, ktoré obsahuje prehľad bezpečnostných opatrení požadovaných VoKB, vrátane spôsobu ich plnenia v prípade aplikovaných bezpečnostných opatrení, prípadne vrátane odôvodnenia neaplikovania konkrétnych opatrení?

1	g), i)	Je spracovaný a zavedený plán zvládania rizík, ktorý obsahuje ciele a prínosy bezpečnostných opatrení pre zvládanie jednotlivých rizík, určenie osoby zaisťujúcej presadzovanie bezpečnostných opatrení pre zvládanie rizík, potrebné finančné, technické, ľudské a informačné zdroje, termín ich zavedenia, popis väzieb medzi rizikami a príslušnými bezpečnostnými opatreniami a spôsob realizácie bezpečnostných opatrení, a sú v súlade s plánom zvládania rizík zavedené príslušné bezpečnostné opatrenia?

§ 6 – Organizační bezpečnost

Tab. B.4: Zoznam auditných položiek k § 6 VoKB.

Odst.	Písm.	Auditná položka
1	a)	Je stanovená bezpečnostná politika a ciele ISMS podľa § 3 VoKB?
1	b)	Je zaistená integrácia ISMS do procesov organizácie?
1	c)	Je zaistená dostupnosť zdrojov potrebných pre ISMS?
1	d)	Sú zamestnanci informovaní o význame ISMS a význame dosiahnutia zhody s jeho požiadavkami so všetkými dotknutými stranami?
1	e)	Je zaistená podpora k dosiahnutiu zamýšľaných výstupov ISMS?
1	f)	Sú zamestnanci vedení k rozvíjaniu efektivity ISMS a podporovaní pri tomto rozvíjaní?
1	g)	Sú presadzované neustále zlepšovania ISMS?
1	h)	Sú podporované osoby zastávajúce bezpečnostné role pri presadzovaní kybernetickej bezpečnosti v oblasti ich zodpovednosti?
1	i)	Sú stanovené pravidlá pre určenie administrátorov a osôb zastávajúcich bezpečnostné role?
1	j)	Je zaistené, že administrátori a osoby zastávajúce bezpečnostné role zachovávajú mlčanlivosť?
1	k)	Je zaistené, že osoby zastávajúce bezpečnostné role majú príslušné právomoci a dostupné zdroje k naplňovaniu ich rolí a plneniu súvisiacich úloh?
1	l)	Dochádza k pravidelnému testovaniu plánov kontinuity činností, obnovy a procesov spojených so zvládaním kybernetických bezpečnostných incidentov?
2		Je určené zloženie výboru pre riadenie kybernetickej bezpečnosti a bezpečnostné role a ich práva a povinnosti súvisiace s ISMS?

3	a)	Je určená osoba, ktorá zastáva bezpečnostnú rolu manažéra kybernetickej bezpečnosti?
3	b)	Je určená osoba, ktorá zastáva bezpečnostnú rolu architekta kybernetickej bezpečnosti?
3	c)	Je určená osoba, ktorá zastáva bezpečnostnú rolu garanta aktíva?
3	d)	Je určená osoba, ktorá zastáva bezpečnostnú rolu audítora kybernetickej bezpečnosti?
5, 6		Je zaistená zastupiteľnosť bezpečnostných rolí uvedených v § 6 odst. 3 VoKB?

§ 8 – Řízení dodavatelů

Tab. B.5: Zoznam auditných položiek k § 8 VoKB.

Odst.	Písm.	Auditná položka
1	a)	Sú stanovené pravidlá pre dodávateľov, ktoré zohľadňujú požiadavky ISMS?
1	b), c)	Je vedená evidencia významných dodávateľov, sú títo dodávatelia informovaní o ich evidencii?
1	d)	Sú dodávatelia oboznámení so stanovenými pravidlami a je dodržiavanie týchto pravidiel po dodávateľoch vyžadované?
1	e)	Je realizované riadenie rizík spojených s dodávateľmi?
1	f)	Obsahujú zmluvy uzatvorené s významnými dodávateľmi relevantné oblasti uvedené v prílohe č. 7 VoKB?
1	g)	Je pravidelne vykonávané preskúmavanie zmlúv s významnými dodávateľmi z hľadiska ISMS?
2	a)	Je v rámci výberového konania vykonané hodnotenie rizík súvisiacich s plnením predmetu výberového konania primerane podľa prílohy č. 2 VoKB?
2	b)	Sú v zmluvách stanovené spôsoby a úrovne realizácie bezpečnostných opatrení a sú ďalej určené vzájomné zmluvné povinnosti za zavedenie a kontrolu bezpečnostných opatrení?
2	c)	Je vykonávané pravidelné hodnotenie rizík a pravidelná kontrola zavedených bezpečnostných opatrení?
2	d)	Je zaistené riešenie identifikovaných rizík a zistených nedostatkov?

§ 9 – Bezpečnost lidských zdrojů

Tab. B.6: Zoznam auditných položiek k § 9 VoKB.

Odst.	Písm.	Auditná položka
1	a)	Je stanovený plán rozvoja bezpečnostného povedomia, ktorého cieľom je zaistiť odpovedajúcu úroveň vzdelávania a zlepšovania bezpečnostného povedomia?
1	b)	Sú určené osoby zodpovedné za realizáciu jednotlivých činností, ktoré sú v pláne rozvoja bezpečnostného povedomia uvedené?
1	c)	Je v súlade s plánom rozvoja bezpečnostného povedomia zaistené poučenie užívateľov, administrátorov, osôb zastávajúcich bezpečnostné role a dodávateľov o ich povinnostiach a o bezpečnostnej politike formou vstupných a pravidelných školení?
1	d)	Sú pre osoby zastávajúce bezpečnostné role v súlade s plánom rozvoja bezpečnostného povedomia zaistené pravidelné odborné školenia, ktoré vychádzajú z aktuálnych potrieb povinnej osoby v oblasti kybernetickej bezpečnosti?
1	e)	Sú v súlade s plánom rozvoja bezpečnostného povedomia zaistené pravidelné školenia a overovanie bezpečnostného povedomia zamestnancov v súlade s ich pracovnou náplňou?
1	f)	Je zaistená kontrola dodržiavania bezpečnostnej politiky zo strany užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role?
1	g)	Je v prípade ukončenia zmluvného vzťahu s administrátormi a osobami zastávajúcimi bezpečnostné role zaistenie predanie zodpovedností?
1	h)	Je hodnotená účinnosť plánu rozvoja bezpečnostného povedomia, vykonaných školení a ďalších činností spojených so zlepšovaním bezpečnostného povedomia?
1	i)	Sú určené pravidlá a postupy pre riešenie prípadov porušenia stanovených pravidiel zo strany užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role?
2		Sú o vykonaných školeniach vedené záznamy, ktoré obsahujú predmet školenia a zoznam osôb, ktoré školenie absolvovali?

§ 10 – Řízení provozu a komunikací

Tab. B.7: Zoznam auditných položiek k § 10 VoKB.

Odst.	Písm.	Auditná položka
1	a)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií práva a povinnosti administrátorov, užívateľov a osôb zastávajúcich bezpečnostné role?
1	b)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií postupy pre spustenie a ukončenie chodu systému, pre reštart alebo obnovenie chodu systému po zlyhaní a pre ošetrenie chybových stavov alebo mimoriadnych udalostí?
1	c)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií postupy pre sledovanie kybernetických bezpečnostných udalostí a opatrenia pre ochranu prístupu k záznamom o týchto udalostiach?
1	d)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií pravidlá a postupy pre ochranu pred škodlivým kódom?
1	e)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií riadenie technických zraniteľností?
1	f)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií spojenia na kontaktné osoby, ktoré sú poverené výkonom systémovej a technickej podpory?
1	g)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií postupy riadenia a schvaľovania prevádzkových zmien?
1	h)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií postupy pre sledovanie, plánovanie a riadenie kapacity ľudských a technických zdrojov?
1	i)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií pravidlá a postupy pre ochranu informácií a dát v priebehu celého životného cyklu?
1	j)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií pravidlá a postupy pre inštaláciu technických aktív?
1	k)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií vykonávanie pravidelného zálohovania a kontroly použiteľnosti vytvorených záloh?

1	l)	Obsahujú pravidlá a postupy stanovené v rámci riadenia prevádzky a komunikácií pravidlá a postupy pre zaistenie bezpečnosti sieťových služieb?
2		Sú stanovené pravidlá a postupy v rámci riadenia prevádzky a komunikácií dodržiavané a aktualizované v súvislosti s vykonávanými alebo plánovanými zmenami?
3		Je zaistené oddelenie vývojového, testovacieho a prevádzkového prostredia?

§ 11 – Řízení změn

Tab. B.8: Zoznam auditných položiek k § 11 VoKB.

Odst.	Písm.	Auditná položka
1	a)	Sú preskúmavané možné dopady zmien informačného a komunikačného systému?
1	b)	Sú určované významné zmeny informačného a komunikačného systému?
2	a)	Je dokumentované riadenie významných zmien?
2	b)	Je v súvislosti s významnými zmenami vykonávaná analýza rizík?
2	c)	Sú prijímané opatrenia za účelom zníženia všetkých nepriaznivých dopadov spojených s významnými zmenami?
2	d)	Je v súvislosti s významnými zmenami aktualizovaná bezpečnostná politika a bezpečnostná dokumentácia?
2	e)	Je zaistené testovanie významných zmien?
2	f)	Je zaistená možnosť navrátenia do pôvodného stavu po výskyte významných zmien?
3, 4		Sú na základe výsledkov analýzy rizík vykonanej podľa § 11 odst. 2 písm. b) VoKB vykonané penetračné testy alebo testovanie zraniteľností?

§ 12 – Řízení přístupu

Tab. B.9: Zoznam auditných položiek k § 12 VoKB.

Odst.	Písm.	Auditná položka
1		Je riadený prístup k informačnému a komunikačnému systému?
2	a)	Je prístup riadený na základe skupín a rolí?
2	b)	Má každý užívateľ a administrátor pristupujúci k informačnému a komunikačnému systému pridelené prístupové práva a oprávnenia a jedinečný identifikátor?
2	c)	Sú riadené identifikátory, prístupové práva a oprávnenia aplikácií a technických účtov?
2	d)	Sú zavedené bezpečnostné opatrenia pre riadenie prístupu zariadení k prostriedkom informačného a komunikačného systému?
2	e)	Sú zavedené bezpečnostné opatrenia potrebné pre bezpečné používanie mobilných zariadení a iných technických zariadení?
2	f)	Sú prideľované privilegované oprávnenia obmedzené na úroveň nevyhnutnú k výkonu náplne práce?
2	g)	Je používanie programových prostriedkov, ktoré môžu byť schopné prekonať systémové alebo aplikačné kontroly, obmedzené a kontrolované?
2	h)	Sú prístupové oprávnenia prideľované a odoberané v súlade s politikou riadenia prístupu?
2	i)	Je vykonávané pravidelné preskúmanie nastavenia všetkých prístupových oprávnení vrátane rozdelenia do prístupových skupín a rolí?
2	j)	Je pre správu a overovanie identít využívaný nástroj podľa § 19 VoKB a pre riadenie prístupových oprávnení nástroj podľa § 20 VoKB?
2	k)	Sú užívatelia vedení k dodržiavaniu stanovených postupov pri používaní privátnych autentizačných informácií?
2	l)	Je pri zmene pozície alebo zradenia užívateľov, administrátorov alebo osôb zastávajúcich bezpečnostné role zaistené odobratie alebo zmena prístupových oprávnení?
2	m)	Je pri ukončení alebo zmene zmluvného vzťahu zaistené odobratie alebo zmena prístupových oprávnení?
2	n)	Je prideľovanie a odoberanie prístupových oprávnení dokumentované?

§ 13 – Akvizice, vývoj a údržba

Tab. B.10: Zoznam auditných položiek k § 13 VoKB.

Odst.	Písm.	Auditná položka
	a)	Sú v súvislosti s plánovanou akvizíciou, vývojom a údržbou informačného a komunikačného systému riadené riziká podľa § 5 VoKB?
	b)	Sú v súvislosti s plánovanou akvizíciou, vývojom a údržbou informačného a komunikačného systému riadené významné zmeny podľa § 11 VoKB?
	c)	Sú v súvislosti s plánovanou akvizíciou, vývojom a údržbou informačného a komunikačného systému stanovené bezpečnostné požiadavky?
	d)	Sú do projektu akvizície, vývoja a údržby zahrnuté bezpečnostné požiadavky?
	e)	Je zaistená bezpečnosť vývojového a testovacieho prostredia a ochrana používaných testovacích dát?
	f)	Je realizované bezpečnostné testovanie významných zmien pred ich zavedením do prevádzky?

§ 14 – Zvládání kybernetických bezpečnostních událostí a incidentů

Tab. B.11: Zoznam auditných položiek k § 14 VoKB.

Odst.	Písm.	Auditná položka
1	a)	Je zavedený proces detekcie a vyhodnocovania kybernetických bezpečnostných udalostí a zvládania kybernetických bezpečnostných incidentov?
1	b)	Sú pridelené zodpovednosti a stanovené postupy pre detekciu a vyhodnocovanie kybernetických bezpečnostných udalostí a incidentov a pre koordináciu a zvládanie kybernetických bezpečnostných incidentov?
1	c)	Sú definované a aplikované postupy pre identifikáciu, zber, získanie a uchovanie vierohodných podkladov potrebných pre analýzu kybernetického bezpečnostného incidentu?
1	d)	Je zaistená detekcia kybernetických bezpečnostných udalostí?
1	e)	Je pri detekcii kybernetických bezpečnostných postupované podľa § 22 a § 23 VoKB?

1	f)	Užívatelia, administrátori, osoby zastávajúce bezpečnostné role, ďalší zamestnanci a dodávatelia oznamujú neobvyklé prejavy informačného a komunikačného systému a podozrenia na akékoľvek zraniteľnosti?
1	g)	Je zaistené posudzovanie kybernetických bezpečnostných udalostí, pri ktorom musí byť rozhodnuté, či majú byť tieto udalosti klasifikované ako kybernetické bezpečnostné incidenty podľa § 31 VoKB?
1	h)	Je zaistené zvládanie kybernetických bezpečnostných incidentov podľa stanovených postupov?
1	i)	Sú prijímané opatrenia pre odvrátenie a zmiernenie dopadu kybernetického bezpečnostného incidentu?
1	j)	Sú hlásené kybernetické bezpečnostné incidenty podľa § 32 VoKB?
1	k)	Sú vedené záznamy o kybernetických bezpečnostných incidentoch a o ich zvládaní?
1	l)	Kybernetické bezpečnostné incidenty sú prešetrené a sú určené ich príčiny?
1	m)	Je vyhodnotená účinnosť riešenia kybernetického bezpečnostného incidentu a na základe vyhodnotenia sú stanovené nutné bezpečnostné opatrenia, popr. sú aktualizované existujúce bezpečnostné opatrenia za účelom zamedzenia opakovania riešeného kybernetického bezpečnostného incidentu?
2		Je pre detekciu kybernetických bezpečnostných udalostí používaný nástroj podľa § 24 VoKB?

§ 15 – Řízení kontinuity činností

Tab. B.12: Zoznam auditných položiek k § 15 VoKB.

Odst.	Písm.	Auditná položka
	a)	Sú stanovené práva a povinnosti administrátorov a osôb zastávajúcich bezpečnostné role v rámci riadenia kontinuity činností?
	b)	Sú pomocou hodnotenia rizík a a analýzy dopadov vyhodnotené a dokumentované možné dopady kybernetických bezpečnostných incidentov a sú posúdené možné riziká súvisiace s ohrozením kontinuity činností?

	c)	Sú na základe výstupov hodnotenia rizík a analýzy dopadov stanovené ciele riadenia kontinuity činností, ktoré definujú minimálnu úroveň poskytovania služieb, ktorá je prijateľná pre užívanie, prevádzku a správu informačného a komunikačného systému, dobu obnovenia chodu, počas ktorej bude po kybernetickom bezpečnostnom incidente obnovená minimálna úroveň poskytovaných služieb informačného a komunikačného systému, a bod obnovenia dát ako časové obdobie, počas ktorého musia byť spätne obnovené dáta po kybernetickom bezpečnostnom incidente alebo po zlyhaní?
	d)	Je stanovená politika riadenia kontinuity činností, ktorá obsahuje naplnenie stanovených cieľov?
	e)	Sú vypracované, aktualizované a pravidelne testované plány kontinuity činností a havarijné plány súvisiace s prevádzkovaním informačného a komunikačného systému a súvisiacich služieb?
	f)	Sú realizované opatrenie pre zvýšenie odolnosti informačného a komunikačného systému voči kybernetickým bezpečnostným incidentom a obmedzeniu dostupnosti?

§ 16 – Audit kybernetické bezpečnosti

Tab. B.13: Zoznam auditných položiek k § 16 VoKB.

Odst.	Písm.	Auditná položka
1	a)	Je vykonávaný a dokumentovaný audit dodržiavania bezpečnostnej politiky, vrátane preskúmania technickej zhody, a sú výsledky auditu zohľadnené v pláne rozvoja bezpečnostného povedomia a v pláne zvládania rizík?
1	b)	Je posudzovaný súlad bezpečnostných opatrení s najlepšou praxou, právnymi predpismi, internými predpismi, inými predpismi a zmluvnými záväzkami vzťahujúcimi sa k informačnému a komunikačnému systému a sú určené prípadné nápravné opatrenia pre zaistenie súladu?
2, 3		Je audit kybernetickej bezpečnosti vykonávaný pri významných zmenách, v rámci ich rozsahu, a v pravidelných intervaloch podľa § 16 odst. 2 písm. b), c) VoKB?

4		Je audit kybernetickej bezpečnosti vykonávaný oprávnenou osobou, ktorá spĺňa podmienky uvedené v § 7 odst. 4 VoKB, a ktorá nezávisle hodnotí správnosť a účinnosť zavedených bezpečnostných opatrení?

§ 17 – Fyzická bezpečnost

Tab. B.14: Zoznam auditných položiek k § 17 VoKB.

Odst.	Písm.	Auditná položka
	a)	Je predchádzané poškodeniu, krádeži alebo zneužitiu aktív alebo prerušeniu poskytovania služieb informačného a komunikačného systému?
	b)	Je stanovený fyzický bezpečnostný perimeter ohraničujúci oblasť, v ktorej sú uchovávané a spracovávané informácie a umiestnené technické aktíva informačného a komunikačného systému?
	c)	Sú prijaté nevyhnutné opatrenia a uplatnené prostriedky fyzickej bezpečnosti k zamedzeniu neoprávneného vstupu, k zamedzeniu poškodenia a neoprávneným zásahom a pre zaistenie ochrany na úrovni objektov a v rámci objektov?

§ 18 – Bezpečnost komunikačních sítí

Tab. B.15: Zoznam auditných položiek k § 18 VoKB.

Odst.	Písm.	Auditná položka
	a), e)	Je zaistená segmentácia komunikačnej siete, a to s využitím nástroja, ktorý zaistí ochranu integrity komunikačnej siete?
	b), e)	Je zaistené riadenie komunikácie v rámci komunikačnej siete a perimetru komunikačnej siete, a to s využitím nástroja, ktorý zaistí ochranu integrity komunikačnej siete?
	c)	Je s využitím kryptografie zaistená dôvernosť a integrita dát pri vzdialenom prístupe, vzdialenej správe alebo pri prístupe do komunikačnej siete pomocou bezdrôtových technológií?
	d)	Sú implementované prostriedky pre aktívne blokovanie nežiadúcej komunikácie?

§ 19 – Správa a ověřování identit

Tab. B.16: Zoznam auditných položiek k § 19 VoKB.

Odst.	Písm.	Auditná položka
1		Je využívaný nástroj pre správu a overenie identity užívateľov, administrátorov a aplikácií informačného a komunikačného systému?
2	a)	Zaisťuje nástroj pre správu a overenie identity užívateľov, administrátorov a aplikácií overenie identity pred zahájením aktivít v informačnom a komunikačnom systéme?
2	b)	Zaisťuje nástroj pre správu a overenie identity užívateľov, administrátorov a aplikácií riadenie počtu možných neúspešných pokusov o prihlásenie?
2	c)	Zaisťuje nástroj pre správu a overenie identity užívateľov, administrátorov a aplikácií odolnosť uložených alebo prenášaných autentizačných údajov proti neoprávnenému odcudzeniu a zneužitiu?
2	d)	Zaisťuje nástroj pre správu a overenie identity užívateľov, administrátorov a aplikácií ukladanie autentizačných údajov vo forme odolnej proti offline útokom?
2	e)	Zaisťuje nástroj pre správu a overenie identity užívateľov, administrátorov a aplikácií opätovné overenie identity po určenej dobe nečinnosti?
2	f)	Zaisťuje nástroj pre správu a overenie identity užívateľov, administrátorov a aplikácií dodržanie dôvernosti autentizačných údajov pri obnove prístupu?
2	g)	Zaisťuje nástroj pre správu a overenie identity užívateľov, administrátorov a aplikácií centralizovanú správu identít?
3		Je pre overenie identity užívateľov, administrátorov a aplikácií využívaný autentizačný mechanizmus, ktorý nie je založený len na použití identifikátoru účtu a hesla, ale je založený na viacfaktorovej autentizácii s najmenej dvoma rôznymi typmi faktorov?
4		Pokiaľ nie je splnená požiadavka podľa § 19 odst. 3 VoKB, je využívaný taký nástroj pre overenie identity užívateľov, administrátorov a aplikácií, ktorý používa autentizáciu pomocou kryptografických kľúčov a ktorý dokáže zaručiť obdobnú úroveň bezpečnosti

5		Pokiaľ nie sú splnené požiadavky podľa § 19 odst. 3 a odst. 4 VoKB, je využívaný taký nástroj pre overenie identity užívateľov, administrátorov a aplikácií, ktorý používa k autentizácii identifikátor účtu a heslo a ktorý vynucuje nasledujúce pravidlá: i) dĺžka hesla musí byť najmenej 12 znakov u užívateľov a 17 znakov u administrátorov a aplikácií, ii) nástroj umožňuje zadať heslo s dĺžkou aspoň 64 znakov, iii) nástroj neobmedzuje použitie malých a veľkých písmen, číslic a špeciálnych znakov, iv) nástroj umožňuje užívateľom zmenu hesla, pričom obdobie medzi dvoma zmenami hesla nemôže byť kratšie ako 30 minút, v) nástroj neumožňuje užívateľom a administrátorom zvoliť si najčastejšie používané heslá, tvoriť heslá na základe mnohonásobne opakujúcich sa znakov, prihlasovacieho mena, e-mailu, názvu systému alebo obdobným spôsobom a neumožňuje ani opätovné použitie už predtým používaných hesiel s pamäťou aspoň 12 predchádzajúcich hesiel, vi) je vyžadovaná povinná zmena hesla v intervale max. po 18 mesiacoch.
6	a)	Pokiaľ je využívaná autentizácia len účtom a heslom, je vynútená bezodkladná zmena východzieho hesla po jeho prvom použití?
6	b)	Pokiaľ je využívaná autentizácia len účtom a heslom, je bezodkladne zneplatnené heslo slúžiace k obnoveniu prístupu po jeho prvom použití alebo po uplynutí najviac 60 minút od jeho vytvorenia?
6	c)	Pokiaľ je využívaná autentizácia len účtom a heslom, sú zhrnuté pravidlá tvorby bezpečných hesiel do plánu rozvoja bezpečnostného povedomia podľa § 9 VoKB?

§ 20 – Řízení přístupových oprávnění

Tab. B.17: Zoznam auditných položiek k § 20 VoKB.

Odst.	Písm.	Auditná položka
	a)	Je používaný nástroj pre riadenie prístupových oprávnení, ktorým je zaistené riadenie oprávnení pre prístup k jednotlivým aktívam informačného a komunikačného systému?
	b)	Je používaný nástroj pre riadenie prístupových oprávnení, ktorým je zaistené riadenie oprávnení pre čítanie dát, zápis dát a zmenu oprávnení?

§ 21 – Ochrana před škodlivým kódem

Tab. B.18: Zoznam auditných položiek k § 21 VoKB.

Odst.	Písm.	Auditná položka
1	a)	Je využívaný nástroj pre nepretržitú automatickú ochranu koncových staníc, mobilných zariadení, serverov, dátových úložísk a výmenných dátových nosičov, komunikačnej siete a prvkov komunikačnej siete a obdobných zariadení?
1	b)	Dochádza k monitorovaniu a riadeniu používania výmenných zariadení a dátových nosičov?
1	c)	Je riadené automatické spúšťanie obsahu výmenných zariadení a dátových nosičov?
1	d)	Sú riadené oprávnenia k spúšťaniu kódu?
1	e)	Je vykonávaná pravidelná a účinná aktualizácia nástroja pre ochranu pred škodlivým kódom?

§ 22 – Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

Tab. B.19: Zoznam auditných položiek k § 22 VoKB.

Odst.	Písm.	Auditná položka
1	a)	Je využívaný nástroj pre zaznamenávanie bezpečnostných a iných potrebných prevádzkových udalostí dôležitých aktív informačného a komunikačného systému?
1	b)	Je aktualizovaný rozsah aktív, u ktorých je zaznamenávanie bezpečnostných a prevádzkových udalostí vykonávané?
2	a)	Je zaistená jednoznačná sieťová identifikácia zariadenia pôvodcu, pokiaľ je v komunikačnej sieti použitý nástroj meniaci jeho sieťovú identifikáciu?
2	b)	Je zaistený zber informácií o bezpečnostných a prevádzkových udalostiach, a to najmä nasledujúcich informácií: i) dátum a čas vrátane špecifikácie časového pásma, ii) typ činnosti, iii) identifikácia technického aktíva, ktoré činnosť zaznamenalo, iv) jednoznačná identifikácia účtu, pod ktorým bola činnosť vykonaná, v) jednoznačná identifikácia zariadenia pôvodcu, vi) úspešnosť alebo neúspešnosť činnosti?

2	c)	Je zaistená ochrana zaznamenaných informácií pred neoprávneným čítaním alebo akoukoľvek zmenou?
2	d)	Sú zaznamenávané následujúce činnosti: i) prihlasovanie a odhlasovanie ku všetkým účtom, a to vrátane neúspešných pokusov, ii) činnosti vykonané administrátormi, iii) úspešné aj neúspešné manipulácie s účtami, oprávneniami a právami, iv) nevykonanie činností v dôsledku nedostatku prístupových práv a oprávnení, v) činnosti užívateľov, ktoré môžu myť vplyv na bezpečnosť informačného a komunikačného systému, vi) zahájenie a ukončenie činností technických aktív, vii) kritické a chybové hlásenia technických aktív, viii) prístupy k záznamom o udalostiach, pokusy omanipuláciu so záznamami o udalostiach a zmeny nastavení nástrojov pre zaznamenávanie udalostí?
2	e)	Je zaistená synchronizácia jednotného času technických aktív najmenej raz za 24 hodín?
3, 4		Sú záznamy o udalostiach uchovávané po dobu definovanú v § 22 odst. 3 a 4 VoKB?

§ 23 – Detekce kybernetických bezpečnostních událostí

Tab. B.20: Zoznam auditných položiek k § 23 VoKB.

Odst.	Písm.	Auditná položka
1	a)	Je využívaný nástroj pre detekciu kybernetických bezpečnostných udalostí, ktorý zaistí overenie a kontrolu prenášaných dát v rámci komunikačnej siete a medzi komunikačnými sieťami?
1	b)	Je využívaný nástroj pre detekciu kybernetických bezpečnostných udalostí, ktorý zaistí overenie a kontrolu prenášaných dát na perimetri komunikačnej siete?
1	c)	Je využívaný nástroj pre detekciu kybernetických bezpečnostných udalostí, ktorý zaistí blokovanie nežiadúcej komunikácie?
2		Je zaistená detekcia kybernetických bezpečnostných udalostí primerane s ohľadom na dôležitosť aktív v rámci koncových staníc, mobilných zariadení, serverov, dátových úložísk a výmenných dátových nosičov, komunikačnej siete a prvkov komunikačnej siete a obdobných aktív?

§ 24 – Sběr a vyhodnocování kybernetických bezpečnostních událostí

Tab. B.21: Zoznam auditných položiek k § 24 VoKB.

Odst.	Písm.	Auditná položka
	a)	Je používaný nástroj pre zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožní zber a vyhodnocovanie udalostí zaznamenaných na základe § 22 a § 23 VoKB?
	b)	Je používaný nástroj pre zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožní vyhľadávanie a zoskupovanie súvisiacich záznamov?
	c)	Je používaný nástroj pre zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožní poskytovanie informácií pre určené bezpečnostné role o detekovaných kybernetických bezpečnostných udalostiach?
	d)	Je používaný nástroj pre zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožní vyhodnocovanie kybernetických bezpečnostných udalostí s cieľom identifikácie kybernetických bezpečnostných incidentov, vrátane včasného varovania určených bezpečnostných rolí?
	e)	Je používaný nástroj pre zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožní obmedzenie prípadov nesprávneho vyhodnotenia udalostí pravidelnou aktualizáciou nastavenia pravidiel pre vyhodnocovanie kybernetických bezpečnostných udalostí a včasné varovanie?
	f)	Je používaný nástroj pre zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožní využívanie informácií získaných nástrojom pre zber a vyhodnocovanie kybernetických bezpečnostných udalostí pre optimálne nastavenie bezpečnostných opatrení informačného a komunikačného systému?

§ 25 – Aplikační bezpečnost

Tab. B.22: Zoznam auditných položiek k § 25 VoKB.

Odst.	Písm.	Auditná položka
1	a), b)	Sú realizované penetračné testy so zameraním na dôležité aktíva, a to pred ich uvedením do prevádzky a v súvislosti s významnou zmenou?
2	a), b)	Je zaistená trvalá ochrana aplikácií, informácií a transakcií pred neoprávnenou činnosťou a pred poprením vykonaných činností?

§ 26 – Kryptografické prostředky

Tab. B.23: Zoznam auditných položiek k § 26 VoKB.

Odst.	Písm.	Auditná položka
	a)	Sú používané aktuálne odolné kryptografické algoritmy a kryptografické kľúče pre ochranu aktív informačného a komunikačného systému?
	b)	Je používaný systém správy kľúčov a certifikátov, ktorý zaistí generovanie, distribúciu, ukladanie, zmeny, obmedzenie platnosti, zneplatnenie certifikátov a likvidáciu kľúčov a ktorý umožní kontrolu a audit?
	c)	Je presadzované bezpečné zaobchádzanie s kryptografickými prostriedkami?
	d)	Sú zohľadnené odporúčania v oblasti kryptografických prostriedkov vydané Národním úřadem pro kybernetickou a informační bezpečnost?

§ 27 – Zajišťování úrovně dostupnosti informací

Tab. B.24: Zoznam auditných položiek k § 27 VoKB.

Odst.	Písm.	Auditná položka
	a)	Je zaistená dostupnosť informačného a komunikačného systému pre splnenie cieľov podľa § 15 VoKB?
	b)	Je zaistená odolnosť informačného a komunikačného systému voči kybernetickým bezpečnostným incidentom, ktoré by mohli znížiť jeho dostupnosť?
	c)	Je zaistená dostupnosť dôležitých technických aktív informačného a komunikačného systému?
	d)	Je zaistená redundancia aktív nevyhnutných pre zaistenie dostupnosti informačného a komunikačného systému?

§ 28 – Průmyslové, řídicí a obdobné specifické systémy

Tab. B.25: Zoznam auditných položiek k § 28 VoKB.

Odst.	Písm.	Auditná položka
	a)	Sú používané nástroje a opatrenia, ktoré zaistia použitie technických a programových prostriedkov, ktoré sú určené do špecifického prostredia?
	b)	Sú používané nástroje a opatrenia, ktoré zaistia obmedzenie fyzického prístupu k zariadeniam priemyselných a riadiacich systémov a ku komunikačnej sieti?
	c)	Sú používané nástroje a opatrenia, ktoré zaistia vyčlenenie komunikačnej siete určenej pre priemyselné a riadiace systémy od ostatnej infraštruktúry?
	d)	Sú používané nástroje a opatrenia, ktoré zaistia obmedzenie a riadenie fyzického prístupu k priemyselným a riadiacim systémom?
	e)	Sú používané nástroje a opatrenia, ktoré zaistia ochranu jednotlivých technických aktív priemyselných a riadiacich systémov pred využitím známych zraniteľností?
	f)	Sú používané nástroje a opatrenia, ktoré zaistia obnovenie chodu priemyselných a riadiacich systémov po kybernetickom bezpečnostnom incidente?

C Záverečná správa z auditu kybernetickej bezpečnosti

Príloha obsahuje **ukážku záverečnej správy (reportu)** z vykonaného auditu kybernetickej bezpečnosti, ktorá bola automaticky vygenerovaná ako primárny výstup z auditu realizovaného v prostredí platformy Penterep.

Seznam nálezů

Audit dle VoKB § 5 – Řízení rizik

V této kategorii byly nalezeny nedostatky v následujících kategorií:

- VoKB-5-1a Metodika hodnocení rizik
- VoKB-5-1b Identifikace hrozeb a zranitelností
- VoKB-5-1c,d Hodnocení rizik
- VoKB-5-1e Zpráva o hodnocení rizik
- VoKB-5-1f Prohlášení o aplikovatelnosti
- VoKB-5-1g,i Plán zvládání rizik

VoKB-5-1a Metodika hodnocení rizik

Nedostatek:
Metodika pro hodnocení rizik, včetně kritérií pro akceptovatelnost rizik, není stanovena.

Odůvodnění:
Povinná osoba dle ZoKB musí stanovit metodiku pro hodnocení rizik, včetně kritérií pro akceptovatelnost rizik.

VoKB-5-1b Identifikace hrozeb a zranitelností

Nedostatek:
Relevantní hrozby a zranitelnosti, které mohou být významné pro aktiva, nejsou identifikovány.

Odůvodnění:
Povinná osoba dle ZoKB musí s ohledem na aktiva identifikovat relevantní hrozby a zranitelnosti, přičemž musí být zváženy zejména kategorie hrozeb a zranitelností uvedených v příloze č. 3 k VoKB.

VoKB-5-1c,d Hodnocení rizik

Nedostatek:
Hodnocení rizik není prováděno v pravidelných intervalech a/nebo při významných změnách.

Odůvodnění:
Povinná osoba dle ZoKB musí provádět hodnocení rizik v pravidelných intervalech a při významných změnách. Povinná osoba uvedená v § 3 písm. c), d) a f) ZoKB provádí hodnocení rizik alespoň jednou ročně a povinná osoba uvedená v § 3 písm. e) ZoKB alespoň jednou za tři roky.

VoKB-5-1e Zpráva o hodnocení rizik

Nedostatek:
Zpráva o hodnocení rizik není zpracována.

Odůvodnění:
Povinná osoba dle ZoKB musí zpracovat zprávu o hodnocení rizik.

VoKB-5-1f Prohlášení o aplikovatelnosti

Nedostatek:
Prohlášení o aplikovatelnosti, které obsahuje přehled bezpečnostních opatření požadovaných VoKB, není zpracováno nebo rozsah a/nebo obsah jeho zpracování není dostatečný.

Odůvodnění:
Povinná osoba dle ZoKB musí zpracovat na základě bezpečnostních potřeb a výsledků hodnocení rizik prohlášení o aplikovatelnosti, které obsahuje přehled bezpečnostních opatření požadovaných VoKB, která: (i) nebyla aplikována, včetně odůvodnění, (ii) byla aplikována, včetně způsobu plnění.

VoKB-5-1g,i Plán zvládání rizik

Nedostatek:
Plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení, popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a způsob realizace bezpečnostních opatření, není zpracován a zaveden nebo rozsah a/nebo obsah jeho zpracování není dostatečný.

Odůvodnění:
Povinná osoba dle ZoKB musí zpracovat a zavést plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení, popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a způsob realizace bezpečnostních opatření.

D Obsah elektronickej prílohy

Obsahom elektronickej prílohy je táto záverečná diplomová práca vo formáte PDF. Ďalej elektronická príloha zahŕňa archív s názvom `dp-analyza-rizik.zip`, ktorý obsahuje všetky zdrojové kódy implementovanej webovej aplikácie pre zobrazenie výstupov analýzy rizík. Súčasťou priloženého archívu je taktiež súbor s názvom `template.xlsx`, ktorý obsahuje všetky podstatné výstupy z vykonanej analýzy rizík bezpečnosti informácií v prostredí Spoločnosti a ktorý slúži ako primárny zdrojový súbor dát k zobrazeniu pre webovú aplikáciu.

- `/` ..... koreňový adresár archívu s elektronickou prílohou
  - `2023_DP_Voskárová.pdf` ..... diplomová práca vo formáte PDF
  - `dp-analyza-rizik.zip` ..... adresár obsahujúci zdrojové kódy webovej aplikácie
  - `template.xlsx` ..... výstupy z analýzy rizík
  - `webová-aplikácia` ..... hypertextový odkaz s prepojením na webovú aplikáciu