VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2020 Bc. Veronika Doubková

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

BEZPEČNOSTNÍ RIZIKA PODLE STANDARDU ISO 27001
SECURITY RISKS ACCORDING TO ISO 27001

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Veronika Doubková**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Tomáš Horváth, Ph.D.**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Informační bezpečnost**

Ústav telekomunikací

Studentka: Bc. Veronika Doubková ***ID:*** 208303

Ročník: 2 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Bezpečnostní rizika podle standardu ISO 27001

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce bude analyzovat bezpečnostní rizika podle normy ISO 27005 v souladu s požadavky ISO 27001. Teoretická část práce se bude zabývat procesem řízení rizik, od jejich identifikace až k aplikaci opatřeni pro optické přenosové systémy. Rizika budou pokrývat jak úniky informací z optického vlákna, tak i z aktivních prvků v přenosové soustavě. V rámci diplomové práce bude provedena aplikace procesu řízení rizik dle ISO 27005 na optické přenosové systémy a kritické infrastruktury v prostředí Verinice. Výsledkem diplomové práce bude katalog rizik, scénářů a opatřeni ve formátu .VNA pro ochranu kritické infrastruktury a zamezení úniků informací z optického vlákna v návaznosti na uvedené normy.

DOPORUČENÁ LITERATURA:

[1] WHITMAN, Michael E. a Herbert J. MATTFORD. Management of information security. Sixth edition. Boston, Massachusetts: Cengage Learning, [2019]. ISBN 978-1337405713.

[2] TAYLOR, Andy. Information security management principles. Second edition. Swindon, UK: BCS, the Chartered Institute for IT, [2013]. ISBN 978-1780171753.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 1.6.2020

Vedoucí práce: Ing. Tomáš Horváth, Ph.D.

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Tato diplomová práce se zabývá procesem řízení rizik bezpečnosti informací, dle ISO/IEC 27005 a jeho realizací v prostředí softwaru Verinice. Proces řízení rizik bezpečnosti informací je aplikován na kritickou infrastrukturu, která je připojena k optické síti. V rámci práce jsou vytvořené scénáře incidentu zaměřené především na únik dat z optických vláken a aktivních síťových prvků v přenosové soustavě. Výstupem práce je vytvořený katalog rizik ve formátu .VNA obsahující identifikovaná rizika, na která jsou implementována vhodná opatření v návaznosti na požadavky normy ISO/IEC 27001, pro ochranu kritické infrastruktury a přenášených dat v přenosové soustavě.

KLÍČOVÁ SLOVA

Bezpečnost informací, bezpečnostní triáda, kybernetická bezpečnost, kritická infrastruktura, kritická informační infrastruktura, optická přenosová síť, riziko, systém řízení rizik bezpečnosti informací

ABSTRACT

This diploma thesis deals with the process of information security risk management, according to ISO/IEC 27005 and its implementation in the Verinice software environment. The risk information management process is applied to a critical infrastructure, that is connected to an optical fiber network. Incident scenarios are focused mainly on data leakage from optical fibers and active network elements in the transmission system. The output of the work is a catalog of risks in .VNA format containing identified risks, for which appropriate measures are implemented according to the requirements of ISO/IEC 27001, for the protection of critical infrastructure and transmitted data in the transmission system.

KEYWORDS

Information security, security triad, cyber security, critical infrastructure, critical information infrastructure, optical transmission network, risk, information security risk management system

DOUBKOVÁ, Veronika. *Bezpečnostní rizika podle standardu ISO 27001*. Brno, Rok, 99 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Tomáš Horváth, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Bezpečnostní rizika podle standardu ISO 27001“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucímu diplomové práce panu Ing. Tomáši Horváthovi, Ph.D. za odborné vedení, konzultace, trpělivost, podnětné návrhy k práci, vstřícný přístup, ochotu a čas, který mi věnoval během tvorby diplomové práce. Dále bych na tomto místě ráda poděkovala své rodině, příteli a přátelům, kteří mě během studia podporovali.

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

Úvod

S rozmachem informačních a komunikačních systému narůstají i požadavky na bezpečnost informací před možnými riziky. Informační a komunikační systémy hrají zásadní roli při fungování základních služeb v moderní společnosti. Bezpečnost informací těchto systému a sítí se stává prioritou, jak pro organizace, tak i pro vlády.

Významné narušení uvedených systému by mohlo vést k narušení poskytování základních služeb nebo narušení bezpečnosti informací. Organizace proto implementují systém řízení bezpečnosti informací pro snížení rizik plynoucích z provozování těchto systému.

V diplomové práci je popsán proces řízení rizik bezpečnosti informací, dle dle normy ISO/IEC 27005. Dále jsou definovány normy řady ISO/IEC 27000, sloužící k systematickému řízení rizik v organizaci. Pro orgány nebo osoby splňující kritéria pro určení prvků kritické infrastruktury je nezbytné, dle zákona o kybernetické bezpečnosti, implementovat systém řízení rizik bezpečnosti informací. Práce se zabývá stanovením kritérií pro určení prvku kritické infrastruktury a kritické informační infrastrukturu. Vysvětlením uvedených pojmů a dalších definic vycházejících z kybernetické bezpečnosti.

Cílem diplomové práce je aplikace procesu řízení rizik realizovaný v prostředí softwaru Verinice, který vychází z procesu řízení rizik, dle normy ISO/IEC 27005 a je v souladu s požadavky ISO/IEC 27001. Pro analýzu rizik je vybráno datové centrum patřící do kritické infrastruktury a optické sítě, které jsou využity pro přenos dat po optických vláknech patřících do kritické informační infrastruktury. V procesu řízení rizik jsou identifikována aktiva datového centra a prvky přenosové soustavy. Dále jsou identifikovány zranitelnosti a hrozby mířené na bezpečnost informací s cílem narušení funkčnosti datového centra nebo přenosové soustavy.

Podstatná část práce je věnována popisem navržených scénářů vedoucích k odposlechu, úniku dat, selhání nebo smazání dat a dalším rizikovým scénářům. Následně budou rizika ohodnocena a ošetřena vhodnými opatřeními.

Výsledným řešením je vytvořený katalog rizik ve formátu .VNA v prostředí softwaru Verinice a na základě hodnocení rizik se stanovila vhodná opatření pro jejich snížení.

1 Kybernetická bezpečnost a kybernetický prostor

V této kapitole budou vymezeny nejdůležitější pojmy související s problematikou kybernetické bezpečnosti a pojmů souvisejících s procesem řízení rizik bezpečnosti informací. Dále budou vymezeny nejdůležitější zákony, směrnice a normy, které se týkají kybernetické bezpečnosti.

1.1 Definice pojmů

Než bude vymezen pojem kybernetická bezpečnost je důležité nejprve porozumět významu slova bezpečnost, jelikož kybernetickou bezpečnost můžeme chápat jako podmnožinu bezpečnosti. Následně budou vymezeny další pojmy a definice související s kybernetickou bezpečností.

Bezpečnost „*je chápána jako vlastnost prvku (např. informačního systému, komunikačního systému), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany proti ztrátám. Bezpečnost v informačních technologiích zahrnuje ochranu důvěrnosti, dostupnosti a integrity a dosažitelnosti při zpracování, úschově, distribuci a prezentaci informace*“ [1]. V obecném slova smyslu lze říct, že bezpečnost znamená ochranu aktiv.

1.1.1 Informační a komunikační systém

Informační systém je komplex funkčních prvků zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky [1].

Komunikační systém zajišťuje přenos informací mezi koncovými účastníky. Komunikační systém může být popsán jako množina uzlů připojená prostřednictvím linek. Informace mohou být zpracovány a uloženy v uzlu a přenášeny z jednoho uzlu do druhého skrze linku. Uzel se může skládat z hardwaru, systémového softwaru a aplikačního softwaru. Komunikační systém tedy zahrnuje koncové komunikační zařízení, přenosové prostředí, správu systému, personální obsluhu a může zahrnovat i prostředky kryptografické ochrany [1].

1.1.2 Aktivum

Je vše, co má hodnotu pro jednotlivce, organizaci nebo veřejnou správu, a co tedy vyžaduje ochranu před hrozbami [1]. Aktivum může být věcí hmotnou například

budova, optický kabel, zboží, počítačový systém, informační a komunikační sítě atd., nebo nehmotnou například data, informace, know-how, software a další.

Dle *Vyhlášky č. 82/2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech po dání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*, dále jen VoKB, mohou být aktiva [2]:

- **podpůrná** – jedná se o technická aktiva, zaměstnance a dodavatele, kteří se podílejí na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému. Technické aktivum je míněno technické vybavení, komunikační prostředí a programové vybavení informačního a komunikačního systému a objekty, jejichž selhání může mít dopad na informační nebo komunikační systém,
- **primární** – jedná se o informace nebo služby, které zpracovává nebo poskytuje informační a komunikační systém.

1.1.3 Hrozba

Výkladový slovník kybernetické bezpečnosti definuje hrozbu jako *„Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizaci“* [1]. Hrozba má za následek poškození aktiva, jako jsou informace, procesy a systémy. Hrozba tedy poškozuje organizaci nebo jednotlivce. Podle ISO/IEC 27001 (Systémy řízení bezpečnosti informací – Požadavky) je příčinnou nechtěného incidentu, který ve výsledku vede nebo může vést k poškození systému nebo organizace.

Hrozby mohou být přírodního nebo i lidského původu. Měly by být tedy identifikovány zdroje hrozby, které mohou být spuštěny náhodně nebo úmyslně [3]. Josef Požár kategorizuje hrozby do dvou skupin [4]:

- **subjektivní** – jedná se o hrozby způsobené člověkem. Může se jednat o úmyslné hrozby motivující útočníka poškodit nebo zničit aktivum,
- **objektivní** – kam zařazuje hrozby přírodního nebo fyzického charakteru. Příkladem takových hrozeb mohou být povodně, požáry, výpadky napětí, zemětřesení atd.

1.1.4 Riziko

Rizikem se rozumí nebezpečí, možnost ztráty, škody, nezdaru v dosažení cílů, které si organizace stanovila. Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu [1].

Riziko je také chápáno jako účinek nejistoty na dosažení vytyčených cílů organizace. Nejistota je neschopnost přesně určit pravděpodobnost vzniku událostí a s ním spojený dopad na organizaci nebo společnost [5].

1.1.5 Zranitelnost

Zranitelnosti se rozumí slabé místo aktiva, řízení nebo slabé místo v bezpečnostním opatření, které může být využito jednou nebo kombinací více hrozeb [1], [2].

1.2 Kybernetická bezpečnost

S neustále se zlepšujícími a měnícími se kybernetickými hrozbami se organizace a vlády potýkají s řadou útoků mířených na informační a komunikační systémy v kybernetickém prostoru.

Kybernetickým prostorem je myšleno digitální prostředí, které umožňuje vznik, zpracování, ukládání a výměnu elektronických informací, tvořené informačními systémy, službami a sítěmi, elektronických komunikací [1], [6].

Kybernetická bezpečnost tak v posledních desetiletí narůstá na významu a stala se tak hlavní prioritou pro národní politiky. Nalézt komplexní definici kybernetické bezpečnosti je velmi obtížné, jelikož se jedná o rozsáhlou problematiku. Uvedeny budou jen některé ustálené definice [6]:

- Oxford Dictionaries definuje kybernetickou bezpečnost jako *„Situaci, kdy dochází k ochraně před kriminálním či neautorizovaným užitím elektronických dat“* [7],
- slovník Merriam Webster definuje kybernetickou bezpečnost jako *„Opatření přijatá k ochraně počítače nebo počítačového systému proti neoprávněnému přístupu nebo útoku“* [8],
- výkladový slovník kybernetické bezpečnosti uvádí, že se jedná o *„Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru“* [1],
- The European Union Agency for Network and Information Security, dále jen ENISA, ve svém terminologii uvádí, že kybernetická bezpečnost zahrnuje veškeré činnosti nezbytné k ochraně kybernetického prostoru, jeho uživatelů a ovlivněných osob před kybernetickými hrozbami.

„Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)“, dále jen ZoKB, přesnou definici neobsahuje. Zákon pouze upravuje práva a povinnosti osob, působnost a pravomoci orgánu veřejné moci v oblasti kybernetické bezpečnosti, dále pak zpracovává příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů [9].

Každá z uvedených definic se různí a obsahuje značné nepřesnosti. První z nich se zaměřuje pouze na elektronická data a opomíná uvést veškeré systémy vztahující

se ke kybernetickému prostoru, taktéž i druhá z uvedených definic. Tato definice se zaměřuje jen na ochranu počítačů a jeho systému.

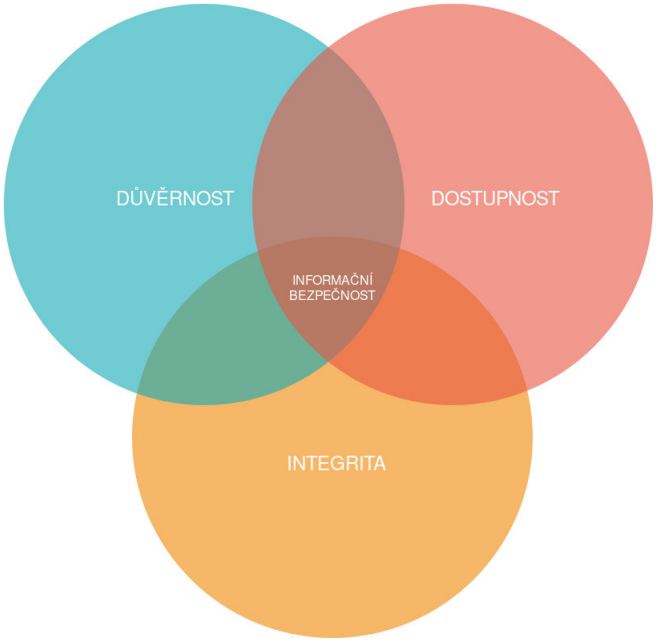
Výkladový slovník se zaměřuje na zajištění ochrany kybernetického prostoru, ale ne na zajištění ochrany subjektů využívající systémy nebo služby v tomto prostoru. ENISA už je v definici podrobnější, avšak pro pochopení celé problematiky kybernetické bezpečnosti je třeba přistupovat k této otázce komplexně.

1.2.1 Bezpečnost informací

Dalším pojmem, který je velice důležitý pro kybernetickou bezpečnost je bezpečnost informací. V některých literaturách uváděna jako informační bezpečnost. Jedná se o soubor obecných bezpečnostních opatření vedoucích k ochraně informací a informačních systému před neautorizovaným přístupem, užitím, zveřejněním, narušením, modifikací nebo jeho zničením [1], [10].

Informace obsahují výsledky lidského poznání, jedná se o každý znakový projev, který má smysl pro komunikujícího a příjemce. Výsledkem zpracování informace jsou data, která lze přenášet, uchovávat nebo zpracovávat [1].

Bezpečnostní triáda byla vytvořena pro snadnější pochopení bezpečnosti informací. Vytvořený model, který je znázorněn na obrázku 1.1 zachycuje sjednocení nejdůležitějších prvků bezpečnosti informací s cílem jejich ochrany v organizaci.



Obr. 1.1: Model CIA.

Model CIA zkratka pro anglické [1]:

- **C** – confidentiality (důvěrnost) – je důležitý prvek zajišťující schopnost ochránit data před neautorizovanými stranami. Jako příklad mechanismu zajišťující důvěrnost lze uvést šifrování dat,
- **I** – integrity (integritu) – poskytuje jistotu, že data nebyla změněna nebo smazána neoprávněným uživatelem,
- **A** – availability (dostupnost) – poskytuje přístup a použitelnost oprávněným uživatelům k jejich datum, kdykoliv mají zájem k nim přistoupit nebo užívat.

Cílem pro každou organizaci je sjednocení těchto prvků pro zajištění ochrany bezpečnosti informací. Komplexnější pohled na bezpečnost informací uvedl Donn Parker v modelu „The Parkerian Hexad“, kde k CIA triádě jsou přidány další tři prvky [11]:

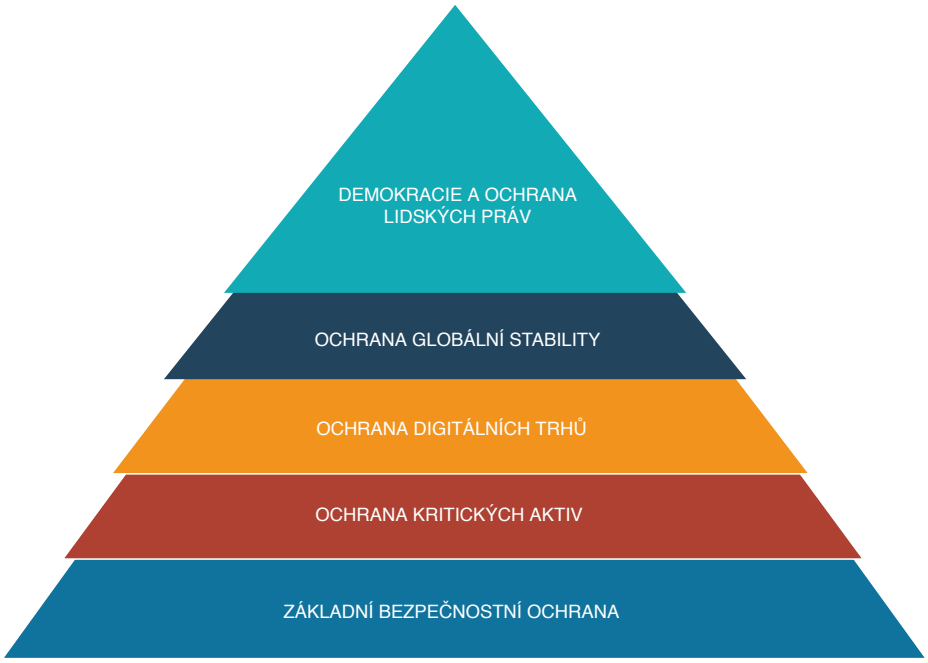
- **A** – authenticity (autentičnost),
- **P/C** – possession/Control (držení či kontrola),
- **U** – utility (užitečnost).

1.3 Kybernetický prostor

Následující část se bude věnovat kybernetickému prostoru a prohloubením pojmu kybernetická bezpečnost.

V kybernetickém prostoru člověk pracuje na různých úrovních a jednou z funkcí strategie by mělo být souvislé řešení všech různých úrovní kybernetického prostoru. Obrázek 1.2 čerpá z přístupu „Maslowovy“ pyramidy ke kategorizaci potřeb kybernetického prostoru hierarchickým způsobem. Podle ENISA musí být do pyramidy zahrnuty všechny aspekty kybernetického prostoru, aby byl zajištěn komplexní přístup k řešení kybernetických problémů [6].

Kybernetické bezpečnosti nelze v současném kontextu dosáhnout, aniž by byl řešen v rámci globálního kontextu. Měly by být zavedeny základní hodnoty, normy, směrnice, zákony, včetně etiky, které musí být aplikovány na všech úrovních v kybernetickém prostoru, tj. na všechny produkty a služby nezávisle na místě jejich výroby nebo vývoji na celém světě.



Obr. 1.2: Kategorizace potřeb kybernetického prostoru.

Klíčová je ochrana kritických aktiv, tedy ochrana kritické informační infrastruktury, jednotného digitálního trhu, včetně podniků i občanů. Významem kritická informační infrastruktura se bude zabývat kapitola 2.3.

Následující odstavce poskytují stručný popis pyramidy a vrstev pro požadavky kybernetické bezpečnosti [6], [12], [13]:

- **základní bezpečnostní ochrana** – bezpečnost pro uživatele v kybernetickém prostoru je bezesporu jedna z nejdůležitějších vrstev této pyramidy. Za žádných okolností by neměla být ohrožena bezpečnost uživatelů v důsledků akcí v kybernetickém prostoru. Měla by být přijata a implementována preventivní opatření. Dále pak vzdělanost a informovanost uživatelů je klíčem k ochraně před kybernetickými hrozbami. Každý uživatel by si měl být vědom toho, jaká rizika mohou nastat, a proto by měl přijmout vhodná opatření. Příkladem může být firewall, software s detekcí škodlivého kódu, aktualizace a opravy zabezpečovacího zařízení nebo softwaru,
- **ochrana kritických aktiv** – práce je především zaměřena na ochranu kritické infrastruktury a kritické informační infrastruktury, proto tato vrstva bude detailněji popsána. V posledních deseti letech se volalo po potřebě ochrany kritické informační infrastruktury. Na tento popud vznikla *„Směrnice Evropského parlamentu a Rady Evropské Unie 2016/1148 se dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systému v Unii (směrnice NIS)“*, dále jen NIS.
  Směrnice o bezpečnosti sítí a informačních systémů NIS, představuje první

celoevropská pravidla týkající se kybernetické bezpečnosti. Cílem směrnice je dosáhnout vysoké společné úrovně bezpečnosti síťových a informačních systémů v EU. Zlepšení možnosti spolupráce na vnitrostátní úrovni a posílení spolupráce na úrovni EU. Směrnice ukládá povinnosti provozovatelů základních a digitálních služeb hlásit bezpečnostní incidenty a podporuje kulturu řízení rizik bezpečnosti informací. Směrnice NIS je významným mezníkem při budování kybernetické bezpečnosti na evropské úrovni.

Směrnice NIS v článku 12 zřizuje síť vnitrostátních týmů CSIRT (Skupina pro reakce na počítačové bezpečnostní incident–Computer security incident response team), rovněž označované jako týmy CERT (Skupina pro reakci na počítačové hrozby – Computer Emergency Response Team), které mají za cíl přispívat k budování důvěry mezi členskými státy a podpořit rychlou a účinnou operativní spolupráci. Síť CSIRTs poskytuje fórum, kde mohou členové spolupracovat, vyměňovat si informace a budovat důvěru. Členové budou moci zlepšit řešení přeshraničních incidentů a dokonce diskutovat o tom, jak koordinovaně reagovat na konkrétní incidenty. Povinnosti, které směrnice NIS ukládá jsou zavedeny v České republice ZoKB,

- **ochrana digitálních trhů** – vývoj počítačového prostředí a technologií poskytuje příležitost pro rozvoj podnikání. Vzhledem ke kritické infrastruktuře je třeba chránit všechny podniky, protože jejich závislost na kybernetickém prostoru roste. Vstup EU je nezbytný pro řešení kybernetických incidentů realizovaných v rámci unie.
- **ochrana globální stability** – kybernetická válka nebo kybernetická špionáž, o nichž existuje několik diskuzí o potřebě vytvoření norem. Kybernetickou válkou se zabývá „Tallin Manual“, který nebude dále v práci popsán,
- **demokracie a ochrana lidských práv** – nové technologie jako např. autonomní vozidla vyžadují diskuse o etických aspektech provozu nové technologie. Online ochrana lidských práv je další výzvou pro ochranu v kybernetickém prostoru. Dopad nových technologií, produktů a služeb musí být posuzovány a měly by být zavedeny odpovídající opatření. Tedy poslední vrstva poukazuje na to, že jakákoliv nová technologie by neměla podkopávat lidská práva, svobody a demokracii.

Pyramida znázorňuje co vše by mělo být v kybernetickém prostoru chráněno a na co se podrobněji zaměřit. Kybernetická bezpečnost se tedy vztahuje na bezpečnost kybernetického prostoru (zahrnující právnické, organizační, technické a vzdělávací prostředky).

Kybernetická bezpečnost bude zahrnovat vzor „CIA“ triády pro vztahy a objekty v rámci kybernetického prostoru a zároveň bude tento model rozšiřován z důvodu zajištění ochrany soukromí subjektů (fyzických a právnických osob) a odolnosti proti

kybernetickým hrozbám. [1], [6].

2 Kritická infrastruktura

Bezpečnost kritické infrastruktury se stává pro vlády a organizace prioritou, zejména je kladen důraz na dodržování a doplňování legislativních nařízení, směrnic a doporučení. Cílem je přijetí legislativy a jejich dodržování pro zajištění ochrany kritické infrastruktury.

Kritickou infrastrukturou, dále jen KI se dle *„zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)“* rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu [14].

2.1 Kritéria pro určení prvku kritické infrastruktury

Prvek kritické infrastruktury je především stavba, zařízení, prostředek nebo veřejná správa. Jestliže je prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury.

Evropskou kritickou infrastrukturou se rozumí kritická infrastruktura na území České republiky, jejíž narušení by mělo závažný dopad na členské státy EU [1], [14]. Dle *„Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění novely č. 315/2014 Sb.“* jsou určena průřezová a odvětvová kritéria pro určení prvku KI. *„Novela č. 315/2014 Sb.“*, rozšiřuje nařízení o oblast kybernetické bezpečnosti.

2.1.1 Průřezová kritéria

Hlediskem pro určení průřezových kriterií jsou [15]:

- *„oběti s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,*
- *ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu nebo,*
- *dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob“.*

2.1.2 Odvětvová kritéria

Odvětvová kritéria jsou značně rozsáhlá. Dotýká se energetiky, vodního hospodářství, potravinářství, zemědělství a dalších oblastí, proto budou vybrány oblasti tý-

kající se kybernetické bezpečnosti. Celkem je definováno devět odvětví, včetně jednotlivých odvětvových kritérií pro určení prvku KI.

Do komunikačních a informačních systémů spadají technologické prvky pevné sítě elektronických komunikací. Jedná se o [15]:

- centrum řízení a podpory sítě,
- řídící ústředna,
- mezinárodní ústředna,
- transitní ústředna,
- datová centra,
- telekomunikační vedení.

Dále jsou uvedeny technologické prvky mobilní sítě elektronických komunikací, jedná se o [15]:

- centrum řízení a podpory sítě,
- ústředna mobilní sítě,
- základnová řídící jednotka sítě pokrývající strategickou lokalitu,
- základnová stanice sítě pokrývající strategickou lokalitu,
- datová centra.

Dále jsou uvedeny technologické prvky sítí pro rozhlasové a televizní vysílání. Zde jsou uvedeny [15]:

- vysílací zařízení pro šíření televizního nebo rozhlasového signálu určené pro informovanost obyvatelstva za krizové situace s vysílacím výkonem nejméně 1kW,
- řídící pracoviště provozu,
- datová centra,
- síť pro rozhlasové a televizní vysílání.

Uvedeny jsou taktéž prvky pro satelitní komunikaci, prvky pro poštovní služby a technologické prvky informačních systémů, kam spadá [15]:

- řídicí centra,
- datová centra,
- sítě elektronických komunikací,
- technologický prvky zajišťující provoz registru doménových jmen „CZ“.

„Novela č. 315/2014 Sb“., rozšiřuje nařízení o oblast kybernetické bezpečnosti pod posledním písmenem „G“, kam spadá [15]:

- *„informační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,“*
- *„komunikační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,“*

- *„informační systém spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300 000 osobách,“*
- ***„komunikační systém, zajišťující připojení nebo propojení prvku kritické infrastruktury, s kapacitou garantovaného datového přenosu nejméně 1 Gbit/s“***.

Všechna uvedená odvětvová kritéria se užijí přiměřeně pro oblast kybernetické bezpečnosti. Pokud prvek splňuje uvedená kritéria, stává se prvkem kritické informační infrastruktury. V případě optických sítí se jedná o prvek kritické informační infrastruktury.

2.2 Povinnosti subjektů kritické infrastruktury

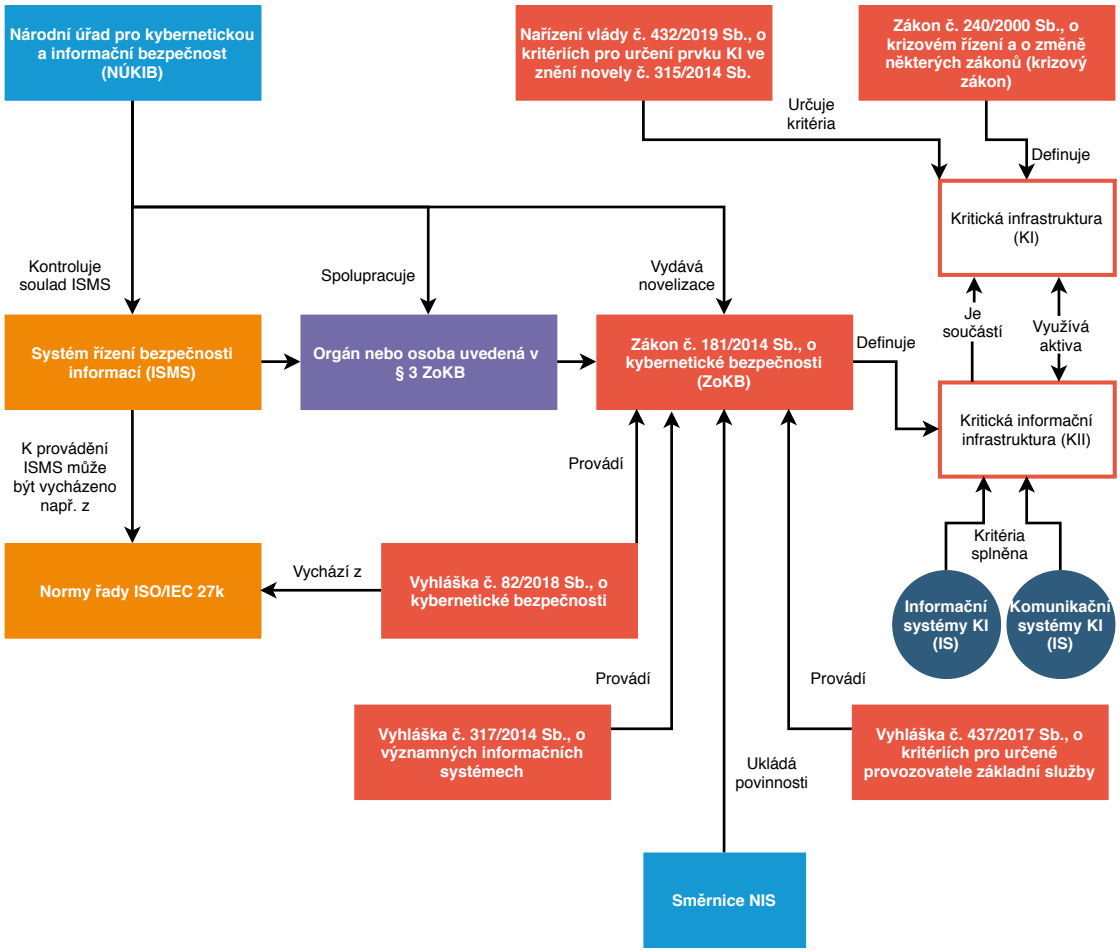
Subjektem KI je provozovatel prvku KI nebo provozovatel prvku evropské kritické infrastruktury. V případě splnění kritérií pro určení prvku KI je na výzvu příslušného správního úřadu provozovatel povinen poskytnout informace nezbytné k určení prvku KI a prvku evropské kritické infrastruktury a další součinnosti pří ochraně KI. Součinností je myšlena bližší spolupráce a komunikace s příslušnými ústředními správními úřady, ministerstvy, ale i kraji. Subjekt kritické infrastruktury odpovídá za ochranu prvku kritické infrastruktury. Za tímto účelem je dle *„zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)“* je povinen [14], [16]:

- vypracovávat plán krizové připravenosti subjektu kritické infrastruktury do jednoho roku od rozhodnutí vlády nebo ode dne nabytí právní moci opatření obecné povahy,
- umožnit příslušnému ministerstvu nebo jinému ústřednímu správnímu úřadu vykonání kontroly plánu krizové připravenosti subjektu KI a ochranu prvku kritické infrastruktury včetně umožnění vstupů a vjezdů na pozemky a do prostorů, ve kterých se prvek KI nachází,
- oznámit příslušnému ministerstvu nebo jinému ústřednímu správnímu úřadu bez zbytečných odkladů informace o organizační, výrobní, nebo jiné změně, která může mít vliv na určení prvku KI, zejména informace o trvalém zastavení provozu, ukončení činnosti, nebo restrukturalizaci.

Plány krizové připravenosti subjektu KI kontrolují ministerstva a jiné ústřední správní úřady. Plány krizové připravenosti obsahují identifikaci možných ohrožení funkce prvku KI a stanovují vhodná opatření na jeho ochranu.

2.3 Kritická informační infrastruktury

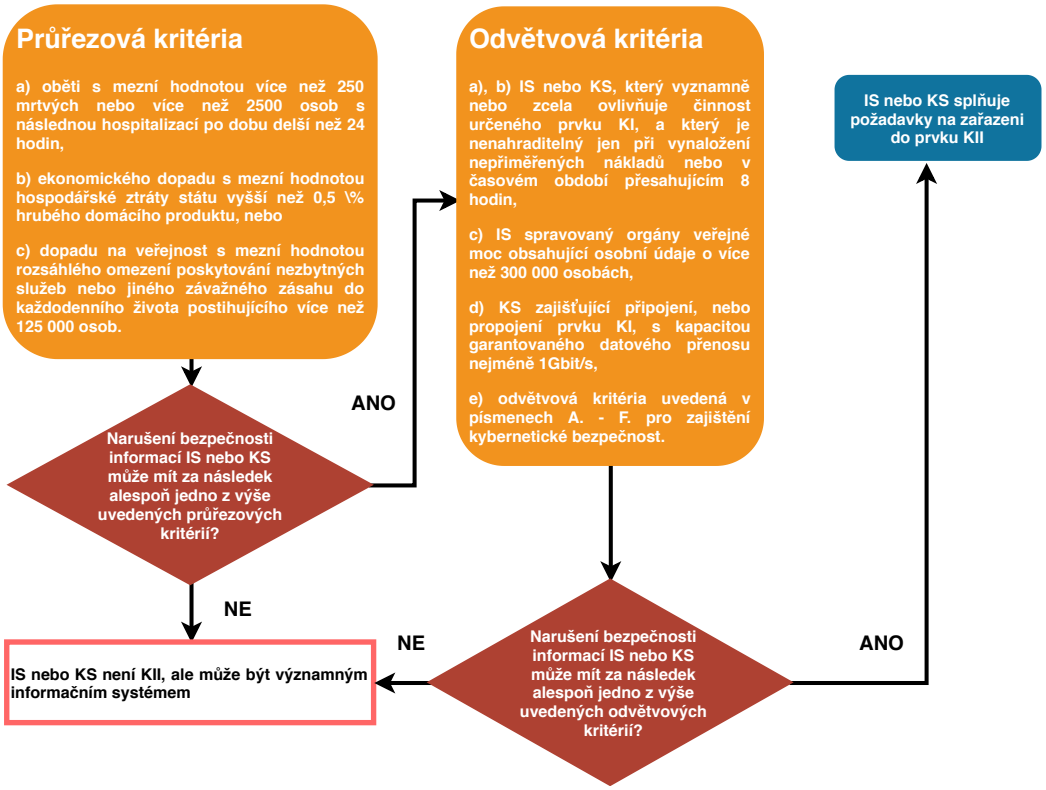
Kritická informační infrastruktura, dále jen KII, je součástí kritické infrastruktury, pokud splňuje výše uvedená kritéria pro určení prvku kritické infrastruktury. Orgány nebo osoby splňující kritéria jsou povinni, podle ZoKB zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačních systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému a vést o nich bezpečnostní dokumentaci [9]. Obrázek 2.1 znázorňuje blokové schéma ZoKB a jeho prováděcích předpisů.



Obr. 2.1: Blokové schéma ZoKB.

2.3.1 Proces určování prvku kritické informační infrastruktury

Celý proces je znázorněn na obrázku 2.2. V případě narušení bezpečnosti informací (důvěrnosti, dostupnosti a integrity) informačního nebo komunikačního systému, vedoucí za následek alespoň jedno z výše uvedených průřezových kritérií a odvětvových kritérií se stává prvkem kritické informační infrastruktury.



Obr. 2.2: Proces určování prvku kritické informační infrastruktury [15].

3 Systém řízení bezpečnosti informaci

Pro každou organizaci je klíčová bezpečnost informací. Znamenající uplatnění obecných bezpečnostních opatření a postupů sloužících k zajištění ochrany před ztrátou integrity, dostupnosti a důvěrnosti. Systém řízení bezpečnosti informací, dále jen ISMS, představuje základní přístup pro vytvoření podmínek v organizaci, které zajistí potřebnou ochranu informací před ztrátou důvěrnosti, dostupnosti a integrity. ISMS lze aplikovat jak na celou organizaci, tak na organizační složku v rámci organizace nebo na specificky určený komunikační a informační systém.

3.1 Normy řady ČSN ISO/IEC 27000

Procesem a řízením rizik v kybernetické bezpečnosti zaměřené na organizace se zaměřuje sada norem ISO/IEC 27000, vydané mezinárodní organizací pro standardizaci ISO. Níže je uvedená sada norem napomáhající organizacím zavést a provozovat ISMS:

- ISO/IEC 27000 Systémy řízení bezpečnosti informací – Přehled a slovník,
- **ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky**,
- ISO/IEC 27002 Soubor postupů pro opatření bezpečnosti informací,
- ISO/IEC 27003 Směrnice pro implementaci systému řízení bezpečnosti informací,
- ISO/IEC 27004 Řízení bezpečnosti informací – Měření,
- **ISO/IEC 27005 Řízení rizik bezpečnosti informací.**

Výše uvedené normy lze označit za základní sadu norem zabývající se problematikou bezpečnosti informací, implementaci a požadavky na ISMS. Další uvedené normy doplňují a rozšiřují jednotlivé dílčí části, které jsou nezbytné ke komplexnímu zajištění kybernetické bezpečnosti v organizaci. Jedná se o tyto normy:

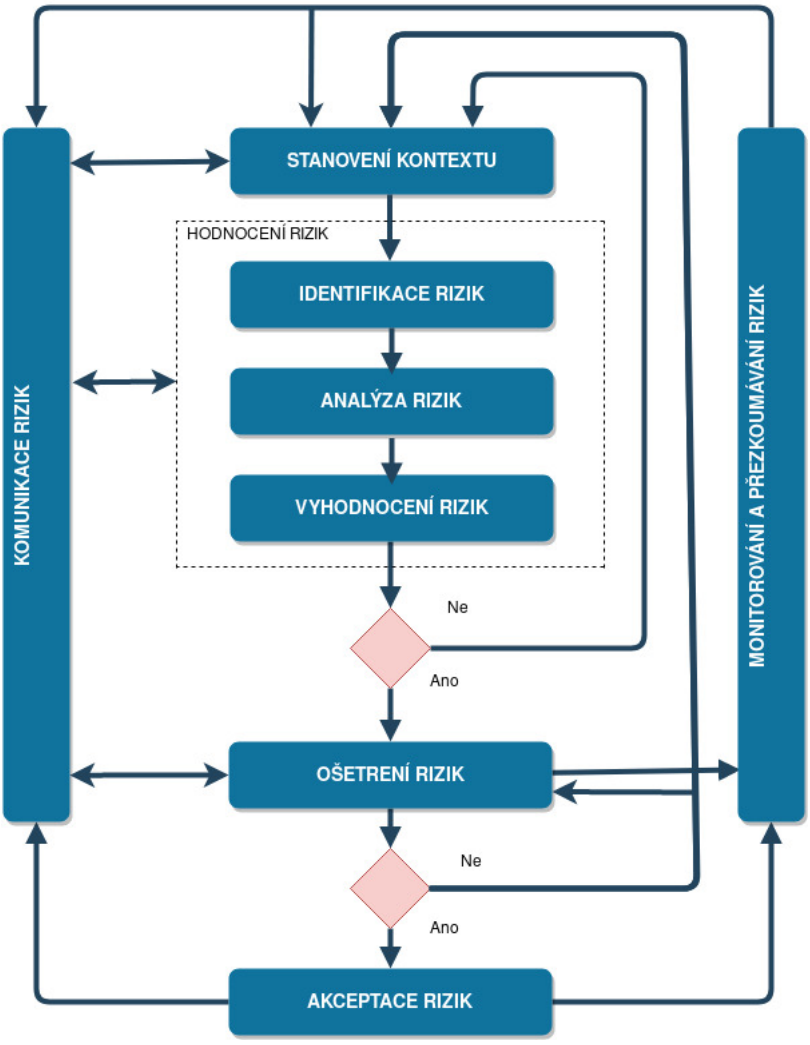
- ISO/IEC 27006 Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací,
- ISO/IEC 27007 Směrnice pro audit systémů řízení bezpečnosti informací,
- ISO/IEC TR 27008 Směrnice pro auditory opatření bezpečnosti informací,
- ISO/IEC 27009 Oborově specifická aplikace ISO/IEC 27001 – Požadavky,
- ISO/IEC 27010 Řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi,
- ISO/IEC 27011 Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002,
- ISO/IEC 27013 Pokyn pro integrovanou implementaci ISO/IEC 27001,
- ISO/IEC 27014 Správa a řízení bezpečnosti informací,

- ISO/IEC TR 27015 Směrnice pro řízení bezpečnosti informací pro finanční služby,
- ISO/IEC TR 27016 Řízení bezpečnosti informací – Organizační ekonomika,
- ISO/IEC 27017 Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002,
- ISO/IEC 27018 Soubor postupů pro ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII,
- ISO/IEC 27019 Směrnice pro řízení bezpečnosti informací na základě ISO/IEC 27002 pro systémy řízení procesů specifické pro odvětví energetiky.

Řízení rizik bezpečnosti informaci je systémový a komplexní přístup, který dodržuje principy a prvky v rámci celého životního cykly kybernetické bezpečnosti. Řízení rizik bezpečnosti informaci je definována v ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informaci, která poskytuje doporučení pro řízeni rizik bezpečnosti informací v rámci organizace s ohledem na požadavky řízení bezpečnosti informací podle ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systém řízení bezpečnosti informací - Požadavky. V práci je využita sada norem ISO/IEC 27001 a ISO/IEC 27005.

4 Proces řízení rizik bezpečnosti informací

Norma ISO/IEC 27005 obsahuje popis procesu řízení rizik bezpečností informací a jeho činnosti, které lze aplikovat pro celou organizaci nebo jakoukoliv samostatnou část organizace (např. oddělení, fyzické místo, službu)nebo jakýkoliv informační systém, který vyžaduje řízení rizik a bezpečnost informací. Dále norma obsahuje doporučení a obecný koncept pro řízení rizik s ohledem na požadavky řízení bezpečnosti informací podle ISO/IEC 27001. Řízení rizik bezpečnosti informací by měl být nepřetržitý proces. Celý proces je znázorněn na obrázku 4.1.



Obr. 4.1: Proces řízení rizik bezpečnosti informací.

4.1 Stanovení kontextu

Je prvním krokem v procesu řízení rizik bezpečnosti informací, kde organizace formuluje své cíle, základní kritéria, rozsah, hranice, role a odpovědnosti v procesu řízení rizik.
V procesu stanovení kontextu by měly být určeny vnější a vnitřní aspekty, které jsou klíčové ke stanovení rozsahu systému řízení rizik bezpečnosti informací. Tyto aspekty mohou významně ovlivňovat dosažení cílů organizace a proto by měly být vyjádřeny a zohledněny v procesu řízení rizik bezpečnosti informací.

Stanovení vnějšího kontextu zahrnuje vnější prostředí, ve kterém organizace usiluje o dosažení cílů. V tomto kroku je také důležité porozumět potřebám a očekáváním zainteresovaných stran, které jsou ve vztahu k systému řízení rizik bezpečnosti informací. Vnější kontext může zahrnovat [17]:

- kulturní závislosti, politické prostředí, legislativní dokumenty, finanční prostředí, technologické prostředí, ekonomické prostředí, přírodní a konkurenční prostředí,
- vztahy se třetími stranami.

Stanovení vnitřního kontextu se týká vnitřního prostředí, ve kterém organizace usiluje o dosažení svých cílů. Vnitřní kontext může zahrnovat následující aspekty [17], [18]:

- hlavní účel organizace, obchodní činnost a strategie,
- vedení, role a odpovědnosti v organizaci, organizační strukturu, politiku organizace vztahující se k bezpečnosti informací,
- organizační kulturu, hodnoty a vztahy uvnitř organizace,
- finanční hledisko a zdroje,
- informační aktiva.

Po stanovení rozsahu a cílech organizace by měl být vybrán vhodný přístup, řešící základní kritéria. Základní kritéria se skládají z kritérií pro hodnocení rizik, kritérií dopadu a kritérií akceptace rizik [18]:

- kritéria pro hodnocení rizik – měla by být vytvořena vhodná metodika pro stanovení hodnocení rizik na jejichž základě se následně rizika ošetřují,
- kritéria dopadu – organizace by měla vytvořit kritéria dopadu, která jsou odvozena od stupně škod nebo ztrát způsobených bezpečnostním incidentem,
- kritéria akceptace rizik – akceptovatelné riziko je pro organizaci riziko, které je přijatelné a nevyžaduje bezpečnostní opatření. Kritéria pro akceptaci rizik se mohou v čase měnit, a proto by se taková rizika měla nadále monitorovat.

4.2 Hodnocení rizik

Hodnocení rizik nebo také posouzení rizik. Jedná se o celkový proces zahrnující identifikaci rizik, analýzu rizik a hodnocení rizik. Podle požadavků plynoucích z normy ISO/IEC 27001 musí organizace definovat a aplikovat proces posuzování rizik bezpečnosti informací [3].

Proces posouzení rizik zahrnuje i identifikaci stávajících opatření, které byly implementovány a jsou dokumentovány již v předešlých zprávách auditu ISMS. Tento krok ušetří organizaci čas stráveným nad tímto úkolem. V případě nefunkčnosti opatření se musí implementovat dodatečná opatření. Výstupem identifikace stávajících opatření je seznam stávajících a plánovaných opatření, jejich zavádění a stav užívání [18].

4.2.1 Identifikace rizik

Slouží k odhalení zdrojů rizik, které jsou nebo nejsou pod kontrolou organizace. Dále oblasti dopadu, následků a příčin, které vedou k potencionálním ztrátám. Identifikace rizik zahrnuje identifikaci všech aktiv, která mají pro organizaci hodnotu a vyžadují ochranu. U každého aktiva by měl být identifikován jeho vlastník a odpovědnost za aktivum. Každé aktivum by mělo být ohodnoceno na základě jeho důležitosti pro organizaci. Organizace si sama stanoví škálu pro hodnocení aktiv, podle vlastních potřeb. Nejvíce se využívá pro hodnocení aktiv stupnice o čtyřech úrovních, ve kterých se posuzuje, jaký by byl dopad v případě narušení bezpečnosti informací u jednotlivých aktiv. Výstupem identifikace aktiv je seznam všech aktiv u nichž je třeba zajistit řízení rizik [2].

Následně by měly být identifikovány hrozby, které mají potenciál poškodit aktivum. Hrozba může být přírodního nebo lidského původu a může být úmyslná nebo náhodná. Hrozba jako taková využívá zranitelnosti například v systémech nebo sítích informačních a komunikačních technologií. Zranitelnost nepůsobí škody, pokud neexistuje hrozba. Zranitelnost se identifikuje například v organizaci, hardwaru, softwaru, procesech, postupech, ale také i u pracovníků a to v případě jejich neznalosti, neodbornosti ve využívaných systémech. Výstupem z identifikace hrozeb by měl být seznam zranitelností, hrozeb a aktiv [18].

Dalším bodem v procesu identifikace rizik je identifikace následků. V tomto případě by měly být identifikovány následky vztahující se k aktivu, které povedou ke ztrátě důvěrnosti, dostupnosti nebo integrity. Následkem je myšlena realizace scénářů incidentu, které povedou ke škodám nebo dopadům na organizaci. Ve scénáři incidentů se identifikují hrozby využívající určité zranitelnosti nebo souboru zranitelností. Následky mohou poškodit nebo ovlivnit jedno a více aktiv v organizaci.

Výstupem identifikace scénářů by měl být seznam všech scénářů incidentů s jejich následky, identifikovaná aktiva, hrozby a zranitelnosti [18].

4.2.2 Analýza rizik

Analýza rizik slouží jako vstup pro hodnocení rizik. Výstupem z analýzy rizik je matice rizik, která je kombinací pravděpodobností a dopadu. U analýzy rizik je důležité zvolit vhodnou metodu pro vyjádření veličin analýzy rizik. Mezi tyto metody se řadí [18], [19]:

- **kvalitativní** – metoda postavena na slovním vyjádření dopadu nežádoucí události (např. nízká, střední, vysoká, kritická) a slovního vyjádření pravděpodobnosti (frekvence), že daná událost vznikne (například velmi nízká, nízká, střední, vysoká, velmi vysoká),

  V praxi se nejdříve provede kvalitativní metoda pro systémy u kterých nebyla provedena analýza rizik. Výhodou je rychlost zhodnocení a identifikování kritických rizik a následná implementace opatření na snížení rizik. Další výhodou jsou nižší náklady a nároky na lidské zdroje, využití jednoduchých výpočtů a snadnější pochopení výstupu. Nevýhodou této metody je subjektivní výběr škály, nižší správnost výstupu, nižší spolehlivost získaných výstupů a problémy při stanovení finančních prostředku pro zvládání hrozeb,
- **kvantitativní** – metoda využívá stupnici s číselnými hodnotami, jak pro pravděpodobnost vzniku události, tak pro ohodnocení dopadu. Tato metoda se nejvíce ujala v oblasti bezpečnosti informačních systému. Výhodu této metody o proti kvalitativní je vyšší správnost a spolehlivost výstupů. Kvantitativní metoda využívá historická data incidentů. Nevýhodou tedy může být nedostatek těchto dat u nových rizik nebo slabých míst v bezpečnosti, další nevýhodou je náročnost na zpracování výsledků o proti kvalitativní metodě,
- **kombinace obou** – metoda kombinující kvalitativní a kvantitativní metody. Tedy slovní i numerické vyjádření pro pravděpodobnost vzniku události a dopadu.

Příklad využití kvalitativní metody je uveden v tabulce 4.1, ve kterém jednotlivá písmena značí úrovně rizika:

- A – nízká,
- B – střední,
- C – vysoká,
- D – kritická,

Matice rizik je vstupem pro hodnocení rizik. Pro analýzu rizik musí být posouzeny dopady. V tomto kroku se ohodnocují obchodní dopady na organizaci, které mohou vyplývat z možných nebo skutečných incidentů. Organizace by měla brát

Pravděpodobnost/Dopad	Nízká	Střední	Vysoká	Kritická
Velmi nízká	A	A	A	B
Nízká	A	B	B	C
Střední	A	B	C	C
Vysoká	B	C	C	D
Velmi vysoká	B	C	D	D

Tab. 4.1: Ukázka matice rizik.

v úvahu náklady na obnovu nebo náhradu aktiv, obchodní následky, které mohou plynout ze ztráty integrity, dostupnosti, důvěrnosti a mnoho dalších. Následky se nejčastěji vyjadřují v peněžních jednotkách.

Dále v matici rizik musí být určena pravděpodobnost vzniku scénáře incidentu. Pravděpodobnost je založena na platných statistikách, zkušenostech, na známých zranitelnostech v systémech, na motivaci a schopnostech útočníků a dalších [18].

4.2.3 Hodnocení rizik

Hodnocení rizik zahrnuje proces, ve kterém se posuzují úrovně rizik získané z matice rizik a porovnávají se s kritérii hodnocení rizik v kontextu se scénáři incidentu. Výstupem hodnocení rizik by měl být seznam rizik, kterým byla dána priorita. Pokud jsou splněna všechna kritéria, postupy a existuje dostatek informací o rizicích následuje ošetření rizik. V případě nesrovnalostí nebo detailnějšího přezkoumání se postup opakuje od stanovení kontextu. [18].

4.3 Ošetření rizik

Jedná se o neustálý opakující se cyklus. Opakování vede k zajištění, že rizika s vysokou úrovní jsou náležitě posouzena. Vstupem je seznam rizik, kterým byla přidělena priorita, podle kritérií pro hodnocení rizik v souvislosti se scénáři incidentů. Měla by být vybrána a implementována vhodná opatření pro snížení rizik.

Existují čtyři možnosti pro ošetření rizik [3], [18]:

- **modifikace rizika** – u modifikace rizik se vybírají vhodná a odůvodněná opatření. Organizace by při výběru opatření měla brát v úvahu časové, finanční, technické, provozní a jiné omezení uvedené v ISO/IEC 27005. Například finanční omezení je chápáno ve smyslu, kdy přijení nebo udržování opatření by bylo finančně dražší, než hodnota rizika. Cílem je tedy přijmout takové opatření, které by vedlo ve prospěchu organizace,

- **vyhnutí se riziku** – organizace se může rizikům vyhnout a to v případě plánovaných činností, kde by byla rizika vysoká a jejich ošetření by převyšovalo náklady. Příkladem může být výstavba budovy se zařízením v záplavových oblastech, kde s největší pravděpodobností plyne vysoké riziko způsobené přírodními vlivy,
- **podstoupení rizika** – o podstoupení rizik rozhoduje organizace v případě, kdy je výstupem z hodnocení rizik, riziko přijatelné pro organizaci. V takovém případě nemusí být implementována žádná opatření, avšak taková rizika se musí i nadále monitorovat. Organizace učiní formální rozhodnutí o podstoupení rizik a odpovědnosti za toto rozhodnutí v souvislosti s ISO/IEC 27001. Výstupem je seznam akceptovaných rizik,
- **sdílení rizik** – riziko může být sdíleno se třetí stranou. Příkladem může být pojištění, uzavřením smluv se třetí stranou, která může monitorovat informační systémy a v případě výpadku poskytnout podporu.

Po výběru z uvedených možností se rozhoduje o zbytkovém riziku. Zbytkové riziko je takové riziko, které zůstává i po zavedení příslušných opatření, ale je sníženo na příslušnou úroveň a nadále se monitoruje. V případě, kdy je zbytkové riziko přijatelné pro organizaci následuje akceptace rizik. V opačném případě je nutné znovu posoudit riziko a změnit parametry kontextu [18].
Výstupem z procesu ošetření rizik je plán ošetření rizik a seznam zbytkových rizik, které vyžadují rozhodnutí vedoucího pracovníka organizace pro jejich akceptaci [18].

4.4 Akceptace rizik

Akceptace rizik je posledním krokem v procesu řízení rizik bezpečnosti informací. Zde by měla být učiněna formální rozhodnutí o akceptaci rizik a odpovědnosti za toto rozhodnutí v souvislosti s ISO/IEC 27001. Výstupem procesu akceptace rizik je seznam akceptovaných rizik a rizik, které nesplňují kritéria pro akceptaci rizik v organizaci [18], [3].

4.5 Komunikace, monitorování a přezkoumání rizik

Komunikace je důležitou součástí v celém procesu řízení rizik bezpečnosti informací. Komunikace rizik zahrnuje informace o rizicích, prováděných akcí, sdílení nových informací mezi zainteresovanými stranami, koordinaci apod. Komunikace zajišťuje chápání celého procesu řízení rizik bezpečnosti informací a pochopení jednotlivých výsledků v procesu řízení rizik v organizaci [18].
Monitorování a přezkoumání rizik slouží k identifikaci změn u hrozeb, zranitelností,

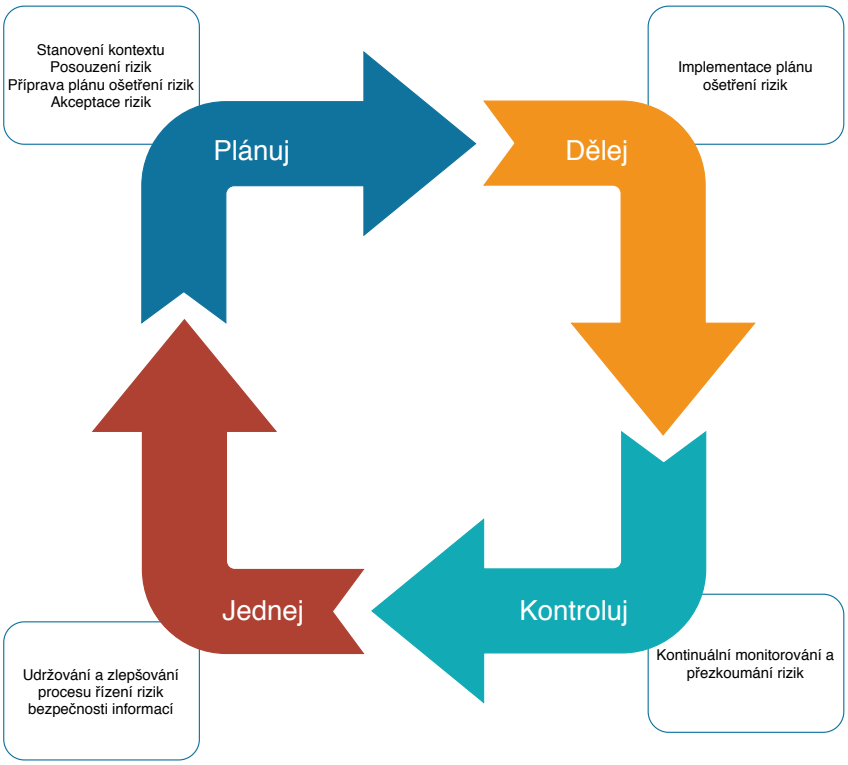
pravděpodobností nebo dopadů. Monitorování mohou provádět externí služby, které poskytují informace o hrozbách nebo zranitelnostech [18].

4.5.1 PDCA cyklus v procesu systému řízení rizik

ISMS je založen na „Demingově cyklu“, známe také jako „PDCA“cyklus:

- **P** – plan (plánuj),
- **D** – do (dělej),
- **C** – check (kontroluj),
- **A** – act (jednej).

„PDCA“ cyklus je základním manažerským principem spočívající v postupném zlepšování kvality procesů, služeb, dat, aj. Norma ISO/IEC 27005 využívá tento cyklus v rámci činností řízení rizik bezpečnosti informací. Obrázek 4.2 znázorňuje „PDCA“ cyklus poskytující ucelený přehled jednotlivých fází procesu řízení rizik, které byly detailně popsány v 4.



Obr. 4.2: Propojení PDCA cyklu s ISMS.

5 Software verinice

Následující sekce praktické části se budou věnovat popisem softwaru Verinice a procesem řízení rizik bezpečnosti informací, podle standardu ISO/IEC 27005, s ohledem na požadavky standardu ISO/IEC 27001. Předpokladem pro proces řízení rizik je organizace splňující kritéria pro určení prvku kritické infrastruktury a současně tento prvek bude spojen s KII. Proces řízení rizik bezpečnosti informací se proto aplikuje na datové centrum v rámci objektu. Zároveň nebude opomenuto zahrnout do procesu optické kabely vedoucí z datového centra mimo areál objektu. Přístup do internetu je poskytován centrální jednotkou OLT (Optické linkové zakončení – Optical Link Termination).
Pro pochopení fungování a využívání softwaru Verinice bude na jednom příkladu uvedeno aktivum a k němu příslušící scénář incidentu. Na zmíněném příkladu bude vytvořena matice rizik, kde se následně rizika ohodnotí a rozhodne se o jejich akceptaci.

5.1 Software Verinice

Je Open Source nástroj pro řízení rizik bezpečností informací a tvorbu ISMS v souladu s řadou norem ISO 27000, umožňující následující procesy:

- analýzu rizik podle ISO 27005,
- importování vlastního katalogu rizik a součástí ve formátu XML.

Software Verinice byl využit pro tvorbu vlastního katalogu rizik ve formátu .VNA.

5.1.1 Vytvoření organizace

Prvním krokem je vytvoření organizace a stanovení kritérií pro akceptaci rizik. Tato kritéria závisí na politikách, záměrech, cílech organizace a zájmech zainteresovaných stran. Pro stanovení kritérií akceptace rizik software Verinice nabízí následující hodnoty:

- důvěrnost (0–11),
- integrita (0–10),
- dostupnost (0–12).

Pro účely práce byly nastaveny následující hodnoty akceptace rizik:

- důvěrnost 7,
- integritu 6,
- dostupnost 6.

Tyto hodnoty určují rozsah akceptovaných rizik, které se promítají v maticích rizik ve výsledném katalogu rizik nacházejícím se v příloze B. Vhodně zvolená kritéria pro

akceptaci rizik závisí na organizaci a cílech, které chce dosáhnout. Software Verinice na základě těchto hodnot odlišně zvýrazní výsledné matice. Pokud by byly zvoleny příliš nízké hodnoty, například 3 pro důvěrnost, ve výsledné matici rizik by chyběla škála pro rizika nízká (zvýrazněná zelenou barvou). Tímto způsobem by organizace nedosáhla přijatelnosti rizika. Postupem výpočtů se blíže věnuje kapitola 5.2.

Dále software nabízí stanovení dopadu v peněžních jednotkách. Výstup stanovení těchto hodnot je uvedený v příloze B. Tyto hodnoty neodpovídají přesným peněžním jednotkám konkrétní organizace, jedná se pouze o demonstraci využití dopadu s konkrétními částkami.

5.1.2 Identifikace aktiv

Následuje identifikace aktiv, která jsou pro organizaci hodnotná. Software rozlišuje primární a podpůrná aktiva. Primárními aktivy se rozumí hlavní procesy v organizaci, jejichž ztráta nebo omezení by neumožnila plnit poslání organizace. V softwaru byly definovány dva hlavní procesy:

- **přenos dat** – pro přenos dat byla nastavena kritéria dopadu na důvěrnost 3, integritu 2, dostupnost 3. Jedná se o nejvyšší hodnoty dopadu na proces,
- **záloha dat** – pro zálohu dat byla stanovena kritéria dopadu pouze na dostupnost 3.

Podpůrná aktiva mají zranitelnosti, které mohou být využity hrozbami s cílem poškození primárních aktiv, vedoucích k znemožnění dosažení stanovených cílů organizace. U každého aktiva musí být identifikován vlastník a vedoucí pracovníci organizace, kteří mají za toto aktivum zodpovědnost. V softwaru byly identifikovány následující skupiny podpůrných aktiv:

- **hardware** – data storage, optické kabely, optická vlákna, servery, rozbočovače, EDFA (Vláknový erbiem dopovaný zesilovač – Erbium Doped Fiber Amplifier), DWDM (Hustý vlnový multiplex – Dense Wavelength Division Multiplex) MUX/DEMUX, OADM (Pasivní optický Add/drop multiplexer – Optical Add Drop Multiplexor), ONU (Optická síťová jednotka – Optical Network Unit), SOA (Polovodičový zesilovač – Semiconductor Optical Amplifier), Raman zesilovač, CWDM (Hrubý vlnový multiplex – Coarse Wavelength Division Multiplex) MUX/DEMUX, transceiver, switch,
- **software** – databáze, operační systémy, systém pro kontrolu vstupu,
- **komunikační síť** – optická síť, Ethernet,
- **data a informace** – konfigurační data, záznamy, data třetích stran, přenášená data, dokumentace,
- **jiné vybavení** – klimatizace, kabeláž, kamerový systém, hasící přístroj, rack, čtečky identifikačních karet zaměstnanců, identifikační karty zaměstnanců.

Pro ohodnocení podpůrných aktiv software nabízí následující hodnoty:

- důvěrnost (0–3),
- integrita (0–2),
- dostupnost (0–4).

Alternativou může být automatické přidělení hodnot z procesu, ve kterém se ručně zvolí hodnoty pro důvěrnost, dostupnost a integritu s uvedenou škálou. Následně se procesy spojí s jednotlivými souvisejícími aktivy. Pokud je definováno dva a více procesů pro jedno aktivum dědí se vždy nejvyšší hodnoty z daného procesu.

Pro lepší orientaci v hodnotách aktiv software nabízí v záložce **Edit > Preferences > General Settings > Show icon overlay for risk analysis values**, možnost rozlišit aktiva s nejvyšší a nejmenší hodnotou rizika podle barev a to [20]:

- zelenou (0, 1, 2),
- žlutou (3, 4, 5),
- červenou (6, 7 8).

5.1.3 Identifikace hrozeb

Dalším krokem je identifikace a vyhodnocení relevantních hrozeb. Vstupem pro identifikaci hrozeb jsou informace o hrozbách získaných z přezkoumání incidentů, od vlastníků aktiv, uživatelů, jiných zainteresovaných osob nebo z katalogu vnějších hrozeb. V prostředí Verinice byly vytvořeny 4 skupiny hrozeb:

- **hrozby mířené na informace** – odposlech, únik dat, smazání dat, *SQL injection*, *phishing*, krádež informací, infikovaný flash disk USB (Univerzální sériová sběrnice – Universal Serial Bus), zneužití oprávnění,
- **hardwarové hrozby** – krádež zařízení, zlomení optického vlákna, zničení prvku optické sítě, prach, selhání dat na disku,
- **hrozba ztráty základních služeb** – odepření služby, narušení dodávky elektrické energie, těžká nehoda,
- **přírodní hrozby** – povodeň, zemětřesení, požár, vlhkost a mráz,
- **softwarove hrozby** – *zero–day* útok, škodlivý kód.

U každé hrozby byla stanovena pravděpodobnost vzniku. Software nabízí šest úrovní pravděpodobnosti a to:

- 0 zřídka,
- 1 každoročně,
- 2 měsíčně,
- 3 týdně,
- 4 denně,
- 5 hodinově.

Hrozby jsou taktéž rozlišeny barvami a to [20]:

- zelenou (0, 1),
- žlutou (2, 3),
- červenou (4, 5).

5.1.4 Identifikace zranitelností

Pro každé aktivum jsou zvažovány zranitelnosti a k nim příslušící hrozby. Výstupem je seznam aktiv, seznam hrozeb a zranitelností, u nichž je třeba zajistit řízení rizik. U zranitelností je třeba vyplnit úroveň. V softwaru jsou definovány čtyři úrovně [20]:

- 0 velmi nízká – využití zranitelnosti vyžaduje přímý útok, znalosti nebo dovednosti útočníka a zdroje, které nejsou běžně dostupné,
- 1 nízká – využití zranitelnosti vyžaduje přímý útok odhodlaného útočníka s vysokými znalostmi a dovednostmi,
- 2 vysoká – využitím zranitelnosti může nastat automatickým útokem, například využitím škodlivého kódu,
- 3 velmi vysoká – zranitelnost může nastat náhodně s vysokou pravděpodobností.

V softwaru byly identifikovány 4 skupiny zranitelností:

- **hardware** – nesprávně nastavené parametry, nedostatečná údržba zařízení, špatná politika bezpečnosti informací, citlivost na změny frekvence, nechráněné komunikační linky, nedostatečná ochrana optického vlákna, špatná manipulace nebo výrobní vada, nedodržení pravidelných výměn zařízení, nedostatečné postupy likvidace dat nebo zařízení, nestabilní elektrická síť,
- **software** – neznámé chyby v programech, chybné přiřazení přístupových práv, nedodržování pravidel uzamknuté obrazovky a počítače, špatný návrh zabezpečení webové stránky, nezaškolení zaměstnanci v oblasti kybernetické bezpečnosti KB, nedodržení pravidel bezpečnostní politiky,
- **lokace** – nedostatečné fyzické kontroly, pozice v záplavové oblasti, pozice na tektonickém zlomu,
- **síťové zranitelnosti** – nedostatečný návrh výměny klíčů, nestabilní elektrická síť, otevřený port 3389 RDP (Protokol vzdálené plochy – Remote Desktop Protocol).

Zranitelnosti taktéž mohou být označeny barvami a to [20]:

- zelenou (0),
- žlutou (1),
- červenou (2, 3).

5.1.5 Vytvoření scénáře

Dalším krokem je vytvoření scénáře incidentu, který se v softwaru spojí se všemi aktivy, na nichž má uvedený scénář dopad. Vstupem pro vytvoření je identifikace hrozeb, včetně ovlivněných aktiv, využitých zranitelností a dopadu na aktiva. Kromě toho by měl být vyhotoven seznam všech existujících a plánovaných opatření.

Identifikované hrozby a zranitelnosti se spojí s příslušným scénářem. V softwaru Verinice byly vytvořeny následující skupiny scénářů:

- únik přenášených dat z optických sítí,
- únik dat z databáze,
- degradace služby,
- narušení komunikace,
- nedostupnost optických sítí,
- zneužití oprávnění,
- poškození nebo zničení dat v databázi,
- zničení zařízení.

5.2 Příklad fungování softwaru Verinice

Pro pochopení celkového fungování softwaru a jeho výpočtu hodnoty rizika budou vytvořeny matice, které nejsou součástí softwaru Verinice. Na příkladu bude uveden scénář, který povede ke zničení optického kabelu.

Nejdříve se stanový hodnoty akceptace rizika, dále se identifikuje aktivum, kterým je optický kabel a primární aktivum, kterým je proces přenosu dat. Proces se ohodnotí na základě dopadu na organizaci a spojí se s aktivem. Aktivum automaticky dědí z procesu zvolené hodnoty:

- důvěrnost 3,
- dostupnost 3,
- integrita 2.

Následně se definuje scénář, k němuž se nalinkuje příslušná zranitelnost, například nechráněné komunikační linky a hrozba, například zničení optické kabelu. Kombinací pravděpodobnosti výskytu hrozby a zneužitím zranitelnosti se stanoví hodnota pravděpodobnosti vzniku scénáře. Hodnota pravděpodobnosti vzniku scénáře je automaticky generována na základě uvedených hodnot hrozeb a zranitelnosti.

Tabulka 5.1 znázorňuje hodnotu pravděpodobnosti vzniku scénáře v případě, kdy pravděpodobnost vzniku hrozby byla stanovena na hodnotu 1 a hodnota zranitelnosti na 3. V tabulce je reprezentováno i procentuální vyjádření hodnoty pravděpodobnosti. Výsledná hodnota je 4, tedy 50 % pravděpodobnost vzniku scénáře bez implementovaných opatření.

Tab. 5.1: Hodnota pravděpodobnosti vzniku scénáře

Úroveň hrozby	0				1				2				3				4				5			
Úroveň zranitelnosti	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
Pravděpodobnost	0	1	2	3	1	2	3	4	2	3	4	5	3	4	5	6	4	5	6	7	5	6	7	8
Pravděpodobnost [%]	10	20	30	40	20	30	40	50	30	40	50	60	40	50	60	70	50	60	70	80	60	70	80	90

5.2.1 Určení hodnoty rizik

Pro identifikaci hodnoty rizik v softwaru Verinice musí být propojen scénář s aktivem, na který má dopad. Hodnota rizika je založena na hodnotě dopadu a pravděpodobnosti vzniku scénáře. Software Verinice udává hodnoty rizik pro každý prvek z bezpečnostní triády zvlášť. Výsledný katalog rizik tak bude obsahovat tři matice. Pro hodnocení rizik software využívá následující funkci:

$$Riziko = dopad + pravděpodobnost$$

Na příkladu je uveden postup pro stanovení hodnoty rizik u důvěrnosti. Hodnota výsledného rizika vyplývá ze znalosti pravděpodobnosti vzniku scénáře a odhadovaného dopadu. Z příkladu, který byl uveden 5.2 byla výsledná hodnota pravděpodobnosti 4 a dopad na důvěrnost byl stanoven na hodnotu 3.

$$4 + 3 = 6$$

V tabulce 5.2 je zvýrazněna výsledná hodnota rizika 6. Výsledné riziko se měří na stupnici od (0–11) a dále je vyhodnoceno na základě stanovení kritérií akceptace rizik.

Tab. 5.2: Matice hodnoty výsledného rizika.

Dopad	0	1	2	3
Pravděpodobnost				
0	0	1	2	3
1	1	2	3	4
2	2	3	4	5
3	3	4	5	6
4	4	5	**6**	7
5	5	6	7	8
6	6	7	8	9
7	7	8	9	10
8	8	9	10	11

Tabulka 5.3 slouží pro stanovení úrovně rizika. Nízká rizika jsou pro organizaci akceptovatelná a nepotřebují dodatečné opatření. Výsledkem analýzy rizik na uvedeném příkladu byla stanovena hodnota rizika na úroveň středního rizika. Následuje tedy proces ošetření rizik, ve kterém se implementují nezbytná opatření pro snížení rizik.

Tab. 5.3: Úroveň rizika

Úroveň rizika	Hodnota rizika	Popis rizika
Nízké riziko	0–4	Riziko je akceptovatelné pro organizaci
Střední riziko	5–7	Riziko může být sníženo méně nebo více náročnými opatřeními Musí být stanoveny systematické kroky pro jeho snížení
Vysoké riziko	6–11	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění

6 Navržené scénáře

Optické sítě dnes tvoří velkou část internetové infrastruktury nabízející velké výhody, pokud jde o poskytování stabilní, rychlé a škálovatelné sítě. Mnoho poskytovatelů internetu je přímo nebo nepřímo připojeno k optické sítě. Je tomu proto, že poskytovatelé páteřních sítí investovali do technologií optických vláken, aby lépe vyhověli rostoucí poptávce po vysokorychlostním a digitálním provozu.

S rozvojem optických sítí přicházejí i nová rizika, jako například zničení optických kabelů, odposlouchávání nebo narušení signálu v procesu přenosu informací po optických vláknech. Tato rizika přinášejí značné problémy v každodenní komunikaci a je nutno je identifikovat a řídit. Navržené scénáře budou zaměřeny na datová centra (kritickou infrastrukturu) v rámci namodelovaného objektu, jehož síť je tvořena optickými vlákny. Vysokorychlostní přenos je zajištěn pomocí optických kabelů vedoucích z datového centra. Samotný optický kabel je také náchylný k útokům, proto budou navrženy scénáře a vyhodnocena rizika i pro optické kabely vedoucí mimo datové centrum. Tabulka 6.1 poskytuje stručný náhled na vytvořené scénáře a k nim příslušící příklad jedné hrozby a zranitelnosti.

Tab. 6.1: Seznam scénářů, hrozeb a zranitelností

Scénář	**Příklad zranitelnosti**	**Příklad hrozby**
Únik přenášených dat z optických sítí	Nechráněné komunikační linky, nedostatečný návrh výměny klíčů	Odposlech
– Odposlech metodou optického rozdělení	Nechráněné komunikační linky	Odposlech
– Odposlech metodou optického ohybu vlákna	Nechráněné komunikační linky	Odposlech
– Odposlech metodou V-drážky	Nechráněné komunikační linky	Odposlech
– Odposlech metodou založenou na mřížce	Nechráněné komunikační linky	Odposlech
– Odposlech skrze evanescentní vlnu	Nechráněné komunikační linky	Odposlech
– *TEMPEST* útok	Nechráněné komunikační linky	Odposlech
–> Únik dat		
Únik dat z databáze	Nezaškolený zaměstnanec v oblasti KB	*Phishing*
– *Phishing* útok	Nezaškolený zaměstnanec v oblasti KB	*Phishing*
– Spuštění škodlivého kódu	Špatná politika bezpečnosti informací	Škodlivý kód
–> Únik dat nebo zašifrování disku		
– Únik dat skrze RDP	Otevřený port 3389 RDP	Zneužití oprávnění
–> Únik dat		
– Získání dat z databáze pomocí SQL injektování	Špatný návrh zabezpečení webové stránky	SQL injektování
–> Únik dat		
Odepření služby	Nechráněné komunikační linky	Odepření služby
– Odesílání dat mimo časový úsek,	Nechráněné komunikační linky	Odepření služby
– *ARP spoofing* útok	Špatná politika bezpečnosti informací	Odepření služby
–> Odepření služby		
Narušení komunikace	Citlivost na změny frekvence	Odepření služby
– *Jamming* útok	Špatně chráněné komunikační spojení	Odepření služby
–> Narušení komunikace/odepření služby		
Nedostupnost optické sítě	Nechráněné komunikační linky	Zničení prvku optické sítě
– Fyzické zničení prvku optické sítě útočníkem,	Nechráněné komunikační linky	Zničení prvku optické sítě
–> Nedostupnost služby		
– Prasknutí optického vlákna	Nedostatečná ochrana optického vlákna	Vlhkost, mráz
–> Nedostupnost služby		
– Degradace a deformace optického vlákna,	Špatná manipulace nebo výrobní vada	Zlomení optického vlákna
–> Nedostupnost služby		
– Zničení optických prvků	Pozice na tektonickém zlomu	Zemětřesení
–> Nedostupnost služby		
– Elektrický zkrat	Nedostatečná údržba zařízení	Prach
–> Nedostupnost služby		
– Výpadek elektrické energie	Nestabilní elektrická síť	Narušení dodávky elektrické energie
–> Nedostupnost služby		
Zneužití oprávnění	Nedostatečné fyzické kontroly při vstupu do objektu	Únik dat
– Krádež zařízení	Chybějící fyzické bezpečnostní kontroly	Krádež zařízení
– Klonování disku	Chybějící fyzické bezpečnostní kontroly	Únik dat
–> Únik dat		
– Získání dat z médií	Nedostatečný postup likvidace dat nebo médií	Krádež informací
–> Únik dat		
Infikování sítě škodlivým softwarem	Nedodržení pravidel politiky bezpečnosti informací	Infikované USB zařízení
–> Únik dat		
Poškození nebo zničení dat v databázi	Špatná politika bezpečnosti informací	Selhání nebo smazání dat
– Smazání databáze	Chybné přiřazení přístupových práv	Smazání dat
– Poškození databáze	Nedodržení pravidelných výměny zařízení	Selhání dat
– Získání dat z databáze	Nedodržování pravidel uzamknuté obrazovky a počítače	Únik dat
– Objevení kritické chyby v systému	Neznámé chyby v programech	*Zero–day* útok
–> Selhání nebo smazání dat		
Zničení zařízení	Nedostatečná údržba zařízení/ špatné umístění zařízení	Zničení zařízení
– Exploze	Nesprávně nastavené parametry	Těžká nehoda
– Vytopení datového centra	Pozice v záplavové oblasti	Povodeň
– Požár	Nedostatečná údržba zařízení	Požár
–> Zničení zařízení nebo dat		

6.1 Únik přenášených dat z optických sítí

Odposlech je stará praxe a byla provedena různými způsoby. Následující sekce práce poskytne stručný popis scénářů vedoucích k odposlechu přenášených dat z optických sítí. U odposlechu obecně dochází k úniku přenášených dat, což představuje značné riziko pro organizaci. Pro odposlech lze využít různé metody:

- ohýbání vlákna,

- optické rozdělení.

Ačkoli jsou optická vlákna imunní vůči elektromagnetickému rušení a nevyzařují přenášené signály do okolí, vystavení optických sítí odposlouchávání představuje velké riziko. Cílem odposlechu obecně je získat neoprávněný přístup k datům za účelem sběru nebo analýzy provozu. V dnešní digitální éře dochází k odposlouchávání ve všech síťových vrstvách od aplikační po fyzickou vrstvu, přičemž nové útoky jsou odhaleny téměř denně.

Bylo zaznamenáno několik výskytů odposlechů v optických síti, zaměřených především na vlády, finanční, energetický, dopravní nebo farmaceutický sektor. Na základě způsobu realizace lze útoky odposlechu klasifikovat na útoky s přímým přístupem k nešifrovanému optickému kanálu a útoky založené na porušení šifrovacího klíče v šifrovaných optických systémech.

Odposlech metodou optického rozdělení

Běžným způsobem realizace útoků odposlechu je přímý přístup k optickému vláknu. Útočník připojí rozbočovač, který rozdělí vstupní optický signál do více výstupů. Útočník se pak může vrátit na místo připojené kabelem a provést odposlech. Po rozdělení vlákna rozbočovačem však dochází ke zvýšení celkového útlumu na trase v závislosti na použitém dělicím poměru [21]. V případě spojení vlákna pomocí *coupleru* nedochází k takovému útlumu signálu, jako v případě použití rozbočovače.

Scénář úniku přenášených dat pracuje s variantou optického rozdělení. Útočník rozdělí pomocí rozbočovače signál do své ONU jednotky. Při zahájení komunikace v GPON (Gigabitová pasivní optická síť – Gigabit Passive Optical Network) se musí jednotky OLT a ONU mezi sebou synchronizovat. Zranitelností v tomto scénáři jsou zprávy PLOAM (Provoz, správa a údržba fyzické vrstvy – Physical Layer Operation, Administration and Maintenance), které jsou přenášeny ve formátu prostého textu nesoucí hodnotu klíče. V případě, kdy je útočník schopen se připojit k volnému portu rozbočovače může uskutečnit útok zvaný jako MitM („Člověk uprostřed“ – Man in the Middle). Následně se může vydávat za důvěryhodnou entitu, opakovat zprávy PLOAM vedoucí k odepření služby.

Dále mohou být přenášená data útočníkem vzestupném směru odposlouchávána, pokud útočník zná hodnotu klíče, dokáže data dešifrovat [22].

Odposlech metodou optického ohybu vlákna

Útočník se přímo dostane k optickému kabelu, odstraní plášť kabelu a odizoluje jednotlivá optická vlákna. Útočník může optické vlákno ohnout například pomocí

coupleru. Následně dochází k úniku optického signálu, který může být odposlouchán. Pokud je útok úspěšně dokončen dochází k minimálnímu útlumu přenášeného signálu. Také nedochází k poškození optického vlákna a přerušení přenášeného optického signálu, jako v případě odposlechu optickým rozdělením, který by mohl být detekovatelný poplašným monitorovacím alarmem [23], [24].

Odposlech metodou V-drážky

Útočník musí mít přímý přístup k optickému kabelu. Tato metoda je založena na vyříznutí V-drážky do obalu kabelu tak, aby byla co nejblíže jádru. Úhel mezi povrchem V-drážky a optického přenášeného signálu musí být větší než kritický úhel úplného vnitřního odrazu. Pokud je tato podmínka splněna světelný signál se začne odrážet do V-drážky a uniká ven z druhé strany vlákna. Metoda řezání V-drážky je velmi náročná, vyžaduje přesné řezání a leštění optického vlákna. Výhodou je nízký útlum signálu a proto je velmi těžké detekovat takový útok vedoucí k odposlechu a úniku dat z přenášeného signálu [23].

Odposlech metodou založenou na mřížce

Použití „Braggovi“ mřížky je nejpokročilejší metodou odposlouchávání. Metoda vyžaduje použití speciálního ultrafialového laseru. Po zasvícení ultrafialovým laserem dochází k odrazu části optického signálu od „Braggovi“ mřížky do cílového optického vlákna. Tato metoda způsobuje lehký útlum, který je těžko detekovatelný a monitorovatelný [23].

Odposlech skrze evanescentní vlnu

Útočník se musí dostat až k plášti optického vlákna. Následně dostatečným leštěním pláště, dochází ke snížení odrazivosti optického signálu z jádra. Část optického signálu začne unikat a může být zachycen do cílového vlákna útočníka. Při využití této metody dochází k viditelným optickým ztrátám [25].

TEMPEST útok

Útočník musí zachytit EMR (Elektromagnetické záření – Electromagnetic radiation), které je emitované digitálními zařízeními (optickými kabely). Špatně uzemněné optické kabely mohou fungovat jako přijímač i vysílač EMR. Část vysílaných vln může unikat do okolí. Útočník pomocí aktivní směrové antény přivádí vlny do monitoru. Následně vhodnou technikou zrekonstruuje podstatnou část přenášených dat z optické sítě [26].

6.2 Únik dat z databáze

Scénář je zaměřen na hrozbu *phishingu*, následný únik dat a zašifrování databáze. Zaměstnanci přijde *phishingovi* e-mail obsahující přílohu „výplata.xlsl“, kterou otevře pomocí „Thunderbird“. „Thunderbird“ spustí „excel.exe“ proces a otevře soubor „výplata.xlsl“, který obsahuje škodlivý kód. Po navázání spojení s útočníkem pomocí povolení maker, který spustí makro kód způsobující následující akce:

- začne spouštět powershell příkazy,
- makro v sobě obsahuje zakódovanou binární aplikaci, kterou dekóduje a uloží do dočasného adresáře a nakonec ji spustí,
- makro stáhne payload z internetu a následně se uloží do dočasného adresáře.

Škodlivý kód se snaží zabezpečit si odolnost v systému a okamžitě vykonat operace potřebné k dosažení tohoto cíle. Mezi tyto operace patří například:

- skrze registry,
- skrze pokročilé techniky.

Škodlivý kód se pokouší o připojení k „C&C serveru“ a následnou komunikaci pomocí protokolu, které jsou nejméně nápadné. Často využívanými protokoly jsou například HTTPS nebo DNS, které jsou povoleny směrem ven z organizace. Cílem útočníka je přenos dat na „C&C server“ a vykonávat příkazy na napadeném systému:

Útočník může přepsat privilegia na lokálním systému a extrahovat z operačního paměti a SAM souboru hashe uživatelů. S pomocí například nástroje „Mimikatz“ útočník využívá hashe uživatelských jmen a hesel pro autentizaci do jiných systému v síti [27]. Pokud se útočníkovi podaří dostat se do systému, vykoná stejnou extrakci jako v systému předtím. Takovým způsobem může útočník pokračovat, až do doby, kdy získá potřebné údaje a rozšíří se po celé síti.

V případě, kdy útočník není schopen přepsat privilegia může procházet sdílená úložiště na síti s cílem získat konfigurační soubory, ve kterých se mohou vyskytovat přihlašovací údaje privilegovaných uživatelů.

Útočník může skenovat síť a nacházet zranitelnosti v systémech pomocí nástroje „Nmap“ [28]. Po získání dostatku dat se útočník snaží tyto zranitelnosti zneužít pro získání přístupu do systému.

Dalším způsobem je *exploitace* zranitelných služeb pro rozšíření po celé síti organizace. Po získání větší části interní sítě útočník pošle instrukce škodlivému kódu k zašifrování souborů nebo k zálohovacímu serveru.

Únik dat skrze RDP

Útočník pomocí webové stránky „Shodan“ objeví otevřený port protokolu RDP (Protokol vzdálené plochy – Remote Desktop Protocol) 3389 na serveru nebo pomocí skenovacího nástroje „Nmap“. Pomocí „Shodan“ může útočník zjistit operační systém, veřejné klíče certifikátů, polohu zařízení a mnoho dalších informací [29], [30].

Následně útočník hledá zranitelnosti, pro průnik do systému. Takovou zranitelností může být například BlueKeep, která umožňuje vzdáleně spouštět škodlivý kód útočníka na starších neaktualizovaných operačních systémech. Pokud se útočníkovi nepodaří nalézt zranitelnost v systému, pokusí se získat pomocí slovníkového útoku přístup na server RDP. Útok může být cílen na administrátora nebo na konkrétního uživatele [31].

Po získání všech potřebných informací, jako heslo, IP (Adresa internetového protokolu – Internet Protocol address) adresa, uživatelské jméno se útočník může pomocí RDP vzdáleně připojí do systému. Následně dochází k podobnému scénáři popsaném v 6.2. Útočník může nasadit do systému škodlivý kód, získat data, mazat data atd.

Získání dat z databáze pomocí SQL injektování

Scénář je zaměřen na hrozbu SQL (Strukturovaný dotazovací jazyk - Structured Query Language) injection. Programátor nedostatečně zabezpečil stránku před spuštěním cizího kódu. V některých situacích může útočník eskalovat SQL injection útok, aby ohrozil základní server nebo jinou infrastrukturu typu *back-end* nebo provedl útok odmítnutí služby.

Útočník na místo vstupu, který od něj požaduje webová stránka vloží škodlivý kód. Na místo uživatelského ID (Identifikace – Identification) se využije kód pro databázi SQL, jako například:

- uživatelské jméno: 6 OR 1=1

Při nezabezpečené webové stránce se vrátí útočníkovi uživatelské ID, jméno nebo heslo. Následně může útočník získat uživatelská jména, hesla nebo jiná data, která jsou v tabulce databáze.

6.3 Degradace služby

PON (Pasivní optická síť – Passive Optical Network) pro přenos dat využívá TDMA (Časový multiplex s vícenásobným přístupem – Time Division Multiple Access) pro umožnění sdílení vzestupného kanálu. Každá jednotka ONU v sítí má přidělený

přesný a nepřekrývající se časový interval pro odesílaní dat. Časový interval je přidělen staticky nebo dynamicky na základě vytížení sítě pomocí jednotky OLT. Tímto způsobe je zaručeno, že nedojde ke kolizi přenášených dat [32].

Předpokladem k realizaci scénáře je zapojení útočníkovy ONU jednotky přes rozbočovač. Útočník nemusí dodržovat ujednaná pravidla a následně začne odesílat data mimo časový úsek, čímž může dojít k degradaci služby [32].

Zahlcení rozbočovače

V některých případech mohou útočníci také použít spoofing ARP (Protokol rozlišení adresy – Address Resolution Protocol), ve kterém kus softwaru odešle rozbočovači mimořádně velký počet MAC (Řízení přístupu na médium – Medium Access Control) adres. To přetíží tabulku ARP starších nebo levných rozbočovačů a zakáže vyhrazené směrování na konkrétní porty.

6.4 Narušení komunikace

Scénář se zaměřuje na hrozbu *jammingu*, který povede k narušení komunikace v optických sítích. Útočník rozdělí pomocí rozbočovače optický signál. Následně realizuje útok pomocí vložení optického signálu s nadměrným výkonem do sítě. Rušivé signály musí být na stejné vlnové délce, jako legitimní signály uživatelů. V PON, ve kterých je přidán OADM můžou vysoce výkonné signály poškodit koexistenci uživatelských signálů uvnitř optických vláken.

Na EDFA (Vláknový erbiem dopovaný zesilovač - Erbium Doped Fiber Amplifier) může rušivý signál mimo jeho pracovní rozsah způsobit konkurenční zesílení. Slabší legitimní signály jsou okradeny o zisk, který získá rušivý signál. Předpokladem je, že na trase nebudou optické zeslabovače [21].

6.5 Nedostupnost optické sítě

Uvedené scénáře povedou ke ztrátě dostupnosti optické sítě. Nejspíš jeden z nejjednodušších útoků je přeřezání optických vláken. Tento útok nevyžaduje žádné vyšší znalosti, jako například při útoku ohýbáním vláken nebo optického rozdělení signálu rozbočovačem. Útočník se musí dostat k optickému kabelu, který následně zničí nebo může poškodit optická vlákna.

Nedávný útok na optické kabely přerušil přístup k internetu v částech východní Evropy, Íránu a Turecka. Problém, který trval nejméně dvě hodiny byl způsoben fyzickým poškozením více optických vláken současně, což byla velmi neobvyklá věc.

„Google“ uvedl, že jeho služby byly nedostupné v uvedených regionech po dobu třiceti minut [33].

Prasknutí optického vlákna

Nejenom fyzické poškození optických vláken může způsobit zničení zařízení a následný výpadek služby. Scénář prasknutí vláken je zaměřen na riziko plynoucí z přírodních vlivů.

V tomto scénáři může být zranitelností nedostatečná ochrana optického vlákna před vlhkostí. V zimních měsících může dojít k zamrznutí optického vlákna, které následně může prasknout [34].

Degradace a deformace optického vlákna

Nadměrným ohybem optického vlákna (kabelu), může docházet ke zvyšování optických ztrát. Následně mohou vzniknout optické trhliny. Tyto trhliny v optických vláknech mohou způsobit zlomení vlákna a tím jeho degradaci.

Deformace optického vlákna může být zapříčiněna jeho kroucením, ohybem, napětím, manipulací apod. Deformace optických vláken vede ke zvyšování optických ztrát [34].

Elektrický zkrat

Zaprášené zařízení a nedostatečná pravidelná údržba může zapříčinit zkrat v zařízení a následně může dojít i k jeho zničení.

Výpadek elektrické energie

Rizik souvisejících s výpadkem elektrické energie může být hned několik a měla by být brána v úvahu. V práci je uvedeno riziko narušení dodávky elektrické energie ze strany dodavatele, avšak existují i další rizika související s kybernetickými útoky, terorismem, přírodními vlivy apod.

6.6 Zneužití oprávnění

Scénář je zaměřen na hrozbu odcizení zařízení a následný únik dat z databáze. Zaměstnanci je odcizena čipová karta pro vstup do data centra. Útočník vnikne do nechráněného objektu a odcizí zařízení nebo použije techniku otisku disku na zkopírování dat ze serveru. Útočník má vlastní notebook, který připojí do serveru. Po zadání příkazu 6.1 v příkazové řádce se spustí kopírování souboru ze serveru na cílový notebook útočníka:

Výpis 6.1: Příkaz na vytvoření otisku disku

```
# dd if=/dev/sda of=/dev/sdb status=progress
```

Krádež a kopírování dat ze zařízení může být provedena i zaměstnancem nebo třetí stranou, poskytující službu pro organizaci. Příkladem může být firma, která provádí pravidelný úklid datového centra.

Získání dat z médií

Pouhé smazání souboru nebo operačního systému z nosiče dat nezaručuje kompletní likvidaci dat. V případě vyřazení nosičů dat musí být fyzicky zlikvidován, aby nedošlo k zneužití dat útočníkem. Pokud má útočník přímý přístup k nosiči dat, lze na jeho obnovu využít nejrůznější softwary.

V rámci systému řízení bezpečnosti informací musí být u řízení aktiv stanoven i způsob likvidace dat, provozních údajů, informací a jejich kopií. Dále by mělo být definováno, kde a kdo bude likvidaci provádět, časová náročnost likvidace, dostupnost zařízení na likvidaci dat apod. Vyhláška také definuje tři způsoby likvidace nosičů z nichž nejbezpečnější je fyzická likvidace nosičů dat [2].

Infikování sítě škodlivým softwarem

Velmi jednoduchý a známý scénář je napadení interní sítě pomocí infikovaného USB (Univerzální sériová sběrnice – Universal Serial Bus) zařízení škodlivým kódem. Na jedné straně scénáře stojí zaměstnanec firmy a na straně druhé útočník s infikovaným USB zařízením. Útočník zanechá USB zařízení na místě, kde může být nalezeno zaměstnancem. Zaměstnanec pokud je nedbalý a nedodržuje bezpečnostní politiku organizace zapojí infikované USB zařízení do portu firemního počítače. Následně se spustí škodlivý kód, který umožňuje vzdálené připojení k síti. Může nastat podobný scénář popsaný v 6.2.

6.7 Poškození nebo smazání databáze

Scénář poškození databáze způsobuje mnoho různých hardwarových nebo softwarových vad. Poškození databáze může být způsobena vadným diskem, řadičem, chybným převrácením bitů na disku nebo chybou v operačním systému. Rizikem může být selhání dat nebo poškození dat [35].

Scénář smazání databáze se opírá o chybné přiřazení přístupových práv administrátora na server. Administrátor v tomto případě dostane přístupová práva na testovací server, kde měl smazat celou databázi příkazem 6.2:

Výpis 6.2: Příkaz na vymazání dat

```
# rm -rf
```

Chybným přiřazením přístupových práv však dostal práva na produkční server obsahující uložená data a celou databázi smazal.

Odlišný scénář je zaměřen na útočníka, který má přístup k neuzamčenému monitoru počítače zaměstnance. Následně může provést smazání databáze nebo kopírování disku popsaném v 6.6.

Objevení kritické chyby v systému

Scénář se opírá o *zero–day* útok. Útočník se snaží využít programátorské chyby v softwaru, pokud se mu podaří chybu odhalit, uživatel je nechráněn, až do vydání aktualizace. Rizik plynoucích z toho scénáře bude několik, záleží na objevené zranitelnosti a systému.

Exploze

Scénář exploze může vyvolat technické selhání zařízení z důvodů špatně nastavených parametrů.

Poškození zařízení vlivem přírodních katastrof

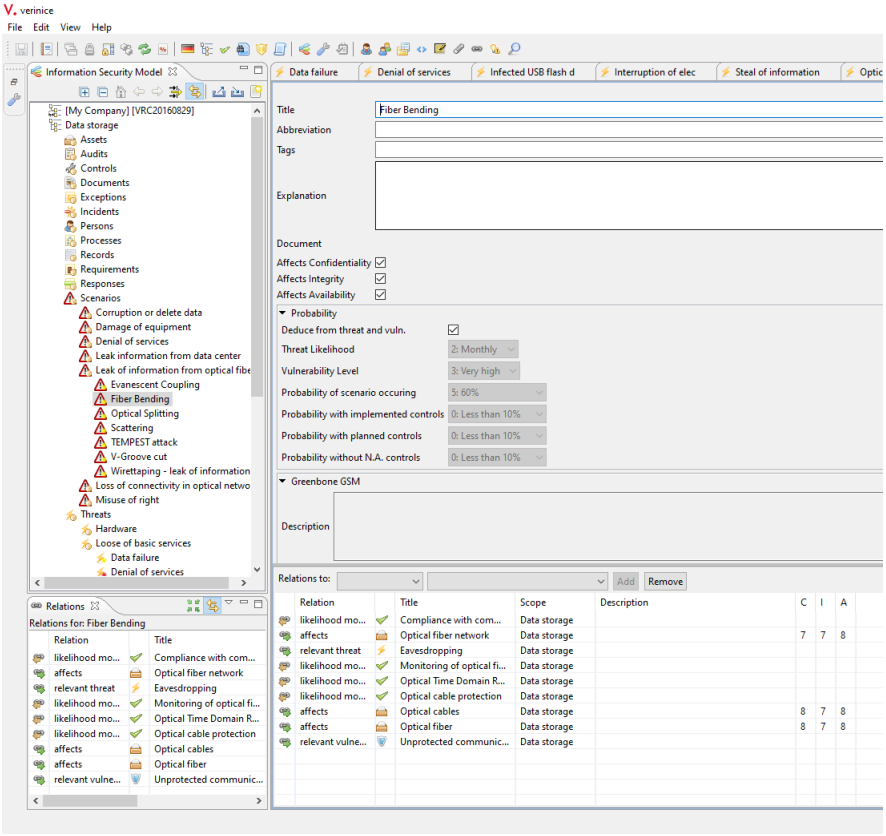
Scénář se opírá a rizika plynoucích z přírodních katastrof jako je povodeň, zemětřesení a požár.

6.8 Opatření pro snížení rizik

Po hodnocení rizik následuje ošetření rizik. U rizik středních a vysokých budou implementována opatření. Každý scénář v softwaru Verinice je spojen s kontrolou. Tabulka 6.2 poskytuje přehled implementovaných opatření u skupin scénářů. Detailní pohled na zavedené opatření k jednotlivým scénářům je možné vidět v příloze A. Opatření vycházejí z požadavků normy ISO/IEC 27001 a dodatečných specifických bezpečnostních opatření, vedoucích ke snížení rizik.

Obrázek 6.1 ukazuje prostředí softwaru Verinice a vytvořený scénář vedoucí k úniku přenášených dat z optických sítí. Konkrétně je vidět scénář na ohyb optického vlákna. V pravé liště je uvedena hodnota pravděpodobnosti vzniku hrozby 2, hodnota zranitelnosti 3 a kombinaci těchto hodnot pravděpodobnost vzniku scénáře 5, tedy 60%. Dále pravděpodobnost vzniku scénáře po zavedení vhodných opatření

na daný scénář. Ve spodní liště je ukázka vztahů k aktivum a jejich hodnoty rizik, zavedené opatření, příslušná hrozba a zranitelnost.



Obr. 6.1: Ukázka prostředí softwaru Verinice

Tab. 6.2: Souhrn scénářů a implementovaných opatření [3].

Scénář	**Navržené opatření**
Únik přenášených dat z optických sítí	1. Ochrana optických kabelů, vláken a aktivních síťových prvků, 2. kryptografická ochrana QKD (Kvantové rozdělení klíčů – Quantum key distribution), 3. OTDR (Optická reflektometrie v časové oblasti – Optical Time DomainReflectometry), 4. systém sběru síťových dat a detekce anomálií, 5. whitelisting zařízení, 6. záznamy dat – zaznamenávání událostí formou logů, ochrana logů 7. dodržování komunikačních standardu a protokolu (IPsec, atd.), 8. bezpečnostní politika, 9. školení, povědomí a vzdělání v oblasti bezpečnosti informací, 10. odpovědnosti, postupy a hlášení bezpečnostních incidentů, 11. hlášení slabých míst v systému, 12. monitorování optické sítě, vláken a aktivních prvku, 13. VPN (Virtuální privátní síť – Virtual private network).

Únik dat z databáze	1. Pravidelná aktualizace softwaru, 2. omezení instalace softwaru, 3. antivirový software, 4. bezpečnostní politika, 5. systém sběru síťových dat a detekce anomálií, 6. školení, povědomí a vzdělání v oblasti bezpečnosti informací, 7. záznamy dat – zaznamenávání událostí formou logů, ochrana logů, 8. odpovědnosti, postupy a hlášení bezpečnostních incidentů, 9. hlášení slabých míst v systému, 10. penetrační testování – testování bezpečnosti systému, 11. anti–spam, 12. automatická kontrola příloh e–mailu, 13. disciplinární řízení v případě, kdy se zaměstnanec dopustí narušení bezpečnosti informací. 14. VPN, 15. zakázat RDP z veřejné sítě, 16. zásady blokování účtu, 16. politika hesel.
Odepření služby	1. Ochrana optických kabelů a vláken, 2. kryptografická ochrana, 3. OTDR, 4. systém sběru síťových dat a detekce anomálií, 5. whitelisting zařízení, 6. školení, povědomí a vzdělání v oblasti bezpečnosti informací, 7. odpovědnosti, postupy a hlášení bezpečnostních incidentů, 8. vyrovnávání zatížení sítě – *load balancing*, 9. RWA (Směrování a přiřazení vlnové délky – Routing and wavelength assignment), 10. robustnost sítě, 11. kontrola aktivních síťových prvků – monitorování, 12. systém sběru síťových dat a detekce anomálií, 13. speciální techniky strojového učení – ANN (Umělá neuronová síť – Artificial neural networks), 14. bezpečnostní politika, 15. OSA (Optická spektrální analýza – Optical Spectral Analysis Methods).

Nedostupnost optické sítě	1. RWA, 2. robustnost sítě, 3. systém sběru síťových dat a detekce anomálií, 4. bezpečnostní politika, 5. dohody s dodavateli poskytující službu nebo produkt informačních a komunikačních technologií. Dohody musí zahrnovat požadavky na rizika bezpečnosti informací, 6. podpůrné služby – záložní zdroje elektrické energie, 7. monitorování a přezkoumání služeb dodavatelů, 8. pravidelné monitorování síťových prvků, 9. fyzické bezpečnostní periferie – kamerový systém, alarmy, oplocení, fyzické kontroly při vstupu do objektu, 10. OFDR (Optická reflektometrie ve frekvenční oblasti – Optical Frequency Domain Reflectometry), 11. ochranné obaly proti vlhkosti, 12. plnící materiály v optických kabelech (gel), 13. umístění zařízení – zařízení by mělo být umístěno tak, aby se snížila rizika hrozeb daná prostředím, 14. údržba zařízení, 15. odpovědnosti, postupy a hlášení bezpečnostních incidentů, 16. záloha dat, 17. vyrovnávání zatížení sítě – *load balancing*, 18. ochrana optických kabelů a vláken, 19. kontrola aktivních síťových prvků – monitorování, 20. umístění zařízení a jeho ochrana – zařízení by mělo být umístěno na bezpečném místě, aby se snížila rizika poškození zařízení, 21. záložní zdroj elektrické energie.
Zneužití oprávnění	1. Šifrování disku, 2. školení, povědomí a vzdělání v oblasti bezpečnosti informací, 3. bezpečnostní politika, 4. fyzické bezpečnostní periferie – kamerový systém, alarmy, oplocení, fyzické kontroly při vstupu do objektu, 5. bezpečná likvidace zařízení nebo dat: (a) síťová zařízení a magnetická zařízení – rozebrání zařízení a zničení nosiče informací, (b) cloud computing – přepsání dat, 6. zabezpečení místností – systém kontroly přístupu (čtečky karet, identifikační karty zaměstnanců), 7. přezkoumání přístupových práv uživatelů, 8. odebrání přístupových práv pří ukončení pracovního poměru nebo úprava přístupových práv, 9. omezení přístupu k informacím – přidělení přístupových práv do systému, 10. autentizace a autorizace při vstupu do prostor, 11. záznamy dat – zaznamenávání událostí formou logů, ochrana logů, 12. disciplinární řízení v případě, kdy se zaměstnanec dopustí narušení bezpečnosti informací, 13. odpovědnosti, postupy a hlášení bezpečnostních incidentů, 14. hlášení slabých míst v systému, 15. zakázání USB portu, 16. záloha dat, 17. omezení instalace softwaru, 18. antivirový software.

Poškození nebo zničení databáze	1. Záloha dat, 2. školení, povědomí a vzdělání v oblasti bezpečnosti informací, 3. bezpečnostní politika, 3. řízení přístupu – k serveru nebo zdrojovým kódům programu, 4. přezkoumání přístupových práv uživatelů, 5. odebrání přístupových práv pří ukončení pracovního poměru nebo úprava přístupových práv, 6. správa uživatelských přístupu – přidělování a odebírání přístupových práv, 7. odpovědnosti, postupy a hlášení bezpečnostních incidentů, 8. hlášení slabých míst v systému, 9. záznamy dat – zaznamenávání událostí formou logů, ochrana logů, 10. dodržování komunikačních standardu a protokolu (NIST), 12. autentizace a autorizace uživatele, 13. správa hesel pro přístup do systému, 14. zabezpečení místností – systém kontroly přístupu (čtečky karet, identifikační karty zaměstnanců), 15. zásada prázdného stolu a uzamčené obrazovky monitoru, 16. fyzické bezpečnostní periferie – kamerový systém, alarmy, oplocení, fyzické kontroly při vstupu do objektu, 17. šifrování disku.
Zničení zařízení	1. Hasicí přístroje – halogenové, 2. pravidelná kontrola nastavených parametrů, 3. údržba zařízení, 4. umístění zařízení a jeho ochrana – zařízení by mělo být umístěno na bezpečném místě, aby se snížila rizika poškození zařízení, 5. odpovědnosti, postupy a hlášení bezpečnostních incidentů.

6.9 Katalog rizik

Výstupem ze softwaru Verinice je katalog rizik obsahující výsledky identifikovaných a posouzených rizik. První část katalogu obsahuje zvolené hodnoty akceptace rizik u důvěrnosti, integrity a dostupnosti. V další části katalogu jsou grafy s identifikovanými riziky. Celkem bylo identifikováno 277 rizik, z nichž největší zastoupení mají rizika mírná, dále následují rizika vysoká a nízká. Podstatná část katalogu zahrnuje hodnocení rizik bez implementovaných kontrol u vytvořených scénářů. Tento ucelený přehled poskytuje nejrizikovější scénáře, u nichž je třeba implementovat opatření na snížení rizik.

Dále katalog obsahuje tabulku „Assets with Hight Risk“, znázorňující skóre pro jednotlivá aktiva. Nalezení skóre pro aktivum se skládá z následujících kroků:

- nejprve se stanový hodnota pravděpodobnosti scénáře, která je stanovena kombinací pravděpodobnosti vzniku hrozby a zranitelnosti, viz. tabulka 5.1,
- následně se stanový hodnota rizika nalezením průsečíku hodnoty pravděpodobnosti a dopadu na organizaci, viz. tabulka 5.2,

- jednotlivá skóre se sečtou a výsledkem je celkové skóre aktiva. Tento princip je důležitý pro rozlišování aktiv, kterým by měla být přidělena priorita,
- nejvyšší celkové skóre bylo vypočítáno u optické sítě s hodnotou 15 a dále u přenášených dat s hodnotou 12. Zmíněné hodnoty a další vypočítaná skóre u jednotlivých aktiv jsou uvedeny v příloze B.

Souhrn automatických výpočtů a následné generování katalogu rizik umožňuje přehledný výstup hodnocených rizik, u kterých je nezbytné implementovat opatření.

Závěr

S rostoucím rozvojem technologií se objevují stále nová rizika, která je nutno identifikovat a řídit tak, aby bylo dosaženo zachování důvěrnosti, integrity a dostupnosti informací. Organizace a orgány implementují pro tuto potřebu systém řízení bezpečnosti informací. Implementace systému řízení bezpečnosti informací poskytuje jistotu zainteresovaným stranám a samotné organizaci, že jsou rizika přiměřeně řízena. Pokud osoba nebo orgán splňuje kritéria pro určení prvků kritické infrastruktury nebo kritické informační infrastruktury musí mít zaveden systém řízení rizik bezpečnosti informací.

Diplomová práce se zaměřovala na problematiku kybernetické bezpečnosti, souvisejících pojmů, legislativních dokumentů a definic. V rámci práce byla vysvětlena kritická infrastruktura, která je základem využívajícím prvky kritické informační infrastruktury. Dále byly popsány povinnosti subjektů kritické infrastruktury a proces určování prvku kritické informační infrastruktury, kde byla definována kritéria pro určení těchto prvků.

Detailně byl popsán proces řízení rizik bezpečnosti informací, dle normy ISO/IEC 27005, který byl následně realizován v prostředí softwaru Verinice. V Kapitole 5.2 bylo vysvětleno fungování softwaru Verinice s využitím matice rizik. Na jednom scénáři byl vysvětlen celý proces řízení rizik softwaru Verinice. Tato kapitola sloužila k pochopení výpočtů a následného stanovení hodnoty rizika ve výsledném katalogu rizik.

Cílem práce bylo identifikovat aktiva, hrozby, zranitelnosti, procesy a scénáře pro kritickou infrastrukturu a kritickou informační infrastrukturu. Ke scénářům incidentu byla identifikována příslušná hrozba, zranitelnost a dopad na identifikovaná aktiva. Scénáře byly vytvořeny především za účelem popsání incidentu odposlechu a úniku přenášených dat z optických sítí a kritické infrastruktury. V rámci procesu řízení rizik bylo identifikováno celkem 277 rizik, z nichž největší zastoupení měla rizika mírná, dále následovala rizika vysoká a nízká. Aktivum, které dosáhlo celkově nejvyššího skóre rizika byla optická síť s hodnotou 15 identifikovaných hodnot rizik s vysokou úrovní.

Na základě výstupu ze softwaru Verinice byla implementována příslušná opatření pro snížení rizik na základě požadavků ISO/IEC 27001. Výstupem ze softwaru Verinice je katalog rizik ve formátu .VNA obsahující výsledky identifikovaných a posouzených rizik.

Literatura

[1] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0. Dostupné z URL: <https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2193-vykladovy-slovnik-kyberneticke-bezpecnosti-druhe-vydani/>

[2] *Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).* In: Sbírka zákonů. Praha: Aleš Čeněk, 2018, ročník 2018, číslo 82.

[3] *ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.* Praha: Úřad pro technickou normalizaci, meteorologii a státní zkušebnictví, 2014.

[4] POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.

[5] DVOŘÁČEK, JIří. *Audit podniku a jeho operací.* 1. Praha: C H Beck, 2005. ISBN 8071798096.

[6] *ENISA overwiew of cybersecurity and related terminology* [online]. 2017, **1**, 1-8 [cit. 2019-12-20]. Dostupné z URL: <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology>

[7] Cybersecurity. *Lexico* [online]. Oxford Dictionaries, 2019 [cit. 2019-12-20]. Dostupné z URL: <https://www.lexico.com/definition/cybersecurity>

[8] Cybersecurit. *Merriam-webster* [online]. 2019 [cit. 2019-12-20]. Dostupné z URL: <https://www.merriam-webster.com/dictionary/cybersecurity>

[9] ZÁKON o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky.* 2014, číslo 181. Dostupné také z URL: <https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/>

[10] *The basic of information security* [online]. USA: Elsevier, 2011 [cit. 2019-12-20]. ISBN 978-1-59749-653-7. Dostupné z URL: <https://books.google.cz/books?id=E3jTrBwpWPoC&pg=PA6&dq=CIA+triad&hl=en&sa=X&ved=0ahUKEwjwg7X7yabmAhVRfMAKHes4AIcQ6AEIKDAA#v=onepage&q=CIA%20triad&f=false>

[11] *CyberSecurity* [online]. Praha: CZ.NIC, z. s. p. o, 2019 [cit. 2019-12-20]. ISBN 978-80-88168-34-8. Dostupné z URL: <https://knihy.nic.cz/files/edice/cybersecurity.pdf>

[12] *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii*. Brusel: Úřední věstník Evropské unie, 2016, ročník 2016, číslo 1148. Dostupné z URL: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016L1148#document1>

[13] CSIRTs Network. *Enisa* [online]. [cit. 2019-12-20]. Dostupné z URL: <https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network>

[14] Zákon o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Sbírka zákonů*. PRAHA, 2000, ročník 2000, číslo 240. Dostupné z URL: <https://www.zakony.cz/zakon-SB2000240>

[15] *Nařízení vlády o kritériích pro určení prvku kritické infrastruktury*. In: Sbírka zákonů. ročník 2010, číslo 432. Dostupné z URL: <https://www.govcert.cz/download/kii-vis/urc_kriteria_KII.pdf>

[16] Ochrana kritické infrastruktury. *Mvcr* [online]. 2019 [cit. 2019-12-20]. Dostupné z URL: <https://www.mvcr.cz/cthh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx>

[17] *ČSN ISO 31000 Management rizik - Princypy a směrnice*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

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

[19] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4. Praha: Grada Publishing, 2013. ISBN 978-80-247-4644-9.

[20] *Verinice. User Guide 1.19*. SerNet, 2019. Dostupné z URL: <https://github.com/SerNet/verinice/tree/master/doc/manual>

[21] FURDEK, Marija, Nina SKORIN-KAPOV, Szilard ZSIGMOND a Lena WOSINSKA. Vulnerabilities and security issues in optical networks. In: *International Conference on Transparent Optical Networks (ICTON)* [online]. Graz, Austria: IEEE, 2014, s. 1-4 [cit. 2020-05-23]. DOI: 10.1109/ICTON.2014.6876451. ISBN 978-1-4799-5601-2. ISSN 2161-2064. Dostupné z URL: <https://ieeexplore.ieee.org/document/6876451>

[22] HORVATH, Tomas, Lukas MALINA a Petr MUNSTER. On Security in Gigabit Passive Optical Networks. In: *International Workshop on Fiber Optics in Access Network (FOAN)* [online]. Brno, 2015, s. 51-55 [cit. 2020-05-23]. DOI: 10.1109/FOAN.2015.7320479. ISBN 978-1-4673- 7625-9. ISSN 2378-847X. Dostupné z URL: <https://ieeexplore.ieee.org/document/7320479>

[23] SHANEMAN, K. a S. GRAY. *Optical network security: technical analysis of fiber tapping mechanisms and methods for detection & prevention* [online]. 2004 [cit. 2020-05-25]. Dostupné z URL: <https://ieeexplore.ieee.org/document/1494884>

[24] GOMEZ, Paulina. How To Hack an Optical Fiber in Minutes- And How You Can Secure It. *Ciena* [online]. 2016 [cit. 2020-05-27]. Dostupné z URL: <https://www.ciena.com/insights/articles/How-to-hack-an-optical-fiber-in-minutes-and-how-you-can-secure-it.html>

[25] IQBAL, Zafar M. a H. FATHALLAH. *Optical fiber tapping: Methods and precautions* [online]. 2011 [cit. 2020-05-27]. DOI: 10.1109/HONET.2011.6149809. Dostupné z URL: <https://www.researchgate.net/publication/254050694_Optical_fiber_tapping_Methods_and_precautions

[26] GOODMAN, Cassi. An Introduction to TEMPEST. In: *SANS* [online]. National Communications Security Committee Directive 4 sets U.S. TEMPEST standards, 2001 [cit. 2020-05-28]. Dostupné z: <hhttps://www.sans.org/reading-room/whitepapers/privacy/paper/981>

[27] WHAT IS PASS THE HASH? *Stealthbits* [online]. [cit. 2020-05-26]. Dostupné z URL: <https://attack.stealthbits.com/pass-the-hash-attack-explained/>

[28] Nmap. *Nmap* [online]. [cit. 2020-05-26]. Dostupné z URL: <https://nmap.org/>

[29] *Shodan* [online]. [cit. 2020-05-31]. Dostupné z URL: <https://www.shodan.io/>

[30] ALBATAINEH, Areej a Izzat ALSMADI. IoT and the Risk of Internet Exposure: Risk Assessment Using Shodan Queries. *IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)* [online]. 2019 [cit. 2020-05-31]. Dostupné z URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8792986>

[31] Windows BlueKeep Vulnerability: Deja Vu Again With RDP Security Weaknesses. *Varonis* [online]. [cit. 2020-05-31]. Dostupné z URL: <https://www.varonis.com/blog/windows-bluekeep-vulnerability-\deja-vu-again-with-rdp-security-weaknesses/>

[32] ATAN, F.M., A.M ZIN, N.A. ISMAIL, N. ZULKIFLI a S. M. IDRUS. An Overview on Security Issues in The Optical Access Network. In: *IEEE 7th International Conference on Photonics (ICP)* [online]. Kuah, Malaysia, 2018, s. 1-3 [cit. 2020-05-23]. DOI: 10.1109/ICP.2018.8533171. ISBN 978-1-5386-1187-6. ISSN 2330-5665. Dostupné z URL: <https://ieeexplore.ieee.org/document/8533171>

[33] Google goes offline after fibre cables cut. In: *BBC NEWS* [online]. London: BBC, 2019 [cit. 2019-12-21]. Dostupné z URL: <https://www.bbc.com/news/technology-50851420>

[34] FILKA, Miloslav. *Optické sítě - přednášky*. FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ, 2007. Dostupné z URL: <https://optolab.utko.feec.vutbr.cz/wp-content/uploads/Opticke_site_prednasky_P.pdf>

[35] Preventing, Detecting, and Repairing Block Corruption: Oracle Database 12c. In: *Oracle Maximum Availability Architecture White Paper* [online]. ORACLE, 2014 [cit. 2020-05-24]. Dostupné z URL: <https://www.oracle.com/technetwork/database/availability/corruption-bestpractices-12c-2141348.pdf>

Seznam symbolů, veličin a zkratek

ANN	Umělá neuronová síť – Artificial neural networks
ARP	Protokol rozlišení adresy – Address Resolution Protocol
CERT	Skupina pro reakci na počítačové hrozby – Computer Emergency Response Team
CSIRT	Skupina pro reakce na počítačové bezpečnostní incident – Computer security incident response team
CWDM	Hrubý vlnový multiplex – Coarse Wavelength Division Multiplex
DoS	Odepření služby – Denial of Service
DWDM	Hustý vlnový multiplex – Dense Wavelength Division Multiplex
EDFA	Vláknový erbiem dopovaný zesilovač – Erbium Doped Fiber Amplifier
EMR	Elektromagnetické záření – Electromagnetic radiation
ENISA	Evropská agentura pro bezpečnost sítí a informací – The European Union Agency for Network and Information Security
EU	Evropská unie – European union
GPON	Gigabitová pasivní optická síť – Gigabit Passive Optical Network
ID	Identifikace – Identification
IP	Adresa internetového protokolu – Internet Protocol address
ISMS	Systém řízení bezpečnosti informací – Information security management system
KB	Kybernetická bezpečnost – Cyber security
KI	Kritická infrastruktura – Critical infrastructure
KII	Kritická informační infrastruktura – Critical information infrastructure
MAC	Řízení přístupu na médium – Medium Access Control
MitM	„Člověk uprostřed“ – Man in the Middle
NIS	SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii – DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
OADM	Pasivní optický Add/drop multiplexer – Optical Add Drop Multiplexor
OFDR	Optická reflektometrie ve frekvenční oblasti – Optical Frequency Domain Reflectometry

OLT	Optické linkové zakončení – Optical Link Termination
ONU	Optická síťová jednotka – Optical Network Unit
OTDR	Optická reflektometrie v časové oblasti – Optical Time Domain Reflectometry
PLOAM	Provoz, správa a údržba fyzické vrstvy – Physical Layer Operation, Administration and Maintenance
PON	Pasivní optická síť – Passive Optical Network
RDP	Protokol vzdálené plochy – Remote Desktop Protocol
RWA	Směrování a přiřazení vlnové délky – Routing and wavelength assignment
TDMA	Časový multiplex s vícenásobným přístupem – Time Division Multiple Access
OSA	Optická spektrální analýza – Optical Spectral Analysis Methods
QKD	Kvantová distribuce klíčů – Quantum key distribution
SOA	Polovodičový zesilovač – Semiconductor Optical Amplifier
SQL	Strukturovaný dotazovací jazyk – Structured Query Language
USB	Univerzální sériová sběrnice – Universal Serial Bus
VoKB	Vyhlášky č. 82/2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
VPN	Virtuální privátní síť – Virtual private network
ZoKB	Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Seznam příloh

A Obsah přiloženého CD

V přiloženém CD se nachází exportovaný projekt ze softwaru Verinice ve formátu .VNA a elektronická verze diplomové práce.

B Katalog rizik

Příloha B obsahuje vygenerovaný katalog rizik ze softwaru Verinice.

IS Risk Assessment

SerNet verinice.

Scope / Client: Data storage

Date: 1 June 2020

Risk Assessment

Risk Acceptance Criteria

Category	Tolerable risk level
Confidentiality	7
Integrity	6
Availability	6

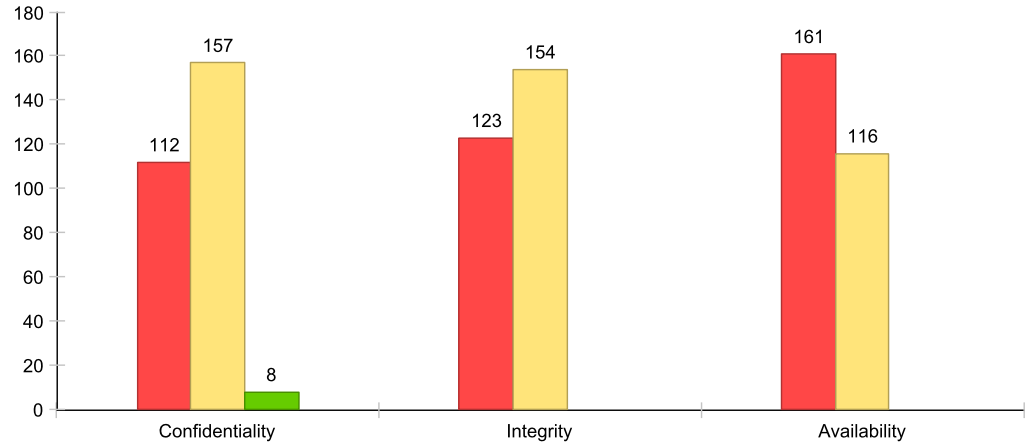
The following risk assessment was performed as detailed in the approved risk assessment method and is in accordance with international standard ISO / IEC 27005.
Risk acceptance criteria shown on the left are defined in the risk assessment policy and approved by senior management.

Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Integrity: property of protecting the accuracy and completeness of assets
Availability: property of information being accessible and usable upon demand by an authorized entity
(ISO/IEC 27000:2009)

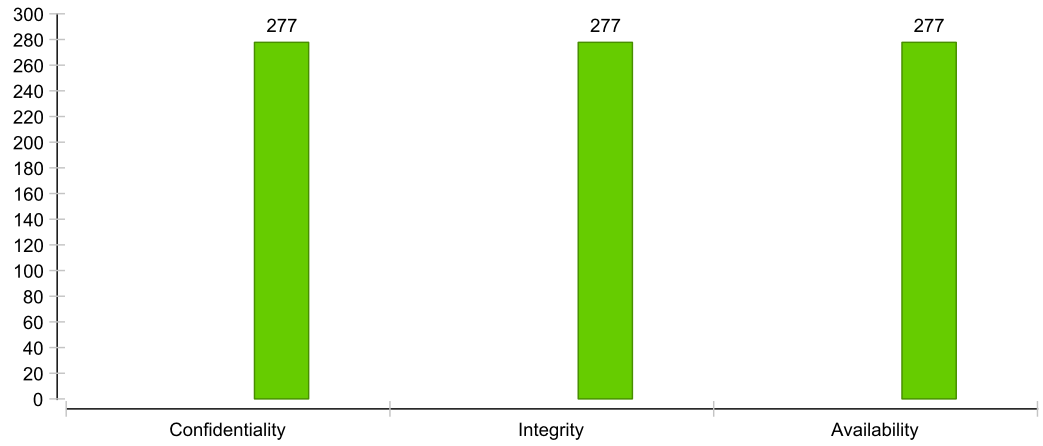
Risk Classification

RED: The risk exceeds the risk acceptance criteria and must be addressed according to the risk assessment policy.
YELLOW: The risk falls just under the risk acceptance criteria. It may need to be addressed according to the risk assessment policy.
GREEN: The risk falls within risk acceptance criteria.

Identified Risks



Remaining Risks with implemented Controls



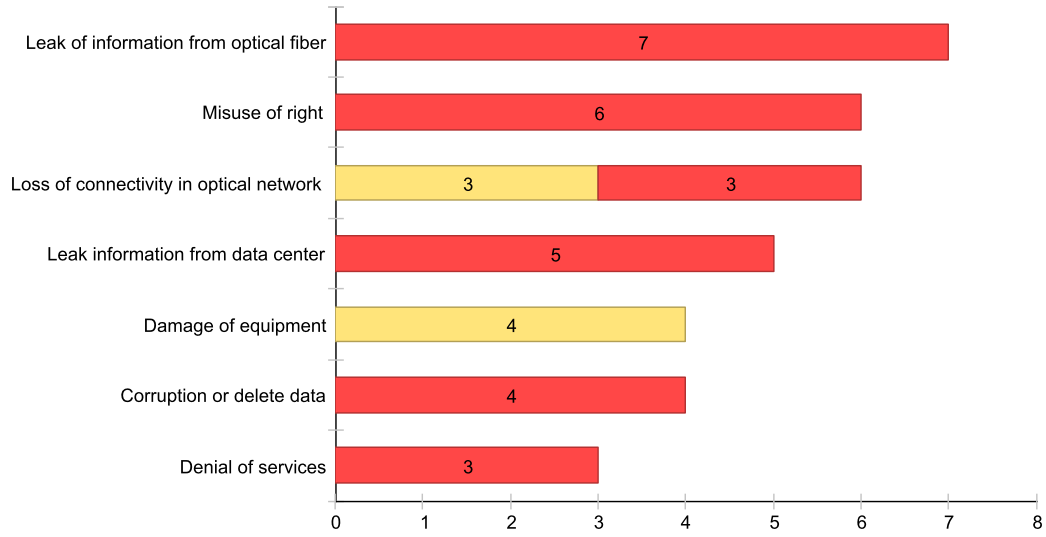
Assets with High Risks (without Controls)

Asset	Risk
Access control system	2
Cameras	1
Card reader	1
Configuration data	10
CWDM MUX/DEMUX	2
Data of comercial interest	10
Data storage	6
Database	4
Documentation	10
DWDM MUX/DEMUX	2
Erbium Doped Fiber Amplifier - EDFA	3
Ethernet	5
ID card	1
Operating system	3
Optical add/drop multiplexer - OAMD	2
Optical cables	8
Optical fiber	10
Optical fiber network	15
Optical Network Unit - ONU	2
Raman amplifier	3
Semiconductor Optical Amplifier - SOA	3
Servers	7
Splitter	3
Switch	2
Tranfer data	12
Transceiver	1
Air conditioning	4
Rack	4

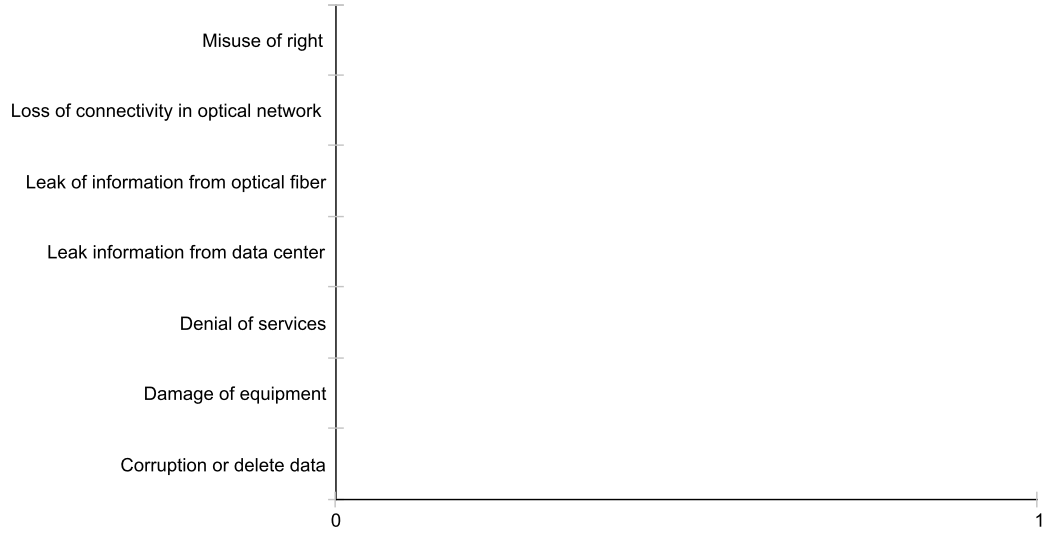
Assets with High Risks (with implemented Controls)

Asset	Risk

High Risk Areas without Controls



High Risk Areas with implemented Controls



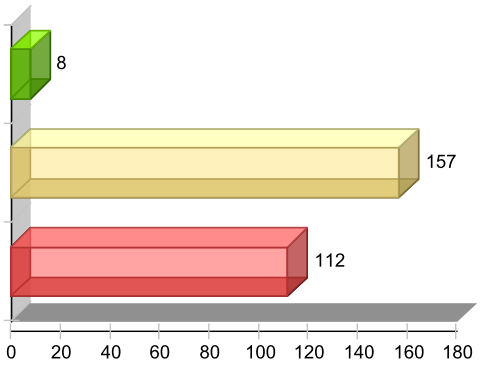
Risk Matrix: Confidentiality (without Controls)

Number of identified Risks

Impact / Probability	0	1	2	3
0	0	0	0	0
1	0	0	0	0
2	0	0	0	0
3	4	4	3	105
4	0	0	2	26
5	6	0	3	38
6	4	0	0	16
7	8	0	7	32
8	2	0	3	14

Table shows the number of identified risks and their severity. See below for classification of probability and business impact levels.

Total Count



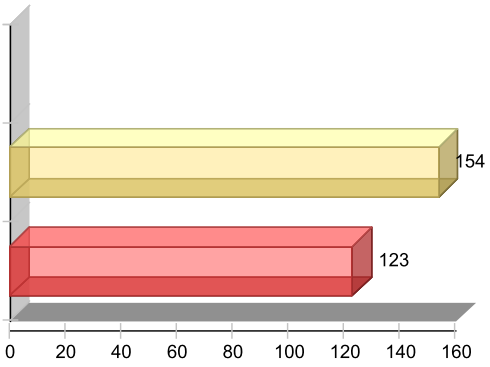
Risk Matrix: Integrity (without Controls)

Number of identified Risks

Impact / Probability	0	1	2
0	0	0	0
1	0	0	0
2	0	0	0
3	8	0	108
4	0	0	28
5	6	0	41
6	4	0	16
7	8	0	39
8	2	0	17

Table shows the number of identified risks and their severity. See below for classification of probability and business impact levels.

Total Count



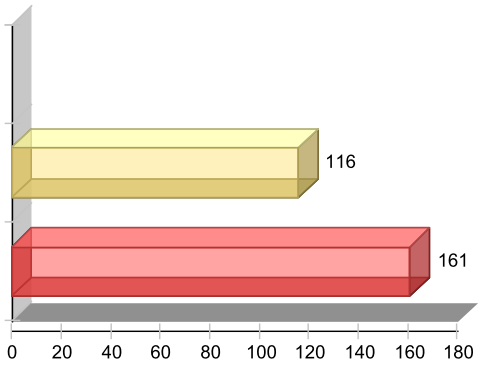
Risk Matrix: Availability (without Controls)

Number of identified Risks

Impact / Probability	0	1	2	3	4
0	0	0	0	0	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	4	0	112	0
4	0	0	0	28	0
5	0	0	0	47	0
6	0	0	0	20	0
7	0	0	0	47	0
8	0	0	0	19	0

Table shows the number of identified risks and their severity.
See below for classification of probability and business impact levels.

Total Count



Business Impact and Risk Classification

Business Impact Classification	
Confidentiality	0 Public: No special requirements. 1 External Use: Information for internal use and customers or partners. Possible financial loss is between 10 and 50, breach of legal requirements with financial penalties is possible. 2 Internal Use: Information for internal use only. Financial loss between 60 and 100. Breach of legal requirements could lead to high financial penalties. Personal injury could result by breach of confidentiality. 3 Sensitive: Possible financial loss higher than 100. Breach of legal requirements could lead to prosecution and a prison sentence. Information loss could lead to serious injury or loss of life.
Integrity	0 None: Possible financial loss below 10-30 1 Normal: Possible financial loss between 40 and 90. Breach of legal requirements could lead to financial penalties. Breach could result in personal injury. 2 High: Possible financial loss higher than 100. Breach of legal requirements could lead to prison sentence. Breach could result in personal injury or death.
Availability	0 Basic: Possible financial due to downtime loss below 100. Recovery time objective (RTO) is higher than one week. 1 Normal: Possible financial loss due to downtime between 10 and 30. RTO is lower than 8. Downtime could impair public image 2 High: Possible financial loss due to downtime between 40 and 60. RTO is lower than 12. Downtime could impair public image or client relationship. 3 Very high: Possible financial loss due to downtime between 70 and 100. RTO is lower than 24. Downtime could seriously impair public image or end client relationship. 4 Exceptional: Special agreements with individual clients which do not fall in one of the above categories.
Threat Classification	
	Threats are classified by the likelihood of their ocurrence as follows: 0 Rare 1 Annually 2 Monthly 3 Weekly 4 Daily 5 Hourly
Vulnerability Classification	
	0 Very low: Exploitation of the vulnerability requires a directed attack, highly special knowledge or skill and ressources that are not ordinarily available to an attacker. Rare Natural events or technical failures of a large scale could trigger the vulnerability. 1 Low: Exploitation of the vulnerability requires a directed attack by a determined attacker. Natural events or technical failures could affect the vulnerability. 2 High: Exploitation of the vulnerability could occur by an automated attack (i.e. scripted attacks) or any attacker even with limited capabilities. Natural events or technical failures could affect the vulnerability. 3 Very high: Exploitation of the vulnerability could occur randomly and is highly likely. Even someone without bad intentions could trigger the vulnerability inadvertently. Common events would almost certainly trigger the vulnerability.

Remaining High Risks (with implemented Controls)

Process	Asset	Scenario	C	I	A	Overall

Detailed Risk Assessment (without Controls)

Abbr.	Name	Confidentiality	Integrity	Availability
	Data backup	**0**	**0**	**3**

Assets and Risk Scenarios			Risk			Total Risk Figure
Abbr.	**Name**	**Type**	**Confidentiality**	**Integrity**	**Availability**	
	Total residiual risk for Data backup:		**569**	**511**	**641**	**1721**
	Air conditioning	**Physical**	**16**	**12**	**16**	**44**
	Damage of equipment and optical cable					
Earthquake	0: Rare		4	3	4	11
Position in earthquake area	3: Very high					
	Explosion					
Severe accident	0: Rare		4	3	4	11
Incorrect parametr setting	3: Very high					
	Fire					
Fire	1: Annually		4	3	4	11
Insufficient equipment maintenance	2: High					
	Flooding data center					
Flood	0: Rare		4	3	4	11
Position in flood area location	3: Very high					
	Cameras	**Physical**	**31**	**26**	**31**	**88**
	Damage of equipment and optical cable					
Earthquake	0: Rare		6	5	6	17
Position in earthquake area	3: Very high					
	Discovere of a critical error in the system					
Zero-day	1: Annually		7	6	7	20
Unknown bugs in programs	3: Very high					
	Explosion					
Severe accident	0: Rare		6	5	6	17
Incorrect parametr setting	3: Very high					
	Fire					
Fire	1: Annually		6	5	6	17
Insufficient equipment maintenance	2: High					
	Flooding data center					
Flood	0: Rare		6	5	6	17
Position in flood area location	3: Very high					
	Card reader	**Physical**	**31**	**26**	**31**	**88**

Damage of equipment and optical cable		6	5	6	17
Earthquake	0: Rare				
Position in earthquake area	3: Very high				
Discovere of a critical error in the system		7	6	7	20
Zero-day	1: Annually				
Unknown bugs in programs	3: Very high				
Electric short		6	5	6	17
Dust	1: Annually				
Insufficient equipment maintenance	2: High				
Fire		6	5	6	17
Fire	1: Annually				
Insufficient equipment maintenance	2: High				
Flooding data center		6	5	6	17
Flood	0: Rare				
Position in flood area location	3: Very high				
Configuration data	**Information**	**63**	**63**	**93**	**219**
Abuse of permission		7	7	10	24
Leak of information	4: Daily				
Missing efficient physical protection	3: Very high				
Database corruption		5	5	8	18
Data failure	2: Monthly				
Failure to comply with regular media changes	3: Very high				
Delete database		6	6	9	21
Data delete	3: Weekly				
Incorrect assignment of access rights	3: Very high				
Disk encryption		8	8	11	27
Malicious code	5: Hourly				
Poor security policies	3: Very high				
Getting data from database		7	7	10	24
Leak of information	4: Daily				
Failure to follow teh rules of locking the monitor screen and computer	3: Very high				
Getting data from databasee - SQL injecting		5	5	8	18
SQL injecting	2: Monthly				
Poorly website security design	3: Very high				
Infecting the network with malicious software		5	5	8	18
Infected USB flash driver	2: Monthly				
Failure to comply the security policy rules	3: Very high				
Leak of information		7	7	10	24
Leak of information	4: Daily				
Failure to comply the security policy rules	3: Very high				
Leak of information		7	7	10	24
Leak of information	4: Daily				
Missing efficient physical protection	3: Very high				
Open RDP port		6	6	9	21
Misuse of permissions	3: Weekly				
Open port 3389 RDP	3: Very high				
Data of comercial interest	**Information**	**93**	**83**	**93**	**269**

Abuse of permission					
Leak of information	4: Daily	10	9	10	29
Missing efficient physical protection	3: Very high				
Database corruption					
Data failure	2: Monthly	8	7	8	23
Failure to comply with regular media changes	3: Very high				
Delete database					
Data delete	3: Weekly	9	8	9	26
Incorrect assignment of access rights	3: Very high				
Disk encryption					
Malicious code	5: Hourly	11	10	11	32
Poor security policies	3: Very high				
Getting data from database					
Leak of information	4: Daily	10	9	10	29
Failure to follow teh rules of locking the monitor screen and computer	3: Very high				
Getting data from databasee - SQL injecting					
SQL injecting	2: Monthly	8	7	8	23
Poorly website security design	3: Very high				
Infecting the network with malicious software					
Infected USB flash driver	2: Monthly	8	7	8	23
Failure to comply the security policy rules	3: Very high				
Leak of information					
Leak of information	4: Daily	10	9	10	29
Failure to comply the security policy rules	3: Very high				
Leak of information					
Leak of information	4: Daily	10	9	10	29
Missing efficient physical protection	3: Very high				
Open RDP port					
Misuse of permissions	3: Weekly	9	8	9	26
Open port 3389 RDP	3: Very high				
Data storage	**Physical**	**77**	**67**	**77**	**221**

Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Database corruption					
Data failure	2: Monthly	8	7	8	23
Failure to comply with regular media changes	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Disk cloning					
Leak of information	4: Daily	10	9	10	29
Missing efficient physical protection	3: Very high				
Disk encryption					
Malicious code	5: Hourly	11	10	11	32
Poor security policies	3: Very high				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Retriveing data from media					
Steal of information	2: Monthly	8	7	8	23
Insufficient data or media disposal procedure	3: Very high				
Theft of media					
Steal device	3: Weekly	9	8	9	26
Missing efficient physical protection	3: Very high				
Database	**Software**	**38**	**33**	**38**	**109**
Database corruption					
Data failure	2: Monthly	8	7	8	23
Failure to comply with regular media changes	3: Very high				
Delete database					
Data delete	3: Weekly	9	8	9	26
Incorrect assignment of access rights	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Infecting the network with malicious software					
Infected USB flash driver	2: Monthly	8	7	8	23
Failure to comply the security policy rules	3: Very high				
Documentation	**Information**	**63**	**63**	**93**	**219**

Abuse of permission					
Leak of information	4: Daily	7	7	10	24
Missing efficient physical protection	3: Very high				
Database corruption					
Data failure	2: Monthly	5	5	8	18
Failure to comply with regular media changes	3: Very high				
Delete database					
Data delete	3: Weekly	6	6	9	21
Incorrect assignment of access rights	3: Very high				
Disk encryption					
Malicious code	5: Hourly	8	8	11	27
Poor security policies	3: Very high				
Getting data from database					
Leak of information	4: Daily	7	7	10	24
Failure to follow teh rules of locking the monitor screen and computer	3: Very high				
Getting data from databasee - SQL injecting					
SQL injecting	2: Monthly	5	5	8	18
Poorly website security design	3: Very high				
Infecting the network with malicious software					
Infected USB flash driver	2: Monthly	5	5	8	18
Failure to comply the security policy rules	3: Very high				
Leak of information					
Leak of information	4: Daily	7	7	10	24
Failure to comply the security policy rules	3: Very high				
Leak of information					
Leak of information	4: Daily	7	7	10	24
Missing efficient physical protection	3: Very high				
Open RDP port					
Misuse of permissions	3: Weekly	6	6	9	21
Open port 3389 RDP	3: Very high				
ID card		**33**	**28**	**33**	**94**
Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Theft of media					
Steal device	3: Weekly	9	8	9	26
Missing efficient physical protection	3: Very high				
Operating system	**Software**	**26**	**23**	**26**	**75**

	Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20	
Unknown bugs in programs	3: Very high					
	Infecting the network with malicious software					
Infected USB flash driver	2: Monthly	8	7	8	23	
Failure to comply the security policy rules	3: Very high					
	Running malicious code					
Malicious code	5: Hourly	11	10	11	32	
Failure to comply the security policy rules	3: Very high					
	Rack		**12**	**12**	**24**	**48**
	Damage of equipment and optical cable					
Earthquake	0: Rare	3	3	6	12	
Position in earthquake area	3: Very high					
	Explosion					
Severe accident	0: Rare	3	3	6	12	
Incorrect parametr setting	3: Very high					
	Fire					
Fire	1: Annually	3	3	6	12	
Insufficient equipment maintenance	2: High					
	Flooding data center					
Flood	0: Rare	3	3	6	12	
Position in flood area location	3: Very high					
	Servers	**Physical**	**86**	**75**	**86**	**247**

Damage of equipment and optical cable		6	5	6	17
Earthquake	0: Rare				
Position in earthquake area	3: Very high				
Database corruption		8	7	8	23
Data failure	2: Monthly				
Failure to comply with regular media changes	3: Very high				
Discovere of a critical error in the system		7	6	7	20
Zero-day	1: Annually				
Unknown bugs in programs	3: Very high				
Disk cloning		10	9	10	29
Leak of information	4: Daily				
Missing efficient physical protection	3: Very high				
Disk encryption		11	10	11	32
Malicious code	5: Hourly				
Poor security policies	3: Very high				
Explosion		6	5	6	17
Severe accident	0: Rare				
Incorrect parametr setting	3: Very high				
Fire		6	5	6	17
Fire	1: Annually				
Insufficient equipment maintenance	2: High				
Flooding data center		6	5	6	17
Flood	0: Rare				
Position in flood area location	3: Very high				
Open RDP port		9	8	9	26
Misuse of permissions	3: Weekly				
Open port 3389 RDP	3: Very high				
Retriveing data from media		8	7	8	23
Steal of information	2: Monthly				
Insufficient data or media disposal procedure	3: Very high				
Theft of media		9	8	9	26
Steal device	3: Weekly				
Missing efficient physical protection	3: Very high				

Abbr.	Name	Confidentiality	Integrity	Availability
	Data transmission	**3**	**2**	**3**

Assets and Risk Scenarios			Risk			Total Risk Figure
Abbr.	**Name**	**Type**	**Confidentiality**	**Integrity**	**Availability**	
	Total residiual risk for Data transmission:		**1460**	**1283**	**1478**	**4221**
	Access control system		**42**	**36**	**42**	**120**
	Damage of equipment and optical cable					
Earthquake		0: Rare	6	5	6	17
Position in earthquake area		3: Very high				
	Discovere of a critical error in the system					
Zero-day		1: Annually	7	6	7	20
Unknown bugs in programs		3: Very high				
	Explosion					
Severe accident		0: Rare	6	5	6	17
Incorrect parametr setting		3: Very high				
	Fire					
Fire		1: Annually	6	5	6	17
Insufficient equipment maintenance		2: High				
	Flooding data center					
Flood		0: Rare	6	5	6	17
Position in flood area location		3: Very high				
	Running malicious code					
Malicious code		5: Hourly	11	10	11	32
Failure to comply the security policy rules		3: Very high				
	CWDM MUX/DEMUX	**Physical**	**45**	**38**	**45**	**128**

Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Electric short					
Dust	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Cameras	**Physical**	**31**	**26**	**31**	**88**
Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Card reader	**Physical**	**31**	**26**	**31**	**88**

	Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17	
Position in earthquake area	3: Very high					
	Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20	
Unknown bugs in programs	3: Very high					
	Electric short					
Dust	1: Annually	6	5	6	17	
Insufficient equipment maintenance	2: High					
	Fire					
Fire	1: Annually	6	5	6	17	
Insufficient equipment maintenance	2: High					
	Flooding data center					
Flood	0: Rare	6	5	6	17	
Position in flood area location	3: Very high					
	DWDM MUX/DEMUX	**Physical**	**45**	**38**	**45**	**128**
	Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17	
Position in earthquake area	3: Very high					
	Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23	
Unprotected communication links	3: Very high					
	Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20	
Unknown bugs in programs	3: Very high					
	Electric short					
Dust	1: Annually	6	5	6	17	
Insufficient equipment maintenance	2: High					
	Explosion					
Severe accident	0: Rare	6	5	6	17	
Incorrect parametr setting	3: Very high					
	Fire					
Fire	1: Annually	6	5	6	17	
Insufficient equipment maintenance	2: High					
	Flooding data center					
Flood	0: Rare	6	5	6	17	
Position in flood area location	3: Very high					
	Data of comercial interest	**Information**	**93**	**83**	**93**	**269**

Abuse of permission					
Leak of information	4: Daily	10	9	10	29
Missing efficient physical protection	3: Very high				
Database corruption					
Data failure	2: Monthly	8	7	8	23
Failure to comply with regular media changes	3: Very high				
Delete database					
Data delete	3: Weekly	9	8	9	26
Incorrect assignment of access rights	3: Very high				
Disk encryption					
Malicious code	5: Hourly	11	10	11	32
Poor security policies	3: Very high				
Getting data from database					
Leak of information	4: Daily	10	9	10	29
Failure to follow teh rules of locking the monitor screen and computer	3: Very high				
Getting data from databasee - SQL injecting					
SQL injecting	2: Monthly	8	7	8	23
Poorly website security design	3: Very high				
Infecting the network with malicious software					
Infected USB flash driver	2: Monthly	8	7	8	23
Failure to comply the security policy rules	3: Very high				
Leak of information					
Leak of information	4: Daily	10	9	10	29
Failure to comply the security policy rules	3: Very high				
Leak of information					
Leak of information	4: Daily	10	9	10	29
Missing efficient physical protection	3: Very high				
Open RDP port					
Misuse of permissions	3: Weekly	9	8	9	26
Open port 3389 RDP	3: Very high				
Data storage	**Physical**	**77**	**67**	**77**	**221**

Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Database corruption					
Data failure	2: Monthly	8	7	8	23
Failure to comply with regular media changes	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Disk cloning					
Leak of information	4: Daily	10	9	10	29
Missing efficient physical protection	3: Very high				
Disk encryption					
Malicious code	5: Hourly	11	10	11	32
Poor security policies	3: Very high				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Retriveing data from media					
Steal of information	2: Monthly	8	7	8	23
Insufficient data or media disposal procedure	3: Very high				
Theft of media					
Steal device	3: Weekly	9	8	9	26
Missing efficient physical protection	3: Very high				
Database	**Software**	**38**	**33**	**38**	**109**
Database corruption					
Data failure	2: Monthly	8	7	8	23
Failure to comply with regular media changes	3: Very high				
Delete database					
Data delete	3: Weekly	9	8	9	26
Incorrect assignment of access rights	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Infecting the network with malicious software					
Infected USB flash driver	2: Monthly	8	7	8	23
Failure to comply the security policy rules	3: Very high				
Erbium Doped Fiber Amplifier - EDFA		**55**	**47**	**55**	**157**

Communication distruption					
Denial of services	5: Hourly	10	9	10	29
Sensitive to frequency changes	2: High				
Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Electric short					
Dust	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Ethernet	**Service**	**48**	**43**	**48**	**139**
Degradation of services					
Denial of services	5: Hourly	11	10	11	32
Unprotected communication links	3: Very high				
Infecting the network with malicious software					
Infected USB flash driver	2: Monthly	8	7	8	23
Failure to comply the security policy rules	3: Very high				
Loss of availability					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Running malicious code					
Malicious code	5: Hourly	11	10	11	32
Failure to comply the security policy rules	3: Very high				
Wirettaping - leak of information					
Eavesdropping	4: Daily	10	9	10	29
Insufficient key exchange of definition in standard, Poorly protected communication links	3: Very high				
ID card		**33**	**28**	**33**	**94**

Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Theft of media					
Steal device	3: Weekly	9	8	9	26
Missing efficient physical protection	3: Very high				
Operating system	**Software**	**26**	**23**	**26**	**75**
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Infecting the network with malicious software					
Infected USB flash driver	2: Monthly	8	7	8	23
Failure to comply the security policy rules	3: Very high				
Running malicious code					
Malicious code	5: Hourly	11	10	11	32
Failure to comply the security policy rules	3: Very high				
Optical Network Unit - ONU	**Physical**	**45**	**38**	**45**	**128**
Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Electric short					
Dust	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Optical add/drop multiplexer - OAMD		**45**	**38**	**45**	**128**

	Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17	
Position in earthquake area	3: Very high					
	Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23	
Unprotected communication links	3: Very high					
	Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20	
Unknown bugs in programs	3: Very high					
	Electric short					
Dust	1: Annually	6	5	6	17	
Insufficient equipment maintenance	2: High					
	Explosion					
Severe accident	0: Rare	6	5	6	17	
Incorrect parametr setting	3: Very high					
	Fire					
Fire	1: Annually	6	5	6	17	
Insufficient equipment maintenance	2: High					
	Flooding data center					
Flood	0: Rare	6	5	6	17	
Position in flood area location	3: Very high					
Optical cables	**Physical**	**102**	**89**	**102**	**293**	

Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Degradation and deformation of optical fiber					
Optical fiber breakage	1: Annually	6	5	6	17
Insufficient handling or manufacture defect	2: High				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Evanescent Coupling					
Eavesdropping	4: Daily	10	9	10	29
Unprotected communication links	3: Very high				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fiber Bending					
Eavesdropping	4: Daily	10	9	10	29
Unprotected communication links	3: Very high				
Fiber breakage					
Freeze, humudity	1: Annually	7	6	7	20
Insufficient protection of the optical fiber	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Optical Splitting					
Eavesdropping	4: Daily	10	9	10	29
Unprotected communication links	3: Very high				
Scattering					
Eavesdropping	4: Daily	10	9	10	29
Unprotected communication links	3: Very high				
V-Groove cut					
Eavesdropping	4: Daily	10	9	10	29
Unprotected communication links	3: Very high				
Optical fiber	**Physical**	**114**	**100**	**114**	**328**

Communication distruption					
Denial of services	5: Hourly	10	9	10	29
Sensitive to frequency changes	2: High				
Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Degradation and deformation of optical fiber					
Optical fiber breakage	1: Annually	6	5	6	17
Insufficient handling or manufacture defect	2: High				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Evanescent Coupling					
Eavesdropping	4: Daily	10	9	10	29
Unprotected communication links	3: Very high				
Fiber Bending					
Eavesdropping	4: Daily	10	9	10	29
Unprotected communication links	3: Very high				
Fiber breakage					
Freeze, humudity	1: Annually	7	6	7	20
Insufficient protection of the optical fiber	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Optical Splitting					
Eavesdropping	4: Daily	10	9	10	29
Unprotected communication links	3: Very high				
Scattering					
Eavesdropping	4: Daily	10	9	10	29
Unprotected communication links	3: Very high				
TEMPEST attack					
Active wirettapng	2: Monthly	8	7	8	23
Poorly protected communication links	3: Very high				
V-Groove cut					
Eavesdropping	4: Daily	10	9	10	29
Unprotected communication links	3: Very high				
Optical fiber network	**Service**	**141**	**141**	**159**	**441**

Communication distruption		9	9	10	28
Denial of services	5: Hourly				
Sensitive to frequency changes	2: High				
Damage of fiber network components		7	7	8	22
Damage of fiber network units	2: Monthly				
Unprotected communication links	3: Very high				
Degradation and deformation of optical fiber		5	5	6	16
Optical fiber breakage	1: Annually				
Insufficient handling or manufacture defect	2: High				
Degradation of services		10	10	11	31
Denial of services	5: Hourly				
Unprotected communication links	3: Very high				
Discovere of a critical error in the system		6	6	7	19
Zero-day	1: Annually				
Unknown bugs in programs	3: Very high				
Evanescent Coupling		9	9	10	28
Eavesdropping	4: Daily				
Unprotected communication links	3: Very high				
Explosion		5	5	6	16
Severe accident	0: Rare				
Incorrect parametr setting	3: Very high				
Fiber Bending		9	9	10	28
Eavesdropping	4: Daily				
Unprotected communication links	3: Very high				
Fiber breakage		6	6	7	19
Freeze, humudity	1: Annually				
Insufficient protection of the optical fiber	3: Very high				
Flooding splitter with request		10	10	11	31
Denial of services	5: Hourly				
Poor security policies	3: Very high				
Infecting the network with malicious software		7	7	8	22
Infected USB flash driver	2: Monthly				
Failure to comply the security policy rules	3: Very high				
Loss of availability		7	7	8	22
Damage of fiber network units	2: Monthly				
Unprotected communication links	3: Very high				
Optical Splitting		9	9	10	28
Eavesdropping	4: Daily				
Unprotected communication links	3: Very high				
Power failure		5	5	6	16
Interruption of electricity supply	0: Rare				
Unstable electrical network	3: Very high				
Running malicious code		10	10	11	31
Malicious code	5: Hourly				
Failure to comply the security policy rules	3: Very high				
Scattering		9	9	10	28
Eavesdropping	4: Daily				
Unprotected communication links	3: Very high				

V-Groove cut					
Eavesdropping	4: Daily	9	9	10	28
Unprotected communication links	3: Very high				
Wirettaping - leak of information					
Eavesdropping	4: Daily	9	9	10	28
Insufficient key exchange of definition in standard, Poorly protected communication links	3: Very high				
Raman amplifier		**55**	**47**	**55**	**157**
Communication distruption					
Denial of services	5: Hourly	10	9	10	29
Sensitive to frequency changes	2: High				
Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Electric short					
Dust	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Semiconductor Optical Amplifier - SOA		**55**	**47**	**55**	**157**

Communication distruption					
Denial of services	5: Hourly	10	9	10	29
Sensitive to frequency changes	2: High				
Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Electric short					
Dust	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Servers	**Physical**	**86**	**75**	**86**	**247**

Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Database corruption					
Data failure	2: Monthly	8	7	8	23
Failure to comply with regular media changes	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Disk cloning					
Leak of information	4: Daily	10	9	10	29
Missing efficient physical protection	3: Very high				
Disk encryption					
Malicious code	5: Hourly	11	10	11	32
Poor security policies	3: Very high				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Open RDP port					
Misuse of permissions	3: Weekly	9	8	9	26
Open port 3389 RDP	3: Very high				
Retriveing data from media					
Steal of information	2: Monthly	8	7	8	23
Insufficient data or media disposal procedure	3: Very high				
Theft of media					
Steal device	3: Weekly	9	8	9	26
Missing efficient physical protection	3: Very high				
Splitter		**56**	**48**	**56**	**160**

Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Electric short					
Dust	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Flooding splitter with request					
Denial of services	5: Hourly	11	10	11	32
Poor security policies	3: Very high				
Switch		**39**	**33**	**39**	**111**
Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Discovere of a critical error in the system					
Zero-day	1: Annually	7	6	7	20
Unknown bugs in programs	3: Very high				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				
Tranfer data	**Information**	**120**	**107**	**120**	**347**

Abuse of permission					
Leak of information	4: Daily	10	9	10	29
Missing efficient physical protection	3: Very high				
Degradation of services					
Denial of services	5: Hourly	11	10	11	32
Unprotected communication links	3: Very high				
Delete database					
Data delete	3: Weekly	9	8	9	26
Incorrect assignment of access rights	3: Very high				
Flooding splitter with request					
Denial of services	5: Hourly	11	10	11	32
Poor security policies	3: Very high				
Getting data from database					
Leak of information	4: Daily	10	9	10	29
Failure to follow teh rules of locking the monitor screen and computer	3: Very high				
Getting data from databasee - SQL injecting					
SQL injecting	2: Monthly	8	7	8	23
Poorly website security design	3: Very high				
Infecting the network with malicious software					
Infected USB flash driver	2: Monthly	8	7	8	23
Failure to comply the security policy rules	3: Very high				
Leak of information					
Leak of information	4: Daily	10	9	10	29
Missing efficient physical protection	3: Very high				
Leak of information					
Leak of information	4: Daily	10	9	10	29
Failure to comply the security policy rules	3: Very high				
Loss of availability					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Open RDP port					
Misuse of permissions	3: Weekly	9	8	9	26
Open port 3389 RDP	3: Very high				
Power failure					
Interruption of electricity supply	0: Rare	6	5	6	17
Unstable electrical network	3: Very high				
Wirettaping - leak of information					
Eavesdropping	4: Daily	10	9	10	29
Insufficient key exchange of definition in standard, Poorly protected communication links	3: Very high				
Transceiver	**Physical**	**38**	**32**	**38**	**108**

Damage of equipment and optical cable					
Earthquake	0: Rare	6	5	6	17
Position in earthquake area	3: Very high				
Damage of fiber network components					
Damage of fiber network units	2: Monthly	8	7	8	23
Unprotected communication links	3: Very high				
Electric short					
Dust	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Explosion					
Severe accident	0: Rare	6	5	6	17
Incorrect parametr setting	3: Very high				
Fire					
Fire	1: Annually	6	5	6	17
Insufficient equipment maintenance	2: High				
Flooding data center					
Flood	0: Rare	6	5	6	17
Position in flood area location	3: Very high				