MORAVSKÁ VYSOKÁ ŠKOLA OLOMOUC

UI - Ústav informatiky

Kybernetické hrozby a jejich dopad na ekonomickou oblast organizace

DIPLOMOVÁ PRÁCE

Bc. Martin Řihošek

Vedoucí práce: Ing. Lukáš Pavlík, Ph.D.

Olomouc 2021

PROHLÁŠENÍ

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a použil jen ty zdroje, které jsou uvedené v seznamu literatury a použitých zdrojů.

Tištěná verze textu práce je shodná s textem práce na CD nosiči a elektronickou verzí vloženou do studijního systému IS/STAG.

V Uhřičicích dne 25.3.2021 Martin Řihošek

PODĚKOVÁNÍ

Děkuji svému vedoucímu Ing. Lukáši Pavlíkovi, Ph.D. za odborné vedení práce, za cenné rady a ochotu v průběhu zpracování práce.

Moravská vysoká škola Olomouc
Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Martin Řihošek**
Osobní číslo:	**M19041**
Studijní program:	**N0413P050002 Ekonomika a management**
Studijní obor:	**Ekonomika a management malých a středních podniků**
Téma práce:	**Kybernetické hrozby a jejich dopady na ekonomickou oblast organizace**
Zadávající katedra:	**Ústav informatiky a aplikované matematiky**

Zásady pro vypracování

1. Definujte základní problematiku kybernetické bezpečnosti.
2. Pojednejte o scénářích kybernetických hrozeb a jejich možných dopadech na aktiva organizace.
3. Proveďte analýzu metod oceňování aktiv organizace s ohledem na možné dopady kybernetických hrozeb.
4. Analyzujte kybernetické hrozby a navrhněte způsob stanovení jejich dopadů na vybraná aktiva organizace.
5. Vyhodnoďte výsledky provedené analýzy a navrhěte doporučení pro další vývoj.

Rozsah pracovní zprávy:
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Praha: Aleš Čeněk, 2018, 936 s. ISBN 978-80-7380-720-7.
2. ŠILEROVÁ, Edita, Klára HENNYEYOVÁ a N.N. BALASHOVA. *Informační systémy v podnikové praxi*. Praha: Poweprint, 2016, 163 s. ISBN 978-80-87994-78-8.
3. SVAČINA, Pavel. Oceňování nehmotných aktiv. Praha: Ekopress, 2010, 211 s. ISBN 978-80-86929-62-0.
4. MAŘÍK, Miloš. *Metody oceňování podniku*. 4. vydání. Praha: Ekopress, 2018, 550 s. ISBN 978-80-87865-38-5.
5. KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
6. ČAPEK, Jan, Miloslav HUB, Radim ROUDNÝ, Hana KOPÁČKOVÁ, Jan FUKA a Martin IBL. Vybrané aspekty kybernetické bezpečnosti. Pardubice: Univerzita Pardubice, 2015. Monografia. ISBN 978-80-7395-953-1.

Vedoucí diplomové práce: **Ing. Lukáš PAVLÍK, Ph.D.**
Ústav informatiky a aplikované matematiky

Datum zadání diplomové práce: **24. dubna 2020**
Termín odevzdání diplomové práce: **31. března 2021**

Podpis studenta: Datum: 30. 7. 2020

Podpis vedoucího práce: Datum: 3. 7. 2020

Moravská vysoká škola Olomouc, o.p.s.
L.S.

Mgr. Irena KOVAČIČINOVÁ
prorektorka

Mgr. Veronika ŘÍHOVÁ, Ph.D.
manažer ústavu

V Olomouci dne 11. května 2020

ANOTACE

Bibliografický údaj: Řihošek, Martin. Kybernetické hrozby a jejich dopad na ekonomickou oblast organizace. Olomouc 2021. Diplomová práce. Moravská vysoká škola Olomouc. Vedoucí práce: Ing. Lukáš Pavlík, Ph.D.

Název práce: Kybernetické hrozby a jejich dopad na ekonomickou oblast organizace

Autor: Martin Řihošek

Ústav: Ústav informatiky a aplikované matematiky

Vedoucí práce: Ing. Lukáš Pavlík, Ph.D.

Abstrakt: Rozvoj technologií a jejich aplikace napříč procesy v organizacích a firmách způsobuje mimo pozitivního dopadu také nárůst příležitostí pro selhání nebo zneužití těchto technologií s negativním dopadem na hospodaření podniku.

Tato práce si dává za cíl možné hrozby přicházející z oblasti kyberprostoru popsat, definovat a rozčlenit dle stanovených kritérií a to včetně určení potenciálních dopadů do ekonomické sféry organizace. Stanovení kritérií vychází z právního rámce platného v České republice, především pak zákona o kybernetické bezpečnosti a navazujících doporučení vydaných Národním úřadem pro kybernetickou a informační bezpečnost - NÚKIB. Metodika pro posuzování kybernetických hrozeb staví na normách ČSN EN ISO/IEC 27000. U vybrané podnikatelského subjektu je provedena analýza kybernetických hrozeb včetně určení aktiv, která jsou potenciálně ohrožena kybernetickými hrozbami. U vybraných nejzávažnějších kybernetických hrozeb je provedena hlubší analýza, jejímž výstupem je určení dopadu hrozby a předložení doporučení pro mitigaci dané hrozby. Na základě provedeného rozčlenění kybernetických hrozeb a určení jejich potenciálního dopadu na vybraná aktiva společnosti je proveden výběr metod vhodných pro ocenění dopadu těchto kybernetických hrozeb.

Analýza kybernetických hrozeb a posouzení vhodnosti vybraných metod pro oceňování nehmotných aktiv je provedeno v reáliích existujícího podniku poskytujícího služby v oblasti informačních technologií.

Klíčová slova: kybernetická hrozba, kybernetická bezpečnost, kyberbezpečnost, aktiva, nehmotná aktiva, řízení rizik

Title: Cyber Threats and their Impacts on the Economic Area of the Organization

Author: Martin Řihošek

Department: Department of Informatics and Applied Mathematics

Supervisor: Ing. Lukáš Pavlík, Ph.D.

Abstract: The expansion of technologies and their application across processes in organizations and companies causes, in addition to a positive impact, also an increase in opportunities for failure or misuse of these technologies with a negative impact on the company's assets.

This thesis aims to describe, define and break down possible threats coming from the field of cyberspace according to established criteria, including the definition of potential impacts on the economic sphere of the organization. The determination of the criteria is based on the legal framework valid in the Czech Republic, especially the Act on Cyber Security, and the follow-up recommendations issued by the National Cyber and Information Security Agency – the NÚKIB. The methodology for assessing cyber threats is based on the standards ČSN EN ISO/IEC 27000.

The identification of threats and their impact on assets is used to determination of appropriate methods to quantify the above impacts, focusing primarily on the company's intangible assets. A deeper analysis is performed on selected most serious cyber threats. Based on this analysis are determined threats' impacts and recommendations for mitigating the threats is presented as well.

The assessment of the suitability of selected methods is performed in the realities of an existing company providing IT services.

Keywords: cyberthreat, cybersecurity, assets, intangible assets, risk management

OBSAH

ÚVOD

Pojem kybernetická bezpečnost patří mezi hojně používané výrazy a to ve spojení s řadou obecných i specializovaných činností a situací. V dnešní době řešení kybernetické bezpečnosti podnikové infrastruktury nabývá na naléhavosti s ohledem také na vynucený hromadný přechod na práci z domova. Tato situace sama o sobě přináší v oblasti kybernetické bezpečnosti dilemata a nové výzvy. Pracovníci oddělení správy informačních technologií podniků jsou konfrontováni s otázkami, jak skloubit zajištění kybernetické bezpečnosti podniku s nutností provozovat firemní zařízení připojené do domácí sítě propojené s cizími nedůvěryhodnými prvky, a nebo umožnit přístup do vnitřní sítě společnosti z nezajištěných soukromých počítačů zaměstnanců. Tyto nesnadné otázky související se zajištěním bezpečnosti v oblasti ICT[1] je nutno doplňovat o požadavky na zachování produktivity práce a uživatelského komfortu na dané úrovni.

Tato práce si klade za cíl jednotlivé hrozby pocházející z kyberprostoru a nebo související s provozem ICT v podniku popsat, definovat možné scénáře vzniku dané hrozby a určit dopad na hmotná i nehmotná aktiva podniku. Provedená analýza se z praktických důvodů omezuje na kontext malého nebo středního podniku.

Charakter dopadu kybernetického hrozby, ať už má tato hrozba charakter úmyslného činu pocházejícího z vnějšího prostředí nebo jde o projev náhodného selhání, je zpravidla primárně nehmotný. Důsledkem kybernetického útoku nebo naplněné hrozby bývá velmi často ztráta dat, kompromitace, poškození dobrého jména, případně odcizení duševního vlastnictví. U podnikových aktiv tohoto typu však bývá zpravidla velmi obtížné kvantifikovat dopad kybernetické hrozby, respektive škody způsobené kybernetickým útokem. Důvodem je především fakt, že samotné ocenění dotčeného nehmotného aktiva bývá velmi komplikované, a to zda pro daný druh nehmotného aktiva existuje vhodná metoda ocenění, nemusí být vždy zřejmé na první pohled.

Z tohoto důvodu si práce staví jako stěžejní motivaci určení metod vhodných pro ocenění ekonomického dopadu konkrétních kybernetických hrozeb, a to v kontextu zvoleného podnikatelského subjektu. Provedení uvedené analýzy předchází zmapování zranitelnosti vybraného podnikatelského subjektu a stanovení rizik vybraných kybernetických incidentů.

1 ICT – Information and Communication Technologies (Informační a komunikační technologie)

Na základě podkladů získaných pro potřeby řešení modelového příkladu a na základě uvedených analýz rizik dojde k posouzení vhodnosti vybraných metod pro oceňování nehmotných aktiv organizace, a to s cílem určit ty metody, jejichž použití je pro kvantifikaci dopadů vybraných kybernetických hrozeb vhodné a případně určit za jakých podmínek toto použití možné je.

I. TEORETICKÁ ČÁST

1 KYBERNETICKÁ BEZPEČNOST

Na úvod je třeba říci, že výklad a definici obecného pojmu bezpečnost právní řád České republiky nijak nedefinuje, ani nezmiňuje v žádném ze svých zákoníků. Nicméně, pojem bezpečnosti lze vymezit jako stav, kdy se subjekt, firma či stát necítí být ohrožen hrozbami, případně se tyto subjekty cítí být před těmito hrozbami dostatečně chráněny. Pojem hrozba je pak třeba definovat jako objektivní skutečnost, která může mít negativní dopad na daný subjekt.

Pojem kybernetická bezpečnost přenáší výše uvedené vymezení do reálií kybernetického prostoru, tedy do oblasti navzájem propojených informačních systémů a zařízení. Samotný pojem kybernetická bezpečnost je odvozen od anglického pojmu cybersecurity[2]. Svým významem představuje ochranu před hrozbami v obecnosti souvisejícími s počítači a počítačovou infrastrukturou. V rámci kybernetické bezpečnosti hovoříme také o pojmu kyberprostor. Jedná se o slovo odvozené z anglického pojmu cyberspace[3]. Za kyberprostor je v dnešní době považováno celé prostředí počítačových sítí a počítačů, které tyto sítě spojují. Do tohoto světa (kyberprostoru) se díky nutnosti zvyšování konkurenceschopnosti a efektivity práce stále více integruje i svět podnikových systémů. Podniky výrobní i podniky poskytující služby se tedy stávají stále více součástí výše zmíněného kyberprostoru. Sekundární efekt zmíněného propojování je fakt, že v důsledku vytvořených propojení dochází i ke zvyšování dostupností vnitřních podnikových zařízení zvenčí. V důsledku této zvýšené dostupnosti dochází i ke zvyšování míry rizika, resp. hrozbám, kterým musí podnikový systém čelit. Nicméně, informační systémy nečelí pouze hrozbám pocházejícím z vnějšího prostředí. Je nutné zmínit, že i možnost vzniku hrozby pro aktiva podniku uvnitř. V tomto případě se nejedná pouze o možnosti cílených útoku, ale je třeba vzít v potaz i další hrozby jako je například vliv lidského faktoru, nehody, selhání techniky, vlivy poruch jiných zařízení, elektrické výboje, požáry, zaplavení a další přírodní vlivy.

S ohledem na to skutečnost, že závislost podniku, bez ohledu na charakter jeho produkce, na technologiích neustálé vzrůstá, narůstá také potřeba přítomnosti regulace procesů spojených s administrací prvků ICT[4] a stanovení pravidel jejich vzájemného propojování a komunikace nejen mezi podniky, ale i mezi podnikem a službami poskytovaných státem,

2 Cybersecurity- kybernetická bezpečnost
3 Cyberspace – kybernetický prostor
4 ICT (Information and comnuniction technologies) - Informační a komunikační technologie

případně státními autoritami. Následující kapitoly představují normy, jejichž úloha je tuto regulaci definovat včetně příslušných metodik. [1] , [2],[3], [4]

1.1 Legislativní rámec

Právní systém České republiky postihuje problematiku kybernetické bezpečnosti a související pojmy předpisy uvedenými v následující tabulce:

Tab. 1. Právní předpisy ČR související s kybernetickou bezpečností

Zákon, norma	Popis
Zákon č.181/2014 Sb.	Zákon č.181/2014 Sb. ze dne 23. července 2014, o kybernetické bezpečnosti a o změnách souvisejících zákonů, novelizován zákonem č. 205/2017 Sb., který zapracovává směrnici NIS[5]
Vyhláška č.317/2014 Sb.	Vyhláška č.317/2014 Sb. ze dne 15. prosince 2014, o významných informačních systémech a jejich určujících kritériích. Vyhláška stanovuje kritéria pro určování významných informačních systémů.
Vyhláška č. 82/2018 Sb	Vyhláška o kybernetické bezpečnosti č. 82/2018 Sb. ze dne 21. května 2018 zapracovává směrnici NIS a pro informační systémy a jejich prvky upravuje obsah a strukturu bezpečnostní dokumentace, rozsah a strukturu bezpečnostních opatření, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů, náležitosti protokolování kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku, způsob likvidace dat a provozních informací.
Zákon č. 412/2005 Sb.	Zákon č. 412/2005 Sb. ze dne 21. září 2015, o ochraně utajovaných informací a bezpečnostní způsobilosti. Upravuje zásady pro stanovení informací jako informací utajovaných, podmínky přístupu k informacím, požadavky na jejich ochranu, zásady pro stanovení citlivosti.
Zákon č. 365/2000 Sb.	Zákon č. 365/2000 Sb. ze dne 14. září 2000, o informačních systémech veřejné správy a o změně některých dalších zákonů. Zákon stanoví práva a povinnosti související s vytvořením, správou, provozem, rozvojem a užíváním informačních systémů veřejné správy, vyjma systémů určených pro administraci utajovaných informací a systémů bezpečnostních služeb.

5 NIS – Network and information systems, směrnice EU 2016/1148 o opatřeních na zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů

Zákon, norma	Popis
Zákon č. 480/2004 Sb.	Zákon č. 480/2004 Sb. ze dne 29. července 2004, o některých službách informační společnosti. Jedná se přepis směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o určitých aspektech služeb informačních společností, zejména elektronického obchodního styku v rámci vnitřního trhu a směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. června 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.
Zákon č. 127/2005 Sb.	Zákon č. 127/2005 Sb. ze dne 14. září 2000, o elektronických komunikacích a o změně některých souvisejících zákonů, upravuje na základě práva Evropské unie podmínky podnikání a výkon státní správy, včetně regulace trhu, v oblasti elektronických komunikací. Stanoví práva a povinnosti související s poskytováním služeb elektronických komunikací, provozováním komunikačních sítí a ochranou údajů. Nastavuje rámec regulace komunikačních činností a definuje úkoly Českého telekomunikačního úřadu.

Pramen: Smejkal, V.: Bezpečnost informačních systémů [5]

Výše uvedené zákonné úpravy vychází z právních předpisů Evropské unie případně se odkazují na mezinárodní normy. Předpisy EU aplikované do právního řádu ČR nebo jinak související jsou uvedeny v následující tabulce.

Tab. 2. Právní předpisy Evropské unie související s kybernetickou bezpečností

Zákon, norma	Popis
Směrnice EP a Rady 2013/40/EU	Směrnice EP a Rady 2013/40/EU o útocích na informační systémy, kterou se nahrazuje rámcové rozhodnutí Rady 2005/222/SW. Směrnice stanovuje minimální pravidla týkající se vymezení trestných činů a sankcí, spolupráce členských států v oblasti kybernetické kriminality.
Nařízení Evropského parlamentu a Rady č. 910/2014	Nařízení Evropského parlamentu a Rady č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS[6]). Nařízení implementuje pravidla pro elektronický podpis a otázky související s elektronickou identifikací a autentizací. Směrnice je promítnuto do národního právního rámce v zákonu č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Zákon, norma	Popis
Usnesení Evropského parlamentu 2017/2068 (INI)	Usnesení Evropského parlamentu ze dne 3. října 2017 o boji proti kyber kriminalitě (2017/2068 (INI)). Usnesení shrnuje současný stav a přináší návrhy opatření v oblastech prevence, posílení odpovědnosti a ručení poskytovatelů služeb, posílení spolupráce justice a policejních složek, prosazování právního státu v kyberprostoru. V usnesení je také požadováno zvýšení investic do infrastruktury za účelem zvýšení odolnosti vůči kybernetickým útokům.
Prováděcí nařízení EK ke Směrnici NIS	Prováděcí nařízení EK ke Směrnici NIS, které stanoví bezpečnostní opatření a parametry významnosti dopadu pro poskytovatele digitálních služeb. Prováděcí nařízení stanovuje pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148 (Směrnice NIS). Obsahem nařízení je upřesnění bezpečnostních opatření požadovaných po poskytovatelích digitálních služeb.

Pramen: Smejkal, V.: Bezpečnost informačních systémů

1.1.1 Zákon o kybernetické bezpečnosti

Základní normou upravující práva a povinnosti osob a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti je zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

Účelem zákona je především stanovení rámce pro spolupráci mezi veřejnou správou a státním sektorem při řešení kybernetických bezpečnostních incidentů. Z tohoto důvodu zákon zakotvuje pravidla a povinnosti s cílem zvýšení bezpečnosti kyberprostoru. Kyberprostor definuje zákon jako digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací. Působnost zákona je omezena obecně na oblast kybernetické bezpečnosti s výjimkou. Touto výjimkou jsou informační systémy určené pro nakládání s utajovanými informacemi. [6]

Zákon o kybernetické bezpečnosti definuje základní pojmy z oblasti kybernetické bezpečnosti. Přehled těchto pojmu uvádí následující tabulka.

6 eIDAS – electronic Identification, Authentication and trust Services

Tab. 3. Vymezení základních pojmů dle zákona o kybernetické bezpečnosti

Pojmy dle ZKB	Definice
Kritická informační infrastruktura	Prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.
Významný informační systém	Informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou, a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.
Významná síť	Síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.
Informační systém základní služby	Informační systém, na jehož fungování je závislé poskytování základní služby.
Základní služba	Služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech, a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z odvětví uvedených v §3m písm. i).
Digitální služba	Služba informační společnosti podle zákona upravujícího některé služby informační společnosti, která spočívá v provozování činností uvedených v §3 písm l), tj. : - online tržiště - internetové vyhledávače - cloud computing

Pramen: Smejkal, V.: Bezpečnost informačních systémů

1.1.2 Vyhláška o kybernetické bezpečnosti č. 82 /2018 Sb. (směrnice NIS)

Dále je třeba zmínit vyhlášku o kybernetické bezpečnosti č. 82/2018 Sb., která do právního rámce ČR implementuje směrnici Evropského parlamentu a Rady (EU) 2016/1148 (směrnice NIS). Obsahem vyhlášky je definice pravidel a metodik bezpečnostních opatření obecně formulovaných zákonem o kybernetické bezpečnosti.

Vyhláška o kybernetické bezpečnosti dle §2 vymezuje pojmy uvedené v následující tabulce.

Tab. 4. Vymezení základních pojmů dle vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti

Pojem	Definice
Administrátor	Osoba zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva.
Akceptovatelné riziko	Riziko, které je přijatelné pro povinnou osobu[7] a není nutné jej zvládat pomocí dalších bezpečnostních opatření.
Bezpečnostní politika	Soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv.
Hodnocení rizika	Celkový proces identifikace, analýzy a vyhodnocení rizik.
Hrozba	Potenciální příčina kybernetické bezpečnostní události nebo kybernetického incidentu, která může způsobit škodu.
Podpůrné aktivum	Technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému.
Primární aktivum	Informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém.
Riziko	Možnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu.
Řízení rizik	Činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik.
Systém řízení bezpečnosti informací	Část systému řízení povinné osoby založená na přístupu k rizikům informačního a komunikačního systému, která stanoví způsob ustanovení, zavádění, provozování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací a dat.
Technické aktivum	Technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na informační a komunikační systém.
Uživatel	Fyzická nebo právnická osoba a nebo orgán veřejné moci, který využívá aktiva.
Vrcholové vedení	Osoba nebo skupina osob, která řídí povinnou osobu, nebo statutární orgán povinné osoby.
Významný dodavatel	Provozovatel informačního nebo komunikačního systému a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému.
Významná změna	Změna, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko.
Zranitelnost	Slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

Pramen: *Smejkal*, V.: *Bezpečnost informačních systémů*

Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti je prováděcím předpisem zákona o kybernetické bezpečnosti, jak již bylo zmíněno výše, vyhláška tedy metodicky pokrývá jednotlivé aspekty kybernetické bezpečnosti v návaznosti na části zákona o

7 Pod pojem povinná osoba se rozumí osoba nebo orgán, který je podle zákona o kybernetické bezpečnosti povinen zavést bezpečnostní opatření, která povedou ke snížení rizika na akceptovatelnou míru

kybernetické bezpečnosti. Z pohledu analýzy dopadů kybernetické bezpečnosti se jedná o významný stavební kámen a z toho důvodu je vhodné zmínit jednotlivé paragrafy vyhlášky:

Tab. 5. Obsah vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti

Část vyhlášky	Obsah
§3 Systém řízení bezpečnosti informací	Definuje systém řízení informací (ISMS) ve shodě s normou ČSN EN ISO/IEC 27001. Jde o formalizovaný systém řízení a správy informačních aktiv organizace za účelem eliminace hrozeb. Dle normy ČSN EN ISO/IEC 27001 je tento systém postaven na principech modelu PDCA.
§4 Řízení aktiv	Asset management – řízení aktiv spojených s oblastí IS/IT (hmotných i nehmotných).
§5 Řízení rizik	V rámci §5 jsou definovány postupy související s procesem řízení rizik a povinnosti povinné osoby v souvislosti s uvedenými procesy. Paragraf staví především na normě ČSN EN ISO/IEC 27005.
§6 Organizační bezpečnost	Definuje úkoly povinné osoby v oblasti organizační bezpečnosti.
§8 Řízení dodavatelů	Definuje povinnosti týkající se řízení dodavatelů pro povinné osoby.
§9 Bezpečnost lidských zdrojů	Definuje povinnosti týkající se řízení lidských zdrojů pro povinné osoby.
§10 Řízení provozu a komunikací	Definuje povinnosti týkající se řízení provozu a komunikací pro povinné osoby.
§11 Řízení změn	Definuje povinnosti týkající se řízení změn pro povinné osoby.
§12 Řízení přístupu	Definuje povinnosti týkající se řízení přístupů pro povinné osoby.
§13 Akvizice, vývoj a údržba	Definuje povinnosti týkající se oblasti akvizic, vývoje a údržby pro povinné osoby.
§14 Zvládání kybernetických bezpečnostních událostí a incidentů	Definuje povinnosti v rámci zvládání kybernetických bezpečnostních událostí a incidentů pro povinné osoby.
§15 Řízení kontinuity činností	Definuje povinnosti týkající se oblasti řízení kontinuity činností pro povinné osoby.
§16 Audit kybernetické bezpečnosti	Definuje povinnosti týkající se oblasti auditu kybernetické bezpečnosti pro povinné osoby. V rámci auditu lze postupovat dle metodik popsaných v ČSN EN ISO/IEC 27006 a ČSN EN ISO/IEC 27007.
§17 Fyzická bezpečnost	Definuje povinnosti týkající se oblasti fyzické bezpečnosti pro povinné osoby.
§18 Bezpečnost komunikačních sítí	Definuje povinnosti týkající se oblasti bezpečnosti komunikačních sítí pro povinné osoby.
§19 Správa a ověřování identit	Definuje povinnosti týkající se oblasti správy a ověřování identit pro povinné osoby.
§20 Řízení přístupových oprávnění	Definuje povinnosti týkající se oblasti řízení přístupových oprávnění pro povinné osoby.
§21 Ochrana před škodlivým kódem	Definuje povinnosti týkající se oblasti ochrany před škodlivým kódem pro povinné osoby.
§22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	Definuje povinnosti týkající se oblasti logování, respektive zaznamenávání událostí pro povinné osoby.
§23 Detekce kybernetických bezpečnostních událostí	Definuje povinnosti týkající se oblasti detekce kybernetických bezpečnostních událostí pro povinné osoby.

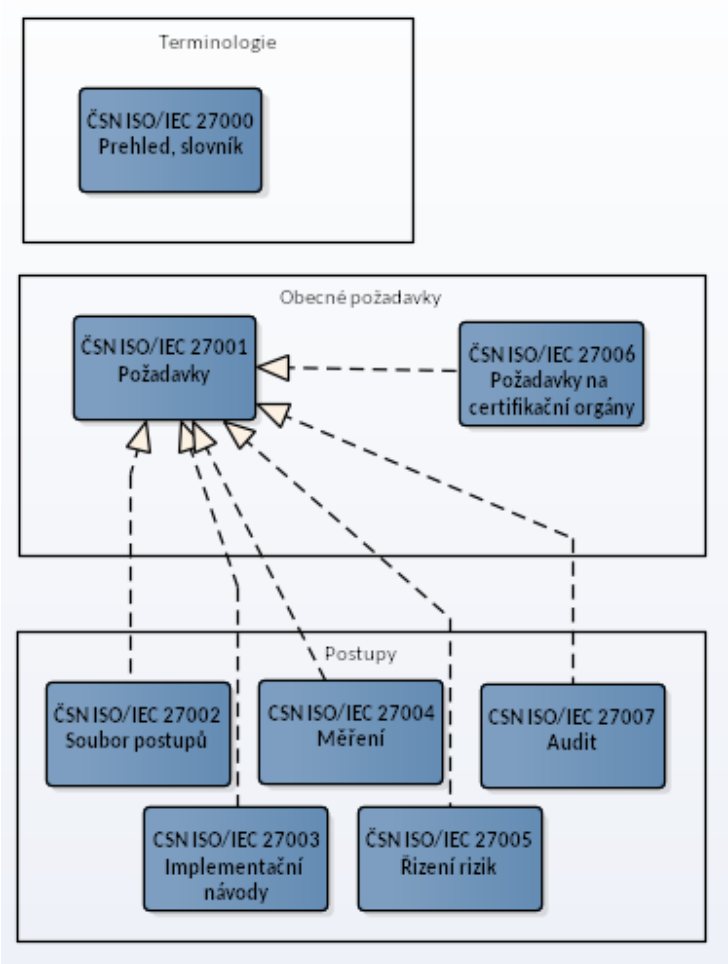
Část vyhlášky	Obsah
§24 Sběr a vyhodnocování kybernetických bezpečnostních událostí	Definuje povinnosti týkající se oblasti sběru a vyhodnocování kybernetických bezpečnostních událostí pro povinné osoby.
§25 Aplikační bezpečnost	Definuje povinnosti týkající se oblasti aplikační bezpečnosti pro povinné osoby.
§26 Kryptografické prostředky	Definuje povinnosti týkající se oblasti kryptografických prostředků pro povinné osoby.
§27 Zajišťování úrovně dostupnosti informací	Definuje povinnosti týkající se oblasti zajišťování úrovně dostupnosti informací pro povinné osoby.
§28 Průmyslové, řídící a obdobné specifické systémy	Definuje povinnosti týkající se oblasti průmyslových, řídících a obdobných specifických systémů pro povinné osoby.
§29 Digitální služby	Definuje povinnosti týkající se oblasti digitálních služeb pro povinné osoby.
§30 bezpečnostní politika a bezpečnostní dokumentace	Definuje povinnosti týkající se oblasti bezpečnostní politiky a bezpečnostní dokumentace pro povinné osoby.

Pramen: *Smejkal*, V.: *Bezpečnost informačních systémů*

1.1.3 Normy, standardy a metodiky

Jak již bylo zmíněno v předchozí kapitole, i zákon a vyhláška o kybernetické bezpečnosti ve svých pasážích reflektují mezinárodní normy z rodiny ISO/IEC 27000 aplikované v rámci národních norem řady ČSN EN ISO/IEC 27000. Rodina norem ČSN EN ISO/IEC 27000 pokrývá problematiku hodnocení bezpečnosti informačních systémů z různých pohledů, definuje rozsah bezpečnostních funkcí, zásady pro řízení bezpečnosti a stanovuje kritéria pro hodnocení situace z pohledu bezpečnosti informací. [7]

Následující diagram zobrazuje vztahy, respektive závislosti mezi jednotlivými vybranými normami rodiny ISO 27000.



Obr. 1. Struktura a vazby mezi vybranými normami rodiny ISO 27000

Jak naznačuje diagram, norma ISO 27001 definuje obecné požadavky na kybernetickou bezpečnost. Na tuto normu se následně odkazují normy obsahující metodiky pro jednotlivé oblasti kybernetické bezpečnosti. Podrobněji viz. následující tabulka.

Tab. 6. Přehled vybraných norem ISO/IEC 27000 a jejich implementace do systému národních norem ČSN

Označení	ČSN	Popis
ISO 27000	ČSN EN ISO/IEC 27000	Terminologický slovník
ISO 27001	ČSN EN ISO/IEC 27001:2014[8]	Norma systému řízení bezpečnosti informací. Je návodem pro organizace, jak postupovat při implementaci bezpečnostní politiky.

Označení	ČSN	Popis
ISO 27002	ČSN EN ISO/IEC 27002:2014	Metodika určená certifikačním autoritám používaná při udělování certifikátů.
ISO 27003	ČSN EN ISO/IEC 27003 (369790)[9]	Návod, metodika pro implementace norem rodiny ISO 27000.
ISO 27004	ČSN EN ISO/IEC 27004 (369790)	Metriky pro hodnocení zaváděných opatření.
ISO 27005	ČSN EN ISO/IEC 27005 (369790)[10]	Metodika pro analýzu bezpečnostních rizik informačních systémů.
ISO 27006	ČSN EN ISO/IEC 27006 (369790)	Rozšíření ISO 27001 a zajištění souladu s normou ISO 17021. Požadavky na certifikační autority.
ISO 27007	ČSN EN ISO/IEC 27007 (369790)	Metodiky a doporučení pro provádění auditu bezpečnosti.
ISO 27017	ČSN EN ISO/IEC 27017 (369710)	Rozšíření pokrývající problematiku bezpečnosti informací ukládaných v systémech cloud-computing.
ISO 27018	ČSN EN ISO/IEC 27018 (369710)	Soubor postupů na ochranu osobně identifikovatelných informací uložených v cloud systémech.
ISO 27033	ČSN EN ISO/IEC 27033-1 až 5 (369701)	Doporučení pro implementaci protiopatření v oblasti bezpečnosti sítí.
ISO 27034	ČSN EN ISO/IEC 27034-1 (369703)	Doporučení pro tvorbu, implementaci a užívání software.
ISO 27035	ČSN EN ISO/IEC 27035-1 (369799) a ČSN EN ISO/IEC 27035-2 (369799)	Řízení bezpečnostních incidentů. 1 - principy řízení incidentů 2 – směrnice pro plánování a řízení odezvy na incidenty

Označení	ČSN	Popis
ISO 27038	ČSN EN ISO/IEC 27038 (369847)	Doporučení pro správu a publikaci digitálních dokumentů.
ISO 27040	ČSN EN ISO/IEC 27040 (369849)	Doporučení pro bezpečné ukládání dat.

Pramen: Smejkal, V.: Bezpečnost informačních systémů

Z uvedených norem rodiny ISO 27000 je nutné poukázat na normy ISO 27001, ISO 27003, ISO 27005, ISO 27007, ISO 27017, které hrají významnou roli při řešení otázek kybernetické bezpečnosti v podnikové sféře. Pro potřebu analýzy rizik je pak stěžejní ČSN EN ISO/IEC 27005.

1.2 Infrastruktura informačních systémů podniků

Z pohledu kybernetických hrozeb, případně kybernetických útoků hraje zásadní roli infrastruktura daného podniku a jeho všeobecná připravenost na řešení bezpečnostních incidentů rozličného původu. Samotné téma infrastruktury informačních systémů je poměrně komplexní a jeho podrobnější popis se svým rozsahem vymyká cíli této práce. Tato kapitola se tedy omezí na představení podnikové infrastruktury na úrovní funkčních vrstev bez ambice na zobrazení hlubšího detailu.

Následující diagram ukazuje příklad topologie podnikové ICT infrastruktury. Jak již bylo zmíněno, jedná se o zobrazení na úrovni jednotlivých funkčních vrstev. V diagramu tedy nejsou promítnuty jednotlivé podnikové aplikace jako je např. aplikace pro vedení účetnictví, systémy pro správu klientských informací CRM či aplikace pro podporu výroby.[11]

Vysvětlení rolí jednotlivých funkčních vrstev:

- uživatelská vrstva: reprezentuje uživatele aplikací podnikových informačních systémů.

- network, síťová infrastruktura: reprezentuje veškerou technologii nutnou pro zajištění komunikačního propojení částí podnikových informačních systémů (kabeláž, routery, switche, repeatery, WI-FI hotspoty, VPN, proxy a firewall servery, DNS servery)[8]

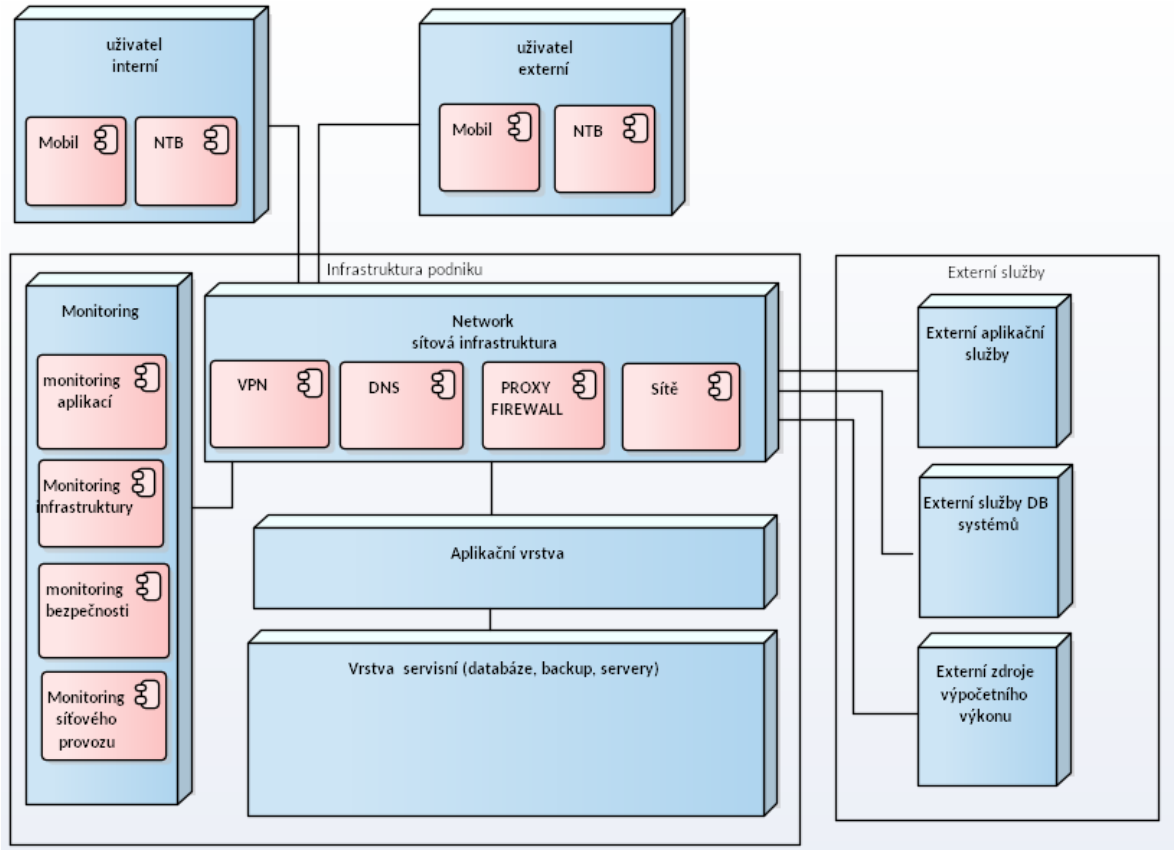
8 routery, switche, repeatery, WI-FI hotspoty – myšleno aktivní síťové prvky

- monitoring: vrstva zajišťující dohled nad funkčností prvků podnikových systémů z hlediska dostupnosti, výkonosti, využití resp. zneužití (bezpečnosti)

- aplikační vrstva: představuje veškeré podnikové aplikace

- servisní vrstva: poskytuje zázemí pro provoz aplikací, do této vrstvy mimo základního serverového vybavení řadíme i databáze, systémy zálohy (backup) a obnovy (recovery). [12], [13],[14]

- externí služby: reprezentují externí aplikace, jejich služby jsou součástí procesů zpracování dat v rámci podnikových procesů, jedná se například o služby poskytované státními autoritami, správci domén, případně služby cloud computingu, atp.



Obr. 2. Obecný diagram podnikové infrastruktury, vlastní zpracování dle Fowler, M.: Patterns of Enterprise Application Architecture

1.3 Kybernetické útoky

Kybernetický útok se postupně stává jednou z nejzávažnějších hrozeb, která může postihnout celou škálu subjektů od privátních osob až po velké korporace a státní instituce. Závažnost problému umocňuje také fakt, že cíl útoku může být napaden z libovolně vzdáleného místa připojeného do infrastruktury Internetu. Jedním z dalších faktorů je také asymetrie v nákladech a vynaloženém úsilí na straně útočníka ve srovnání s dopady na straně postiženého subjektu[1].

Vývoj technologií v posledních letech kybernetickým útokům poměrně výrazně nahrává. Zmíněná dostupnost a konektivita se neustále zlepšuje, tlačená potřebami komerčních subjektů jako jsou poskytovatelé internetového televizního vysílání, dodavatelé komponent a zařízení IoT[9] a v neposlední řadě automobilového průmyslu. Z pohledu útočníka tedy průběžně roste jak počet potenciálních cílů, tak se zlepšuje jejich dostupnost. Nezanedbatelný vliv na růst příležitostí ke kybernetickému útoku má také trend poměrně masivního přechodu na práci z domova, který lze pozorovat v průběhu roku 2020 a je zapříčiněn vládními opatřeními zavedenými ve snaze o zmírnění dopadu pandemie COVID-19. Práce z domova přináší širokou řadu nových bezpečnostních výzev, které souvisí s propojování firemního hardware se soukromým zařízením různého typu, přičemž nad těmito propojeními nemá zpravidla plnou kontrolu ani zodpovědná osoba zaměstnavatele a zpravidla ani sám zaměstnanec. Služební notebook se takto vlastně připojuje do potenciálně toxického prostředí tvořeného nezabezpečenou sítí, ve které se může nacházet řada zařízení nejasného původu a s neznámým programovým vybavením, např. chytré televize, zařízení IoT, chytré telefony a tablety. Vezmeme-li pak v úvahu to, že nejběžnější strategií útočníka je plošné skenování známých slabých míst, pak se dá konstatovat, že vývoj v roce 2020 přináší z pohledu kybernetické kriminality celou řadu nových příležitostí. [15]

1.3.1 Typy útoku z pohledu zacílení

Z tohoto pohledu lze kybernetické útoky rozdělit na kategorií útoků cílených a kategorii útoků plošných:

Cílené útoky – útok zaměřen na konkrétní subjekt, organizaci nebo osobu. Útočník hledá zranitelnosti za použití rozličných metod od sběru dat na bázi sociálního inženýrství po

9 IoT – Internet of Things

skenování infrastruktury vystavené do vnějšího prostředí. Cílem tohoto typu útoku bývá zpravidla :

- odcizení dat, přihlašovacích údajů, interní podniková informace, klientská databáze,

- odcizení finančních prostředků,

- ochromení infrastruktury oběti z důvodu konkurenčního boje,

- defacement (změna webových stránek za účelem poškození dobrého jména)

- získání kontroly nad infrastrukturou z důvodu využití výpočetního výkon pro další aktivity,

- smazání nebo zašifrování dat. [1]

Plošné útoky – v případě plošného útoku je využito známé slabiny k proniknutí do vystavené infrastruktury a převzetí kontroly nad tímto zařízením (získání read/write nebo administrátorského přístupu atp.), případně zapojení ovládnutého výpočetního zařízení do sítě botnetů. Dalším krokem je pak využití takto ovládnutých zařízení např. k další vlně útoku, či rozesílání SPAMu atp. Z pohledu četnosti výskytu vedených útoků, jednoznačně převažují útoky plošné. V literatuře[10] jsou však popsány i případy kombinované strategie, kdy nejprve útočník pomocí plošného útoku získá síť botnetů pro účely cíleného útoku na zvolený cíl. Motivací pro provedení plošného útoku je:

- získání přihlašovacích údajů,

- získání čísel platebních karet,

- získání výpočetního výkonu ovládnutých zařízení,

- smazání nebo zašifrování dat. [1]

1.3.2 Rozčlenění kybernetických útoků

Následující tabulka č. 7 obsahuje rozčlenění způsobu provedení útoku, respektive způsob přenosu škodlivého aplikačního kódu. V tabulce jsou uvedeny a popsány známé způsoby šíření nebo provedení kybernetického útoku.

10 Šulc, V.: Kybernetická bezpečnost

Tab. 7. Způsob šíření kybernetického útoků

Typ přenosu (vektor přenosu)	Popis	Označení
drive-by download	Získání škodlivého software při návštěvě upravené webové stránky.	D
phishing	Získání škodlivého software zaslaného v formě přílohy emailu.	P
aplikace obsahující trojského koně	Upravená legální aplikace, která je obohacena o skrytý škodlivý aplikační kód.	T
virus	Na pozadí skrytě běžící aplikační kód, který samovolně rozšiřuje svoje vlastní kopie do zpřístupněných oblastí.	V
macrovirus	Skript naprogramovaný skriptovacím jazykem VBA, který je omezen na ekosystém MS Office. Šíří se tedy jako makro např. v souborech MS Excel.	m
worm	Tento škodlivý kód se šíří prostřednictvím emailu, a to tím způsobem, že sám sebe odesílá do jiných emailových schránek.	W
malvertising	Získání škodlivého software při návštěvě upravené webové stránky.	M

Pramen: vlastní zpracování na základě Šulc, V.: Kybernetická bezpečnost

V následující tabulce je uveden přehled známých kybernetických útoků. Pro přehlednost jsou typy možných útoku uvedeny v tabulce spolu s možným způsobem přenosu nebo cestou jíž může daný útok probíhat. Sloupec „Přenos“ obsahuje znak označující typ přenosu dle tabulky č. 7. Zpravidla je pro daný typ útoku přípustných nebo známých více způsobů přenosu. Z toho důvodu je ve sloupci „Přenos“ tabulky č. 8 uvedena vždy kombinace znaků označujících možné způsoby přenosu, respektive způsoby šíření daného kybernetického útoku.

Tab. 8. Členění typů možných útoků vedených na podnik z kyberprostoru

Typ útoku	Popis	Přenos
botnet	Ovládnutí napadeného výpočetního zařízení pouze za účelem využití jeho výpočetní síly pro další aktivity.	DPTVWM
Ransomware	Jde o útok kódem, který provede zašifrování uloženého obsahu na dostupných discích za účelem získání výkupného případně zamaskování další aktivit, blokující výpočetní techniku. Tento typ útoku je zpravidla motivován snahou o získání výkupného s příslibem obnovení funkčního stavu po zaplacení.	DPTVWM
Spyware	Krádež dat včetně přihlašovacích údajů, odposlech klávesnice při zadávání hesla atp. Tento typ škodlivého software se používá také pro získání platebních informací a údajů k platebním kartám.	DPTVWM
DDoS	Útok je postavený na zahlcení napadeného zařízení záplavou požadavků, která způsobí změnu stavu zařízení, ve kterém odmítá poskytovat služby.	
APT	Advanced persistent treat - přetrvávající dlouhodobé hrozby. Jedná se o cílené útoky, zpravidla kombinované, dlouhodobé útoky na vybraný cíl.	

Pramen: vlastní zpracování na základě Šulc, V.: Kybernetická bezpečnost

2 ANALÝZA RIZIK

Záměrem práce je ukázat vztah mezi kybernetickou hrozbou a jejím možným dopadem do ekonomické oblasti podniku. Jedním z nezbytných faktorů pro určení možného dopadu hrozby je určení rizika dané hrozby. Následující kapitoly tedy přinášejí stručný nástin problematiky analýzy rizik se zaměřením na vybrané oblasti.

2.1 Základní pojmy analýzy rizik

Jak uvádí [16] pojem riziko je pojem historický, který vyjadřuje „vystavení se nepříznivým okolnostem“. V oblasti ICT a její aplikace v prostředí podniku je pak třeba jako riziko vnímat každý nepříznivý jev s potenciálním dopadem do aktiv podniku. Samotná úroveň rizika je určována hodnotou aktiva, se kterým je riziko spojeno a úrovní hrozby.

Mimo pojmu rizika je vhodné pro potřeby zpracování analýzy rizik definovat i další pojmy:

- aktivum = z pohledu analýzy rizik se jedná o vše co má pro subjekt nějakou hodnotu, aktiva pak dělíme na hmotná (nemovitosti, vybavení, stroje, servery, atd.) a nehmotná (data, informace, licence, goodwill, veškeré duševní vlastnictví, autorská práva atd.). Základní vlastností aktiva je především jeho hodnota.

- hrozba = jev, který má nežádoucí vliv na aktiva podniku. Příčina způsobené škody. U hrozby hodnotíme:

    1, její nebezpečnost

    2, frekvenci výskytu

    3, zdroj (motivaci)

- zranitelnost = slabina daného aktiva, která může být hrozbou využita pro realizaci svého vlivu (dopadu). Atributy zranitelnosti jsou:

    1, citlivost: náchylnost k utrpění újmy danou hrozbou

    2, kritičnost: priorita nebo důležitost aktiva

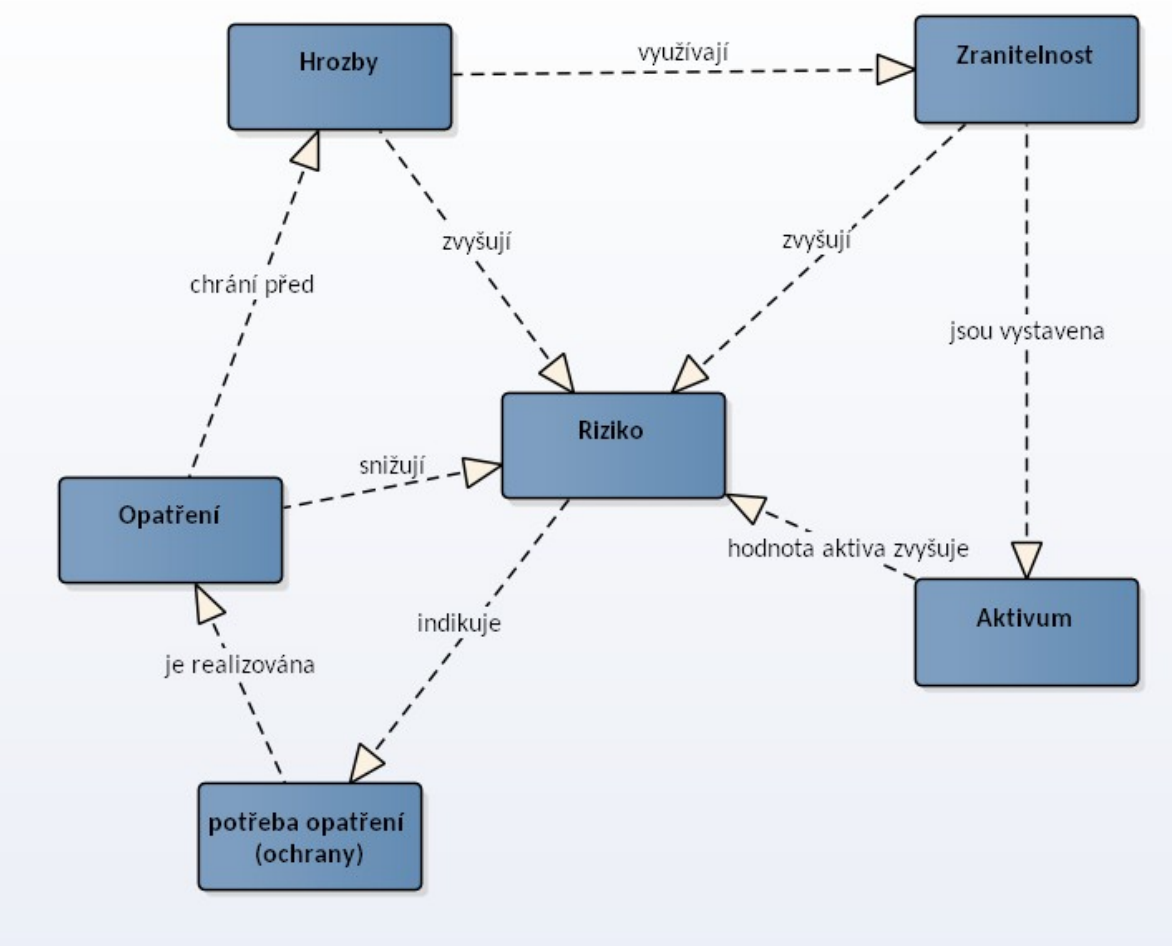
- opatření (protiopatření) = konání vedoucí ke zmírnění dopadu dané hrozby na dané aktivum. Atributy opatření jsou:

1, efektivita

2, cena (náklady)

- riziko = míra ohrožení aktiva danou hrozbou. Atributem rizika je: úroveň rizika.

- rizikovost = kombinace pravděpodobnosti a rozsahu možného dopadu na aktivum [17]



Obr. 3. Vztah mezi jednotlivými pojmy analýzy rizik. Pramen: vlastní zpracování dle Smejkal, V., Rais, K.: Řízení rizik ve firmách a jiných organizacích

2.2 Postup při analýze rizik

Postup prováděný v rámci analýzy rizik lze shrnout do následujících bodů:

1, stanovení hranice analýzy = vymezení aktiv podniku, která budou zahrnuta do prováděné analýzy,

2, identifikace aktiv = charakteristika aktiv zahrnutých do analýzy rizik včetně stanovení jejich hodnoty,

3, identifikace hrozeb = popis hrozeb relevantních pro aktiva zahrnutá do analýzy,

4, analýza hrozeb a zranitelnosti aktiv = hodnocení potencionálních dopadů na jednotlivá aktiva,

5, stanovení pravděpodobnosti jednotlivých jevů = určení pravděpodobnosti výsky tu dané hrozby. [16]

2.3 Metody analýzy rizik

Ke zjištění hodnot veličin zmíněných výše lze použít přístup buď kvantitativní, kvalitativní, případně kombinaci kvalitativního a kvantitativního přístupu.

2.3.1 Kvantitativní metoda

Metoda vychází z matematického výpočtu stanovení rizika. Vstupem pro výpočet je známá frekvence výskytu hrozby. Výstupem metody je obvykle vyjádření dopadu hrozby na dané aktivum, tedy vyjádření škody v konkrétní částce. Lze říci, že slabinou kvantitativních metod je jejich závislost na kvalitě vstupních dat.

Pro potřeby hodnocení bezpečnostních hrozeb v oblasti ICT jsou pak nejčastěji používány metodiky CRAMM[11] nebo COBRA[12].

2.3.2 Kvalitativní metoda

Principem kvalitativní metody je stanovení kombinace závažnosti dopadu hrozby, např. stupnicí <1;10> nebo slovním ohodnocením <nízká, střední, vysoká> a pravděpodobnosti výskytu dané hrozby. Stanovení závažnosti je prováděno u těchto metod expertním odhadem. Je tedy nutné toto hodnocení považovat za poměrně subjektivní.

11 CRAMM – CCTA Risk and Management Method (CCTA – Central Computerand Telecommunication agency)
12 COBRA – Co-benefits Risk Assessment

2.3.3 Kombinované metody

Kombinované metody spojují výhody kvantitativního i kvalitativního přístupu. Metody staví na číselných vstupních datech, na něž jsou však aplikovány škály definované expertním způsobem pro potřeby kvalitativního hodnocení.

2.4 Řízení rizik z pohledu kybernetické bezpečnosti

Proces řízení rizik v oblasti kybernetické bezpečnosti zachycuje v rámci národní legislativy vyhláška č. 82/2018 Sb. §4, §5. Ve svých přílohách dále vyhláška uvádí kategorizaci hrozeb a zranitelnosti (příloha vyhlášky č.3), hodnocení rizik (příloha vyhlášky č.2) a hodnocení možných dopadů na aktiva organizace (příloha vyhlášky č. 1).

2.5 Hrozby

V předchozích kapitolách byly představeny možnosti napadení infrastruktury útočníkem. Toto napadení může mít přímý či nepřímý dopad na aktiva společnosti zasažené útokem. Problematikou členění hrozeb a jejich potenciálních dopadů se zabývá norma ČSN EN ISO/IEC 27005. Norma definuje takzvané generické hrozby. Jedná se o výčet, který je obecný a popisuje základní typy hrozeb. K tomuto výčtu je nutné doplnit hrozby, které je možné identifikovat pro danou organizaci, respektive její informační systémy. Jak uvádí [18] je doporučováno v rámci procesu identifikace hrozeb provézt jejich rozčlenění:

- dle úmyslu na: - hrozby úmyslné
  - hrozby náhodné
- dle původu na: - vnitřní hrozby
  - vnější hrozby

Tab. 9. Členění hrozeb dle původu hrozby a úmyslu

hrozba	náhodná	úmyslná
externí	Přírodního původu	hacking
interní	Technické selhání, lidská chyba	sabotáž

Pramen: Požár, J.: Informační bezpečnost

3 METODY OCEŇOVÁNÍ NEHMOTNÝCH AKTIV

Následující kapitoly představí charakteristiky jednotlivých typů nehmotných aktiv, jejich kategorizaci a metody oceňování.

Pod pojmem nehmotná aktiva rozumíme dle občanského zákoníku práva nebo jiné majetkové hodnoty, které nespadají do kategorií definovaných §118 a §119. Účetní standard IFRS IAS 38 pak definuje nehmotná aktiva následovně:

- nepeněžní aktivum bez hmotné povahy (přestože je zachyceno na hmotném nosiči, není téže povahy)

- je výsledkem minulých událostí (koupě licence nebo vývoj)

- je identifikovatelné (podmínka je splněna pokud lze aktivum oddělit od podniku a nebo k danému statku existuje smluvní nebo zákonné právo)

- pravděpodobně v budoucnu přinese ekonomický užitek

- je kontrolovatelné (držitel má jistou exkluzivitu na budoucí prospěch z aktiva) [19][20], [21]

3.1 Klasifikace nehmotných aktiv

Dle [19] je považována za nejúplnější klasifikaci nehmotných aktiv definice dle IFRS: IAS38 - Nehmotná aktiva a IFRS 3 - Podnikové kombinace. Norma IAS 38 především předepisuje způsob vykazování nehmotných aktiv v účetní závěrce podniku. Norma IFRS 3 definuje metody oceňování nově nabytých aktiv v rámci nákupů a akvizic. [22], [23]

Tab. 10. Členění vybraný nehmotných aktiv dle IFRS 3[13]

Marketing	Zákazníci	Smlouvy	Technologie	Umění
Ochranné známky	Seznamy zákazníků	Licence	Patenty	Filmová díla
Nechráněná označení	Smluvní zákaznické vztahy	Franšízy	Užitné vzory	Obrazy
Certifikační označení	Nesmluvní zákaznické vztahy	Nájemní smlouvy	Obchodní tajemství	Hudební nahrávky
Obchodní firma	Nevyřízené objednávky	Stavební povolení	Software	Jiná díla
Domény		Vysílací práva	Databáze	

13 Výběr položek obsažených v IFRS 3 vhodný pro testování při akvizicích na splnění podmínek pro vykázání do bilance

Marketing	Zákazníci	Smlouvy	Technologie	Umění
Dohody o nekonkurenci		Zaměstnanecké smlouvy	Průmyslové vzory	
Názvy novinových titulů		Manažerské smlouvy		
Firemní jednotné ošacení		Vysílací smlouvy		

Pramen: Svačina, P.: Oceňování nehmotných aktiv, IFRS 3

3.2 Metody oceňování nehmotných aktiv

Úkolem při oceňování nehmotného aktiva je primárně určení tržní hodnoty oceňovaného aktiva. Následující kapitoly představí vybrané metody pro oceňování nehmotných aktiv včetně naznačení způsobu výpočtu a vhodnosti aplikace pro vybraná nehmotná aktiva.

3.2.1 Metoda násobitelů

Metoda je vhodná pro typy nehmotných aktiv, u nichž existuje srovnání s nehmotným aktivem se známou tržní cenou. Tato metoda je tedy vhodná dle [19] pro určité typy doménových jmen a pro soubory vybraných patentů a přihlášek.

Matematicky lze vyjádřit vztah mezi zjišťovanou hodnotou aktiva a hodnotou aktiva se známou tržní cenou následovně:

$$H_{NA} = C_S \, x \, \frac{X_{NA}}{X_S}$$

kde H_{NA} výsledná hodnota nehmotného aktiva

C_S známá tržní cena srovnatelného (referenčního) nehmotného aktiva

X_S klíčová ekonomická charakteristika referenčního nehmotného aktiva (EBITDA, EBIT, tržby, návštěvnost domény)

X_{NA} klíčová ekonomická charakteristika oceňovaného nehmotného aktiva (EBITDA, EBIT, tržby, návštěvnost domény)

Z uvedeného vztahu je zřejmé, že použitelnost metody je dána dvěma faktory:

- zda je možné nalézt obdobné nehmotné aktivum ke srovnání

- na vymezení ekonomického kritéria vhodného pro stanovení srovnávacího koeficientu.

3.2.2 Metoda nákladů reprodukce a nahrazení

Metoda je postavena na předpokladu, že hledaná tržní cena nehmotného aktiva odpovídá ceně, za kterou je typický kupující a typický prodávající ochoten toto aktivum směnit. Ochota ke směně je pak dána tím, že obě strany nabyly přesvědčení, že náklady reflektují potenciální užitek plynoucí z daného aktiva.

Dle [19] jsou pro účely ocenění nehmotného aktiva vhodné metody:

- metoda nákladů a reprodukce

- metoda nákladů nahrazení

Matematické vyjádření metody nákladů reprodukce:

$$H_{NA} = \sum_{i=1}^{n} \sum_{t=0}^{T} [N_i \, x \, (1 + I_{CPI})^t \, x \, (1 + i)^t] \, x \, (1 - A) + TAB$$

kde H_{NA} výsledná hodnota nehmotného aktiva

N_i hodnota nákladové položky vynaložené na vytvoření původního nehmotného aktiva

I_{CPI} míra změny ceny položek N_i mezi obdobími

t datum vynaložení nákladové položky

T datum ocenění nehmotného aktiva

i náklady ušlé příležitosti

A amortizace vynaložených nákladů k datu ocenění T

TAB přínos, který přináší možnost daňového odpisu

Matematické vyjádření metody nákladů nahrazení:

$$H_{NA} = \sum_{i=1}^{n} N_i x (1+i)^t + TAB$$

kde N_i hodnota nákladové položky vynaložené na vytvoření nehmotného aktiva srovnatelné užitečnosti

3.2.3 Výnosové metody

Dle [19] je princip určení hodnoty nehmotného aktiva postavené na výnosovém přístupu postaven na určení rozdílu hodnoty podniku, který dané aktivum užívá a hodnotou podniku, které takové či srovnatelné aktivum neužívá.

S ohledem na složitost zjištění rozdílů hodnot celých podniků se v praxi užívají pro zjištění zmíněného rozdílu jiné, vhodnější ukazatele. Jedná se například o rozdíl v cash-flow, případně rozdíl v zisku či ztrátě.

3.2.4 Metoda licenční analogie

V případě této metody dochází k odvození tržní hodnoty nehmotného aktiva z hodnoty licenčních poplatků, které jsou spojeny s oceňovaným nehmotným aktivem. Zde se má za to, že velikost licenčních poplatků odráží ekonomický přínos získaný nabytím licence.

Způsob užití metody má 3 způsoby:

- analogie nabytí licence
- analogie poskytnutí licence
- kombinovaná analogie

Matematicky lze metodu licenční analogie vyjádřit následujícím způsobem:

$$H_{NA} = \sum_{t=1}^{n} \left(\frac{T_t x PM x LP x K_t x (1-d)}{(1+i)^t} \right) + TAB$$

kde H_{NA} výsledná hodnota nehmotného aktiva

T_t plán objemu prodeje výrobku obsahujícího oceňované nehmotné aktivum

PM podíl nehmotného aktiva na objemu prodejem výrobku obsahujícího nehmotné aktivum

LP licenční poplatek (sazba) - údaj v procentech

K_t index zastarání (týká se pouze designu a některých technických řešení)

i náklady ušlé příležitosti

t životnost nehmotného aktiva

d sazba daně z příjmu

n životnost nehmotného aktiva

TAB přínos, který přináší možnost daňového odpisu

3.2.5 Metoda podílu na zisku

Metoda je založena na odhadu hodnoty nehmotného aktiva na základě jeho podílu na zisku, kterého bylo dosaženo užitím daného nehmotného aktiva.

Matematicky lze výpočet metody podílu na zisku vyjádřit následujícím způsobem:

$$H_{NA} = \sum_{t=1}^{n} \left(\frac{T_t \, x \, ZM \, x \, PM \, x \, LP^{ZM} \, x \, K_t \, x \left(1-d\right)}{\left(1+i\right)^t} \right) + TAB$$

kde H_{NA} výsledná hodnota nehmotného aktiva

T_t plán objemu prodeje výrobku obsahujícího oceňované nehmotné aktivum

ZM zisková marže z prodeje výrobku

PM podíl nehmotného aktiva na objemu prodejem výrobku obsahujícího nehmotné aktivum

LP licenční poplatek (sazba) - údaj v procentech

K_t index zastarání (týká se pouze designu a některých technických řešení)

i náklady ušlé příležitosti

t životnost nehmotného aktiva

d sazba daně z příjmu

TAB přínos, který přináší možnost daňového odpisu

3.2.6 Metody prémií

Metody prémií jsou založeny na odhadu vlivu nehmotného aktiva na ekonomický přínos. Tento odhadnutý vliv je považován za alternativní způsob výpočtu hypotetické licenční úplaty. Tato úvaha je postavena na předpokladu, že tržní zájemce nebude ochoten zaplatit za nehmotné aktivum více než je dodatečný přínos odpovídající odhadnuté hodnotové prémii [19]. Pro účely určení hodnoty nehmotného aktiva rozlišujeme následující typy prémií:

- cenová prémie
- zisková prémie
- nákladová prémie
- prémie výnosnosti.

V případě **cenové prémie** je odhad ceny nehmotného aktiva založen na rozdílu mezi cenou výrobku, který toto nehmotné aktivum neobsahuje a cenou výrobku, který oceňované aktivum obsahuje. Matematicky lze hodnotu nehmotného aktiva vyjádřit následujícím způsobem:

$$H_{NA} = \sum_{t=1}^{n} \left(\frac{Q_t \, x \left(P_{ts} - P_{tbez} \right) x \, K_t \, x \left(1 - d \right)}{\left(1 + i \right)^t} \right) + TAB$$

kde H_{NA} výsledná hodnota nehmotného aktiva

Q_t objem prodeje výrobku

P_{tS} cena výrobku obsahujícího oceňované nehmotné aktivum

P_{tBEZ} cena výrobku bez oceňovaného nehmotného aktiva

K_t index zastarání (týká se pouze designu a některých technických řešení)

i náklady ušlé příležitosti

t životnost nehmotného aktiva

d sazba daně z příjmu

TAB přínos, který přináší možnost daňového odpisu

Aplikací marže místo ceny výrobku lze dosáhnout výsledku ocenění nehmotného aktiva na základě **ziskové prémie**, kterou lze vyjádřit matematicky:

$$H_{NA} = \sum_{t=1}^{n} \left(\frac{Q_t \, x \left(ZM_{ts} - ZM_{tbez} \right) x \, K_t \, x \left(1 - d \right)}{\left(1 + i \right)^t} \right) + TAB$$

kde H_{NA} výsledná hodnota nehmotného aktiva

Q_t objem prodeje výrobku

ZM_{tS} prodejní marže výrobku obsahujícího oceňované nehmotné aktivum

Zm_{tBEZ} prodejní marže výrobku bez oceňovaného nehmotného aktiva

Obdobně lze upravit výpočet pro určení hodnoty nehmotného aktiva na základě předpokladu, že vliv aktiva se promítá čistě do hodnoty nákladů. V takovém případě hovoříme o **nákladové prémii:**

$$H_{NA} = \sum_{t=1}^{n} \left(\frac{Q_t \, x \left(N_{tbez} - N_{tS} \right) x \, K_t \, x \left(1 - d \right)}{\left(1 + i \right)^t} \right) + TAB$$

kde H_{NA} výsledná hodnota nehmotného aktiva

Q_t objem prodeje výrobku

N_{tS} průměrné provozní náklady výrobku obsahujícího oceňované nehmotné aktivum

N_{BEZ} průměrné provozní náklady výrobku bez oceňovaného nehmotného aktiva

Metoda výpočtu **prémie z výnosnosti kapitálu** pak staví ocenění nehmotného aktiva na srovnání ukazatele výnosnosti kapitálu u podniku, který aktivem disponuje s podnikem, který aktivem nedisponuje:

$$H_{NA} = \sum_{t=1}^{n} \left(\frac{A_t \, x \left(ROA_{tS} - ROA_{tBEZ} \right) x \, K_t \, x \left(1 - d \right)}{\left(1 + i \right)^t} \right) + TAB$$

kde H_{NA} výsledná hodnota nehmotného aktiva

A_t provozně potřebná aktiva podniku užívajícího oceňované nehmotné aktivum

ROA_{tS} rentabilita aktiv podniku, který užívá oceňované nehmotné aktivum

ROA_{tBEZ} rentabilita aktiv podniku, který oceňované nehmotné aktivum neužívá

3.2.7 Metoda čisté současné hodnoty

Metoda čisté současné hodnoty staví způsob ocenění nehmotného aktiva na sledování cash-flow, přičemž výsledek poskytnutý touto metodou nelze chápat jako absolutní vyjádření hodnoty nehmotného aktiva, ale je třeba jej vnímat jako mezní hodnotu licenčního poplatku. Uvedená metoda však nerozlišuje hodnoty jednotlivých nehmotných aktiv, naopak u této metody je možné získat obrázek pouze za celek, kterým může být sledovaný ucelený projekt nebo výroba podniku. Z tohoto důvodu se u této metody běžně aplikuje analogie obvyklého rozdělení zisku mezi poskytovatele a nabyvatele v rozsahu 20 – 40%.

Matematické vyjádření:

$$CSH = -I + \sum_{t=1}^{n} \frac{CF_t}{(1+i)^t}$$

$$CSH = -I + \sum_{t=1}^{n} \frac{T_t x\, ZM_t x(1-d) + O_t}{(1+i)^t}$$

$$CSH = -I + \sum_{t=1}^{n} \frac{T_t x\,(ZM_t - T_t x\, LP)\, x(1-d) + O_t}{(1+i)^t}$$

kde H_{NA} výsledná hodnota nehmotného aktiva

I, CF investiční výdaj a peněžní toky

T_t čisté tržby z licenční výroby

ZM_{tS} prodejní marže výrobku obsahujícího oceňované nehmotné aktivum (licence)

O_t odpisy

Zde pak při dosazení CSH=0 lze po úpravě vztahu získat hodnotu LP_{MAX}:

$$0 = -I + \sum_{t=1}^{n} \frac{T_t x\,(ZM_t - T_t x\, LP_{MAX})\, x(1-d) + O_t}{(1+i)^t}$$

3.2.8 Diskontní míra pro výnosové oceňování nehmotných aktiv

Tato metoda staví na předpokladu existence tendence ke spotřebě současného kapitálu na úkor budoucí spotřeby. U této metody se tedy zohledňuje diskontování postavené na principu obětované příležitosti. Výše obětované příležitosti je dána, obdobně jako u jiných typů aktiv, časovým horizontem a rizikem podstoupeným při investici.

Oceňování se provádí metodou srovnávací, kdy se hledá analogie k danému případu. Tento aspekt je však určitým úskalím této metody, neboť je poměrně složité pro řadu druhů nehmotných aktiv nalézt odpovídající alegorii, která by umožnila přesněji kvantifikovat danou diskontní míru.

Pro stanovení diskontní míry je dle [19] nejvhodnější užití modelu CAPM.

Model CAPM[14] umožňuje aplikaci následujících analogií:

- analogie vypořádání licenčního obchodu, kde se vychází z úvahy, že lze porovnávat ekonomické transakce jako je nákup licencí s transakcí s daným nehmotným aktivem,

- analogie financování vlastním kapitálem, kde se bere v potaz způsob financování daného nehmotného aktiva,

- analogie podniku s vysokým podílem nehmotných aktiv, kde se pro výběr analogie hledá podnik s vysokým podílem nehmotných aktiv ve svém majetku. Pro účely výběru takového podniku je doporučován některý z tímto směrem zaměřených akciových indexů, vhodným příkladem je dle [19] Ocean Tomo 300 Patent Index[15].

3.2.9 Metoda nadměrných zisků a proces alokace kupní ceny podniku (PPA[16])

Metoda nadměrných zisků je komplexní metoda pro ocenění a určení kupní ceny podniku (Purchase Price Allocation) podle IFRS 3. Metoda tedy nachází využití především při akvizicích.

Tato metoda je vhodná pro oceňování specifických nehmotných aktiv, u nichž je uplatnění výnosových a ostatních dříve zmíněných metod obtížné. Mezi tyto aktiva patří:

- vztahy se zákazníky

14 CAPM – Capital Asset pricing model

15 Index obsahuje 1000 nejlikvidnějších cenných papírů obchodovaných na amerických burzách rozčleněných do 50 patentových skupin dle metodiky OT PatentRatings.

16 PPA – Purchace price allocation

- unikátní software

- výsledky výzkumných projektů

- unikátní licence k podnikání.

Ocenění nehmotného aktiva je v případě této metody založeno na principu nájmu aktiv. Oceňované aktivum je u této metody vyčleněno od ostatních aktiv, která jsou zde vnímána pouze v roli nájmu. U těchto ostatních aktiv se bere v potaz jejich cena nájmu, o který je ponížen zisk. Zbývající hodnota pak odpovídá hodnotě oceňovaného aktiva.

Matematické vyjádření výpočtu hodnoty nehmotného aktiva metodou nadměrných zisků:

$$H_{NA} = \sum_{t=1}^{n} \sum_{i=1}^{m} \frac{PVH_t \, x \, (1-d) - nájemné_t^i}{(1+i)^t} + TAB$$

po úpravě pak:

$$H_{NA} = \sum_{t=1}^{n} \sum_{i=1}^{m} \frac{PVH_t \, x \, (1-d) - (H_i \, x \, r_i)_t}{(1+i)^t} + TAB$$

kde PVH_I provozní výsledek hospodaření před zdaněním

H_i hodnota i-tého aktiva užitého při výrobě

r_i tržní nájemné

d sazba daně z příjmu

i požadovaná výnosnost pro oceňované nehmotné aktivum

3.2.10 Metoda podle zákona o oceňování majetku

Mimo zmíněné metody právní rámec České republiky obsahuje zákonné nástroje pro oceňování nehmotných aktiv. Tyto nástroje staví na zákonu č. 151/1997Sb., o oceňování majetku a vyhlášce č. 540/2002Sb., k zákonu o oceňování majetku.

Metody popsané v uvedených zákonech řeší ocenění nehmotného aktiva pro specifické účely popsaných v dalších zákonných úpravách, jde například o účely výpočtu daní, notářských, správních a soudních poplatků atp.

Dle zákona se nehmotné aktivum oceňuje na základě diskontovaných budoucích ročních čistých výnosů, které vyplývají z užívání nehmotného aktiva.

Matematické vyjádření:

$$C = \sum_{j=1}^{n} \frac{z_j}{\left(1 + \frac{p}{100}\right)^j}$$

kde z_j roční čistý výnos z užívání práva

p míra kapitalizace

j rok, ve kterém je aktivum užíváno

n počet let

II. METODICKÁ ČÁST

4 SBĚR A PŘÍPRAVA DAT

4.1 Sběr dat pro analýzu aktiv

Výběr aktiv pro potřeby analýzy dopadu kybernetických hrozeb u společnosti, jejíž charakter odpovídá malému nebo střednímu podniku nelze provézt pouze na základě dat, která poskytuje účetní evidence. Důvodem je především charakter aktiv dotčených kybernetickými hrozbami, neboť z hlediska kybernetických hrozeb jsou relevantní především aktiva nehmotná. Tento typ aktiv se však zpravidla v účetnictví odráží neúplně. Z tohoto důvodu byla pro získání přehledu o aktivech ohrožených kybernetickými hrozbami zvolena metoda šetření pomocí dotazníku. Předpokládá se, že pomocí dotazníkového šetření bude možné získat nejen úplnější představu o aktivech společnosti, ale v rámci tohoto šetření bude možné získat od respondentů i kvalitativní ohodnocení jednotlivých aktiv.

Cílová skupina: pracovníci oddělení marketingu, administrátoři IT, ekonomické oddělení.

Vzor dotazníku: viz. příloha č. 1

4.2 Sběr dat pro určení hrozeb a rizik

Pro potřeby identifikace hrozeb pro zjištěná aktiva společnosti byl sestaven dotazník určený pro skupiny zaměstnanců společnosti zodpovědné za bezpečnost informačních technologií, z pohledu zákona o kybernetické bezpečnosti se jedná o tzv. osoby povinné. U této skupiny osob se předpokládá potřebná expertní znalost a schopnost hrozby identifikovat a určit jejich četnost na základě historické zkušenosti.

Cílová skupina: zaměstnanci, jejichž role odpovídá definici osoby povinné dle zákona o kybernetické bezpečnosti.

Vzor dotazníku: viz. příloha č. 2

5 ANALÝZA RIZIK

Pro samotnou analýzu identifikovaných rizik byla zvolena kombinace kvalitativního a kvantitativního přístupu. Vstupem pro analýzu jsou data získaná z dotazníkového šetření popsaného níže. Výstupem provedené analýzy je ohodnocení jednotlivých hrozeb parametrem Fraud Risk Rating[17] a heat-map diagram hrozeb. Tyto získané podklady slouží dále pro výběr nejzávažnějších hrozeb, u nichž je následně provedena hlubší analýza.

5.1 Aktiva a jejich ohodnocení

Na základě dotazníkového šetření je sestavena tabulka označená dále TBAK[18]. Obsahem tabulky je výčet aktiv společnosti, která byly vyhodnocena jako relevantní z pohledu kybernetických hrozeb. U každého aktiva je stanoveno jeho ohodnocení expertním odhadem. Ohodnocení je provedeno pomocí stupnice 1 až 5, kde hodnota 1 reprezentuje malou váhu aktiva, hodnota 5 reprezentuje velkou váhu aktiva. Váhou aktiva je myšlen jeho subjektivní význam pro ekonomiku podniku.

5.2 Určení hrozeb a rizika

Na základě dotazníkového šetření je sestavena tabulka označená dále TBIH. Obsahem tabulky je výčet identifikovaných kybernetických hrozeb (v tabulce značeny HR01 až HR14). Pro každou identifikovanou hrozbu je stanoven stupeň rizika, tedy pravděpodobnost výskytu dané hrozby. Pro stanovení pravděpodobnosti výskytu byla zvolena stupnice 1 až 5 odvozená ze stupnice rizika definované dle ČSN EN ISO/IEC 27005 a dle směrnice NIS. Hodnota 1 reprezentuje nejnižší možný stupeň rizika, hodnota 5 pak reprezentuje nejvyšší možné riziko.

17 Rating je výstupem analýzy rizik provedené nástrojem Fraud Risk Management Tool 2 na základě zjištěné závažnosti hrozby a četnosti jejího výskytu.

18 Pro snadnější orientaci ve výpočtu rizikovosti byly pro jednotlivé tabulky zavedený významové akronymy, např. TBIH – tabulka identifiovaných hrozeb, TBAK – tabulka aktiv, TBHZ -tabulka relevance hrozeb

5.3 Stanovení celkové závažnosti hrozeb a vytvoření heat-map diagramu

5.3.1 Matice relevance hrozeb pro daná aktiva

Dopad dané kybernetické hrozby na různé typy aktiv společnosti není vždy stejný. Toto je ovlivněno především charakterem daného aktiva, na příkladu nehmotného aktiva označovaného jako goodwill lze demonstrovat minimální dopad hrozby způsobený selháním technického vybavení, nicméně únik klientských dat na toto aktivum má dopad zásadní. Zde se tedy jeví jako nutné vyjádření závažnosti jednotlivých kybernetických hrozeb ve vztahu ke konkrétnímu aktivu. Z tohoto důvodu je zavedena do analýzy matice označována TBHZ, ve které je tento vztah mezi jednotlivými aktivy společnosti a danými kybernetickými hrozbami vyjádřen. K vyjádření relevance dané hrozby k danému aktivu byla použita stupnice s hodnotami 1 až 5, kde hodnota 1 reprezentuje nejnižší možnou relevanci a hodnota 5 reprezentuje relevanci nejvyšší.

5.3.2 Určení celkové závažnosti hrozby

Pro určení celkové závažnosti každé z identifikovaných hrozeb je třeba znát její dopad na všechna aktiva společnosti, která jsou předmětem analýzy. Vstupem je tedy ohodnocení jednotlivých aktiv a stanovení relevance dané hrozby vůči danému aktivu dle matice TBHZ. Tyto hodnoty jsou propojeny v tabulce nazvané matice rizikovosti TBR.

Matematické vyjádření výpočtu závažnosti hrozby:

$$R_{HR} = S_A \, x \, S_{AT}$$

kde S_A stupeň ohodnocení aktiva dle tabulky TBAK

S_{AT} selace (váha) vztahu daného aktiva a dané kybernetické hrozby dle matice relevance hrozeb TBHZ

Celkovou závažnost pro každou z uvedených hrozeb HR01-HR14 lze pak získat následujícím výpočtem:

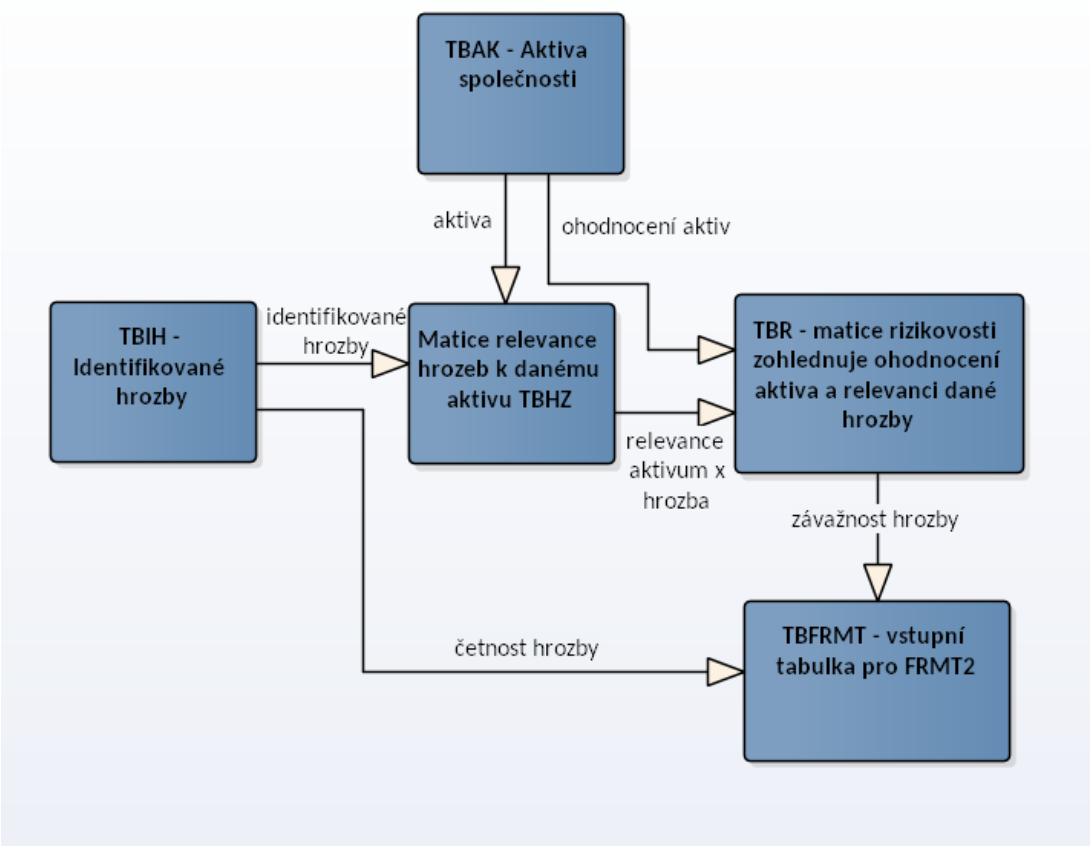
$$TR_{HR} = \sum R_{HR}$$

kde TR_{HR} celková závažnost hrozby

R_{HR} dílčí závažnost hrozby ve vztahu k danému aktivu

Získaná hodnota celkové závažnosti dané hrozby je vložena do tabulky TBFRMT (vstupní tabulka pro FRMT2[19]). Tato tabulka slouží jako příprava vstupních dat pro analytický nástroj Fraud Risk Management Tool 2, který je dále použit pro výpočet parametru Fraud Risk Rating a vygenerování Heat-map diagramu kybernetických hrozeb. Pro potřeby zadání celkové závažnosti hrozeb do uvedeného nástroje je nutné provést transformaci získaných hodnot do stupnice 1 až 5. Tato transformace je provedena v rámci tabulky TBFRMT. Data z tabulky jsou pak následně použita jako vstup do uvedeného nástroje FRMT2.

Celý postup zpracování vstupních dat a jejich následná transformace je znázorněn na následujícím diagramu č. 4.



Obr. 4. Diagram navrženého procesu pro určení závažnosti rizik s přípravou dat pro FRMT2[20]. Pramen: vlastní zpracování

19 Fraud Risk Management Tool 2, nástroj vyvinutý univerzitou FAU – Florida Atlantic University jako součást ACG – Accounting and Auditing Guide
20 Fraud Risk Management Tool

5.4 Určení dopadu kybernetických hrozeb obecně na jednotlivá aktiva společnosti

Na základě hodnocení závažnosti jednotlivých kybernetických hrozeb bude možné dále určit aktiva, která jsou kybernetickými hrozbami nejvíce ohrožena. Určení dopadu vychází z vyhodnocení rizikovosti všech rozpoznaných kybernetických hrozeb, které mají vztah k danému aktivu[21]. Výpočet uvedený níže umožní kvantifikovat celkový dopad kybernetických hrozeb na jednotlivá podniková aktiva.

Výpočet dopadu kybernetických hrozeb na aktiva je vyjádřen poměrově [%] na základě výpočtu provedeného dle vztahu:

$$Imp_{AKTi} = \frac{\sum_{HR\,01}^{HRn} S_{Ai} x S_{ATin} x P_n}{\sum_{Akt\,01}^{Aktm} \sum_{HR\,01}^{HRn} S_{Am} x S_{ATmn} x P_n} x\,100$$

kde S_A Stupeň ohodnocení aktiva dle tabulky TBAK

S_{AT} Relace (váha) vztahu daného aktiva a dané kybernetické hrozby dle tabulky TBR

P Pravděpodobnost výskytu hrozby dle tabulky TBFRMT

Vypočtený relativní dopad kybernetických hrozeb na jednotlivá aktiva je pak možné použít pro sestavení žebříčku nejvíce ohrožených aktiv a určit tak aktiva, kterým je třeba při řešení kybernetické bezpečnosti v podniku věnovat zvýšenou pozornost.

5.5 Určení dopadu dané kybernetické hrozby na aktiva společnosti

Pro potřebu určení dopadu kybernetické hrozby na aktiva a určení nejvíce zasažených aktiv bude stanovena míra rizikovosti dané kybernetické hrozby.

Matematické vyjádření výpočtu závažnosti hrozby:

$$RP_{HR} = R_{HR} x P_{HR}$$

21 Tabulka TBR

kde R_{HR} dílčí závažnost hrozby ve vztahu k danému aktivu dle matice TBR

P_{HR} riziko dané hrozby dle tabulky identifikovaných hrozeb TBIH

6 ANALÝZA POUŽITELNOSTI METOD PRO OCEŇOVÁNÍ NEHMOTNÝCH AKTIV

Jedním z cílů práce je porovnání metod pro oceňování nehmotných aktiv a určení možnosti jejich praktického využití v kontextu firmy, u níž je prováděna analýza dopadů kybernetických hrozeb. Porovnání a určení použitelnosti bude tedy provedeno s přihlédnutím k charakteru zde analyzovaných aktiv.

III. PRAKTICKÁ ČÁST

7 CHARAKTERISTIKA SUBJEKTU

Teoretický základ popsaných v předchozích kapitolách je dále aplikován na vybraný existující podnikatelský subjekt. Kritéria, dle kterých byla vybrána konkretní firma byla zvolena tak, aby zaměření podniku dávalo prostor pro zvýšenou přítomnost kybernetických hrozeb. Mezi další důležitá kritéria byly zařazeny ukazatele: počet zaměstnanců, topologie infrastruktury, počet poboček a účetní ukazatele určující kategorii střední účetní jednotky. Lze předpokládat, že na základě takto nastavených výběrových kriterií lze vybrat vhodného reprezentanta s průměrnými vlastnostmi, které odpovídají široké skupině podnikatelských subjektů v ČR.

Pro potřeby reálné aplikace popisovaných metod byla zvolena společnost sídlící v Praze 4 zabývající se dodávkou informačních technologií a poskytováním souvisejících služeb. Název společnosti zůstane nezveřejněn. Tabulka uvedená pod fotografií sídla vybrané obchodní společnosti přináší základní informace o firmě, která bude dále předmětem analýzy.

Obr. 5. Sídlo analyzované společnosti

Tab. 11. Obecné charakteristiky vybrané anonymní firmy

Parametr	Popis
Právní forma	Akciová společnost
Počet zaměstnanců	560
Pobočky	8
Předmět podnikání	koupě zboží za účelem jeho dalšího prodeje a prodej/výjma činností uvedených v příl.2 a 3 zák.č.455/91Sb./ poradenská činnost v oboru výpočetní techniky poskytování software a poradenství v oblasti hardware a software zpracování dat, služby databank, správa sítí výzkum a vývoj v oblasti přírodních a technických věd nebo společenských věd pořádání odborných kurzů, školení a jiných vzdělávacích akcí včetně lektorské činnosti výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona
Sídlo firmy	Praha 4

Pramen: Obchodní rejstřík, www.justice.cz

7.1 Předmět podnikání

Činnost firmy se zaměřuje na technologickou a konzultační činnost. Primárním předmětem podnikání je tedy dodávka služeb, okrajově pak technického vybavení pro ICT technologie. V oblasti služeb lze pak produkty dělit na dodávku know-how v podobě konzultací při realizací projektů, případně dodávky analýz a komplexního nebo dílčího řešení projektů v oblasti ICT. Další oblastí činnosti je poskytování ucelených řešení pro řadu odvětví a agend. Dodávka řešení je možná jak ve formě dodávky hotového řešení s instalací přímo u zákazníka, tak i ve formě služby dostupné u vybraného poskytovatele zdrojů cloud computingu. Níže je uveden výběr vyvinutých produktů, který by měl přispět k vytvoření představy o rozsahu poskytovaných služeb:

AML[22] – analytický tool určení pro stopování podezřelých finančních transakcí

BAAPI – jednotné rozhraní pro přístup k bankovním účtům dle PSD2[23]

Paperless - rychlé řešení pro implementaci paperless formy[24] do podnikových procesů

22 Zde se jedná o obchodní názvy aplikačních řešení
23 PSD2 – Payment service directive, druhá směrnice EU o platebních služba (upravuje provádění online plateb a sdělování informací při platebním styku
24 Též elektronický oběh dokumentů

CRS - Portál pro agregaci mezinárodních daňových pravidel

Digital Mortgage – digitální hypotéka

Digital Loan – řešení pro proces vyřízení půjčky

eDoceo – edukativní portál (firemní školení)

KYC – ověřování totožnosti

Process Discovery – analýza podnikových procesů

Reporting Tool - nástroj pro povinný reporting směrem k ČNB

Semantic Tool – AI analýza nestrukturovaných informacím

uSign, uStamp – řešení pro elektronický podpis

Virtuální asistent – automatizace rutinních operací

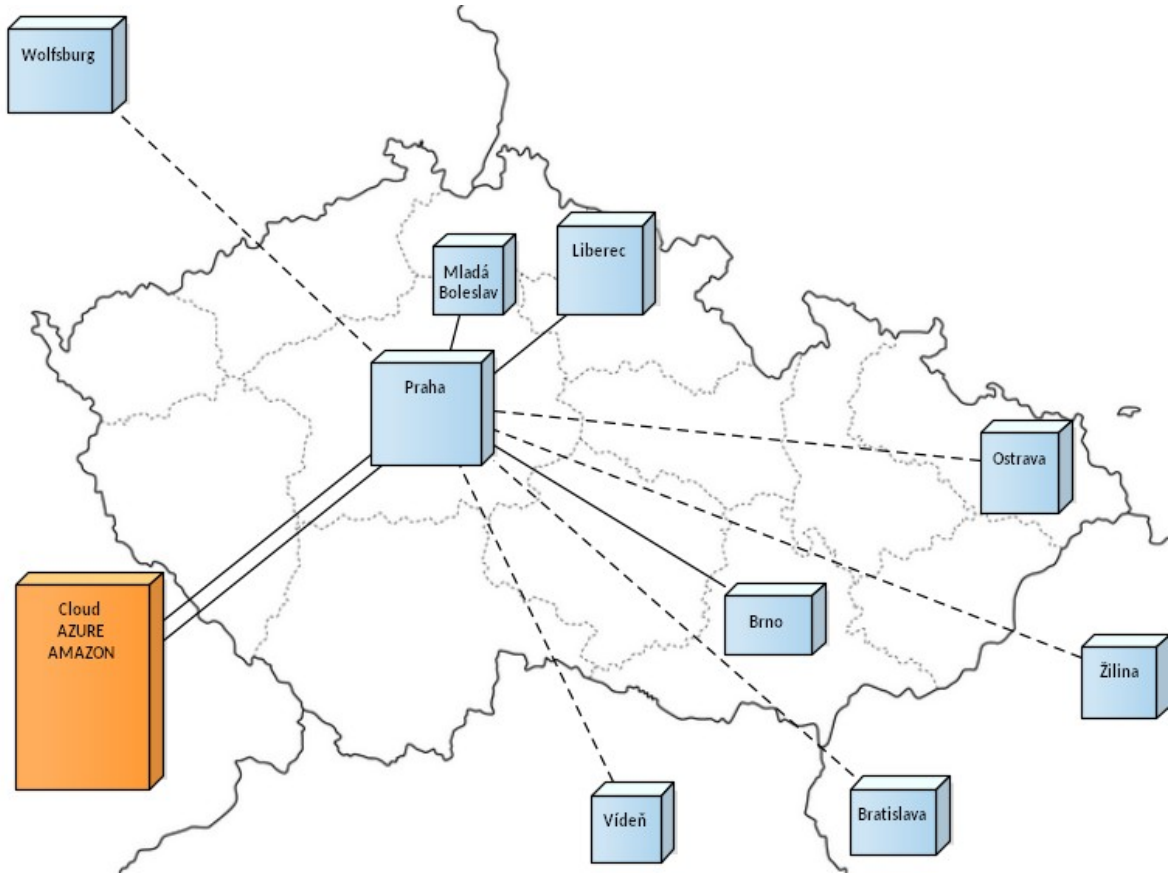
Virtual Case - virtuální složka v souladu s GDPR legislativou

ZenID – AI nástroj pro analýzu dokladů a rozpoznávání falzifikátů.

7.2 Infrastruktura společnosti

Z pohledu analýzy dopadů bezpečnostních incidentů a možných hrozeb je poměrně významné to, jak rozsáhlá je infrastruktura společnosti a to jak z pohledu počtu prvků v daném systému, tak i z pohledu rozmístění jednotlivých prvků v prostoru a způsob jejich propojení. Tento aspekt pak hraje významnější roli v případě propojování systémových prvků mezi jednotlivými geografickými lokacemi. Obrázek níže (obrázek č. 6) ukazuje právě způsob propojení jednotlivých geografických lokací. Spoje vyznačené přerušovanou linkou reprezentují nepřímá spojení (pro spojení poboček je využita infrastruktura třetích strana případně zabezpečené spojení přes VPN tunel). Dále stojí za povšimnutí významnější napojení do cloudových výpočetních zdrojů, zejména pak do Microsoft Azure[25] a AWS[26]. U těchto subjektů je ovšem nejasná jejich geografická poloha. V tomto ohledu existují určitá ujištění a proklamace o uložení klientských dat v regionu Evropské Unie, nicméně obchodní podmínky poskytovatelů cloud computing služeb výslovně regionálně omezené uložení dat negarantují.

25 Služba pro cloud computing od společnosti Microsoft
26 Amazon Web Services - služba pro cloud computing od společnosti Amazon



Obr. 6. Topologie poboček společnosti a jejich síťové propojeními

Dále je vhodné zmínit z pohledu bezpečnosti významné fakty:

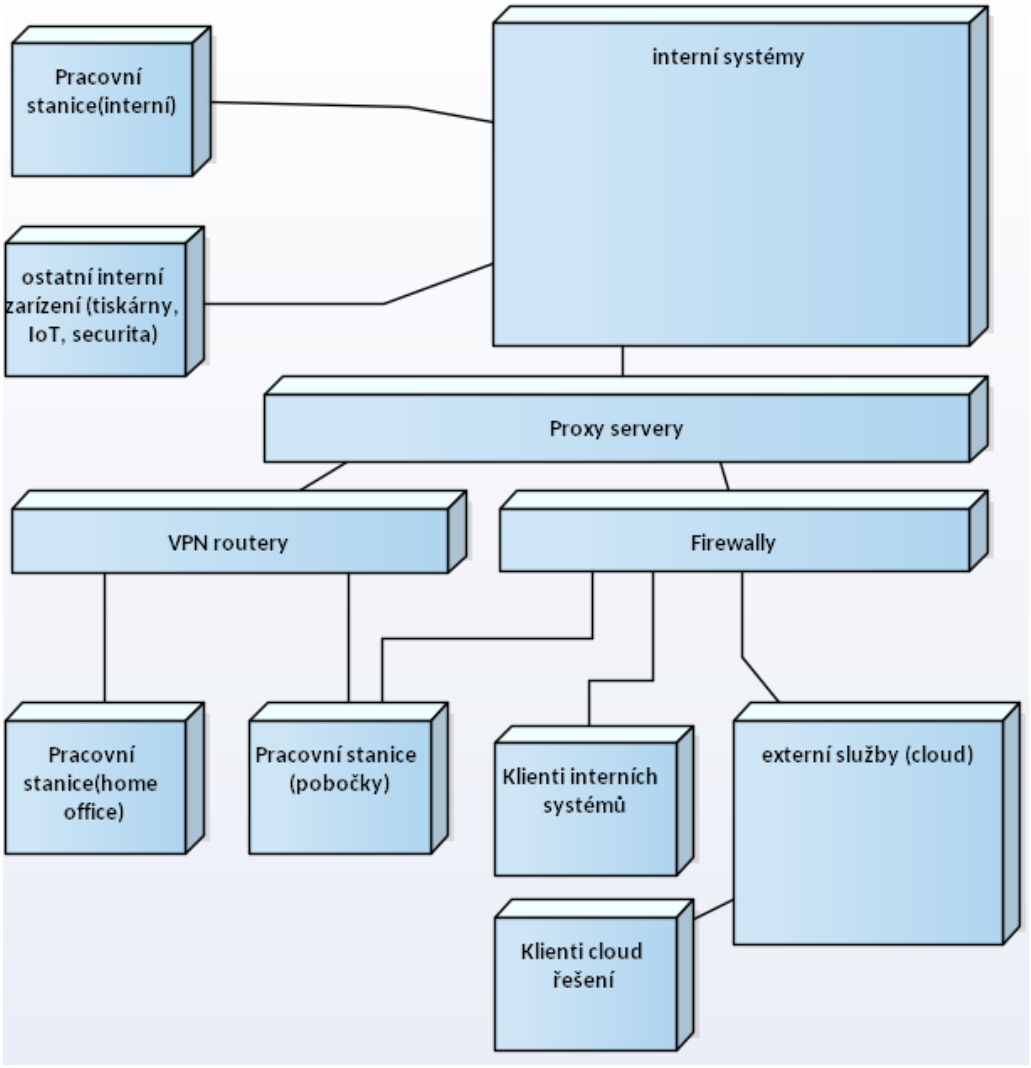
- charakter podnikání popisované společnosti vyžaduje zpřístupnění vybraných podnikových systémů zákazníkům,

- řada poskytovaných služeb je alokována u poskytovatele cloudových výpočetních kapacit s nejasným geografickým umístěním.

- poskytované služby konzultačního charakteru probíhají v režimu on-site[27]

Rozdělení síťových segmentů a konektivitu mezi jednotlivými bloky naznačuje v nízkém rozlišení obrázek č. 7. Diagram nebere nijak v potaz rozdíl mezi produkčními a vývojovými prostředími, zde se omezujeme pouze na zobrazení propojení významných z vnějšího pohledu na infrastrukturu společnosti.

27 Pracovníci vykonávají svoji činnost v prostorách poskytnutých klientem zpravidla na technickém vybavení ve vlastnictví klienta společnosti.



Obr. 7. Řešení síťové konektivity mezi jednotlivými prvky firemní sítě.

Z diagramu zakresleného na obrázku č. 7 je patrné, že přístup k interním systémům společnosti je možný:

1, přímo ze stanic, které jsou připojeny v interní síti společnosti (týká se vybraných poboček a centrály firmy)

2, prostřednictvím VPN tunelu (týká se zaměstnanců pracujících v režimu home-office, pracovníků alokovaných u zákazníků společnosti v režimu on-site a pracovníků všech poboček mimo interní síť)

3, přes firewall společnosti je možné přistupovat na vybrané systémy, zpravidla umístěné v DMZ[28] zóně. Tyto systémy jsou zpravidla určené i pro přístup klientů společnosti, jedná se například o systémy pro zadávání servisních incidentů JIRA, systémy pro podporu vývoje software jako je například GitLab, Artifactory atp.

28 Demilitarizovaná zóna, v oblasti jsou umístěny části informačních systémů určených pro komunikaci s vnějším prostředím.

8 RIZIKA A HROZBY

Kapitola přináší přehled identifikovaných hrozeb s potenciálem způsobit škodu jak na hmotných tak i nehmotných aktivech podniku. Výčet vybraných hrozeb je uveden v tabulce TBIH[29]. U každé hrozby byl stanoven stupeň pravděpodobnosti jejího výskytu. Výčet hrozeb a stanovení míry rizika byl sestaven na základě šetření provedeného formou dotazníku u osob povinných dle zákona o kybernetické bezpečnosti u vybrané společnosti. Hodnota pravděpodobnosti, respektive stupeň pravděpodobnosti výskytu hrozby byl určen empiricky na základě historických zkušeností. Členění pravděpodobnostních stupňů bylo stanoveno na základě doporučení uvedených ve vyhlášce č. 82/2018 Sb. Původní tříbodová škála byla však rozšířena o 2 stupně z důvodu lepšího rozlišení pravděpodobností výskytu hrozby.

Tab. 12. *Tabulka členění pravděpodobnosti výskytu hrozby do stupňů*

Stupeň pravděpodobnosti výskytu hrozby	Rozsah[30] [%]	Popis
1	0-29	Velmi nízká pravděpodobnost výskytu hrozby
2	30-39	Nízká pravděpodobnost výskytu hrozby
3	40-59	Střední pravděpodobnost výskytu hrozby
4	60-79	Vysoká pravděpodobnost výskytu
5	80-100	Velmi vysoká pravděpodobnost výskytu hraničící s jistotou

Následující tabulka uvádí přehled identifikovaných kybernetických hrozeb. Údaje byly získány na základě dotazníkového šetření provedeného u vybraných zaměstnanců společnosti. Vzor použitého dotazníku je uveden v příloze této práce.

29 Označení tabulek TBIH, TBAK, TBHZ, TBR, TBFRMT viz metodická část, TBIH – tabulka identifikovaných hrozeb

30 Předpokládá se, že údaj pravděpodobnosti výskytu hrozby je celočíselný

Tab. 13. Tabulka identifikovaných hrozeb (TBIH)

Označení hrozby	Typ hrozby	Pravděpodobnost výskytu	Popis
HR01	Vyšší moc	2	Zásah bleskem, zaplavení infrastruktury
HR02	Technické závady serverových komponent	2	Selhání hardware.
HR03	Technické závady PC, mobilních telefonů	3	Selhání hardware.
HR04	Ztráta zařízení (a uložených dat)	2	Ztráta a nebo odcizení firemního zařízení, které je nositelem uložených dat a nebo umožňuje přístup k datům uloženým v podnikovém systému.
HR05	Ztráta zařízení (mobilní zařízení, telefon atp.)	4	Ztráta a nebo odcizení firemního zařízení, které je nositelem uložených dat a nebo umožňuje přístup k datům uloženým v podnikovém systému.
HR06	Napadení škodlivým software (malware)	2	Projev škodlivého software bez ohledu, jakým způsobem došlo k infiltraci vnitřního prostředí firmy.
HR07	Neoprávněný přístup (interní)	4	Přístup do systému neoprávněnou osobou na základě chyby v zabezpečení nebo zneužitím cizí identity.
HR08	Neoprávněný přístup (externí)	3	Přístup do systému neoprávněnou osobou na základě chyby v zabezpečení nebo zneužitím cizí identity.
HR09	Nedbalost, lidský faktor	5	Projev selhání lidského faktoru.
HR10	DDoS útok	4	Útok vedený na aplikace dostupné z vně organizace za účelem způsobení jejich dočasné nedostupnosti.
HR11	Ransomware	3	Projev škodlivého software bez ohledu, jakým způsobem došlo k infiltraci vnitřního prostředí firmy za účelem vydírání, případně za účelem poškození společnosti.
HR12	Phishing	3	Přílohy doručené prostřednictvím elektronické pošty obsahující škodlivý kód.
HR13	SPAM	5	Zahlcení poštovních serverů nevyžádanou poštou.
HR14	APT útoky	2	Cílené pokročilé útoky na infrastrukturu společnosti.

9 ANALÝZA AKTIV

Kapitola obsahuje přehled vybraných aktiv, u kterých byl identifikován možný potenciální dopad kybernetických hrozeb. Kritéria výběru byla stanovena na základě provedených dotazníkových šetření mezi vybranými odpovědnými zaměstnanci společnosti (povinné osoby dle zákona o kybernetické bezpečnosti). Výběr je tedy založen na empirických poznatcích a kvalifikovaném odhadu zaměstnance. Stejnou metodou byl také stanoven stupeň významnosti daného aktiva z ekonomického hlediska. Pro potřeby kategorizace a následného určení ekonomických dopadů zavádíme stupnici pro ohodnocení aktiv. Stupnice je uvedena v tabulce č. 14.

Tab. 14. Tabulka členění stanovených stupňů pro ohodnocení významnosti aktiv

Stupeň ohodnocení aktiva	Popis
1	Velmi nízký význam
2	Nízký význam
3	Střední význam
4	Vysoký význam
5	Velmi vysoký význam

Tab. 15. Tabulka vybraných aktiv společnosti a jejich ohodnocení (TBAK[31])

Aktivum	Popis	Ohodnocení
Goodwill[32]	Pověst společnosti	5
Marketingové informace	Informace udržované o stávajících i potencionálních klientech (CRM systém)	4
Data – interní data	Data provozních systémů (docházka, účetnictví)	4
Uložená data vlastněná třetí stranou	Data spravovaná prostřednictvím poskytovaných služeb	5
Duševní vlastnictví – zdrojové kódy	Vývoj vlastních aplikací – zdrojové kódy a další objekty práva duševního vlastnictví	3
Duševní vlastnictví - technologie	Technologické a procesní znalosti uložené na datových nosičích a nebo v systémech (Confluence)	3
Domény	Vlastnictví lokálních domén v jednotlivých státech s umístěnou firemní pobočkou nebo dceřinou společností.	2
Korporátní grafický manuál	Profesionální grafický manuál	2
Data – interní vývojová	Data uložená na vývojových prostředích	1
Data – smlouvy obchodní	Obchodní data, smlouvy	4

31 Označení tabulek TBIH, TBAK, TBHZ, TBR, TBFRMT viz metodická část, TBAK – tabulka aktiv společnosti

32 Goodwill – pověst společnosti na trhu.

Aktivum	Popis	Ohodnocení
Korespondence	Emailová korespondence korporátní	3
Hardware (prac. stanice)	Pracovní stanice zaměstnanců.	2
Hardware (infrastruktura)	Servery, síťová infrastrukturu, backup. Virtuální servery. Cloud.	5
Hardware ostatní (mobilní telefony, tiskárny, vybavení kanceláří)	Mobilní telefony zaměstnanců a další vybavení.	2
Licence SW	Licence SW: operační systémy, antivirové programy, kancelářské balíky, vývojářsky software, software pro virtualizaci, databázový software, BI software, účetnictví, DMS, CRM, backup & recovery atd.	3
Zálohy dat	Uložené zálohy provozních dat.	5

10 ANALÝZA HROZEB

Kapitola obsahuje přehled identifikovaných kybernetických hrozeb. Níže uvedený přehled vychází z provedeného dotazníkového šetření mezi vybranými odpovědnými zaměstnanci společnosti (povinné osoby dle zákona o kybernetické bezpečnosti). Výběr je tedy založen na empirických poznatcích a kvalifikovaném odhadu zaměstnance. Vzor použitého dotazníku je uveden v příloze této práce.

10.1 Stanovení vztahu mezi aktivem společnosti a kybernetickou hrozbou

Aktiva společnosti identifikovaná v předchozích kapitolách nejsou ohrožována jednotlivými kybernetickými hrozbami všechna ve stejné míře. Následující tabulky ukazují vztah mezi danou kybernetickou hrozbou a aktivem společnosti, tj. v následujících tabulkách jsou definovány stupně relevantnosti dané hrozby k danému aktivu. Tabulka č. 16 definuje stupnici, která byla použita pro popis relevantnosti dané hrozby k danému aktivu. Tabulka č. 17 (TBHZ[33]) a tabulka č.18 (TBHZ) představují mapu relevancí mezi aktivem a danou kybernetickou hrozbou. Hodnota vztahu mezi aktivem a danou kybernetickou hrozbou byla stanovena expertním odhadem na základě hodnocení získaných z dotazníku vyplněného vybranými zaměstnanci společnosti.

Tab. 16. Tabulka rozdělení míry relevance kybernetické hrozby k danému aktivu

Stupeň ohodnocení aktiva	Popis
1	Velmi nízká relevance
2	Nízká relevance
3	Střední relevance
4	Vysoký relevance
5	Velmi vysoká relevance

33 Označení tabulek TBIH, TBAK, TBHZ, TBR, TBFRMT viz metodická část, TBHZ – tabulka relevance hrozeb a aktiv

Tab. 17. Tabulka relevance hrozeb a aktiv, část 1 (TBHZ)

Označení hrozby	Goodwill	Market. informace	Data- interní	Uložená data klientská	Duševní vlastnictví – zdrojové kódy	Duševní vlastnictví - technologie	Domény	Korporátní grafický manuál
HR01	1	1	4	4	4	4	1	1
HR02	1	1	5	5	5	5	2	1
HR03	1	1	3	3	3	3	1	1
HR04	2	4	5	5	5	5	1	1
HR05	1	4	5	5	5	5	1	1
HR06	3	3	4	4	4	4	3	1
HR07	2	2	2	2	2	2	2	1
HR08	4	4	4	4	4	4	4	3
HR09	3	2	4	4	4	4	2	5
HR10	4	1	1	1	1	1	5	1
HR11	4	5	4	4	4	4	4	5
HR12	2	2	2	2	2	2	2	2
HR13	1	1	1	1	1	1	1	1
HR14	4	2	4	4	4	4	4	1

Tab. 18. Tabulka relevance hrozeb a aktiv, část 2 (TBHZ[34])

Označení hrozby	Data interní vývojová	Data – smlouvy obchodní Korespondence	Hardware (pracovní stanice)	Hardware (infrastruktura)	Hardware (ostatní)	Licence SW	Zálohy dat
HR01	4	4	4	4	4	1	5
HR02	5	5	5	1	5	1	1	5
HR03	3	3	3	5	1	5	1	1
HR04	3	5	5	5	1	1	4	5
HR05	1	1	1	1	1	1	4	1
HR06	4	4	4	2	2	2	3	4
HR07	2	2	2	1	1	1	2	2
HR08	2	4	4	1	1	1	4	4
HR09	4	4	4	5	5	5	3	4
HR10	1	1	1	1	3	3	1	1
HR11	4	4	4	1	1	1	5	4
HR12	2	2	4	1	1	1	2	2
HR13	1	1	5	1	1	1	1	1
HR14	1	4	4	1	1	1	2	4

34 Označení tabulek TBIH, TBAK, TBHZ, TBR, TBFRMT viz metodická část

10.2 Mapa rizik

Data uvedená v tabulkách č. 13[35], 15[36], 17[37] a 18[38] jsou podkladem pro sestavení mapy rizikovosti jednotlivých kybernetických hrozeb. Na základě těchto vstupů je možné určit mapy rizikovosti, které definují rizikovost pro každou kombinaci hrozby a daného aktiva. Zde je záměr kvantifikovat významnost jednotlivých hrozeb.

Matematické vyjádření výpočtu rizikovosti:

$$R = S_A \, x \, S_{AT}$$

kde S_A Stupeň ohodnocení aktiva dle tabulky č. 13

S_{AT} Relace (váha) vztahu daného aktiva a dané kybernetické hrozby dle tabulek č. 17 a č. 18 (TBHZ)

Tab. 19. Tabulka mapy rizikovosti, část 1 (TBR[39])

Označení hrozby	Goodwill	Market. informace	Data- interní	Uložená data klientská	Duševní vlastnictví – zdrojové kódy	Duševní vlastnictví - technologie	Domény	Korporátní grafický manuál
HR01	5	4	16	20	12	12	2	2
HR02	5	4	20	25	15	15	4	2
HR03	5	4	12	15	9	9	2	2
HR04	10	16	20	25	15	15	2	2
HR05	5	16	20	25	15	15	2	2
HR06	15	12	16	20	12	12	6	2
HR07	10	8	8	10	6	6	4	2
HR08	20	16	16	20	12	12	8	6
HR09	15	8	16	20	12	12	4	10
HR10	20	4	4	5	3	3	10	2
HR11	20	20	16	20	12	12	8	10
HR12	10	8	8	10	6	6	4	4
HR13	5	4	4	5	3	3	2	2
HR14	20	8	16	20	12	12	8	2

35 Tabulka identifikovaných hrozeb TBIH
36 Tabulka vybraných aktiv společnosti a jejich ohodnocení TBAK
37 Tabulka hrozeb a zranitelnosti aktiva, část 1 TBHZ
38 Tabulka hrozeb a zranitelnosti aktiva, část 2 TBHZ
39 Označení tabulek TBIH, TBAK, TBHZ, TBR, TBFRMT viz metodická část, TBR – tabulka rizikovosti

Tab. 20. Tabulka mapy rizikovosti, část 2 (TBR[40])

Označení hrozby	Data interní vývojová	Data – smlouvy obchodní	Korespondence	Hardware (pracovní stanice)	Hardware (infrastruktura)	Hardware (ostatní)	Licence SW	Zálohy dat
HR01	4	16	12	8	20	8	3	25
HR02	5	20	15	2	25	2	3	25
HR03	3	12	9	10	5	10	3	5
HR04	3	20	15	10	5	2	12	25
HR05	1	4	3	2	5	2	12	5
HR06	4	16	12	4	10	4	9	20
HR07	2	8	6	2	5	2	6	10
HR08	2	16	12	2	5	2	12	20
HR09	4	16	12	10	25	10	9	20
HR10	1	4	3	2	15	6	3	5
HR11	4	16	12	2	5	2	15	20
HR12	2	8	12	2	5	2	6	10
HR13	1	4	15	2	5	2	3	5
HR14	1	16	12	2	5	2	6	20

Pro vizualizaci sestavené mapy je použit nástroj Fraud-Risk-Management-Tool-2[41] (dále FRMT2). Vstupem do nástroje jsou data z tabulky č. 17. Hodnoty uvedené ve sloupci závažnosti jsou dány prostým součtem rizikových koeficientů uvedených v tabulkách č. 15 a č. 16 pro jednotlivé typy hrozeb.

Nástroj FRMT2 umožňuje vkládat údaje o závažnosti hrozby ve stupnici 1 – 5, což je v souladu s metodikou analýzy rizik definovanou v ČSN EN ISO/IEC 27005 a vyhláškou č. 82/2018 Sb. Pro účely aplikace získaných údajů o celkové závažnosti jednotlivých hrozeb dat do nástroje FRMT2 je nutné určit převodní matici a rozčlenit identifikované kybernetické hrozby dle dané škály. Rozčlenění získaných údajů celkové závažnosti kybernetických hrozeb do pětistupňové škály je uvedeno v následující tabulce:

40 Označení tabulek TBIH, TBAK, TBHZ, TBR, TBFRMT viz metodická část

41 Nástroj vyvinutý univerzitou FAU – Florida Atlantic University jako součást ACG – Accounting and Auditing Guide

Tab. 21. Tabulka rozdělení míry závažnosti hrozeb

Členění závažnosti hrozby ve FRMT2[42]	Rozsah závažnosti hrozby
1	0 - 89
2	90 - 129
3	130 - 169
4	170 - 189
5	190 -

Tab. 22. Tabulka identifikovaných hrozeb a jejich závažnosti (TBFRMT[43])

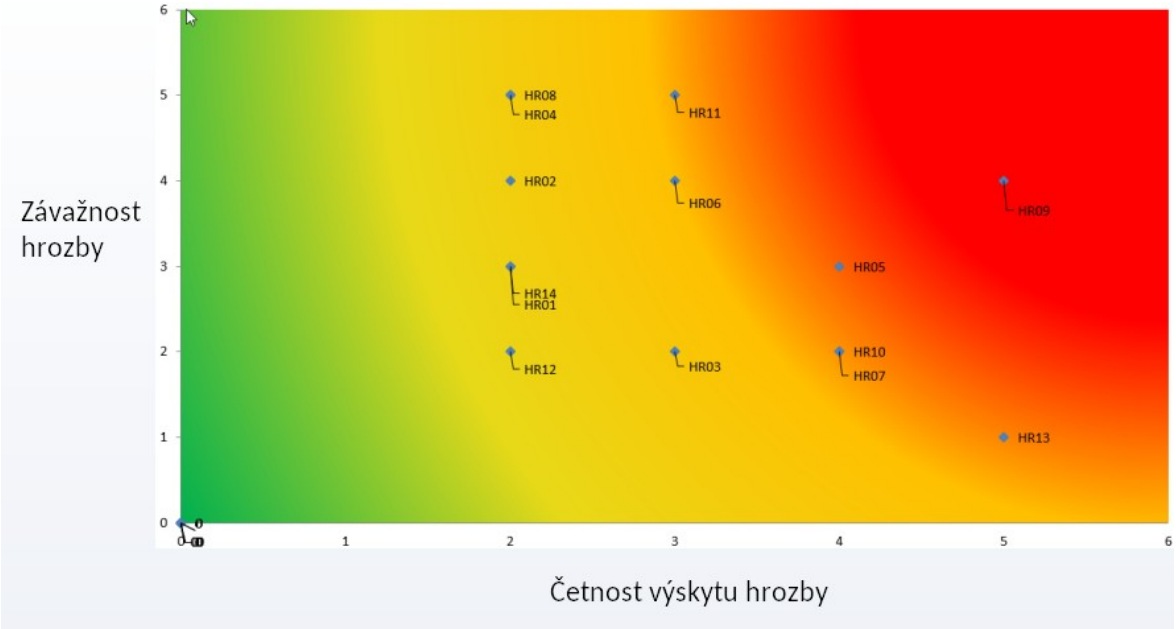
Typ hrozby (ID hrozby ve FRMT2)	Pravděpodobnost výskytu (četnost hrozby)	Celková závažnost hrozby	Celková závažnost hrozby převedená na pětibodovou stupnici FRMT2
HR01	2	169	3
HR02	2	187	4
HR03	3	115	2
HR04	2	197	5
HR05	4	134	3
HR06	3	174	4
HR07	4	95	2
HR08	3	181	5
HR09	5	203	4
HR10	4	90	2
HR11	3	194	5
HR12	2	103	2
HR13	5	65	1
HR14	2	162	3

Po dosazení vstupních údajů do části Risk Assessment Matrix provede nástroj výpočet hodnoty parametru Fraud Risk Rating. Vypočtené hodnoty zobrazuje následující tabulka. Na základě hodnot uvedených v tabulce je nástrojem FRMT2 vygenerován digram heat-map. Takto vytvořený heat-map diagram znázorňuje obrázek č. 8. Výstupem nástroje FRMT2 je také tabulka s vypočtenou hodnotou Fraud Risk Rating, viz. tabulka č. 23.

42 Stupnice vychází ze 3 stupňové stupnice pro určení závažnosti hrozby dle ČSN EN ISO/IEC 27005
43 Označení tabulek TBIH, TBAK, TBHZ, TBR, TBFRMT viz metodická část

Tab. 23. Tabulka hrozeb s určenou hodnotou Fraud Risk Rating

Typ hrozby	Fraud Risk Rating (FRR)
HR01	6
HR02	8
HR03	6
HR04	10
HR05	12
HR06	8
HR07	8
HR08	15
HR09	25
HR10	8
HR11	15
HR12	6
HR13	5
HR14	6



Obr. 8. Heat-map diagram vygenerovaný nástrojem FRMT2

Zobrazený graf heat-map rizikovosti hrozeb umožňuje lépe pochopit vztah mezi četností výskytu dané hrozby a závažností jejího potenciálního dopadu na aktivum společnosti. Pomocí provedené vizualizace je možné zúžit výběr analyzovaných kombinací hrozeb a aktiv společnosti. Dle získaných hodnot parametru FRR[44] a zobrazení heat-map diagramu se jeví jako nejzávažnější hrozby (hrozby s FRR>10):

44 Fraud Risk Rating

HR05 - ztráta zařízení (mobilní zařízení, telefon atp.),

HR08 – neoprávněný přístup externí,

HR09 - nedbalost, lidský faktor,

HR11 – ransomware.

10.3 Rozbor vybraných hrozeb

Kapitola přináší podrobnější analýzu kybernetických hrozeb, které byly v předchozích krocích vyhodnoceny jako nejzávažnější. U každé hrozby je uveden přehled jejich parametrů. Tento přehled je dále doplněn o analýzu dopadů dané hrozby na jednotlivá aktiva společnosti. Tato analýza je provedena na základě zjištěné závažnosti hrozby, četnosti hrozby a relevantnosti hrozby k jednotlivým aktivům. Podrobněji viz metodická část. Výpočet dopadů hrozby pro jednotlivá aktiva je proveden pomocí následujícího vzorce:

$$RP_{HR} = R_{HR} \, x \, P_{HR}$$

kde R_{HR} dílčí závažnost hrozby ve vztahu k danému aktivu dle matice TBR

P_{HR} riziko dané hrozby dle tabulky identifikovaných hrozeb TBIH

10.3.1 HR05 - ztráta zařízení (mobilní zařízení, telefon atp.)

Tab. 24. Parametry hrozby HR05

Parametr	Popis, hodnota
Závažnost hrozby[45]	3
Četnost hrozby, riziko	4
FRR (Fraud risk rating)[46]	12

Dopad na aktiva společnosti	Rizikovost[47]
Goodwill	20
Marketingové informace	64
Data – interní data	80
Uložená data vlastněná třetí stranou	100
Duševní vlastnictví – zdrojové kódy	60
Duševní vlastnictví - technologie	60
Domény	8
Korporátní grafický manuál	8
Data – interní vývojová	4
Data – smlouvy obchodní	16

45 Viz tabulka identifikovaných hrozeb a jejich závažnosti
46 Viz tabulka hrozeb s určenou hodnotou Fraud Risk Rating
47 Hodnota RP vypočtená dle tabulky TBR

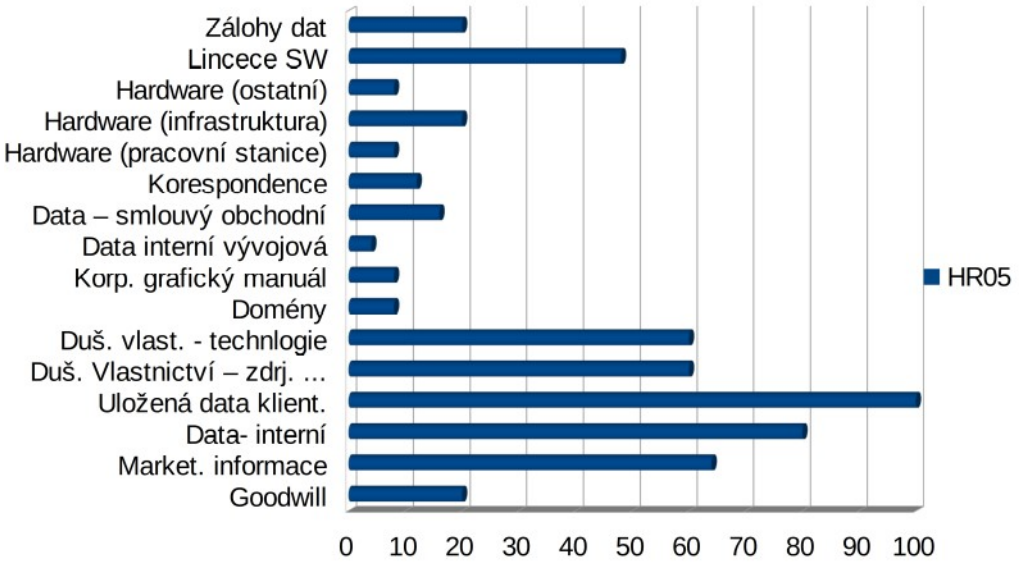
Korespondence	12
Hardware (prac. stanice)	8
Hardware (infrastruktura)	20
Hardware ostatní (mobilní telefony, tiskárny, vybavení kanceláří)	8
Licence SW	48
Zálohy dat	20

Scénář průběhu hrozby

Ztráta mobilního zařízení se stává problémem zejména z důvodu napojení tohoto zařízení na interní systémy podniku. V případě odemknutí zařízení může útočník získat přístup k emailovému účtu, ke kontaktům uložených v mobilním zařízení, k intranetu společnosti, k aplikacím určeným pro dohled a monitoring interních systému, přes nakonfigurované VPN lze pak z takového zařízení přistoupit do interní sítě podniku. Řada aplikací umožňuje uložení hesla a tedy zde lze toto zařízení použít pro přístup k účtům i bez znalosti hesla. Tyto získané informace mohou být dále předmětem vydírání nebo jiného neoprávněného zisku.

Stanovení dopadu hrozby

Následující digram znázorňuje závažnost dopadu kybernetické hrozby na jednotlivá aktiva společnosti. Výpočet dopadu hrozby na jednotlivá aktiva je dán určenou relevantností hrozby k aktivu, závažností hrozby a pravděpodobností výskytu hrozby.



Obr. 9. Zobrazení dopadu hrozby HR05 na jednotlivá aktiva společnosti

Na základě provedeného zobrazení lze usuzovat, že do skupiny aktiv společnosti nejvíce ohrožených hrozbou HR05 patří především data, a to data klientů spravovaná v rámci poskytovaných cloud služeb. Mezi nejvíce ohrožená aktiva dále patří interní data různého určení, zdrojové kódy, technologická data, data obchodního charakteru.

Doporučená opatření

Na základě zjištěných dopadů hrozby HR05 lze doporučit věnovat zvýšenou pozornost následujícím oblastem podnikové infrastruktury:

- zálohování a obnova

- šifrování obsahu mobilních zařízení

- zavedení bezpečnostních politik, které neumožní přístup do mobilního zařezní neoprávněnou osobou

10.3.2 HR08 – neoprávněný přístup externí

Tab. 25. Parametry hrozby HR08

Parametr	Popis, hodnota
Závažnost hrozby	5
Četnost hrozby, riziko	3
FRR (Fraud risk rating)	15

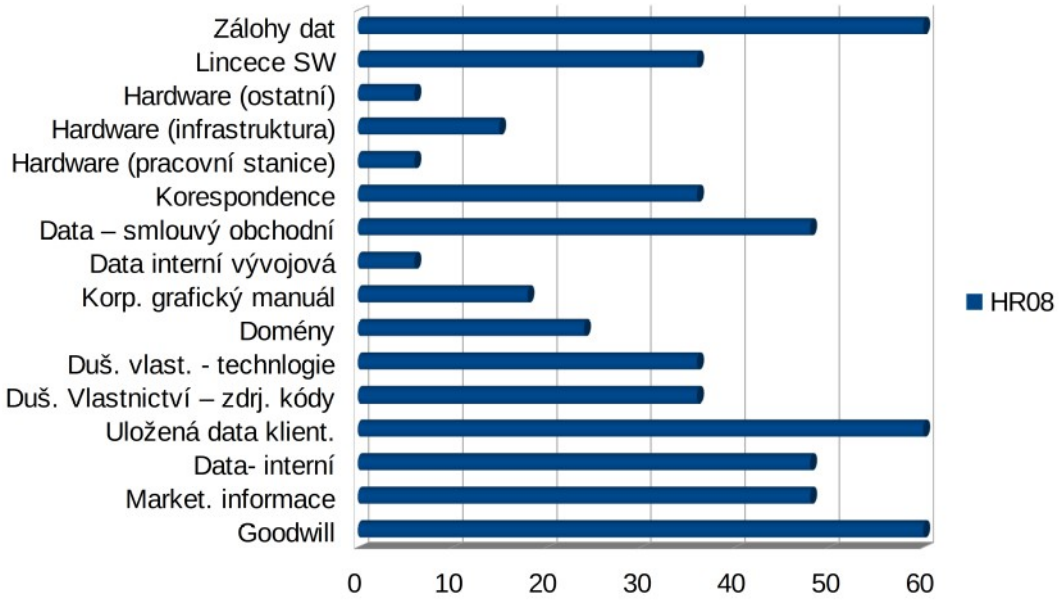
Dopad na aktiva společnosti	Rizikovost
Goodwill	60
Marketingové informace	48
Data – interní data	48
Uložená data vlastněná třetí stranou	60
Duševní vlastnictví – zdrojové kódy	36
Duševní vlastnictví - technologie	36
Domény	24
Korporátní grafický manuál	18
Data – interní vývojová	6
Data – smlouvy obchodní	48
Korespondence	36
Hardware (prac. stanice)	6
Hardware (infrastruktura)	15
Hardware ostatní (mobilní telefony, tiskárny, vybavení kanceláří)	6
Licence SW	36
Zálohy dat	60

Scénář průběhu hrozby

Získání neoprávněného přístupu umožňuje útočníkovi vstupovat do interních podnikových systému, na pracovní stanice či k vybraným serverům. Zde pak v závislosti na motivaci útočníka lze přístup použít k získaní dat nebo například k sabotáži interních systémů, případně k zavlečení škodlivého software do infrastruktury podniku.

Stanovení dopadu hrozby

Následující digram znázorňuje závažnost dopadu kybernetické hrozby na jednotlivá aktiva společnosti. Výpočet dopadu hrozby na jednotlivá aktiva je dán určenou relevantností hrozby k aktivu, závažností hrozby a pravděpodobností výskytu hrozby.



Obr. 10. Zobrazení dopadu hrozby HR08 na jednotlivá aktiva společnosti

Na základě provedeného zobrazení lze usuzovat, že do skupiny aktiv společnosti nejvíce ohrožených hrozbou HR08 jsou především data, a to data klientů spravovaná v rámci poskytovaných cloud služeb, dobré jméno společnosti a zálohy dat. Mezi nejvíce ohrožená aktiva dále patří interní data různého určení, zdrojové kódy, technologická data, data obchodního charakteru.

Doporučená opatření

Na základě zjištěných dopadů hrozby HR08 lze doporučit věnovat zvýšenou pozornost následujícím oblastem podnikové infrastruktury:

- zálohování a obnova

- provedení penetračních testů a ověření odolnosti zabezpečení informačních systémů a komunikace, zejména pak VPN prvků

- testování scénářu dissaster & recovery u všech dotčených systémů

10.3.3 HR09 - nedbalost, lidský faktor

Tab. 26. Parametry hrozby HR09

Parametr	Popis, hodnota
Závažnost hrozby	5
Četnost hrozby, riziko	5
FRR (Fraud risk rating)	25

Dopad na aktiva společnosti	Rizikovost
Goodwill	75
Marketingové informace	40
Data – interní data	80
Uložená data vlastněná třetí stranou	100
Duševní vlastnictví – zdrojové kódy	60
Duševní vlastnictví - technologie	60
Domény	20
Korporátní grafický manuál	50
Data – interní vývojová	20
Data – smlouvy obchodní	80
Korespondence	60
Hardware (prac. stanice)	50
Hardware (infrastruktura)	125
Hardware ostatní (mobilní telefony, tiskárny, vybavení kanceláří)	50
Licence SW	45
Zálohy dat	100

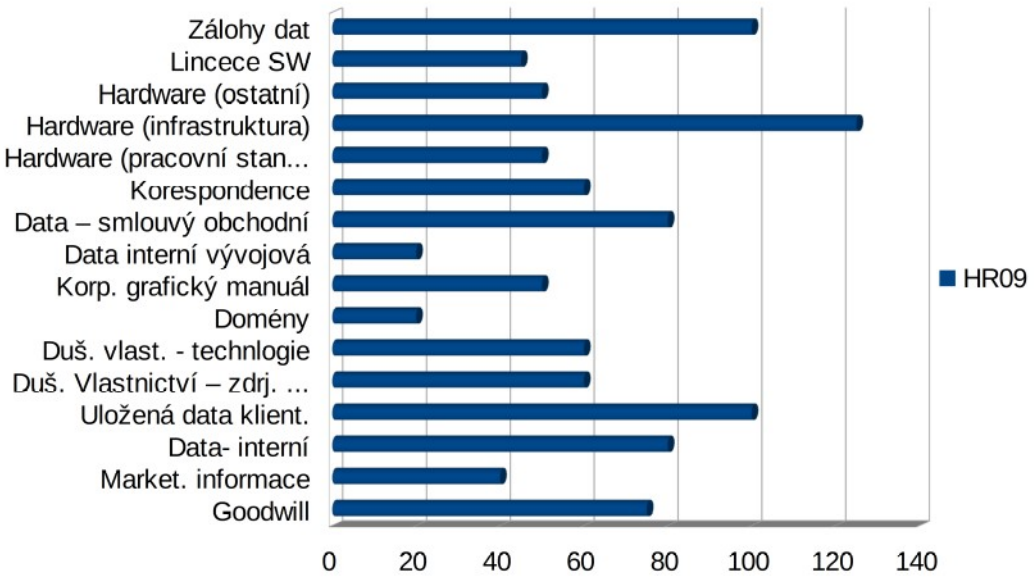
Scénář průběhu hrozby

Selhání lidského faktoru může mít mnoho podob. Pomineme-li projevy nedbalosti jako ponechávání odemknutých pracovních stanic v nepřítomnosti pracovníka, odkládání citlivých tištěných materiálu v nechráněných prostorách, ztráty věcí a zařízení, nezanedbatelnou roli zde hraje i stránka sociálního inženýrství, která je s touto hrozbou spojena. Soci-

ální inženýrství je technika založená na ovlivňování a manipulaci s lidmi. Při aplikaci těchto technik dochází k pokusům o vzbuzení důvěry, případně se pokouší na základě vyvolaných emočních změn o vmanévrování oběti útoku do situace, která vede k provedení vynuceného úkonu nebo poskytnutí informace. Forma vedeného útoku může být rozličná, prakticky lze zvolit jakýkoliv komunikační kanál od odeslání SMS nebo emailu po osobní kontakt. Získaný přístup následně útočník může použít k neoprávněnému přístupu k uloženým informacím či k celým informačním systémům. Následně může dojít k poškození dat nebo jejich odcizení.

Stanovení dopadu hrozby

Následující digram znázorňuje závažnost dopadu kybernetické hrozby na jednotlivá aktiva společnosti. Výpočet dopadu hrozby na jednotlivá aktiva je dán určenou relevantností hrozby k aktivu, závažností hrozby a pravděpodobností výskytu hrozby.



Obr. 11. Zobrazení dopadu hrozby HR09 na jednotlivá aktiva společnosti

Na základě provedeného zobrazení lze usuzovat, že do skupiny aktiv společnosti nejvíce ohrožených hrozbou HR09 jsou především aktiva hardware (infrastruktura), uložená data a jejich zálohy a v neposlední řadě goodwill.

Doporučená opatření

Na základě zjištěných dopadů hrozby HR09 lze doporučit věnovat zvýšenou pozornost následujícím oblastem podnikové infrastruktury:

- zavedení programu školení a vzdělávání

- provedení penetračních testů a ověření odolnosti zabezpečení informačních systémů a komunikace, zejména pak VPN prvků

10.3.4 HR11 – ransomware

Tab. 27. Parametry hrozby HR11

Parametr	Popis, hodnota
Závažnost hrozby	5
Četnost hrozby, riziko	3
FRR (Fraud risk rating)	15

Dopad na aktiva společnosti	Rizikovost[48]
Goodwill	60
Marketingové informace	60
Data – interní data	48
Uložená data vlastněná třetí stranou	60
Duševní vlastnictví – zdrojové kódy	36
Duševní vlastnictví - technologie	36
Domény	24
Korporátní grafický manuál	30
Data – interní vývojová	12
Data – smlouvy obchodní	48
Korespondence	36
Hardware (prac. stanice)	6
Hardware (infrastruktura)	15
Hardware ostatní (mobilní telefony, tiskárny, vybavení kanceláří)	6
Licence SW	45
Zálohy dat	60

Scénář průběhu hrozby

Ransomware je škodlivý kód, který se projevuje viditelným zásahem do funkce informačních systémů. Projev může mít více podob, nejčastěji se však jedná zašifrovaní provozních dat nebo zablokování přístupu do celého systému nebo na pracovní stanice. Po provedení útoku je uživatel zpravidla informován přímo tímto škodlivým software o stavu jeho zařízení včetně podmínek, které je nutné splnit, aby mohl být systém uveden do

48 Dle tabulky TBR

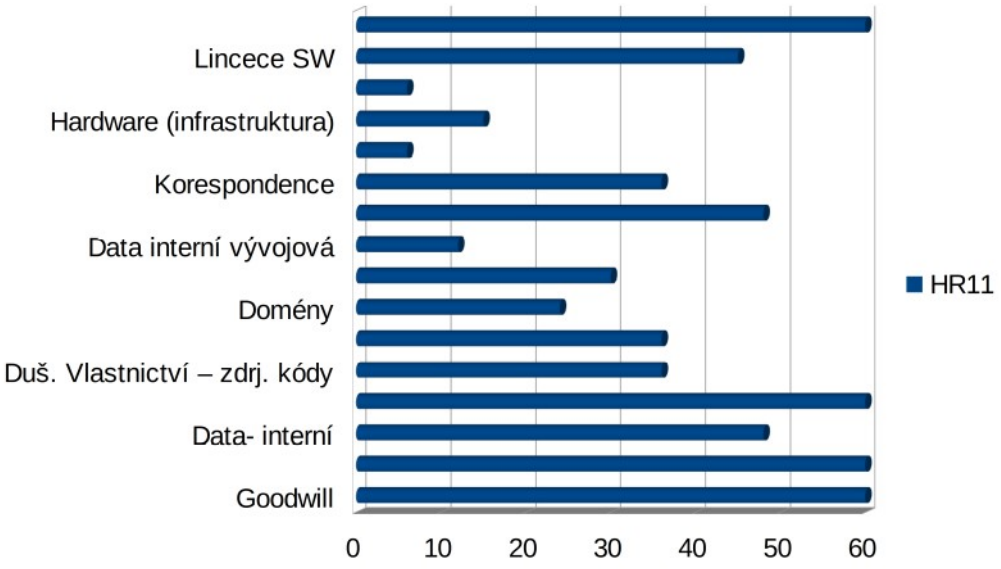
původního stavu. Podmínkami je myšleno například zaplacení výkupného apod. Obvykle však dojde při aktivování ransomware také k vytěžení a odcizení dostupných dat.

K infikování podnikové infrastruktury dochází při návštěvě webových stránek, otevřením přílohy emailu, kliknutím na odkaz na sociální síti.

Primárním cílem útoku je tedy zpravidla finanční zisk útočníka nebo úmyslné způsobení škody cíli útoku. Této motivaci také odpovídá průběh útoku, kdy je zpravidla po provedení útoku oběti oznámena podmínka odstranění překážek v přístupu a způsob provedení úhrady. Provedení platby však není zárukou obnovení přístupu k zařízením a především i po provedení platby zůstávají zařízení stále pod vlivem škodlivého software. Dále je třeba brát v potaz fakt, že během útoku došlo s největší pravděpodobností k odcizení všech dostupných dat, která mohou být dále zneužita.

Stanovení dopadu hrozby

Následující digram znázorňuje závažnost dopadu kybernetické hrozby na jednotlivá aktiva společnosti. Výpočet dopadu hrozby na jednotlivá aktiva je dán určenou relevantností hrozby k aktivu, závažností hrozby a pravděpodobností výskytu hrozby.



Obr. 12. Zobrazení dopadu hrozby HR11 na jednotlivá aktiva společnosti

Na základě provedeného zobrazení lze usuzovat, že do skupiny aktiv společnosti nejvíce ohrožených hrozbou HR11 jsou především data, a to data klientů spravovaná v rámci poskytovaných cloud služeb, dobré jméno společnosti a zálohy dat, marketingové a obchodní informace.

Doporučená opatření

Na základě zjištěných dopadů hrozby HR11 lze doporučit věnovat zvýšenou pozornost následujícím oblastem podnikové infrastruktury:

- zálohování a obnova

- provedení penetračních testů a ověření odolnosti zabezpečení informačních systémů a komunikace, zejména pak VPN prvků

- testování scénářů dissaster & recovery u všech dotčených systémů

- zavedení bezpečnostních politik zejména pak na úrovni firewallů

- nasazení a zajištění permanentní aktualizace ochranného antivirového software

10.4 Přehled ohrožených aktiv

Na základě hodnocení závažnosti jednotlivých kybernetických hrozeb je možné určit aktiva, která jsou kybernetickými hrozbami nejvíce ohrožena obecně. Určení dopadu vychází z vyhodnocení rizikovosti všech hrozeb ve vztahu k danému aktivu[49]. Následující výpočet umožní kvantifikovat celkový dopad kybernetických hrozeb na jednotlivá podniková aktiva.

Výpočet dopadu kybernetických hrozeb na aktiva je vyjádřen poměrově v procentech na základě výpočtu provedené dle vztahu:

$$Imp = \frac{\sum_{HR01}^{HRn} S_A \, x \, S_{AT} \, x \, P}{\sum_{Akt\,01}^{Aktm} \sum_{HR01}^{HRn} S_A \, x \, S_{AT} \, x \, P} \, x \, 100$$

kde S_A Stupeň ohodnocení aktiva dle tabulky č. 13

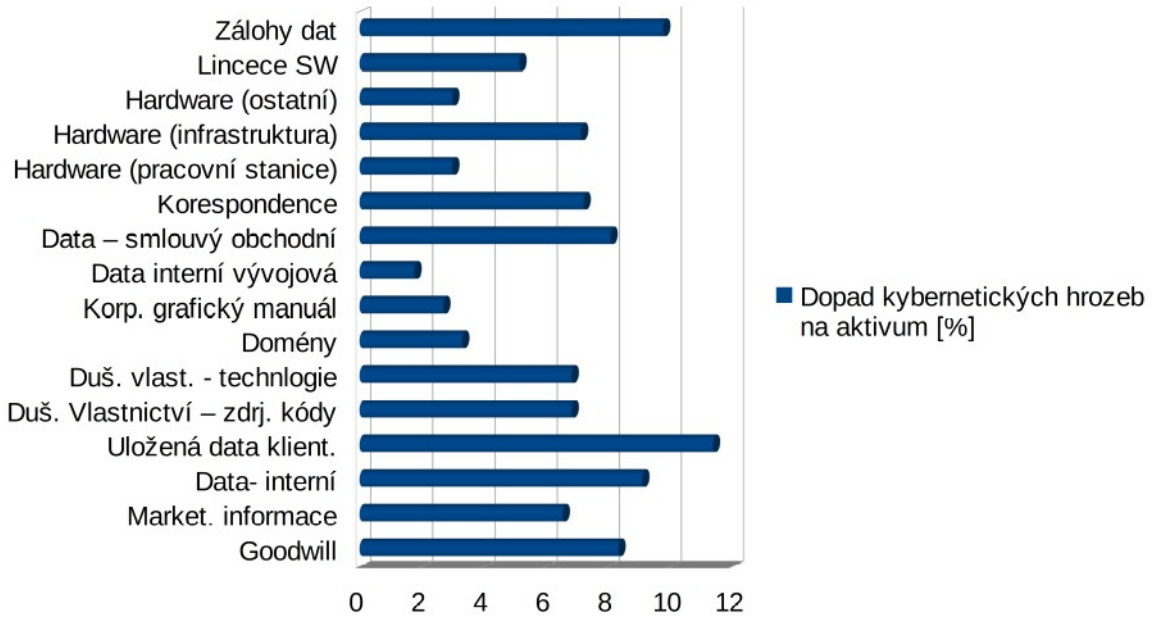
49 Tabulka TBR

S_{AT} Relace (váha) vztahu daného aktiva a dané kybernetické hrozby dle tabulek č. 17 a č. 18 (TBR)

P Pravděpodobnost výskytu hrozby dle tabulky č. 22 (TBFRMT)

Tab. 28. Přehled dopadu kybernetických hrozeb na aktiva podniku

Aktiva společnosti	Poměrný dopad kybernetických hrozeb [%]
Goodwill	8,3
Marketingové informace	6,5
Data – interní data	9,1
Uložená data vlastněná třetí stranou	11,4
Duševní vlastnictví – zdrojové kódy	6,8
Duševní vlastnictví - technologie	6,8
Domény	3,2
Korporátní grafický manuál	2,7
Data – interní vývojová	1,8
Data – smlouvy obchodní	8,1
Korespondence	7,2
Hardware (prac. stanice)	3,0
Hardware (infrastruktura)	7,1
Hardware ostatní (mobilní telefony, tiskárny, vybavení kanceláří)	3,0
Licence SW	5,1
Zálohy dat	9,8



Obr. 13. Zobrazení dopadu kybernetických hrozeb na jednotlivá aktiva společnosti

Zobrazený graf dopadů kybernetických hrozeb dává představu o skupině aktiv, která jsou nejvíce ohrožená kybernetickými hrozbami obecně. Na základě provedené vizualizace je možné určit aktiva, která si z pohledu ochrany před kybernetickými hrozbami zaslouží zvýšenou pozornost:

1, uložená data klientů

2, zálohy

3, data interní

4, data obchodní

11 METODY PRO OCEŇOVÁNÍ NEHMOTNÝCH AKTIV A JEJICH VYUŽITÍ V KONTEXTU VYBRANÉHO PODNIKU

Kapitola přináší srovnání metod pro oceňování nehmotných aktiv. Záměrem je určit metody, které jsou vhodné pro ocenění dopadů kybernetických hrozeb determinovaných v předchozích kapitolách. Primárním kriteriem pro určení vhodnosti jednotlivých metod je především zhodnocení reálné dostupnosti vstupních dat. Dále je třeba brát v potaz účelovost některých metod, tedy samotné zaměření metody na konkrétní typ nehmotného aktiva.

11.1 Stanovení využitelnosti jednotlivých metod pro ohodnocení podnikových aktiv dotčených kybernetickou hrozbou

11.1.1 Metoda násobitelů

Metoda násobitelů je postavena na principu srovnání s existujícím obdobným nehmotným aktivem. Tímto způsobem lze oceňovat typy aktiv jako jsou internetové domény, technologické postupy a software. Praktické využití metod je možné, neboť podklady pro provedenou analýzu jsou snadno dostupné. V případě internetových domén lze čerpat například z nástrojů jako jsou Google Analytics, Google PageRank, Seznam S-Rank.

11.1.2 Metoda nákladu reprodukce a nahrazení

Metoda nákladů reprodukce a nahrazení staví na principu nalezení ceny, za kterou je dané aktivum ochoten směnit jak kupující tak prodejce. Metoda lze aplikovat pro případy nehmotných aktiv, kde jsou známy náklady na jejich pořízení. Příkladem takových aktiv mohou být loga, domény, průmyslové právní ochrana, náklady ušlé příležitosti.

11.1.3 Výnosové metody

Výnosové metody jsou založeny na předpokladu, že u daného nehmotného aktiva lze určit jeho přínos. Zde se tedy staví na tom, že lze určit rozdíl v hodnotě výrobku, který je například opatřen danou značkou a výrobkem, který tuto značku nemá. Metodu lze aplikovat na nehmotná aktiva jako jsou ochranné známky, patenty, případně licence.

11.1.4 Metoda licenční analogie

Metoda používaná pro oceňování nehmotných aktiv jako je duševní vlastnictví a tržní hodnotu určuje na základě analogie licenčního obchodu.

11.1.5 Metoda podílu na zisku

Tato metoda staví na odhadu hodnoty nehmotného aktiva jakožto jeho příspěvku do tvorby zisku. Tento podíl v zásadě odpovídá také případnému licenčnímu poplatku plynoucího z použití daného nehmotného aktiva při realizaci produktu. Využitelnost této metody je obdobná jako u metody licenční analogie.

11.1.6 Metoda prémií

Metoda staví na odhadu hodnoty nehmotného aktiva jakožto jeho vlivu na hodnotu produktu. V zásadě se jedná o analogii licenční úplaty. Zde se tedy hodnota chápe jako cena, kterou je ochoten tržní zájemce zaplatit užití daného aktiva.

11.1.7 Metoda čisté současné hodnoty

Metoda čisté současné hodnoty v kontextu oceňování hodnoty nehmotných aktiv se snaží určit hodnotu aktiva na základě hodnoty maximální výše úplaty pro daný typ produktu. V principu se tedy hledá hodnota, při níž je použití daného nehmotného aktiva ještě rentabilní.

11.1.8 Diskontní míra pro výnosové oceňování nehmotných aktivech

Metoda staví na principu vlivu obětované příležitosti na budoucí peněžní tok. Ocenění nehmotného aktiva staví na srovnání s investicí do obdobného nehmotného aktiva při stanovené diskontní míře. Praktické využití této metody je však velmi omezeno neboť pro určení hodnoty nehmotného aktiva neexistují relevantní srovnání a celý odhad ceny tedy staví na použití analogií.

11.1.9 Metoda nadměrných zisků a proces alokace kupní ceny podniku (PPA)

Metoda nadměrných zisků je určena pro oceňování specifických nehmotných aktiv, jejichž vliv je obtížné oddělit od celkového ekonomického přínosu. Tao metoda je vhodná například ocenění aktiv jako goodwill, zákaznické vztahy a unikátní technologie a licence.

11.1.10 Shrnutí využitelnosti metod pro oceňování nehmotných aktiv podniku

V následující tabulce jsou uvedeny jednotlivé metody pro oceňování nehmotných aktiv a vybraná aktiva společnosti.

Tab. 29. Využitelnost metod pro oceňování nehmotných aktiv u vybraného podniku

			Metody pro oceňování nehmotných aktiv							
Podnikové aktivum	Kategorie aktiva dle IFRS: IAS38	Výnosové metody	Metoda násobitelů	Metody nákladů reprodukce a nahrazení	Metoda licenční analogie	Metoda podílu na zisku	Metody prémií	Metody čisté současné hodnoty	Diskontní míra pro výnosové ocennění nehm. akt.	Metoda nadměrných zisků
Goodwill	Marketing – Obch. firma	Y	N	N	N	N	Y	N	N	Y
Marketingové informace	Zákazníci	Y	N	N	N	N	N	N	N	N
Data – interní data	Technologie - Databáze	N	N	N	N	N	N	N	N	N
Uložená data vlastněná třetí stranou	Technologie – Obchodní tajemství	N	N	N	N	N	N	N	N	N
Duševní vlastnictví – zdrojové kódy	Technologie – Software Smlouvy - Licence	N	Y	Y	Y	Y	Y	N	N	Y
Duševní vlastnictví - technologie	Technologie - Patenty	N	Y	Y	Y	Y	Y	N	N	Y
Domény	Marketing - Domény	N	Y	Y	N	N	N	N	N	N
Korporátní grafický manuál	Marketing – Grafické označení	N	N	Y	N	N	N	N	N	N
Data – interní vývojová	Technologie - Databáze	N	N	Y	N	N	N	N	N	N
Data – smlouvy obchodní	Zákazníci – Smluvní zákaznické vztahy	N	N	Y	N	N	N	N	N	N
Korespondence	Zákazníci – Nesmluvní zákaznické vztahy, Zákazníci – seznamy zákazníků	N	N	Y	N	N	N	N	N	N
Hardware (pracovní stanice)	Hmotné aktivum	-	-	-	-	-	-	-	-	-
Hardware (infrastruktura)	Hmotné aktivum	-	-	-	-	-	-	-	-	-
Hardware ostatní (mobilní telefony, tiskárny, vybavení kanceláří)	Hmotné aktivum	-	-	-	-	-	-	-	-	-
Licence SW	Smlouvy - Licence	Y	N	N	Y	Y	Y	N	N	N
Zálohy dat	Technologie – Databáze, Technologie – Obchodní tajemství	N	N	Y	N	N	N	N	N	N

Hodnoty Y uvedené v tabulce určují kombinací metody a daného aktiva, která lze považovat za použitelnou při oceňování daného aktiva. Kombinace označené písmenem N jsou pak považovány za méně vhodné. Při sestavení tabulky byl brán v potaz charakter jednotlivých metod a požadovaných vstupních hodnot. Reálná možnost praktického využití uvedených metod s ohledem na dostupnost vstupních dat zkoumána nebyla.

ZÁVĚR

Trendem posledních let byl a je přenos podnikových agend do informačních systémů. Motivací pro toto jednání bylo snižování nákladů, zvyšování efektivity práce a tím i přímo zvyšování schopnosti čelit konkurenci. Vývoj v posledním období, především pak vynucený masový přechod do režimu práce z domova, či přinejmenším snaha o minimalizaci fyzického kontaktu na pracovištích vedl ke zvýšení tohoto úsilí vedoucího k dramatickému nárůstu využívání ICT v rámci podnikových procesů. Nárůst využívání ICT v podnikové praxi pak vede k nutnosti intenzivněji řešit hrozby, které používání informačních systémů a především pak jejich propojování do sítí, přináší. Tato práce k této problematice přináší ve své první, teoretické části přehled právního a regulačního rámce, který s kybernetickou bezpečností má souvislost. V metodické částí je představena metodika pro určení podnikových aktiv potenciálně ohrožených kybernetickými hrozbami. Dále je představena metodika pro determinaci kybernetických hrozeb v kontextu vybraného podniku, určení rizikovosti kybernetických hrozeb relevantních pro vybraný podnik a určení vztahu kybernetické hrozby k danému aktivu.

Stěžejním obsahem praktické částí je analýza rizik u vybrané společnosti. Podklady pro provedenou analýzu byly získány na základě provedených dotazníkových šetření a rozhovorů . Získané podklady byly následně posloužily pro sestavení přehledu kybernetických hrozeb a přehledu podnikových aktiv relevantních k dané kybernetické hrozbě. Získané podklady posloužily k vyhodnocení závažnosti jednotlivých kybernetických hrozeb, a to přímo ve vztahu k daným podnikovým aktivům.

Z pohledu oceňování nehmotných aktiv a kvantifikace reálného dopadu kybernetických hrozeb na jednotlivé druhy nehmotných aktiv bylo možné na základě získaných poznatků určit ty metody, jejichž použití je vhodné právě při hodnocení dopadu případného kybernetického útoku. Je nutno však konstatovat, že s ohledem na vysokou pracnost zpracování podkladů pro ocenění, je praktické využití těchto metod poměrně omezené.

Mezi zjištěné nejzávažnější kybernetické hrozby ohrožující vybranou společnost patří: HR05 - ztráta zařízení (mobilní zařízení, telefon atp.), HR08 – neoprávněný přístup externí, HR09 - nedbalost, lidský faktor, HR11 – ransomware. K uvedeným zjištěným nejzávažnějším hrozbám lze s s ohledem na očekávaný dopad do aktiv společnosti vyslovit následující doporučení k zavedení opatření:

- zálohování a obnova dat

- šifrování obsahu mobilních zařízení

- zavedení bezpečnostních politik, které neumožní přístup do mobilního zařízení neoprávněnou osobou

- provedení penetračních testů a ověření odolnosti zabezpečení informačních systémů a komunikace, zejména pak VPN prvků

- testování scénářů disaster & recovery u všech dotčených systémů

- zavedení bezpečnostních politik zejména pak na úrovni firewallů

- nasazení a zajištění permanentní aktualizace ochranného antivirového software

- zavedení programu školení a vzdělávání

Hodnocení ohrožení jednotlivých aktiv společnosti ukázalo, že souhrnný dopad všech identifikovaných kybernetických hrozeb nejvíce ohrožuje aktiva jako jsou uložená data klientů, zálohy dat, data interní a data obchodního charakteru.

Metody pro oceňování nehmotných aktiv obecně staví buď na principu srovnávacím, nákladovém a nebo výnosovém. Praktické využití metod pro oceňování nehmotných aktiv tedy závisí na tom, zda lze získat dostatečné podklady pro naplnění jednoho z těchto uvedených principů, respektive zda lze určit rozdíl v těchto vstupech před zkoumaným kybernetickým útokem a po něm.

SEZNAM POUŽITÉ LITERATURY

[1] Šulc, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 147 s. ISBN 978-80-7380-737-5

[2] Framework for Improving Critical Infrastructure Cybesecurity. : National Institute of Standards and Technology, 2018. 55s.

[3] Singer, P. W.; Friedman, A. Cybersecurity: What Everyone Needs to Know. USA: Oxford University Press, 2013. ISBN0199918112

[4] Graham, J.; Howard, R.; Olson, R. Cyber Security Essentials. : CRC Press, 2011. ISBN 978149851234

[5] ČR. Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kriteriích, 2014.

[6] ČR. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, 2014.

[7] ČR. ČSN EN ISO/IEC 27000, 2018.

[8] ČR. ČSN EN ISO/IEC 27001, 2014.

[9] ČR. ČSN EN ISO/IEC 27003, 2014.

[10] ČR. ČSN EN ISO/IEC 27005, 2019.

[11] Basl, J.; Blažíček, R. Podnikové informační systémy. Praha: Grada, 2012. 328s. ISBN 978-80-247-4307-3

[12] Kolouch, J.; Bašta, P. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7

[13] Šilerová, Edita, Hennyeyová, Klára a N. N. Balashova Informační systémy v podnikové praxi. Praha: Poweprint, 2016. 163s. ISBN 978-80-87994-78-8

[14] Fowler, Martin Patterns of Enterprise Application Architecture. Boston: Addison-Wesley, 2012. ISBN 0-321-12742-0

[15] Eurofound (2020) Living, working and COVID-19 dataset [online]. 2020. https://www.eurofound.europa.eu/data/covid-19/working-teleworking

[16] Smejkal, Vladimír a Rais, Karel Řízení rizik ve firmách a jiných organizacích. 4. vydání. : Grada Publishing, 2013. 488 s. ISBN 978-80-247-4644-9

[17] Novotný, Karel Slovník vybraných pojmů vztahujících se k hodnocení rizik dle § 132a odst. 3 zákoníku práce. Rožnov pod Radhoštěm: RVS, 2000. 104s.

[18] Požár, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005.

[19] Svačina, Pavel Oceňování nehmotných aktiv. Praha: Ekopress, s.r.o., 2010. 211s. ISBN 978-80-86929-62-0

[20] Mařík, MIloš. Metody oceňování podniku. 4 vydání. Praha: Ekopress, 2018. 550s. ISBN 978-80-87865-38-5

[21] Copeland, T.; Koller, T.; Murrin, J. Stanovení hodnoty firem. Praha: Victoria Publishing, 1994. ISBN 8085605414

[22] IAS 38 Intangible Assets [online]. https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/

[23] IFRS: IFRS 3 — Business Combinations [online]. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory – technlogie Microsoftu pro správu uživatelských účtů, adresářů a domén.
ANSI	Americký národní standardizační institut.
CAPM	Capital Asset pricing model – ceonvý model kapitálových aktiv.
CERT	Computer Emergency Response Team
CF, cash-flow	Cash flow
Cloud	Také Cloud computing – model poskytování informačních technologií formou služby.
CRAMM	CCTA Risk Analysis and Management Method – metoda pro analýzu rizik informačních systémů podporovaná legislativně normou ISO/IEC 27001.
COBRA	Consultative, Objective and Bi-functional Risk Analysis - metoda pro analýzu rizik
DevOps	Kombinace anglických výrazů Development a Operations – moderní přístup k vývoji software.
DMZ	Demilitarizovaná zóna – v oblasti informačních systémů se jedná o část systémů umistěnou v nechráněné oblasti určenou pro přístup uživatel z vnějšího prostředí.
DNS	Domain Name server – server doménových jmen, adresář IP adres a jejich přidružených názvů.
Dos/DDoS	Denial of Service, Distributed Denial of Service – technika útoku na vystavenou službu nebo webovou stránku formou zahlcení požadavky.
eIDAS	nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu
EK, EP	Evropská komise, Evropský parlament
EU	Evropská Unie
GDPR	General data protection regulation – Obecné nařízení o ochraně osobních údajů.
HW	Hardware – počítačové vybavení, výpočetní technika, tiskárny a ostatní vybavení
IAS	Internationa Accounting standard.
ICT	Information and Communication Technologies – informační a komunikační technologie.
IFRS	International Financial Reporting Standard.

IP protokol, IP adresa	IP protokol – internet protocol, základní komunikační vrstva používaná pro přenos informací v rámci sítě. Základ rodiny protokolů TCP/IP IP adresa – přidělaná adresa zařízení zapojeného do počítačové sítě postavené na protokolu IP.
IS	Informační systém
ISMS	Information Security Management System (Systém řízení bezpečnosti informací), dle ISO 27001
IT	Informační technologie
IVS	International Valuation Standards
IVSC	International Valuation Standards Council
ISO/IEC	International standardization in the field of Information Technology – mezinárodní standarty v oblasti informačních technologií.
NIS	Network and Information Systems – směrnice EU o bezpečnosti sítí a informačních systémů.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost.
SW	Software – programové vybavení počítačů a dalších zařízení.
VPN	Virtual Private Network – řešení pro vytvoření bezpečného spojení mezi dvěma lokacemi napříč veřejnou počítačovou sítí.

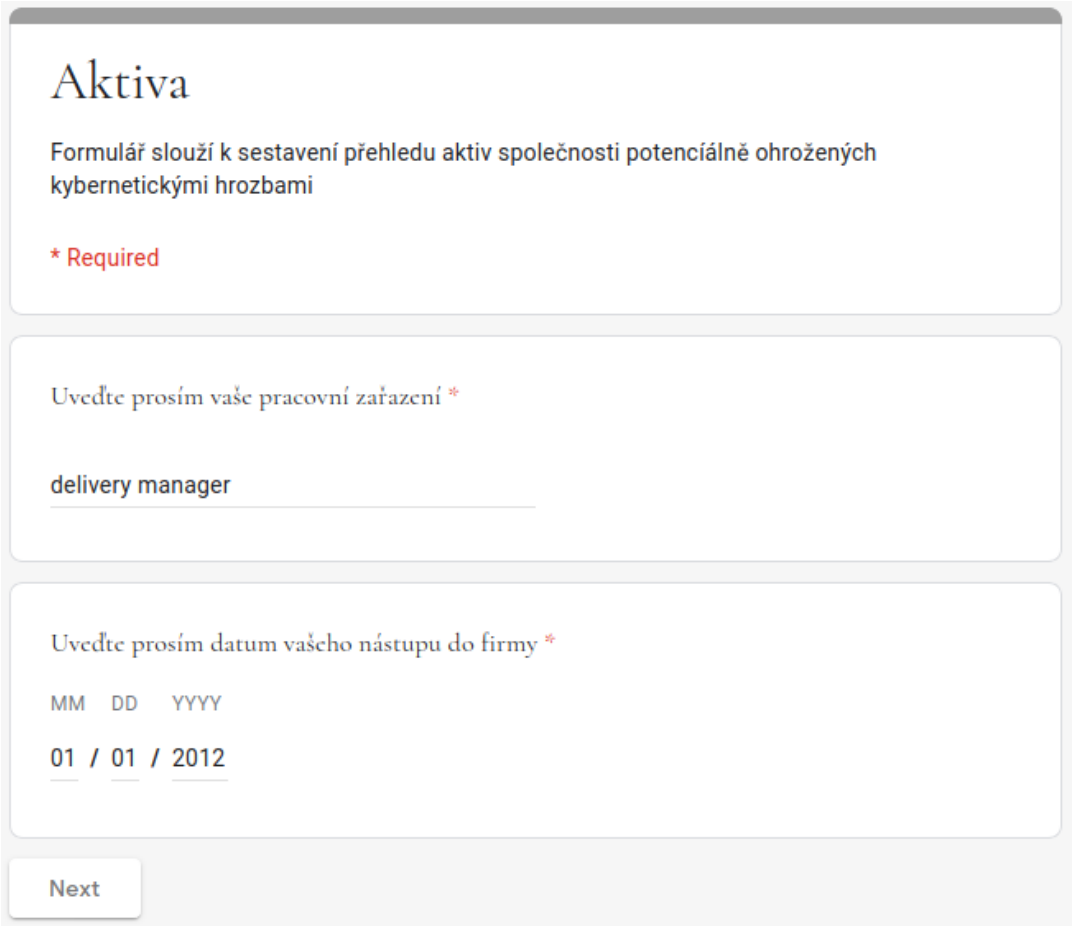
SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P 1: DOTAZNÍK K URČENÍ AKTIV SPOLEČNOSTI DOTČENÝCH KYBERNETICKOU HROZBOU.

Dotazník je sestaven pomocí aplikace Google Forms.



Aktiva

Formulář slouží k sestavení přehledu aktiv společnosti potencíálně ohrožených kybernetickými hrozbami

* Required

Uveďte prosím vaše pracovní zařazení *

delivery manager

Uveďte prosím datum vašeho nástupu do firmy *

MM DD YYYY

01 / 01 / 2012

Next

Aktiva

* Required

Ohodnocení aktiv

Z uvedených možností aktiv vyberte ty, které jsou pro vaši společnost relevantní a které považujete za ohrožená kybernetickými hrozbami. U každého aktiva, které považujete za relevantní zvolte na stupnici 1 až 5 jeho význam pro chod společnosti.

Dobré jméno společnosti (goodwill) *

velmi vysoký význam

Duševní vlastnictví - technologie *

vysoký význam

Duševní vlastnictví - vlastní vývoj software, zdrojové kódy *

střední význam

Domény *

Není relevantní

Uložená data obchodní *

vysoký význam

Uložená data interní, vývojová *

vysoký význam

Obchodní korespondence *

velmi vysoký význam

Hardware (infrastruktura) *

velmi nízký význam

Hardware (pracovní stanice) *

vysoký význam

Hardware ostatní *

střední význam

Licence SW *

vysoký význam

Doplňte prosím další neuvedená aktiva, která považujete za významná z pohledu ekonomiky podniku a mohou být ohrožena kybernetickými hrozbami

Zálohy dat

Ohodnocení významnosti aktiva

velmi vysoký význam

Ohodnocení významnosti aktiva

velmi vysoký význam

Doplňte prosím další neuvedená aktiva, která považujete za významná z pohledu ekonomiky podniku a mohou být ohrožena kybernetickými hrozbami

Your answer

Ohodnocení významnosti aktiva

Choose

Doplňte prosím další neuvedená aktiva, která považujete za významná z pohledu ekonomiky podniku a mohou být ohrožena kybernetickými hrozbami

Your answer

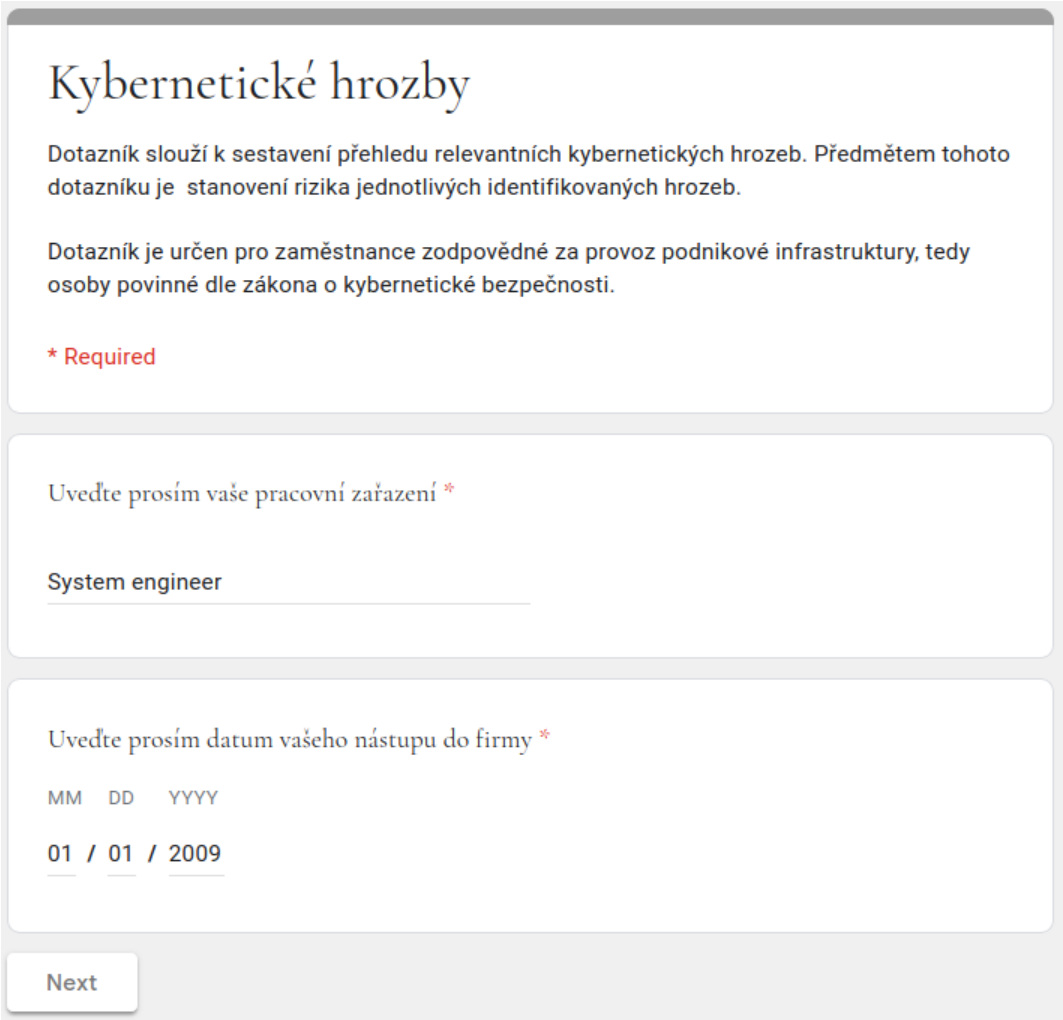
Ohodnocení významnosti aktiva

Choose

Back Submit

PŘÍLOHA P 2: DOTAZNÍK K URČENÍ KYBERNETICKÝCH HROZEB A RIZIK.

Dotazník je sestaven pomocí aplikace Google Forms.



Kybernetické hrozby

Dotazník slouží k sestavení přehledu relevantních kybernetických hrozeb. Předmětem tohoto dotazníku je stanovení rizika jednotlivých identifikovaných hrozeb.

Dotazník je určen pro zaměstnance zodpovědné za provoz podnikové infrastruktury, tedy osoby povinné dle zákona o kybernetické bezpečnosti.

* Required

Uveďte prosím vaše pracovní zařazení *

System engineer

Uveďte prosím datum vašeho nástupu do firmy *

MM DD YYYY

01 / 01 / 2009

Next

Kybernetické hrozby

* Required

Kybernetické hrozby

V této sekci, prosím, ohodnoťte riziko u uvedených hrozeb.

Pro stanovení rizika hrozby je použita 5bodová stupnice, kde:
1 - velmi nízký stupeň rizika
2 - nízký stupeň rizika
3 - střední stupeň rizika
4 - vysoký stupeň rizika
5 - velmi vysoký stupeň rizika

Kybernetický útok - ransomware *

Choose

Kybernetický útok - DDoS *

Choose

Kybernetický útok - phishing *

Choose

Kybernetický útok - malware *

Choose

Kybernetický útok - neoprávněný přístup interní *

Choose

Kybernetický útok - neoprávněný přístup externí *

Choose

Vyšší moc - záplava, zásah bleskem, přírodní katrastrofa *

Choose

Technické závady - servery, infrastrutkura *

Choose

Technické závady - servery, infrastrutkura *

Choose

Nedbalost, lidský faktor *

Choose

Ztráta přiděleného zařízení *

Choose

Doplňte, prosím, další neuvedené hrozby, které považujete za relevantní

Your answer

Doplňte, prosím, další neuvedené hrozby, které považujete za relevantní

Ztráta mobilního zařízení

Ohodnocení rizika *

4 - vysoký stupeň rizika

Doplňte, prosím, další neuvedené hrozby, které považujete za relevantní

APT

Ohodnocení rizika *

3 - střední stupeň rizika

Back Submit

Never submit passwords through Google Forms.