EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY

Evidenčné číslo: 103006/I/2022/36109009600982532

POISTITEĽNOSŤ KYBERNETICKÝCH RIZÍK

Diplomová práca

2022 **Bc. Patrik Bajnok**

EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA HOSPODÁRSKEJ INFORMATIKY

POISTITEĽNOSŤ KYBERNETICKÝCH RIZÍK

Diplomová práca

Študijný program:	Informačný manažment
Študijný odbor:	Ekonómia a manažment
Školiace pracovisko:	Katedra matematiky a aktuárstva FHI
Vedúci záverečnej práce:	Mgr. Ing. Zuzana Krátka, PhD.

Bratislava 2022 **Bc. Patrik Bajnok**

Ekonomická univerzita v Bratislave
Fakulta hospodárskej informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta:	Bc. Patrik Bajnok
Študijný program:	informačný manažment (Jednoodborové štúdium, inžiniersky II. st., denná forma)
Študijný odbor:	ekonómia a manažment
Typ záverečnej práce:	Inžinierska záverečná práca
Jazyk záverečnej práce:	slovenský
Sekundárny jazyk:	anglický
Názov:	Poistiteľnosť kybernetických rizík

Anotácia:

Záverečná práca je zameraná na kybernetické riziká a ich poistiteľnosť. Kybernetické riziká sa dajú ťažko vyhodnotiť, čo súvisí okrem iného so skutočnosťou, že medzi kybernetickými a tradičnými rizikami sú mnohé rozdiely. Historické údaje zvyčajne nemôžu veľa povedať o budúcich kybernetických udalostiach. Problémom je aj tzv. akumulačné riziko, keď jedna kybernetická udalosť môže mať vplyv na mnoho rôznych spoločností súčasne. S tým súvisia problémy s poistiteľnosťou kybernetických rizík. Jedným z cieľov záverečnej práce je prehľad a porovnanie poistných produktov kryjúcich kybernetické riziká na poistnom trhu Európskej únie.

Vedúci:	Ing. Mgr. Zuzana Krátka, PhD.
Katedra:	KMA FHI - Katedra matematiky a aktuárstva FHI
Vedúci katedry:	doc. Ing. Michal Páleš, PhD.
Dátum zadania:	03.11.2020
Dátum schválenia:	04.11.2020

doc. Ing. Michal Páleš, PhD.

vedúci katedry

ABSTRAKT

BAJNOK, Patrik: *Poistiteľnosť kybernetických rizík.* – Ekonomická univerzita v Bratislave. Fakulta hospodárskej informatiky; Katedra matematiky a aktuárstva. – Vedúca záverečnej práce: Mgr. Ing. Zuzana Krátka, PhD. – Bratislava: FHI EU, 2022, 56 s.

Záverečná práca je vypracovaná na tému poistiteľnosť kybernetických rizík. Cieľom diplomovej práce bolo na základe teoretických poznatkov, štruktúrovaného rozhovoru s odborníkmi na kybernetické riziká a analýzy poistného trhu, identifikovať rozdiely pri vnímaní a kategorizovaní kybernetických rizík, identifikovať problémy poistiteľnosti kybernetických rizík a navrhnúť potenciálne vylepšenia pre poisťovanie týchto rizík. Prvá kapitola popisuje čo je to kybernetické riziko, ako sa tieto riziká zvyknú rozdeľovať a zdroj týchto rizík. Nachádza sa v nej vymedzenie pojmu poistiteľnosť a čo tento pojem znamená pre kybernetické riziká. V druhej kapitole sa nachádzajú čiastkové ciele, hlavný cieľ diplomovej práce a metodika, ktorú sme pri práci používali. V tretej kapitole sú najskôr popísané poznatky získané zo štruktúrovaných rozhovorov s manažérmi spoločnosti Tatra banka, ako kybernetické riziká vnímajú oni, či má banka uzavreté poistenie kybernetických rizík a ako banka tieto riziká manažuje. Na základe teoretických poznatkov a poznatkov z praxe získaných od manažérov Tatra banky, sú v tejto kapitole navrhnuté zlepšenia pre poisťovanie kybernetických rizík. Na konci tretej kapitoly sú popísané a porovnané vybrané poistné produkty dostupné na Slovensku a v Európskej únii. Výsledkom riešenia danej problematiky sú navrhnuté zlepšenia pre poisťovanie kybernetických rizík a komparácia vybraných poistných produktov kryjúcich kybernetické riziká spoločností.

Kľúčové slová: Kybernetické riziko, kybernetická hrozba, poistiteľnosť rizík, poistenie kybernetických rizík.

ABSTRACT

BAJNOK, Patrik: *Insurability of cyber risks.* – University of Economics in Bratislava. Faculty of Economic Informatics. Department of Mathematics and Actuarial Science. – Thesis Supervisor: Mgr. Ing. Zuzana Krátka, PhD. – Bratislava: FHI EU, 2022, 56 p.

Diploma thesis is elaborated on the topic of insurability of cyber risks. The aim of the thesis was based on theoretical knowledge, structured interview of cyber risk experts and insurance market analysis, identify differences in the perception and categorization of cyber risks, identify cyber risk insurance problems and propose potential improvements to insure these risks. The first chapter describes what cyber risk is, how these risks tend to be distributed and the source of these risks. It contains a definition of the term insurability and what this term means for cyber risks. The second chapter contains sub-objectives, the main objective of the thesis and the methodology we used in the work. The third chapter first describes the findings obtained from structured interviews with managers of Tatra banka, how they perceive cyber risks, whether the bank has cyber risks insurance and how the bank manages these risks. Based on theoretical and practical knowledge gained from managers of Tatra banka, improvements for cyber risk insurance are proposed in this chapter. At the end of the third chapter, selected insurance products available in Slovakia and in the European Union are described and compared. The result of solving this problem are proposed improvements for cyber risk insurance and a comparison of selected insurance products covering the cyber risks of companies.

Keywords: Cyber risk, cyber threat, insurability, insurability of risks, cyber insurance.

OBSAH

Zoznam obrázkov

Zoznam tabuliek

Zoznam skratiek

BEC	Kompromitácia obchodných e-mailov, angl. Bussines Email Compromise
C&C	Príkaz a ovládanie, angl. Command and Control
CNSS	Výbor pre národné bezpečnostné systémy, angl. Committee on National Security Systems
DDoS	Distribuované odmietnutie služby, angl. Distributed Denial-of-Service
DNS	Systém názvov domén, angl. Domain Name System
ENISA	Agentúra Európskej únie pre bezpečnosť sietí a informácií, angl. The European Union Agency for Network and Information Security
ETL	Prehľad hrozieb ENISA, angl. ENISA Threat Landscape
IEC	Medzinárodná elektrotechnická komisia, angl. International Electrotechnical Commission
IKT	Informačno-komunikačné technológie, angl. Information and Communication Technologies (ICT)
ISO	Medzinárodná organizácia pre štandardizáciu, angl. International Organization for Standardization

NIST	Americký národný inštitút štandardov a technológie, angl. National Institute of Standarts and Technology
PCI-DSS	Štandard zabezpečenia údajov v odvetví platobných kariet, angl. Payment Card Industry Data Security Standard
RDP	Protokol vzdialenej plochy, angl. Remote Desktop Protocol
RaaS	Ransomvér ako služba, angl. Ransomware-as-a-Service
URL	Jednoznačné označovanie objektov, angl. Uniform Resource Locators

Úvod

Žijeme v 21. storočí, keď ľudstvo zažíva technologický rast na takej úrovni ako nikdy predtým. S tým je spojené aj správanie ľudí, ktorí trávia na internete čoraz viac voľného ale aj pracovného času. Dnes si už málokto vie predstaviť, že by na internet prístup nemal. Tomuto trendu sa prispôsobili aj spoločnosti a preto čoraz viac spoločností presúva svoje pôsobenie práve do online sféry. Cez internet sa spájajú so svojimi zákazníkmi, dodávateľmi a partnermi. Všetky nazbierané potrebné dáta si ukladajú na svoje interné siete, aby sa k nim vedel dostať každý zamestnanec, ktorý tieto dáta na svoju prácu potrebuje. Internetu sa zvykne hovoriť aj kybernetický priestor. V tomto priestore však tak isto ako v reálnom svete existujú riziká. S nárastom pôsobenia ľudí a spoločností v online priestore aj tieto riziká narastajú. Kybernetické riziká môžu spôsobiť jednotlivcovi či spoločnostiam nemalé problémy. Čo vlastne kybernetické riziko je, popisujeme v prvej kapitole. Spoločnosti s nárastom rizík budujú aj svoje zabezpečenie voči nim. Hrozby však pôsobia na spoločnosti a jednotlivcov zo všetkých strán a tak rýchlo sa vyvíjajú, že nie je otázkou či sa im cez toto zabezpečenie podarí preniknúť, ale kedy. Z tohto dôvodu by sa voči kybernetickým rizikám malo dať poistiť, tak ako voči tradičným rizikám. Na to aby sa voči rizikám dalo poistiť, musia byť tieto riziká poistiteľné. Problematiku poistiteľnosti taktiež v tejto práci popisujeme. V druhej kapitole sme opísali ciele diplomovej práce a metodiku použitú na dosiahnutie týchto cieľov. V tretej kapitole sa venujeme štruktúrovaným rozhovorom s manažérmi kybernetickej bezpečnosti a rizík v Tatra banke, od ktorých zisťujeme, či sú zozbierané teoretické poznatky skutočne používané aj v praxi. Na základe získaných dát popisujeme ako reálny podnik kybernetické riziká vníma, zaraďuje a či je voči nim poistený. Na základe všetkých zozbieraných informácií sme vypracovali návrhy pre zlepšenie poisťovania kybernetických rizík. Následne uvádzame niekoľko vybraných poistení kybernetických rizík a porovnávame ich z pohľadu rizík, ktoré kryjú.

Túto tému som si vybral pretože už päť rokov pracujem na dohodu v Tatra banke. Každoročne máme online školenie o kybernetickej bezpečnosti a už pred pár rokmi ma kybernetická bezpečnosť cez tieto školenia oslovila. Keď som zbadal túto tému v akademickom systéme vedel som, že bude zaujímavá. Nie je k nej až tak veľa dostupných informácií ale verím, že s rastom informatizácie pribudne aj viac odborníkov, ktorý sa problematikou poistiteľnosti kybernetických rizík budú zaoberať.

1 Súčasný stav riešenej problematiky doma a v zahraničí

V dnešnej dobe spoločnosti spracúvajú a uchovávajú čoraz viac svojich aktív v digitálnej podobe. Zároveň sa pomocou výpočtovej techniky a dátových sietí prepojujú zamestnanci spoločnosti vzájomne medzi sebou alebo aj zamestnanci so zákazníkmi. Táto skutočnosť má za následok, že už nestačí realizovať opatrenia pre zaistenie kybernetickej bezpečnosti na fyzickej úrovni spoločnosti. Každá spoločnosť alebo organizácia by mala analyzovať kybernetické riziká, ktoré jej hrozia a prijať opatrenia pre ich minimalizáciu. Nie vždy je ale schopná sa kybernetickým rizikám vyhnúť. Kybernetické riziká sa čoraz viac vyvíjajú a už nie sú len problémom, ktorý vyriešia zamestnanci spoločnosti starajúci sa o výpočtovú techniku. Kybernetické riziká sa dotýkajú bežných zamestnancov, všetkých úrovní manažmentu a postupujú celou spoločnosťou. Na opatrenia voči kybernetickým rizikám môže spoločnosť vynaložiť nemalé zdroje, no aj tak sa útočníkom môže podariť preniknúť. Pre tieto prípady by bolo dobré, aby bola spoločnosť poistená proti kybernetickým rizikám a práve tomu sa v tejto práci chceme venovať. Akým spôsobom a či vôbec je možné sa proti kybernetickým rizikám poistiť. Nakoľko je internet globálny nástroj, ktorý je využívaný takmer po celom svete a už máloktorá organizácia alebo jednotlivec tento nástroj nepoužíva a na internete nepôsobí, dalo by sa povedať, že súčasný stav riešenej problematiky doma a v zahraničí sa nedá rozdeliť. Spoločnosti a jednotlivci by mali mať možnosť sa voči týmto rizikám poistiť bez ohľadu na to, kde na svete pôsobia. To či to tak naozaj je a či aj u nás na Slovensku je poistenie voči kybernetickým rizikám možné si rozoberieme v neskoršej časti práce. Najskôr je potrebné zadefinovať si základné pojmy, aby sme mohli danej problematike pochopiť.

1.1 Kybernetické riziko

Hoci sa kybernetické riziko môže zdať samozrejmé, nie vždy je jasne definované a pre každého človeka môže mať tento pojem iný význam. Vo svojej najviac základnej úrovni je však kybernetické riziko rizikom poškodenia organizácie prostredníctvom jej informačných systémov. Existuje veľké množstvo definícií pre kybernetické riziko, pre lepšie pochopenie bude ak si ich uvedieme viacero a všimneme si medzi nimi všetky podobnosti ale aj rozdiely.

Slovo kybernetika pochádza z gréckeho slova „kybernetes“ čo v preklade znamená kormidelník, neskôr sa toto slovo pretransformovalo do latinského slova, ktorým Plató

pomenoval guvernérov. Dalo by sa však preložiť aj do slovného spojenia „umenie riadiť“. V modernej dobe sa tento výraz rozšíril, pretože Norbert Wiener v roku 1948 napísal knihu s názvom Kybernetika. Jeho podtitul bol, kontrola a komunikácia u zvierat a strojov. Bolo to dôležité, pretože spája kontrolu (činnosti vykonávané v nádeji na dosiahnutie cieľov) s komunikáciou (prepojenie a tok informácií medzi aktérom a prostredím). Wiener teda poukazuje na to, že efektívne konanie si vyžaduje komunikáciu. Príchod predpony „kyb“ alebo „kyber“ ako odkazu na roboty (kyborgov) alebo internet (kybernetický priestor), kybernetiku ešte viac posunul smerom ku strojom a technike. (Paul Pangaro, 2013)

Kybernetiku teda môžeme v našom odbore chápať ako všetko čo sa týka informačno-komunikačných technológii, čiže sietí, informačných systémov a kybernetického priestoru. Agentúra Európskej únie pre bezpečnosť sietí a informácií (ENISA) v dokumente Definícia kybernetickej bezpečnosti tvrdí, že kybernetická bezpečnosť sa týka pôvodu hrozby, ktorá je predstavená prostredníctvom kybernetického priestoru, skôr ako fyzického útoku. Samotný kybernetický priestor odkazuje na súbor odkazov a vzťahy medzi objektmi, ktoré sú prístupné prostredníctvom zovšeobecnenej telekomunikačnej siete, a k množine samotných objektov, kde predstavujú rozhrania umožňujúce ich diaľkové ovládanie, diaľkový prístup k údajom alebo ich účasť na kontrolných akciách v rámci daného kybernetického priestoru. (ENISA, 2015)

Kybernetický priestor je vzájomne závislá sieť infraštruktúr informačných technológií a zahŕňa internet, telekomunikačné siete, počítačové systémy a vstavané procesory a ovládače v kritických odvetviach. (Výbor pre národné bezpečnostné systémy, CNSS, 2022)

V zbierke zákonov Slovenskej republiky sa v zákone o kybernetickej bezpečnosti č. 69/2018 Z.z. na účely daného zákona rozumie: „kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi.“ V tomto zákone však nie je priamo zadefinované slovné spojenie kybernetické riziko. Pojem riziko je však zadefinovaný ako: „miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami.“ Keďže sa v diplomovej práci bude často vyskytovať pojem incident je potrebné si uviesť jeho definíciu. Zákon o kybernetickej bezpečnosti č. 69/2018 Z.z. definuje „kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je:

1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,

2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,

3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo

4. ohrozenie bezpečnosti informácií.“

Podľa spoločnosti PricewaterhouseCoopers (2017) je kybernetické riziko akékoľvek riziko spojené s finančnou stratou, narušením alebo poškodením dobrého mena organizácie v dôsledku zlyhania, neoprávneného alebo chybného používania jej informačných systémov.

Podľa Amerického národného inštitútu štandardov a technológie v skratke NIST (2019) je kybernetické riziko, riziko finančnej straty, prerušenia prevádzky alebo poškodenia v dôsledku zlyhania digitálnych technológií používaných na informačné a/alebo prevádzkové funkcie zavedené do výrobného systému elektronickými prostriedkami v dôsledku neoprávneného prístupu, použitia, zverejnenia, narušenia, úpravy alebo zničenia výrobného systému. Koncom roku 2021 však pri novšej publikácii uviedli definíciu kratšie a to v znení: Riziko závislosti od kybernetických zdrojov (t.j. riziko závislosti od systému alebo prvkov systému, ktoré existujú v kybernetickom priestore alebo sú v ňom občas prítomné). (NIST, 2021)

Medzinárodný štandard ISO/IEC 27000 (2018) týkajúci sa informačných technológií, bezpečnostných techník a systémov riadenia informačnej bezpečnosti uviedol, že v kontexte systémov riadenia informačnej bezpečnosti môžu byť riziká informačnej bezpečnosti vyjadrené ako vplyv neistoty na ciele informačnej bezpečnosti. V nasledujúcej poznámke bolo pridané, že riziko informačnej bezpečnosti je spojené s potenciálom, že hrozby využijú slabé miesta informačného aktíva alebo skupiny informačných aktív a tým spôsobia škodu organizácii.

Martin Eling a Jan Hendrik Wirfs z Univerzity St. Gallen v spolupráci so Swiss Re vypracovala štúdiu „Kybernetické Riziko: Veľmi veľké na poistenie?“ (2016). V tejto štúdii uvádzajú hneď niekoľko definícií pre toto riziko z viacerých zdrojov:

- Riziko spojené so škodlivými elektronickými udalosťami, ktoré spôsobujú rušenie obchodnej a peňažnej straty. (Mukhopadhyay et al., 2005, 2013)
- Zlyhanie informačných systémov. (Böhme a Kataria, 2006)
- Operačné riziká pre informačné a technologické aktíva, ktoré majú dôsledky ovplyvňujúce dôvernosť, dostupnosť alebo integritu informácií alebo informačných systémov. (Cebula a Young, 2010)

- Riziko informačnej bezpečnosti. (Ögüt, Raghunathan, a Menon, 2011)
- Národná asociácia komisárov pre poisťovníctvo (NAIC, 2013) poskytuje typické príklady na opis kybernetického rizika ako napríklad krádež identity, zverejnenie citlivých informácií a prerušenie podnikania.
- Akékoľvek riziko vyplývajúce z používania elektronických údajov a ich prenos. To zahŕňa fyzické škody spôsobené kybernetickými útokmi, stratu alebo poškodenie údajov a ich finančné dôsledky, podvodu spáchaného zneužitím údajov, ako aj akejkoľvek vzniknutej zodpovednosti z neudržania dostupnosti, integrity a dôvernosť elektronicky uložených informácií, či už s tým súvisia jednotlivci, firmy alebo vlády. V tomto kontexte kybernetické poistenie rieši riziká spojené s prvou a treťou stranou a zahŕňa elektronické podnikanie, internet, siete a informačné aktíva. (Swis Re, 2014)
- Regulačné orgány poistných a finančných trhov kategorizujú kybernetické riziko ako operačné riziko. V rámci regulácie Solventnosť II je operačné riziko definované ako „riziko straty vyplývajúce z nevhodných vnútorných procesov alebo ich zlyhania, z personálu alebo systémov, alebo z nepriaznivých vonkajších udalostí“ (Smernica Solventnosť II, čl. 13).

Ak by sme podľa týchto všetkých vyššie uvedených definícií chceli vytvoriť vlastnú definíciu kybernetického rizika znela by nasledujúco: Kybernetické riziko je miera ohrozenia pôsobiaca na všetky aktíva a všetkých aktérov vyskytujúcich sa v kybernetickom priestore.

1.1.1 Rozdelenie kybernetických rizík

Rozdelenie kybernetických rizík je najčastejšie spomínané z pohľadu zdroja týchto rizík. Martin Eling a Jan Hendrik Wirfs (2016) rozdeľujú vo svojej práci kybernetické riziká tiež podľa zdroja týchto rizík. Kybernetické riziká majú podľa nich dva typy zdrojov. Tieto zdroje sú nekriminálne zdroje a kriminálne zdroje.

Medzi nekriminálne zdroje radia prírodné akty, technické zlyhania a ľudské zlyhania. Prírodné akty môžu byť napríklad výpadok elektrickej energie po prírodnej katastrofe alebo zničenie serverov, alebo inej informačnej techniky po záplavách. Technické zlyhania sa berú ako nejaké zlyhanie hardvéru, napríklad strata dát pri zlyhaní disku, zlyhanie počítača alebo chyba a softvéri. Ľudské zlyhania môžu byť napríklad nechcené zverejnenie informácií na webovej stránke alebo falošná správa.

Kriminálne akty rozdeľujú pod tri zdroje a to sú: fyzické útoky, hackerské útoky a vydieranie. Fyzický útok môže byť napríklad, krádež dôverných bankových údajov zamestnancom alebo zlodejom. Hackerský útok je braný ako krádež dát, špionáž zákazníkov, či sabotáž procesov spoločnosti pomocou škodlivých vírusov.

Cebula a Young (2010), ktorý vnímajú kybernetické riziká z operačného hľadiska ich rozdeľujú na štyri hlavné triedy, každá táto trieda je ďalej rozdelená do niekoľkých podtried. Rozdelenie tried vyzerá nasledujúco:

1. **Činy ľudí**
    - 1.1 Neúmyselné – Činy vykonané neúmyselne alebo bez akéhokoľvek zlého, či škodlivého úmyslu. Ide napríklad o chyby, omyly a opomenutia.
    - 1.2 Úmyselné – Činy vykonané úmyselne za účelom uškodiť. Ide napríklad o podvody, sabotáže, krádeže a vandalizmus.
    - 1.3 Nečinnosť – Nečinnosť alebo zlyhanie v konaní pri danej situácii. Ide napríklad o nedostatok vhodných zručností, vedomostí a schopnosti personálu konať.
2. **Systémové a technologické zlyhania**
    - 2.1 Hardvér – Riziká prameniace zo zlyhania fyzického vybavenia. Ide o poruchy z dôvodu kapacity, výkonu, údržby a zastarávania.
    - 2.2 Softvér – Riziká vyplývajúce zo softvérových aktív všetkých typov, vrátane programov, aplikácií a operačných systémov. Ide napríklad o kompatibilitu, správu konfigurácií, ovládanie zmien, bezpečnostné nastavenia, kódovanie a testovanie.
    - 2.3 Systémy - Zlyhanie integrovaných systémov vo fungovaní tak ako by sa očakávalo. Ide napríklad o dizajn, špecifikácie, integráciu a zložitosť.
3. **Zlyhanie interných procesov**
    - 3.1 Dizajn alebo vyhotovenie procesov – Zlyhanie procesov pri dosiahnutí očakávaných výsledkov, v dôsledku nedostatočného vyhotovenia alebo dizajnu procesov. Ide napríklad o procesný tok, procesnú dokumentáciu, roly a zodpovednosti, oznámenia a výstrahy, tok informácií, eskalácia problémov, dohody na úrovni služieb a úlohy.
    - 3.2 Kontrola nad procesmi – Neadekvátna kontrola nad prevádzkou procesu. Ide napríklad o sledovanie stavu, metriky, periodickú kontrolu a vlastníctvo procesu
    - 3.3 Podpora procesov – Organizačné zlyhanie podpory procesov, v dôsledku zlyhania príslušných zdrojov. Ide napríklad o personálne zabezpečenie, účtovníctvo, školenia a vývoj a obstarávanie.

4. Vonkajšie udalosti

4.1 Katastrofy – Udalosti prírodného aj ľudského pôvodu, nad ktorými organizácia nemá kontrolu a môžu sa stať bez akejkoľvek výstrahy. Ide napríklad o poveternostné katastrofy, požiare, povodne, zemetrasenia a nepokoje.

4.2 Právne problémy - Riziká vznikajúce z právnych problémov. Ide napríklad o dodržiavanie predpisov, legislatívu a súdne spory.

4.3 Problémy pri podnikaní – Riziká vyplývajúce zo zmien v podnikateľskom prostredí organizácie. Ide napríklad o zlyhanie dodávateľov, situáciu na trhu a ekonomické situáciu.

4.4 Závislosť na službách – Riziká pochádzajúce zo závislosti na externých stranách. Ide napríklad o komunálne služby, pohotovostné služby, palivo a dopravu.

Ďalšie rozdelenie kybernetických rizík je na úmyselné kybernetické riziká a neúmyselné kybernetické riziká. Toto rozdelenie uvádza vo svojej diplomovej práci Radek Zajíc (2016).

V oblasti kybernetických rizík identifikuje troch najčastejších pôvodcov úmyselných hrozieb a to zamestnancov, dodávateľov a vonkajšieho útočníka.

Medzi identifikované hrozby, ktoré spomenutí môžu pôsobiť, patrí krádež zariadenia, krádež dát, bezdôvodné zmazanie dát, prienik do kybernetickej siete, preťaženie systému, scudzenie autentizačných údajov, neautorizovaný prístup, odposluch dátových prenosov, úmyselne nesprávny vývoj aplikácií, chyby v aplikáciách a neoprávnená publikácia dát.

Typické incidenty, ktoré sú týmito pôvodcami hrozieb a hrozbami vyvolávané, sú krádež dát, straty dát, odopretie služby, scudzenie autentizačných údajov, neoprávnený prístup a zlyhanie zariadenia.

Pri úmyselných kybernetických rizikách sú typicky ohrozenými aktívami zákaznícke a firemné dáta, finančné aktíva podniku (incidenty vedúce k finančným stratám) a nefinančné aktíva (najmä riziko ohrozenia reputácie a straty zákaziek).

Všetci pôvodcovia hrozby, hrozby, incidenty a ohrozené aktíva sú rozdelené do tabuľky 1 Identifikácia úmyselných kybernetických rizík.

Tabuľka 1 Identifikácia úmyselných kybernetických rizík

Pôvodca hrozby	Hrozba	Incident	Ohrozené aktíva
Zamestnanec	Krádež dát	Krádež dát	Dáta Reputácia Finančné straty
Zamestnanec	Neautorizovaný prístup	Krádež dát	
Vonkajší útočník	Prienik do siete	Krádež dát	
Zamestnanec Vonkajší útočník	Preťaženie systému	Odopretie služby	
Vonkajší útočník	Ukradnutie autentizačných údajov	Ukradnutie autentizačných údajov	
Zamestnanec Vonkajší útočník	Infiltrácia siete	Krádež dát Odopretie služby Ukradnutie autentizačných údajov	
Zamestnanec Vonkajší útočník	Krádež zariadenia	Krádež zariadenia	
Zamestnanec	Bezdôvodné zmazanie dát	Strata dát	
Zamestnanec	Neoprávnená publikácia dát	Zverejnenie dát	
Zamestnanec Dodávateľ	Nesprávny vývoj Chyby v aplikáciách	Strata dát Krádež dát Zverejnenie dát Odopretie služby Ukradnutie autentizačných údajov Ukradnutie identity služby	
Vonkajší útočník	Chyby v aplikáciách		
Vonkajší útočník	Neexistujúce šifrovanie	Krádež dát Publikácia dát	
Vonkajší útočník	Odposluch dát	Krádež dát Publikácia dát	
Dodávateľ	Predčasné ukončenie podpory	Odopretie služby	
Zamestnanec	Zlá starostlivosť o kybernetické prostredie	Zlyhanie zariadení Strata dát Odopretie služby	

Zdroj: Vlastné spracovanie podľa Zajíca (2016)

V prípade neúmyselných kybernetických rizík začína s identifikáciou od ohrozených aktív, medzi ktoré patria typicky zákaznícke a firemné dáta, finančné aktíva podniku (incidenty vedúce k finančným stratám) a nefinančné aktíva (najmä riziko ohrozenia reputácie a straty zákaziek).

Možné incidenty, ktoré vedú k ohrozeniu aktív, sú najčastejšie strata dát, odopretie služby, neoprávnený prístup k dátam a prístup k dátam bez autentizácie (nevyžadovanie autentizácie, žiadna autorizácia). Ďalej scudzenie dát, neoprávnený prístup po sieti k zariadeniam, strata kontroly nad zariadením. Medzi extrémne incidenty patrí kolaps organizácie v dôsledku katastrofickej udalosti, proti ktorej neexistujú havarijné a kontingenčné plány v oblasti kybernetických systémov.

Hrozby, ktoré spôsobujú také incidenty, sú najmä zlyhanie dátového úložiska či nedostatočná dátová redundancia, neexistujúce, neotestované alebo nefunkčné zálohovanie dát, alebo strata prístupu k dátam, ktoré má pod svojou správou zamestnanec (v prípade využívania cloud computingu). Medzi nezanedbateľné hrozby patrí aj prítomnosť počítačových vírusov v kybernetických systémoch organizácií, preťaženia aplikácie a dátovej infraštruktúry. V oblasti prístupu k dátam vedú nedostatočne nastavené oprávnenia, chýbajúca autentizácia a šifrovanie dát. Niektoré incidenty môžu byť vyvolané aj zdieľaním technologických a užívateľských infraštruktúr (najmä sieťových), neriadeným zamestnancom a jeho zariadeniami (v prípade využívania konceptu Bring Your Own Device). Posledná, najzávažnejšia hrozba, je neexistujúci plán pre zotavenie z katastrofickej udalosti.

Typickými pôvodcami incidentu straty dát sú zastaraný hardvér, nedostatočná starostlivosť správcu kybernetického systému, odchod zamestnanca, nedostatočné zabezpečenie terminálov. V oblasti incidentu odopretia služby ide najmä o nedostatočnú redundanciu a kapacitu aplikácie, zastaranú architektúru aplikácie, nedostatočnú kapacitu infraštruktúry a neexistujúcu alebo nefunkčnú sieťovú redundanciu.

V oblasti dát a prístupov ide najmä o nedostatočnú starostlivosť správcu dát (nenastavovanie oprávnení), nevyžadovanie autentizácie a nenastavené šifrovanie. Neoprávnený prístup po sieti k zariadeniam, je často spôsobený neoddelením sietí alebo nedostatočnou vzájomnou ochranou týchto sietí. V oblasti kontroly nad zariadením identifikujem ako pôvodcu najmä zariadenia prítomné v kybernetickom prostredí v rámci konceptu Bring Your Own Device.

Incident kolapsu organizácie v dôsledku neexistujúcich alebo nefunkčných plánov zotavenia sa z katastrofickej udalosti má pôvodca v manažmente organizácie, ktorého povinnosťou je takýto plán zostaviť a kontrolovať jeho platnosť a funkčnosť.

Všetky ohrozené aktíva, incidenty, hrozby a pôvodcovia hrozby sú potom rozdelené do tabuľky 2 Identifikácia neúmyselných kybernetických rizík.

Tabuľka 2 Identifikácia neúmyselných kybernetických rizík

Ohrozené aktíva	Incident	Hrozba	Pôvodca hrozby
Dáta Reputácia Finančné straty	Strata dát	Zlyhanie úložiska	Zastaraný hardvér
		Nedostatočná redundancia	Nedostatočná starostlivosť správcu
		Neexistujúce, netestované alebo nefunkčné zálohovanie	Nedostatočná starostlivosť správcu
		Strata prístupu k dátam, ktoré má pod svojou správou zamestnanec (cloud computing)	Odchod zamestnanca
		Počítačové vírusy v organizácii	Nedostatočné zabezpečenie terminálov
	Odopretie služby	Preťaženie aplikácie	Nedostatočná redundancia a kapacita aplikácie, zastaralá architektúra aplikácie
		Preťaženie dátovej infraštruktúry	Nedostatočná kapacita infraštruktúry
		Strata konektivity	Neexistujúca alebo nefunkčná sieťová redundancia
	Neoprávnený prístup k dátam	Nedostatočné nastavenie oprávnení	Nedostatočná starostlivosť správcu
	Prístup bez autentizácie	Nenastavená autentizácia	Nevyžadovanie autentizácie
	Scudzenie dát	Neexistujúce šifrovanie	Nenastavené šifrovanie
	Neoprávnený prístup po sieti k zariadeniam	Spoločné užívateľské a technologické siete	Nenastavenie oddelených sietí, nedostatočná ochrana sietí
	Strata kontroly nad zariadením	Neriadený zamestnanec	Vlastné zariadenie v sieti
	Kolaps organizácie	Neexistujúci alebo nefunkčný plán pre zotavenie z katastrofickej udalosti	Manažment

Zdroj: Vlastné spracovanie podľa Zajica (2016)

1.1.2 Kybernetická hrozba

V súvislosti so zdrojom rizika sa niekedy používa aj pojem „threat“, ktorý sa prekladá ako „hrozba“. Tento pojem sa zvyčajne používa na vyjadrenie zámeru spôsobiť škodu alebo inú ujmu na ľudskom zdraví, životnom prostredí či materiálnych hodnotách, používa sa však aj ako synonymum pojmu hazard. Niekedy sa nebezpečenstvo chápe ako aktivovaná hrozba, t. j. napríklad existencia potoka v obci je hrozbou, nebezpečenstvom sú dlhotrvajúce dažde, ktoré môžu spôsobiť výrazné zvýšenie hladiny vody. (Krátka, 2009)

Zdrojom kybernetického rizika je kybernetická hrozba, ktorá je zadefinovaná v Zákone o kybernetickej bezpečnosti č. 69/2018 Z.z. ako: „Kybernetická hrozba je každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť.“ Kybernetická hrozba je teda konkrétny zdroj kybernetického rizika, a teda udalosť, ktorá môže nastať. Keďže sa kybernetická hrozba priamo týka pojmu kybernetické riziko a ide o okolnosť, ktorá môže kedykoľvek nastať, musíme si ju lepšie popísať. Kybernetická hrozba zvykne byť často označovaná v praxi ako kybernetický incident. Spoločnosť Kooperativa (2012) má v poistných podmienkach kybernetický incident zadefinovaný ako: „úmyselné konanie tretej osoby vedúce k poškodeniu, zničeniu, strate alebo odcudzeniu dát v počítačovom systéme poisteného (napr. hackerský útok, malware, ransomware), ktoré nie je dôsledkom predchádzajúceho poškodenia, zničenia, odcudzenia alebo straty hardware.“

ENISA v roku 2021 vytvorila analýzu s názvom ENISA Threat Landscape 2021, v skratke nazývanú ETL. Z tejto analýzy vyšla správa, v ktorej sa píše o ôsmych primárnych skupinách kybernetických hrozieb a tie sú:

1. ransomvér (ransomware),
2. malvér (malware),
3. skryté ťaženie kryptomien (cryptojacking),
4. hrozby spojené s e-mailom (e-mail related threats),
5. hrozby voči dátam (threats against data),
6. hrozby proti dostupnosti a integrite (threats against availability and integrity),
7. dezinformácie a nesprávne informácie (disinformation-misinformation),
8. neúmyselné hrozby (non-malicious threats).

Ransomvér (ransomware)

Je typ škodlivého útoku, pri ktorom útočníci zašifrujú údaje organizácie a požadujú výkupné, pre obnovenie prístupu organizácii k ich údajom. V niektorých prípadoch môžu

útočníci tiež ukradnúť informácie organizácie a požadovať ďalšie platby výmenou za nesprístupnenie informácií orgánom, konkurentom alebo verejnosti. Phishingové e-maily a hrubé vynútenie služieb protokolu RDP (Remote Desktop Protocol) sú dva najbežnejšie typy preniknutí. Počas sledovaného obdobia v roku 2021 ENISA zistila, že aktéri hrozby používajúci Conti a REvil dominovali na trhu ransomvéru z hľadiska finančného, ako aj z hľadiska objemu preniknutí. Conti a REvil poskytujú samostatné platformy ransomware-as-a-service (RaaS), prostredníctvom ktorých môžu útočníci efektívne organizovať svoje útoky. Zameranie sa na o modely typu RaaS sa v priebehu roku 2021 zvýšilo, vďaka čomu je ťažšie tieto útoky pripísať individuálnemu aktérovi hrozieb . Počas roku 2021 sa výrazne zvýšil aj výskyt viacnásobných vydieračských schém. Po počiatočnej krádeži a šifrovaní citlivých údajov od organizácií a vyhrážanie sa ich zverejnením, pokiaľ nezaplatia, sa útočníci taktiež zameriavajú aj na zákazníkov a partnerov organizácií, aby získali výkupné aj od nich. Týmto spôsobom sa útočníci snažia maximalizovať svoje zisky. Kryptomeny zostávajú najbežnejšou metódou pre vyplácanie aktérom hrozieb. Útočníci však začali namiesto Bitcoinu preferovať Monero ako ich zvolenú kryptomenu, kvôli jej zvýšenej anonymite a nerozoznateľnosti transakcií. Priemerná výška výkupného sa oproti roku 2020 za posledný rok zdvojnásobila , hoci nižšie výkupné je medzi aktérmi hrozieb stále obľúbené. Nižšie výkupné má tendenciu byť ľahšie vyplácané a má za následok menšiu verejnú expozíciu pre aktéra hrozby. Vyššie výkupné taktiež vzrástli a v priebehu niekoľkých mesiacov sa najvyššia čiastka za výkupné požadovaná v roku 2020, v roku 2021 viac ako zdvojnásobila.

Malvér (malware)

Malvér je zastrešujúci pojem, ktorý popisuje akýkoľvek softvér, firmvér alebo kód určený na vykonanie zlomyseľného neoprávneného procesu, ktorý bude mať nepriaznivý vplyv na dôvernosť, integritu alebo dostupnosť systému. Príkladom škodlivého softvéru môže byť vírus, červ, trójsky kôň alebo iné entity založené na kóde, ktoré infikujú hostiteľa. Spyware a niektoré formy adware sú tiež súčasťou pojmu malvér. Malvér môže mať rôzne a rôzne možnosti v závislosti od cieľa tvorcu. Napríklad RATs (Trójske kone/Nástroje so vzdialeným prístupom) je malvér, ktorý aktérovi umožňuje diaľkové ovládanie infikovaného systému. Infostealers alebo Skimmers sú navrhnuté tak, aby zachytávali informácie o kreditnej karte. Botnety sú robotická sieť počítačov infikovaných škodlivým softvérom a riadené servermi C&C. Trójske kone, ktorými môže byť bankový trójsky kôň alebo mobilný trójsky kôň v závislosti od cieľa, sú malvér, ktorý sa často vydáva za legitímny softvér. Škodlivý softvér je zastrešujúci pojem, ktorý popisuje akýkoľvek softvér, firmvér alebo kód

určený na vykonanie škodlivého procesu. Malvérové útoky počas sledovaného obdobia výrazne poklesli. Výskum ukázal, že útoky v Severnej Amerike poklesli o 43 % v roku 2020 v porovnaní s rokom 2019. Tento pokles bol takmer rovnaký v Európe, v Ázii bol zaznamenaný pokles o 53 %. Jeden z kľúčových faktorov tohto zníženia by mohol súvisieť s pandémiou COVID19. Zamestnanci pracovali viac z domu a využívali svoje osobné počítače na pracovné činnosti. Toto domáce prostredie a infraštruktúra nemajú rovnakú úroveň ochrany a detekcie, čo obmedzuje viditeľnosť malvérových infekcií. Zníženie tejto viditeľnosti môže spôsobovať práve tento pokles, keďže zozbierané štatistické údaje sú založené iba na zisťovaní prienikov v podnikovom prostredí. V prvých šiestich mesiacoch roku 2021 výskyt malvérových infikovaní naďalej klesal a výskum ukázal, že dosiahol zredukovanie o ďalších 22% oproti tej istej perióde v roku 2020.

Skryté ťaženie kryptomien (cryptojacking)

Cryptojacking alebo skryté ťaženie kryptomien je typ počítačovej kriminality, pri ktorej zločinec tajne používa výpočtovú techniku obete na generovanie kryptomeny. K tomu zvyčajne dochádza, keď si obeť nevedomky nainštaluje program so škodlivými skriptami, ktoré umožňujú zločincovi prístup k jeho počítaču alebo iným zariadeniam pripojeným na internet. K tomu dochádza napríklad pri kliknutí na neznámy odkaz v e-maile alebo pri návšteve infikovanej webovej stránky. Zločinci potom používajú programy na vytváranie alebo ťaženie kryptomien. Počas sledovaného obdobia ENISA zaznamenala rastúci trend v cryptojackingu, ktorý by mohol byť spojený so zvýšenou volatilitou na trhu s kryptomenami, ktorá bola počas tohto obdobia pozorovaná. Vzhľadom na to že kryptomeny ponúkajú anonymitu, stávajú sa veľmi atraktívnym a pohodlným prostriedkom výmeny medzi kybernetickými zločincami. V súlade s tým treba poznamenať, že kryptomeny sa vo všeobecnosti vyžadujú ako výkupné pri ransomvérových útokoch. Od roku 2019 sme svedkami neustáleho poklesu ťaženia kryptomien za posledných niekoľko rokov. Pokles je v súlade s klesajúcou hodnotou ziskovosti ťažby a bol urýchlený odstávkou Coinhive v marci 2019 a JSECoin v apríli 2020. Útočníci však prešli k iným typom škodlivých aktivít, pokiaľ ide o cryptojacking. Podľa správy od spoločnosti Cisco 69 % jej zákazníkov bolo v roku 2020 zasiahnutých malvérom ťažiacim kryptomeny. Podľa tej istej správy, ťaženie kryptomien vygenerovalo najväčšiu vyťaženosť DNS oproti akejkoľvek inej zákernej aktivite. V marci 2020 bol zaznamenaný prudký nárast infikovaní, po ktorom miera infikovania dramaticky klesla. Od druhého do posledného štvrťroka 2020 sa objem infekcií pomaly zvyšoval a pokračovalo to aj v roku 2021. V prvom štvrťroku v roku 2021 dosiahol

objem infekcií v porovnaní s poslednými rokmi rekordnú výšku. Potvrdzuje to aj trend, ktorý ukazuje, že počas prvého štvrťroka 2021 sa výskyt malvéru na ťaženie kryptomien zvýšil o 117 %. Na základe kolísajúcej hodnoty kryptomien, ENISA predpokladá, že cryptojacking zostane dôležitým útočným vektorom aj v roku 2022.

Hrozby spojené s e-mailom (e-mail related threats)

Hrozby súvisiace s e-mailom sa už niekoľko rokov neustále umiestňujú na popredných miestach v zozname hlavných hrozieb v ETL. Táto zbierka hrozieb využíva slabé stránky ľudského správania týkajúceho sa e-mailov a ľudských návykov a má za cieľ zmanipulovať ľudí, aby sa stali obeťami útoku. Hrozby súvisiace s e-mailom sú vo všeobecnosti menej zamerané na technickú zraniteľnosť informačných systémov, ale predovšetkým na informovanosť koncových používateľov a využívaní prirodzenej dôvery, ktorú ľudia vkladajú do svojej e-mailovej komunikácie. Tento druh hrozieb pozostáva hlavne z nasledujúcich vektorov: phishing, spear-phishing, whaling, smishing, vishing, kompromitácia obchodných e-mailov (BEC) a spam.

Phishing sa zameriava na odcudzenie dôležitých informácií, ako sú čísla kreditných kariet a heslá, prostredníctvom e-mailov, ktoré zahŕňajú sociálne inžinierstvo a podvod. Spear-phishing je sofistikovanejšia verzia phishingu, ktorá sa zameriava na konkrétne organizácie alebo jednotlivcov. Lov veľrýb je spear-phishingový útok zameraný na používateľov na vysokých pozíciách (riaditeľov, politikov atď.). Smishing, pojem odvodený ako spojenie „SMS“ a „phishing“, nastáva vtedy, keď sa finančné respektíve osobné údaje obetí zhromažďujú prostredníctvom SMS správ. Ďalším typom hrozby súvisiacej s e-mailom je vishing, kombinácia phishingu a hlasu, ku ktorej dochádza pri poskytovaní informácií cez telefonát, v ktorom sa zlomyseľní aktéri pomocou techník sociálneho inžinierstva snažia od používateľov získavať citlivé informácie. Kompromitácia obchodných e-mailov (BEC) je sofistikovaný podvod zameraný na podniky a organizácie. Útočníci využívajú techniky sociálneho inžinierstva, na získanie prístupu k e-mailovému účtu zamestnanca alebo vedúceho pracovníka, za účelom iniciovať bankové prevody za podvodných podmienok. Spam je akýkoľvek druh nechceného, nevyžiadaného digitálneho obsahu, ktorý sa odosiela hromadne. Spam sa často odosiela e-mailom, ale môže sa šíriť aj prostredníctvom textových správ, telefónne hovorov alebo sociálnych sietí. Pandémia umožnila týmto typom hrozieb veľký rozmach. Ľudská potreba komunikácie a teda aj online vystupovanie práve kvôli pandémii a opatreniam narástla. Digitalizácia mnohých doteraz klasických služieb a teda aj

presun z priamej komunikácie, na komunikáciu cez e-mail alebo chat, či iný nástroj kybernetického prostredia, spôsobila nepopierateľný nárast hrozieb spojených s e-mailom.

Hrozby voči dátam (threats against data)

Hrozby voči dátam či údajom tvoria súbor hrozieb, ktoré sa zameriavajú na zdroje údajov s cieľom získať neoprávnený prístup, vyzradiť ich, dezinformovať a podobne. Označujú sa najmä ako úniky údajov alebo úniky dát a týkajú sa vypustenia citlivých, dôverných alebo chránených údajov do nedôveryhodného prostredia. Narušenie údajov môže nastať ako a výsledok kybernetického útoku, neúmyselnej straty alebo vydanie údajov internou osobou spolupracujúcou s útočníkom. Exfiltrácia údajov alebo krádež údajov je a technika, ktorú používajú útočníci na zacielenie, kopírovanie a prenos citlivých údajov. Konkrétny prípad ukradnutých údajov je krádežou identity, pri ktorej útočníci používajú osobné identifikačné informácie. Hrozby voči dátam sú trvalo vysoko medzi poprednými hrozbami ETL a tento trend pokračuje aj v vykazovanom období ETL 2021. Protivníci skúmajú sériu nových techník a využívajú čoraz viac online prítomnosti a používanie online služieb širokou verejnosťou. Navyše, vzhľadom na význam údajov a najmä súkromné a citlivé údaje, protivníci kombinujú sofistikovanejšie hrozby ako je ransomvér alebo útoky na dodávateľský reťazec, aby sa práve na tieto údaje zamerali. ENISA v roku 2021 zaznamenala, že za 85% únikov dát môže ľudský element.

Hrozby proti dostupnosti a integrite (threats against availability and integrity)

Dostupnosť a integrita sú cieľom množstva hrozieb a útokov, medzi ktoré patria a vyčnievajú rodiny distribuovaných odmietnutí služby (DDoS) a webových útokov.

Distribuované odmietnutie služby (DDoS) sa zameriava na dostupnosť systému a údajov. Hoci nejde o novú hrozbu a existuje už 23 rokov, naďalej zostáva významnou hrozbou v kybernetickom prostredí. K útokom dochádza, keď používatelia systému alebo služby nemajú prístup k relevantným informáciám, službám alebo iným zdrojom. Toto sa dá dosiahnuť preťažením služby alebo preťažením komponentu sieťovej infraštruktúry.

Webové útoky sa zameriavajú najmä na integritu a dostupnosť údajov. Sú atraktívnou metódou, ktorou aktéri môžu oklamať obete pomocou webových systémov a služieb. Tento spôsob pokrýva rozsiahlu útočnú plochu, napríklad umožňuje škodlivým adresám URL (Uniform Resource Locators) alebo škodlivým skriptom, nasmerovať používateľa alebo obeť na požadovanú webovú stránku, stiahnuť škodlivý obsah, alebo pomocou zavádzania škodlivého kódu na legitímnu, ale kompromitovanú webovú stránku odcudziť informácie, za účelom finančného zisku a krádeži informácií. DDoS a webové

útoky sú často koordinované aktivity. DDoS útoky môžu byť postavené na webových útokoch, ktoré sú často distribuované prostredníctvom webových aplikácií. Napríklad webové útoky môžu byť adaptované na vybudovanie bot-netu, ktorý sa potom použije na vykonanie DDoS útoku, ktorého cieľom je zneprístupniť systém. Aj tento druh hrozieb narástol počas COVID-19 pandémie. ENISA uvádza, že zaznamenala nárast v roku 2020 o 22% a v prvom kvartáli roku 2021 o 40% oproti poslednému kvartálu v roku 2020.

Dezinformácie a nesprávne informácie (disinformation – misinformation)

Nárast využívania digitálnych technológií a sociálnych médií zmenil spôsob, akým ľudia pristupujú k informáciám a novinkám. Na rozdiel od tradičných médií (napr. noviny, televízia), sociálne médiá zaručujú priamy prístup k informáciám so žiadnymi filtrami. Cena, ktorú platíme za takýto pohodlný spôsob prístupu k informáciám, je zvyšujúce sa riziko získania falošných informácií, správ a zmanipulovaných informácií. V tomto kontexte sociálne médiá preberajú úlohu preferovaného zosilňovača informácií, oveľa viac ako, príchod tradičných médií. Tieto informácie môžu byť falošné (preto sa mení vnímanie reality u ľudí), alebo skutočné (informácie o incidentoch, chybách, stratách, názoroch a povesti spoločnosti). Zosilňujúci efekt sociálnych aj tradičných médií je dôležitou hrozbou pre jednotlivcov, podniky a dokonca aj štáty, pretože nepravdivá správa môže byť vnímaná ako skutočná a zdanlivo nepodstatný problém sa môže stať vo verejnej mienke veľkým incidentom. Sociálne médiá môžu byť manipulované tak, aby sa stali účinnými vektormi dezinformačných či očierňovacích kampaní proti spoločnostiam alebo povesti niektorých z ich najreprezentatívnejších jedincov. Pri týchto hrozbách je ohrozená reputácia značky, finančná spoľahlivosť spoločnosti, dôveryhodnosť a čestnosť spoločnosti alebo jednotlivcov.

Dezinformácie (disinformation) sú vnímané ako úmyselný útok, ktorý pozostáva z vytvárania alebo zdieľania nepravdivých alebo zavádzajúcich informácií. Dezinformačné útoky zaznamenali exponenciálny nárast v období pandémie COVID-19, napríklad dôveru ľudí voči vakcínam.

Nesprávne informácie (misinformation) sa berú ako neúmyselný útok, pri ktorom k zdieľaniu informácií dochádza neúmyselne. Prenesená nepresnosť informácie je neúmyselná a môže sa stať napríklad vtedy, keď novinár uvedie nesprávne informácie s dobrým úmyslom alebo oznamuje nesprávne informácie omylom. K šíreniu nesprávnych informácií patria aj scenáre, v ktorých ľudia veria informácii bez ohľadu na pravdivosť, pretože podporuje ich svetonázor.

Neúmyselné hrozby (non-malicious threats)

Hrozby sa bežne považujú za dobrovoľné a zlomyseľné aktivity vykonávané protivníkmi, ktorí majú podnet pre útok na konkrétny cieľ. V tejto časti sa zaoberáme hrozbami, pri ktorých nie je zjavný zlý úmysel. Neúmyselné hrozby sú väčšinou založené na ľudských chybách a nesprávnej konfigurácii systému, ale môžu sa týkať aj fyzických katastrof, ktoré sa zameriavajú na IT infraštruktúry. Neúmyselné hrozby možno klasifikovať do dvoch kategórií a to sú chyby alebo nesprávna konfigurácia a fyzické katastrofy.

Chyby a nesprávna konfigurácia sú spôsobené nedbalosťou, nedostatočnou informovanosťou alebo jednoducho ľudskými chybami a zahŕňajú:

- **Chyby pri riadení IT systému:** Nesprávne konfigurácie zavedené pri špecifických aplikáciách a systémoch v prípadoch, keď bývajú (re-)konfigurované a aktualizované. Chybné riadenie systému, vrátane chýb pri opravovaní a aktualizácii systému. Chybná správa systému, napríklad pri rozdeľovaní privilégií medzi užívateľov. Problémy v riadení tradičných systémov, ako je sieťová bezpečnosť, kontrola prístupu, správa identity.
- **Chyby v čase vývoja:** Problémy s riadením závislostí, napríklad používané knižnice bez toho, aby si to vývojári všimli. Dlhodobé problémy, napríklad bezpečnosť pamäte, neupravené vstupy a vo všeobecnosti problémy s dobre známymi riešeniami zahŕňajúcimi použitie moderných nástrojov. Iné formy nedbalosti, napríklad ukladanie prihlasovacích údajov aplikácie na verejné úložiská.
- **Chyby na úrovni aplikácie:** Chyby zavedené pri používaní aplikácie alebo systému. Nesprávne nakonfigurované cloudové aplikácie a zlá správa hesiel a kľúčov, napríklad verejne dostupné a nešifrované databázy. Menšie chyby, ako napríklad odoslanie e-mailu nesprávnemu príjemcovi.
- **Fyzické chyby:** zariadenia bez obsluhy, nezabezpečené dokumenty alebo informácie, výnimky z fyzického prístupu k pravidlám .

Fyzické katastrofy môžu byť klasifikované ako:

- Poškodenia alebo zlyhania fyzickej infraštruktúry, ako napríklad neúmyselné poškodenie optických káblov, strata internetového pripojenia, požiar, nestabilné napájanie.
- Prírodné katastrofy, ako sú povodne a zemetrasenia, spôsobujúce nedostupnosť IT infraštruktúry a s tým súvisiace služby a aplikácie.

1.2 Poistiteľnosť rizík

Stanovenie poistiteľnosti je veľmi komplikované. V literatúre sú na toto stanovenie použité rôzne definície a kritériá. Definícia poistiteľnosti sa zvykne posudzovať z určitého hľadiska. Holsboer (1955) definuje poistititeľnosť z hľadiska dopytu. Podľa neho je poistiteľnosť, situácia kedy je umožnené poistníkom zakúpiť si primerané krytie, ktoré potrebujú. Courbage a Liedtke (2003) definujú poistiteľnosť z aktuárskeho hľadiska, pričom riziko je považované za poistiteľné, až keď aplikovateľný zákon veľkých čísel. Kunreuther (1997) definuje poistiteľnosť z hľadiska ponuky a hovorí, že je udalosť poistiteľná, ak sú poisťovatelia schopný stanoviť poistné odrážajúce riziko a toto poistné im umožňuje generovať zisk. Podľa Kartena (1997) sú riziká poistiteľné, ak existuje aj poisťovateľ aj poistník, ktorý akceptuje podmienky a cenu poistného krytia.

Ak chceme, aby bolo riziko poistiteľné je nevyhnutné, aby spĺňalo niekoľko nevyhnutných podmienok. Podľa publikácie ktorú zverejnila Insurance Europe a preložila Slovenská asociácia poisťovní (2012) pod názvom „Ako funguje poisťovníctvo“, sú podmienky poistiteľnosti rizika nasledovné:

- riziko musí byť definovateľné a finančne merateľné,
- riziko musí byť náhodné a nezávislé,
- poistený musí mať o poistenie záujem,
- poisťovňa musí byť schopná vypočítať pre dané riziko primerané poistné,
- pravdepodobnosť výskytu rizika sa musí dať vypočítať,
- riziko katastroficky veľkých strát nesmie byť príliš veľké,
- poistné krytie vo všeobecnosti slúži na odškodnenie.

Riziko musí byť definovateľné a finančne merateľné

Ak dané riziko nastane, poistenie ponúka odškodnenie finančného charakteru alebo inú odmenu či službu. Z tohto dôvodu musí byť riziko jasne definovateľné, aby boli vylúčené budúce spory o to, či poistná udalosť skutočne nastala a teda, či má poistená strana nárok na odškodnenie. Je potrebné, aby bola vyčíslená aj výška možnej straty, aby sa dalo rozhodnúť o výške požadovaného odškodnenia. Napríklad pri poistení proti krádeži vozidla kde je jasne definované kedy poistná udalosť nastala a aj výška poistného plnenia, je to pomerne jasné. Pri zraneniach nadobudnutých nehodou často o výške odškodnenia rozhoduje až súd. Pri životnom poistení kde sa finančné straty nedajú jasne vyčísliť je výška odškodnenia stanovená vopred.

Riziko musí byť náhodné a nezávislé

Ak je isté, že nejaká udalosť nastane, nie je možné sa voči tejto udalosti poistiť, keďže táto skutočnosť nespôsobuje neistotu, a z tohto dôvodu nie je možný ani prenos rizika. Existencia rizika, ktoré je predmetom poistenia, musí byť nepredvídateľná alebo aspoň neovplyvniteľná a nedosiahnuteľná tým, kto má právo za toto poistenie inkasovať odškodnenie. To znamená, že škody spôsobené opotrebovaním, či bežným používaním alebo škody spôsobené vedome a zámerne poistenou osobou, alebo osobou s ktorou sa poistený dohodol, nemôžu byť predmetom poistenia. Tieto zásady sa vzťahujú aj na životné poistenie. Smrť ako poistná udalosť je síce istá, ale čas kedy nastane, sa nedá vopred určiť.

Poistený musí mať o poistenie záujem

Medzi poisteným a rizikom, pred ktorým sa poistil musí existovať jasný vzťah. Bežne je tento záujem naplnený tým, že poistená osoba vlastní predmet, na ktorom poistná udalosť vznikla alebo je v priamom vzťahu s osobou, ktorá zomrela a tým pádom jej môže byť odškodnenie vyplatené. Poistný záujem môžu mať ľudia v prípade svojich áut či domovov, ale nie v prípade domovov či áut svojich susedov, pretože tie nevlastnia.

Poisťovňa musí byť schopná vypočítať pre dané riziko primerané poistné

Skutočnosťou že poisťovňa ponúka poistenie, na seba preberá budúce záväzky, za krytie rizík poisteného. Tým pádom si musí účtovať poistné dostatočne vysoké na to, aby bola v budúcnosti tieto riziká schopná pokryť a zároveň jej to musí priniesť aj zisk, aby mohla naďalej fungovať. Na druhej strane je však jednotlivec či spoločnosť, ktorí poistné platia, nazývaní aj ako poistníci. Výška poistného musí teda dosahovať sumu, ktorú je poistník ochotný platiť. Výška poistného musí byť výrazne nižšia ako je výška poistného krytia, pretože by pre poistníka nemalo zmysel sa poistiť. Rovnováha medzi týmito dvoma skutočnosťami sa najlepšie dosahuje na otvorenom a konkurenčnom trhu komerčného poistenia.

Pravdepodobnosť výskytu rizika sa musí dať vypočítať

Výpočet pravdepodobnosti rizika slúži na to, aby poisťovňa vedela vypočítať primerané poistné. Poisťovňa počíta priemernú výšku škody a frekvenciu výskytu danej alebo podobnej poistnej udalosti, s určitou mierou presnosti. Pre tento výpočet slúži analýza dostatočne veľkého počtu poistných nárokov za rovnakú poistnú udalosť v minulosti a taktiež aj vlastné skúsenosti poisťovne z priemyselných dát či iných zdrojov.

Riziko katastroficky veľkých strát nesmie byť príliš veľké

Finančný dosah strát nemôže dosiahnuť takú vysokú úroveň, pri ktorej by poisťovňa nebola schopná pokrytie týchto strát vyplatiť. V tomto prípade zvyknú poisťovne využívať na zníženie miery vlastného vystavenia sa riziku zaistenie. Zaistenie sa dá považovať ako poistenie pre poisťovne, kde sa časť rizika prenáša na jednu alebo viac zaisťovní. Najčastejším prípadom sú letecké nešťastia alebo poistenia prírodných katastrof, kde sa škody môžu vyšplhať na naozaj vysokú úroveň.

Poistné krytie vo všeobecnosti slúži na odškodnenie

Ak poistník utrpí škodu a nastane poistná udalosť, vyplatenie tejto poistnej udalosti musí byť na zhodujúcej sa úrovni so škodou ktorú poistník naozaj utrpel. V opačnom prípade by to mohlo meniť správanie sa poistníka spôsobom, že by mohol na poistení zarábať a riziko straty by sa stalo pravdepodobnejším.

Na to aby bolo riziko poistiteľné musí podľa P. Chovana (2006) riziko spĺňať nasledujúce podmienky:

- riziko by malo byť identifikovateľné,
    - definovateľné – presné pomenovania a ohraničenia rizika,
    - analyzovateľné – z hľadiska veľkosti rizika a frekvencie jeho výskytu,
- prejav rizika musí byť náhodný,
- straty spôsobené rizikom by mali byť vyčísliteľné,
- malo by byť ekonomicky prijateľné aj pre poisťovňu, aj pre poisteného.

Identifikovateľnosť je teda možnosť jednoznačné určenie príčiny a typu incidentu, ktorý za vniknutú škodu môže. V poistnej zmluve sa musí nachádzať jednoznačná charakteristika rizík a udalostí, na ktoré sa poistenie vzťahuje. Vďaka analýze je možné riziko posúdiť a vypočítať jeho objektívnu sadzbu. To či sa incident udeje alebo neudeje musí byť čisto náhodné. Iba vďaka tomu sa stav vyrovnanosti zachová. Nevyhnutnou podmienkou je vyčíslenie škody, pri ktorej by došlo po incidente. Výška tejto straty alebo škody by nemala byť ovplyvnená subjektívnym pohľadom posudzovateľa a mala by mať objektívne pravidlá. Ekonomicky prijateľné riziko je také , ktoré je dobre plošne a časovo rozložené a umožňuje dosiahnuť ekonomickú vyrovnanosť poistenia. Poistník je však ochotný uzavrieť len také poistenie, pri ktorom je cena tohto poistenia primeraná riziku, ktoré pokrýva.

Riziká spĺňajúce všetky teoretické podmienky poistiteľnosti však nemusia byť poistnej praxi reálne poisťované. Každá poisťovňa si stanovuje svoj zoznam rizík, pre ktoré poistné krytie neposkytujú. Môže to byť z dôvodu, že rozsah licencie poisťovne nepovoľuje tieto riziká danej poisťovni poisťovať, z hľadiska strategických zámerov (poisťovňa nemá záujem o daný segment, v ktorom sa riziká vyskytujú), z hľadiska ekonomickej nevýhodnosti (poisťovňa nie je schopná pokryť výšku možných škôd, alebo mimoriadne škody spôsobujú poisťovni zhoršené ekonomické výsledky a tým pádom poisťovňa vypustí dané riziko z poistenia). (Krátka, 2020)

1.3 Poistiteľnosť kybernetických rizík

Kybernetické riziká sú v dnešnej dobe na vzostupe a stávajú sa najväčšou hrozbou pre podniky. To si uvedomujú aj poisťovne a čím viac sa snažia poskytovať poistenia, práve voči tomuto druhu rizík.

Portál banky.sk (2020) uvádza, že „Kybernetické útoky sú podľa Allianz Risk Barometra 2020 najväčšou celosvetovou hrozbou pre firmy. Za najväčšie riziko, 39 % hlasov, ich označilo 2718 poisťovacích expertov zo 102 krajín, ktorí sa do 9. prieskumu skupiny Allianz zapojili."

Pre to aby sme kybernetické riziká mohli nazvať poistiteľnými, by mali z teoretického pohľadu spĺňať všetky princípy alebo podmienky poistiteľnosti. Pri kybernetických rizikách však prichádzame do problému, že mnoho týchto rizík práve nespĺňa tieto podmienky poistiteľnosti. Ako sme v predchádzajúcej kapitole spomenuli, kritériá pre poistiteľnosť uvádza veľké množstvo autorov. Medzi tie základné však podľa Majtánovej (2005) patria identifikovateľnosť, náhodnosť udalosti, vyčísliteľnosť straty a ekonomická únosnosť.

Podľa týchto kritérií popisuje poistiteľnosť kybernetických rizík aj Brokešová (2014). Z hľadiska identifikovateľnosti nastávajú podľa nej pri kybernetických rizikách dva problémy. Prvým problémom je to, že kybernetický priestor sa nedá ohraničiť a všetky siete sú vďaka nemu celosvetovo prepojené. Vďaka tomuto prepojeniu sa nedajú informačné systémy spoločnosti posudzovať samostatne. Druhým uvedeným dôvodom je to, že podstata straty je pri tomto prípade nefyzická. To znamená, že pri údajoch ktoré boli spoločnosti odcudzené, napríklad osobné údaje zákazníka, nie je skoro vôbec možné dokázať čo bolo spoločnosti odcudzené. Napríklad v prípade odcudzenia osobného automobilu sa na základe vlastníctva dá dokázať, že bol tento automobil odcudzený. No v prípade krádeže údajov je

to zložitejšie, pretože si útočník mohol údaje len skopírovať a spoločnosť k nim stále môže mať prístup. Dôsledné vymedzenie a charakteristika jednotlivých rizík v poistných podmienkach, však pomáhajú tento problém poisťovniam riešiť.

Podľa Brokešovej je náhodnosť pri kybernetických rizikách veľmi špecifická oblasť. Uvádza, že z hľadiska poisteného môžu byť kybernetické riziká chápané ako náhodné, no pri technológiách je tento problém náhodnosti limitovaný. Ako dve hladné problémové oblasti uvádza zlyhanie technického a programového vybavenia a činnosť tretích osôb. Ani jedna z týchto oblastí však skutočnosti nemôže byť braná ako jednoznačne náhodná. Za vznikom týchto hrozieb môže stáť ľudský faktor. Kvôli výskytu ľudského faktora za týmito hrozbami, nie je možné označiť všetky kybernetické riziká ako náhodné.

Ako Brokešová udáva, problém vyčíliteľnosti straty je úzko spätý s problémom nejednoznačnej identifikovateľnosti. Pokiaľ nie je možné riziko jednoznačne identifikovať nastáva veľký problém aj pri vyčíslení straty, ktorá nastala alebo nastať môže. Ako príklad uvádza veľké databázy údajov o zákazníkoch . Tieto databázy majú pre spoločnosti nevyčísliteľnú hodnotu, keďže sa v nich často nachádzajú údaje, ktoré sa už vôbec alebo len veľmi ťažko znovu dajú získať. Firma taktiež pri strate týchto údajov môže prísť o reputáciu a dôveru zákazníkov, čo môže viesť až ku likvidačnému dopadu na spoločnosť. Reálna hodnota údajov o zákazníkoch sa však skladá z hodnoty vynaložených prostriedkov na získanie týchto údajov. Eling a Wirfs (2016) udávajú, že veľký problém pri vyčísliteľnosti nastáva hlavne kvôli nedostatku informácií o kybernetických rizikách. Keďže je táto téma vo svete veľmi krátko a kybernetické riziká sa vyvíjajú enormným tempom, neexistuje dostatočné množstvo štatistík, podľa ktorých by vedeli poskytovatelia tohto druhu poistení objektívne kybernetické riziká ohodnotiť a rovnako aj vypočítať pravdepodobnosť výskytu daných incidentov. Poisťovatelia teda tieto riziká hodnotia na základe subjektívneho postoja a ich ochoty tieto riziká poisťovať. Aj v prípade kybernetických rizík je ekonomická únosnosť nevyhnutná podmienka poistiteľnosti. Podľa tejto podmienky by poisťovne mali byť schopné ponúknuť poistenie kybernetických rizík za takú sumu a v takej výške poistného krytia, aby budúci poistníci mali o toto poistenie záujem, aby sa im oplatilo danú sumu za poistenie z pohľadu na krytie platiť. Zároveň musí byť toto poistné krytie v takej výške, aby pri prípadnom incidente vedela toto krytie poisťovňa vyplatiť. Ekonomická únosnosť úzko súvisí s problémom akumulačného rizika. Význam akumulačného rizika uvádzajú Hannover Re na svojej internetovej stránke pod rovnakou definíciou ako je akumulačná strata. Hannover Re uvádzajú, že **akumulačná strata** je „súčet niekoľkých individuálnych strát, ktoré vznikli rôznym poistencom v dôsledku tej istej škodovej udalosti

(napr. veterná smršť, zemetrasenie). To môže viesť k vyššej škode pre priameho poisťovateľa alebo zaisťovateľa, ak je uvedenou spoločnosťou poistených viacero dotknutých poistencov.“ Pri kybernetických rizikách je pravdepodobnosť vniknutia akumulačnej straty naozaj vysoká. Hackeri sú schopní zaútočiť na viacero spoločností súčasne alebo na takú časť kybernetického priestoru, ktorej výpadok spôsobí škodu viacerým spoločnostiam naraz. Z tohto dôvodu poisťovne často nepoisťujú riziká spojené s tretími stranami alebo kybernetickým terorizmom.

2 Cieľ práce, metodika a metódy skúmania

Záverečnú prácu sme rozdelili na jeden hlavný cieľ a niekoľko čiastkových praktických a teoretických cieľov, ktoré nám tento hlavný cieľ pomôžu naplniť. Hlavným cieľom diplomovej práce je na základe teoretických poznatkov, štruktúrovaného rozhovoru s odborníkmi na kybernetické riziká a analýzy poistného trhu, identifikovať rozdiely pri vnímaní a kategorizovaní kybernetických rizík, identifikovať problémy poistiteľnosti kybernetických rizík a navrhnúť potenciálne vylepšenia pre poisťovanie týchto rizík.

Medzi čiastkové teoretické ciele patria:

- vymedzenie definícií a základných pojmov pre lepšie vysvetlenie problematiky záverečnej práce,
- začlenenie kybernetických rizík podľa druhu a vyjadrenie ich pôvodu na základe najčastejšie vyskytujúcich sa hrozieb,

Medzi čiastkové praktické ciele patria:

- získanie informácií a poznatkov o kybernetických rizikách zo reálneho podniku,
- návrh zlepšenia pre poisťovanie kybernetických rizík,
- analýza poistení kybernetických rizík na poistnom trhu európskej únie a ich porovnanie.

Zisťovali sme ako teoretické poznatky v skutočnosti fungujú a či je možné na základe týchto poznatkov kybernetické riziká analyzovať a prakticky poistiť. Pre lepšie vnímanie chápania a určovania kybernetických rizík sme spolupracovali s poprednými manažérmi spoločnosti Tatra banka a.s..

V tejto časti záverečnej práce sa zameriavame aj na metodiku, ktorú sme pri písaní práce zvolili. Na začiatok charakterizujeme naše objekty skúmania. Potom popisujeme aké pracovné postupy sme pri písaní zvolili. V sekcii spôsob získavania údajov a ich zdroje popisujeme odkiaľ sme údaje čerpali. V časti použité metódy vyhodnotenia a interpretácie výsledkov popisujeme aký spôsobom sme získané informácie vyhodnotili.

Charakteristika objektu skúmania

Náš objekt skúmania sme rozdelili na dve časti. Ako prvý objekt pozorovania vnímame akciovú spoločnosť Tatra banka. Tatra banka a.s. vznikla v roku 1990 a stala sa prvou súkromnou bankou na Slovensku. Od tohto roku získala viac ako 130 ocenení od 30

vyhlasovateľov. Tatra banka je súčasťou najsilnejšej rakúskej bankovej skupiny Raiffeisen Bank International Group. V posledných rokoch sa na trhu prezentuje ako líder v inováciách a získala niekoľko ohodnotení ako najlepšia digitálna banka na Slovensku. Práve preto si myslíme, že kybernetické riziká a poistenie voči nim musia mať veľmi dobre pokryté.

Ako druhý objekt skúmania by vnímame trh s poisťovacími službami v Európskej únii. Zameriavame sa však len na malú časť tohto trhu, keďže nie každá poisťovňa ponúka poistenie voči kybernetickým rizikám. Snažili sme sa teda nájsť niekoľko najznámejších poisťovní v rámci Slovenskej republiky a v rámci Európskej únie a porovnať poistenia voči kybernetickým rizikám, ktoré ponúkajú.

Pracovný postup

Pri vypracovávaní záverečnej práce sme postupovali podľa nasledujúcich krokov. Tieto kroky nám slúžili na dodržiavanie postupnosti pri vypracovávaní a zároveň nám pomáhali zachovať našej práci správny tvar. Kroky ktoré sme dodržovali sú:

- definovanie primárneho cieľa,
- určenie čiastkových cieľov,
- nadobudnutie teoretických poznatkov v danej problematike,
- návrh metodiky a metód skúmania,
- vypracovanie štruktúrovaných rozhovorov,
- spracovanie získaných poznatkov zo štruktúrovaných rozhovorov,
- získavanie údajov o dostupných poisteniach voči kybernetickým rizikám,
- porovnanie kybernetických poistení ,
- vlastný návrh na spôsob poisťovania kybernetických rizík a vytvorenie vlastnej definície pre kybernetické riziká,
- vyhodnotenie získaných dát.

Spôsob získavania údajov a ich zdroje

V teoretickej časti sme využívali na získavanie údajov hlavne internetové a knižné zdroje. Pri definíciách pojmov nám slúžili hlavne direktívy, zákon o kybernetickej bezpečnosti č. 69/2018 Z.z., norma ISO/IEC 27000 s názvom Cyber security, štandardy a rôzne glosáre, či štúdie od uznávaných inštitúcií. Na popísanie pojmu poistiteľnosť sme používali informácie od popredných autorov, ktorý sa touto problematikou zaoberajú. Pre

popísanie poistiteľnosti rizík sme informácie čerpali prevažne zo štúdií a vedeckých prác zaoberajúcich sa touto problematikou.

V praktickej časti sme informácie získavali pomocou štruktúrovaných rozhovorov s poprednými manažérmi v oblasti kybernetickej bezpečnosti zo spoločnosti Tatra banka a.s. Zdrojom informácií ohľadom poistenia Tatra banky voči kybernetickým rizikám bol vedúci oddelenia bezpečnosti informačných systémov Marek Zeman. Informácie ohľadom vnímania, kategorizovania a vyhodnocovania kybernetických rizík v Tatra banke nám poskytol Jozef Uroda, ktorý v banke zastupuje pozíciu ICT and security Risk Manager. Pre porovnanie dostupných poistení kybernetických rizík nám slúžili hlavne internetové zdroje, a teda informácie o poisteniach dostupné na internetových portáloch poisťovní, ktoré tieto poistenia poskytujú.

Použité metódy vyhodnotenia a interpretácie výsledkov

V teoretickej časti diplomovej práce sme pracovali hlavne s analýzou a syntézou. Analýzu môžeme chápať ako abstraktný alebo reálny rozklad predmetov, alebo javov na základné zložky. Syntéza je zase spájanie týchto jednotlivých zložiek do celku. Pomocou analýzy sme rozdelili názov diplomovej práce (Poistiteľnosť kybernetických rizík) na základné zložky. Prvou zložkou bolo definovanie kybernetických rizík pomocou rôznych odborných zdrojov. V druhej zložke sme objasnili pojem poistiteľnosť a na základe získaných údajov sme popísali, čo je pre dosiahnutie poistiteľnosti nutné splniť. Pomocou syntézy sme tieto zložky spojili a v kapitole Poistiteľnosť kybernetických rizík sme pomocou získaných údajov túto problematiku objasnili.

V praktickej časti záverečnej práce sme používali štruktúrovaný rozhovor, komparáciu a zovšeobecnenie. Štruktúrovaný rozhovor sme viedli s dvoma manažérmi Tatra banky, pôsobiacimi v oblasti kybernetickej bezpečnosti. Pri týchto rozhovoroch sme nazbierali informácie z praxe, ktoré sme zhrnuli vo výsledkoch práce. Komparáciu sme použili pri porovnávaní poistení kybernetických rizík. Zovšeobecnenie sme použili pri objasnení problémov poistiteľnosti kybernetických rizík a pri vlastnej definícii pojmu kybernetické riziko.

3 Výsledky práce a diskusia

V tejto kapitole záverečnej práce sa zameriavame na praktickú časť. Praktickú časť sme rozdelili do troch podkapitol. V prvej podkapitole sa zaoberáme vnímaním kybernetických rizík a poistením sa voči nim v konkrétnom podniku, pôsobiacom na území Slovenskej republiky viac ako tridsať rokov. Touto spoločnosťou je Tatra banka a.s.. V druhej podkapitole predstavujeme návrhy na zlepšenia poisťovania kybernetických rizík, na základe získaných teoretických poznatkov a poznatkov získaných pri štruktúrovaných rozhovoroch. V tretej podkapitole porovnávame poistenia kybernetických rizík. Tieto poistenia nie je možné porovnať až tak dobre z kvantitatívneho hľadiska, ale skôr z kvalitatívneho hľadiska.

3.1 Kybernetické riziká a poistenie voči nim v spoločnosti Tatra banka, a.s.

V tejto kapitole praktickej časti sme sa zamerali na kybernetické riziká a na poistenie sa voči nim v konkrétnej organizácii. Vďaka štruktúrovaným rozhovorom s poprednými manažérmi spoločnosti Tatra banka a.s., sa nám podarilo zistiť ako tieto riziká spoločnosť vníma a ako sa k nim stavia. Prvý štruktúrovaný rozhovor sme viedli s Marekom Zemanom, vedúcim oddelenia bezpečnosti informačných systémov. Marek Zeman má na starosti bezpečnosť informačných systémov v celej spoločnosti a má pod sebou veľký tím ľudí, ktorý s ním na bezpečnosti informačných systémov spolupracujú. Ak sa vyskytne nejaký problém alebo čokoľvek čo je treba konzultovať s predstavenstvom, je to práve on, ktorý to má na starosti.

Naše prvé otázky na neho sa týkali poistenia voči kybernetickým rizikám. Pýtali sme sa či má banka uzavreté poistenie kybernetických rizík a či je možné ho bližšie špecifikovať. Dostali sme jasné a stručné odpovede. Marek zeman odpovedal, že banka má uzavreté poistenie kybernetických rizík, no nemôže nám povedať v akej výške ani v akej poisťovni. Odôvodnenie prečo nám to nemôže povedať bolo, že by to mohlo odhaliť ako veľmi je banka zabezpečená voči kybernetickým rizikám a teda keby bola výška sumy za poistenie nízka, poukazovalo by to na to, že má banka kvalitné zabezpečenie. Naopak ak by bola suma za poistenie vysoká, znamenalo by to, že banka v tejto oblasti moc kvalitne zabezpečená nie je. Poskytovateľa poistenia nám tiež povedať nechcel z podobných dôvodov, nakoľko aj podľa toho by sa dalo nejakým spôsobom vydedukovať do akej výšky toto poistenie siaha. Na záver dodal, že sa poznáme len päť minút a tieto údaje sú tak dôverné, že ich poznajú iba traja členovia predstavenstva. Spomínal však, že poistenia na trhu v súčasnosti z veľkej časti

pokrývajú len riziká, ktoré sa týkajú kriminálnej činnosti a teda kybernetických útokov. Na štatistické otázky ako často banka čelí rizikám a kedy najviac narástli tiež odpovedať nemohol, kvôli dôvernosti údajom.

Na otázku či má banka nejaké povinné nariadenia ohľadom kybernetickej bezpečnosti odpovedal, že na Slovensku sú tri direktívy, ktoré tieto nariadenia stanovujú:

- sektorové direktívy (pre banky konkrétne direktíva od Európskeho orgánu pre bankovníctvo (EBA- European Banking Authority)),
- zákon o kybernetickej bezpečnosti č. 69/2018 Z.z.,
- zákon o ochrane osobných údajov č. 18/2018 Z.z. (GDPR).

Banka sa musí ďalej riadiť normami ISO, konkrétne v tomto prípade ide o normu ISO 27000 zaoberajúcu sa kybernetickou bezpečnosťou. Táto norma obsahuje štandardy bezpečnosti informácií publikované Medzinárodnou organizáciou pre normalizáciu spoločne s Medzinárodnou elektrotechnickou komisiou. Aj napriek tomu že banka má uzavreté poistenie kybernetických rizík, musí si vytvárať aj vlastný vnútorný fond, ktorý na pokrytie týchto rizík slúži. Tento fond sa vytvára každý rok a musí sa odhadnúť čo najpresnejšie jeho výška, aby počas obdobia na ktoré je určený, bol schopný pokryť plnú výšku hrozieb a prípadných zabezpečení, aby sa hrozby nediali.

Po tomto úvodnom stretnutí nám Marek Zeman dohodol stretnutie s členom jeho tímu. Toto ďalšie stretnutie bolo s Jozefom Urodom, ktorý zastupuje pozíciu ICT and security Risk Manager. Po slovensky by sa táto pozícia dala nazvať manažér rizík informačno-komunikačných technológií a bezpečnosti. Jozef Uroda nám vysvetlil ako Tatra banka vníma kybernetické riziká a ako v nej funguje ICT risk management. V prvom rade spomenul, že na to aby kybernetické riziko existovalo, musí spĺňať tri elementy:

1. Musí existovať nejaké aktívum. Tatra banka vníma ako aktívum prevažne aplikácie, ktoré používajú zamestnanci alebo klienti.
2. Toto aktívum musí byť zraniteľné. Aplikácia musí mať slabé miesto, cez ktoré sa dá preniknúť a ohroziť jej funkčnosť alebo údaje, čo sa v nej nachádzajú.
3. Na základe zraniteľnosti môže vzniknúť hrozba. Hrozba pre aplikáciu môže byť napríklad nejaký druh kybernetického útoku.

V Tatra banke rozdeľujú kybernetické riziká na týchto päť druhov:

- IT availability risk (riziko dostupnosti informačnej techniky),
- IT security risk (riziko bezpečnosti informačnej techniky),

- Outsorcing risk (riziko podnikových procesov, ktoré vykonáva externý poskytovateľ služieb),
- Data integrity risk (riziko integrity dát),
- Change risk (riziko zmeny).

Pre každý druh rizika merajú Total impact, čiže úplný dopad. Tento dopad sa určuje na stupnici od jedna po štyri. Pričom jednotka sa berie ako Low (nízky), dvojka ako Medium (stredný), trojka ako High (vysoký) a štvorka ako Critical (kritický). Pre každý druh taktiež vyhodnocujú takzvaný Likelyhood, čiže pravdepodobnosť výskytu rizika. Túto pravdepodobnosť určujú na stupnici od jedna po päť, a riadia sa na základe výskytu incidentov v minulosti, bezpečnostnej politiky a nálezov pri penetračných testoch. Pre lepšie pochopenie celkového dopadu nakreslil tabuľku 3 ako príklad. V tejto tabuľke dal výpadok aplikácie Gate ako príklad pre konkrétne riziko. Gate je aplikácia, ktorá sa v Tatra banke používa na dennej báze.

Tabuľka 3 Prikladné znázornenie dopadu pre riziko výpadku aplikácie Gate

	Výška dopadu			
Druh dopadu	1	2	3	4
Financial		•		
Reputation		•		
Strategic	•			
Bussines production			•	
Privacy	•			

Zdroj: Vlastné spracovanie podľa Urodu

V tejto tabuľke sa nachádza päť druhov dopadu: finančný, reputačný, strategický, produkčný a dopad na súkromie. Finančný dopad je ako jediný z týchto piatich kvantitatívny a teda dá sa zmerať jeho výška a uviesť v eurách. Výška finančného dopadu sa ako jediná odosiela na ďalšie spracovanie oddeleniu pre operačné riziko. Finančný dopad je vlastne suma o koľko môže prísť spoločnosť v prípade incidentu. Banka má pod jednotlivými číslami konkrétnu hodnotu v eurách, no tá nám nemohla byť zverejnená. Ostatné dopady sú kvalitatívne a teda nedajú sa zmerať konkrétnou veličinou a sú vyhodnocované len číslom na stupnici. Reputačný dopad je vlastne to ako môže dané riziko ohroziť reputáciu spoločnosti. Kde jednotka môže byť napríklad ohrozenie reputácie v meste kde sa spoločnosť nachádza a štvorka môže byť ohrozenie reputácie po celom svete. Strategický

dopad je vlastne dopad na strategické ciele, ktoré chce spoločnosť dosiahnuť. Produkčný dopad znamená ako moc môže byť daným rizikom ovplyvnená výroba , respektíve v našom prípade poskytovanie služieb. Dopadom na súkromie môžeme chápať napríklad možné zverejnenie osobných údajov klientov.

Hodnoty všetkých dopadov sa sčítajú a podľa súčtu hodnôt kategorizujú, a prevedú na celkový dopad. Súčet hodnôt môže dosiahnuť minimum päť a maximum dvadsať. V prípade príkladu výpadku aplikácie Gate to môže byť deväť a teda Total Impact je na úrovni Medium. Ďalej sa uvádza namiesto hodnoty deväť už len prevedená hodnota dva, keďže to je na rovnakej úrovni.

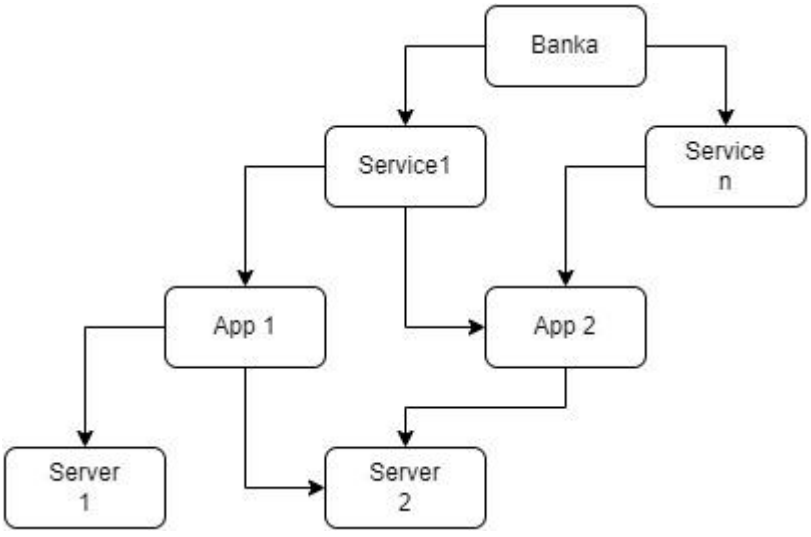
Tabuľka 4 Prepočet dopadu

Low	Medium	High	Critical
5-8	9-12	13-16	17-20

Zdroj: Vlastné spracovanie podľa Urodu

Podľa European Banking Authority direktív musí každá banka v Európskej únii robiť súbor listín, podľa ktorých sa by sa malo vymedziť, ako finančné inštitúcie prevádzkujú, monitorujú a kontrolujú svoje IKT systémy a služby vrátane zaznamenávania kritických prevádzok IKT, a mali by finančným inštitúciám umožniť udržiavať aktuálny súpis IKT aktív. Pomocou tohto súpisu aktív má banka vytvorený model aktív. Jozef Uroda nám nakreslil zjednodušený model aktív, podľa ktorého nám ďalej vysvetľoval ako riziká fungujú.

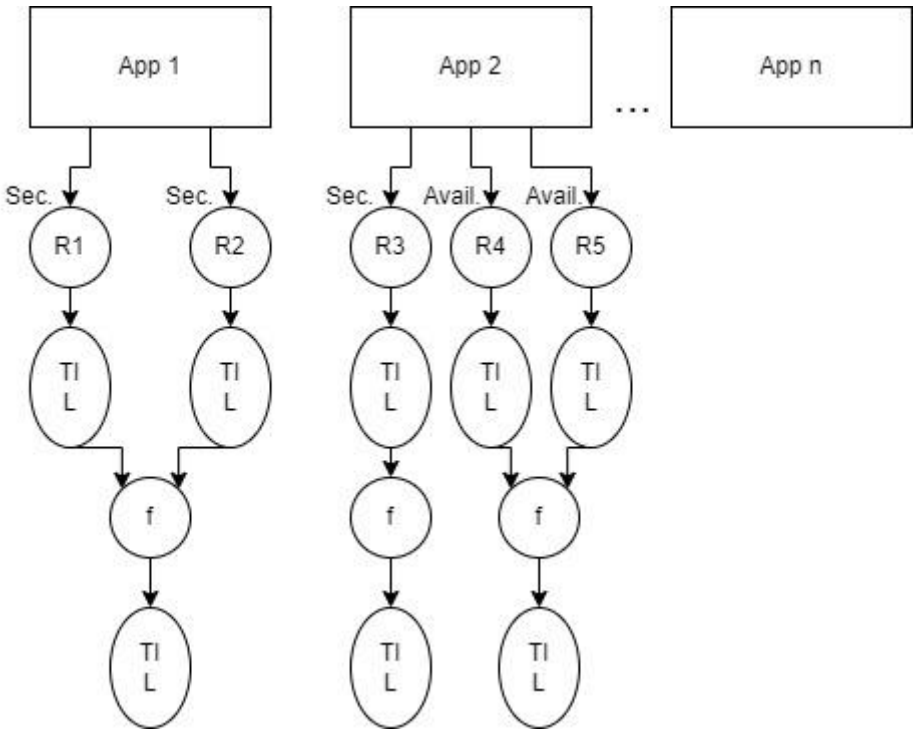
Obrázok 1 Model IKT aktív



Zdroj: Vlastné spracovanie podľa Urodu

Na začiatku celého modelu sa nachádza inštitúcia. V našom prípade je to Banka. Služby poskytované bankou sa nachádzajú hneď pod ňou. V tomto modeli máme znázornenú službu jedna a služieb môže byť až n. Služba jedna potrebuje pre svoj chod Aplikáciu 1 a Aplikáciu 2 a tieto aplikácie bežia na Serveri 1 a Serveri 2. Tento model nám bol znázornený čisto len ako príklad a v skutočnosti je oveľa zložitejší a obsahuje úplne všetky IKT aktíva spoločnosti. Pri tomto modeli nám Jozef Uroda spomenul, že banka sleduje z pohľadu bezpečnosti všetky aplikácie, ktoré používa a pre každú aplikáciu vyhodnocuje riziká. Napríklad pre Aplikáciu 1 sú na analýzu použité SDLC (Software Development Life Cycle) a Risk Assesment (čo je vlastne identifikácia rizík na základe Bezpečnostnej Politiky). Software Development Life Cycle alebo po slovensky životný cyklus vývoja systému sa skladá z plánovania, analýzy, dizajnu, implementácie, testovania a integrácie, údržby. Risk Assesment môže mať druhy ako sú kvalitatívne hodnotenie rizika, kvantitatívne hodnotenie rizika, všeobecné hodnotenie rizika, hodnotenie rizika špecifického pre lokalitu a dynamické hodnotenie rizika. Uroda nám ďalej nakreslil príklad ako aplikáciám priraďujú konkrétne riziká a ako hodnotia ich úplný dopad a pravdepodobnosť výskytu.

Obrázok 2 Príklad priraďovania rizík



Zdroj: Vlastné spracovanie podľa Urodu

V tomto príklade máme znázornené aplikácie. Ku každej aplikácii je potom priradené riziko, ktoré jej hrozí a je rozdelené podľa druhu kam ho v banke zaraďujú. Tieto druhy sme si rozdelili hneď na začiatku. Konkrétne v tomto príklade má aplikácia 1 priradené dve riziká. Obe tieto riziká patria do IT security risk kategórie. Pre každé jedno zvlášť sa vyhodnotí Total Impact a Likelyhood. Ak sú tieto riziká rovnakého druhu vkladajú sa do agregačnej funkcie, ktorá nám nemohla byť zverejnená. Výsledok vyzerá nasledujúco: R1: TI=3, L=2, toto riziko patrí do kategórie IT Sec. Risk a keďže má celkový dopad 3, finančný dopad tohto rizika je napríklad do 250 000€. Výsledok tejto funkcie sa vkladá do tabuľky 5, ktorú uvádzame ako nasledujúcu. V prípade aplikácie 2 sú k nej priradené tri riziká, jedno označené ako R3 patrí do druhu IT security risk a zvyšné dve patria do IT availability risk. Následne sa pokračuje rovnakým spôsobom ako pri aplikácii 1, len s tým rozdielom že pre každý druh rizika sa vyhodnotí Total Impact a Likelyhood samostatne. Tie sa nakoniec tak isto vložia do tabuľky.

Tabuľka 5 Finálna tabuľka s aplikáciami a druhmi rizík

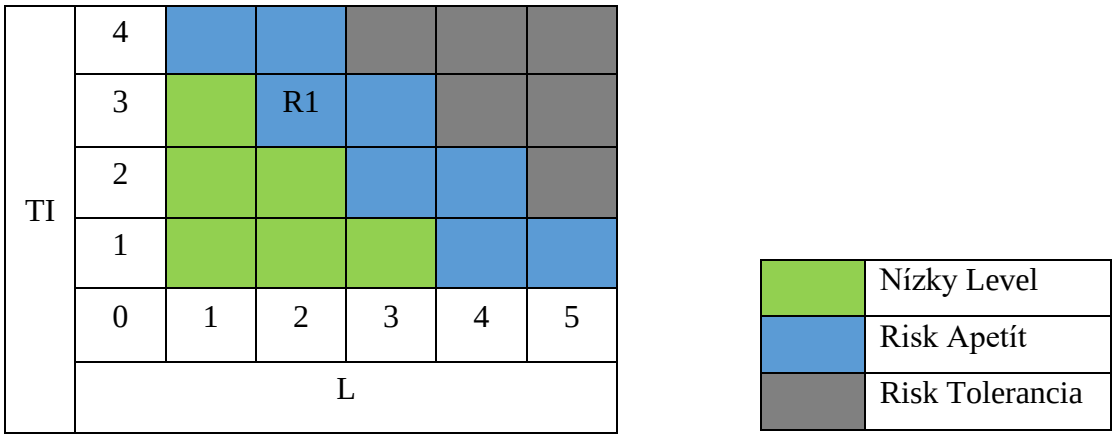
	Druhy Rizík									
	IT Avail. R.		IT Sec. R.		Outsourcing		Data Integrity		Change	
App	TI	L	TI	L	TI	L	TI	L	TI	L
App1	-	-	2	3	-	-	-	-	-	-
App2	3	2	1	2	-	-	-	-	-	-

Zdroj: Vlastné spracovanie podľa Urodu

V tejto tabuľke sa už priraďujú ku konkrétnym aplikáciám všetky riziká, ktoré im hrozia. Ku každému druhu sa priraďuje celkový dopad a pravdepodobnosť výskytu, na základe predošlého príkladu a teda Obrázku 2. Môžeme vidieť, že aplikácia 1 má len IT Security riziká a aplikácia dva má IT Availability a IT Security riziká, práve pre to sme v našom prípade do tabuľky vyplnili len tieto polia a ostatné ostali prázdne. V tejto tabuľke sú polia vyplnené náhodne čisto len ako príklad. Celkový dopad ostáva na stupnici od 1 po 4 a pravdepodobnosť výskytu na stupnici od 1 po 5.

Po tomto všetkom nám Jozef Uroda ešte vysvetlil čo znamená Risk Apetít a Risk Tolerancia. Najjednoduchšie vysvetlenie bude pomocou tabuľky 6, ktorú nám nakreslil.

Tabuľka 6 Risk Tolerancia a Risk Apetít



Zdroj: Vlastné spracovanie podľa Urodu

V tabuľke 6 nám Jozef Uroda názorne popísal ako banka rozdeľuje úroveň rizík podľa Total Ipact a Likelyhood. Povedzme, že riziko 1 má Total Impact na úrovni 3 a Likelyhood na úrovni 2. Potom podľa tejto tabuľky môžeme povedať, že sa nachádza v úrovni Risk Apetítu. Nízky level rizika znamená, že je banka spokojná s touto úrovňou a je to veľmi dobrá pozícia, ak sa v nej riziko nachádza. Risk Apetít je úroveň rizika, ktorú je organizácia bez potrebných opatrení na zníženie rizika, pri dosahovaní svojich cieľov pripravená prijať. Ak sa riziko dostane na úroveň Risk Tolerancie, organizácia prestáva toto riziko tolerovať a začína vykonávať opatrenia na zníženie tohto rizika.

3.2 Porovnanie poistení kybernetických rizík

V tejto časti diplomovej práce uvádzame a porovnávame niekoľko dostupných poistení kybernetických rizík. Zamerali sme sa na vybrané produkty dostupné na území Slovenskej republiky a vybrané produkty poisťovní v Európskej únii. Uvádzame a porovnávame produkty dostupné a označované ako poistenia kybernetických rizík, kybernetické riziká pokryté v inom druhu poistení napr. poistenie majetku alebo zodpovednosti zamestnanca sme nebrali do úvahy.

UNIQA - KYBER BALÍK

Ide o jedno z mála kybernetických poistení poskytovaných na Slovensku. Poisťovňa UNIQA ho začala poskytovať v roku 2016 no až v poslednom roku je viac propagované a viditeľné. Okrem spoločnosti UNIQA sa dá toto poistenie zakúpiť aj online prostredníctvom Tatra banky. Tatra banka a.s. vykonáva finančné sprostredkovanie ako

viazaný finančný agent zapísaný v registri NBS. UNIQA v rámci tohto produktu poskytuje pomoc nepodnikateľom pri škode zapríčinenej kybernetickým útokom. Zároveň hradí aj škody na zdraví a majetku, ktoré neúmyselne spôsobí poistený alebo členovia jeho domácnosti iným osobám. Poistné pre toto poistenie je 34,89 EUR ročne. Poistenie automaticky kryje aj rodinných príslušníkov poisteného. Toto „kyber“ poistenie poskytuje:

- nonstop asistenčnú službu a právne poradenstvo špecialistov ako aktívnu pomoc pri riešení konkrétnych prípadov zneužitia,
- náhradu za nedoručený, poškodený alebo nekompletný tovar, vzniknutú škodu alebo právne zastupovanie v prípade sporu s e-shopom,
- kompletnú asistenciu v súvislosti s podvodnou online transakciou, uhradí náklady na súdne konanie a zabezpečí právne zastúpenie,
- odstránenie alebo vytesnenie nepravdivých informácií o poistenom či o blízkych poisteného v prípade, ak sa stane obetou šikany na internete,
- uhradenie škody alebo nákladov na právne zastupovanie, právnu pomoc v prípade, ak poistenému niekto odcudzí virtuálnu identitu,
- uhradenie škody na zdraví a majetku, ktoré neúmyselne spôsobí poistený alebo členovia jeho domácnosti iným osobám.

Členovia domácnosti alebo blízki poisteného sú pri tomto poistení manžel/manželka, druh/družka a deti.

Poistné krytie je nasledujúce: Ak sa poistený stane obeťou útoku – má nárok na kompletnú asistenciu pre nápravu, právne služby alebo uhradenie vzniknutých škôd. Poistenie sa týka aj zahraničných e-shopov, ak bol tovar zaslaný z územia členských štátov EÚ, Švajčiarska a Nórska. V prípade, ak sa asistenčnej službe nepodarí obhájiť záujem klienta, má klient nárok na poistné plnenie pri priamo vzniknutých škodách do výšky 2 000 EUR a právne zastupovanie do výšky 12 000 EUR. Bližšie krytie rizík je uvedené v tabuľke 7.

Tabuľka 7 Riziká pokryté produktom UNIQA - KYBER BALÍK

	Poistený má nárok na
Riziko pri online nákupoch	• Výplatu náhrady za nedoručený, poškodený alebo nekompletný tovar, • Úhradu priamo vzniknutých škôd.
Útoky v rámci online platieb	• Úhradu škody v súvislosti s podvodnou transakciou, • Úhradu nákladov na súdne konanie.
Poškodzovanie online povesti	• Odstránenie nepravdivých a poškodzujúcich informácií na internete, • Vytlačenie nepravdivých informácií z popredných miest vyhľadávačov.
Odcudzenie identity	• Úhradu vzniknutých škôd, • Úhradu nákladov na vydanie nových dokladov.
Zodpovednosť za škodu spôsobenú poisteným	• Náhradu škôd na živote, zdraví alebo majetku.

Zdroj: Vlastné spracovanie podľa Tatra Banka a.s.

Všetky uvedené informácie sú dostupné na internetových stránkach Tatra Banky a poisťovne UNIQA.

ČSOB - Poistenie kybernetických rizík

Tento produkt poskytuje ČSOB poisťovňa na území Českej a Slovenskej republiky. Poistenie sa dá uzatvoriť na ktorejkoľvek pobočke poisťovne alebo banky. Produkt poskytujú od roku 2018. Ako sami na svojich weboch uvádzajú, je to podľa nich ideálne poistenie pre ochranu podnikateľov a organizácií. Cenu poistenia a maximálne poistné plnenie neuvádzajú. Sumy neuvádzajú pravdepodobne z dôvodu, že sa môžu pre jednotlivých poistníkov líšiť podľa veľkosti ich spoločnosti alebo jej zabezpečenia voči kybernetickým rizikám. Poisťovňa uvádza na svojej web stránke, že toto poistenie kryje:

- **Narušenie ochrany dát**
    - Náklady a finančné straty, ktoré vzniknú v súvislosti s kybernetickým incidentom.
    - Náklady na odborníkov:
        - IT špecialisti na prešetrenie kybernetického incidentu
        - právny zástupca pre právnu obhajobu a zastupovanie s úradmi
        - PR agentúry zamerané na krízovú komunikáciu
    - Finančnú stratu spôsobenú prerušením alebo obmedzením prevádzky.

- Náklady, ktoré vzniknú v súvislosti s odstraňovaním následkov kybernetického incidentu, vrátane práce zamestnancov nadčas alebo monitorovania situácie.

- **Obnova dát**
  - Náklady na obnovu dát a softvér po kybernetickom incidente (napríklad hacking alebo omylom vymazané dáta) za podmienky, že existujú použiteľné zálohy.
- **Zodpovednosť za ujmu vyplývajúcu z porušenia ochrany údajov**
  - Zodpovednosť poisteného za ujmu/škodu spôsobenú tretej strane porušením ochrany dát, spôsobeným kybernetickým incidentom.
  - Náhodné alebo nezákonné zničenie, strata, zmena, neoprávnené zverejnenie alebo prístup k dôverným informáciám alebo osobným údajom prenášaným, uloženým alebo spracovávaným na počítačových systémoch poisteného.
- **Zodpovednosť za bezpečnosť sietí**
  - Poistenie sa vzťahuje aj na zodpovednosť poisteného za ujmu/škodu spôsobenú tretej strane kybernetickým incidentom v počítačovom systéme poisteného, ktorému poistený nedokázal zabrániť a spôsobil poškodenie, zmenu, zničenie alebo krádež dát alebo útok Denial of Service (DoS) na počítačovom systéme tretej strany.
- **Prerušenie prevádzky**
  - Finančnú stratu poisteného vzniknutú prerušením alebo obmedzením prevádzky po kybernetickom incidente na počítačových systémoch poisteného.
- **Kybernetické vydieranie**
  - V prípade, že odstránenie následkov kybernetického incidentu nebude úspešné z krytia rizika narušenia ochrany dát, poisťovňa nahradí výkupné zaplatené po súhlase poisťovateľa a primerané a nevyhnutné náklady na vyriešenie kybernetického vydierania.
- **Kybernetický zločin**
  - Akékoľvek peňažné prostriedky, o ktoré príde poistený priamo v dôsledku neoprávneného elektronického prevodu z bankového účtu poisteného, pokiaľ poistený nie je schopný tieto prostriedky získať späť.

- **Porušenie štandardov PCI-DSS**
    - Porušenie štandardov PCI-DSS spôsobené nedbalosťou, neoprávneným zásahom zamestnanca, odcudzeným vybavením alebo zlyhaním zabezpečenia siete.
- **Zodpovednosť za ujmu spôsobenú aktivitami v on-line médiách**
    - Poistenie sa vzťahuje na zodpovednosť poisteného za ujmu/škodu spôsobenú tretej strane vzniknutej ohováraním, poškodením dobrého mena, porušením autorského práva či obchodnej značky alebo porušením práv na ochranu súkromia.
- **IT Asistencia aj pre prípady bežnej nefunkčnosti IT techniky mimo kybernetický incident**
    - Riešenie úplnej alebo čiastočnej nefunkčnosti hardvéru alebo softvéru stolného počítača, notebooku, tabletu alebo routera vzniknutej na území SR. Poistenie kryje náklady na telefonickú konzultáciu s IT technikom alebo na zásahy IT technika zo vzdialeného pripojenia.

Colonnade Insurance S.A. - Poistenie Cyber

Poisťovňa Colonnade Insurance S.A. vstúpila v roku 2016 na stredoeurópsky a východoeurópsky poistný trh v prvom kole prevzatím poistných aktivít austrálskej poisťovne QBE a v roku 2017 následne pokračovala v expanzii akvizíciou lokálnych pobočiek americkej AIG.

V roku 2018 poisťovňa reagovala na sprísnenie legislatívy v oblasti ochrany osobných údajov produktom „Poistenie zodpovednosti za škodu v súvislosti so spracovaním osobných údajov a nariadením GDPR“. Je to poistenie zodpovednosti za škodu spôsobenú tretej osobe v súvislosti so spracúvaním osobných údajov. Ako rozšírenie tohto poistenia taktiež v roku 2018 uviedli na trh poistenie „Poistenie Cyber“. Tak ako pri predošlom poistení od ČSOB poisťovne ani Colonnade Insurance neudáva presné ceny tohto produktu, a záleží teda asi na veľkosti spoločnosti, sile zabezpečenia spoločnosti a na voliteľných doplnkoch poistenia, ktoré si spoločnosť vyberie. Rozsah poistného krytia tohto poistenia je uvedený na stránkach poisťovne a pokrýva:

- **Pomoc pri riešení dopadov na spracované údaje alebo bezpečnosť siete**
    - Náklady na špecialistov na kybernetické riziká,

- Náklady na odborné služby za účelom zaistenia možnosti obnovy, znovu zhromaždenia alebo znovu vytvorenia elektronických dát.

- **Pomoc pri poškodení dobrého mena**
  - Náklady na odborné služby za účelom zabránenia či zmiernenia nepriaznivého vplyvu na dobré meno spoločnosti,
  - Náklady na odborné služby za účelom zabránenia či zmiernenia nepriaznivého vplyvu na dobré meno konkrétnej osoby pracujúcej pre spoločnosť,
  - Náklady na oznámenie straty či úniku dát poškodeným osobám alebo príslušnému dozornému orgánu.
- **Zmierňovanie finančných následkov**
  - Škody a náklady na právne zastúpenie súvisiace s porušením ochrany osobných údajov alebo dôverných informácii spoločnosti,
  - Škody a náklady na právne zastúpenie, pokiaľ dôjde k narušeniu bezpečnosti siete,
  - Pri porušení povinností i voči dozorným orgánom,
  - Škody a náklady na právne zastúpenie v prípade porušenia práv duševného vlastníctva tretej osoby alebo nedbalosti pri správe elektronického obsahu médií (voliteľné),
  - Škody spôsobené vydieraním (voliteľné),
  - Stratu zisku spoločnosti z dôvodu prerušenia funkcie systému či siete, ktoré je spôsobené neoprávneným vniknutím do počítačového systému (voliteľné).

Kooperativa - Poistenie kybernetických rizík

Kooperativa pojišťovna, a.s. toto poistenie priniesla na Český trh v roku 2018. Na Slovenskej internetovej stránke toto poistenie ako produkt neponúkajú. Toto poistenie je určené pre podnikateľov, firmy aj neziskové organizácie. Uvádzajú, že poistenie kybernetických rizík je možné dojednať v prípade, že spoločnosť dbá na určité bezpečnostné opatrenia, ako je napríklad používanie silných hesiel a antivírusov, práca v oficiálnych a aktuálnych verziách programov alebo pravidelné zálohovanie dát. Taktiež neudávajú sumu poistného ani maximálnu výšku krytia. Toto poistenie kryje:

- škody na dátach v elektronickej podobe,
- nefunkčnosť počítačového systému,

- náklady regulačného riadenia,
- náklady public relations – obnovu dobrého mena zodpovednosť za ujmu spôsobenú únikom dát v elektronickej podobe ,
- prerušenie prevádzky (voliteľné pripoistenie),
- DDoS útok – úmyselné preťaženie alebo zahltenie počítačového systému, ktoré spôsobí odopretie služby (nefunkčnosť, zablokovanie systému).

Tieto krytia mala Kooperativa uvedené na svojej web stránke, bližší popis krytí uvádzajú až v poistnej zmluve.

AXA - FirmenFlex, ByteProtect Compact, ByteProtect

AXA Versicherung AG ponúka na nemeckom trhu až tri typy poistení kybernetických rizík. Bližší popis týchto produktov je uvedený v tabuľke 8.

Tabuľka 8 Kybernetické poistenia AXA

	FirmenFlex	**ByteeProtect Compact**	**ByteProtect**
	Pre menšie firmy a živnostníkov	Pre malé a stredné firmy	Pre stredne veľké a väčšie firmy
Obrat spoločnosti	Do 5 miliónov eur	Od 5 do 10 miliónov eur	Tržby cez 10 miliónov eur
Druh zabezpečenia	Flexibilná ponuka s výberom alebo zrušením modulov (prerušenie prevádzky, strata zárobku alebo internetový podvod)	Flexibilná ponuka s výberom alebo zrušením modulov (zmluvné sankcie PCI-DSS, technické poruchy a e-discovery)	Úplne individuálna ponuka
Zmluvná doba	1 rok	1 alebo 3 roky	1 rok

Zdroj: Vlastné spracovanie podľa AXA Versicherung AG (2022)

Tieto poistenia kryjú:

- Hackerský útok, manipuláciu zo strany zamestnancov alebo napríklad zlyhanie poskytovateľa IT služieb: dodatočné náklady alebo ušlý zisk a priebežné náklady vyplývajúce z prerušenia podnikania.
- Náklady na expertízu a poradenstvo, ktoré vyplývajú napríklad z priemyselnej špionáže alebo z porušenia zákonov o ochrane údajov.
- Náklady na obnovenie dát a programov do predchádzajúceho prevádzkového stavu. Podobne pri odstraňovaní malvéru alebo pri výmene/obnovení kmeňových a transakčných údajov. Náklady na výmenu hardvéru, keď obnova nie je možná.
- V reputácii a krízovom manažmente, napr. v prípade hackerského útoku alebo distribuovaného odmietnutia služby, sa poisťovňa preberá náklady na odvrátenie alebo zníženie poškodenia dobrého mena vrátane externého krízového alebo komunikačného poradenstva.
- Škody z kybernetickej zodpovednosti, ktoré vzniknú napríklad zmazaním, stratou, úpravou alebo nedostupnosťou údajov alebo programov od tretej strany alebo porušením zákonov o ochrane údajov.
- Náklady na vymáhanie, ktoré vzniknú napríklad zablokovaním prístupu k údajom a programom alebo narušením IT systému, alebo internetových služieb, alebo webovej stránky.
- Porušenie ochrany údajov, bez ohľadu na druh, je pokryté prevzatím nákladov, napríklad zákonom požadované informácie od úradov, verejnosti a potenciálne dotknutých osôb.
- V prípade internetových podvodov spôsobených napríklad manipuláciou s webovou stránkou alebo databázami a programami, ktoré sú k nej pripojené, sú poistené aj priame finančné straty (napr. podvody) spôsobené úmyselným a nelegálnym útokom hackerov.

Všetky dostupné informácie udáva AXA Versicherung AG na svojom webe.

Porovnanie kybernetických poistení

Ak by sme tieto vyššie uvedené poistenia chceli porovnať z kvantitatívneho hľadiska, bolo by to veľmi komplikované, pretože väčšina produktov je poskytovaná na mieru pre konkrétnu spoločnosť a výška poistného, výška krytia a výška spoluúčasti sú teda veľmi individuálne. Vo väčšine prípadov záleží na veľkosti alebo zabezpečení spoločnosti, ktorá má o poistenie kybernetických rizík záujem. Tieto poistenia sa však dajú porovnať z kvalitatívneho hľadiska a to podľa uvedených krytí. Z tohto porovnania však vynechávame poistenie od spoločnosti UNIQA, keďže ide o poistenie pre bežných občanov a ich domácnosti. Ostatné poistenia sú určené pre spoločnosti a ich porovnanie sa nachádza v tabuľke 9.

Tabuľka 9 Kvalitatívne porovnanie kybernetických poistení

	Poistenia			
Krytie	ČSOB	Colonnade	Kooperativa	AXA AG
Poškodenie dobrého mena	✓	✓	✓	✓
Narušenie ochrany dát	✓	✓	✓	✓
Obnova dát	✓	✓	✗	✓
Ujma tretej strane	✓	✓	✓	✓
Prerušenie prevádzky	✓	✓	✓	✓
Vydieranie	✓	✓	✗	✓
PCI-DSS	✓	✗	✗	✓
Pokuty, sankcie	✗	✓	✗	✗
Právne zastupovanie	✓	✓	✓	✓
DDoS útok	✓	✓	✓	✓

Zdroj: Vlastné spracovanie

V tabuľke 9 môžeme vidieť, že väčšina poisťovní poskytuje veľmi podobné krytie. Najhoršie zo všetkých porovnávaných poisťovní dopadla česká Kooperativa pojišťovna, a.s., ktorá neposkytuje až 4 z 10 druhov krytí. Na Slovenskom trhu by sme odporúčali ČSOB poisťovňu alebo Colonnade Insurance S.A.. Obe tieto poisťovne pokrývajú širokú škálu kybernetických rizík a poskytujú dobré služby. Nezaostávajú dokonca ani za poprednou nemeckou poisťovňou AXA Versicherung AG.

3.3 Návrhy na zlepšenie poisťovania kybernetických rizík

V tejto časti záverečnej práce navrhujeme zlepšenia pre poisťovanie kybernetických rizík. Na základe štruktúrovaného rozhovoru s Jozefom Urodom, ktorý zastupuje v Tatra banke pozíciu ICT and security Risk Manager, navrhujeme, aby poisťovne realizovali poistenia podobným spôsobom ako v banke kybernetické riziká vnímajú. V štruktúrovanom rozhovore sme sa dozvedeli, že na základe direktív a nariadení od národných či nadnárodných inštitúcií, finančné inštitúcie kategorizujú kybernetické riziká veľmi podobným spôsobom. Iné sektory však môžu kategorizovať kybernetické riziká odlišným spôsobom. Preto navrhujeme, aby poisťovne vytvorili kategorizáciu kybernetických rizík pre každý sektor samostatne, na základe takých druhov kybernetických rizík, ktoré daný sektor najviac ohrozujú. Napríklad pre bankový sektor by mohli byť kybernetické riziká rozdelené rovnako ako v Tatra banke:

- IT availability risk (riziko dostupnosti informačnej techniky),
- IT security risk (riziko bezpečnosti informačnej techniky),
- Outsorcing risk (riziko podnikových procesov, ktoré vykonáva externý poskytovateľ služieb),
- Data integrity risk (riziko integrity dát),
- Change risk (riziko zmeny).

Ak by mala inštitúcia, ktorá má záujem o toto poistenie trochu inú kategorizáciu rizík, poisťovňa by vytvorila takzvané prevodné tabuľky pomocou ktorých, by sa prevádzali kybernetické riziká inštitúcie na rovnaký druh rizík ako by boli kategorizované v poisťovni. Na základe týchto druhov rizík by sa dal vypočítať aj dopad rizika a pravdepodobnosť, že toto riziko nastane. Z úrovne úplného dopadu rizika by bolo možné vyčísliť finančné škody, ktoré toto riziko môže spôsobiť. Poisťovňa by si však musela spraviť posudok ku každému záujemcovi o poistenie samostatne, nakoľko každá spoločnosť má inú veľkosť a iné množstvo aktív s rôznou hodnotou. Týmto spôsobom by sa dalo aspoň zabezpečiť to, že by poskytovateľ poistenia a poistník mali rovnaký spôsob vyhodnocovania rizík.

Veľkým prínosom pre poistenie kybernetických rizík by bolo zapojenie štátnych orgánov do tejto problematiky. Keďže spoločnosti musia reportovať údaje o prienikoch a všetkých na nich smerujúcich kybernetických útokoch štátnym inštitúciám, tieto inštitúcie majú v tejto oblasti prístup k obrovskému množstvu dát. Nezávislí poisťovatelia však prístup k týmto dátam nemajú a nevedia si na základe nich vypracovať vlastné štatistické databázy, ktoré by im pri krytí kybernetických rizík veľmi pomohli.

Priestor na zlepšenie vidíme aj v systematickom zbere dát. Napríklad poisťovatelia by mohli buď kombinovať zdroje a vymieňať si údaje na multilaterálnom základe, ako sa to robí napríklad v prípade operačných rizík v bankovníctve aj poisťovníctve, alebo ako alternatívu by mohli regulačné orgány poskytnúť spoločnú anonymizovanú platformu na zdieľanie tohto typu údajov.

Pre mnoho spoločností sú reputácia alebo dobré meno spoločnosti veľmi významná veličina. Pri poškodení mena spoločnosti napríklad v dôsledku úniku citlivých údajov o zákazníkoch, dezinformačnej kampani alebo iného kybernetického incidentu, by mohla spoločnosť prísť o veľa svojich zákazníkov a zároveň by ku nej neprichádzali noví. S tým by bola spojená aj strata výnosov respektíve zisku spoločnosti. Nakoľko však poisťovne túto časť kybernetických rizík nepoisťujú, navrhujeme, aby si vypracovali plán na to, ako poistiť časť kybernetických rizík spojených s poškodením dobrého mena spoločnosti. Niektoré poistenia pokrývajú náklady spojené s odstránením poškodzujúcich informácií na internete, s obnovením dobrého mena spoločnosti, alebo aspoň s vytlačením takýchto informácií z predných miest vyhľadávačov. Poisťovne by však mohli pokrývať v rámci poistení aj škody, spôsobené stratou zákazníkov. Výška škody by sa dala vypočítať na základe porovnania ziskov spoločnosti pred incidentom a napríklad mesiac po incidente. Rozdiel v týchto ziskoch by sa potom zohľadnil v poistnom krytí vyplácanom poistenému.

Záver

Každoročne spoločnosti zaznamenávajú vyššiu frekvenciu kybernetických útokov. S týmito útokmi na spoločnosti pôsobia aj iné kybernetické hrozby. Aj keď spoločnosti vynakladajú nemalé náklady na zabránenie uskutočnenia týchto hrozieb, nie je úplne možné, aby sa im vyhli. Z tohto dôvodu by sa voči kybernetickým rizikám mali poistiť.

Hlavným cieľom diplomovej práce bolo na základe teoretických poznatkov, štruktúrovaného rozhovoru s odborníkmi na kybernetické riziká a analýzy poistného trhu, identifikovať rozdiely pri vnímaní a kategorizovaní kybernetických rizík, identifikovať problémy poistiteľnosti kybernetických rizík a navrhnúť potenciálne vylepšenia pre poisťovanie týchto rizík. Tento cieľ považujeme za splnený, keďže sa nám podarilo nazbierať dostatok teoretických informácií, ktoré sme potom porovnali s informáciami získanými pri štruktúrovaných rozhovoroch a pri vybraných poistných produktoch.

Štruktúrované rozhovory považujeme za najväčší prínos našej diplomovej práce. Dozvedeli sme sa v nich, že Tatra banka rozdeľuje kybernetické riziká do piatich kategórií. Každému riziku vypočítava, aký bude mať úplný dopad na spoločnosť a aká je pravdepodobnosť, že sa riziko uskutoční. Na základe úplného dopadu je Tatra banka schopná približne vyhodnotiť, akú finančnú škodu toto riziko spoločnosti prinesie.

Splnenie hlavného cieľa bolo podmienené splnením niekoľkých čiastkových cieľov. Podarilo sa nám získať dostatok teoretických informácií, aby sme mohli vymedziť všetky potrebné definície, predovšetkým kybernetické riziko, kybernetická hrozba a poistiteľnosť.

Kybernetické riziká sa nám podarilo kategorizovať na základe viacerých teoretických zdrojov a tiež na základe risk manažmentu v Tatra banke.

Podarilo sa nám navrhnúť aj niekoľko zlepšení, ktoré by mohli pomôcť pri poisťovaní kybernetických rizík. Tieto návrhy sme zostavili na základe štruktúrovaných rozhovorov ale aj na základe analýzy vybraných produktov poistenia kybernetických rizík poistného trhu Európskej únie. Vzhľadom na to, že rôzne sektory môžu kategorizovať kybernetické riziká odlišným spôsobom, navrhli sme, aby poisťovne vytvorili kategorizáciu kybernetických rizík pre každý sektor samostatne, na základe takých druhov kybernetických rizík, ktoré daný sektor najviac ohrozujú. Veľkým prínosom pre poistenie kybernetických rizík by podľa nášho názoru bolo zapojenie štátnych orgánov do tejto problematiky, keďže spoločnosti im musia reportovať údaje o všetkých kybernetických incidentoch. Ďalej navrhujeme zlepšenie systematického zberu dát o škodách spôsobených realizáciou

kybernetických rizík, ktoré by si mohli poisťovne vymieňať na multilaterálnom základe, alebo by mohli regulačné orgány poskytnúť spoločnú anonymizovanú platformu na zdieľanie tohto typu údajov.

Pri komparácii poistení kybernetických rizík pre spoločnosti sme zistili, že vybrané poisťovne (Kooperativa pojišťovna, a.s., ČSOB poisťovňa, a.s., Colonnade Insurance S.A., AXA Versicherung AG) poskytujú približne rovnaké poistné krytie. Vybrané poistenia kybernetických rizík sme porovnali na základe konkrétnych kategórií rizík, ktoré kryjú. Všetky štyri poisťovne kryli poškodenie dobrého mena, narušenie ochrany dát, ujmu tretej strane, prerušenie prevádzky, právne zastupovanie a DDoS útoky. Pokuty a sankcie kryl iba poistný produkt od Colonnade Insurance. PCI-DSS (Štandard zabezpečenia údajov v odvetví platobných kariet) kryjú ČSOB poisťovňa a AXA Versicherung. Najhoršie z týchto štyroch porovnávaných poisťovní dopadla česká Kooperativa pojišťovna, ktorá nekryla ako jediná z nich riziká spojené s vydieraním a obnovou dát.

Zoznam použitej literatúry

[1] AXA Versicherung AG. 2022. Cyber-Versicherung. [online]. [cit. 6-4-2022]. Dostupné na internete:<https://www.axa.de/geschaeftskunden/cyber-versicherung>

[2] Banky.sk. 2020. Kybernetické útoky sú najväčšou hrozbou pre firmy, ukázal Allianz Risk Barometer 2020 [online]. [cit. 6-2-2022].Dostupné na internete: <https://banky.sk/kybernetickе-utoky-su-najvacsou-hrozbou-pre-firmy-ukazal-allianz-risk-barometer-2020/>

[3] BROKEŠOVÁ, Zuzana – MARKO, Peter – ONDRUŠKA, Tomáš. *Vývojové trendy v poisťovníctve 2014* [online]. Bratislava: Vydavateľstvo EKONÓM, 2014, CD-ROM [258 s., 12,9 AH] [cit. 2022-2-21]. ISBN 978-80-225-3846-6.

[4] CEBULA, J., James, Lisa R. YOUNG, *A Taxonomy of Operational Cyber Security Risks*. [online]. Dostupné na internete: <https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf>

[5] CHOVAN. Pavel. Poisťovníctvo v kocke. *Poistné rozhľady: časopis slovenského poisťovníctva*. Bratislava: Slovenská asociácia poisťovní, 2006, 12(4), 19. ISSN 1335-1044.

[6] COLONNADE INSURANCE S.A.. 2018. *Poistenie kybernetických rizík cyber ako rozšírenie poistenia GDPR.* [online]. [cit. 3-4-2022].Dostupné na internete:<https://assets-eu-01.kc-usercontent.com/65b2eb68-cf8e-0106-94e7-7fcbfbaa6c5e/a9df9b07-3691-45e0-bd0c-d5ae039f697a/06_pl_ci_cyber-gdpr_19_09.pdf>

[7] Committee on National Security Systems. 2022. *CNSS Glossary* . [elektronický zdroj]. [cit. 10-3-2022]. Dostupné na internete: < https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf >

[8] COURBAGE, C., LIEDTKE, P. M., 2003. *Insurability, its limits and extensions. Insurance research and practice*, str. 44-49.

[9] ČSOB pojišťovna a.s.. 2022. Poistenie kybernetických rizík. [online]. [cit. 3-4-2022].Dostupné na internete: <https://www.csobpoj.cz/pojisteni/podnikatele-firmy/pojisteni-kybernetickych-rizik#portlet_com_liferay_nested_portlets_web_portlet_NestedPortletsPortlet_INSTANCE_zZC3XvCR7ETG>

[10] HANNOVER RE. *Glossary*. [online]. [cit. 12-2-2022].Dostupné na internete: <https://www.hannover-re.com/16383/a>

[11] HOLSBOER, J. H., 1995. *Insurability and uninsurability: An introduction. The Geneva Papers on Risk and Insurance*, str. 407-413.

[12] INTERNATIONAL STANDARD ISO/IEC 27000. 2018. *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. [online]. [cit. 8-2-2022]. Dostupné na internete: <https://akela.mendelu.cz/~lidak/IPI/ISO_IEC_27000_2018.pdf >

[13] KARTEN, W. T., 1997. *How to Expand the Limits of Insurability. The Geneva Papers on Risk and Insurance*, , str. 515-522.

[14] Kooperativa poisťovňa a.s.. Poistné podmienky pre poistenie majetku a zodpovednosti za škodu malých a stredných podnikateľov. [elektronický zdroj]. [cit. 9-2-2022].Dostupné na internete: <https://kooperativa.sk/content/userfiles/insuranceterms/Poistn%C3%A9%20podmienky%20pre%20poistenie%20majetku%20a%20zodpovednosti%20za%20%C5%A1kodu%20mal%C3%BDch%20a%20stredn%C3%BDch%20podnikate%C4%BEov%20PODNIKATE%C4%BD%20produkt%20462_platne%20od%2015.12.2020.pdf>

[15] Kooperativa pojišťovna, a.s.. 2022. Pojištění kybernetických rizik. [online]. [cit. 4-4-2022].Dostupné na internete:<https://www.koop.cz/pojisteni/pojisteni-malych-a-strednich-podnikatelu/pojisteni-kybernetickych-rizik>

[16] KRÁTKA, Zuzana. 2009. *Vplyv globalizácie na riziká v poisťovníctve a ich efektívne riadenie: dizertačná práca*. Bratislava : Ekonomická univerzita v Bratislave, 2009. 172 s.

[17] KRÁTKA, Zuzana. 2020. Underwriting Risk Management: Riadenie upisovacieho rizika. *Aktuárska veda v teórii a v praxi 2020: recenzovaný monografický zborník vedeckých prác: Reviewed Collection of Resarch Papers*. Brno: H.R.G. spol. s r.o., 2020, , 57-63. ISBN 978-80-88320-36-4.

[18] KUNREUTHER, H., 1997. *Rethinking Society's Management of Catastrophic Risks. Geneva Papers on Risk and Insurance*, str. 51–177.

[19] MAJTÁNOVÁ, A. a kol.: *Poisťovníctvo*. Bratislava: EKONÓM, 2005. 184 s. ISBN 80-225-1940-5, s. 52

[20] ELING, Martin – WIRFS, Jan Hendrik. 2016. *Cyber Risk: Too Big to Insure?*. [online]. [cit. 11-12-2021]. Dostupné na internete: <https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf>

[21] National Institute of Standarts and Technology. 2019. *Cybersecurity Framework Manufacturing Profile Low Impact Level Example*. [online]. [cit. 11-12-2021]. Dostupné na internete: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8183A-3.pdf>

[22] National Institute of Standarts and Technology. 2021. *Developing Cyber-Resilient Systems*. [online].[cit. 11-12-2021]. Dostupné na internete: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf>

[23] Paul Pangaro.PhD. 2013 "*Getting Started" Guide to Cybernetics*. [online]. [cit. 6-1-2022].Dostupné na internete: < https://www.pangaro.com/definition-cybernetics.html>

[24] PricewaterhouseCoopers. 2017. Cyber Risk – *Enlightenment through information risk management*. [elektronický zdroj]. [cit. 10-12-2021]. Dostupné na internete: <https://www.pwc.com.au/consulting/assets/cyber-risk-paper-july2017.pdf>

[25] Slovenská asociácia poisťovní. 2012. *Ako funguje poisťovníctvo*. [online]. [cit. 6-2-2022].Dostupné na internete: <https://www.slaspo.sk/tmp/asset_cache/link/0000045011/21025%20IE%20Ako%20funguje%20poistovnictvo.pdf>

[26] Smernica Európskeho parlamentu a Rady 2009/138/ES z 25. novembra 2009 o začatí a vykonávaní poistenia a zaistenia (Solventnosť II). [online]. [cit. 12-2-2022].Dostupné na internete:<https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32009L0138&from=sk >

[27] Tatra banka a.s.. 2022. Kyber poistenie. [online]. [cit. 3-4-2022].Dostupné na internete:<https://www.tatrabanka.sk/sk/personal/sporenie-investovanie-poistenie/kyber-poistenie/>

[28] The European Union Agency for Network and Information Security (ENISA). 2015. *Definition of Cybersecurity*. [online]. [cit. 8-2-2022]. Dostupné na internete: <https://www.enisa.europa.eu/publications/definition-of-cybersecurity>

[29] The European Union Agency for Network and Information Security (ENISA). 2021. *ENISA THREAT LANDSCAPE 2021*. [online]. [cit. 8-2-2022]. Dostupné na internete: < https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>

[30] UNIQA poisťovňa, a.s.. 2022. Kyber balík. [online]. [cit. 3-4-2022].Dostupné na internete:< https://www.uniqa.sk/kyber-balik/>

[31] ZAJÍC. Radek. 2015. *Vybraná kybernetická rizika a jejich předcházení*. [online].[cit. 13-12-2021]. Dostupné na internete:

<https://dspace.cvut.cz/bitstream/handle/10467/66235/MU-DP-2016-Zajic-Radek-thesis.pdf?sequence=-1>

[32] Zbierka Zákonov Slovenskej Republiky. 2018. Zákon o kybernetickej bezpečnosti 69/2018. [online]. [cit. 10-3-2022]. Dostupné na internete: <https://www.slov-lex.sk/static/pdf/2018/69/ZZ_2018_69_20220226.pdf>

[33] Zbierka Zákonov Slovenskej Republiky. 2018. Zákon o ochrane osobných údajov č. 18/2018. [online]. [cit. 15-3-2022]. Dostupné na internete: < https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20180525>