Univerzita Pardubice

Fakulta ekonomicko-správní

Pojištění kybernetických rizik

Diplomová práce

2023 Bc. Magdaléna Schejbalová

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Magdaléna Schejbalová**
Osobní číslo:	**E21186**
Studijní program:	**N0412A050013 Finance**
Téma práce:	**Pojištění kybernetických rizik**
Zadávající katedra:	**Ústav matematiky a kvantitativních metod**

Zásady pro vypracování

Cílem práce je nastavení optimální pojistné ochrany proti kybernetickým rizikům. V rámci práce bude provedena detailní analýza pojistných produktů zaměřených na krytí kybernetických rizik nabízených na českém pojistném trhu a srovnání souvisejících pojistných podmínek.

Osnova:
- Vymezení pojmu pojištění.
- Charakteristika kybernetických rizik.
- Analýza pojistných produktů zaměřených na kybernetická rizika na českém pojistném trhu.
- Porovnání souvisejících pojistných podmínek jednotlivých pojistných produktů zaměřených na kybernetická rizika.

Rozsah pracovní zprávy: **50**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

ANTONUCCI, Domenic. *The cyber risk handbook: Creating and measuring effective cybersecurity capabilities*. New Jersey: Wiley, 2017. ISBN 978-1-119-30880-5.
KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80--88168-31-7.
SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.
ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

Vedoucí diplomové práce: **Mgr. Hana Boháčová, Ph.D.**
Ústav matematiky a kvantitativních metod

Datum zadání diplomové práce: **1. září 2022**
Termín odevzdání diplomové práce: **30. dubna 2023**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

doc. Ing. Jan Černohorský, Ph.D. v.r.
vedoucí ústavu

V Pardubicích dne 1. září 2022

PROHLÁŠENÍ

Prohlašuji:

Práci s názvem Pojištění kybernetických rizik jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 24. dubna 2023

Bc. Magdaléna Schejbalová v. r.

PODĚKOVÁNÍ

Tímto bych ráda poděkovala své vedoucí diplomové práce Mgr. Haně Boháčové, Ph.D., za odborné vedení a cenné připomínky, které mi při zpracování práce pomohly. Dále bych chtěla poděkovat vybrané společnosti za ochotu a čas při poskytnutí potřebných informací.

ANOTACE

Diplomová práce se zabývá problematikou pojištění kybernetických rizik. V práci je nejprve vymezen pojem pojišťovnictví, dále obsahuje charakteristiku kybernetické bezpečnosti, kde se podrobněji věnuje kybernetickým útoků a vývoji kybernetické bezpečnosti v České republice. Dále je v práci provedena analýza pojistných produktů zaměřených na kybernetická rizika pro podnikatelské subjekty na českém pojistném trhu, které jsou poté mezi sebou porovnány. Následně je charakterizována vybraná společnost a její kybernetická rizika a na základě toho je pro ni vybrán optimální pojistný produkt.

KLÍČOVÁ SLOVA

pojištění, kybernetická rizika, kybernetická bezpečnost, kybernetické útoky, kyberprostor

TITLE

Cyber Risk Insurance

ANNOTATION

This Diploma thesis follows up a problematic of cyber risk insurance. The thesis first defines the concept of the insurance industry, then it contains the characteristics of cyber security, where it deals in more detail with cyber attacks and the development of cyber security in the Czech Republic. The thesis also includes an analysis of insurance products focused on cyber risks for business entities on the Czech insurance market, which are then compared with each other. Subsequently, the selected company and its cyber risks are characterized, and based on this, the optimal insurance product is selected for it.

KEYWORDS

insurance, cyber risks, cyber security, cyber attacks, cyberspace

OBSAH

SEZNAM OBRÁZKŮ, GRAFŮ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

ČR	Česká republika
ČSOB	Československá obchodní banka
ČEZ	České energetické závody
EU	Evropská unie
GB	Gigabyte
IT	Informační technologie
NATO	North Atlantic Treaty Organization
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OSN	Organizace spojených národů
PCI DSS	Payment Card Industry Data Security Standard
PR	Public Relations
RKB	Rada pro kybernetickou bezpečnost

ÚVOD

Problematika kybernetických rizik je v dnešním světě velice aktuální téma. Kybernetická rizika jsou rizika, která se objevují v digitálním prostředí. Číhají na nás v běžném životě ze všech stran, přece jenom máme asi každý mobilní telefon nebo počítač a internetové připojení. Mnohem více také začínají využívat informační technologie příslušníci starší generace, kteří ale nemusí mít tak dobré znalosti o tom, jak se na internetu chovat a na co si dávat pozor. V dnešní době je také velký rozmach digitalizace a s tím je spojená i větší možnost právě těchto rizik. Útočníci přichází stále s novými typy kybernetických útoků, kterými jsou ohrožena všechna odvětví. Denně je na všelijaké společnosti vedeno tisíce kybernetických útoků. Každá společnost má jistě různé antivirové programy, ale i s těmi si některé druhy útoků poradí.

S dobou pandemie Covid-19 se rozvinula jak již zmíněná digitalizace, tak i mnoho lidí začalo více pracovat z domova. I v rámci veřejné správy si můžeme plno věcí vyřešit pomocí internetu. S tím samozřejmě přichází další rizika, například rizika spojená s připojením pracovního počítače k nezabezpečené síti, což může vést k úniku citlivých dat.

Pojištění kybernetických rizik je v současné době nejvíce rozvíjející se oblast v pojišťovnictví. Mohou si ho sjednat podnikatelské i nepodnikatelské subjekty. Toto pojištění by mělo být důležitou součástí pojistné ochrany každé společnosti, ale i běžného člověka, protože pomáhá snižovat finanční dopady v případě kybernetického incidentu. Některé kybernetické události mohou napáchat obrovské finanční škody. Pojištění ale nepomůže vyřešit špatné zabezpečení počítače či softwaru, špatně zvolená slabá hesla nebo chybu způsobenou člověkem. Proto by měla každá podnikatelská společnost dbát na důsledné zabezpečení svých zařízení a také proškolení svých zaměstnanců.

Ke splnění hlavního cíle této diplomové práce je nutné nejprve provést detailní analýzu pojistných produktů zaměřených na krytí kybernetických rizik nabízených na českém pojistném trhu a dále srovnání jejich souvisejících pojistných podmínek. Na základě výše uvedeného je **cílem práce nastavení optimální pojistné ochrany proti kybernetickým rizikům.**

V práci budou nejprve naplněny tyto dílčí cíle a následně bude charakterizována vybraná společnost a její možná kybernetická rizika. Dále bude pro tuto společnost posouzena vhodnost jednotlivých pojistných produktů, které jsou nabízené na českém pojistném trhu. Nakonec bude pro společnost vybrán nejvhodnější optimální pojistný produkt na základě jejích možných kybernetických rizik.

1 POJIŠŤOVNICTVÍ

V této kapitole si nejprve vymezíme základní pojmy týkající se pojišťovnictví, jako je například pojistník, pojištěný, pojistitel nebo pojistné plnění. Dále se budeme věnovat obecné charakteristice pojištění. Následující podkapitola nás bude informovat o tom, jak pojištění členíme a v neposlední řadě bude podrobněji vysvětleno komerční pojištění.

Než se přesuneme k podrobnějšímu výkladu pojišťovnictví, vysvětlíme si základní pojmy týkající se této oblasti. **Pojistník** uzavře smlouvu s pojišťovnou a zavazuje se hradit pojistné. Pojistníkem nemusí být totožná osoba s pojištěným, je to například v případě, kdy zákonný zástupce (pojistník) pojistí své dítě (pojištěný) pro případ úrazu. **Pojištěný** je osoba, která je v pojistné smlouvě uvedena jako osoba, na kterou se pojištění vztahuje, tzn. je chráněna pro případ úrazu, poškození majetku atd. **Pojistitel** je právnická osoba či jiná společnost s oprávněním vykonávat pojišťovací činnost, která uzavře a pojistníkem smlouvu a chrání majetek či život pojištěného. **Obmyšlený** je osoba, které bude vyplaceno pojistné plnění v případě smrti pojištěného. Ve většině případů je obmyšlená osoba uvedená v pojistné smlouvě. **Pojistné** je pravidelná částka, kterou platí pojistník v předem dohodnuté výši a intervalech. **Pojistné plnění** je finanční částka, která byla ujednána v pojistné smlouvě. Má na něj nárok pojištěný v případě nastání pojistné události. U některých pojištění může být sjednaný limit maximální částky, která bude pojišťovnou vyplacena. **Pojistná událost** je nahodilá situace, např. poškození majetku, při které vzniká nárok na vyplacení pojistného plnění, tzn. splní podmínky v pojistné smlouvě. Posledním pojmem, který si vysvětlíme je **zajišťovna**. Zajišťovna je vlastně pojišťovna pro pojišťovny. Přebírá část rizika za pojišťovny, aby neměly v budoucnu v případě velkých škod problém s likviditou.

Pojišťovnictví je specifická oblast každé ekonomiky sloužící ke krytí rizik, která vznikají v podnikání ale i v běžném životě. Podstatou pojišťovnictví je skutečnost, že nabízí pojistnou ochranu před riziky. Vybírá finanční prostředky pomocí pojistného, tím tvoří určité rezervy, se kterými dále pracuje. Většinu z těchto rezerv dále investuje

Zásadním pojmem v pojišťovnictví je riziko. Riziko je nejistota, kterou můžeme měřit mírou pravděpodobnosti. Riziko můžeme dále vysvětlit jako událost, která může v budoucnu nastat s určitou pravděpodobností, ale s výsledkem odlišným od očekávaného výsledku. Pojištěním tedy přesuneme riziko, resp. jeho dopady, na pojistitele. Nesnižujeme jím míru rizika, ale pouze jeho finanční dopady.

1.1 Pojištění

Existují dva způsoby, jak mohou ekonomické subjekty řešit finanční problémy v návaznosti na nahodilou situaci. První možností je financování z vlastních zdrojů, tzv. samopojištění, druhou možností je využití pojištění (přesunutí finančních dopadů plynoucích z rizika na pojišťovací instituci). Pojištění sice neovlivňuje vznik pojistných událostí a škod, ale pojišťovny se snaží ovlivňovat pojištěné různými bonusy, spoluúčastmi, malusy a dalšími, aby se snažili svým chováním předejít případným škodám. Pojišťovny takto ovlivňují klienty především v případě subjektivních rizik. Jako příklad si můžeme uvést pojištění odpovědnosti z provozu vozidla, nesprávně nazývané jako povinné ručení. U tohoto pojištění pojišťovny zohledňují škodní průběh pojištění v předcházejícím období. Pokud pojistník nezpůsobil žádnou škodu, tzn. pojišťovna nemusela vyplácet žádné pojistné plnění z pojištění odpovědnosti, poskytne mu pojišťovna slevu. V opačném případě, pokud pojistník způsobil v předešlém období nějakou škodu, pojišťovna mu připočítá přirážku k pojistnému.

Pojištění se řadí mezi finanční služby. Je to služba, která je poskytnutá za úplatu a poskytuje pojistnou ochranu na základě pojistné smlouvy. Pojištění jako součást ekonomické infrastruktury působí na proces reprodukce tak, že finanční prostředky přesune s ohledem na výskyt pojistných událostí tam, kde jsou v danou chvíli potřeba. Pojištění jako finanční službu můžeme charakterizovat následujícími znaky:

- má abstraktní charakter – pojišťovna se v pojistné smlouvě zavazuje, že v případě nastání přesně stanovené nahodilé události vyplatí předem stanovenou výši pojistného plnění;
- závisí na nahodilé události – pojišťovací instituce dopředu neví, kdy a jestli vůbec se daná událost vyskytne, dále není zřejmé, jaký ekonomický subjekt bude danou událostí zasažen a v neposlední řadě také není známa výše dopadů případné nahodilé události;
- je většinou dlouhodobé povahy;
- je tam určitá asymetrie informací – všechny smluvní strany nemají stejný přístup k informacím;
- za službu se platí předem – je to tzv. obrácený výrobní cyklus;
- spojeno s investováním dočasně volných peněžních prostředků (na budoucí platby pojistného plnění v případě nahodilé události).

Z právního hlediska můžeme říci, že pojištění je právní vztah. Tento vztah je upraven v pojistné smlouvě uzavřené mezi pojistníkem a pojistitelem. Pojistník se zavazuje poskytnou výplatu

pojistného plnění v případě nahodilé události, která je podrobněji definovaná ve sjednaných pojistných podmínkách. Pojistník ale na sebe přebírá závazek, že bude za tuto službu platit pojistné v předem stanovém termínu a výši. (Ducháčková, 2015)

1.2 Druhy pojištění

Pojištění můžeme členit podle různých hledisek, podle právního hlediska a podle způsobu financování. Z pohledu právního hlediska můžeme dělit pojištění na:

- dobrovolné,
- povinné.

U dobrovolného pojištění záleží jen na daném ekonomickém subjektu, zda si pojištění sjedná či nikoliv. Jako příklad dobrovolného pojištění si můžeme uvést úrazové pojištění, pojištění majetku nebo cestovní pojištění.

Povinné pojištění je stanoveno zákonem, tzn. musí ho každý bez výjimky platit. Dále dělíme povinné pojištění na:

- smluvní povinná pojištění,
- zákonná pojištění.

U smluvního povinného pojištění je povinnost uzavřít pojištění daná zákonem. Ekonomický subjekt si toto pojištění musí sjednat, ale může si sám vybrat, u které pojišťovací instituce smlouvu uzavře. Příkladem může být již zmiňované pojištění odpovědnosti z provozu vozidla. Ze zákona musíme mít toto pojištění sjednané, pokud chceme používat automobil, ale můžeme si k uzavření vybrat kteroukoliv pojišťovnu. (Černohorský, 2020)

Zákonné pojištění je opět povinné ze zákona, ale rozdílem oproti smluvnímu povinnému pojištění je, že se v těchto případech neuzavírá pojistná smlouva. U tohoto pojištění je lhůta platby pojistného, výše pojistného a pojišťovací instituce jasně vymezená. Jako příklad si můžeme uvést sociální a zdravotní pojištění. Zákonné pojištění s ohledem na obecné definování pojmu pojištění není v pravém slova smyslu pojištěním. Především není naplněna skutečnost, že platba do kolektivního pojistného fondu je stanovena podle výše rizika. U zákonného pojištění je pojistné pevně stanoveno.

Dalším hlediskem, podle kterého dělíme pojištění, je způsob financování. Podle způsobu financování rozlišujeme dva systémy:

- sociální pojištění,
- komerční pojištění. (Ducháčková, 2015)

1.2.1 Sociální pojištění

Sociální pojištění je spojeno s krytím rizik sociálního charakteru. Kryje rizika spojená s dlouhodobou nebo krátkodobou pracovní neschopností, různé pracovní úrazy či nemoci, dále kryje potřebu zdravotní péče, nebo pokud se ocitneme v tíživé situaci zapříčiněné nezaměstnaností. Sociální pojištění je ve většině zemí povinné. Forma tohoto pojištění, jako podmínky, obsah či výše příspěvků a dávek, je vymezena v právních předpisech jednotlivých států.

Pro sociální pojištění je charakteristická skutečnost, že tvorby rezerv nejsou podmíněny rizikem. To znamená, že výše pojistného není určena ve vazbě na riziko, ale všichni účastníci sociálního pojištění ji mají stanovenou stejně, většinou procentem z příjmu. Tímto se odlišuje od komerčního rizika, u kterého je stanovena výše pojistného v závislosti na velikosti rizika.

V rámci sociálního pojištění je uplatňován princip solidarity, což znamená že všichni účastníci se na platbě pojistného podílí stejně (platí stejné procento), ale náhrady se poskytují jen těm, kteří to v danou chvíli opravdu potřebují. Můžeme říci, že někteří lidé v rámci určitého časového úseku budou třeba jen pojistné platit a žádné pojistné náhrady dostávat nebudou, ale až budou i oni postiženi nějakým sociálním rizikem, příspěvek či dávku dostanou vyplacenou také. (Ducháčková, 2015; Černohorský, 2020)

Na sociálním pojištění se podílí také stát, který platí pojistné za děti, studenty nebo lidi v důchodovém věku. Dalším subjektem, který se podílí na platbě pojistného sociálního pojištění, jsou zaměstnavatelé, kteří odvádí část pojistného za své zaměstnance.

1.2.2 Komerční pojištění

U komerčního neboli soukromého pojištění platí zásada ekvivalence. Zásada ekvivalence znamená, že velikost pojistného účastníků je závislá na velikosti možného rizika. Komerční pojištění má ve většině případů dobrovolnou podobu a je zprostředkováváno komerčními pojišťovnami.

Komerční pojištění můžeme rozdělovat podle způsobu tvorby rezerv nebo podle druhu krytých rizik. Podle způsobu tvorby rezerv rozlišujeme:

- riziková pojištění,
- rezervotvorná pojištění.

U rizikových pojištění platí tzv. podmíněná návratnost peněžních prostředků. Tato návratnost je podmíněna vznikem pojistné události, ale není však jisté, jestli tato událost nastane. Běžně se stává, že daný ekonomický subjekt platí pojistné, ale žádná riziková událost nenastane, tudíž mu není vyplaceno žádné pojistné plnění během platnosti pojistné smlouvy. Příkladem rizikového pojištění je úrazové pojištění.

Rezervotvorná pojištění jsou charakteristická vytvářením rezervy na budoucí vyplacení sjednaného pojistného plnění. U tohoto druhu pojištění je jisté, že sjednaná rizika někdy v budoucnosti vzniknou. Z toho vyplývá, že pojistné plnění je vyplaceno. Jako příklad si uvedeme životní pojištění, konkrétně spojení pojištění úmrtí a dožití. Pokud se pojištěný dožije sjednaného věku, pojistné plnění mu bude vypláceno. V opačném případě, pokud se sjednaného věku nedožije, peněžní prostředky budou vypláceny obmyšlenému. (Černohorský, 2020)

Dalším hlediskem je druh krytých rizik. Podle tohoto hlediska rozlišujeme:

- životní pojištění,
- neživotní pojištění.

Životní pojištění slouží ke krytí životních rizik. Jsou to rizika, která ohrožují životy lidí (riziko smrti a riziko dožití). Výše pojistného plnění se stanovuje podle velikosti pojistné částky. Často se životní pojištění kombinuje i s neživotním rizikem, jako například rizikem invalidity či úrazu. Životní pojištění je spojením pojištění a investování. Principem životního pojištění je, že část platby pojistného je investováno dále do fondů a zhodnocováno a část je určena na krytí sjednaných rizik. Takto nashromážděná a zhodnocená částka z fondů je v případě dožití sjednaného věku vyplacena klientovi. V případě klientovy smrti se částka vyplatí pozůstalým.

Neživotní pojištění je určeno ke krytí neživotních rizik. Nenabízí možnost spoření (investice), jako je tomu u životního pojištění. Neživotní pojištění můžeme dále rozdělit na:

- pojištění osob – neživotní,
- pojištění majetku,
- pojištění odpovědnosti,
- pojištění právní ochrany,

- cestovní pojištění.

Neživotní pojištění osob se týká úrazového pojištění pro případ smrti, úrazu či trvalých následků. Dále se může jednat o pojištění příjmu v případě pracovní neschopnosti nebo pojištění pro případ vážného onemocnění. Hlavní funkcí tohoto pojištění je krytí trvalých následků způsobených úrazem, resp. smrti zapříčiněné úrazem.

Pojištění majetku slouží ke krytí rizik spojených se ztrátou, zničením či poškozením majetku. Může se jednat o rizika způsobená živelní pohromou, havárií, cizí osobou, riziko přerušení provozu a jiné. Příkladem pojištění majetku může být pojištění domácnosti, havarijní pojištění, pojištění hospodářských zvířat a plodin nebo pojištění majetkových práv (know-how).

Pojištění odpovědnosti se vztahuje na rizika, která může způsobit pojištěný. Jedná se o majetkovou či nemajetkovou újmu způsobenou jinému ekonomickému subjektu. Újma se může týkat zdraví, majetku včetně finanční ztráty či ušlého zisku. Do této kategorie pojištění můžeme zařadit například již zmiňované pojištění odpovědnosti z provozu vozidla nebo pojištění odpovědnosti za škody při výkonu povolání. V rámci této kategorie pojištění se rozlišuje dobrovolné a povinně smluvní pojištění, které jsme si vysvětlili již výše.

Pojištění právní ochrany zahrnuje krytí rizik spojených se soudním řízením. Mohou to být například soudní výdaje, poskytnutí právního servisu a další náklady s tímto spojené. Klienti ho využívají v případě obvinění, přestupkových či správních řízeních, ale i při záporně uznané reklamaci nebo pokud nějaký ekonomický subjekt nedodrží sjednané smluvní podmínky. (Černohorský, 2020; Ducháčková, 2015)

Cestovní pojištění se zřizuje v případě vycestovaní do zahraničí. Při sjednávání tohoto pojištění si může klient vybrat z nepřeberného množství kombinací různých druhů neživotních pojištění. Především se jedná o zdravotní pojištění, pojištění úrazu, odpovědnosti či storna zájezdu.

V této diplomové práci se dále budeme zabývat pouze komerčním pojištěním, a to konkrétně pojištěním kybernetických rizik, kde se podrobněji podíváme na pojistné podmínky jednotlivých pojišťovacích institucí.

2 KYBERNETICKÁ BEZPEČNOST

S vymezením pojmu kybernetická bezpečnost velice úzce souvisí pojem kyberprostor a s ním spjaté pojmy kybernetické riziko a kybernetická hrozba. Kybernetické riziko je riziko vyvolané kybernetickou hrozbou. Kybernetická hrozba je hrozba vyskytující se v kybernetickém prostoru.

V této kapitole bude nejprve vymezen kyberprostor a následně samotná kybernetická bezpečnost, kde budou vysvětleny jednotlivé triády, jako je CIA, prvky kybernetické bezpečnosti a životní cyklus kybernetické bezpečnosti. Následně si popíšeme vybrané kybernetické útoky, například malware, phishing, botnet a další. Poslední podkapitola bude věnována Vývoji kybernetické bezpečnosti v České republice, kde bude popsáno, jak se vyvíjela legislativa v této oblasti.

2.1 Kyberprostor

Kyberprostor je fiktivní digitální prostředí, v němž dochází k výměně a zpracování informací, které pochází z počítačových sítí, služeb a informačních systémů (Sedlák a Konečný, 2021).

Kybernetický prostor je virtuální svět, který není ohraničený začátkem ani koncem. Tento virtuální svět je ale závislý na hmotných médiích (technologiích), které se však nachází v reálném světě. Pokud by se tato hmotná média zcela poškodila, došlo by i k zániku samotného kyberprostoru. Kyberprostor můžeme vymezit také jako prostředí vytvářené komunikačními a informačními technologiemi. (Kolouch a Bašta, 2019)

Kyberprostor je vnímán jako prostor, který se skládá z těchto tří následujících vrstev:

- fyzická vrstva,
- logická vrstva,
- sociální vrstva.

Vrstvy jsou pak dále složeny z pěti komponentů.

Fyzická vrstva obsahuje geografické komponenty a fyzické síťové komponenty. Geografickými komponenty se rozumí fyzické umístění síťových prvků a fyzickými síťovými komponenty je myšlen veškerý hardware a infrastruktura, jako jsou kabely, routery, servery, počítače, různé konektory a další. Můžeme říct, že geopolitické hranice je možno

v kybernetickém prostoru překročit opravdu snadno a rychle, ale existují stále určitá omezení, která vycházejí z reálného fyzického světa.

Logická vrstva zahrnuje logické síťové komponenty, které jsou technické povahy a představují logická spojení mezi jednotlivými uzly sítě. Tyto uzly jsou různá síťová zařízení jako telefony, počítače nebo osobní digitální asistenti. V internetové síti je to jakékoliv zařízení s IP adresou.

Třetí vrstvou je sociální vrstva, kterou tvoří komponenty osobnost a kyberosobnost. Kyberosobnost zahrnuje identifikační údaje osoby nebo identifikaci osoby v síti. Mezi tyto údaje můžeme zařadit emailovou adresu, telefonní číslo, IP adresu počítače a další. Komponenta osobnost představuje lidi, kteří jsou skutečně připojeni na síti. Jedna osoba může mít několik kyberosobností, jsou to například různé emailové adresy na různých počítačích, a zároveň jedna kyberosobnost může mít několik uživatelů (více lidí sdílí jeden konkrétní účet). (United States Army, 2010)

2.2 Vymezení kybernetické bezpečnosti

Odvětví kybernetické bezpečnosti se v současné době s vývojem různých technologií stává stále významnější. Komunikační a informační technologie se stále více využívají, ať už ve veřejné nebo soukromé sféře. Můžeme říci, že se bez nich už téměř neobejdeme. Z využívání těchto technologií vyplývá ale bohužel i nespočet kybernetických rizik.

Národní úřad pro kybernetickou a informační bezpečnost ve své Národní strategii kybernetické bezpečnosti České republiky uvádí, že kybernetická bezpečnost je soubor opatření a nástrojů, které mají zabezpečit ochranu a odolnost kybernetického prostoru i jeho okolí. Dále slouží k identifikaci, hodnocení a řešení kybernetických hrozeb a pomáhá zmírnit rizika a dopady možných kyberútoků. (NÚKIB, 2015)

Při realizaci kyberbezpečnosti by mělo dojít k naplnění těchto principů:

- CIA,
- prvky kybernetické bezpečnosti,
- životní cyklus kybernetické bezpečnosti.

Uvedené principy můžeme také nazývat jako triády kybernetické bezpečnosti. (Hsu a Marinucci, 2013)

2.2.1 CIA

Nejvíce používanou triádou je CIA. Využívání této základní triády bez využití dalších principů je však k zajištění kybernetické bezpečnosti nedostatečné. Zkratka je vytvořena z počátečních písmen anglických slov Confidentiality (důvěrnost), Integrity (celistvost) a Availability (dostupnost). CIA je většinou spojována s ochranou informací, dále je ale nutno tuto triádu implementovat na další složky kybernetické bezpečnosti, jako například data.

Důvěrnost znamená, že jen oprávněné osoby mají možnost dostat se k určitým informacím či datům nebo jen oprávněným osobám jsou tyto informace sděleny. Porušení důvěrnosti nastane například v případě, kdy někdo zneužije heslo k přihlášení do cizího uživatelského účtu.

Pojem **integrita** definuje skutečnost, že žádná nepovolaná osoba nesmí zasahovat do informací, dat, ani jejich nastavení. Musí být zaručeno, že informace a data jsou úplné a správné. Příkladem porušení integrity může být poškození pevného disku nebo záměrné padělání dokumentu.

Posledním pojmem je **dostupnost**, která představuje zaručený přístup k informacím a datům v případě jejich potřeby. Jako příklad porušení dostupnosti můžeme uvést selhání serveru. Dostupnost může být zajištěna zálohováním informací a dat. (Kolouch a Bašta, 2019; Šulc, 2018)

2.2.2 Prvky kybernetické bezpečnosti

Dalším principem jsou prvky kybernetické bezpečnosti. Prvky kybernetické bezpečnosti, přesněji řečeno jejich vzájemné působení, pomáhají zajistit kybernetickou bezpečnost. Mezi tyto prvky patří:

- lidé,
- technologie,
- procesy.

Lidé, neboli personální bezpečnost, v souvislosti s kyberbezpečností mohou být tvůrcem bezpečnosti, příjemcem pravidel kyberbezpečnosti, těmi, které je potřeba chránit před kyberútoky, těmi, u kterých je potřeba školení o pravidlech a principech kyberbezpečnosti a v neposlední řadě mohou být lidé také riziko nebo hrozba právě při budování kybernetické bezpečnosti. Lidé jsou nejdůležitější složkou v kterékoliv bezpečnosti. Jejich role se u kyberbezpečnosti ještě zvyšuje, jsou to právě lidé, kteří jsou její nejslabší složkou, a na které

jsou cíleny různé kybernetické útoky. Prvním důvodem tohoto tvrzení je, že počítačové a informační systémy jsou používány zatím krátce. Většina lidí je začala používat až po roce 1990 a internet ještě o pět let déle, v roce 1995. Sociální sítě, které jsou dnes nezbytnou součástí každodenního života, jsou využívány teprve deset let. Dalším důvodem je rychlost a různorodost vývoje hardwaru, ale především různých softwarů. Právě kvůli této rychlosti se nestíhají uživatelé zabývat bezpečností, která s využíváním softwaru souvisí. Třetí důvod je ten, že bez informačních a komunikačních systémů a technologií se v dnešní době již neobejdeme. Lidé, kteří využívají informační technologie, by měli znát základní pravidla chování v kyberprostoru, u využívaných počítačových softwarů alespoň jejich základní funkce, dále by měli prozkoumat využívané aplikace, především jejich smluvní podmínky a případně takovou aplikaci nevyužívat a neposlední řadě by se všichni lidé využívající informační technologie měli vzdělávat. Při dodržování těchto předcházejících kroků můžeme být v kyberprostoru alespoň trochu více chráněni a útoky hackerů či jiných útočníků budou méně pravděpodobné.

Technologie, neboli fyzická bezpečnost, jsou pro běžného uživatele nástrojem, díky kterému mohou posílat emaily, připojit se k sociálním sítím, sledovat různá videa a používat další aplikace. Tento uživatel využívá především koncové technologie, jako je počítač, mobil či tablet. O dalších technologických vrstvách nutných pro funkci této technologie neví nebo se o ně nezajímá.

Na technologiích běžní uživatelé i organizace ve většině případů nešetří a jsou za ně ochotni zaplatit nemalé peníze, ať už je to z důvodu zastaralosti nebo jen, protože potřebují novější telefon či počítač. Je potřeba je udržovat ve stavu, kdy jsou schopny reagovat na vývoj IT. Technologie by měly být především pravidelně aktualizované a zabezpečené. (Kolouch a Bašta, 2019)

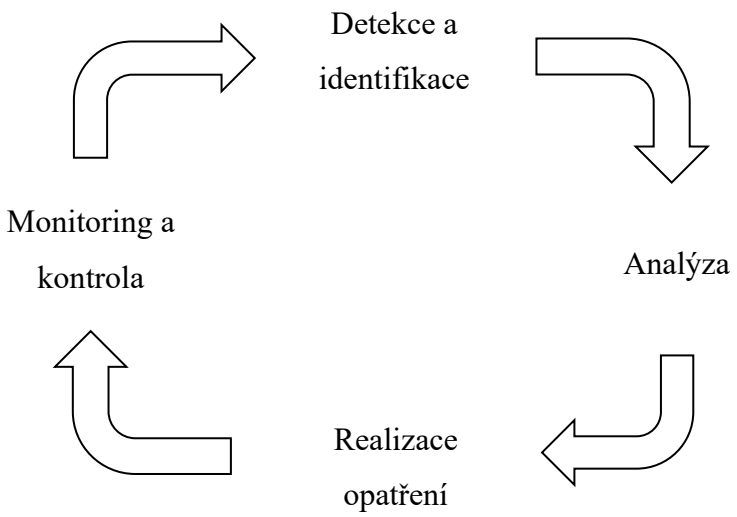
Procesy, neboli organizační bezpečnost, je nutné vytvořit z toho důvodu, aby lidé mohli používat technologie. Procesy je třeba vyvíjet ke snižování rizik nebo předcházení a zjišťování kybernetických útoků. Především by se ale organizace při nastavování procesů kybernetické bezpečnosti měly zaměřit na důkladné proškolení lidských zdrojů využívajících technologie, aby byly schopny včas útoky rozpoznat. (Microsoft, 2023)

K otestování svých zaměstnanců mohou využívat i různé simulace kybernetických útoků, například zasílání podvodných emailů, kde vybízejí příjemce emailu k přihlášení do různých

programů, aplikací apod. Pomocí těchto simulací se lidé lépe naučí rozpoznávat nebezpečné emaily.

2.2.3 Životní cyklus kybernetické bezpečnosti

Posledním principem kybernetické bezpečnosti je životní cyklus kybernetické bezpečnosti. Při budování kybernetické bezpečnosti nemůžeme nikdy říct, že jsme v bodě či stavu, kdy jsme chráněni před kybernetickými útoky. Kybernetická bezpečnost je proces, který se neustále vyvíjí. Tento proces je možné přirovnat k analýze rizik. Můžeme ho znázornit následujícím diagramem na obrázku č. 1. (Janko, © 2023)



Obrázek 1: Životní cyklus kybernetické bezpečnosti

Zdroj: vlastní zpracování (podle Janka, © 2023)

Nejprve hrozbu či útok identifikujeme a poté provedeme jeho analýzu. Tím zjistíme, jaká a jak velká rizika z útoku vyplývají. Následuje realizace opatření, což mohou být různá doporučení vytvořená na základě předchozí analýzy nebo již zmíněná školení či edukace lidských zdrojů. Opatření slouží k lepšímu předcházení a zvládání útoků v budoucnu nebo, aby jejich následek byl co nejnižší. Další fází je kontrola a monitoring. V rámci této fáze probíhá audit a kontrolují se zavedená opatření.

2.3 Kybernetické útoky

S kybernetickými útoky se můžeme setkávat čím dál tím častěji a škody jimi způsobené mohou být obrovské. Nebezpečné jsou především kvůli své asymetrii, protože náklady na vytvoření

těchto rizik jsou minimální oproti škodě, kterou způsobí. Je jasné, že počet těchto útoků bude růst s přibývajícím počtem zařízení, která jsou připojena k internetu. Každé zařízení připojené k internetu může být napadeno. (Šulc, 2018)

Na začátek si vysvětlíme dva pojmy související s kybernetickými útoky, těmi jsou hacker a cracker. Hacker pomocí svých znalostí a dovedností odhaluje slabá místa aktiv ve prospěch jejich uživatelů. Hledá řešení, jak slabá místa odstranit, dále může hledat různé programátorské chyby nebo programovat algoritmy. Hacker má mnohem větší počítačové znalosti než cracker. Zatímco cracker úmyslně poškozuje počítačovou bezpečnost za účelem svého vlastního prospěchu a zisku. Je schopen pomocí svých znalostí získat neoprávněné informace nebo proniknout do různých počítačových systémů. (Sedlák a Konečný, 2021)

Ještě před pár desítkami let bylo některé kybernetické útoky téměř nemožné provést a v dnešní době jsou již zcela běžné. Dříve byl málokdo připojený k internetu, většina firem i domácností byla připojena přes pevnou linku, kde byl objem přenesených dat velice omezený. Útok tedy mohl spočívat jenom ve fyzickém vniknutí do systému a za využití technik sociálního inženýrství. Technika sociálního inženýrství představuje ovlivňování a manipulaci s lidmi. Sociotechnik je osoba ovládající tuto techniku. Sociotechnik se snaží přesvědčit či zmanipulovat oběť, aby mu poskytla potřebné informace, nebo aby udělala to, co po ní chce bez toho, aby si všimla, že byla zneužita. Sociotechnik má snahu vypadat důvěryhodně a vydává se za výše postavenou autoritu, tím pádem se daná oběť snaží žádosti co nejrychleji vyhovět.

K internetu se dokáže připojit nespočet zařízení, které máme doma. Ať už jsou to stolní počítače, notebooky, tablety, mobilní telefony, nebo televize, herní konzole, ale už i domácí spotřebiče a auta. Tato zařízení obsahují různé operační systémy a aplikace, které jsou čím dál složitější a zároveň je v nich stále více chyb. Systémy a aplikace stále vytváří pouze lidé a tak je jasné, že v systému o velikosti několika GB bude větší množství chyb. (Šulc, 2018)

Z předcházejících odstavců můžeme říct, že roste jak počet uživatelů zařízení připojených k internetu, tak i složitost a rozmanitost systémů a objem přenosu dat. Jedinou zanedbávanou položkou je povědomí o bezpečnosti těchto zařízení a systémů. Toto bezpečnostní povědomí je bohužel už několik let stále stejné. Je to z toho důvodu, že zařízení jsou v dnešní době běžně využívána prakticky všemi lidmi včetně malých dětí. Špatné bezpečnostní návyky můžeme ukázat například na heslech, kdy i přes neustále požadavky na různorodá a silná hesla, lidé používají hesla typu 12345 nebo svá jména, která jsou lehce prolomitelná. Dále lidé mají i mobilní telefony bez zámku obrazovky, kdy stačí přejet po displeji nebo zadat jednoduché gesto

a kdokoliv se do telefonu může dostat. Bezpečnosti nepřispívá ani sdílení informací na sociálních sítích. Všechny tyto okolnosti nahrávají útočníkům, kterých je stále více.

Typy kybernetických útoků, se kterými se můžeme v životě setkat, budou vysvětleny v následujících podkapitolách. Nejčastějšími typy útoku jsou malware, phishing, DDoS či spam.

2.3.1 Malware

Malware je zkrácený výraz pro malicious software. Je to škodlivý software, jehož cílem může být téměř cokoliv a projevit na zařízení se může různě. Cílem je většinou získání informací, špionáž či krádež identity. Součástí malwaru je několik dalších typů nebezpečných softwarů. Jsou jimi například adware, ransomware, červi, spyware či scareware.

Adware je aplikace, při jejímž používání uživatelům neustále vyskakuje nějaká reklama. Ransomware bude podrobněji vysvětlen v textu níže. Počítačový červ se dokáže sám šířit na jiná zařízení, automaticky posílá svoji kopii na ostatní počítače. Po infikování přebírá kontrolu nad zařízením ve svůj prospěch. Spyware je špionážní program, který odesílá data pomocí internetu bez uživatelova vědomí. Sleduje uživatelovo chování a zvyklosti při prohlížení internetu. Scareware je označení pro falešný antivirový program. Ve většině případů se uživateli zobrazí nabídka k jeho stažení při prohlížení nějaké nakažené webové stránky.

Pomocí malwaru může útočník získat přístup k našim datům či účtům, včetně internetového bankovnictví, nebo zcela převzít kontrolu nad naším zařízením. Jsou využívány různé způsoby, jak dostat malware do zařízení. Ve většině případů je ale potřeba, aby uživatel stáhl infikovaný soubor nebo klikl na podezřelý odkaz, a malware se jednoduše dostane do jeho počítače. (Šulc, 2018; Kresa, 2018)

2.3.2 Phishing

Phishing jsou útoky, které využívají technik sociálního inženýrství ke zneužití uživatelských dat, jako jsou přihlašovací nebo platební údaje. Zaměřuje se tedy na naše citlivé a osobní údaje. Útočníci napadají uživatele prostřednictvím e-mailu nebo v poslední době stále více prostřednictvím falešných profilů na sociálních sítích. Uživateli přijde email či zpráva, která vypadá velice důvěryhodně. Zpráva se tváří, že je odeslaná ze školy, zaměstnání nebo třeba banky. Útočník, vydávající se za tuto organizaci, požaduje po uživateli většinou velmi jednoduchou věc, při čemž je potřeba přihlášení k jeho uživatelskému účtu v dané organizaci.

Když uživatel otevře odkaz v e-mailu, kde zadá své údaje, přesně v tu chvíli se k nim útočník dostane a může je podle svojí libosti zneužít. Může například úplně vybrat náš bankovní účet. V České republice počet těchto útoků neustále roste a s tím bohužel i počet lidí, kteří se stanou obětí phishingu. (Sedlák a Konečný, 2021; Kresa 2018)

2.3.3 Botnet

Botnet je síť tzv. zombie počítačů infikovaných malwarem. Tyto počítače jsou rozestavěny po celém světě a jsou poskytovány za určitý poplatek ke zneužití různými kyberútoky. Botnet se může skládat ze stovek, ale i miliónů nakažených počítačů, které obsahují software, který umožní útočníkovi spravovat a zneužívat daný počítač k všelijakým útokům. Infikovaný počítač může být použit k rozesílání nevyžádané pošty, dále k prolamování hesel nebo těžení bitcoinů atd. (Šulc, 2018)

Ve chvíli, kdy je počítač napadený botem, začíná pracovat samostatně a uživatel nemá šanci si všimnout, že je jeho zařízení infikované. Bot se spojí s centrálním uzlem, C&C serverem, který mu zadá úkoly ke své práci. Pokud mu C&C server nezadá instrukce ihned, přepne se do vyčkávacího režimu a snaží se nedávat najevo, že je uvnitř uživatelova zařízení. C&C server může být kterýkoliv web, na který lze vložit nějaký obsah. Tento obsah musí být zakódovaný nebo zašifrovaný a pouze zombie počítač bude znát klíč, proto ho bude moct dešifrovat.

Botnet nemá za cíl poškození uživatelova zařízení či dat, ale peněžní zisk. Zakladatel botnetu (pasák) pronajímá armádu napadených zombie zařízení dalším útočníkům k provádění škodlivých činností. (Internetem bezpečně, © 2018)

2.3.4 Ransomware

Ransomware je škodlivý software, který se ve většině případů rozšiřuje jako tzv. drive-by down-load malware. To znamená, že se na zařízení dostane již při pouhé návštěvě nakažené webové stránky. Objevit se ale může i na důvěryhodných stránkách, u kterých stačí, když mají zobrazenou reklamu. Případně pokud oběť klikne na podezřelý odkaz v e-mailu, může si ransomware touto cestou nainstalovat také sám. Útočník může příjemce také přesvědčit, že má v zařízení nějaký vir a nabádá ho k tomu, aby provedl určitou akci, kterou problém vyřeší. Tím se ale začne do zařízení stahovat ransomware.

Nejvíce napadány jsou hlavně počítače s operačním systémem Microsoft Windows a dále také zařízení se systémem Google Android. V poslední době dochází také k napadání databázových

serverů, kdy útočník ovládne a poté zašifruje uložená data. Ransomware, na rozdíl od ostatních kybernetických útoků, nám úplně zabrání s počítačem či mobilním zařízením jakkoliv pracovat. Za opětovné zprovoznění zařízení útočník požaduje zaplatit tzv. výpalné (ransom), proto se tomuto útoku říká ransomware.

Rozlišujeme dva základní druhy:

- ransomware šifrující soubory,
- ransomware blokující počítač.

Popřípadě můžeme uvést ještě třetí, který je kombinací uvedených druhů, tzn. že zašifruje soubory a současně zabrání pracovat se zařízením. Ransomware, který zašifruje soubory, uživateli napíše, že po zaplacení určité částky mu bude poskytnut klíč k dešifrování jeho souborů. Pokud ransomware šifruje data od těch nejstarších, může se stát, že nebude úspěšný. Uživatel nemusí být ochotný zaplatit za tato data, protože je má zálohované nebo je už třeba nepotřebuje. Ransomware, který blokuje práci s počítačem, většinou vymění plochu počítače nebo úvodní obrazovku mobilního telefonu za svoji vlastní, na níž nelze nic spustit. Návrat do původního stavu slibuje opět po zaplacení určité částky. Nelze použít žádné klávesové zkratky ani ikonu start, nelze spustit ani správce úloh, tudíž proces nemůžeme nijak ukončit. Na displeji se objeví pouze zpráva, která říká, proč k blokování došlo a pokyny k zaplacení požadované částky. (Šulc, 2018; Antonucci, 2017)

2.3.5 Trojský kůň

Do zařízení se trojský kůň dostane buď společně s aplikací, nebo samotná aplikace provádí nějakou činnost, o které uživatel neví a nesouhlasí s ní. Útočníci většinou využívají toho, že si uživatelé chtějí nelegálně stáhnout nějakou aplikaci, za kterou se by museli za normálních okolností zaplatit. Škodlivý kód je tak součástí stahované aplikace. Trojský kůň se nedokáže šířit sám ani nakazit ostatní soubory.

Útočníci vkládají trojské koně i do aplikací a souborů, které vypadají věrohodně. Často si ho uživatel spustí ve svém zařízení i sám v domnění, že dělá dobrou věc. Trojský kůň odesílá útočníkovi data, stahuje a spouští jiný škodlivý software a podobně. Pro odstranění zranitelnosti se doporučuje pravidelně aktualizovat operační systémy a aplikace ve svých zařízení, ale například i router. (ESET, © 2023)

2.3.6 DDoS

DDoS (Distributed Denial of Service) je útok na webové stránky, který zamezí přístup na stránky ostatním uživatelům. K těmto útokům je využíváno velké množství infikovaných počítačů z celého světa, jedná se o tzv. botnet síť. Botnet jsme si podrobněji popsali výše. Útočník zašle přes počítače v botnet síti velmi velké množství příkazů, tím server webové stránky zahltí a zpomalí se nebo dokonce spadne. Tímto útokem pouze zamezí přístup uživatelům na stránku, ale neovládne ji. DDoS útoky se využívají k zastrašování nebo vydírání. Tyto útoky jsou v České republice považovány za trestný čin. (Kresa, 2018)

DDoS útoky se dělí na dva typy, volumetrické a aplikační. Volumetrické útoky se řadí mezi nejstarší typy těchto útoků. DDoS útoky mohou být vedeny na nadnárodní korporace nebo různé vládní organizace, respektive na jejich webové stránky a sítě, kdy jejich cílem je tyto systémy přetížit a shodit a ukázat tak, jakou mají sílu. Útoky můžeme zachytit i ze strany konkurence na různých e-shopech. Většinou se objevují v době, kdy jsou prodeje na svém vrcholu, například v období Vánoc. Cílem útočníka je omezit přístup na konkurenční webové stránky, protože pokud zákazník nenakoupí u konkurenčního e-shopu, s velkou pravděpodobností nakoupí na e-shopu útočníka. Pár hodin takového výpadku může způsobit ztrátu několik miliónů korun.

Dále se objevují útočníci, kteří ani nemají v plánu útočit, ale pouze vyhrožují a požadují zaplatit určitou částku ta to, že útočit nebudou. Předem informují vybranou firmu e-mailem, kde jim oznámí, že pokud nezaplatí danou částku, bude na ně proveden DDoS útok. Ani po zaplacení ale firma nemá jistotu, že útok neproběhne.

DDoS útoky mohou být zaznamenány na různé organizace v různých odvětvích, na každý z nich mohou mít jiný dopad. Útoky mohou být vedeny na:

- internetové vyhledávače,
- webové stránky bank,
- e-shopy,
- internetové bankovnictví,
- zpravodajské weby,
- portály telefonních operátorů.

Pokud služby nefungují pouze krátkodobě, nemusí to znamenat vždy ztrátu, uživatel ponechá danou činnost na později. Dlouhodobé několikadenní výpadky už ale mohou ohrozit i chod celé ekonomiky. (Šulc, 2018)

2.3.7 Spam

Spam je jedním z nejstarších kybernetických útoků. Jedná se o nevyžádanou poštu (nejčastěji reklamní sdělení), též můžeme označovat jako junk mail, od subjektu, kterému jsme nedali souhlas na zasílání takovéto pošty.

Nemusí se jednat pouze o nabídku zboží a služeb. Až 95 % rozesílané pošty je tvořeno spamem. Ve většině případů je však zachycen filtrem, který spam eliminuje. O takovém filtru nemusíme ani vědět. Kolik e-mailů nakonec dorazí do našich e-mailových schránek pak závisí na tom, jak je tento filtr nastavený. Antispamové filtry jsou schopné zachytit spam, který pochází z nedůvěryhodných či pochybných zdrojů nebo, pokud obsahuje určité slovní spojení, u kterého je pravděpodobné, že se může jednat o spam. (Sedlák a Konečný, 2021)

Za spam může být někdy vyhodnocena i zpráva či e-mail, který je naprosto bez závady nebo naopak filtry zprávu nevyhodnotí jako spam a ta je pak doručena do naší e-mailové schránky. Spam je škodlivý především tím, že zatěžuje přenosovou infrastrukturu, zbytečně zabírá místo ve schránce, efektivita práce příjemce je snížena z toho důvodu, že musí sám projít každý e-mail a vyhodnotit, zda se jedná o spam či ne. Z toho vyplývá i riziko, že příjemce může špatně vyhodnotit daný e-mail. Pokud uživatel e-mail obsahující spam otevře, jeho odesílatel se to dozví a tím zjistí, že je daná e-mailová adresa aktivní. Následně na ní může zasílat další nevyžádané e-maily.

Může se ale taky stát, že antispamový filtr či sám příjemce vyhodnotí zprávu jako nevyžádanou, a ta bude smazána i přesto, že měla být zpracována. Dále může uživatel nějakou důležitou zprávu přehlédnout mezi množstvím zpráv, co mu chodí do schránky. (Šulc, 2018)

2.3.8 Hoax

Posledním typem kybernetického útoku, který si popíšeme, je hoax. Hoax je stejně jako spam nevyžádaná hromadně šířená zpráva. Hoax pomáhají šířit ve většině případů jeho příjemci, kteří rozesílané zprávě uvěří a poslechnou pobídnutí k šíření zprávy dál. Šíří se pomocí e-mailů nebo sociálních sítích.

Nejčastějšími hoaxy jsou různá varování před neexistujícím virem či hrozbou, prosby o pomoc nebo různé zprávy štěstí. Odesílatel e-mailu pod známou autoritou (například Microsoft) ve zprávě oznamuje, že daná společnost vydala oznámení o nové zranitelnosti a k tomu jsou uvedena různá doporučení, jak se hrozbě bránit. V případě proseb o pomoc se snaží autor hrát na city a ve zprávě píše, že například nějaké dítě má rakovinu a za každé sdílení daná sociální síť zaplatí určitou částku rodině tohoto dítěte. U zpráv štěstí autor například píše, že pokud tuto zprávu příjemce odešle alespoň deseti lidem, bude mít štěstí, ale pokud to neudělá, stane se opak.

Tyto zprávy jsou škodlivé z toho důvodů, že můžou šířit paniku, obtěžují příjemce, zbytečně zatěžují přenosovou infrastrukturu nebo ten, kdo zprávy rozesílá, se může stát v očích ostatních méně důvěryhodným. Především ale dochází k prozrazování e-mailových adres přátel tím, jak se hoax šíří po celém internetu. Tyto adresy mohou být později využity k rozesílání další nevyžádané pošty. (Šulc, 2018)

2.4 Vývoj kybernetické bezpečnosti v České republice

Lidé jsou v dnešní době velmi závislí na využívání informačních technologiích a kyberprostoru. Tohoto faktu jsou si vědomy určité skupiny lidí, kteří této závislosti mohou zneužít a dost často také zneužívají. Tato skutečnost je jedním z hlavních důvodů, proč vznikla regulace kybernetické bezpečnosti, která stanovuje základní bezpečnostní pravidla v kyberprostoru. Dalším hlavním důvodem regulace je růst rizik a jejich dopadů v důsledku používání informačních technologií, rychlý vývoj těchto technologií, dále zvyšování četnosti kybernetických útoků nebo požadavky ze strany institucí, jako jsou NATO, Evropská unie nebo OSN. Kyberprostor přesahuje hranice států, proto je potřeba určit pravidla globálně. Dalším důvodem regulace je skutečnost, že pro investory je kybernetická bezpečnost dané země jedním z důležitých hodnotících faktorů a je jednou ze složek konkurenceschopnosti každé země. (Doucek, Konečný a Novák, 2019)

Stát v České republice začal poprvé systémově řešit kybernetickou bezpečnost v roce 2000, kdy byla Ministerstvem vnitra České republiky vydána „Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření“. Tato koncepce se hlavně věnuje problematice trestných činů v odvětví informačních technologií, ale můžeme vidět i náznak již zmíněného systémového řešení státu kybernetické trestné činnosti. (Kolouch a Bašta, 2019)

V roce 2004 byl usnesením vlády ČR schválen dokument „Státní informační a komunikační politika“. Tento dokument se věnoval oblastem jako jsou rozvoj trhu, dostupnost a bezpečnost elektronických komunikací, informační gramotnost, dále veřejným online službám, jakou jsou e-government, e-procurement nebo e-zdravotnictví, a v neposlední řadě se také věnoval oblasti rychlého vývoje prostředí pro elektronický obchod. (Vláda ČR, 2004)

V roce 2005 vznikla „Národní strategie informační bezpečnosti ČR“, která navazovala na novelu výše uvedené „Státní informační a komunikační politiky“. Gestorem Národní strategie bylo nejdříve již neexistující Ministerstvo informatiky, poté výkon jeho činností převzalo Ministerstvo vnitra, Ministerstvo pro místní rozvoj a Ministerstvo průmyslu a obchodu. V této strategii bylo stanoveno šest cílů. Mezi cíle bylo zařazeno například zlepšení znalostí v oblasti informační bezpečnosti, zlepšení řízení rizik a informační bezpečnosti, dále podpora konkurenceschopnosti národní ekonomiky a ochrany lidských práv a svobod.

„Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření“ vydaná v roce 2000, byla o osm let později, tedy v roce 2008, nahrazena dokumentem „Koncepce boje proti organizovanému zločinu“, která se již více věnovala problematice kybernetických hrozeb a trestné činnosti.

V roce 2011 stanovila vláda ČR gestorem kybernetické bezpečnosti Národní bezpečnostní úřad. Zároveň také vytvořila Radu pro kybernetickou bezpečnost. (Kolouch a Bašta, 2019)

Rada pro kybernetickou bezpečnost (RKB) je poradním a koordinačním orgánem předsedy vlády v problematice kybernetické bezpečnosti. Cílem tohoto orgánu je také podpora funkce gestora kybernetické bezpečnosti (dříve jím byl Národní bezpečnostní úřad, nyní Národní úřad pro kybernetickou a informační bezpečnost), která vyžaduje spolupráci subjektů kritické infrastruktury státu a státních institucí. Rada je složena z předsedy, místopředsedy, tajemníka a členů rady. Funkci předsedy zastává předseda vlády a funkci místopředsedy plní ředitel NÚKIB (dříve NBÚ). Tajemník je jmenovaný předsedou a jeho funkci vykonává pracovník NÚKIB (dříve NBÚ). Členové jsou delegováni státními institucemi. Členy rady pro kybernetickou bezpečnost mohou především být zástupci ministerstev, zpravodajských služeb a dalších ústředních správních úřadů, jako je například Úřad pro ochranu osobních údajů nebo Český telekomunikační úřad. Povinností RKB je zasedat minimálně jednou ročně. Pokud to situace vyžaduje, může rada přizvat na své zasedání zástupce subjektů kritické infrastruktury nebo další odborné externí subjekty. Rada pro kybernetickou bezpečnost musí například především koordinovat činnost různých státních institucí a dále jejich plnění závazků v oblasti

kyberbezpečnosti, kontrolovat členy rady a jejich plnění závěrů z jednání RKB nebo předkládat odborná doporučení vládě vyplývající z řešení aktuálních problémů v oblasti kybernetické bezpečnosti. Rada pro kybernetickou bezpečnost by měla také spolupracovat s externími subjekty a využívat ke své práci jejich doporučení, aby byla v České republice zajištěna co nejlepší kybernetická bezpečnost.

V roce 2011 NBÚ začal také připravovat věcný záměr zákona o kybernetické bezpečnosti. V roce 2012 byl tento věcný záměr zákona vládou schválen. Národní bezpečnostní úřad předložil v roce 2013 návrh tohoto zákona vládě ČR, kdy schvalování proběhlo bez větších připomínek. Proto zákon č. 181/2014 Sb., o kybernetické bezpečnosti vstoupil v platnost v srpnu 2014 a účinný byl od začátku roku 2015. Současně s tímto zákonem nabyly účinnosti i některé prováděcí předpisy, příkladem může být Vyhláška o kybernetické bezpečnosti. (Doucek, Konečný a Novák, 2019)

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů nabyl účinnosti tedy 1. ledna roku 2015. Od této doby byl zákon několikrát novelizován, z toho dvakrát významně. První významnější novela, která byla účinná od července roku 2017, zařadila do okruhu povinných osob tohoto zákona také provozovatele informačních systémů. Touto novelou byly také pozměněny některé sankce, u kterých došlo zejména k významnému navýšení horních hranic pro udělení těchto sankcí. Druhá významná novela, která nabyla účinnosti v srpnu roku 2017, zapříčinila mimo jiné vznik nového úřadu, a tím byl Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). NÚKIB si podrobněji popíšeme v textu níže. Dále byly v rámci novely zapracovány do zákona zkušenosti pracovníků NÚKIB, které získávali v průběhu své praxe. Před tím, než vznikl zákon o kybernetické bezpečnosti, byla v České republice kybernetická bezpečnost řešena a zajišťována pomocí soukromých osob bez jakékoliv specifické regulace.

Vznik zákona byl do značné míry podpořen požadavky kladenými mezinárodními společenstvími a také závazky, které má ČR vůči Evropské unii a Severoatlantické alianci (NATO). Dalším důvodem vzniku byly také DDoS útoky. Tento typ útoku, který jsme si popsali podrobněji výše, cílí zejména na servery bankovních a finančních institucí, ke kterým patří například i Česká národní banka a Burza cenných papírů Praha. Dále mohou zaútočit i na stránky mobilních operátorů. V České republice jsme se mohli s DDoS útoky setkat především na začátku roku 2013.

Cílem vytvoření zákona o kybernetické bezpečnosti byla tvorba zákonného postavení státní instituce, která by zodpovídala za zabezpečování kybernetické bezpečnosti a měla pravomoc regulovat určité subjekty. Zákon definuje povinné subjekty, které podléhají jeho regulaci, a dále jim ukládá určité povinnosti, které musí tyto subjekty dodržovat. (Kolouch a Bašta, 2019; Doucek, Konečný a Novák, 2019)

K lednu 2023 je momentálně nejaktuálnější znění zákona o kybernetické bezpečnosti s účinností od 6. srpna 2022.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je od roku 2017 ústředním správním orgánem zákona o kybernetické bezpečnosti a celkově kybernetické bezpečnosti v České republice. NÚKIB vznikl 1. srpna 2017. Tento úřad převzal agendu po Národním bezpečnostním úřadu, který byl původně ústředním správním orgánem kybernetické bezpečnosti. Převzal agendu včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a dále také včetně kryptografické ochrany. Mimo těchto činností je NÚKIB také správním orgánem pro oblast veřejně regulované služby evropského navigačního družicového systému Galileo. Práva a povinnosti tohoto úřadu jsou definovány v zákoně o kybernetické bezpečnosti. Pokuty za neplnění či porušení práv a povinností vyplývajících ze zákona o kybernetické bezpečnosti vybírá a přestupky projednává NÚKIB.

Národní úřad pro kybernetickou a informační bezpečnost má sídlo v Brně, má ale také další pracoviště, které se nachází v Praze. V současné době je od 1. července 2022 ředitelem NÚKIB Ing. Lukáš Kintr. Ředitel NÚKIB také pravidelně chodí na jednání Bezpečnostní rady státu a zároveň je členem Výboru pro kybernetickou bezpečnost, což je pracovní orgán Bezpečnostní rady státu. Ředitele jmenuje a odvolává vláda ČR po projednání ve Výboru Poslanecké sněmovny. Ředitel se zodpovídá předsedovi vlády nebo jinému členovi vlády, který byl touto činností pověřen.

Činnost NÚKIB je kontrolována Poslaneckou sněmovnou. Ta pro tuto kontrolu vytváří zvláštní kontrolní orgán. Kontrolní orgán musí mít minimálně sedm členů, přičemž počet musí být vždy lichý. Členy kontrolního orgánu se mohou stát jen poslanci Poslanecké sněmovny. (NÚKIB, 2023; Zákon č. 181/2014 Sb.)

Současně s novelizací zákona byla také NÚKIB vytvořena a vládou ČR schválena „Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020“. Tento dokument je nástrojem k zabezpečení kybernetické bezpečnosti ČR pomocí rychlé a účinné reakce na všechny aktuální, ale i budoucí kybernetické hrozby, které se v čase neustále mění,

protože kyberprostor se velice rychle vyvíjí. Tato strategie má úlohu základního dokumentu k tvorbě dalších souvisejících právních předpisů, standardů či směrnic v oblasti zabezpečení kyberprostoru.

Následně byla NÚKIB vydána „**Národní strategie kybernetické bezpečnosti České republiky na období let 2021 až 2025**“, která je momentálně aktuální. S novou strategií přišly také tři nové vize – Sebevědomě v kyberprostoru, Silná a spolehlivá spojenectví a Odolná společnost 4.0. V rámci první vize je důležitou složkou zabezpečování kybernetické bezpečnosti v České republice. Objevuje se nový pojem atribuce. Atribuci můžeme vysvětlovat jako připisování škodlivých činností v kyberprostoru k činnostem dané země nebo k činnostem, které jsou nezávislé na státních strukturách. Druhá vize je zaměřena na aktivní roli státu při navazování mezinárodních spoluprací a z toho vyplývající růst společné obranyschopnosti a bezpečnosti. Ve třetí vizi bylo definováno pár nových pojmů – odolná společnost 4.0, digitální hygiena a odolný systém zajištění kybernetické bezpečnosti. Odolná společnost 4.0 představuje společnost, která plně využívá nejrůznější moderní technologie, ale zároveň je dokáže do svého života implementovat tak, aby kybernetická rizika z nich vyplývající byla co nejmenší. Digitální hygiena znamená zásady, přístup či návyky uživatelů, díky kterým je jejich pohyb v digitálním světě bezpečnější (například proaktivní přístup k zabezpečení). Odolný systém zajištění kybernetické bezpečnosti představuje soubor kvalitního a moderního vzdělávání všech obyvatel, čímž se zvyšuje informační gramotnost a odolnost lidí, kteří jsou vystaveni negativním vlivům digitálních technologií. (NÚKIB, 2021; Sedlák a Konečný, 2021)

Obrázek 2: Odolný systém zajištění kybernetické bezpečnosti

Zdroj: NÚKIB, 2021

Současně s Národní strategií kybernetické bezpečnosti je vydáván také „Akční plán k Národní strategii kybernetické bezpečnosti“. Ke kladnému dosažení cílů stanovených Národní strategií kybernetické bezpečnosti je potřebné plnit jednotlivé úkoly, které jsou vypsané v Akčním plánu. (Sedlák a Konečný, 2021)

Z výše popsaného vývoje legislativy můžeme říct, že se stát snaží zajistit co největší kybernetickou bezpečnost a dále také zvyšovat obecné povědomí o této bezpečnosti či různých kybernetických útocích.

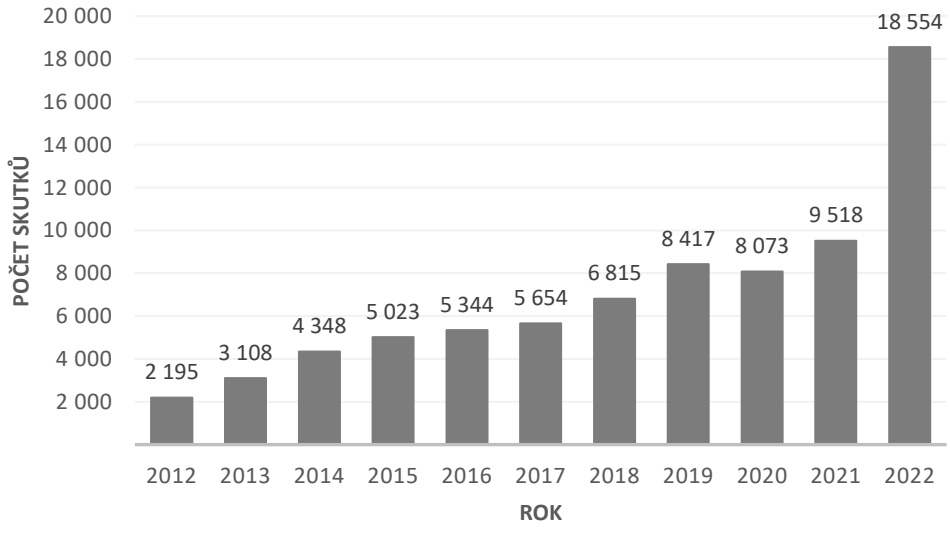
3 POJIŠTĚNÍ KYBERNETICKÝCH RIZIK NA ČESKÉM POJISTNÉM TRUHU

V této kapitole se budeme věnovat jednotlivým pojistným produktům nabízeným na českém pojistném trhu, u kterých si detailněji popíšeme jejich pojistné podmínky, na co se dané pojištění vztahuje a naopak, jaké jsou jeho výluky. Nejprve si uvedeme příklad pojištění kybernetických rizik pro nepodnikatelské subjekty a následně se budeme věnovat produktům pro podnikatelské subjekty a firmy. Z pojistných produktů pro podnikatele se budeme zabývat produkty od ČSOB Pojišťovny, Maxima pojišťovny, pojišťovny Colonnade Insurance S.A. a Chubb. U každého produktu budou detailněji rozebrány jeho pojistné podmínky. V další části této kapitoly budou pojistné podmínky jednotlivých produktů porovnány.

S vývojem informačních a komunikačních technologií se zvyšuje i počet kybernetických rizik, která mohou nastat. Zaměstnanci firem stále více využívají možnost práce z domova tzv. homeoffice, pokud jim to jejich zaměstnavatel umožňuje. To může vést k například k úniku citlivých dat, protože uživatelé mohou být připojeni k internetu odkudkoliv i k nezabezpečeným sítím. Dále k růstu kybernetických rizik přispěla také nedávná pandemie Covid-19, při které ještě více lidí začalo pracovat z domova.

Na grafu číslo 1 můžeme vidět vývoj kybernetické kriminality v posledních deseti letech. Z grafu je zřejmé, že počet skutků kybernetické kriminality meziročně dlouhodobě roste. V roce 2022 se dokonce tento počet skoro dvojnásobně zvýšil oproti roku 2021.

Graf 1: Vývoj kybernetické kriminality v letech 2012 - 2022



Zdroj: vlastní zpracování na základě dat z Policie ČR, © 2023

V roce 2022 představoval počet skutků kybernetické kriminality 10,2 % z celkového počtu registrované kriminality. Dvojnásobně narostla oproti předešlému roku kybernetická kriminalita v Karlovarském kraji, kde byl nárůst téměř o 218 %. Velký nárůst této kriminality byl zaznamenán také ve Středočeském, Pardubickém, Moravskoslezském nebo Královéhradeckém kraji a dále také v hlavním městě Praha. Například od srpna roku 2022 se stále častěji začaly objevovat podvodné SMS zprávy, které vypadaly, že jsou zasílány Ministerstvem práce a sociálních věcí. Cílem útočníka bylo zjistit od napadeného přístupové údaje do jeho bankovnictví, které měl poté v plánu zneužít. (Moravčík, 2023)

Řešením, jak zmírnit kybernetická rizika (respektive snížit jejich dopady), je využití pojistných produktů nabízených na pojistném trhu. Pojištěním přeneseme finanční dopady na danou pojišťovací instituci, a tak nám alespoň z části tato instituce pomůže s řešením případných nahodilých událostí.

Pojištění kybernetických rizik je oblast pojišťovnictví, která v posledních letech zaznamenává velký rozvoj. Na českém pojistném trhu je pojišťovacími institucemi nabízeno pojištění kybernetických rizik pro nepodnikající osoby, ale i pro osoby podnikající a firmy. Pojištění pro podnikající osoby v tuto chvíli nenabízí mnoho pojišťovacích institucí, z větších a známějších pojišťoven je pojištění nabízeno například ČSOB Pojišťovnou. Naopak pojištění pro nepodnikající osoby nabízí daleko více institucí. Nabízí je například AXA, ČSOB Pojišťovna nebo UNIQA.

3.1 Pojistné produkty pro nepodnikatelské subjekty

Jako příklad pojistných produktů pro nepodnikatelské osoby si popíšeme produkt od ČSOB Pojišťovny. ČSOB Pojišťovna nabízí produkt, který se nazývá **Pojištění internetových rizik**. Produkt poskytuje pojištění právní ochrany a finančních ztrát, které mohou nastat při využívání internetu nebo při provádění bezhotovostního platebního styku. V rámci tohoto pojištění je také poskytována asistenční služba.

Pomoc v rámci Pojištění internetových rizik je poskytována v následujících případech:

- identita pojištěného na internetu je zneužita,
- pojištěný nakupuje zboží či služby přes internet,
- platební karta či jiné platební prostředky jsou zneužity nebo neoprávněně použity,
- pověst pojištěného je na internetu či sociálních sítích poškozena.

V případě, že je identita pojištěného na internetu zneužita, je v rámci pojištění poskytnuta právní ochrana a finanční náhrada. Vztahuje se na protiprávní jednání třetí osoby, která neoprávněně použila identifikační nebo autorizační údaje pojištěného v rámci internetu, a tím podvodník pojištěnému způsobil určitou finanční škodu. Finanční škodou se myslí škoda, která pojištěnému vznikla neoprávněným odčerpáním peněžních prostředků z jeho bankovního účtu třetí osobou nebo pokud pojištěnému vznikl dluh vlivem činnosti třetí osoby. Za identifikační údaje se považuje především telefonní číslo, adresa, rodné číslo, číslo občanského a řidičského průkazu či cestovního pasu. Mezi autorizační údaje v rámci tohoto pojištění patří přihlašovací údaje, jako jsou uživatelská jména a hesla, dále e-mail, čísla bankovních účtů a platebních karet nebo IP adresy.

Pojišťovna zprostředkuje pojištěnému právní ochranu v případě pojistné události při uplatňování práv, která vedou k navrácení neoprávněně odčerpaných peněžních prostředků nebo zproštění jeho neoprávněných dluhů. Pokud pojištěný do tří měsíců od doby doručení podkladů k řešení této pojistné události pojišťovně neuspěje ani s pomocí asistenčních služeb nabízených v rámci tohoto pojištění při uplatňování jeho práv a není mu vyplacena náhrada škody, má oprávněná osoba nárok na vyplacení pojistného plnění ve výši způsobené finanční škody, nejvýše však do 250 000 Kč na jednu pojistnou událost.

V případě nakupování zboží přes internet se pojištění vztahuje na nedodání či částečné dodání movité věci, která byla zakoupena pomocí internetu u provozovatele nějakého e-shopu. Pojištění se týká zboží, které pojištěný koupil jako nové, jehož kupní cena byla v rozmezí od 650 Kč do 50 000 Kč a tato kupní cena byla včas a řádně zaplacena. Pojistné plnění může být vyplaceno pouze v případech, kdy zboží nebylo doručeno nebo bylo doručeno poškozené, nějaká část nákupu chyběla, či bylo dodáno jiné zboží. Dále se pojistné plnění vztahuje na zboží, jehož doba dodání byla opožděna o více než pět dní (v případě e-shopu se sídlem v EU), nebo o více než deset dní (v případě e-shopu se sídlem mimo EU), než bylo sjednáno v kupní smlouvě. Pojistné plnění je také vyplaceno v případě, že zboží nebylo dodáno vůbec.

Pojištění se dále vztahuje na finanční ztráty, které vznikly pojištěnému v důsledku objednání či poskytnutí služeb přes internet, které už byly částečně či úplně uhrazeny nebo pouze objednány. Mezi tyto služby patří například vlakové a autobusové jízdenky, letenky, nákup zájezdů, dálniční a poštovní známky, dárkové poukazy, kolky nebo vstupenky na různé kulturní akce. Kupní cena služby musí být opět v rozmezí od 650 Kč do 50 000 Kč. Právo na pojistné plnění

má pojištěný u služeb, které nebyly poskytnuty nebo byly poskytnuty v rozporu se sjednanou smlouvou s provozovatelem e-shopu.

Výlukou z pojištění je nákup zboží podléhající rychlé zkáze, nákup rostlin či zvířat, nelegální zboží a služby, zbraně, služby zakoupené na různých slevových portálech nebo nákup cenných papírů s výjimkou již uvedených poštovních a dálničních známek a kolků. Pojištění se dále nevztahuje na zboží, které bylo zabráno celní správou či jiným orgánem veřejné správy.

Pokud nastane pojistná událost, pojistitel poskytne pojištěnému právní ochranu na uplatnění práv z vadného plnění prostřednictvím odborné pomoci při reklamačním řízení. Pokud se pojištěnému nepodaří uspět v reklamačním řízení ani s pomocí asistenční služby nebo právní ochrany do tří měsíců od doby doručení veškerých podkladů k řešení pojistiteli, bude pojištěnému poskytnuta finanční náhrada. Pojistné plnění bude vyplaceno ve výši kupní ceny zboží či služeb sjednané v kupní smlouvě mezi pojištěným a internetových obchodem, nejvýše však do částky 50 000 Kč na jednu pojistnou událost.

Pojištění neoprávněného použití platební karty se týká poskytnutí právní ochrany a náhrady vzniklé škody v případě neoprávněného použití platební karty. Za platební karty se považují všechny elektronické platební prostředky, které vlastní pojištěný. Pojištění se vztahuje na neoprávněné výběry z bankomatů a neoprávněné provedení platby debetní či kreditní kartou třetí osobou. Právní ochrana je v případě pojistné události poskytnuta s cílem navrácení neoprávněně použitých peněžních prostředků zpět pojištěnému. Dále má oprávněná osoba nárok na náhradu škody ve výši jeho finanční ztráty, ale nejvýše mu bude poskytnuto 50 000 Kč na jednu pojistnou událost.

Toto pojištění se vztahuje také na poškození pověsti na internetu. Jedná se především o pomluvy, urážky nebo neoprávněné zveřejnění soukromých informací. Pomluva je nepravdivé vyjádření nějaké skutečnosti o pojištěném, která mu může vážně poškodit vztahy s lidmi, zejména pak s rodinnými příslušníky, nebo způsobit další újmu. Urážkou se rozumí jakýkoliv urážlivý výrok vůči pojištěnému, hanlivý či vulgární výraz, eventuálně jiný slovní nebo nonverbální projev vztahující se k pojištěnému, které mu sníží důstojnost nebo poškodí pověst na internetu. Neoprávněným zveřejněním soukromých informací je myšleno sdělení rasového původu, politických či náboženských postojů, zdravotního stavu a podobně.

Pojištěnému je poskytnuta právní ochrana při uplatňování jeho práv proti osobě, která mu způsobila újmu, ale také proti provozovateli internetových stránek, kde byla informace zveřejněna. Je to z důvodu zjištění zdroje, odkud pochází informace, která poškodila

pojištěnému pověst, dále aby byla negativní informace z internetu či sociálních sítí odstraněna a byla pojištěnému poskytnuta omluva, případně poskytnuta finanční náhrada za způsobenou újmu. V rámci pojištění se bude asistenční služba prostřednictvím odborné pomoci co nejvíce snažit, aby byla negativní informace z internetu vymazána nebo alespoň aby nebylo jednoduché se k této informaci dostat, a to až do výše limitu 50 000 Kč na jednu pojistnou událost.

Výlukami z pojištění jsou případy, kdy si pojištěný svoji pověst poškodí sám, dále pokud je pověst poškozena jinde než na internetu či sociálních sítích. Pojištění se také nevztahuje na poškození pověsti zpravodajskými médii, jako je televizní či rozhlasové vysílání atd., nebo pokud pojištěný na internetu nevystupuje pod svým vlastním jménem, ale pod pseudonymem nebo anonymně.

ČSOB Pojišťovna nabízí toto pojištění ve dvou variantách, „Single“ nebo „Family“. Varianta Single se týká pouze pojištěného, který je v pojistné smlouvě jmenovitě napsaný. Varianta Family se týká jak pojištěného jmenovitě napsaného ve smlouvě, tak i jeho rodinných příslušníků, kteří s ním žijí ve společné domácnosti v době nastání nahodilé události. Pojištění je platné na území celého světa.

Pokud pojištěný již při sjednávání pojištění věděl nebo s přihlédnutím na jeho aktuální situaci mohl vědět o událostech, které by mohly vést ke vzniku nahodilé události kryté tímto pojištěním, žádné z výše uvedených pojištění se na takového události nevztahuje. Dále pojištění nelze uplatnit na neshody mezi pojištěnými osobami, neshody mezi pojištěným a pojistníkem nebo neshody mezi pojištěným a jeho blízkými. Pojištění se také netýká pojistných událostí, u kterých pojištěný úmyslně uvede lživé podstatné informace nebo jejich část zatají nebo je úmyslně způsobil sám pojištěný. Další případné výluky byly uvedeny u jednotlivých částí tohoto pojištění. (ČSOB Pojišťovna, 2022a)

Pojištění internetových rizik je sjednáváno na dobu neurčitou, přičemž pojistné období je určeno na jeden rok. Výše pojistného je závislá na sjednaném rozsahu pojištění a spoluúčasti. Pojištění může být zrušeno do dvou měsíců od podepsání pojistné smlouvy s osmidenní výpovědní lhůtou, do tří měsíců po vzniku pojistné události, kdy výpovědní lhůta je jeden měsíc, nebo lze také pojištění ukončit na konci pojistného období. (ČSOB Pojišťovna, 2022b)

Roční pojistné u varianty Single je k únoru 2023 ve výši 900 Kč, při sjednání online je poskytována sleva 20 %, tudíž je roční pojistné po slevě ve výši 720 Kč. Za variantu Family pojištěný zaplatí roční pojistné ve výši 1 180 Kč, při sjednání online je pojistné za rok ve výši 950 Kč. (ČSOB Pojišťovna, © 2023)

3.2 Pojistné produkty pro podnikatelské subjekty

Pro podnikatelské osoby nabízí pojištění kybernetických rizik na českém pojistném trhu celkem čtyři pojišťovny, ČSOB Pojišťovna, Maxima pojišťovna, Colonnade Insurance S.A. a Chubb.

3.2.1 ČSOB Pojišťovna

Prvním pojistným produktem, kterému se budeme věnovat, je Pojištění kybernetických rizik od ČSOB Pojišťovny. Pojištěním je kryta majetková škoda na datech podnikatele a odpovědnost za škodu, dále jsou v rámci pojištění poskytovány asistenční služby, pokud tak bylo ujednáno ve smlouvě.

Pojištění majetkové škody na datech je určeno pro situace, kdy pojištěný utrpí finanční ztrátu tvořenou náklady, které vznikly v důsledku skutečného nebo domnělého úniku dat pojištěného v důsledku kybernetické události. Do těchto nákladů se započítávají náklady na práce odborné osoby, která kybernetické události vyšetřuje, na přesčasy pracovníků příslušného oddělení krizového managementu pojištěného po dobu třiceti dnů od nahlášení kybernetického incidentu pojišťovně, na právní obhajobu před soudem, která bude potřeba v důsledku podání žaloby na pojištěného příslušným státním orgánem a na odborné služby zaměřené na budování dobrého jména a vztahy s veřejností po dané kybernetické události po dobu ochranné lhůty dobrého jména podniku. Dále do těchto nákladů mohou být zahrnuty výdaje na kontrolování neoprávněného využívání především různých věrnostních či přístupových karet a dalších situací po nastání dané pojistné události nebo náklady na splnění právních předpisů o ochraně dat a ochraně osobních údajů. Pojišťovna dále poskytne i peněžní náhradu za uvalené sankce a pokuty příslušnými orgány, související s porušením dat a osobních údajů v důsledku kybernetického incidentu krytého tímto pojištěním. (ČSOB Pojišťovna, 2018)

Pojištění majetkové škody se dále vztahuje na peněžní ztráty související s obnovou softwaru a ztracených dat podniku v důsledku kybernetické události, a to do stavu, ve kterém se nacházel těsně před nastáním nahodilé situace. Pojištění se také vztahuje na náhradu ušlého zisku a fixních nákladů podniku v době omezení nebo přerušení jeho činnosti v důsledku kybernetického incidentu. Pojištění majetkové škody lze zjednat i na finanční ztrátu ve formě výkupného, které útočník po podniku požadoval a ten jej zaplatil, a další nutné náklady k vyřešení tohoto finančního vydírání. Dále pojistitel pojištěnému nahradí veškeré finanční prostředky, které mu byly zcizeny v důsledku kybernetického útoku. V neposlední řadě se také pojištění vztahuje na pokuty a sankce, které na podnik uvalí poskytovatel platebních karet kvůli

porušení standardů PCI DSS, což bylo důsledkem kybernetického útoku. Tyto pokuty a sankce pojistitel pojištěnému uhradí spolu s dalšími souvisejícími nutnými náklady, jako jsou například forenzní vyšetřovatel, opětovná certifikace nebo opakované vystavení platebních karet. PCI DSS je soubor bezpečnostních pravidel, která mají zamezit zneužití dat o platebních kartách. Tato pravidla platí po celém světě a jsou určena pro organizace, která shromažďují data o držitelích platebních karet nebo zprostředkovávají platební transakce prostřednictvím těchto platebních karet. (ČSOB Pojišťovna, 2018; SBK, © 2023)

V pojistných podmínkách je dále uvedeno velké množství výluk, na které se pojištění majetkové škody nevztahuje. Vyloučeny z pojištění jsou například situace, kdy si podnik způsobí úmyslně škodu sám nebo je škoda způsobená kvůli vědomé nedbalosti či trestným činem samotného pojistníka, pojištěného a jejich blízkých osob. Ani škody způsobné v rozporu s právními předpisy, osobou bez požadované kvalifikace, pod vlivem návykových a dalších psychotropních látek nelze do tohoto pojištění zahrnout. Pokud je v zemi vyhlášen válečný či jiný mimořádný stav, nebo pokud je v zemi revoluce, občanská válka, demonstrace či zásahy státních orgánů i bez vyhlášení válečného a jiného mimořádného vztahu, a v důsledku toho vznikne kybernetická událost, pojišťovna neuhradí s tím vzniklé náklady. Do výluk se zahrnují i náklady vzniklé v důsledku nařízení vlády. Z pojištění jsou vyloučeny také škody vzniklé nebezpečnými a škodlivými látkami, užíváním věci nekompetentní osobou a dále škody, které byly způsobeny ve spojitosti s nějakým teroristickým útokem. Výlukou z pojištění jsou dále škody, které vzniknou v důsledku výpadků či omezení telekomunikačních či internetových služeb nebo výpadků elektřiny, vody a plynu. Pokud podnik používá nelicencovaný software, poruší pravidla hospodářské nebo veřejné soutěže, poruší autorský zákon, nemůže po pojišťovně požadovat finanční náhradu. Zároveň není poskytnuto pojistné plnění ani v případě škody v důsledku odcizení či poškození hmotného majetku, škody při poskytování cloudových úložišť pojištěným, nebo pokud podniku vznikne škoda zapříčiněná kybernetickým útokem na počítačové softwary, které jsou využívány pro řízení dopravních prostředků. V neposlední řadě se pojištění nevztahuje na náhradu nákladů na obnovení dat, pokud pojištěný neprovádí zálohování svých dat minimálně jednou za týden, což je jednou z povinností pojištěného uvedených níže v textu. Dále také pokud ztracená data nepůjdou obnovit kvůli tomu, že již před uzavřením pojistné smlouvy pojištěný svoje data dostatečně nezálohoval.

Pojistnou událostí je okamžik, kdy byla škoda krytá tímto pojištěním odhalena. Aby bylo vyplaceno pojistné plnění, musí se příčina vzniku pojistné události vytvořit během trvání

pojištění a škoda musí být nahlášena pojišťovně nejpozději třicet dní po ukončení pojištění, zároveň musí být daná škoda odhalena v době trvání pojištění.

Pojištění odpovědnosti za škodu se týká situací, kdy je pojištěnému zákonem stanovena náhrada škody za újmu třetí osobě způsobenou porušením ochrany dat. Náhrada nákladů na obhajobu právním zástupcem v případě porušení ochrany důvěrných informací se také může sjednávat v rámci pojištění. Dále může být ve smlouvě ujednána náhrada škod způsobených kybernetickým útokem prostřednictvím počítačových systémů pojištěného třetí straně na jeho počítačových systémech (ztráta nebo poškození dat, DDoS útoky). Mohou být hrazeny i náklady na obhajobu pojištěného, pokud se tak pojistitel a pojištěný dohodnou. Ve smlouvě můžou být dále ujednány náhrady nároků třetí strany z důvodu zákonné odpovědnosti jako jsou například pomluvy, porušení autorského zákona, poškození dobrého jména, obchodní značky, nerespektování ochrany soukromí, které mohou vzniknout při činnosti pojištěného v rámci internetových médií. Náklady na právního zástupce mohou být opět se souhlasem hrazeny.

Z pojištění je vyloučena jakákoliv odpovědnost za škodu, která vznikla v souvislosti s protiprávní činností, bez potřebné kvalifikace či oprávnění nebo po požití návykových a jiných psychotropních látek. Odpovědnost za škodu v rámci tohoto pojištění se nevztahuje na odpovědnost, kterou na sebe pojištěný převzal nad rámec zákona. Většina výluk z pojištění odpovědnosti vyjmenovaných v pojistných podmínkách je stejná nebo alespoň podobná jako u pojištění majetkové škody popsané výše. Výlukou z pojištění je dále odpovědnost za škodu, kterou pojištěný či pojistník způsobí své blízké osobě, osobě, která s ním žije ve společné domácnosti nebo právnické osobě, ve které má on nebo i jeho osoba blízká nějaký podíl nebo je jejím orgánem. Pojištění se také nevztahuje na škody, které pojištěný způsobil své mateřské společnosti, která má nad ním dohled nebo jeho dceřiné společnosti a dále dceřiné společnosti této dceřiné společnosti.

Za vznik pojistné události odpovědnosti za škodu se považuje okamžik vzniku újmy třetí osobě. Pojistné plnění může být vyplaceno pouze v případě, kdy k oznámení události došlo nejpozději třicátý den po ukončení pojištění, ale škoda a její příčina a uplatnění práva na náhradu škody třetí osobou, které byla způsobena újma, proběhlo v době platnosti pojištění. Územní rozsah pojištění je v rámci celého světa mimo státy, kterým byly uloženy sankce od Organizace spojených národů nebo země, na které se rozhodla Organizace spojených národů, vláda ČR nebo Evropská unie uvalit embargo. Embargo může být na tyto země uvaleno před, ale i v průběhu uzavřeného pojištění.

Pojištěný je mimo jiné povinen provádět zálohování svých dat alespoň jednou týdně, mít nainstalovaný aktuální profesionální antivirový software, který ho ochrání před malware a pravidelně se chránit před kybernetickými útoky například změnou hesel a podobně, jinak mu nemusí být vyplaceno pojistné plnění.

Pojištěnému jsou poskytnuty také asistenční služby v podobě IT asistence, pokud se pojištěný a pojistitel dohodnou v pojistné smlouvě. IT asistence pomůže pojištěnému vyřešit problém v případě, že mu nefunguje hardware či software v jeho zařízení. Toto zařízení musí pojištěný provozovat oprávněně. Konzultace s IT odborníkem uvedeným v pojistné smlouvě je možná pouze, pokud nefunkčnost zařízení uživateli brání v jeho používání, zároveň vznikla na území České republiky a pojištěný se obrací na IT asistenci v době platnosti sjednaného pojištění. IT konzultace je zajišťována prostřednictvím telefonické komunikace s IT odborníkem nebo pomocí vzdáleného připojení do zařízení pojištěného. Pokud problém technik nevyřeší, informuje pojištěného o možnostech servisů v jeho okolí. IT konzultace jsou poskytovány celkem třikrát ročně v délce 180 minut na jednu konzultaci. Výlukou z asistenčních služeb je poskytnutí náhrady výdajů na opravu zařízení. (ČSOB Pojišťovna, 2018)

3.2.2 Maxima pojišťovna

Druhou pojišťovnou, která poskytuje pojištění na kybernetická rizika, je Maxima pojišťovna. Maxima pojišťovna poskytuje produkt s názvem Pojištění kybernetických rizik a odpovědnosti za data. Toto pojištění je vhodné pro firmy, které mají obrat v celkové výši do 500 milionů korun. Pojištění kryje škody, jakou jsou ušlý zisk nebo fixní náklady, které vzniknou z důvodu pozastavení či omezení provozu podniku způsobené kybernetickou událostí, náklady spojené s odpovědností za data a zabezpečením sítě (obnovení dat, právní zástupce, kybernetické vydírání, náklady na obnovení dobrého jména a vztahů s veřejností nebo náklady spojené s vyšetřováním příčiny škod). Předmětem pojištění jsou dále náhrady škod, které vznikly v souvislosti se sankcemi a pokutami a dalšími výdaji vyplývajícími ze zákona (například při porušení standardů PCI DSS v souvislosti s platebními kartami nebo při porušení právních předpisů) uloženými z důvodu odpovědnosti za data. Pojištěný si volí limity pojistného plnění podle svého uvážení, nejvýše může zvolit limit 40 milionů korun. (Maxima pojišťovna, © 2023a; Maxima pojišťovna, © 2023b)

V pojistných podmínkách jsou dále uvedeny výluky z pojištění. Pojem pojištěný v těchto pojistných podmínkách znamená pojištěného, pojistníka a jeho dceřinou společnost, která musí být uvedena v pojistné smlouvě. Pojištění se nevztahuje na škody, jejichž příčina byla

pojištěnému známa již před uzavřením smlouvy nebo mohl tuto příčinu předpovídat a na škody, které byly spáchány úmyslně nebo protizákonně samotným pojištěným, pojistníkem nebo osobou spojenou s danou poškozenou společností (společník, statutární orgán, atd.), nebo dále ze strany poskytovatele cloudových uložišť a dalších služeb. Škody, které vzniknou v důsledku válečného konfliktu, revoluce, teroristického útoku, občanské války nebo zásahem státních orgánů, nejsou předmětem tohoto pojištění. Dále se pojištění nevztahuje na újmu, která byla způsobena výpadkem elektrické energie, telekomunikačních a internetových sítí a dalších podobných služeb. Ani u škod vzniklých z důvodu platební neschopnosti pojištěného nebo jiné osoby a škod vzniklých ve spojení s neoprávněnou činností provozovanou pojistitelem nevzniká nárok na pojistné plnění. Vyloučeny jsou dále škody a náklady, které vyplývají z vylepšování a upgradování nějaké aplikace či systému pojištěného podniku nebo škody vzniklé v souvislosti s připojení k nezabezpečené síti. Škody způsobené vlivem působení azbestu, radioaktivními, jedovatými nebo výbušnými látkami, jaderným odpadem a únikem znečišťujících látek do tohoto pojištění nejsou zahrnuty. Mezi výluky z pojištění patří také škody způsobené elektromagnetickým zářením nebo živelní událostí a přírodními vlivy, jako jsou například silný vítr, zemětřesení, požár, blesk, sesuvy půdy a další. Pokud pojištěný nebude mít zabezpečený počítač, tablet či mobilní telefon především nějakým heslem, pojištění se na náhrady škody vyplývající ze ztráty těchto zařízení nebude vztahovat. Náhrady škod, které vznikly v důsledku porušení zákona v oblasti ochrany proti spamu a telemarketingu, toto pojištění kybernetických rizik nekryje. V neposlední řade se také pojištění nevztahuje na náhrady škod vzniklé z důvodu odpovědnosti, kterou na sebe pojištěný podnik převzal nad rámec zákona a dále z důvodu porušení obchodního tajemství nebo zákonné ochrany vynálezu (patentu). (Maxima pojišťovna, © 2023b; Maxima pojišťovna, © 2023c)

Územní rozsah pojištění je na území celého světa. Pokud je při pojistné události nutný IT odborník, pojištění se vztahuje pouze na náklady na jeho zásahy provedené z České republiky. Pojištěný má povinnost zajišťovat po celou dobu pojištění alespoň takovou úroveň zabezpečení svých zařízení a systémů, jakou měl a uvedl do dotazníku při podepisování pojistné smlouvy, a pravidelně aktualizovat různé antivirové systémy, hesla a podobně. V pojistné smlouvě je dále uvedena spoluúčast, kterou se pojištěný v případě pojistné události podílí na pojistném plnění. Všechny škody, které jsou předmětem tohoto pojištění, musí pojištěný ihned při zjištění oznámit pojistiteli. Pojištěný nesmí souhlasit s žádným rozhodnutím o odpovědnosti, pokutách a náhradách škody v jeho neprospěch, dokud s tím pojistitel písemně nesouhlasil. (Maxima pojišťovna, © 2023b)

3.2.3 Colonnade Insurance S.A.

Dalším pojišťovacím subjektem, který nabízí na českém pojistném trhu pojištění kybernetických rizik je Colonnade Insurance S.A. Tento pojistný produkt Pojištění kybernetických rizik CyberPlus a je určen především pro společnosti pracující v telekomunikacích nebo IT, společnosti, které pracují s velkým množstvím osobních údajů a dat, ale i například pro výrobní podniky nebo dopravní společnosti. Je vhodný pro všechny velikosti společností. (Colonnade Insurance S.A., © 2023)

Pojištění se vztahuje na náhradu škody, kterou požaduje třetí osoba po pojištěném, spojenou s domnělým nebo skutečným neoprávněným nakládáním s osobními údaji nebo důvěrnými informacemi. Předmětem pojištění jsou dále náhrady škody a náklady na právního zástupce, pokud jsou prostřednictvím pojištěného zničena nebo poškozena data třetí osobě, pokud jsou virem či škodlivým programem poškozena nebo zničena data třetí osoby v systému pojištěného, pokud zaměstnanec pojištěné společnosti neoprávněně zpřístupní data třetí osobě, nebo pokud je ukradeno IT vybavení pojištěného (hardware a software, který je využívaný k uchovávání, ochraně, přenosu a vytvoření elektronických dat) třetí osobou. Pojištění kryje náklady na služby právního zástupce (do výše sjednaného limitu v pojistné smlouvě), které podnik využívá při regulatorním řízení při šetření dozorovým orgánem například při domnělém či skutečném zneužití důvěrných informací. Pojistitel také uhradí náklady na sankce, které byly pojištěnému uloženy v regulatorním řízení, avšak opět pouze do výše limitu uvedeného v pojistné smlouvě. Pojištění se dále vztahuje na úhradu nákladů za odborné služby, které pojištěný využívá při řešení kybernetických událostí. Pojistitel uhradí kybernetického odborníka, krizového poradce a právního poradce v oblasti medií, kteří pomohou ke zlepšení špatné pověsti podniku po kybernetickém incidentu, dále pojistitel uhradí náklady na pomoc s obnovením dobrého jména jednotlivce (statutární orgán), který je součástí pojištěného podniku, náklady na šetření a shromažďování informací a následné oznámení dozorovému orgánu při domnělém nebo skutečném porušení ochrany osobních údajů a v neposlední řadě jsou z pojištění hrazeny náklady na obnovení informací a dat, která byla zničena či poškozena při kybernetickém útoku nebo selhání techniky. Všechny tyto náklady jsou ale hrazeny jen do výše limitu stanoveného v pojistné smlouvě.

K tomuto pojištění lze sjednat ještě různá připojištění. Jedno z těchto volitelných připojištění se vztahuje na náhradu škody či výdajů na právního zástupce v případě nějakého porušení při zveřejňování mediálního obsahu. Může jím být například pomluva třetí osoby, kopírování či zneužití cizích informací, nevědomé porušení obchodního jména, ochranné známky či

autorského práva, případně nekalá soutěž ve všech těchto vyjmenovaných případech. Dále je možné připojistit vydírání společnosti prostřednictvím internetových sítí. Pojištění kryje veškeré škody vzniklé v důsledku vydírání s cílem získat od poškozeného peníze, jako například náklady k ukončení či zamezení vydírání nebo náklady vynaložené na vyšetřování tohoto vydírání. Dalším možným připojištěním je pojištění v případě výpadků sítí. Pojistitel uhradí škody, které jsou způsobeny přerušením či omezením počítačové sítě nebo narušením zabezpečení počítače neoprávněným přístupem, šířením škodlivého viru nebo znepřístupněním dat uživatelům DDoS útokem.

Pojištění má také následující výluky. Pokud ztráty vzniknou v souvislosti s činností, která je nekalou soutěží, mimo výjimky uvedené u připojištění v oblasti zveřejňování mediálního obsahu, pojištění se na jejich náhrady nevztahuje. Další výlukou z pojištění jsou újmy na zdraví vzniklé v důsledku porušení právních předpisů o ochraně osobních údajů. Pojištění se také nevztahuje na povinnosti nahradit škody dané smlouvou či smluvní záruku nebo povinnosti, které pojištěný převezme nad rámec zákona. Pokud statutární orgán, společník nebo zaměstnanec pojištěné společnosti, který konal ve spolupráci se statutárním orgánem nebo společníkem, způsobí svým nezákonným jednáním škodu nebo pokud společnost vědomě poruší právní předpisy či vědomě nesplní nějakou povinnost, pojistitel není povinen pojištěnému hradit takto způsobené škody. Dále jsou z pojištění vyloučena riziková data. Jsou to ta data, jejichž vlastnosti, jako je například citlivost či kvalita, se závažně liší od těch, které byly uvedeny v dotazníku při uzavírání pojistné smlouvy. Vyloučeny jsou i škody způsobené porušením práv duševního vlastnictví. Mezi porušení práv duševního vlastnictví patří například zneužití různých licencí, patentů a porušení autorských práv. Tato výluka se ovšem netýká náhrady škody třetí osobě z důvodu porušení ochrany osobních údajů či důvěrných informací pojištěnou společností. Pokud statutární orgán či jiný člen vedení společnosti úmyslně jedná tak, že pojištěné společnosti jeho činností vznikne nárok na pojistné plnění a mohl vznik této skutečnost předpokládat, pojišťovna pojištěnému náhradu škody nevyplatí. Na nárok na pojistné plnění vyplývající ze skutečností, o kterých pojištěný věděl nebo vědět mohl ještě před podepsáním pojistné smlouvy, se pojištění také nevztahuje. Další výlukou jsou poplatky za licence nebo porušení právních předpisů při obchodování s cennými papíry. Pojištění se dále nevztahuje na škody, které vzniknou v souvislosti s válkou či terorismem nebo v důsledku výpadků elektřiny, telekomunikačních a internetových sítí. Pojištění se nevztahuje ani na škody a závazky vyplývající z toho, že společnost provozuje svoji činnost na kapitálovém trhu nebo na tomto trhu podniká neoprávněně. Dále jsou z pojištění vyloučeny náhrady škody, které

vzniknou, pokud pojištěný podnik neoprávněně shromažďuje a uchovává data a informace třetích osob a v neposlední řadě se pojištění nevztahuje na takzvané nepojistitelné ztráty podle právního řádu České republiky. (Colonnade Insurance S.A., 2019)

Všechny škody, které nastanou během trvání pojištění musí pojištěný při jejich objevení včas nahlásit pojistiteli, nejpozději ale poslední den platnosti pojištění uvedená v pojistné smlouvě. V pojistné smlouvě může být opět sjednána určitá spoluúčast a limity plnění u každé oblasti krytí zvlášť. Pojištění se vztahuje na pojistné události po celém světě. Pojišťovna Colonnade Insurance S.A. poskytuje také nově od roku 2022 pro své klienty v rámci tohoto pojištění bezplatnou asistenční linku Cyber Services 24/7, která funguje nonstop. Na tuto linku se klienti mohou kdykoliv obrátit v případě kybernetického útoku. (Colonnade Insurance S.A., 2019; Colonnade Insurance S.A., 2022)

3.2.4 Chubb

Poslední pojišťovací společností, která poskytuje pojištění kybernetických rizik, je Chubb. Pojišťovna Chubb nabízí produkt, který se jmenuje Cyber Enterprise Risk Management. Pojištění kryje rizika, která vyplývají z neoprávněného nakládání s osobními a důvěrnými údaji. Pokud je proti pojištěnému vedeno správní řízení, rozhodčí řízení, občanskoprávní řízení, je podána jiná výzva k náhradě škody nebo pojištěný nahlásí pojišťovně možné důvody vzniku těchto řízení nebo výzev v souvislosti s neoprávněným nakládáním s údaji a informacemi, pojišťovna poskytne pojistné plnění pojištěnému v případech uvedených v pojistné smlouvě. Pojistné plnění je poskytnuto, pokud se pojištěný podnik při shromažďování a uchovávání citlivých informací a dat, jako jsou osobní údaje nebo obchodní informace, dopustí domnělé či skutečné chyby nebo porušení jeho povinnosti, včetně pokusu o takováto jednání. Neoprávněné zacházení s údaji zahrnuje také nezáměrné nezákonné uchovávání osobních údajů. Pojistné plnění je poskytnuto na náhradu škody a nákladů, které souvisí s náklady na právního zástupce či další odborné osoby a náklady na záruky potřebné při podávání odvolání a další takové záruky, avšak pouze se souhlasem pojišťovny a dále také výdaje na zabezpečení řádného plnění právních předpisů upravujících povinnosti při nakládání s citlivými údaji, na forenzního vyšetřovatele nebo právního poradce. Pojištění se dále vztahuje na případy, kdy pojištěný naruší bezpečnost sítě. Toto pojištění kryje škody narušení bezpečnosti sítě způsobené skutečnou či domnělou chybou, porušením povinnosti i jejich pokusem, útokem hackerů, DDoS útoky, malware a dalšími neoprávněnými přístupy. Pojistné plnění je vyplaceno v případě, že je zahájeno správní, rozhodčí či občanskoprávní řízení, nebo pokud pojištěný obdrží výzvu

k náhradě finanční škody nebo sám nahlásí možné zahájení těchto řízení z důvodu narušení bezpečnosti sítě. Pojistné plnění opět hradí náklady na právního zástupce a další odborné osoby a náklady na finanční záruky potřebné při podávání odvolání, pouze ale se souhlasem pojišťovny, dále náklady na forenzního vyšetřovatele, právního poradce nebo zabezpečení správného dodržování právních předpisů v této oblasti. Další oblastí, na kterou se pojištění vztahuje, je odpovědnost v případě protiprávního jednání při vytváření a šíření obsahu v médiích. Odpovědnost za tato protiprávní jednání může vzniknout v případě odposlechu, psychické újmy třetí osoby, pokud pojištěný poškodí dobré jméno třetí osoby, šíří nějaké lživé informace a pomluvy o této osobě, poruší autorská práva, zneužije obchodní značku a nápad jiné osoby a další jednání způsobené nedbalostí. Nárok na pojistné plnění má pojištěný na základě občanskoprávního a rozhodčího řízení, které je proti pojištěnému podniku vedeno, na základě výzvy k náhradě finanční škody, nebo pokud pojištěný sám ohlásí pojišťovně možné protizákonné jednání z jeho strany, které by mohlo vést k zahájení těchto řízení. V rámci pojistného plnění jsou hrazeny náklady na právního zástupce a další odborné osoby, náklady na finanční záruky nutné pro podání odvolání a další takové záruky a náklady na krizové řízení a PR, avšak také pouze se souhlasem pojišťovny. Pojištění dále kryje škody způsobené kybernetickým vydíráním. Kybernetické vydírání pojištěného je na základě těchto pojistných podmínek hrozba útočníka, že zpřístupní chráněné údaje v systémech podniku, změní, smaže nebo nějak poškodí jeho elektronická data nebo vloží malware do systému pojištěného podniku, který může zničit či poškodit elektronická data nebo omezit přístup uživatelům do těchto systémů. Pojištěnému je vyplaceno v případě uhrazení peněžní částky k odvrácení vydírání (se souhlasem pojišťovny) ve výše popsaných situacích pojistné plnění do výše škody, která by vznikla, pokud by tato částka nebyla uhrazena. Dále jsou do pojistného plnění zahrnuty náklady na IT poradce, PR a krizové řízení. Pojištění se také vztahuje na škody způsobené ztrátou nebo poškozením dat. Pojistné plnění je vyplaceno ve výši nákladů nutných k obnovení dat, které byly zničeny a poškozeny z důvodu útoku malwaru, hackera, DoS útokem, neoprávněného přístupu, lidského nebo technologického pochybení, ale také pokud vypadla elektřina a ovlivnilo to software podniku. V neposlední řadě pojištění kryje také škody způsobené přerušením provozu podniku. Přerušení provozu může být z důvodu poškození dat, softwaru nebo znepřístupnění softwaru či dat uživatelům, což způsobil malware, DoS útok, pochybení lidí či softwaru, přístup neoprávněnou osobu nebo výpadek elektřiny, který ovlivnil daný software. Pojistné plnění je vyplaceno ve výši nákladů na obnovu dat (nevztahuje se na obnovu či aktualizaci softwaru) a ušlého zisku podniku, způsobeného právě přerušením provozu. Ušlý

zisk je vyplácen maximálně za období tří měsíců, pokud přerušení provozu trvá déle, může pojistitel tuto dobu upravit.

Výlukami z pojištění jsou škody, které jsou pojištěným způsobeny úmyslným porušením zákona, podvodem nebo trestným činem. Do této výluky se nezahrnují zaměstnanci pojištěného s výjimkou statutárního orgánu, generálního ředitele, risk manažera a dalších vedoucích zaměstnanců pojištěného podniku. Dále se pojištění nevztahuje na náhrady škod související s věcnou škodou a škodou na zdraví. Výlukou jsou také škody, které vycházejí z porušení smluvního závazku a záruky, dále náhrady škod, které přijme nad rámec povinností stanovených zákonem. Pojištění se také nevztahuje na škody, které vyplývají z činnosti prováděné statutárním orgánem a dalšími vedoucími zaměstnanci ještě před podepsáním smlouvy, u kterých pojištěný věděl, že mohou způsobit škodu, která je předmětem tohoto pojištění. Vyloučeny z pojištění jsou dále škody způsobené výpadky či omezením služeb webhostingu, pokud jsou poskytovány externím dodavatelem. Pojištění se dále nevztahuje na náhrady škod, které vzniknou v souvislosti s živelními událostmi, válkou, terorismem (s výjimkou kyberterorismu), revolucí, stávkou, občanskou válkou a dalšími podobnými událostmi. Ani škody, které souvisí s porušením obchodního tajemství nebo patentu, nejsou předmětem tohoto pojištění. Výlukou jsou také škody vzniklé v souvislosti s duševním vlastnictvím třetí osoby, jako je například porušení autorského práva (s výjimkou odpovědnosti v oblasti médií) nebo obchodního jména třetí osoby. Pojištění se nevztahuje ani na vědomé protiprávní zpracování citlivých údajů a také na neoznámení jejich zpracovávání. Z pojištění jsou vyloučeny náklady na aktualizaci a vylepšení zabezpečení dat a sítě, pokuty, sankce a další poplatky. Mezi škody způsobené omezením provozu v rámci tohoto pojištění nepatří vzniklé ztráty kvůli přerušení obchodování na kapitálových trzích nebo nemožnost zhodnotit nějaké aktivum. A v neposlední řadě se dále pojištění nevztahuje na běžné opotřebení softwaru a v něm uložených dat a zabavením dat a softwaru státním orgánem.

Územní rozsah tohoto pojištění je na území celého světa. V pojistné smlouvě je sjednán celkový limit pojistného plnění, a zároveň u každé oblasti pojištění jsou sjednány dílčí limity. Sjednána může být také určitá spoluúčast v každé oblasti tohoto pojištění zvlášť. Pojištěný má povinnost v případě zjištění pojistné události bezodkladně písemně ohlásit pojistiteli tuto skutečnost. Pokud při oznamování pojistné události pojištěný uvede lživé informace, může pojistník vyplacení pojistného plnění zamítnout. (Chubb, 2016)

3.3 Srovnání pojistných podmínek jednotlivých produktů

V této kapitole se zaměříme na porovnání pojistných podmínek jednotlivých produktů nabízených na českém pojistném trhu. Pojištění kybernetických rizik pro podnikatelské subjekty nabízí v České republice celkem čtyři pojišťovací subjekty, z toho vyplývá, že konkurence v této oblasti pojištění není až tak velká. Všechny porovnávané pojistné produkty jsou velmi podobné, liší se pouze v pár bodech. Jednotlivé pojišťovací subjekty umožňují jejich produkty upravit na míru podle vlastních potřeb zájemců o pojištění. Každý zájemce nejprve vyplní dotazník, který mu pojišťovna poskytne. Každá pojišťovna má svůj vlastní dotazník, ale informace v něm vyplňované jsou velice podobné. V dotazníku klient vyplňuje informace o společnosti, kterou chce pojistit a všech jejích dceřiných společnostech, dále předmět činnosti, obrat společnosti a jednotlivé pojistné nebezpečí, na které chce společnost pojistit. U každého pojistného nebezpečí uvede limit pojistného plnění a spoluúčast v případě pojistné události. V dotazníku musí dále uvést dosavadní zabezpečení počítačových systémů a dat, počet počítačů a odpovědět na další doplňující otázky, které potřebuje pojišťovna vědět k správnému nastavení pojištění pro jednotlivé společnosti, případně aby věděla, jaké pojistné plnění na základě těchto informací nebude poskytovat. Každá společnost má jiné potřeby a podmínky.

V tabulce 1 můžeme vidět porovnání vybraných dílčích pojistných nebezpečí, na které se lze v rámci pojištění kybernetických rizik pojistit. Tabulka ukazuje, zda je dané nebezpečí možné u konkrétní pojišťovny pojistit či nikoliv. Můžeme vidět, že nejvíce pojistných nebezpečí můžeme pojistit u ČSOB Pojišťovny. Neznamená to ale, že je to nejlepší možná volba, jakou by měla každá společnost zvolit. Každá společnost má jiné požadavky, a proto musí zvážit sama, jaký pojistný produkt vybrat. Některá uvedená pojistná nebezpečí jsou pojišťovnami nabízena jako volitelná připojištění. Tabulka ukazuje, že odpovědnost v oblasti médií, odpovědnost za narušení bezpečnosti sítě, kybernetické vydírání a odpovědnost za osobní údaje třetích osob poskytují všechny zmíněné pojišťovny. Zrovna tak všechny pojišťovny kryjí ztrátu a poškození dat a také náklady, které jsou spojeny s omezením nebo přerušením provozu, jako je ušlý zisk a další fixní náklady, které musí společnost pravidelně platit. Dále můžeme vidět, že jediná pojišťovna Chubb vyplácí pojistné plnění i v případě škod v důsledku výpadku elektrické sítě. Škody způsobené neoprávněným převodem peněžních prostředků z bankovního účtu třetí osobou kryje naopak pouze ČSOB Pojišťovna. Pokuty a sankce v případě porušení přepisů o ochraně osobních údajů a dat hradí pojištěnému všechny analyzované pojišťovny, kromě pojišťovny Chubb. Dalším typem pokut, které pojišťovny v rámci pojištění kybernetických rizik hradí, jsou pokuty v oblasti platebních karet, pokud společnost nedodrží

standardy PCI DSS. Pojistné plnění k náhradě těchto pokut poskytují všechny zmíněné pojišťovny s výjimkou Colonnade Insurance. Náklady na uvedení ztracených či poškozených dat do původního stavu (pokud je to možné) hradí v rámci pojistného plnění všechny zkoumané pojišťovny. Pokud se ale data poškodí v důsledku nějaké živelní události či války, pojištění se na tyto případy nevztahuje u žádné pojišťovny.

Tabulka 1: Porovnání pojistných podmínek jednotlivých pojistných produktů

Pojistné nebezpečí	**ČSOB Pojišťovna**	**Maxima pojišťovna**	**Colonnade Insurance**	**Chubb**
Odpovědnost v oblasti médií	✓	✓	✓	✓
Odpovědnost za narušení bezpečnosti sítě	✓	✓	✓	✓
Kybernetické vydírání	✓	✓	✓	✓
Ztráta a poškození dat	✓	✓	✓	✓
Odpovědnost za údaje třetích osob	✓	✓	✓	✓
Přerušení provozu podniku (ušlý zisk, …)	✓	✓	✓	✓
Ztráta dat při výpadku elektřiny	X	X	X	✓
Neoprávněný převod peněz z bankovního účtu	✓	X	X	X
Pokuty a sankce při porušení ochrany dat	✓	✓	✓	X
Pokuty v oblasti platebních karet	✓	✓	X	✓
Uvedení dat do původního stavu	✓	✓	✓	✓
IT asistenční služby	✓	X	✓	X
Ztráta dat při živelních událostech nebo válce	X	X	X	X

Zdroj: vlastní zpracování

Colonnade Insurance a ČSOB Pojišťovna nabízí v rámci pojištění také asistenční služby v oblasti IT. Tyto služby fungují dvacet čtyři hodin denně, sedm dní v týdnu. Asistenční linka Colonnade Insurance poskytuje rady ke snížení dopadu kybernetických událostí a navrhuje

jejich další řešení. V rámci této linky se poskytuje rovněž zásah bezpečnostního odborníka v místě pojištěné společnosti. Asistenční služby ČSOB Pojišťovny poskytují řešení situací, kdy pojištěnému nefunguje software či hardware v jeho zařízení. Odborník řeší tyto problémy prostřednictvím telefonické komunikace nebo vzdálených přístupem do zařízení pojištěného. Pokud si nebude vědět rady, nalezne pojištěnému příslušné servisy v jeho okolí.

Výluky z pojištění jsou vesměs u všech analyzovaných pojistných produktů stejné. Liší se v pár menších drobnostech. Pojištění se u všech analyzovaných pojišťoven nevztahuje na škody, které vznikly činností v rozporu s právními předpisy, nebo bez příslušného oprávnění. ČSOB Pojišťovna jako jediná uvádí výluku na škody, které vzniknou po požití alkoholu či jiných omamných a psychotropních látek. Na nároky, které na sebe převezme společnost nad rámec zákona, se pojištění nevztahuje ani u jedné pojišťovny. Zrovna tak i na škody, jak už bylo uvedeno výše, které vzniknou v období trvání války či demonstrace nebo vzniknou v důsledku živelních událostí, žádná z pojišťoven nevyplácí pojistné plnění. Všechny pojišťovny mají v pojistných podmínkách uvedenou výluku na škody způsobené výpadkem dodávky plynu, telekomunikačních, internetových či elektrických sítí. Jediná pojišťovna Chubb však vyplácí pojistná plnění na ztrátu či poškození dat i v důsledku výpadku elektrické sítě. ČSOB Pojišťovna uvádí ještě například výluku ohledně odpovědnosti za data v případě poskytování cloudových úložišť nebo výluku ohledně odpovědnosti za škody způsobené blízké osobě, dceřiné a mateřské společnosti či společnosti, ve které má pojištěný majetkový podíl. U Colonnade Insurance a ČSOB Pojišťovny se podle pojistných podmínek pojištění nevztahuje také na škody způsobené činností, která je proti hospodářské soutěži. Škody související s úmyslným neoprávněným zpracováním osobních údajů jsou u Maxima pojišťovny a Chubb vyloučeny. U Maxima pojišťovny se pojištění dále nevztahuje na škody a náklady na modernizaci či inovaci softwarů. A v neposlední řadě mají všechny analyzované pojišťovny uvedenou v pojistných podmínkách výluku na porušení práv duševního vlastnictví, jako jsou například různé patenty nebo licence. Každá pojišťovna má u svého produktu uvedeno velké množství výluk, na které se pojištění nevztahuje, jejich nejobsáhlejší výčet má ale ČSOB Pojišťovna.

4 POJISTNÁ OCHRANA VYBRANÉ SPOLEČNOSTI

V této kapitole se budeme zaměřovat na výběr optimální pojistné ochrany pro vybranou společnost. Nejprve bude vybraná společnost stručně popsána, dále si vymezíme její činnost, IT vybavení a další doplňující informace. Následně se budeme zabývat kybernetickými riziky, která by u ní mohla nastat. V další části této kapitoly bude vybrán optimální pojistný produkt na základě předchozí podrobné analýzy pojistných produktů v oblasti kybernetických rizik na českém pojistném trhu.

4.1 Popis vybrané společnosti a jejích kybernetických rizik

Pro tuto diplomovou práci byla vybrána společnost, která si vzhledem k oblasti, kterou se práce zabývá, nepřála být jmenována. Společnost se zabývá službami v oblasti elektro, zajišťují různá projektování, provádí elektroinstalace a revize. Tato společnost byla vybrána z toho důvodu, aby bylo poukázáno na to, že kybernetickými riziky jsou ohroženy nejen společnosti, které pracují s velkým množstvím osobních údajů a dat, ale i společnosti, které se zabývají nějakou řemeslnou činností. Společnost vznikla v roce 2018, jako společnost s ručením omezeným, z již existující živnosti jednoho z jednatelů. Původní živnost působila na trhu již téměř třicet let. Sídlí v Královéhradeckém kraji a má dvanáct zaměstnanců. Tato společnost je také smluvním partnerem energetické společnosti ČEZ.

Mezi informační aktiva společnosti patří počítače, mobilní telefony, účetní softwary, softwary k projektování, databáze zákazníků a dodavatelů, databáze zaměstnanců, různá zálohovaná data, internetové bankovnictví, webové stránky, účet na sociální síti a v neposlední řadě jsou informačním aktivem také zaměstnanci. Webové stránky a účet na sociální síti si společnost spravuje sama.

V následující tabulce číslo 2 je uveden seznam kybernetických rizik, která by mohla ve vybrané společnosti nastat. Seznam rizik byl vytvořen společně s jednateli této společnosti. Prvním rizikem pro společnost je ztráta dat při nějakém kybernetickém incidentu. Data mohou být poškozena nebo ztracena, například z důvodu napadení zařízení ransomwarem nebo malwarem. Zrovna tak mohou být data poškozena v důsledku výpadku elektrické energie nebo jejím přepětím, kdy se v průběhu práce data nemusí stihnout uložit nebo se vyskytne chyba při jejich zálohování. Dalším nebezpečím, které může v této společnosti nastat, je neoprávněné odčerpání peněžních prostředků z bankovního účtu. Útočník může zjistit přihlašovací údaje do internetového bankovnictví pomocí phishing útoku či malwaru a poté je zneužít ve svůj

prospěch. V důsledku kybernetického útoku mohou také uniknout osobní údaje a informace o zákaznících, dodavatelích, smluvních partnerech, ale i o samotných zaměstnancích společnosti. Stačí, když někomu přijde email, ve kterém odesílatel požaduje přihlášení do nějakého programu s evidencí těchto osob. Když se uživatel podle pokynů přihlásí, útočník získá do tohoto programu přístup.

Rizikem pro vybranou společnost může být také situace, kdy útočník využije její počítače k útoku na třetí osobu. Tím může společnost způsobit škodu další osobě, aniž by o tom věděla. Kvůli kybernetické události může být také omezen či dokonce přerušen provoz společnosti, v jehož důsledku může společnost přijít o zisk, dále musí také platit určité fixní náklady, i když je její provoz přerušený. Dalším kybernetickým nebezpečím může být ztráta dat při požáru, vichřici a dalších živelních událostech. Ztráta dat v důsledku povodní této společnosti nehrozí, protože se nenachází v povodňové oblasti, v jejím okolí není žádná řeka nebo přehrada. Společnost se může dále stát obětí útoku ransomwaru, kdy útočník zablokuje určitá data nebo dokonce celý počítač a společnost vydírá tím, že požaduje za jeho odblokování výkupné. Po zaplacení určité částky pošle oběti jeho útoku klíč k odšifrování dat. Dále mohou být také zneužity přihlašovací údaje. Toto nebezpečí může nastat v případě, že některému ze zaměstnanců přijde do schránky zdánlivě věrohodný email, který požaduje provést přihlášení do nějaké aplikace či softwaru, stejně jako bylo popsáno výše, v případě úniku osobních údajů. V případě provedení přihlášení útočník okamžitě zjistí tyto přihlašovací údaje daného uživatele. Rizikem může být také situace, kdy se vyskytne nějaká chyba při zálohování dat, a v důsledku toho jsou data ztracena. Důležité je pravidelně data zálohovat a kontrolovat úplnost zálohovaných dat. Může se stát, že v případě kybernetické události se ztratí data z počítače, a pokud se vyskytla nějaká chyba při zálohování, nebude už třeba možné data znovu získat, i přestože byla zálohována.

Společnost může být také ohrožena tím, že v případě nějakého kybernetického incidentu může být poškozeno její dobré jméno. Může se to stát například právě, když je způsobena nějaká škoda třetí osobě prostřednictvím počítačů společnosti. V důsledku výpadku internetového připojení zaměstnanci společnosti nemohou používat softwary, které toto připojení k jejich funkci potřebují, to může způsobit omezení provozu společnosti nebo může být kvůli výpadku omezena bezpečnost (funkčnost antivirového systému). Dalším nebezpečím jsou škodlivé nevyžádané emaily. Nejen, že zahlcují emailovou schránku, ale některé mohou být i nebezpečné. Pokud příjemce zprávy otevře nebezpečný odkaz uvnitř takového emailu, může si

stáhnout do počítače například nějaký vir, nebo pokud vyplní požadované údaje, může také přijít i o peníze nebo data.

Dalším nebezpečím může být pochybení ze strany zaměstnance společnosti. Zaměstnanec může otevřít nebezpečný email nebo třeba stáhnout nakažený soubor, tím se v počítači mohou například zašifrovat nebo ztratit data. Dále může zaměstnanec nedopatřením zveřejnit osobní údaje třetí osoby tím, že pošle emailovou zprávu nesprávnému adresátovi, ten může tato data zneužít. Zaměstnanec také může v důsledku pochybení smazat důležitá data uložená v počítači. Společnost má účet na sociální síti Facebook a svoje webové stránky, z toho vyplývá poslední uvedené riziko, které může nastat. Útočník se může nabourat do účtu na sociální síti nebo webové stránky, kde může sdílet různé příspěvky nebo informace, které mohou poškodit dobré jméno společnosti.

Tabulka 2: Seznam kybernetických nebezpečí vybrané společnosti

	Kybernetická nebezpečí
1.	Ztráta dat při kybernetickém incidentu
2.	Ztráta dat při výpadku elektřiny
3.	Neoprávněné odčerpání peněz z bankovního účtu
4.	Únik osobních údajů zákazníků
5.	Únik osobních údajů zaměstnanců
6.	Využití počítačů společnosti útočníkem k útoku na třetí osobu
7.	Ušlý zisk z důvodu přerušení provozu kybernetickým incidentem
8.	Ztráta dat při požáru nebo vichřici
9.	Vydírání společnosti a požadování výkupného
10.	Zneužití přihlašovacích údajů
11.	Selhání zálohování
12.	Poškození dobrého jména z důvodu kybernetického incidentu
13.	Škoda v důsledku výpadku internetu
14.	Působení škodlivé nevyžádané pošty
15.	Škoda v důsledku pochybení zaměstnance
16.	Nabourání na webové stránky či sociální sítě

Zdroj: vlastní zpracování

4.2 Výběr optimální pojistné ochrany

V předchozí kapitole byly detailně analyzovány a porovnány pojistné produkty v oblasti kybernetických rizik, které jsou nabízeny na českém pojistném trhu. V návaznosti na tuto analýzu bude v této podkapitole vybrán nejvhodnější pojistný produkt pro vybranou společnost, která byla definována výše.

Všechny analyzované pojistné produkty kryjí velké množství kybernetických rizik. Každá pojišťovna se snaží pro společnosti udělat pojistný produkt velmi flexibilní, to znamená, že si každá společnost zvolí jaká připojištění k základnímu pojištění chce a dále si také určí pojistné sublimity a spoluúčast ke každému pojistnému nebezpečí. V následujícím odstavci si u jednotlivých pojistných nebezpečí vybrané společnosti určíme, u jaké pojišťovny se na ně lze pojistit.

První pojistné nebezpečí zvolené společnosti (ztráta dat při kybernetickém incidentu) je možné pojistit u všech čtyř pojišťoven. Pojistné plnění se vztahuje na náklady na obnovu těchto dat. Ztráta dat při výpadku elektřiny je předmětem pojištění pouze u pojišťovny Chubb. Neoprávněná ztráta finančních prostředků z bankovního účtu lze naopak pojistit pouze u ČSOB Pojišťovny. Dalším rizikem vybrané společnosti, které by mohlo nastat, je únik osobních údajů zákazníků, dodavatelů, ale i smluvních partnerů. Z takového porušení ochrany dat vyplývají různé sankce, na které se lze pojistit u ČSOB Pojišťovny, Maxima pojišťovny a Colonnade Insurance. Škody v důsledku odpovědnosti za narušení bezpečnosti sítě v případě, že útočník využije počítače vybrané společnosti, a tím způsobí škodu třetí osobě, jsou předmětem pojištění opět u všech čtyř analyzovaných pojišťoven. V rámci tohoto pojištění jsou hrazeny také náklady na právního zástupce. Ušlý zisk a fixní náklady, v případě omezení či přerušení provozu společnosti, je také možné sjednat u všech pojišťoven. Náhradu ztráty či poškození dat v případě požáru a různých přírodních vlivů, jako je například vichřice, bohužel neposkytuje žádná z uvedených pojišťoven. V případě kybernetického vydírání společnosti všechny zmíněné pojišťovny po předchozím souhlasu pojištěnému uhradí přiměřenou částku a další s tím spojené náklady, které musel zaplatit, aby kybernetické vydírání odvrátil. Zneužití přihlašovacích údajů útočníkem můžeme zařadit do oblasti pojistného nebezpečí ztráty a zneužití dat, u kterého bylo již výše uvedeno, že je předmětem pojištění všech čtyř analyzovaných pojišťoven. Pokud nastane nějaká chyba při zálohování, pojišťovny bohužel pojistné plnění na tyto škody nevyplácí. Zálohování je ale podmínkou pro náhradu škody při poškození či ztrátě dat. Pokud je společnosti poškozeno její dobré jméno, pojišťovny Maxima, ČSOB a Colonnade Insurance jí uhradí náklady na odborné služby k nápravě a zmírnění

následků takového poškození. Chubb poskytuje náhradu škody pouze, pokud sám pojištěný někomu způsobí škodu na jeho dobrém jménu. Škody v důsledku výpadku internetových služeb nejsou předmětem pojištění u žádné z uvedených pojišťoven. Působení škodlivé nevyžádané pošty a škoda v důsledku pochybení zaměstnance spolu může souviset. Zaměstnanec svojí chybou otevře nakažený soubor či odkaz, a tím způsobí zašifrování počítače, ztrátu dat či dokonce peněžních prostředků. Jak už bylo uvedeno výše, náhradu nákladů na obnovu dat, včetně kybernetického vydírání, poskytují všechny pojišťovny. Neoprávněné odčerpání peněžních prostředků je ale předmětem pojištění pouze u ČSOB Pojišťovny. V případě, že zaměstnanec pochybí tím, že nedopatřením zveřejní osobní údaje třetí osoby, náhradu nákladů na řešení této pojistné události poskytnou pojištěné společnosti všechny analyzované pojišťovny. Všechny uvedené pojišťovny poskytují náhradu nákladů v oblasti odpovědnosti za osobní údaje třetích osob. Posledním zmíněným rizikem, které by mohlo u vybrané společnosti nastat, je nabourání na jejich webové stránky či sociální sítě. Tato skutečnost by mohla společnosti například poškodit její dobré jméno. Jak už bylo zmíněno výše, náhrady nákladů na zmírnění následků poškození dobrého jména podniku poskytují pojišťovny ČSOB, Maxima a Colonnade Insurance. Všechny tyto uvedené náklady a náhrady škod uhradí pojišťovny pouze do výše sjednaných limitů v pojistné smlouvě.

Z výše uvedeného můžeme konstatovat, že jako nejvhodnější pojistný produkt v oblasti pojištění kybernetických rizik se pro vybranou společnost jeví produkt od ČSOB Pojišťovny. Většinu pojistných nebezpečí, která byla stanovena u této společnosti, je ČSOB Pojišťovna schopna pojistit. Jedinými riziky, na které se pojištění nevztahuje, jsou škody v důsledku výpadku elektrické energie, internetového připojení a škody v důsledku požáru a přírodních vlivů. Tato rizika ale nejsou předmětem pojištění u žádné z analyzovaných pojišťoven, s výjimkou škod v důsledku výpadku elektřiny, které je možné pojistit u pojišťovny Chubb. Velkou výhodou je také možnost pojištění kybernetické kriminality, to znamená pojištění neoprávněného odčerpání finančních prostředků z bankovního účtu, což nabízí pouze právě ČSOB Pojišťovna. Toto kybernetické nebezpečí je ze všech stanovených rizik pro vybranou společnost jedním z největších. Protože společnost nepracuje s velkým množstvím citlivých dat, rizika ohledně zveřejnění či poškození těchto dat nejsou až tak velká.

Výhodou je dále hustá pobočková síť, kdy ČSOB Pojišťovnu můžeme nalézt téměř v každém větším městě. Ostatní pojišťovny mají svoji pobočku pouze v Praze, což je pro společnost z Královéhradeckého kraje nevýhodné. Pojištění od ČSOB Pojišťovny poskytuje služby různých odborníků, například IT odborníky, právní zástupce nebo PR odborníky. Další velkou

výhodou tohoto pojištění je také možnost asistenčních služeb v oblasti IT, které může společnost využít celkem třikrát za rok v délce 180 minut na konzultaci. Asistenční služby jsou dostupné celodenně, každý den v týdnu. IT specialista pomůže telefonicky nebo pomocí vzdáleného přístupu vyřešit problém s poškozeným softwarem nebo hardwarem v zařízení společnosti.

Důležitým faktorem předcházení kybernetických rizik jsou ale v první řadě různá bezpečnostní opatření (například antivirové a další bezpečnostní softwary) a vzdělávání všech zaměstnanců pracujících s počítačovým zařízením, ale i těch ostatních. Pokud budou všichni zaměstnanci informováni o možných hrozbách v oblasti kybernetických rizik, je možné předejít velké části následků těchto hrozeb. Kybernetické útoky se nedotýkají pouze velkých společností nebo společností pracujících s velkým množstvím citlivých dat, ale také malých živnostníků a firem podnikajících například v řemeslném nebo potravinářském odvětví.

ZÁVĚR

Cílem této diplomové práce bylo nastavení optimální pojistné ochrany proti kybernetickým rizikům. Zároveň k dosažení tohoto hlavního cíle byly stanoveny dílčí cíle, které spočívaly v analýze pojistných produktů zamřených na krytí kybernetických rizik nabízených na českém pojistném trhu a následném srovnání pojistných podmínek těchto produktů. Práce se nejprve zabývala teoretickým vymezením pojišťovnictví, kde byly charakterizovány základní pojmy týkající se tohoto odvětví a dále také druhy pojištění. Následující část se věnovala kybernetické bezpečnosti. Právě kybernetická bezpečnost je v současné době s vývojem informačních technologií stále významnějším tématem. Informační technologie využívá postupem času více a více lidí, tím se bohužel zvyšuje i pravděpodobnost možných kybernetických útoků. Dále bylo v práci navázáno vymezením principů kybernetické bezpečnosti a charakteristikou kybernetických útoků. V dnešní době se můžeme setkat s velkým množstvím druhů kybernetických útoků, které se vyvíjí současně s vývojem technologií. Nejčastěji se setkáme s malwarem, phishingem nebo nevyžádanou poštou. V následující části byl popsán vývoj kybernetické bezpečnosti v České republice, kde byla vymezena česká legislativa a také instituce, které se v ČR zabývají kybernetickou bezpečností. Bylo zjištěno, že se stát snaží zvyšovat kyberbezpečnost a také povědomí o nebezpečí, které může nastat.

V následující části diplomové práce byly naplněny dílčí cíle. Nejprve byla provedena detailní analýza pojistných produktů, zaměřených na kybernetická rizika, nabízených na českém pojistném trhu. Bylo zjištěno, že na našem trhu není mnoho pojišťovacích institucí, které by nabízely pojištění kybernetických rizik pro podnikatelské subjekty. Toto pojištění nabízí ČSOB Pojišťovna, Maxima pojišťovna, Colonnade Insurance S.A. a Chubb. Při analýze pojistných podmínek jednotlivých produktů bylo zjištěno, že předmětem pojištění může být velké množství kybernetických rizik. Společnost si může u pojistného produktu velmi flexibilně zvolit, o jaká pojištění bude mít zájem a v jakém pojistném limitu. Pojištění lze sjednat například na odpovědnost v oblasti médií nebo za narušení bezpečnosti sítě, na kybernetické vydírání, kybernetický zločin, dále některé pojišťovny hradí pokuty uložené v oblasti platebních karet nebo při porušení ochrany dat. Pojistné plnění vyplácí pojišťovny i v případě přerušení provozu společnosti v důsledku kybernetického incidentu. Naopak výlukou z pojištění je například ztráta dat v důsledku živelní události, války, škody způsobené trestnou činností nebo při požití alkoholu a drog. Pojistné plnění pojišťovny nevyplácí ani při přerušení dodávek plynu nebo internetových či telekomunikačních služeb.

Dále byly jednotlivé pojistné podmínky pojistných produktů porovnány mezi sebou. Bylo zjištěno, že pojistné produkty se od sebe nějak výrazně neliší. Odlišují se pouze v pár pojistných nebezpečích. Například náhradu škody při ztrátě dat v důsledku výpadku elektrické energie poskytuje pouze pojišťovna Chubb. Pojištění kybernetického zločinu je možné naopak sjednat jen u ČSOB Pojišťovny. Náhradu pokut v oblasti platebních karet poskytují všechny analyzované pojišťovny, s výjimkou Colonnade Insurance. ČSOB Pojišťovna a Colonnade Insurance mají v rámci pojištění kybernetických rizik zahrnuty také IT asistenční služby, které fungují nonstop.

V další části diplomové práce byla vybrána společnost, pro kterou byla následně zvolena optimální pojistná ochrana. Společnost byla krátce charakterizována a dále vymezena její kybernetická rizika. Byla vybrána menší společnost, která se zabývá službami v oblasti elektro. Jejími kybernetickými riziky mohou být například škody v důsledku chyby zaměstnance, únik osobních údajů zaměstnanců nebo zákazníků, ztráta dat při kybernetickém incidentu, zneužití přihlašovacích údajů, působení nevyžádané pošty, poškození dobrého jména nebo neoprávněné odčerpání peněžních prostředků z bankovního účtu. Nejvíce kybernetických nebezpečí vybrané společnosti lze pojistit u Pojišťovny ČSOB. Jediným pojistným nebezpečím společnosti, které lze pojistit pouze u pojišťovny Chubb, je ztráta dat v důsledku výpadku elektrické energie. Ostatní rizika lze pojistit buď u ČSOB Pojišťovny, nebo pojištění daného rizika neposkytuje žádná z pojišťoven. Z toho vyplývá, že optimální pojistnou ochranou pro vybraný podnik je pojištění od ČSOB Pojišťovny. Velkou výhodou je pojištění kybernetického zločinu, které tato pojišťovna poskytuje jako jediná. Další výhodou jsou také již zmíněné IT asistenční služby nebo hustá pobočková síť. Ostatní pojišťovny mají pobočku pouze v Praze.

S kybernetickými riziky se setkáváme téměř v každodenním životě, proto by měl být každý velice obezřetný. Stačí jedno špatné kliknutí a problém je na světě. Důležitým faktorem ochrany před těmito riziky je kvalitní softwarová ochrana a v neposlední řadě také důkladné proškolení zaměstnanců. Pokud zaměstnanci budou vědět, jaká nebezpečí mohou čekat, společnost se vyvaruje velkému množství kybernetických incidentů. Všechny společnosti by měly také zvážit sjednání pojištění kybernetických rizik, aby v případě kybernetické události alespoň zmírnily její finanční dopady. Finanční dopady těchto událostí mohou být opravdu obrovské.

POUŽITÁ LITERATURA

ANTONUCCI, Domenic, 2017. *The cyber risk handbook: Creating and Measuring Effective Cybersecurity Capabilities*. Hoboken, New Jersey: Wiley. ISBN 978-1-119-30880-5.

COLONNADE INSURANCE S.A, 2019. *Pojistné podmínky - CyberPlus pojištění kybernetických rizik* [online]. [cit. 2023-03-13]. Dostupné z: https://www.colonnade.cz/cdn/65b2eb68-cf8e-0106-94e7-7fcbfbaa6c5e/4940bf70-0339-4654-80dc-3dee175661b5/VPP_CyberPlus.pdf?_gl=1*1nh4vao*_up*MQ..*_ga*Mzc4MjE2NzA1LjE2NzgyODY4NzY.*_ga_GSXM0FS53F*MTY3ODI4Njg3NS4xLjAuMTY3ODI4Njg3NS4wLjAuMA..

COLONNADE INSURANCE S.A, 2022. *Colonnade Cyber Services 24/7* [online]. [cit. 2023-03-13]. Dostupné z: https://assets-eu-01.kc-usercontent.com/65b2eb68-cf8e-0106-94e7-7fcbfbaa6c5e/ce3178a5-906e-46fd-8cb7-c354f9cc576d/Colonnade%20Cyber%20Services.pdf

COLONNADE INSURANCE S.A, © 2023. *Pojištění kybernetických rizik* [online]. [cit. 2023-03-13]. Dostupné z: https://www.colonnade.cz/firmy/pojisteni-financnich-rizik/pojisteni-kybernetickych-rizik

ČERNOHORSKÝ, Jan, 2020. *Finance: od teorie k realitě*. Praha: Grada Publishing. ISBN 978-80-271-2215-8.

ČSOB POJIŠŤOVNA, 2018. *Pojištění kybernetických rizik: Všeobecné pojistné podmínky - zvláštní část* [online]. [cit. 2023-03-04]. Dostupné z: https://www.csobpoj.cz/documents/10332/32946/10N9059+VPP_CRC_2018_10-2018.pdf/dc55ba8d-b5e3-17c8-0954-63591b631e67?t=1576162606907

ČSOB POJIŠŤOVNA, 2022a. *Všeobecné pojistné podmínky: Pojištění internetových rizik* [online]. [cit. 2023-02-27]. Dostupné z: https://www.csobpoj.cz/documents/10332/2572720/11N9355_VPP-PIR-2022.pdf/1399ed2c-e7b8-30ba-e4fa-9f76b7f52705?t=1646749063575

ČSOB POJIŠŤOVNA, 2022b. *Pojištění internetových rizik: Informační dokument o pojistném produktu* [online]. [cit. 2023-02-27]. Dostupné z:

https://www.csobpoj.cz/documents/10332/2572720/11N9356_IPID-PIR-2022.pdf/20df5ff3-3e24-9745-73dc-0b8954c518c5?t=1646749062420

ČSOB POJIŠŤOVNA, © 2023. *Kalkulačka Pojištění internetových rizik* [online]. [cit. 2023-02-27]. Dostupné z: https://kalkulacka.csobpoj.cz/pojisteni-internetovych-rizik

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

DUCHÁČKOVÁ, Eva, 2015. *Pojištění a pojišťovnictví*. Praha: Ekopress. ISBN 978-80-87865-25-5.

ESET, © 2023. *Trojský kůň* [online]. [cit. 2023-01-25]. Dostupné z: https://www.eset.com/cz/trojsky-kun/

HSU, D. Frank a Dorothy MARINUCCI, 2013. *Advances in Cyber Security: Technology, Operations and Experiences*. New York: Fordham University Press. ISBN 978-0-8232-4456-0.

CHUBB, 2016. *Pojistné podmínky pro pojištění Cyber Enterprise Risk Management* [online]. [cit. 2023-03-18]. Dostupné z: https://www.chubb.com/content/dam/chubb-sites/chubb-com/cz-cz/for-business/financial-risk-professional-liability-insurance/documents/pdf/chubb_pp-cyber-risk-management.pdf

INTERNETEM BEZPEČNĚ, © 2018. *Botnet* [online]. [cit. 2023-01-25]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/botnet/

JANKO, David, © 2023. *Lekce 1 - Základní pojmy a zásady kybernetické bezpečnosti* [online]. [cit. 2023-01-18]. Dostupné z: https://www.itnetwork.cz/bezpecnost/zakladni-pojmy-a-zasady-kyberneticke-bezpecnosti

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-31-7.

KRESA, Dan, 2018. *Jaké jsou nejčastější typy kybernetických útoků?* [online]. [cit. 2023-01-24]. Dostupné z: https://www.kybez.cz/jake-jsou-nejcastejsi-typy-kybernetickych-utoku/

MAXIMA POJIŠŤOVNA, © 2023a. *Pojištění kybernetických rizik a odpovědnosti za data (GDPR)* [online]. [cit. 2023-03-08]. Dostupné z:

https://www.maximapojistovna.cz/cs/podnikatele-prumysl/pojisteni-kybernetickych-rizik-odpovednosti

MAXIMA POJIŠŤOVNA, © 2023b. *Zvláštní pojistné podmínky pro pojištění kybernetických rizik* [online]. [cit. 2023-03-08]. Dostupné z: https://www.maximapojistovna.cz/sites/default/files/2019-05/zvlastni_pojistne_podminky_cyber_risk_700-1.pdf

MAXIMA POJIŠŤOVNA, © 2023c. *Všeobecné pojistné podmínky pro pojištění podnikatelů* [online]. [cit. 2023-03-08]. Dostupné z: https://www.maximapojistovna.cz/sites/default/files/2019-05/vseobecne_pojistne_podminky_pro_pojisteni_podnikatelu_vpp_300-2.pdf

MICROSOFT, © 2023. *Co je kybernetická bezpečnost?* [online]. [cit. 2023-01-18]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-cybersecurity

MORAVČÍK, Ondřej, 2023. Vývoj registrované kriminality v roce 2022. *Policie ČR* [online]. [cit. 2023-02-19]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2015. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* [online]. [cit. 2022-11-06]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2015-2020.pdf

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2021. *Národní strategie kybernetické bezpečnosti České republiky pro období let 2021 až 2025* [online]. [cit. 2023-02-08]. Dostupné z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2023. *O NÚKIB* [online]. [cit. 2023-02-08]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

POLICIE ČR, © 2023. *Kriminalita* [online]. [cit. 2023-02-19]. Dostupné z: https://www.policie.cz/statistiky-kriminalita.aspx

SDRUŽENÍ PRO BANKOVNÍ KARTY, © 2023. *O PCI DSS - úvod. PCI DSS* [online]. [cit. 2023-03-04]. Dostupné z: https://www.pcistandard.cz/pcidss/

SEDLÁK, Petr a Martin KONEČNÝ, 2021. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství. ISBN 978-80-7623-068-2.

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-737-5.

THE UNITED STATES ARMY, 2010. *Cyberspace Operations Concept Capability Plan 2016-2028* [online]. CreateSpace Independent Publishing Platform. [cit. 2022-11-01]. Dostupné z: https://irp.fas.org/doddir/army/pam525-7-8.pdf

VLÁDA ČR, 2004. *Státní informační a komunikační politika: e-Česko 2006* [online]. [cit. 2023-02-04]. Dostupné z: https://www.esfcr.cz/documents/21802/761522/St%C3%A1tn%C3%AD+informa%C4%8Dn%C3%AD+a+komunika%C4%8Dn%C3%AD+politika/9a6117ea-24a8-484f-8d08-07365057e12b

Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů. In: *Sbírka zákonů České republiky*. 2014, ISSN 1211-1244.