UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2025 HOSSAM ABOUSHANAB

Univerzita Pardubice

Fakulta ekonomicko-správní

Pojištění kybernetických rizik

Bakalářská práce

2025 Hossam Aboushanab

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Hossam Aboushanab**
Osobní číslo:	**E21785**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
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. K volbě optimální pojistné ochrany budou využity metody vícekriteriálního rozhodování. Rozhodovací kritéria budou vycházet z chráněných aktiv a konkrétních požadavků na zabezpečení.

Osnova:
- Úvod do problematiky kybernetických rizik.
- Vysvětlení významu pojištění kybernetických rizik.
- Nabídka pojištění kybernetických rizik.
- Stanovení hodnotících kritérií, aplikace metod vícekriteriálního rozhodování.
- Výběr optimální varianty pojištění.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
DUCHÁČKOVÁ, Eva. Pojištění a pojišťovnictví. Praha: Ekopress, 2015. ISBN 978-80-87865-2-5.
SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert. ISBN 978-80-247-4644-9.
ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

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

Datum zadání bakalářské práce: **1. září 2024**
Termín odevzdání bakalářské práce: **30. dubna 2025**

L.S.

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

prof. Ing. Jitka Komárková, Ph.D. v.r.
garant studijního programu

V Pardubicích dne 1. září 2024

Prohlašuji:

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

Byl jsem seznámen 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 směrnici 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 26. 6. 2025

Hossam Aboushanab v.r.

PODĚKOVÁNÍ

Tímto bych rád poděkoval své vedoucí bakalářská práce Mgr. Haně Boháčové, Ph.D., za odborné vedení, trpělivost a cenné připomínky, které mi při zpracování práce nesmírně pomohly. Dále bych chtěl poděkovat vybrané společnosti za ochotu a čas při poskytnutí potřebných informací.

ANOTACE

Tato bakalářská práce se zaměřuje na problém kybernetických rizik a jejich pojištění. Jejím cílem je vybrat nejlepší pojistný produkt pomocí metod rozhodování na základě více kritérií. Nejprve představíme terminologii, která nám pomůže lépe porozumět kybernetickým rizikům, a poté představíme pojištění a některé jeho pojmy, které přiblíží a vysvětlí různé nabídky pojišťoven. Abychom mohli vybrat optimální alternativu, definujeme soubor kritérií, určíme jejich důležitost a vyhodnotíme je s ohledem na každou alternativu. Nakonec využijeme jednu z metod hodnocení alternativ, abychom mohli určit optimální variantu.

KLÍČOVÁ SLOVA

Pojištění, kybernetická rizika, kybernetická bezpečnost, kybernetické útoky, kybernetický prostor, malware, vícekriteriální rozhodování

TITLE

Cyber Risk Insurance

ANNOTATION

This bachelor thesis focuses on the problem of cyber risks and their insurance. The aim of this thesis is to select the best insurance product using multi-criteria decision making methods. First, we will introduce terminology that will help us to better understand cyber risks, and then we will introduce insurance and some of its concepts that will help us to understand the different offerings of insurance companies. In order to select an alternative, we will define a set of criteria, determine their importance and evaluate them with respect to each alternative. Finally we utilize one of the methods for evaluating alternatives to be able to determine the optimal variant.

KEYWORDS

Insurance, cyber risks, cyber security, cyber attacks, cyber space, malware, multi-criteria decision-making

OBSAH

SEZNAM ILUSTRACÍ

SEZNAM TABULEK

Seznam zkratek

AI	Artificial Intelligence
apod.	a podobně
atd.	a tak dále
CSIRT	Computer Security Incident Response Team
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability
ČR	Česká republika
DDoS	Distributed Denial of Service
DoS	Denial of Service
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IT	Inofrmation Technonlgy
MCDM	Multi-Criteria-Decision-Making
Např.	Například
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PCI-DSS	Payment Card Industry – Data Security Standard
PR	Public Relations
SIEM	Security Information and Event Management
tj.	to je
USD	United States Dollar

ÚVOD

V dnešním světě téměř každá firma, ať už malá, střední nebo velká, zařazuje počítače do svých každodenních obchodních aktivit, což většinou znamená používání internetu nebo nějaké formy sociálních sítí, jež firmě umožňuje sdílet informace mezi různými odděleními, ukládat a analyzovat informace, zpracovávat platby, spravovat zdroje, marketing nebo řadu dalších aktivit, které vyžadují počítače.

Proto mohou aktéři se zlými úmysly, jako jsou hackeři, ale nejen ti, představovat obrovskou hrozbu pro společnost a její zdroje. Mohou krást informace, manipulovat s nimi nebo bránit v přístupu k nim, což může společnosti způsobit obrovské finanční ztráty v mnoha formách, o kterých budeme hovořit v této práci. Kromě hackerů může finanční ztráty společnosti způsobit mnoho dalších faktorů, hrozby mohou pocházet zevnitř, nebo zvenčí, mohou být úmyslné, nebo neúmyslné, způsobené člověkem nebo přírodními katastrofami atd.

Vzhledem k rostoucí závažnosti a četnosti výskytu kybernetických rizik je nutné, aby se společnosti před těmito riziky chránily. Eliminovat dopady kybernetických útoků umožňuje efektivní pojištění.

V teoretické části této práci představíme problém kybernetických rizik, vysvětlíme různé typy hrozeb, kterým jsou společnosti vystaveny, poté vysvětlíme význam pojištění kybernetických rizik a pojištění. V praktické části zhodnotíme současné produkty pojištění kybernetických rizik dostupné na trhu pro podniky a k tomu použijeme metodu rozhodování na základě více kritérií k určení nejlepšího pojistného produktu s ohledem na vybraný seznam kritérií.

Abychom určili kritéria z pohledu reálného světa, na začátku praktické části této práce přezkoumáme reálnou středně velkou společnost, která si přála pro účely této práce zůstat anonymní. Poskytla nám však obecný přehled o rizicích, kterým je vystavena, což nám pomůže stanovit kritéria pro multikriteriální rozhodovací analýzu.

1 Úvod do problematiky kybernetických rizik

1.1. Základní pojmy

Každý rok je v České republice spácháno tisíce kybernetických trestných činů, ne všechny souvisejí s podnikatelskou činností, nicméně kyberprostor se každým dnem stává stále nebezpečnějším, což je jasně patrné z údajů českých policejních orgánů, NÚKIB a údajů zveřejněných na zdrojích jako Statista, které si probereme v další kapitole.

Nejprve je důležité vysvětlit některé pojmy týkající se kybernetických rizik, aby nám pomohly lépe porozumět problematice kybernetických rizik.

Hrozba

Hrozba je potenciální příčinou nežádoucích incidentů souvisejících s kyberprostorem, které mohou poškodit systém nebo organizaci a jsou způsobeny kybernetickými riziky.

Riziko

Riziko je možnost, že hrozba využije zranitelnost aktiva a způsobí na něm škodu.

Útok

Pokus o zničení, vystavení hrozbě, změnu nebo krádež aktiva nebo získání neoprávněného přístupu k aktivu či neoprávněné použití aktiva.

Kyber

Přívlastek kyber pochází z angličtiny (Cyber) a je používán v souvislosti s počítači a počítačovými sítěmi [7].

Kyberprostor

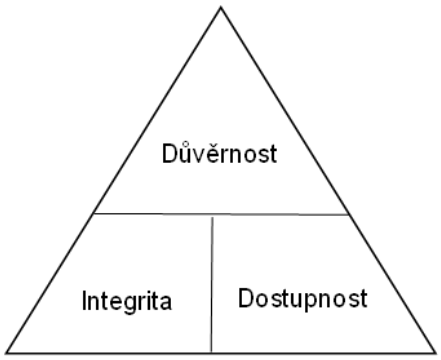
Virtuální prostor je tvořený internetem a připojenými počítačovými sítěmi, systémy a dalšími digitálními zařízeními a službami. Poskytuje obchodním organizacím potřebný prostor pro komunikaci a široké spektrum obchodních aktivit.

Kybernetická bezpečnost

Je ochrana počítače a počítačové sítě před útoky pocházející z kyberprostoru.

1.2. CIA triáda

Kyberbezpečnost požaduje striktní dodržování několika pilířů známých jako CIA triáda kybernetické bezpečnosti. Tyto pilíře jsou cíle kybernetické bezpečnosti, což je zajištění. Dostupnost počítače a počítačové sítě a další dva pilíře jsou spojené s daty a informacemi, zajišťují její důvěrnost a integritu. Tyto pojmy krátce vysvětlíme.



Obrázek: 1 CIA triáda

Zdroj: vlastní zpracování

V obrázku 1 vidíme triádu CIA, kterou tvoří:

Důvěrnost (Confidentiality): znamená, že data by měla být sdílena a zpřístupněna pouze mezi oprávněnými osobami.

Integritu (Integrity): znamená, že je zajištěno, že data jsou aktuální, úplná a nedošlo k jejich modifikaci.

Dostupnost (Availability): To znamená, že data jsou na požádání přístupná oprávněné osobě.

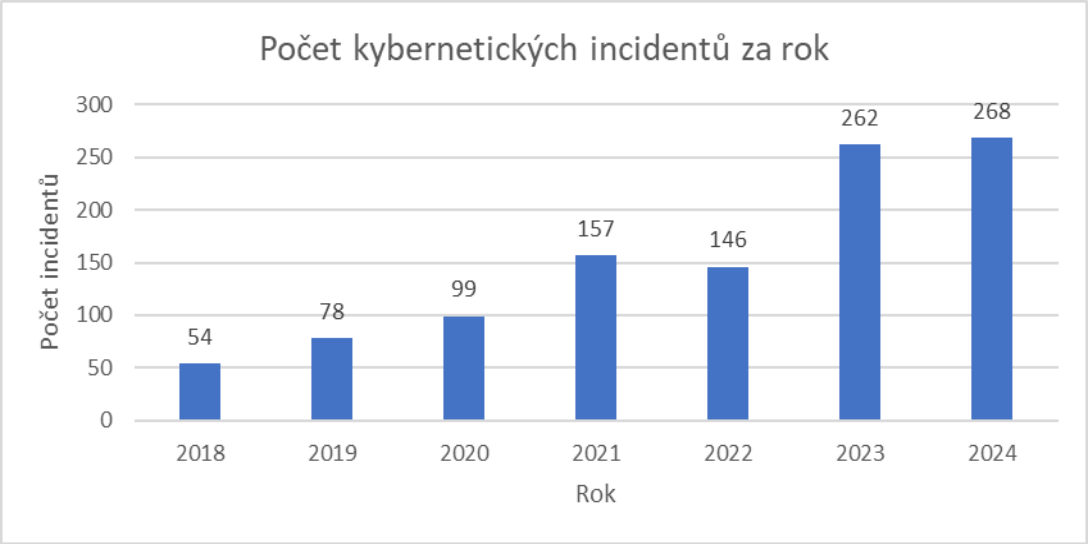
1.3. Stav kybernetické bezpečnosti v České republice

1.3.1. Kybernetické útoky v ČR podle dat NÚKIB

Abychom pochopili situaci v oblasti kybernetických rizik v České republice, prozkoumáme data z nejnovější výroční zprávy NUKIB z let 2024 a 2023 a data ze Statista. Nejprve představíme zdroje dat a nastíníme jejich typy, jež zaznamenávají konkrétní informace, které shromažďují a považují je za relevantní.

NÚKIB je Národní úřad pro kybernetickou a informační bezpečnost, ústřední správní úřad pro kybernetickou bezpečnost, včetně ochrany utajovaných informací v informačních a komunikačních systémech a kryptografické ochrany (NÚKIB 2025).

Způsob, jakým se NÚKIB popisuje jako organizace, naznačuje, že nesleduje všechny incidenty, ale spíše ty, které spadají do její pravomoci, takže počet hlášených incidentů bude výrazně nižší, protože se na rozdíl od jiných zdrojů zaměřuje hlavně na vybraný okruh incidentů, jak uvidíme dále.



Obrázek: 2 Počet kybernetických incidentů za rok podle NÚKIB

Zdroj: vlastní zpracování na základě [13]

Na obrázku 2 vidíme, že ačkoli mezi lety 2020 a 2024 zaznamenáváme výrazný nárůst počtu incidentů, a to o 170 %, bylo v roce 2024 podle NÚKIB v České republice zaznamenáno 268 incidentů, což je 2% nárůst oproti předchozímu roku. To naznačuje, že tempo růstu bylo mezi těmito dvěma roky stabilní, ale nemáme dostatek dat, abychom mohli posoudit, zda zůstane stabilní i nadále.

Největší část těchto incidentů v roce 2023 a 2024 byly DDoS (Distributed Denial of service) – útoky skupiny známé jako NoName057, která vedla DDoS útoky proti České republice, jež zapříčinily výpadky některých webových stránek, ale nezpůsobily skutečné škody [13].

Stejná skupina vedla další útoky DDoS proti dalším zemím Evropské unie.

V prosinci 2023 došlo meziročně k nárůstu o 33 %. Podle přehledu kybernetických hrozeb za rok 2023 bylo nejvíce útoků vedeno v následujících kategoriích:

1. Phishing – 53 %
2. Scanning – 28 %
3. Podvodný e-mail – 17 %

4. Jiné – 12 %

5. Škodlivý obsah – 10 %

6. Spear-phishing – 7 %

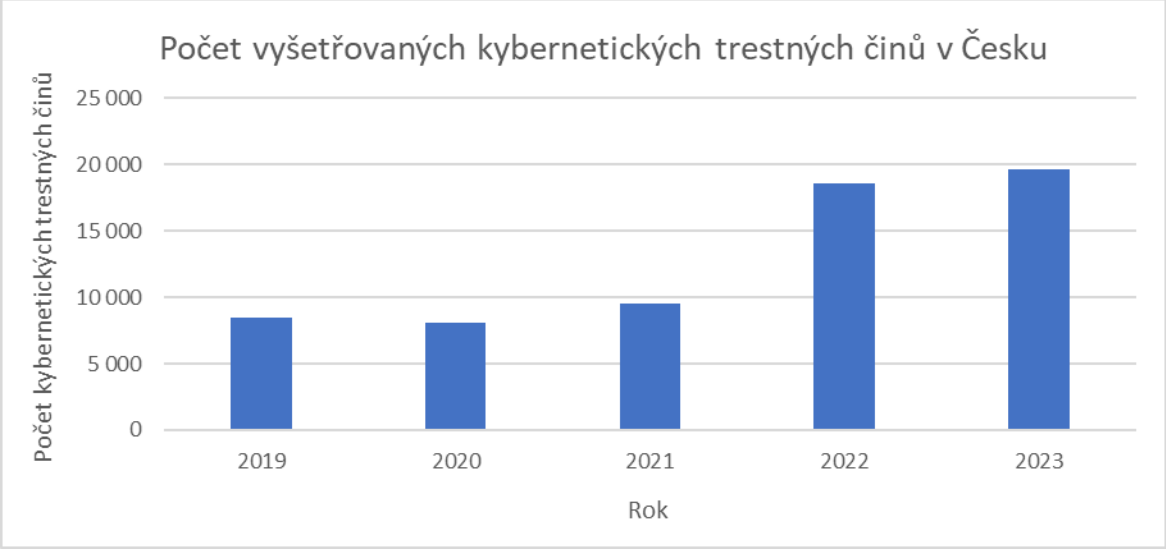
1.3.1.1. Hlavní aktéři

Zpráva o stavu kybernetické bezpečnosti v České republice pro rok 2023 uvádí 4 hlavní aktéry: Rusko, Čína, Severní Korea a Írán.

Zpráva zmiňuje, že útoky ze strany Ruska byly součástí dlouhodobé kampaně proti České republice a spojencům, stejně tak útoky ze strany Číny a severní Koreje, nicméně do detailů těchto útoků nebudeme pronikat, protože se netýkaly podniku, ale spíše byly zaměřeny na vojenské a vládní organizace. Útoky ze strany Íránu byly zaměřeny na vodohospodářské systémy v České republice [13].

1.3.2. Kybernetické útoky v ČR podle dat Statista

Statista je online platforma pro data a obchodní informace, založená v Německu v roce 2007. Obsahuje rozsáhlou sbírku statistik, zpráv a analýz na širokou škálu témat z různých zdrojů. Některé zprávy jsou k dispozici zdarma, zatímco jiné zprávy a další funkce vyžadují předplatné.



Obrázek: 3 Počet vyšetřovaných kybernetických trestných činů v Česku podle Statista

Zdroj: vlastní zpracování na základě [27]

Na obrázku 3 vidíme data ze Statista na základě dat od České policie. Vidíme, že počet kybernetických trestných činů má vzestupnou tendenci. Vzrostl z 8 417 v roce 2019 na 19 592 v roce 2023, což představuje nárůst o 132,8 %.

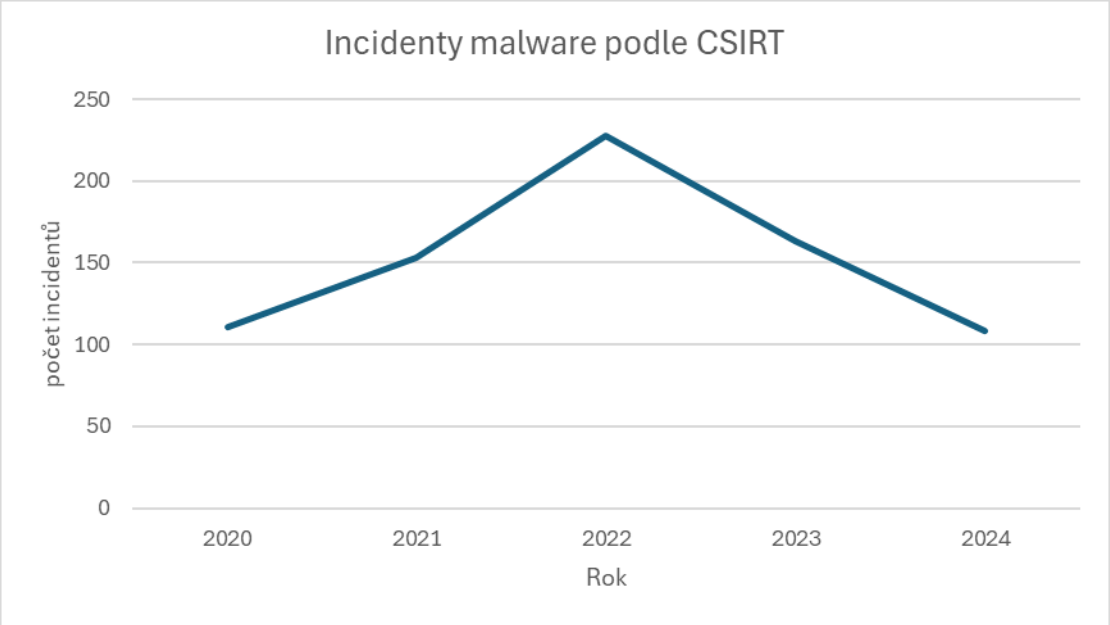
1.3.3. Kybernetické útoky v ČR podle dat CSIRT

Další organizací, která informuje o incidentech v oblasti kybernetické bezpečnosti v České republice, je CSIRT.

CSIRT je akronym pro anglický výraz „Computer Security Incident Response Team“.

CSIRT.CZ je český tým CSIRT a je to organizace, která v koordinaci s CERT „Computer Emergency Response Team“ řeší bezpečnostní incidenty vzniklé v počítačových sítích, koordinují jejich řešení a snaží se jim předcházet. [18]

Každý rok zveřejňuje výroční zprávu o incidentech, které řešila, včetně malwaru, DoS útoků, spamu a dalších incidentů souvisejících s počítačovými sítěmi.



Obrázek: 4 Počet incidentů Malware za rok podle CSIRT

Zdroj: vlastní zpracování na základě [12]

Jak vidíme z obrázku 4, počet incidentů souvisejících s malwarem, které řešila organizace CSIRT, klesl z maxima 228 v roce 2022 zpět na 108 v roce 2024, což je přibližně stejná úroveň jako v roce 2020. Je však důležité zdůraznit, že organizace CSIRT sleduje hlavně incidenty související se síťovými senzory a phishing [21].

1.4.Hrozby

V kyberprostoru existuje široká škála hrozeb. V této kapitole se zmíníme o některém z nejčastějších a nejvýznamnějších hrozeb, které byly zdrojem škod a finančních ztrát pro mnoho subjektů. Jedná se o hrozby jako malware, DDoS, phishing a ransomware. Skutečný

rozsah hrozeb a metod provádění kybernetických útoků pomocí těchto hrozeb je příliš velký a komplexní na to, aby mohl být zahrnut do této práce.

1.4.1. Malware

Malwarem rozumíme jakýkoliv škodlivý software. Většina malwaru se dokáže skrýt a být odolná i přes restartování počítače, to znamená, že dokáže pokračovat ve fungování a restartování nepřerušuje jeho běh.

Příkladem malwaru může být např: malware typu Drive-by download, trojské koně, viry, spyware, scareware, ransomware, adware, backdoor a logická bomba.

Drive-by downaload malware je typ malwaru, kdy uživatel nemusí nic stahovat, aby byl malwarem ovlivněn, malware stahuje svůj kód na pozadí při pouhém prohlížení webových stránek, využívá zastaralý broswer, aplikaci nebo operační systém [30].

Příklady malwaru jsou:

Trojské koně: jsou typem malwaru, který je maskován jako legální software, po stažení se škodlivý kód spustí v zařízení uživatele. Existují různé typy trojských koní, včetně rootkitů, trojských zadních vrátek, špionážních trojských koní apod. [29].

Viry: jsou dnes chápány jako jakýkoli škodlivý kód nebo software, který může způsobit poškození uživatelského zařízení, nicméně abychom byli konkrétnější, počítačové viry jsou podobné biologickým virům, infikují zařízení, replikují se a šíří do dalších zařízení [11].

Adware: je obecně typ reklamy, obvykle vyskakovací okno, které se zobrazuje v rozhraní prohlížeče uživatele, nebo pokud je staženo, v rozhraní systému. Cílem adwaru je typicky vytvářet příjmy, a to buď generováním prokliků, nebo hromaděním marketingových údajů, které chtějí aktéři později využít k analýze toho, jaké webové stránky uživatel obvykle navštěvuje, aby na něj mohli cílit relevantnější reklamy [8].

Příkladem adwaru mohou být vyskakovací reklamy, plovoucí reklamy a falešné bannery.

1.4.2. DDoS

DDoS je zkratka pro distributed denial of service a podle souhrnné zprávy NUKIB se jedná o nejčastější útok v České republice. Jedná se o dva hlavní typy útoků, a to objemové a aplikační.

DDoS útoky jsou specifické tím, že si útočník může pronajmout botnet (zombie počítač), s jehož pomocí posílá na server nebo webovou stránku obrovské množství požadavků, které by pak vedly k jejímu zpomalení nebo úplnému zastavení.

Provést takový útok je relativně velmi snadné, protože pronájem 1000 zombie počítačů může např. v Rusku stát kolem 25 USD.

Nejčastějším typem těchto útoků jsou útoky na vládní organizace, jejichž hlavním cílem je zastavit provoz webových stránek těchto organizací a v důsledku toho přestat poskytovat služby veřejnosti.

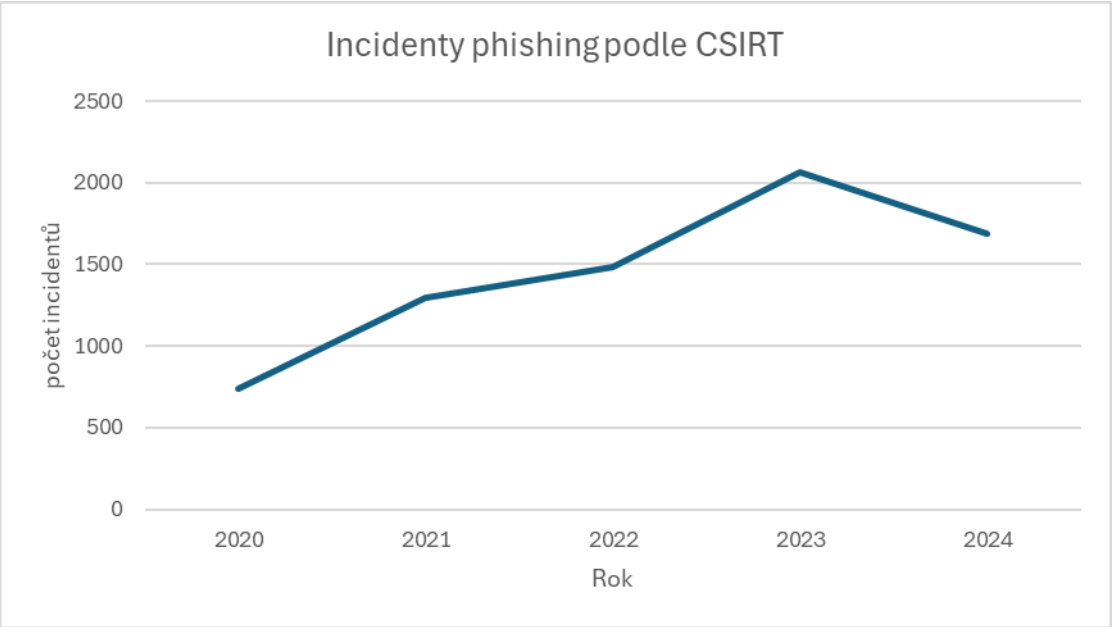
Horším typem útoků DDoS jsou útoky na síťovou infrastrukturu země jako celku, které mohou vést k výpadkům postihujícím soukromý sektor.

Takové útoky mohou provádět také obchodní konkurenti, například pokud podnikatel provede útok DDoS na hostingový server e-shopu, může ovlivnit velký počet konkurentů najednou, čímž přenese provoz a tržby na sebe a způsobí konkurentům ztráty.

Takové útoky mohou subjektu způsobit řadu ztrát, např.: finanční ztráty, sankce kvůli smlouvám, ztrátu návštěvníků, negativní publicitu, ztrátu produktivity, výpadek bankovních služeb, výpadek vládních služeb.

1.4.3. Phishing

Phising jsou podvodné e-maily, textové zprávy, telefonáty, e-maily, někdy i pošta, jejichž cílem je vylákat od lidí citlivé údaje. Phisihing využívá sociální inženýrství k přesvědčení nebo nátlaku na oběť, aby tyto informace sdílela. Na rozdíl od útoků, které se přímo zaměřují na infrastrukturu, Phising spoléhá na lidskou chybu [31].



Obrázek: 5 Počet incidentů Phishingu za rok podle CSIRT

Zdroj: vlastní zpracování na základě [12]

Na obrázku 5 vidíme, že počet případů phishingu, které řešila organizace CSIRT.CZ, vzrostl ze 738 v roce 2020 na 1690 v roce 2024, což představuje nárůst o 129 %. Ačkoli mezi lety 2023 a 2024 došlo k mírnému poklesu, nárůst za posledních 5 let byl významný.

Hackeři se obvykle vydávají za důvěryhodný zdroj, kolegu nebo autoritu. Pomocí sociálního inženýrství zneužívají lidskou důvěru nebo strach, aby přiměli oběť sdílet informace, kliknout na odkaz, stáhnout přílohu nebo zaplatit fakturu.

Některé trendy a techniky phisingu: Spear-phishing, Vishing, Whaling a Deepfake AI.

Spear-phising: Je z anglického slova spear (kopí) a je zaměřen na určitou skupinu nebo určité jednotlivce s cílem získat přístup k finančním informacím nebo specializovaným databázím. Na rozdíl od phishingu, který lze provádět hromadně a používá obecný tón, může spear-phishing měnit tón a přístup, aby byl pro daný cíl přesvědčivější.

Vishing: Je hlasový phising, spočívá v telefonování cílům, využívá prvek překvapení a naléhavosti, aby přesvědčil tagert o určitém postupu, například předstírá, že je osoba v nouzi, nebo předstírá, že je banka, aby získal přístup k finančním informacím nebo požádal o platby.

Deepfake AI: Využívá rychle se rozvíjející technologie umělé inteligence, aby přesvědčila cíl k určitému jednání, například k převodu peněz, metody se mění každý den, protože se neustále vyvíjejí nové technologie, jako jsou falešné fotografie, videa nebo klonování hlasu [9].

1.4.4. Ransomware

Ransomware byl široce chápán jako malware, který šifruje soubory, avšak s vývojem se začal vnímat jako malware, který uzamkne počítač nebo obrazovku oběti, znemožní přístup a požaduje platbu za navrácení přístupu k zařízení.

V roce 2023 dosáhly celkové platby za ransomware v celosvětovém měřítku 1,1 miliardy dolarů, což je dvojnásobek oproti předchozímu roku a ukazuje to na rostoucí trend [28].

Hrozba útoku závisí na sofistikovanosti použitého ransomwaru, v některých případech lze například soubory zašifrované pomocí ransomwaru CryptoLocker odšifrovat pomocí nástrojů, jako je nástroj vývojáře FOX IT a FireEye.

2. Vysvětlení významu pojištění kybernetických rizik

2.1. Riziko

Riziko je pojem, který označuje možnost vzniku události, která může mít negativní důsledky. V našem případě hovoříme o pravděpodobnosti, že hrozba může nastat a ovlivnit finance nebo každodenní fungování společnosti.

Řízení rizik se stává nezbytností, protože hraje klíčovou roli při identifikaci a včasném odhalování hrozeb a určování, zda představují riziko dříve, než se z nich stane skutečný incident.

2.1.1. Kybernetická rizika

Pokud je ohroženo digitální médium společnosti, jako jsou počítačové systémy, síťové systémy, platební systémy, kamery nebo jakékoli jiné digitální médium, hovoříme o kybernetickém riziku. Útočník může tyto systémy zneužít, přerušit jejich funkci nebo získat přístup k jejich datům. Tato rizika mohou být úmyslná ze strany hackera nebo útočníka, stejně jako neúmyslná v důsledku systémových chyb nebo lidské chyby.

Jak již bylo zmíněno, některá z těchto rizik mohou být například: únik dat, malware, phishing a DDoS útoky.

2.2. Ochrana před kybernetickými riziky

Postupem času se zvyšuje závažnost dopadů, frekvence výskytu i sofistikovanost provedení kybernetických hrozeb. Je tedy mimořádně důležité se před nimi chránit. Tato ochrana musí být soustavná a průběžně aktualizovaná. Mezi základní možnosti ochrany před kybernetickými riziky patří:

Základní technická opatření

Řadě kybernetických útoků je možné předcházet používáním základních technických opatření, mezi která patří:

- Antivirový software a firewall – chrání před malwarem a neoprávněným přístupem.
- Pravidelná aktualizace systémů a aplikací – aktualizace opravují bezpečnostní chyby.
- Používání silných a unikátních hesel a jejich pravidelná obměna.
- Dvoufaktorové ověření při přihlašování do systému.

Bezpečnostní povědomí

Vzhledem k tomu, že složitost kybernetických hrozeb stále roste, je třeba udržovat si a rozšiřovat si povědomí o nových typech útoků a možnostech, jak se jim bránit. Do této kategorie můžeme zařadit například tato opatření:

- Školení a osvěta – znát rizika phishingu, sociálního inženýrství apod.
- Ověřování e-mailových adres a odkazů – vždy kontrolovat adresu, ze které e-mail přišel, neklikat na podezřelé odkazy, neotevírat podezřelé přílohy.
- Bezpečné chování na internetu – nepoužívat veřejné nezabezpečené Wi-fi připojení pro citlivé operace.

Organizační a právní opatření

Pro společnosti je důležité mít stanovená i základní organizační a právní opatření a důsledně vyžadovat jejich dodržování. Jedná se zejména o tato opatření:

- Pravidelné zálohování dat – chrání před jejich ztrátou např. při ransomwaru.
- Právní soulad (např. GDPR) – ochrana osobních údajů a dodržování legislativy.
- Bezpečnostní politika – jasně daná srozumitelná pravidla pro práci s daty a technologiemi.

Pokročilé technologie

- Šifrování dat při přenosu i ukládání.
- SIEM systémy – pro monitoring a analýzu bezpečnostních událostí.
- Penetrační testování – simulace útoků pro odhalení slabin.

Pojištění

Pojištění samo o sobě nemůže samozřejmě chránit před výskytem kybernetických rizik, může ale zmírnit jejich dopad na pojištěného. Pojištění kybernetických rizik je proto hlavním tématem této práce.

2.3. Pojištění

Po seznámení se s riziky v kyberprostoru je pro společnost důležité, aby se dokázala chránit před finančními dopady, které mohou taková riziky způsobit. K ochraně před finančními

dopady těchto hrozeb může společnost využít vlastní zdroje, nebo může riziko přenést na třetí stranu, která se postará o kompenzaci finančních dopadů. V tomto případě hovoříme o pojištění kybernetických rizik.

Nejprve je důležité vysvětlit některé základní pojmy související s pojištěním, jako například co je pojištění, pojistitel, pojistník, pojistné a další pojmy.[2]

Pojištění: Nástroj používaný pro eliminaci finanční odpovědnosti nebo negativních důsledků nahodilosti.

Pojistitel: Pojišťovna, instituce nebo obecně právnická osoba, která má oprávněni provozovat pojištění. Potřebuje k tomu povolení k provozování pojištění.

Pojistník: Osoba (Fyzická nebo právnická), která uzavřela pojistnou smlouvu s pojistitelem a která se ve smlouvě zavázala platit pojistné za pojistnou ochranu.

Pojištěný: Osoba, která získává na základě uzavřené pojistné smlouvy právo na pojistné plnění, a to bez ohledu na to, jestli pojištění objedná sama, nebo jiná osoba (pojistník).

Pojistná smlouva: Právní dokument, který vzniká mezi pojistitelem a pojistníkem a na jeho základě vzniká pojištění.

Pojistné: Cena pojištění.

2.3.1. Členění pojištění

Pojištění jako pojem může odkazovat na více typů pojištění, z hlediska právního je rozdělení na: pojištění dobrovolné a pojištění povinné. Dále můžeme specifikovat různé druhy jako např. sociální a komerční, které se dělí na životní a neživotní.

Rozsah krytí neživotního pojištění se dá ještě dělit podle krytí na krytí:

rizika vztahujících se k osobám, majetková rizika, rizika související s finančními ztrátami a rizika spojená s odpovědností za škodu.

2.3.2. Pojištění kybernetických rizik

Pojištění kybernetických rizik je speciální typ pojištění, který v sobě skrývá více druhů pojištění jako majetkové, odpovědnost za škodu a finanční ztráty. Jeho cílem je chránit podniky proti kybernetickým útokům, nahodilostem a jejich důsledkům bud přímo na podnik nebo třetí stranu.

Existuje několik pojišťoven, které nabízí produkty zaměřené na kybernetická rizika, však ne všechny jejich produkty jsou určené pro podniky, některé pojistné produkty jsou určené pro fyzické osoby. V dalším kapitole se budeme představovat 3 pojistným produktům, které jsou určené pro podniky různých velikostí.

2.4. Rozvoj trhu pojištění kybernetických rizik

Pojišťovací trh v České republice v posledních letech výrazně vzrostl. Jen v roce 2024 zaznamenal růst o 8,13 %. [32]

Počet pojistných událostí souvisejících s pojištěním majetku, které pojišťovny vyplatily, se zvýšil o 127 %. Pojištění kybernetických rizik nebylo v této zprávě zvlášť zdůrazněno, ale je považováno za zvláštní druh pojištění, které zahrnuje i pojištění majetku.[32]

Trh kybernetické bezpečnosti v České republice navíc do roku 2029 očekává roční růst tržeb o 7,35 %, což naznačuje rostoucí potřebu kybernetických řešení, kybernetických rizik a nebezpečí.[14]

Zpráva zveřejněná v roce 2018 zdůrazňuje, že český trh byl v oblasti pojištění kybernetických rizik stále nováčkem a pouze několik společností nabízelo omezená řešení, která nebyla zaměřena na podniky, ale spíše na jednotlivce a jejich každodenní používání internetu. Po zavedení zákona GDPR v roce 2018 reagovaly pojišťovny na tento zákon uvedením pojistných produktů, které mají za cíl zmírnit finanční dopady kybernetických rizik. Jednou ze společností, která výslovně zdůrazňuje, že její produkt je reakcí na zavedení GDPR, je pojišťovna Maxima, kterou budeme mít možnost podrobně analyzovat v následujících kapitolách. [15]

2.4.1. Regulační faktory a požadavky na dodržování předpisů

S nárůstem rizik se zavádí více regulačních zákonů a zákonů o dodržování předpisů. Cílem těchto zákonů je chránit jak kontinuitu podnikání, tak práva a soukromí jednotlivců.

Mezi takové zákony patří **GDPR**, které v České republice vstoupilo v platnost v květnu 2025 a jehož cílem je chránit soukromí a údaje fyzických osob. Pojišťovny mohou nabídnout řešení pro zmírnění finančních ztrát vzniklých v důsledku nedodržení GDPR.

Dalším zákonem, který byl zaveden, je **NIS2**, jenž vstoupil v platnost v říjnu 2024. Zavedení tohoto zákona bylo řízeno NÚKIB. V tomto zákoně se počet společností, které podléhají zvýšeným bezpečnostním opatřením, zvýšil ze 400 na 6000. Tato opatření zahrnují především bezpečnost dodavatelského řetězce a bezpečnost dostupnosti služeb.

V neposlední řadě je třeba zmínit zákon **DORA**, který vstoupil v platnost letos 17. ledna 2025. Zákon DORA zavedl nové povinnosti v oblasti řízení rizik ICT, hlášení incidentů, testování digitální provozní odolnosti a řízení rizik při spolupráci s poskytovateli ict. zákon se týká široké škály podnikatelských subjektů. [16,17]

2.5.Shrnutí

Na základě toho, co jsme si ukázali v první kapitole, je patrné, že rizika jsou na vzestupu, s novými technologiemi a prudkým nárůstem umělé inteligence je stále obtížnější bojovat s hrozbami, které zvyšují rizika kybernetických incidentů a finančních ztrát. Český trh začal na tyto rostoucí změny v kybernetické bezpečnosti reagovat teprve nedávno, a to zaváděním nových zákonů a nových regulatorních a compliance požadavků na podnikatelské subjekty. České pojišťovny začaly na tyto změny reagovat také až po zavedení těchto zákonů. V tomto velmi dynamickém prostředí je role pojištění kybernetických rizik stále zřejmější pro společnosti, které chtějí zajistit kontinuitu a nepřerušenou podnikatelskou činnost, aniž by se musely obávat dopadů kybernetických rizik na ně. Pro tyto společnosti je však důležité správně identifikovat rizika, která mohou z těchto hrozeb vyplynout, a předem přijmout správná opatření, aby bylo zajištěno nastavení správných kritérií pro výběr optimálního pojistného produktu.

3. Vícekriteriální rozhodování

3.1. Teorie vícekriteriálního rozhodování

Vícekriteriální rozhodování (anglicky Multi-Criteria Decision Making – MCDM) je metoda používaná k výběru nejlepší varianty z několika možností, kdy je třeba zohlednit více různých kritérií. Je velmi užitečná v situacích, kdy rozhodnutí není jednoznačné a každá alternativa má své výhody i nevýhody.

Rozhodovací problém je situace, kdy je třeba zvolit jednu nebo více variant z množiny dostupných možností na základě určitých kritérií a podmínek. Typicky se vyskytuje v managementu, ekonomii, technice, ale i v běžném životě.

Základní prvky rozhodovacího problému

Cíl rozhodování

Cíl, kterého se snažíme dosáhnout na základě analýzy (např. vybrat nejlepší variantu)

Alternativy (varianty)

Možnosti, mezi kterými se rozhodujeme (např. různé pojistné produkty).

Kritéria hodnocení

Podle čeho hodnotíme alternativy (např. cena, reputace, rozsah, riziko).

Omezení

Podmínky, které musí být splněny (např. rozpočet, čas, technické limity).

Rozhodovatel

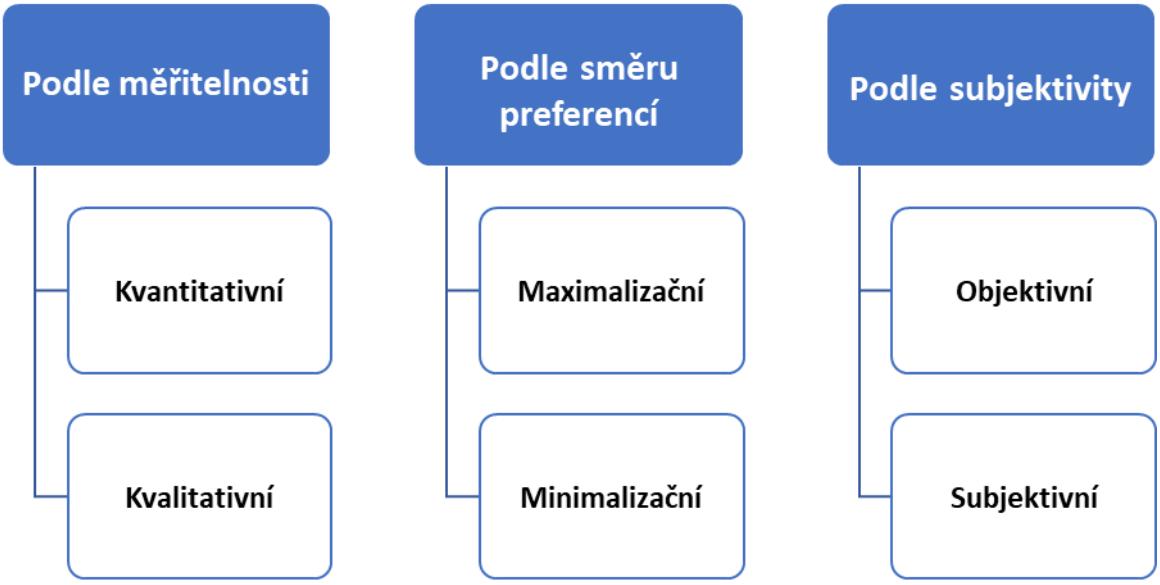
Osoba nebo skupina, která rozhodnutí činí.

Prostředí rozhodování

- **Určité** – známe jaké budou důsledky rozhodnutí.
- **Rizikové** – známe pravděpodobnosti výsledků.
- **Neurčité** – nemáme dostatek informací o výsledcích.

Klasifikace rozhodovacích kritérií:

Typy kritérií v rozhodovacím procesu lze rozdělit podle různých hledisek. Zde je přehled nejčastějších typů kritérií, která se používají při hodnocení alternativ:



Obrázek: 6 Klasifikace rozhodovacích kritérií

Zdroj: vlastní zpracování

Podle měřitelnosti

- **Kvantitativní kritéria** – Jsou měřitelná čísly (např. cena)
- **Kvalitativní kritéria** – Jsou subjektivní nebo slovní (např. spokojenost zákazníků)

Podle směru preferencí

- **Maximalizační kritéria** – Čím vyšší hodnota, tím lepší (např. kvalita).
- **Minimalizační kritéria** – Čím nižší hodnota, tím lepší (např. náklady).

Podle subjektivity

- **Objektivní kritéria** – Založená na faktech a datech (např. počet reklamací).
- **Subjektivní kritéria** – Založená na osobním názoru nebo vnímání (např. důvěra, image firmy).

Při vícekriteriálním rozhodování hledáme optimální variantu s ohledem na více atributů.

Váha kritérií může být popsána jako důležitost kritérii. Čím vyšší je váha kritéria, tím větší je jeho význam. Je důležité normovat váhu kritérií, aby bylo možné dosáhnout vzájemné porovnatelnosti mezi kritérii.

Existuje mnoho způsobů, jak nastavit váhu kritérií. A jsou hlavně rozdělené do metody se znalostí důsledků variant a metody bez znalosti důsledků variant. Metody bez znalosti důsledků variant se rozdělují na metody přímé a nepřímé. Během uplatnění přímé metody stanovení vah kritérii není potřeba normovat váhu kritérií, ale je to potřeba u nepřímé metody. K normování vah používáme následující vzorec:

Rovnice 1 Normalizace vah

$$v_i = nv / \sum_{j=1}^{m} nv_j \, , pro \; i \; a \; j = 1,2, \dots , m$$

Zdroj:[19]

Kde v_i je normovaná váha a nv je nenormovaná váha i-teho kritéria, m je počet těchto kritérii.

Metodou, kterou jsme zvolili pro stanovení váhy kritérií v této bakalářské práci, bude Fullerova metoda pro párové srovnání (Fullerova trojúhelník) [20].

3.2.Fullerova metoda

Spadá pod „metody bez znalosti důsledků variant“ a jedná se o nepřímou metodu. V této metodě musíme porovnat důležitost každého kritéria s ohledem na všechna ostatní kritéria v rámci rozhodovacího problému.

A toto porovnání provedeme tak, že spočítáme počet preferencí pro každé kritérium, tj. počet 1 v řádku a počet 0 ve sloupci. Následně normalizujeme váhy podle:

Rovnice 3 Normalizace vah podle počtu preferencí

$$v_i = \frac{f_i}{m(m-1) \; / \; 2}$$

Zdroj:[19]

Kde: f_i je počet preferencí kritérií; m je počet kritérií a $m(m-1) \; / \; 2$ je počet uskutečněných srovnání kritérií.

Podle tohoto vzorce vypočítáme celkovou váhu a vydělíme jí jednotlivé váhy, abychom získali normalizovanou váhu, avšak tato metoda nebere v úvahu situace, kdy máme kritérium s 0 preferencemi, což neznamená, že má pro nás nulový význam. Při použití této metody bychom 0 dělili celkovou váhou vypočtenou podle vzorce, což by vedlo k 0 relevantnímu

významu. Abychom to obešli, použijeme modifikaci vah přidáním 1 do sloupce s počtem preferencí, aby se zabránilo případům 0 preferencí.

Použitím této metody zajistíme odstranění jakéhokoli součtu 0 preferencí a získáme skutečný vliv kritéria.

V případech, kdy máme podobnou důležitost kritérií, přičteme 5, abychom vyjádřili stejnou důležitost. Pak přičteme k součtu počet preferencí.

Toto jsou kroky, které se používají při aplikaci Fullerovy metody pro stanovení vah kritérií, nicméně po provedení těchto kroků nám zbývá ještě metoda, kterou budeme moci vybrat optimální variantu. Dále si vysvětlíme metodu, kterou jsme pro tento účel zvolili, a to metodu vážených součtů.

3.3. Metoda váženého součtu

Abychom určili optimální variantu, musíme mluvit o užitku. Existují dva typy kritérií, maximalizační a minimalizační. Maximalizační typ znamená, že s růstem hodnoty daného kritéria získáváme větší užitek, takže čím více, tím lépe. Minimalizační typ je naopak. Vyšší hodnota představuje menší přínos. U většiny rozhodovacích metod je nutné, aby všechna použitá kritéria byla stejného typu, vyžaduje to i metoda váženého součtu, obvykle se minimalizační kritéria převádějí na maximalizační. Abychom eliminovali vliv různých jednotek u hodnot jednotlivých kritérií, obvykle se provádí tzv. standardizace.

Metoda určení optimální varianty spočívá v použití stejných kroků jako u Fullerovy metody pro určení vah kritérií, pouze tentokrát vytvoříme matici pro každé jednotlivé kritérium, abychom ohodnotili kritérium z hlediska příslušných variant. Tímto krokem můžeme vypočítat dílčí ohodnocení, které bude použito v dalším kroku pro určení optimální varianty.

Posledním krokem je vynásobení dílčího hodnocení každého kritéria vzhledem k příslušným variantám vypočtenou váhou kritérií vypočtenou dříve pomocí Fullerovy metody.

Výsledky porovnáme a za optimální variantu považujeme variantu s nejvyšším ohodnocením, je to varianta s nejvyšším H^j podle vzorce:

Rovnice 4 Ohodnocení variant

$$H^j = \sum_{i=1}^{m} \left(v_i \cdot h_i^j\right)$$

Zdroj:[19]

Kde: v_i je váha kritéria pro i = 1, 2, …, m.

h_i^j je ohodnocení variant pro dané kritérium.

4. Nabídka pojištění kybernetických rizik

Poskytovatelé pojištění obvykle nabízejí řadu produktů přizpůsobených různým rizikovým profilům. Ty mohou zahrnovat krytí úniku dat, kybernetického vydírání, odpovědnosti za bezpečnost sítě a další. Je důležité porovnat podmínky, limity krytí, výluky a pojistné různých pojistek, abyste našli tu, která nejlépe vyhovuje potřebám společnosti.

Při zkoumání českého trhu pojišťoven je možné najít například ČSOB, Maxima a Colonnade. Pro účely této bakalářské práce budeme představovat a porovnávat všechny uvedené pojišťovny.

4.1. ČSOB

ČSOB Pojišťovna, a. s., člen holdingu ČSOB (dále jen ČSOB Pojišťovna) je univerzální pojišťovna, která nabízí ucelené pojišťovací služby občanům a živnostníkům stejně jako malým a středním podnikům i velkým korporacím. Poskytne služby v oblasti životního i neživotního pojištění.

ČSOB nabízí pojištění kybernetických rizik pod názvem Pojištění kybernetických rizik. Pojištění se vztahuje na:

Narušení ochrany dat: Nabízejí krytí finančních ztrát způsobených kybernetickým incidentem, pokrytí nákladů na profesionální IT specialisty, kteří incident vyšetřují, nákladů na právní zastoupení a obhajobu, nákladů na přerušení nebo omezení služeb a také nákladů na přesčasy zaměstnanců, kteří incident monitorují. Poskytují také služby PR agentur zaměřených na komunikaci v oblasti krizí [22].

Obnova dat: Pokud existují použitelné zálohy, nabízejí pokrytí nákladů na obnovu náhodně smazaných dat nebo dat smazaných v důsledku incidentu, například hackerského útoku. Nepokrývají však náklady na hodnotu samotných dat ani náklady na aktualizaci dat nebo softwaru [22].

Únik dat: Včetně odpovědnosti za škodu způsobenou třetí straně v důsledku úniku dat způsobeného kybernetickým incidentem. Kryté jsou náhodné nebo protiprávní incidenty související s důvěrností, dostupností nebo integritou dat [22].

Odpovědnost za újmu vyplývající z porušení ochrany dat: Pokrývá odpovědnost v případě škody nebo ztráty způsobené třetí straně v důsledku narušení bezpečnosti dat způsobeného kybernetickým incidentem. To zahrnuje náhodné nebo protiprávní zničení, ztrátu, změnu,

neoprávněné zveřejnění nebo přístup k důvěrným informacím uloženým nebo zpracovávaným v počítačových systémech klienta [22].

Síťové zabezpečení: Krytí nákladů na nezabránění kybernetickým incidentům, které způsobily škodu třetí straně prostřednictvím pojištěného počítačového systému [22].

Nabízejí také **volitelné připojištění**, které se vztahuje na:

Přerušení provozu, kybernetické vydírání, kybernetický zločin, porušení standardů PCI-DSS, phishing, odpovědnost za újmu způsobenou aktivitami v on-line médiích, IT asistence i pro případy běžné nefunkčnosti IT techniky mimo kybernetický incident [22].

Výluky:

specifikuje okolnosti a rizika, která nejsou kryta pojistitelem. [25]

Pro ČSOB je jich hodně, ale hlavně to jsou:

- Úmyslné jednání nebo hrubá nedbalost.
- Porušení zákona nebo podnikání bez příslušného oprávnění.
- Neoprávněné shromažďování osobních údajů.
- Požití alkoholu nebo drog.
- Jaderné riziko, ionizující záření, elektromagnetická pole.
- Válečné události, terorismus, kyber-terorismus.
- Pokuty, penále a sankce uložené úřady.
- Insolvence, platební neschopnost pojištěného nebo obchodních partnerů.
- Konfiskace, vyvlastnění, zásahy státu (včetně kybernetických).
- Finanční újmy spojené s tělesným zraněním nebo poškozením majetku,
- Neplnění bezpečnostních opatření, nespolupráce s úřady,
- Investiční nebo tržní ztráty (např. výkyvy ceny cenných papírů).
- Neodstranění osobních údajů po žádosti subjektu.
- Škody způsobené blízkými osobami nebo propojenými subjekty.

- Selhání kritické infrastruktury třetích stran (elektřina, voda, internet).

4.2.Maxima

Maxima pojišťovna je česká firma se sídlem v Praze, která působí na trhu již od roku 1994. Nabízí produkty v oblasti životního pojištění, pojištění majetku a odpovědnosti, zdravotního pojištění cizinců i pojištění podnikatelů a průmyslu. Je známější spíše pro zdravotní pojištění cizinců.

Nabízí pojištění kybernetických rizik pod názvem Pojištění kybernetických rizik, které spadá pod pojištění majetku a odpovědnosti pro podnikatele a právnické osoby [21].

Produkt reaguje na nařízení o ochraně osobních údajů (GDPR) a je určeno pro podnikatele s ročním obratem do 500 milionů korun. Pojištění se vztahuje na:

Náklady pojištěného na uvedení počítačů, jeho sítě nebo podnikání do původního stavu: V případě porušení bezpečnosti dat nebo sítě pojištění kryje: Náklady na obnovu dat, Forenzní náklady, Náklady spojené s kybernetickým vydíráním, Výdaje právního zastupování, Náklady vynaložené na povinné oznámení a na vztahy s veřejností a Náklady a pokuty v oblasti platebních karet. [24]

Pokrývá odpovědnost v případě škody nebo ztráty způsobené třetí straně: Náhrada škody nebo pokuta v důsledku odpovědnosti za předání malwaru z počítačového systému pojištěného, Ztrátu neveřejných dat či informací třetí strany, Porušení legislativy, závazku mlčenlivosti nebo práva na ochranu osobních údajů a Chybu zabezpečení počítačového systému pojištěného, Nezabránění před rozšířením DoS, DDoS útoku z počítačového systému pojištěného [24].

Ušlý zisk a stálé náklady v případě přerušení nebo omezení provozu pojištěného: v případě Neoprávněného přístupu, Chyby operátora, DoS, DDoS útoku a Zavedení malwaru do sítě pojištěného [24].

Nabízejí také **volitelné připojištění**, které se vztahuje na:

- Riziko vydírání prostřednictvím sítě.
- Ztráta způsobená výpadkem sítě.
- Zveřejnění digitálního obsahu v multimédiích.

Výluky:

- Úmyslné porušení právních předpisů.

- Neoprávněně shromažďovaná data.
- Jednání proti hospodářské soutěži. [21,24]

4.3. Colonnade

Firma Colonnade Insurance S. A. (Colonnade) je neživotní pojišťovnou se sídlem v Lucembursku. Firma je 100% vlastněná společností Fairfax Financial Holding, kanadskou společností založenou v roce 1985.

Colonnade nabízí pojištění kybernetických rizik pod názvem Pojištění kybernetických rizik.

Pojištění je určeno pro široké spektrum subjektů, např. pro společnosti, které pracují s osobními nebo firemními daty, výrobní podniky, IT a telekomunikační firmy a dopravce. Je určeno pro společnosti všech velikostí, které chtějí chránit svá data, provoz a reputaci před kybernetickými hrozbami.[20] Pojištění se vztahuje na:

Různé IT dopadůy: Pojištění kryje náklady na specialisty na kybernetická rizika a náklady na odborné služby, jejichž cílem je zjistit možnosti obnovy, znovushromáždění či znovuvytvoření elektronických dat [23].

Poškození dobrého jména: Pojištění kryje náklady na odborné služby zaměřené na zabránění či zmírnění nepříznivého vlivu na dobré jméno společnosti nebo konkrétní osoby pracující pro společnost a náklady na oznámení ztráty či úniku dat poškozeným osobám nebo příslušnému regulatornímu orgánu [23].

Finanční zmírnění: Pojištění také pokrývá závazky vůči regulačním orgánům a kryje škody a náklady spojené s následujícími situacemi: právní zastoupení v případě porušení ochrany osobních údajů nebo důvěrných informací společnosti, právní služby v souvislosti s porušením bezpečnosti sítě, náhrada ušlého zisku způsobeného přerušením provozu systémů nebo sítí v důsledku porušení jejich bezpečnosti, finanční náhrada třetím stranám, které utrpěly bezpečnostní hrozbu v důsledku narušení systémů společnosti, a právní zastoupení v případech porušení práv duševního vlastnictví třetích stran nebo nedbalého nakládání s obsahem elektronických médií [23].

Výluky:

- Porušení hospodářské soutěže, antitrustové činy.

- Tělesné újmy nebo škody na fyzickém majetku (s výjimkou následných škod způsobených daty).
- Smluvní odpovědnost přesahující běžné právní závazky.
- Porušení práv duševního vlastnictví (např. patenty, obchodní tajemství).
- Neoprávněné používání dat nebo neplacení licenčních poplatků.
- Válečné události, občanské nepokoje, převraty, terorismus a kyber-terorismus.
- Ztráty z obchodování nebo finančních transakcí (např. neoprávněné převody peněz).
- Incidenty, které již nastaly nebo byly známy před uzavřením pojistky.
- Insolvence nebo úpadek pojištěného nebo jeho dodavatelů.
- Trestné činy, úmyslné jednání nebo hrubá nedbalost.
- Požití alkoholu nebo omamných látek.
- Škody nepojistitelné podle místní legislativy. [20,23]

5. Pojištění kybernetických rizik vybrané společnosti

5.1. Představení společnosti

Vzhledem k citlivosti tématu odmítla být společnost uváděna pod svým pravým jménem. Budeme ji tedy označovat jako společnost XYZ.

Fiktivní adresa: Průmyslová 1234/56,100 00 Praha 1, Česká republika

Je zařazena do kategorie středních podniků s počtem zaměstnanců nižším než 250.

Společnost podniká v České republice od počátku 90. let a je vlastněna jinou mateřskou společností mimo Českou republiku.

Společnost má více divizí a její obecná obchodní činnost spočívá v dovozu.

5.2. Přehled kybernetických rizik ve firmě

Vzhledem k citlivosti a přísnému dodržování kybernetické bezpečnosti pilířů mi společnost byla ochotna poskytnout pouze obecný přehled o tom, co se děje v oblasti bezpečnostních rizik, s nimiž se setkává při každodenních činnostech; obecně však proces začíná kategorizací těchto rizik pomocí platformy řízení, která se řídí konkrétními klíčovými ukazateli výkonnosti v oblasti kybernetické bezpečnosti a zajišťuje, že rizika jsou kategorizována, měřena a vyřešena.

Rizika, která společnost XYZ sdílela, lze rozdělit do 4 hlavních kategorií:

- **Lidské chyby (T1):**

Tabulka 1 Kybernetická rizika T1

Hrozba	Popis
Uživatelské chyby (T1.1)	Náhodné vymazání nebo změna uživatelů.
Operační chyba (T1.2)	Chybná konfigurace personálem odpovědným za provoz a údržbu.
Slabé procesy (T1.3)	Chybějící definice a odpovědnosti v provozních a obchodních procesech.

Zdroj: e-mailová komunikace

Tabulka 1 uvádí seznam hrozeb způsobených lidskými chybami.

- **Úmyslné jednání (T2):**

Existuje celá řada úmyslných činů, se kterými se společnost XYZ v průběhu let setkala a které řešila, což vyvolává potřebu pojištění kybernetických rizik, jako např:

Tabulka 2 Kybernetická rizika T2

Hrozba	Popis
Neoprávněný přístup k informacím (T2.1)	Vydávání se za oprávněné uživatele, hackerské útoky nebo rozšiřování přístupových oprávnění.
Zneužití oprávněnými uživateli, zrada (T2.2)	Úmyslné prozrazení údajů.
Útoky na dostupnost informací (T2.3)	Útoky typu Denial of Service.
Sabotáž (T2.4)	Zničení zařízení nebo dat zasvěcenými osobami nebo osobami zvenčí.
Krádež (T2.5)	Zasvěcenými osobami nebo osobami zvenčí.
Škodlivý software (T2.6)	Červi, viry, trojské koně, logické bomby.
Sociální inženýrství (T2.7)	Manipulování s lidmi, aby prozradili důvěrné informace.

Zdroj: e-mailová komunikace

Tabulka 2 uvádí hrozby způsobené úmyslnými jednáním.

- **Technická selhání (T3):**

Tabulka 3 Kybernetická rizika T3

Hrozba	Popis
Selhání informačních systémů (T3.1)	Závady hardwaru nebo chyby softwaru.
Selhání komunikační infrastruktury (T3.2)	Problémy se síťovými prvky nebo nedostupnost poskytovatele služeb.
Selhání komponent infrastruktury (T3.3)	Závady na klimatizaci, napájení, UPS atd.

Výpadek napájení / výpadek proudu (T3.4)	Výpadek externího zdroje napájení.

Zdroj: e-mailová komunikace

Tabulka 3 uvádí seznam hrozeb způsobených technickými selháními.

- **Vyšší moc (T4):**

Tabulka 4 Kybernetická rizika T4

Hrozba	Popis
Nedostatek personálu (T4.1)	Z důvodu stávky, výluky, války, politických nepokojů nebo epidemií.
Požár (T4.2)	Zasažení systémů IT, včetně následných škod.
Škody způsobené vodou (T4.3)	Záplavy.
Přírodní katastrofa (T4.4)	Sesuvy půdy, zemětřesení, hurikány
Katastrofická nehoda (T4.5)	Havárie letadla nebo železnice.
Terorismus (T4.6)	Útoky na zařízení, zejména datová centra.

Zdroj: e-mailová komunikace

Tabulka 4 obsahuje seznam hrozeb, které můžou být způsobeny vyšší mocí.

5.3. Potřeba pojistné ochrany

Vzhledem k široké škále rizik by společnosti měly hledat způsob, jak eliminovat finanční dopad kybernetických incidentů. Pojištění může pokrýt náklady spojené s obnovou dat, soudní poplatky, náklady na oznámení, přerušení provozu a další. Společnosti často vystavují svou expozici rizikům a potenciálním finančním dopadům, aby určily úroveň potřebného pojistného krytí. Součástí tohoto procesu mohou být i pojišťovny, které na základě dohod s pojištěnou stranou provádějí vlastní hodnocení hrozeb.

Také v závislosti na způsobu fungování společnosti, zda je její provoz založen na cloudu, nebo na místě, může být dalším faktorem při určování potřeby kybernetického pojištění.

V našem případě je společnost XYZ dceřiná firma a mateřská společnost je se sídlem mimo Českou republiku, kde jsou rizika vyhodnocována a zmírňována, takže místní poskytovatelé pojištění nejsou v tomto případě relevantní, protože o pojištěnou společnost se postará mateřská společnost.

Na základě těchto informací budeme hledat pojištění v České republice, které pokrývá dříve uvedená rizika, a porovnáme dostupné dodavatele pomocí vícekriteriální rozhodovací analýzy, abychom určili, který dodavatel nejlépe odpovídá situaci společnosti XYZ, pokud by nebyla pojištěna mateřskou společností a za předpokladu, že zmírňuje vlastní kybernetická rizika.

6. Stanovení hodnoticích kritérií, aplikace metod vícekriteriálního rozhodování

6.1. Kritéria

Z rozhovoru s odpovědnou osobou ze společnosti vyplynulo, že je důležité, aby pojištění pokrývalo porušení ochrany osobních údajů, kybernetické vydírání, odpovědnost za bezpečnost sítě a další rizika. Podle společnosti je také důležité vzít v úvahu faktory, jako cena, reputace poskytovatele a konkrétní podmínky pojistné smlouvy.

Tato doporučení budou zohledněna jako důležité faktory pro požadované pojištění, což je cílem analýzy. Kritéria stanovíme na základě analýzy nabídek pojišťoven a podrobností o jejich pojistných produktech.

Poté použijeme metodu párového porovnání (Fullerova metoda) pro stanovení váhy kritérií, následně provedeme hodnocení alternativ pomocí metody váženého součtu a vybereme optimální variantu.

Tabulka 5 Seznam kritérií

	Kritérium
1	Obnova dat
2	Bezpečnost dat firmy
3	Právní zastoupení v různých situacích
4	IT specialista
5	PR
6	Zabezpečení dat třetích stran
7	Duševní vlastnictví
8	Škoda třetím stranám způsobená malwarem
9	Incidenty s platebními kartami
10	Kybernetické vydírání

11	Přerušení provozu
12	Cena
13	Reputace

Zdroj: vlastní zpracování

Tabulka 5 obsahuje seznam použitých kritérií.

Nyní vysvětlíme jednotlivá kritéria a provedeme srovnání dostupných alternativ, abychom získali přehled o tom, kdo tato kritéria splňuje. Toto srovnání bude základem pro krok srovnání alternativ z hlediska jednotlivých kritérií v našem MCDM.

Obnova dat se vztahuje na pokrytí nákladů na obnovení dat v případě incidentu, který způsobí ztrátu dat společnosti. Tyto incidenty mohou být způsobeny omylem vymazanými daty nebo v důsledku hackerských útoků či podobných incidentů. Je důležité zdůraznit, že pro obnovení dat je nutné mít k dispozici jejich existující zálohy. Pokrytí nákladů nezohledňuje hodnotu samotných dat.

Bezpečnost dat společnosti se konkrétně týká zabezpečení dat společnosti, nikoli třetí strany. Obecně se jedná o možnost pokrytí finančních ztrát v případě porušení důvěrnosti, dostupnosti nebo integrity dat společnosti. Mezi finanční náklady, které lze v rámci tohoto kritéria přímo zohlednit, patří náklady na přesčasy zaměstnanců za účelem monitorování a analýzy incidentu nebo náklady na profesionální IT specialisty, kteří incident řeší. Další náklady jsou podrobněji popsány v samostatných kritériích.

Právní zastoupení v různých situacích: Existují různé situace, které vyžadují dodržení specifických právních postupů, jako jsou právní prezentace v případě incidentu ovlivňujícího třetí stranu, povinnost informovat o některých incidentech příslušné strany, další právní prezentace potřebné v oblasti public relations a médií, porušení duševního vlastnictví a další. Toto kritérium se týká poskytování těchto právních služeb a úhrady nákladů na tyto služby.

IT specialista: Toto kritérium se týká poskytování nebo úhrady nákladů na IT specialisty, kteří jsou potřební k monitorování, analýze a reakci na různé incidenty, jako jsou útoky hackerů, útoky malwaru nebo jiné incidenty, které vyžadují IT specialisty. Později uvidíme, že ne všechny pojistné produkty poskytují nebo hradí náklady na IT specialisty jako základní službu, a ne pro všechny situace. Může se také jednat o volitelné IT služby, které mohou poskytovat podporu i bez výskytu incidentů.

PR: Různé incidenty mohou mít vliv na společnost v oblasti public relations. Příkladem incidentu může být hackerský útok, při kterém jsou z firmy odcizeny údaje o uživatelích, což může vést k tomu, že uživatelé budou společnost obviňovat z toho, že nechrání jejich data. Zákony jako GDPR existují za účelem ochrany údajů uživatelů a pojištění může zmírnit finanční dopady v důsledku možných právních kroků uživatelů proti společnosti v takové situaci, ale image společnosti může být poškozena a toto kritérium se týká pokrytí nákladů na zlepšení PR.

Zabezpečení dat třetích stran: Jak již bylo zmíněno, existují incidenty, které mají dopad na bezpečnost dat společnosti, ale existují i jiné, které mohou mít dopad na data třetí strany. Toto kritérium se týká pokrytí nákladů na škody, které vzniknou třetí straně v důsledku porušení bezpečnosti dat třetí strany. To zahrnuje i porušení GDPR.

Duševní vlastnictví se týká úhrady nákladů v důsledku porušení konkrétních zákonů, jako je například zneužití duševního vlastnictví. Rozsah tohoto porušení je široký, obvykle však k němu dochází v důsledku nezískání konkrétních licencí potřebných k použití materiálu.

Škoda třetím stranám způsobená malwarem: Stejně jako existuje kritérium týkající se úhrady nákladů třetí straně v důsledku porušení bezpečnosti dat, toto kritérium se týká škod, které vzniknou třetí straně v důsledku malwaru přeneseného na třetí stranu ze systému pojištěného, což může být důsledkem nedostatečné ochrany sítě pojištěného.

Incidenty s platebními kartami: Toto kritérium se obecně týká pokrytí nákladů v důsledku selhání ochrany údajů platebních karet. Některé alternativy poskytují toto konkrétní pokrytí nákladů jako standard, jiné jako volitelnou možnost.

Kybernetické vydírání: Toto kritérium se týká pokrytí nákladů v případě kybernetického vydírání, známého také jako ransomware, což je forma malwaru, která vede k zašifrování dat oběti a následně požaduje peníze za dešifrování těchto dat.

Přerušení provozu: Některé útoky mohou, ale nemusí nutně vést k přerušení služeb, avšak jiné útoky, jako jsou DoS (Denial of Service) a DDoS (Distributed Denial of Service), mají za hlavní cíl přerušit služby oběti s cílem způsobit finanční škodu. Toto kritérium zahrnuje finanční náklady, které vzniknou v důsledku takového přerušení obchodní činnosti.

Cena: Toto kritérium bylo zmíněno jako důležitý faktor při určování optimální varianty, takže je pro naše MCDM velmi důležité. Společnost, kterou jsme kontaktovali, nám však z důvodu citlivosti tématu neposkytla konkrétní informace, které by mohly být použity k určení

skutečného rozsahu rizik, což by nám umožnilo odhadnout jejich cenu. Bohužel tedy toto konkrétní kritérium nebude použito, protože podle našeho hodnocení bychom jej museli označit jako „podle rozsahu“, což by mu dalo stejnou váhu, takže by to nemělo vliv na MCDM.

Reputace: Kritérium reputace může být otázkou, na kterou je obtížné objektivně odpovědět, protože různí respondenti mají různé subjektivní zkušenosti s těmito pojišťovnami a jejich názory mohou vycházet z úplně jiných pojistných produktů než pojištění kybernetických rizik. Rozhodli jsme se proto hodnotit reputaci na základě údajů o tržním podílu počtu uzavřených smluv o neživotním pojištění za rok 2024. Čím vyšší hodnota, tím lepší reputace, takže se jedná o kritérium maximalizačního typu. [26]

6.2. Stanovení vah kritérií

Rozhodovací proces budeme provádět pomocí softwaru Microsoft Excel.

Prvním krokem je stanovení váhy (relevantní důležitosti) kritérií, což provedeme, jak již bylo zmíněno, pomocí párového srovnání (Fullerova metoda).

Tabulka 6 Seznam zkratky kritérií

Zkratka	Kritérium
K1	Obnova dat
K2	Bezpečnost dat firmy
K3	Právní zastoupení v různých situacích
K4	IT specialista
K5	PR
K6	Zabezpečení dat třetích stran
K7	Duševní vlastnictví
K8	Škoda třetím stranám způsobená malwarem
K9	Incidenty s platebními kartami
K10	Kybernetické vydírání
K11	Přerušení provozu
K12	Reputace

Zdroj: vlastní zpracování

V tabulce 6 vidíme Seznam kritérií a jejich zkratek. Abychom mohli lépe zobrazit párové srovnání, budeme se na každé kritérium odkazovat ve formátu „K?“, kde K znamená kritérium a „?“ odkazuje na číslo kritéria.

Tabulka 7 Porovnání pojistných produktů

Zkratka	Kritérium	ČSOB	Maxima	Colonnade
K1	Obnova dat	Ano	Ano	Ano
K2	Bezpečnost dat firmy	Ano	Ano	Ano
K3	Právní zastoupení v různých situacích	Ano	Ano	Ano
K4	IT specialista	Ano	Ne	Ano
K5	PR	Ano	Ano	Ano
K6	Zabezpečení dat třetích stran	Ano	Ano	Ne
K7	Duševní vlastnictví	Ne	Ne	Ano
K8	Škoda třetím stranám způsobená malwarem	Ano	Ano	Ano
K9	Incidenty s platebními kartami	Volitelne	Yes	Ne
K10	Kybernetické vydírání	Volitelne	Yes	Ne
K11	Přerušení provozu	Volitelne	Yes	Ne
K12	Reputace	9 %	0,7 %	0,9 %

Zdroj: vlastní zpracování

V tabulce 7 porovnáváme pojistné produkty nabízené společnostmi ČSOB, Maxima a Colonnade. Tato tabulka poslouží jako základ pro proces MCDM.

Prvním krokem tohoto procesu je párová analýza, při které porovnáváme každé kritérium s ostatními kritérii a určujeme jeho relativní význam. Kritérium s nejvyšší váhou představuje nejdůležitější kritérium.

Tabulka 8 Párové srovnání

Kritéria	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12	Počet preferencí fi	Váhy vi	P+1	upr. Váhy vi
K1		0	0	1	0	0	0	0	0	0	0	0	1,0	0,015	2,0	0,025
K2			1	1	1	0,5	1	0,5	1	0,5	1	0,5	9,0	0,134	10,0	0,127
K3				1	1	0	1	0	1	0	1	0	6,0	0,090	7,0	0,089
K4					0	0	0	0	0	0	1	0	1,0	0,015	2,0	0,025
K5						0	0,5	0	1	0	1	0	4,5	0,067	5,5	0,070
K6							1	0,5	1	1	1	1	10,0	0,149	11,0	0,139
K7								0	0,5	0	0,5	0	3,5	0,052	4,5	0,057
K8									0	0	1	1	8,0	0,119	9,0	0,114
K9										0	0,5	0	4,0	0,060	5,0	0,063
K10											1	0,5	10,0	0,149	11,0	0,139
K11												0	2,0	0,030	3,0	0,038
K12													8,0	0,119	9,0	0,114
											Suma		67	1	79	1

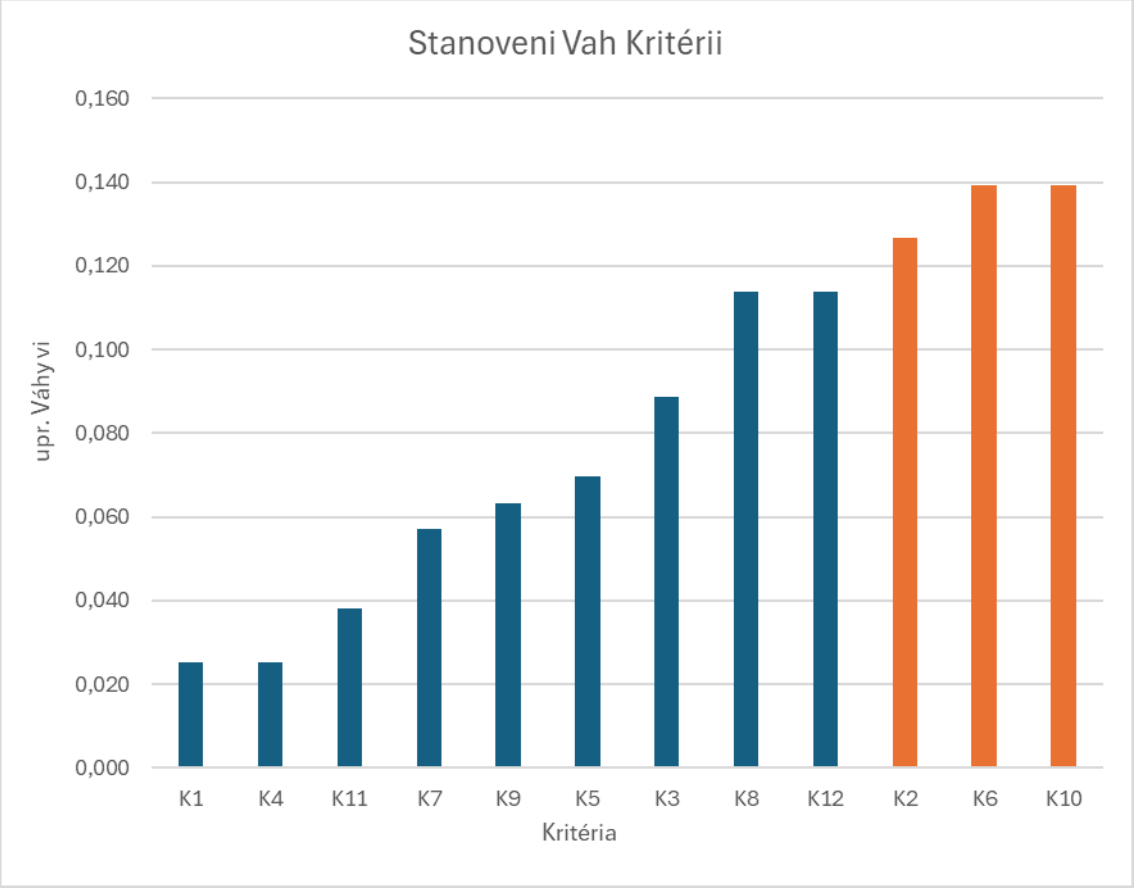
Zdroj: vlastní zpracování

Tabulka 7 obsahuje proces párového srovnání. Vidíme, že v sloupci 1 je seznam kritérií, ve sloupcích 2–8 vidíme opět seznam kritérií, abychom mohli porovnat, která z nich jsou pro nás nejdůležitější. Pokud K1 v řádku je pro nás důležitější než K2 v sloupci, označíme 1, v opačném případě označíme 0 a pokud jsou stejně důležité, označíme 0,5.

V následujícím sloupci 9 vidíme počet preferencí, který je součtem 0 v řádcích a 1 ve sloupci. Kdykoli předpokládáme stejnou důležitost, přiřadíme hodnotu 0,5 k celkovému součtu.

Ve sloupci 10 potom normalizujeme váhy jednotlivých kritérií podle rovnice 2, ale vzhledem k tomu, že K7 má preferenční počet 0, musíme upravit celý sloupec přidáním 1, aby se zabránilo interpretaci preferenčního čísla 0 jako kritéria s absolutně nulovou důležitostí, což provádíme ve sloupci 11.

Nakonec ve sloupci 12 jsou upravené váhy kritérií po zohlednění hodnoty 0.



Obrázek: 7 Upravené váhy kritérií

Zdroj: vlastní zpracování

Vidíme v obrázku 7 vypočítané váhy kritérií, které odpovídají důležitosti těchto konkrétních kritérií. Zde vidíme, že nejdůležitějšími 5 kritérii jsou K2, K6 a K10, následované dvěma kritérii stejné důležitosti K8 a K12. Nejméně důležitými kritérii jsou K1 a K4.

Jak vidíme, srovnání odpovídá důležitosti kritérií zdůrazněných společností, konkrétně K10, K6, K8 a K12.

6.3. Dílčí ohodnocení alternativ

Dále použijeme metodu vážených součtů pro dílčí ohodnocení alternativ s ohledem na jednotlivá kritéria.

Stejným způsobem budeme postupovat i při stanovení váhy kritérií, tentokrát však porovnáním variant. Abychom mohli lépe vidět srovnání, budeme varianty označovat jako „V?“, kde „V“ je varianta a „?“ odkazuje na její číslo.

Tabulka 9 Seznam variant

Varianta
V1 – ČSOB
V2 – Maxima
V3 – Colonnade

Zdroj: vlastní zpracování

V tabulce 9 je uveden seznam variant, ze kterých bude vybrána optimální variantu.

Začneme porovnáním prvním kritériem:

Tabulka 10 K1 – Obnova dat

K1	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		0,5	0,5	1	2	0,333
V2			0,5	1	2	0,333
V3				1	2	0,333
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 10 máme srovnání K1 a vidíme, že všechny tři varianty mají stejnou preferenci, protože ve své nabídce pojištění nabízejí obnovu dat. Je však důležité zdůraznit, že Maxima nabízí také obnovení systému do původního stavu, nejen obnovu dat.

Tabulka 11 K2 – Bezpečnost dat firmy

K2	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		0,5	0,5	1	2	0,333
V2			0,5	1	2	0,333
V3				1	2	0,333
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 11 máme srovnání K2 a vidíme, že opět všechny tři varianty mají stejnou preferenci, protože všechny nabízejí krytí nákladů v případě porušení bezpečnosti dat společnosti.

Tabulka 12 K3 – Právní zastoupení v různých situacích

K3	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		0,5	0,5	1	2	0,333
V2			0,5	1	2	0,333
V3				1	2	0,333
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 12 máme srovnání K3 se stejnou preferencí pro všechny tři varianty. Všechny varianty nabízejí právní zastoupení a v mnoha případech také pokrytí nákladů na soudní řízení

Tabulka 13 K4 – IT specialista

K4	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		1	1	2	3	0,500
V2			0	0	1	0,167
V3				1	2	0,333
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 13 máme srovnání K4 s V1 jako nejpreferovanější variantou, a to z toho důvodu, že kromě standardní nabídky pokrytí nákladů na IT specialisty v případě hackerských útoků a obnovy dat, kterou nabízí také V3, nabízí také volitelné IT služby 24/7, a to i v případě, že nedojde k žádným kybernetickým incidentům. V2 nebyla preferována, protože nenabízí žádné standardní ani volitelné pokrytí IT služeb.

Tabulka 14 K5 – PR

K5	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		0,5	0,5	1	2	0,333
V2			0,5	1	2	0,333
V3				1	2	0,333
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 14 máme srovnání K5. Všechny tři varianty nabízejí pokrytí nákladů v případě poškození reputace společnosti nebo PR v důsledku kybernetického incidentu, a proto mají všechny stejnou preferenci.

Tabulka 15 K6 – Zabezpečení dat třetích stran

K6	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		0,5	1	1,5	2,5	0,417
V2			1	1,5	2,5	0,417
V3				0	1	0,167
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 15 máme srovnání K6. V1 a V2 mají stejnou preferenci, protože nabízejí úhradu nákladů v případě škody způsobené třetí straně v důsledku porušení bezpečnosti jejich údajů, například porušením zákonů GDPR. V3 tuto možnost nenabízí.

Tabulka 16 K7 – Duševní vlastnictví

K7	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		0,5	0	0,5	1,5	0,250
V2			0	0,5	1,5	0,250
V3				2	3	0,500
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 16 máme srovnání K7. Pouze V3 nabízí krytí nákladů v případě poškození nebo zneužití duševního vlastnictví.

Tabulka 17 K8 – Škoda třetím stranám způsobená malwarem

K8	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		0,5	0,5	1	2	0,333
V2			0,5	1	2	0,333
V3				1	2	0,333
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 17 máme srovnání K8. Všechny tři varianty nabízejí krytí nákladů na škody způsobené třetí straně v důsledku selhání ochrany pojištěného síťového systému, které vedlo k šíření malwaru. Všechny tedy mají stejnou preferenci.

Tabulka 18 K9 – Incidenty s platebními kartami

K9	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		0	1	1	2	0,333
V2			1	2	3	0,500
V3				0	1	0,167
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 18 máme srovnání K9. V tomto případě není V3 preferována, protože nenabízí krytí nákladů v případě porušení standardů PCI-DSS. V2 a V1 tyto náklady kryjí, avšak V2 to nabízí jako standard, zatímco V1 jako volitelné pojištění.

Tabulka 19 K10 – Kybernetické vydírání

K10	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		0,5	1	1,5	2,5	0,417
V2			1	1,5	2,5	0,417
V3				0	1	0,167
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 19 máme srovnání K10. V tomto případě není V3 preferována, protože nenabízí krytí nákladů v případě kybernetického vydírání. V2 a V1 tyto náklady kryjí, ale u obou se jedná o volitelné pojištění.

Tabulka 20 K11 – Přerušení provozu

K11	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		0	0	0	1	0,167
V2			1	2	3	0,500
V3				1	2	0,333
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 20 máme srovnání K11. V tomto případě všechny tři varianty nabízejí stejnou možnost, avšak tato preference vyplývá z toho, že V1 má toto krytí pouze jako volitelné, V2 ho má jako standardní i jako doplňkové volitelné pojištění pro širší krytí a V3 ho má pouze jako standardní. Proto je nejpreferovanější V2.

Tabulka 21 K12 – Reputace

K12	V1	V2	V3	Počet preferencí	P+1	Váhy hij
V1		1	1	2	3	0,500
V2			0,5	0,5	1,5	0,250
V3				0,5	1,5	0,250
			Součet	3	6	1

Zdroj: vlastní zpracování

V tabulce 21 máme srovnání K12, posledního kritéria. V tomto případě, založeném na tržním podílu uzavřených smluv neživotního pojištění, V1 výrazně převyšuje V2 a V3, takže je nejvhodnější. Rozdíl mezi V2 a V3 není natolik podstatný, aby bylo možné upřednostnit jedno před druhým. [26]

Pomocí metody vážených součtů můžeme vyhodnotit a vybrat variantu, která podle multikriteriální analýzy rozhodování zaujímá nejvyšší pozici, a je tedy optimální. K získání tohoto hodnocení použijeme vzorec pro stanovení optimální varianty, viz rovnice 3.

Tabulka 22 Ohodnocení alternativ

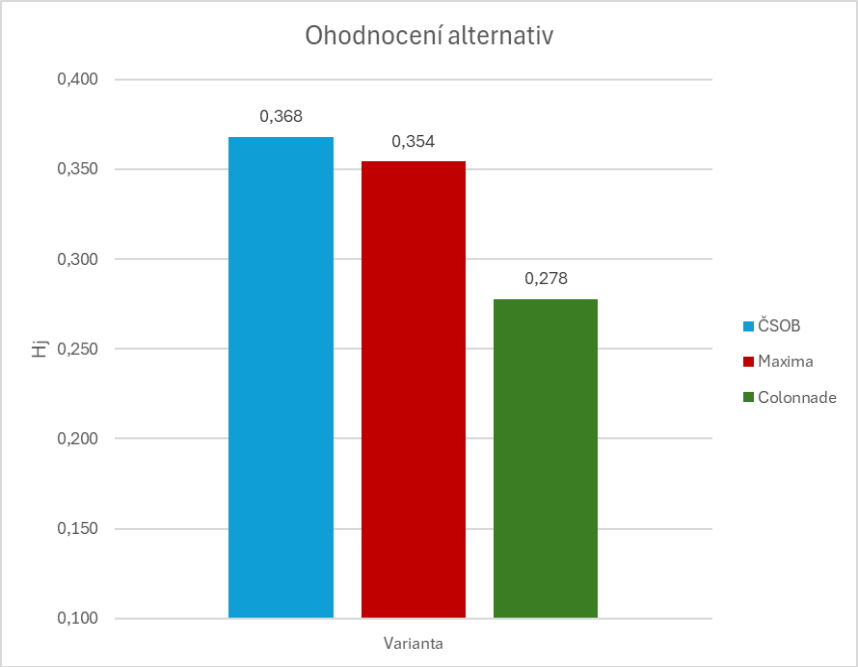
Ohodnocení alternativ	
Varianta	**Hj**
ČSOB	0,368
Maxima	0,354
Colonnade	0,278
Součet	1

Zdroj: vlastní zpracování

V tabulce 22 vidíme, že se jedná o velmi podobné vážené součty, nicméně můžeme dojít k pochopení, že pojištění V1 – ČSOB je optimální volbou podle rozhodovacího procesu, následované pojištěním V2 – Maxima a nakonec V3 – Colonnade.

7. Výběr optimální varianty pojištění

Podle procesu rozhodování je pojištění Maxima optimální variantou ze tří hodnocených variant. Je však důležité poznamenat, že tento výsledek neodráží nejlepší pojišťovnu, ale nejlepší volbu podle důležitosti kritérií vybraných pro účely této analýzy. Jiné metody vícekriteriálního rozhodování mohou přinést odlišné výsledky, takže vzhledem k jednoduchosti této metody může být lepší použít více metod, porovnat je a vybrat tu, která poskytuje výsledky, jež se rozhodujícímu subjektu jeví jako nejvhodnější pro cíl analýzy.



Obrázek: 8 Optimální alternativa

Zdroj: vlastní zpracování

Na obrázku 16 vidíme, že V1 – ČSOB je varianta s MAX H^j 0,368.

Pokud se pokusíme tyto výsledky vyhodnotit, bude těžké s jistotou vybrat pojištění ČSOB, protože výsledky jsou si velmi podobné. Mírná změna v důležitosti jednoho z kritérií, která může být způsobena odlišným vnímáním důležitosti ze strany rozhodujícího činitele nebo odlišnou metodou, může změnit interpretaci výsledků a vést k jinému vítězi. Na základě vyhodnocení těchto výsledků však docházíme k závěru, že vítězem je V1, a pokud učiníme objektivní rozhodnutí, bude to ten, který splní cíle našeho rozhodovacího procesu.

Na základě použitého postupu lze předpokládat, že s větším počtem specifikovaných kritérií by tento postup přinesl přesnější výsledky, ale také by vedl k nejasnostem při určování, která kritéria jsou při párovém srovnání důležitější.

8. Závěr

Tato bakalářská práce se zabývala tématem pojištění kybernetických rizik. Cílem této práce bylo najít optimální pojistný produkt pomocí metod vícekriteriálního rozhodování. Na začátku práce vysvětlujeme problematiku kybernetických rizik a představujeme pojmy související s kyberprostorem a kybernetickou bezpečností, poté představujeme stav kybernetické bezpečnosti, různé typy hrozeb a statistiky kybernetických incidentů v České republice a částečně i ve světě, abychom zdůraznili hrozbu kybernetických rizik pro podniky a potřebu kybernetického pojištění. Ve druhé části této práce představujeme pojmy, typy a rozdělení pojištění. Po položení základů pro pochopení pojištění vysvětlujeme, co je pojištění kybernetických rizik, a poskytujeme podrobnou analýzu současných produktů pojištění kybernetických rizik na českém trhu, konkrétně produktů ČSOB, Maxima a Colonnade. Nakonec představujeme teorii metod, které použijeme k dosažení našeho cíle, jímž je výběr optimální alternativy ze tří produktů, které nabízejí výše uvedené tři společnosti. Těmito metodami jsou párové srovnání a metoda vážených součtů. V poslední části této práce tyto metody aplikujeme v softwaru Excel a na závěr navrhujeme optimální variantu na základě výsledků vícekriteriálního rozhodovacího procesu. Podle našich kritérií bylo nakonec optimální variantou pojištění ČSOB. Ukázalo se, že vykazuje rovnováhu mezi nejdůležitějšími kritérii v našem seznamu kritérií, jež jsou K12 – reputace, K10 – kybernetické vydírání, K2 a K6 – odpovědnost třetí strany a K2 – bezpečnost dat společnosti. Tuto informaci jsme získali od nejmenované společnosti, se kterou jsme v průběhu této práce konzultovali, abychom na základě rizik a hrozeb, kterým čelí, našli optimální variantu pro jejich situaci.

Pomocí metod multikriteriálního rozhodování (MCDM) lze komplexní rozhodovací problémy řešit strukturovaným a systematickým způsobem. Tyto metody pomáhají eliminovat velkou část nejistoty a subjektivity, s nimiž se rozhodující osoby často potýkají, když čelí problémům, které se zdají mít mnoho možných řešení. Techniky MCDM poskytují jasný rámec pro hodnocení více často protichůdných kritérií, což umožňuje rozhodovacím orgánům stanovit priority alternativ na základě logických, transparentních a reprodukovatelných procesů. Výsledkem je, že MCDM zvyšuje kvalitu, konzistentnost a důvěryhodnost rozhodnutí přijímaných v prostředích, kde je nutné pečlivě zvažovat kompromisy.

Konečně otázka výběru optimálního produktu pojištění kybernetických rizik je otázkou, která bude přetrvávat i s měnícími se komplexními pojistnými smlouvami, avšak dodržování těchto metod vždy přinese konzistentní výsledky bez ohledu na to, jak velká je změna. Pokud lze problém definovat, stanovit cíle a kritéria a definovat varianty, lze poskytnout řešení.

POUŽITÁ LITERATURA

Knihy

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

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

[3] REJDA, George E. a MCNAMARA, Michael J. *Principles of risk management and insurance*. Thirteenth edition. Harlow, England: Pearson, 2017. ISBN 978-1-292-15103-8.

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

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

[6] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.

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

Online zdroje

[8] *Adware: a review*. Online. In: Google Scholar. 2015. Dostupné z: https://scholar.googleusercontent.com/scholar?q=cache:H6IOMB7XbxQJ:scholar.google.com/&hl=en&as_sdt=0,5&scilib=1&scioq=adware. [cit. 2025-06-23].

[9] Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study. Online. *Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study*. 2024, roč. 4, č. 1, s. 413–419. ISSN 2807-9035. Dostupné z: https://pdfs.semanticscholar.org/4f44/767f1a0b59241845f47547ff90cac3042afd.pdf. [cit. 2025-06-23].

[10] *Annual number of malware attacks worldwide from 2015 to 2023*. Online. In: Statista. 2024. Dostupné z: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/. [cit. 2025-06-23].

[11] *Co je počítačový virus + druhy virů*. Online. ESET. 2021. Dostupné z: https://www.eset.com/cz/virus/. [cit. 2025-06-23].

[12] CSIRT. *Výroční zpráva za rok 2024*. Online. In: CSIRT. 2025. Dostupné z: https://csirt.cz/media/filer_public/7d/83/7d834129-4826-4bf3-86ed-ac6e546cb650/250319_csirt_vyrocni_zprava_2024_final.pdf. [cit. 2025-04-28].

[13] *CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE*. Online. In: NÚKIB. 2025. Dostupné z: https://nukib.gov.cz/download/publications_en/Cyber-Security-Incidents-from-the-NUKIB-s-Perspective-December-2024.pdf. [cit. 2025-06-23].

[14] *Cybersecurity – Czechia*. Online. Statista. 2024. Dostupné z: https://www.statista.com/outlook/tmo/cybersecurity/czechia. [cit. 2025-06-25].

[15] *Czech Republic: A developing cybersecurity insurance market*. Online. CMS law-now. 2018. Dostupné z: https://cms-lawnow.com/en/ealerts/2018/06/czech-republic-a-developing -cybersecurity-insurance-market. [cit. 2025-06-25].

[16] *DORA regulation comes into effect*. Online. CNB. 2025. Dostupné z: https://www.openkritis.de/eu/eu-nis-2-czech.html. [cit. 2025-06-25].

[17] *EU NIS2 in Czech Republic*. Online. KRITIS. 2024. Dostupné z: https://www.openkritis.de/eu/eu-nis-2-czech.html. [cit. 2025-06-25].

[18] *FAQ*. Online. CSIRT.CZ. 2019. Dostupné z: https://csirt.cz/en/incident-reporting/faq/#whatisripe. [cit. 2025-06-23].

[19] KŘUPKA, Jiří; MÁCHOVÁ, Renata a KAŠPAROVÁ, Miloslava. *Rozhodovací procesy*. Online. 2012. Univerzita Pardubice, 2012. ISBN 978-80-7395-478-9. Dostupné z: https://eshop.upce.cz/epub/9003854/rozhodovaci-procesy. [cit. 2025-06-23].

[20] *Pojištění kybernetických rizik*. Online. Colonnade. Dostupné z: https://www.colonnade.cz/firmy/pojisteni-financnich-rizik/pojisteni-kybernetickych-rizik. [cit. 2025-06-23].

[21] *Pojištění kybernetických rizik a odpovědnosti za data (GDPR)*. Online. Maxima pojišťovna. 2025. Dostupné z: https://www.maximapojistovna.cz/cs/podnikatele-prumysl/pojisteni-kybernetickych-rizik-odpovednosti. [cit. 2025-06-23].

[22] *Pojištění kybernetických rizik*. Online. ČSOB. 2025. Dostupné z: https://www.csobpoj.cz/pojisteni/podnikatele-firmy/pojisteni-kybernetickych-rizik. [cit. 2025-06-23].

[23] *Pojištění kybernetických rizik: Informační dokument o pojistném produktu*. Online. In: Colonnade. 2025. Dostupné z: https://www.colonnade.cz/cdn/65b2eb68-cf8e-0106-94e7-7fcbfbaa6c5e/a2667555-008c-47b1-ace9-467ebe72ad7b/IPID_Pojisteni__kybernetickych_rizik.pdf. [cit. 2025-06-23].

[24] *Pojištění kybernetických rizik: Informační dokument o pojistném produktu*. Online. In: Maxima pojišťovna. 2018. Dostupné z: https://www.maximapojistovna.cz/sites/default/files/2019-05/informacni_dokument_o_pojistnem_produktu_cyberrisk.pdf. [cit. 2025-06-23].

[25] *Pojištění kybernetických rizik: Všeobecné pojistné podmínky*. Online. In: ČSOB. 2018. Dostupné z: https://www.csobpoj.cz/documents/10332/32946/10N9059+VPP_CRC_2018_10-2018.pdf/dc55ba8d-b5e3-17c8-0954-63591b631e67?t=1576162606907. [cit. 2025-06-23].

[26] *Pojištění v ČR 2023: Kdo vévodí trhu?* Online. Fajn pojištění. 2024. Dostupné z: https://www.fajnpojisteni.cz/novinky/1818-pojisteni-v-cr-2023-kdo-vevodi-trhu-a.html. [cit. 2025-06-25].

[27] STATISTA. *Number of cybercrimes investigated in Czechia from 2011 to 2023*. Online. In: Statista. 2025. Dostupné z: https://www.statista.com/statistics/1344671/czechia-number-of-cybercrimes/#:~:text=Number%20of%20cybercrimes%20in%20Czechia%202011%2D2023&text=In%20the%20observed%20period%2C%20the,thousand%20cybercrimes%20investigated%20in%202023.. [cit. 2025-04-28].

[28] *The State of Ransomware*. Online. Ransomware. 2024. Dostupné z: https://ransomware.org/ransomware-survey/. [cit. 2025-06-23].

[29] *Trojan Horse Virus*. Online. Fortinet. 2021. Dostupné z: https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus. [cit. 2025-06-23].

[30] *What is a „Drive-By" Download?* Online. Mcafee. 2023. Dostupné z: https://www.mcafee.com/learn/drive-by-download/#:~:text=A%20drive%2Dby%20download%20refers,and%20has%20a%20security%20flaw.. [cit. 2025-06-23].

[31] *What is phishing?* Online. IBM. 2024. Dostupné z: https://www.ibm.com/think/topics/phishing. [cit. 2025-06-23].

[32] *Xprimm insurance report*. Online. In: Xprimm. Bucharest, Romania: XPRIMM insurance publications, 2025. ISSN 1454-525x. Dostupné z: https://www.xprimmpublications.com/books/tmnmzalul/#p=37. [cit. 2025-06-25].