VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU
Nárožní 2600/9a, 158 00 Praha 5

DIPLOMOVÁ PRÁCE

MANAGEMENT FIREM

Vysoká škola ekonomie a managementu
info@vsem.cz / www.vsem.cz

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

NÁZEV DIPLOMOVÉ PRÁCE/TITLE OF THESIS
Pojištění jako nástroj řízení aktuálních podnikatelských rizik ve vybrané společnosti / Insurance as a Tool for Managing Current Business Risks in a Selected Company

TERMÍN UKONČENÍ STUDIA A OBHAJOBA (MĚSÍC/ROK)
Červen/2022

JMÉNO A PŘÍJMENÍ STUDENTA / STUDIJNÍ SKUPINA
Miloš Bednář / KEMMA01

JMÉNO VEDOUCÍHO DIPLOMOVÉ PRÁCE
Ing. Pavla Vrabcová, Ph.D.

PROHLÁŠENÍ STUDENTA
Odevzdáním této práce prohlašuji, že jsem zadanou diplomovou práci na uvedené téma vypracoval samostatně a že jsem ke zpracování této diplomové práce použil pouze literární prameny v práci uvedené. Jsem si vědom skutečnosti, že tato práce bude v souladu s § 47b zák. o vysokých školách zveřejněna, a souhlasím s tím, aby k takovému zveřejnění bez ohledu na výsledek obhajoby práce došlo. Prohlašuji, že informace, které jsem v práci užil, pocházejí z legálních zdrojů, tj. že zejména nejde o předmět státního, služebního či obchodního tajemství či o jiné důvěrné informace, k jejichž použití v práci, popř., k jejichž následné publikaci v souvislosti s předpokládanou veřejnou prezentací práce, nemám potřebné oprávnění. Datum a místo: 30. 4. 2022, Praha

PODĚKOVÁNÍ
Rád bych tímto poděkoval vedoucí diplomové práce za metodické vedení a odborné konzultace, které mi poskytla při zpracování mé diplomové práce. Velké poděkování patří také mé rodině, a hlavně manželce, která mě po celou dobu podporovala. Zároveň tímto děkuji jednateli podniku XYZ za poskytnutou spolupráci.

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

SOUHRN

0. Cíl práce:

Cílem této práce bylo ověřit, zda má podnik XYZ sjednáno pojištění v rozsahu, které dostatečně chrání jeho podnikatelské aktivity proti rizikům, kterým je v současnosti věnována světově i regionálně největší pozornost, a která jsou zároveň na českém trhu pojistitelná, popřípadě zda a jakým způsobem tyto rizika jinak řídí. Konkrétně se jedná o kybernetická rizika, přerušení provozu a přírodní události. Cílem práce je také poskytnout podniku zpětnou vazbu k současnému stavu řízení vybraných rizik, případně navrhnout úpravu aktuálního pojištění, sjednáním nového pojištění, či nastavení preventivních opatření v podniku.

1. **Výzkumné metody**:

V teoreticko-metodologické části práce bylo využito rešerše odborných literárních zdrojů, odborných článků a internetových zdrojů, a to nejen českých, ale i zahraničních, zejména pak Science Direct, World Health Organization, World Meteorological Organization, a dalších. Jako zdroje byly využity také statistické údaje od Swiss Re, Allianz Risk Barometr, NÚKIB atd. V analytické části práce byl nejprve proveden rozbor pojistných podmínek od vybraných pěti pojišťoven, které mají největší podíl předepsaného pojistného v podnikatelském pojištění na českém trhu. Dále byl formou dotazníku a doplňujícího osobního rozhovoru s jednatelem podniku XYZ zjištěn aktuální stav řízení vybraných rizik v daném podniku. Přitom bylo nutné zohlednit nejen jejich předpokládaný budoucí vývoj, ale zda vůbec mohou ohrožovat podnik XYZ s ohledem na specifika daného podniku (jeho činnost, umístění provozovny, nastavená opatření apod.), a také současně nastavená opatření pro řízení těchto rizik v podniku. To bylo dále doplněno o kontrolu aktuálně sjednaného pojistného krytí, tzn. současné pojistné smlouvy, kde bylo zjišťováno, zda má podnik sjednáno pojištění kybernetických hrozeb, přerušení provozu a přírodních událostí.

2. Výsledky výzkumu/práce:

Bylo potvrzeno, že kybernetická rizika, přerušení provozu a přírodní události patří mezi nejzávažnější a nejčetnější podnikatelská rizika. Podnik XYZ nemá proti žádnému z těchto rizik sjednáno pojištění. Vůči kybernetickým rizikům (vnějším i vnitřním) má podnik nastaveno mnoho dnes již standardních preventivních opatření, avšak ne úplně všechna. Pojistné podmínky pro kybernetické pojištění ukládají povinnost i dalších opatření, které podnik nemá. Kybernetické pojištění není na českém trhu běžnou záležitostí. Z pěti vybraných pojišťoven jej nabízí jen dvě (Kooperativa pojišťovna, a.s., Vienna Insurance Group, a ČSOB Pojišťovna, a.s., člen holdingu ČSOB). Podnik XYZ vykonává svoji činnost v pronajaté budově, u které navíc díky svému umístění příliš nehrozí vznik škody způsobené přírodním živlem (např. povodní či sesuvem půdy). Pojištění přírodních rizik tak není pro podnik nutností. Pojištění přerušení provozu standardně nekryje finanční ztráty způsobené pandemií nebo úředním zásahem. Na českém trhu nabízí krytí pro přerušení provozu z důvodu úředního zásahu pouze Kooperativa pojišťovna, a.s., Vienna Insurance Group. Podnik XYZ má připravena opatření pro případ další vlny pandemie. Průzkum Allianz Risk Barometr 2022 ukázal, že obávanější příčinou přerušení provozu jsou právě kybernetické hrozby a přírodní události, a až třetí je pandemie.

3. Závěry a doporučení:

Z chybějícího pojistného krytí je tak podniku XYZ doporučeno zvážit zejména sjednání pojištění kybernetických rizik, které nabízí ČSOB Pojišťovna, a.s., člen holdingu ČSOB. Dále je podniku XYZ doporučeno zavést další opatření v oblasti prevence kybernetických rizik nad rámec těch současných. Mezi taková opatření patří pravidelné aktualizace hesel, nastavení povinnosti používání jen silných hesel, a provádět pravidelná školení a připomínání pravidel v oblasti kybernetické bezpečnosti. Nařízení GDPR je nutné nadále věnovat zvýšenou pozornost, a proto by si podnik například měl dávat pozor, které informace zveřejňuje na svých webových stránkách. Dále pak je podniku doporučeno využívat zabezpečenou formu přenosu/předávání informací, jako je například šifrovaná pošta, heslování souborů a předání hesla jiným kanálem (např. SMS zprávou), předávání přes na zabezpečená uložiště, apod. To platí zejména pro osobní údaje fyzických osob a citlivé informace. Podniku XYZ je dále doporučeno také zvážit pojištění přerušení provozu z důvodu kybernetického incidentu.

KLÍČOVÁ SLOVA

pojištění, pojišťovna, pojistná smlouva, riziko, nebezpečí, NŽP, kybernetické hrozby, Covid-19, Koronavirus, přerušení provozu, přírodní události, katastrofy, řízení rizik

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

SUMMARY

1. Main objective:

The aim of this thesis was to verify whether the company XYZ has arranged insurance to the extent that sufficiently protects its business activities against the risks that are currently receiving the most attention worldwide and regionally, and which are also insurable on the Czech market, or whether and how these risks are otherwise managed. Specifically, these include cyber risks, business interruption and natural events. The aim of the thesis is also to provide the company with feedback on the current state of management of selected risks, possibly suggesting a modification of the current insurance, by arranging new insurance or setting up preventive measures in the company.

2. Research methods:

The theoretical and methodological part of the thesis was based on a search of specialized literature sources, articles and internet sources, not only Czech but also foreign, especially Science Direct, World Health Organization, World Meteorological Organization, and others. Statistical data from Swiss Re, Allianz Risk Barometer, NÚKIB, etc. were also used as sources. In the analytical part of the thesis, the analysis of insurance conditions from selected five insurance companies, which have the largest share of written premiums in business insurance on the Czech market, was carried out. Next, a questionnaire and a supplementary personal interview with the managing director of XYZ company were used to determine the current state of management of selected risks in the company. In doing so, it was necessary to take into account not only their expected future development, but also whether they could threaten the XYZ enterprise at all with regard to the specifics of the enterprise (its activities, location of the establishment, measures set, etc.), and also the measures set for managing these risks in the enterprise. This was further supplemented by a check of the insurance cover currently in place, i.e. the current insurance policy, to ascertain whether the company has insurance for cyber threats, business interruption and natural events.

3. Result of research:

It has been confirmed that cyber risks, business interruptions and natural events are among the most serious and frequent business risks. XYZ has no insurance against any of these risks. Against cyber risks (both external and internal), the company has set up many of the now standard preventive measures, but not all of them. The insurance conditions for cyber insurance oblige other measures that the company does not have. Cyber insurance is not common on the Czech market. Of the five selected insurance companies, only two offer it (Kooperativa pojišťovna, a.s., Vienna Insurance Group, and ČSOB Pojist'ovna, a.s., a member of the ČSOB holding). The XYZ company operates in a rented building, which, thanks to its location, is not at much risk of damage caused by a natural disaster (e.g. flood or landslide). Thus, natural hazard insurance is not necessary for the enterprise. Business interruption insurance does not normally cover financial losses caused by a pandemic or official intervention. On the Czech market, only Kooperativa pojišťovna, a.s., Vienna Insurance Group, offers cover for business interruption due to official intervention. The XYZ company has prepared measures in case of another pandemic wave. The Allianz Risk Barometer 2022 survey showed that cyber threats and natural events are the most feared causes of business interruption, with pandemics coming third.

4. Conclusions and recommendation:

Due to the lack of insurance coverage, XYZ company is recommended to consider in particular arranging cyber risk insurance offered by ČSOB Pojistovna, a.s., a member of the ČSOB holding. Furthermore, XYZ is recommended to introduce additional measures in the area of cyber risk prevention beyond the current ones. Such measures include regularly updating passwords, setting the obligation to use only strong passwords, and conducting regular training and reminders of cybersecurity rules. The GDPR regulation continues to require close attention, so a business should, for example, be careful about what information it publishes on its website. In addition, the business is advised to use a secure form of information transfer/transmission, such as encrypted mail, password encryption of files and transmission of passwords via another channel (e.g. SMS), transmission via secure storage, etc. This applies in particular to personal data of natural persons and sensitive information. XYZ is also advised to consider business interruption insurance due to a cyber-incident.

KEYWORDS

insurance, insurer, insurance contract, risk, peril, non-life insurance, cyber risk, Covid-19, coronavirus, business interruption, natural hazards, catastrophes, risk management

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

JEL CLASSIFICATION
G22 Insurance; Insurance Companies; Actuarial Studies
G32 Financing Policy; Financial Risk and Risk Management; Capital and Ownership Structure; Value of Firms; Goodwill
Q54 Climate; Natural Disasters and Their Management; Global Warming
Q55 Technological Innovation

Vysoká škola ekonomie a managementu
Nárožní 2600/9a, 158 00 Praha 5

ZADÁNÍ DIPLOMOVÉ PRÁCE

Jméno a příjmení:	Miloš Bednář
Studijní program:	Ekonomika a management (Ing.)
Studijní skupina:	KEMMA01
Název DP:	Pojištění jako nástroj řízení aktuálních podnikatelských rizik ve vybrané společnosti
Zásady pro vypracování (stručná osnova práce):	1 Úvod 2 Teoreticko-metodologická část 2.1 Aktuální trendy v oblasti pojištění rizik 2.2 IT hrozby a kybernetické pojištění 2.3 Covid-19 a pojištění přerušení provozu 2.4 Změny klimatu a pojištění přírodních nebezpečí 2.5 Metodika práce 3. Analytická část 3.1 Rozbor pojistných podmínek vybraných pojišťoven 3.2 Případová studie vybraného podniku 3.3 Vyhodnocení 4. Závěr
Seznam literatury: (alespoň 4 zdroje)	• DOBIÁŠ, P. *Pojištění podnikatelů ve vztazích s mezinárodním prvkem.* Praha: Leges, 2019. ISBN 978-80-7502-348-3. • DOUCEK, P., KONEČNÝ, M., NOVÁK, L. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4. • FOJTÍKOVÁ GMENTOVÁ, E. I., ŠÍDLO, D. *Pojištění občanů.* Praha: Eva Gmentová, 2020. ISBN 978-80-906748-6-8. • RAMNATH, S., et al. *What is Business Interruption Insurance and How is it Related to the Covid-19 Pandemic?* 2020, 1 (440), p.1-5. ISSN 0895-0164. • SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.
Harmonogram:	• Zpracování cílů a metodiky do 13. 12. 2021 • Zpracování teoretické části do 28. 2. 2022 • Zpracování výsledků do 20. 4. 2022 • Finální verze do 1. 5. 2022
Vedoucí práce:	Ing. Pavla Vrabcová, Ph.D.

prof. Ing. Milan Žák, CSc.
rektor

V Praze dne 30. 11. 2021

Prof. Ing. Milan Žák CSc.

Digitálně podepsal Prof. Ing. Milan Žák CSc.
DN: cn=Prof. Ing. Milan Žák CSc., c=CZ, o=Vysoká škola ekonomie a managementu, a.s., givenName=Milan, sn=Žák, serialNumber=ICA - 10393535
Datum: 2021.11.30 19:38:59 +01'00'

Obsah

Seznam zkratek

AGCS = Allianz Global Corporate & Specialty SE

AZP = Allianz pojišťovna, a.s.

BIS = Bank for International Settlements (Banka pro mezinárodní vypořádání)

ČAP = Česká asociace pojišťoven

ČHMÚ = Český hydrometeorologický ústav

ČPP = Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group

ČSN = Česká technická norma (dříve československá státní norma)

ČSOBP = ČSOB Pojišťovna, a.s., člen holdingu ČSOB

EIOPA = European Insurance and Occupational Pensions Authority (Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění)

EU = Evropská unie

GČP = Generali Česká pojišťovna a.s.

ISO = International Organization for Standardization (Mezinárodní organizace pro normalizaci)

KOOP = Kooperativa pojišťovna, a.s., Vienna Insurance Group

MERS = Middle East Respiratory Syndrome Coronavirus (respirační syndrom blízkého východu)

NÚKIB = Národní úřad pro kybernetickou a informační bezpečnost

OECD = Organization for Economic Co-operation and Development (Organizace pro hospodářskou spolupráci a rozvoj)

SARS = Severe Acute Respiratory Syndrome (těžký akutní respirační syndrom)

SPG = S&P Global

WHO = World Health Organization (Světová zdravotnická organizace)

WMO = World Meteorological Organization (Světová meteorologická organizace)

1 Úvod

"Kolik věcí se považuje za nemožné, dokud se skutečně nestanou?"

Gaius Plinius Secundus (Plinius starší), Naturalis Historia, VII.i, 6

Starý, ale pravdivý a stálé aktuální citát. Který z českých podniků a podnikatelů by si býval před rokem 2020 představil, že svět ochromí pandemie viru Covid-19, jež kromě ztrát na životech a újmách na zdraví bude působit také velké ekonomické škody. Z novodobé historie jsou z médií známé lokální virové epidemie, které se ale naštěstí celosvětově nerozšířily v takovém rozsahu jako Covid-19. Pro příklad se jednalo třeba o virus SARS, dle Světové zdravotnické organizace (2021a), dále jen WHO, poprvé identifikován na konci února 2003 během epidemie, která se objevila v Číně a rozšířila se do čtyř dalších zemí. Dalším příkladem může být MERS – zkratka v překladu znamená respirační syndrom blízkého východu, zjištěný v roce 2012 a jedná se o virus přenášený z velblouda na člověka (WHO, 2021b). SARS a MERS je stejně jako Covid-19 virové akutní respirační onemocnění a svým charakterem vzájemně velmi blízké. Není to tedy poprvé, a přesto ze strany mnoha českých podniků bylo riziko celosvětového rozšíření epidemie a následného "lockdownu" považováno za nepravděpodobné, až do chvíle, dokud kvůli pandemii nemusely své podnikání dočasně přerušit, omezit či v krajním případě dokonce trvale ukončit. Podobně by do léta roku 2021 málokterý obyvatel České republiky věřil tomu, že oblast jižní Moravy zasáhne tornádo, které dle Českého hydrometeorologického ústavu (2021, s. 3) dosáhne síly F4 na Fujitsově stupnici (druhá nejsilnější úroveň síly tornáda) a přeci se to stalo. Je tomu "teprve" 30 let, kdy se Česká republika připojila ke světové síti internetu. Stalo se tomu tak 13. února 1992 a od té doby roste nejen počet uživatelů internetu, ale také množství informací, které jsou ukládány v digitální podobě. S tím je spojen zvyšující se zájem hackerů tato data a informace získat, jelikož se jedná o velmi cennou komoditu. Každým rokem se také zvyšuje počet vyděračských útoků. Ztráta citlivých údajů může pro podnik znamenat nejen poškození dobrého jména, ale také například nemalou pokutu, propad zisků, ztrátu hodnoty podniku, snížení počtu zákazníků, ztrátu dodavatelů, odběratelů a podobně. Dříve pro někoho nemožné, dnes již vysoce aktuální riziko. Svět se stále mění a mění se také rizika, která mohou ohrozit fungování každého podniku. Z pohledu mediálního zájmu a samozřejmě zájmu veřejnosti posledních let, lze usoudit, že témata jako jsou klimatické změny a s nimi související přírodní katastrofy, virová pandemie a s ní související omezení a dopady na podnikání nebo digitalizace světa a s ní související kybernetické útoky, patří nejen mezi vysoce aktuální témata, ale také i ta nejdiskutovanější. Dokonce se o nich dá hovořit jako o natolik vážných, že dokáží rozdělovat společnost a způsobovat občanské nepokoje. Ovšem diplomová práce se nezabývá politikou, ale dopady těchto rizik na jeden konkrétní podnik, který je předmětem práce. Mohou mít na podnik XYZ dopad uvedená rizika? Podnik XYZ se zabývá vývojem, výrobou a dodáváním automatizační, řídicí a přístrojové techniky. Z předmětu podnikání lze usoudit, že má pravděpodobně pravidelný provoz, který třeba v důsledku vládních omezení může být omezen nebo zastaven. Též lze usoudit, že pracuje s informačními technologiemi, je on-line, komunikuje elektronicky, v digitální podobě zpracovává data o svých klientech, a stejným způsobem má uložené své postupy, patenty a obchodní tajemství. Jinak řečeno může být ohrožena kybernetickým útokem. A samozřejmě lze předpokládat, že vlastní i hmotný majetek a činnost vykonává v nějaké konkrétní budově. To znamená, že může být ohrožena přírodními vlivy, jako je vichřice, krupobití, povodeň, zemětřesení či tornádo. Tato diplomová práce se zaměřuje na možnosti krytí vybraných rizik s cílem najít optimální variantu pojištění pro zvolený podnik, ale zároveň i s ohledem na jeho konkrétní potřeby. Vybrána byla kybernetická rizika, přerušení provozu a přírodní události.

2 Teoreticko-metodologická část práce

Obvyklým zájmem vlastníků, akcionářů a vedení podniku je nejen generovat zisk, ale také například udržitelný růst podniku a jeho ochrana před riziky, která mohou v tom nejhorším případě vést až k zániku podniku. Moderní přístup řízení podniku znamená také řízení rizik neboli management rizik či risk management. Kruliš (2011, s. 91) uvádí navíc výrazy risk control, risk engineering, rizikový management, rizikové inženýrství a ovládání rizik. K tomu dodává, že nevýhodou českých termínů je, že nevyjadřují, co je vlastně předmětem řízení – nejde zde totiž o řízení samotných rizik, ale o řízení podniku a jeho procesů z hlediska minimalizace rizik.

Norma ČSN ISO 31000 (2018) **management rizik** definuje jako koordinované činnosti k vedení a řízení organizace s ohledem na rizika. Častorál (2017, s. 53) považuje management rizik za součást metod managementu, využívající strategický (koordinovaný) přístup manažerských opatření k rizikovým faktorům a rizikovým stavům založený na analýze, rozhodování a implementaci. Management rizik je dle Ducháčkové (2015, s. 24) racionální jednání v rizikové situaci tak, aby se chránila stávající a budoucí aktiva podniku. Kruliš (2011, s. 77) výrazem management rizik označuje postupy omezování (minimalizace) rizikovosti, jehož cílem je analyzovat současná i budoucí rizika a vhodnými opatřeními snižovat pravděpodobnost a závažnost jejich možných nežádoucích následků.

Cílem managementu rizik je dle Ducháčkové (2015, s. 24) dosažení bezpečné činnosti při co nejnižších nákladech na zajištění této bezpečnosti. Veber a kolektiv (2021, s. 365) o cílech managementu rizika píší, že management rizika obvykle sleduje více cílů. Jako jeho základní cíl je možné považovat zajištění přežití podniku (tj. minimalizaci nebezpečí výrazných finančních a jiných otřesů, ohrožujících samu existenci podniku), respektive udržení (či zvýšení pravděpodobnosti tohoto udržení) podnikatelské prosperity podniku.

Definování pojmu **riziko** není dle Ducháčkové (2015, s. 17) jednoduché, neboť pojem riziko je užíván z různého úhlu pohledu (hrozba ztráty, riziko ve spojení s podnikáním, investováním, nebezpečí chybného rozhodnutí, nebezpečí vzniku ztráty, zranitelnost systému, možnost ztráty či zisku), obecně ale pojem riziko zohledňuje odchýlení skutečnosti od očekávaných výsledků či vystavení se nepříznivým okolnostem. Ducháčková také riziko označuje za situaci, kdy buď existuje možnost nepříznivé odchylky od žádoucího výsledku, který je očekáván, nebo budoucí skutečnost je dopředu jednoznačně charakterizována pomocí počtu pravděpodobnosti, a lze vypočítat pravděpodobnost nastání příslušné události.

Veber a kolektiv (2021, s. 358) charakterizují **riziko** jako rys, který je spojen prakticky s každou aktivitou, produktem, ale i jevem a zahrnuje potenciál pozitivní nebo negativní skutečnosti (OK či KO faktoru) a to jak pro jedince, rodinu, podnik, občanskou společnost. Dle Vebera a kolektivu se dá specifikovat, obvykle kombinací pravděpodobnosti či četnosti výskytu a důsledku pro daný subjekt. Píší, že v praxi převažuje zájem o negativní projevy rizik v podobě poruch, podvodů, úrazů, nehod, havárií, požárů, povodní, epidemií, kolapsů, krizí a podobně s cílem jim předcházet nebo se před jejich důsledky chránit. Veber a kolektiv (2021, s. 359) dále uvádějí, že současné chápání rizika není jednotné a v odborné literatuře a stejně tak v praxi se lze setkat s mnoha poněkud odlišnými pojetími. Některá z nich jsou užší a zaměřují se především na negativní stránku rizika. Za riziko se pak například považuje možnost (pravděpodobnost) vzniku ztráty, možnost výskytu událostí, které zabrání či ohrozí dosažení cílů organizace, a nebezpečí (pravděpodobnost) negativních odchylek od stanovených úrovní cílů organizace.

Veber a kolektiv (2021, s. 359) označují tato rizika jako čistá a upozorňují, že v hospodářské praxi obvykle převažují rizika označovaná jako podnikatelská, která mají nejen negativní, ale

i pozitivní stránku. **Čisté riziko** (Pure risk) Veber a kolektiv popisují (2021, s. 360) jako riziko, které má jen stránku negativní, jinak řečeno zde existuje pouze nebezpečí vzniku nepříznivých situací, respektive nepříznivých odchylek od žádoucího stavu, za který se považuje uchování majetku, zdraví a lidských životů. Čistá rizika se obvykle vztahují ke ztrátám a škodám na majetku organizací a jednotlivců, poškození zdraví, respektive ztrátám života jednotlivců a členů organizačních jednotek, vyvolaných přírodními jevy (například povodně, požáry, zemětřesení a jiné), technickými systémy a jejich selháním (např. havárie výrobních zařízení) a jednáním lidí (krádeže a zpronevěry, stávky a podobně)

Stejné druhy rizik, ale trochu jinak, popisuje Ducháčková (2015, s. 18) tak, že v závislosti na povaze příslušného jevu či procesu mohou realizací příslušného rizika vzniknout buď výhradně negativní (záporné) odchylky od cíle, kdy se mluví o tzv. čistém riziku (nebezpečí ztrát), nebo záporné i kladné odchylky od cíle, kdy jde o takzvané spekulativní (záměrné) riziko (situace spojené s hraním hazardních her, sázením, spekulacemi na burze podnikáním a podobně), kdy je příslušným subjektem riziko dobrovolně postupováno. Ducháčková (2015, s. 19 a s. 25–26) používá mnohem komplexnější členění rizik na:

- přírodní vs. vyvolaná lidským faktorem (dále dělená na technická a vyvolaná lidmi),
- objektivní vs. subjektivní,
- systematická vs. jedinečná,
- vnitřní vs. vnější,
- ovlivnitelná vs. neovlivnitelná,
- a pojistitelná vs. nepojistitelná.

Ducháčková (2015, s. 25) uvedené rozdělení upřesňuje následovně. Objektivní se vyskytují nezávisle na lidech, na základě objektivně daných skutečností (například blesk). Subjektivní existují v závislosti na jednání a chování lidí (například neopatrnost). Systematická vyplývají z existence obecných externích faktorů působících na daný subjekt, a působí na všechny subjekty v rámci dané oblasti působení ekonomického subjektu. Jedinečná jsou spojena s podmínkami pouze příslušného ekonomického subjektu. Vnitřní existují podle Ducháčkové v souvislosti s vnitřními podmínkami prostředí a charakterem činnosti daného ekonomického subjektu. Vnější vyplývají z podmínek, ve kterých daný ekonomický subjekt funguje, kdy ekonomický subjekt má jen malou možnost tato rizika ovlivnit. Ovlivnitelná jsou rizika, která lze v rámci procesu managementu rizik řídit, a tedy ovlivňovat opatřeními jejich pravděpodobnost výskytu či velikost dopadů. Neovlivnitelná jsou podle Ducháčkové rizika, která nelze v rámci činnosti managementu rizik ovlivnit (například politická rizika). Pojistitelná jsou rizika, jejichž existenci lze řešit prostřednictvím standardních pojistných produktů, plní kritéria pojistitelnosti, přitom rozsah rizik, jejichž dopady lze řešit prostřednictvím pojištění, se postupně rozšiřuje (například uplatnění pojištění finančních ztrát). Nepojistitelná jsou rizika, jejichž důsledky za standardních podmínek nelze řešit prostřednictvím pojištění (někdy mohou být řešena specifickými finančními postupy).

Častorál (2017, s. 57) **rizika** dělí na řiditelná (ovlivnitelná) a neřiditelná (neovlivnitelná), což doplňuje o následující popis. U řiditelných rizik lze působit na příčinu jejich vzniku, působením na příčiny riziko omezovat nebo zcela vyloučit. Častorál (2017, s. 57) dále vysvětluje, že vzděláním, rozvojem schopností a dovedností lze eliminovat například některé negativní jevy v jednání lidí a v selhávání pracovníků. Upřesňuje, že neřiditelná (neovlivnitelná) jsou zpravidla rizika vnější, související s možnými živelnými pohromami nebo makroekonomickými dopady krizových situací a změn. Také píše, že inovacemi lze snižovat jejich nepříznivé důsledky. Jako smysl řízení rizika uvádí omezování příčin vzniku rizika, omezování četnosti výskytu rizika, snižování negativních důsledků (dopadů) rizika a srovnání nákladů na snížení rizika s přínosy tohoto snížení. Kruliš (2011, s. 91) naopak

uvádí, že rizika nelze v pravém slova smyslu řídit, pouze je lze řízením procesů a činností, které jsou jejich zdrojem, zjišťovat a snižovat jejich závažnost.

Veber a kolektiv (2021, s. 361) také rozlišují **rizika** na ovlivnitelná a neovlivnitelná a dodávají, že toto členění rizik souvisí s možností manažera, respektive firmy, působit na příčinu jejich vzniku. Jako ovlivnitelné pak chápou riziko, které lze eliminovat, respektive oslabit opatřením orientovaným na jeho příčiny, a to ve smyslu eliminace, respektive snížení pravděpodobnosti vzniku či rozsahu možných nepříznivých situací (např. zvýšením kvalifikace pracovníků výzkumu a vývoje a zlepšením jejich přístrojového vybavení lze snížit rizika výzkumu a vývoje výrobků a technologií). U neovlivnitelného rizika píší, že není možnost působit na jeho příčiny (např. nepříznivá změna měnového kursu, povodeň), ale lze přijmout opatření snižující nepříznivé následky těchto rizik (např. formou zajištění, pojištění). Vnitřní rizika jsou spíše ovlivnitelná, vnější rizika spíše neovlivnitelná.

Rizika, která jsou předmětem této diplomové práce, jsou čistá a spadají více do definice těch neovlivnitelných, ale rozhodně ne plně ovlivnitelných. Byť by podnik měl kupříkladu nainstalované ty nejspolehlivější antivirové programy a měl nastavené nejpřísnější bezpečnostní standardy, nikdy nedokáže zcela vyloučit všechny kybernetické hrozby. Jak se říká *„Zločinci jsou vždy o krok napřed“*. Podobně pokud by podnik dodržoval všechna hygienická opatření, umožnil práci na home office a podobně, nikdy nedokáže zcela vyloučit riziko přerušení provozu z důvodu nákazy nebo vládních nařízení. O ovlivnění přírodních událostí ani nemůže být řeč. Uzavření oken pomůže možná před blížící se vichřicí, nikoliv však před tornádem, které se prohnalo jižní Moravou. Proto je také vhodné mít záchrannou brzdu v podobě pojištění.

Ducháčková (2018, s. 18) uvádí, že pojem **riziko** je úzce spojen s **pojištěním**, a opačně. Dále pak, že se pojištění zabývá pouze riziky čistými, jejichž realizací vznikají takzvané náhodné potřeby. Ducháčková (2018, s. 22) rozlišuje dvě podoby těchto potřeb:

- konkrétní potřeby, tedy potřeby vyplývající ze škod, jejichž velikost lze přesně peněžně vyčíslit (například v případě zničení majetkové hodnoty lze určit přesně velikost této škody),
- abstraktní potřeby, tedy potřeby vyplývající ze škod, jejichž velikost nelze bezprostředně peněžně vyčíslit (zejména v případech škod na zdraví a životě člověka).

Účel **pojištění**, tedy jako formu krytí rizik, nepřímo vysvětluje Pacáková a kolektiv (2019, s. 5) takto: *“Pojišťovnictví se účelově věnuje náhodným jevům, jejichž důsledkem je pro osoby anebo podnikatelské subjekty vznik nějaké škody. Tyto jevy jsou nazývané pojistnými riziky a jejich realizace je nazývána pojistnou událostí. Ekonomické subjekty se snaží pomocí různých preventivních opatření předcházet realizaci těchto rizik a jejich možným důsledkům. Obecně však riziko není možné vyloučit. Jednou z možných forem finančního krytí rizika je pojištění. Každá pojistná událost má charakter náhodné události, obvykle velmi málo pravděpodobné, ale s mimořádně závažnými důsledky pro pojištěného v případě jejích vzniku. Pokud pojistná událost nastane, pojišťovna na základě sjednané pojistné smlouvy vyplácí pojistné plnění.”*

Pojištění dle Ducháčkové (2015, s. 23) znamená přenesení rizika na specializovanou instituci – pojistitele, vlastně se rovněž jedná o tvorbu rezerv na krytí rizik (prostřednictvím příspěvků na pojištění od jednotlivých zúčastněných), ovšem jde o tvorbu kolektivní rezervy, o rozdělení rizika mezi více zúčastněných a krytí rizik není ohraničeno naspořenými prostředky jednotlivého účastníka.

Smejkal (2018, s. 858) o **pojištění** píše, že patří mezi speciální, leč historicky zřejmě nejstarší formy přenosu rizika. Princip pojištění je z hlediska teorie rizik směna rizika velké ztráty

(škody) za jistotu malé ztráty (pojistného). Negativní důsledky rizika budoucí nepříznivé situace se přenesou na pojišťovnu, která kryje škody zcela nebo částečně (v závislosti na smlouvě mezi pojištěným a pojišťovnou).

Pojistné riziko Pacáková a kolektiv (2019, s. 7) definují jako možnost vzniku pojistné události, která je vyvolaná pojistným nebezpečím. Jde o událost, jejíž vznik je zpravidla spojen s finanční či jinou újmou. Právě kvůli pojistným rizikům se klienti pojišťují, aby minimalizovali, případně kompenzovali důsledky vzniklých škod. Pacáková a kolektiv (2019, s. 7) tentokrát již přímo popisují **pojištění**, a to jako finanční nástroj eliminace negativních důsledků realizace pojistných rizik.

O **pojištění** Veber a kolektiv (2021, s. 371) píší jako o klasickém nástroji přenosu rizika. Tradiční oblastí pojistné ochrany jsou čistá rizika, kdy pojišťovny nabízejí podnikatelům pojištění majetku pro případ požáru a dalších živelních škod, pojištění pro případ přerušení provozu v důsledku živelní události, pojištění odpovědnosti podnikatele za škody způsobené provozem podniku, včetně odpovědnosti za škodu způsobenou vadou výrobku, rozmanitá pojištění pro případ škod způsobených krádeží a vloupáním.

Kruliš (2011, s. 184) řadí přenos rizik na pojišťovny k běžným způsobům jejich řešení. Podniky placením pojistného snižují rizika velkých ztrát souvisejících s nezvládnutými riziky tím, že v případě nehody (škodní události) jim je část vzniklých škod nahrazena v rámci podnikatelského a majetkového pojištění, ale i pojištění zdraví a života. Pojišťovny a zajišťovny se tak stávají činitelem, který sehrává pozitivní roli při snižování hrozeb pro podniky, jejich pracovníky i materiální hodnoty.

Pro správnou orientaci v pojistných podmínkách jednotlivých pojistitelů je nezbytné znát obecnou terminologii, jinak řečeno základní pojmy, které jsou obecně používané v pojišťovnictví. Fojtíková a kolektiv (2020, s. 26–27) definují pojistnou hodnotu majetku (nová cena, časová cena, obvyklá cena), pojistnou částku, limity pojistného plnění, spoluúčast, indexaci, pojistné a výluky následovně.

Informace o **pojistné hodnotě** věcí jsou dle Fojtíkové a kolektivu (2020, s. 26) uvedeny v pojistných podmínkách, je zde vždy uvedena definice pojistné hodnoty a na jakou cenu jsou věci pojištěny, jedná se konkrétně o:

- **Novou cenu** = cena, za kterou lze stejnou nebo srovnatelnou věc, sloužící ke stejnému účelu, znovu pořídit v daném čase a na daném místě jako věc novou. Zpravidla jsou na novou cenu pojištěny nemovitosti i většina věcí v domácnosti (výjimky jsou uvedeny v pojistných podmínkách).
- **Časovou cenu** = cena, která se stanoví z nové ceny věci, přičemž se přihlíží ke stupni opotřebení nebo jiného znehodnocení anebo ke zhodnocení věci, k němuž došlo opravou, modernizací nebo jiným způsobem. Na časovou cenu jsou pojištěny například starší nemovitosti bez rekonstrukce, cizí věci, stavební materiál, starší elektronika, starší sportovní potřeby.
- **Obvyklou cenu** = cena, která by byla dosažena při prodeji stejné, případně obdobné věci v obvyklém obchodním styku v daném čase a na daném místě. Na obvyklou cenu je pojištěna například bytová jednotka, dále v domácnosti cennosti a věci zvláštní hodnoty.

Dle Fojtíkové a kolektivu (2020, s. 26) by **pojistná částka** měla odpovídat hodnotě pojištěného předmětu, je horní hranicí plnění, a některé pojišťovny stanovují tzv. minimální pojistnou částku, kdy výpočet je zpravidla dle metrů čtverečních a specifikace provedení či vybavení. V případě, že je v době pojistné události hodnota pojištěného předmětu vyšší než sjednaná pojistná částka, jedná se o podpojištění, v tomto případě má pojistitel právo snížit

pojistné plnění v takovém poměru, v jakém je pojistná částka k pojistné hodnotě pojištěného majetku. Většina pojišťoven má v pojistných podmínkách uvedeno, že odpovědnost za správně stanovenou pojistnou částku nese pojistník.

Limity pojistného plnění Fojtíková a kolektiv (2020, s. 27) definují jako horní hranicí plnění. V pojištění majetku se sjednávají limity pro určitá pojistná nebezpečí (např. zkrat a přepětí, atmosférické srážky, vandalismus, rozbití skel z jakékoliv příčiny a podobně) nebo skupiny věcí (např. elektronika, cennosti, věci zvláštní hodnoty, jízdní kola, věci v nebytových prostorech a podobně). Zpravidla jsou limity stanoveny procenty z pojistné částky anebo určitou výší. V některých případech lze limity navýšit za příplatek pojistného. V případě pojištění s limitem se neuplatňuje podpojištění.

Spoluúčast je dle Fojtíkové a kolektivu (2020, s. 27) částka, kterou se pojištěný podílí na pojistném plnění. Zpravidla je základní spoluúčastí částka jeden tisíc Kč, pojišťovnami jsou nabízeny různé spoluúčasti, a v případě vyšší spoluúčasti je nižší pojistné. Některé pojišťovny nabízejí možnost nulové spoluúčasti, a u některých pojistných nebezpečí má pojišťovna stanovenou pevnou spoluúčast, která je nadřazena smluvní spoluúčasti (povodeň a záplava, rozbití skel, elektromotory a podobně).

Indexaci Fojtíková a kolektiv (2020, s. 27) popisují jako aktualizaci pojistných částek, limitů a pojistného v závislosti na vývoji indexu životních nákladů a stavebního cenového indexu za uplynulý pojistný rok, a částečně může klienta chránit před podpojištěním. Indexaci je možné sjednat při uzavření smlouvy, a sjednání není povinné ani automatické.

Pojistné je dle Fojtíkové a kolektivu (2020, s. 27) stanoveno na základě výše pojistné částky, pojistného rozsahu a sazeb pojistného. Pojistné je možné hradit v různé frekvenci dle sjednaného pojistného období, a v případě ročního pojistného je u většiny pojišťoven přiznána sleva na pojistném. Pojišťovnami je nabízeno několik způsobů úhrady pojistného (složenkou, příkazem, SIPO a podobně).

Dle Fojtíkové a kolektivu (2020, s. 27) mají pojišťovny stanoveny **výluky** z pojištění, které jsou podrobně uvedeny v pojistných podmínkách. Ve všeobecných pojistných podmínkách se výluky vztahují k celkovému pojištění majetku, a v doplňkových nebo zvláštních pojistných podmínkách k pojištění určitého předmětu (nemovitost, domácnost).

Ducháčková (2015, s. 45) popisuje hlavní účastníky pojistného vztahu takto:

- **Pojistitel** = právnická osoba, která má oprávnění provozovat pojištění, tj. Pojišťovna případně jiná instituce, které bylo uděleno 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, na jejíž majetek, odpovědnost za škody, život nebo zdraví se pojištění vztahuje. Osoba, které vzniká na základě uzavřené pojistné smlouvy právo na pojistné plnění, a to bez ohledu na to, zda pojištění sjednala sama, nebo jiná osoba (pojistník).
- **Poškozený** = osoba, které bude vyplaceno pojistné plnění v souvislosti se sjednaným pojištěním odpovědnosti za škodu. V rámci pojištění odpovědnosti za škodu jsou hrazeny právní nároky osob za škody, za které odpovídá pojištěná osoba. Osoba poškozený není při sjednávání pojistné smlouvy známa.

Ducháčková (2015, s. 47–48, 51 a 247) uvádí i další základní definice:

- **Pojistný produkt** = určitý druh pojištění, který se vztahuje na vymezená pojistná nebezpečí (například živelní pojištění) nebo na vymezené objekty pojištění (například pojištění domácnosti).
- **Pojistné podmínky** = obsahují právní úpravu určitého pojistného produktu. Uplatňují se všeobecné a tzv. Zvláštní pojistné podmínky.
- **Všeobecné pojistné podmínky** = pojistné podmínky pro určitý pojistný produkt. Všeobecné pojistné podmínky určují charakteristiku pojmu pojistná událost (vymezení rizik krytých v rámci daného pojistného produktu včetně výčtu výluk z pojištění), způsob uzavření pojistné smlouvy, začátek, dobu trvání a ukončení pojištění, výluky z pojištění, předmět pojištění, podmínky poskytování a způsob propočtu velikosti pojistného plnění. Jsou součástí pojistné smlouvy.
- **Zvláštní pojistné podmínky** = konkrétní pojistné podmínky pro dané pojištění, konkretizují všeobecné pojistné podmínky. Zvláštní pojistné podmínky jsou dohodnuty v pojistné smlouvě.
- **Pojistná smlouva** = představuje právní dokument, který završuje dvoustranný právní akt, na jehož základě vzniká smluvní pojištění fyzických a právnických osob. Pojistná smlouva se vyhotovuje v písemné formě podle platných právních předpisů. Vyjadřuje konkrétní pojistné podmínky a podmínky realizace pojištění. Dohodnuté podmínky jsou závazné pro pojišťovnu i pro druhou stranu. V některých případech vzniká pojištění i bez písemné pojistné smlouvy. Jde o zákonná pojištění a o pojištění, která mají krátkodobý charakter (např. pojištění při přepravě zboží, tzv. známkové pojištění). Pojistnou smlouvou se pojistitel zavazuje poskytnout ve sjednaném rozsahu plnění, pokud nastane nahodilá událost, která je ve smlouvě podrobně specifikovaná.
- **Nahodilá událost =** událost, která je možná a u které není jisté, zda v době trvání pojištění vůbec nastane nebo není známa doba jejího vzniku.
- **Pojistná událost** = nahodilá skutečnost blíže označená v pojistné smlouvě nebo ve zvláštním právním předpise, na který se pojistná smlouva odvolává, a se kterou je spojen vznik povinnosti pojistitele poskytnout pojistné plnění.
- **Pojistné plnění** = v případě, že dojde k pojistné události, pojistitel provede náhradu, obvykle v podobě finanční, ovšem v některých případech i ve formě věcného, naturálního plnění. K naturálnímu plnění dochází v případě uplatnění tzv. asistence (technická, právní, zdravotní).

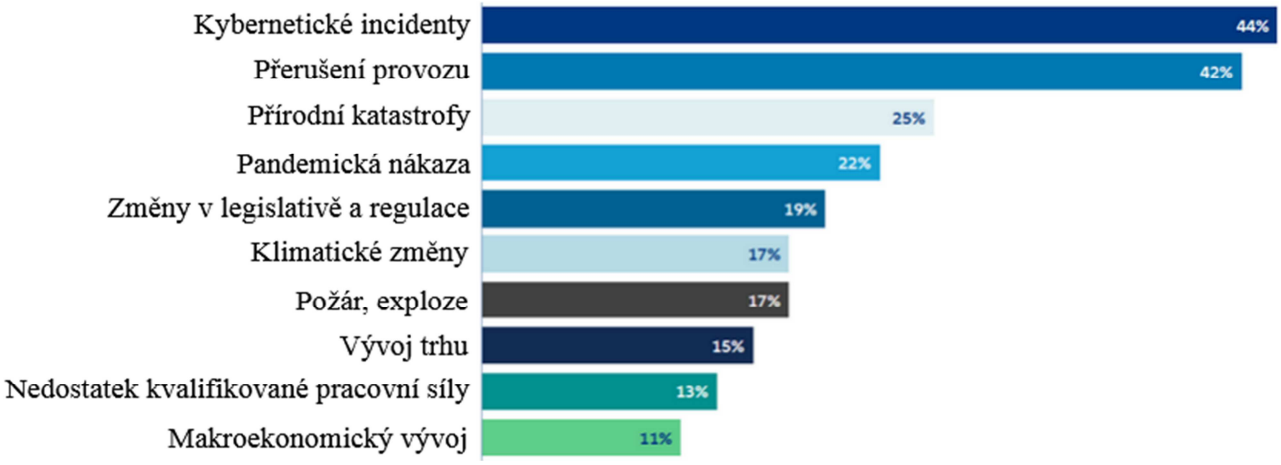
Tyto a další definice jsou běžně součástí pojistných podmínek jednotlivých pojistitelů a vzájemně se mohou lišit v konkrétní formulaci, měně však po obsahové stránce.

2.1 Aktuální trendy v oblasti pojištění rizik

Allianz Global Corporate & Specialty SE (dále jen AGCS) zveřejňuje pravidelně každý rok výsledky průzkumu Risk Barometr, který na základě poznatků 2 650 expertů z oblasti risk managementu z 89 zemí světa sestavuje žebříček nejzávažnějších a nejčastějších celosvětových podnikatelských rizik, kterým je potřeba věnovat pozornost. Průzkum je zaměřen na velké, střední a malé podniky. Nejnovější, jedenáctý průzkum v pořadí, který je pro rok 2022, ukazuje aktuální trendy, kde se na prvním místě umístily kybernetické incidenty, na druhém přerušení provozu, a na třetím přírodní katastrofy. Kybernetické incidenty jsou tak globálně největší obavou podniků, a na první místo jej zařadilo 44 % respondentů (stalo se tak teprve podruhé v historii průzkumu). Přerušení provozu zařadilo na druhou příčku s mírným odstupem 42 % respondentů, a přírodní katastrofy jsou s 25 % na třetím místě. Za zmínku ještě stojí riziko klimatických změn, které v žebříčku velmi rychle

roste napříč podniky a aktuálně zaujímá svou dosud nejvyšší, a to šestou pozici. Celkové pořadí rizik přehledně znázorňuje graf 1.

Graf 1 Celkové pořadí rizik, kterým se aktuálně věnuje největší pozornost

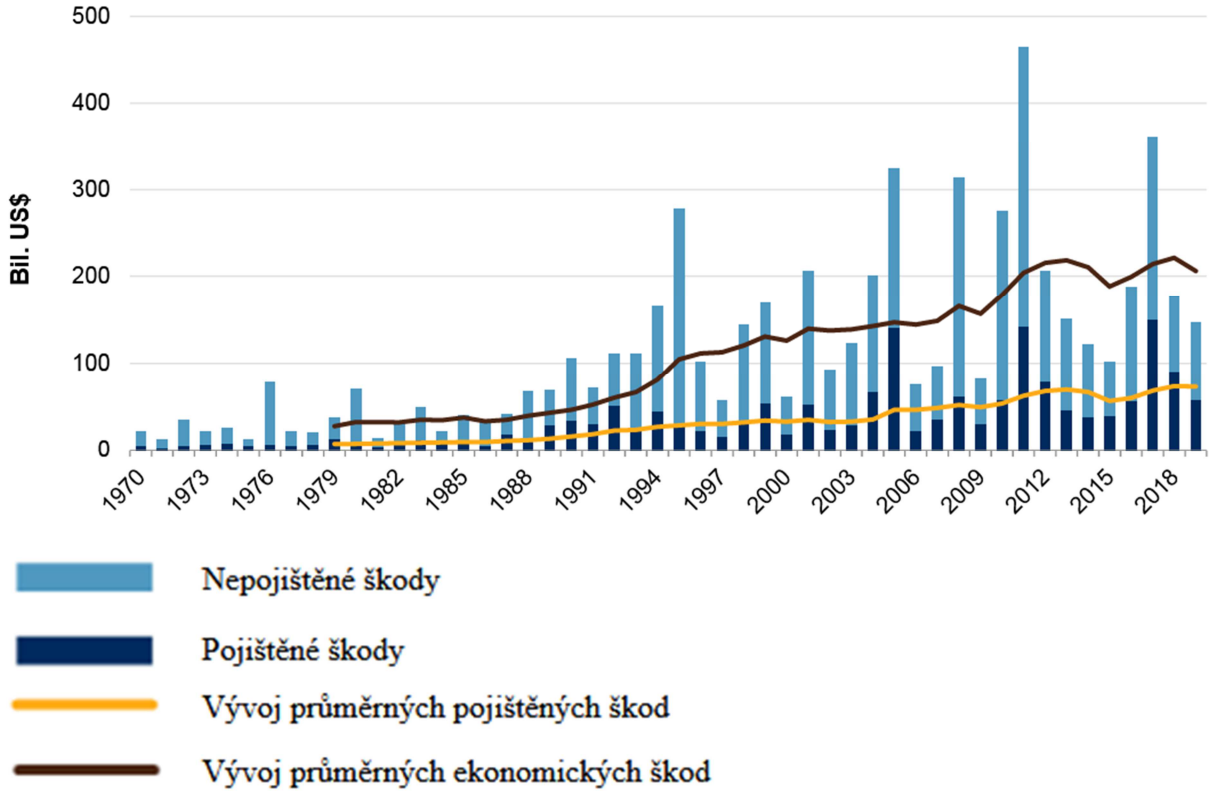


Zdroj: Allianz Global Corporate & Speciality SE (2022)

Dle S&P Global Inc. (2020a), dále jen SPG, pandemie Covid-19 tlačí pojišťovny, aby urychleně zareagovaly na **megatrendy – především změnu klimatu a digitalizaci**, což bylo také probíraným tématem na konferenci SPG, které se účastnili evropští pojišťovací manažeři, experti a analytici. Dle SPG (2020a) změny klimatu a dopad klimatických rizik na současný model pojišťovnictví bylo na konferenci *„více než miliardová otázka“*. Účastnice konference Amanda Blanc, skupinová CEO Aviva PLC, uvedla, že roky 2010–2019 byly pro pojišťovnictví nejnákladnější dekádou vlivem změn klimatu s náklady okolo třech bilionů liber. Bylo zaznamenáno více případů záplav, lesních požárů s nárůstem jejich frekvence a závažnosti, kdy pro pojišťovny bude do budoucna obtížnější poskytnout krytí, pokud se něco nezmění. K tomu ještě dodala, že si myslí, že ve čtyřstupňovém světě, kam pojišťovnictví směřuje, bez změny nebude pojistný model vůbec fungovat. Blanc na konferenci zdůrazňovala, že největším rizikem pro planetu jsou klimatické změny, které podtrhávají důležitost řízení rizik. Zároveň považuje za důležité chopit se těchto rizik a přeměnit je na příležitosti.

SPG (2020b) poukazuje na skutečnost, že přírodní katastrofy, které zahrnují extrémní přírodní události, celosvětově nastávají s čím dál větší frekvencí. Proto očekávají, že v důsledku změn klimatu a rostoucích teplot, poroste i počet extrémních jevů počasí. Zároveň informují, že nepojištěné škody z přírodních nebezpečí rostou rychleji než ty pojištěné, což přehledně ukazuje graf 2.

Graf 2 Porovnání růstu pojištěných a nepojištěných škod z let 1970–2019



Zdroj: Swiss Re Insitute (2020)

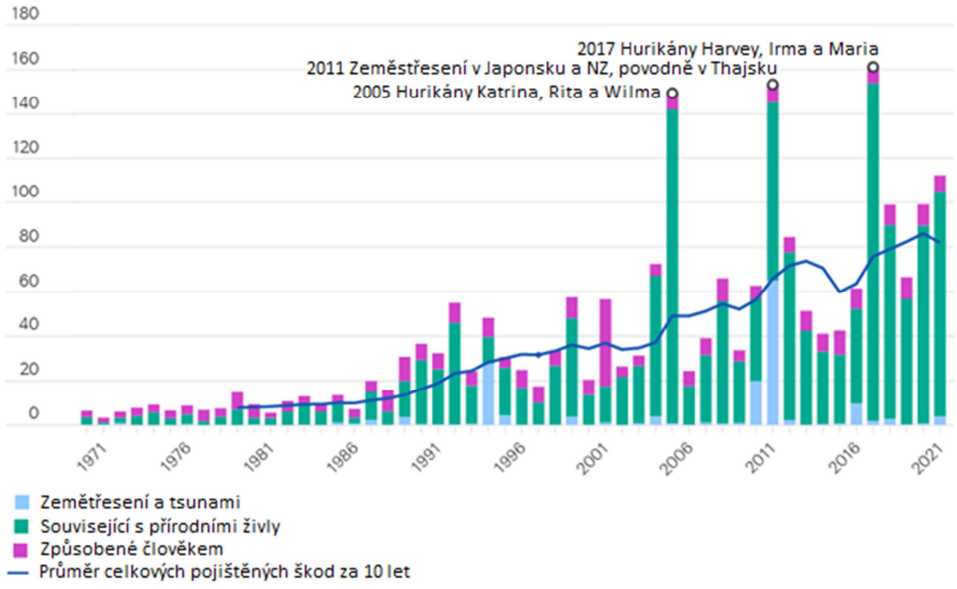
Česká asociace pojišťoven (dále jen ČAP) pravidelně zveřejňuje statistiky, kde uvádí celkové počty škod z pojištění majetku občanů, škody z pojištění majetku podnikatelů a škody na motorových vozidlech. Dle údajů za poslední tři roky a jejich meziročního srovnání patří k nejčetnějším pojistným událostem, a tedy rizikům vodovodní škody, vichřice, atmosférické srážky, povodně a dále pak škody na elektronice (přepětí, zkrat a ostatní poškození). Srovnáním celkové roční výše škod, patří mezi nejzávažnější rizika požár, vichřice, vodovodní škody, poškození nebo zničení stroje, a povodeň. Uvedená data lze nalézt v příloze 1–3. Dále pak dle tiskové zprávy ČAP (2022) došlo v roce 2021 k rekordnímu objemu škod z přírodních katastrof od roku 2013. ČAP (2022) konkrétně píše, že v pojištění majetku řádění živlů (povodně, vichřice, krupobití, srážky, tíha sněhu) v roce 2021 způsobilo škody, které dosáhly enormní částky téměř šest a půl miliardy korun, a proti roku 2020 s objemem škod v úhrnu za skoro tři miliardy korun se jedná o nárůst o 117 %. Jedná se tak celkově o nejvyšší nominální hodnotu pojištěné škody v tomto segmentu od roku 2013, kdy došlo dosud k posledním rozsáhlým povodním na velké části území Čech. Dále uvádí, že rozhodující nárůst škod z přírodních katastrof v roce 2021 nastal v souvislosti s řáděním tornáda na jižní Moravě v segmentu škod z vichřic, krupobití a atmosférických srážek, kde objem pojištěných škod za celý rok 2021 dosáhl v ČR částky 5,77 miliardy Kč a proti 2,175 miliardy Kč v roce 2020 se navýšil o 165 %. Jedná se tak o rekordní hodnotu v této skupině rizik od počátku celé časové řady v roce 2006. ČAP pozoruje i výrazný růst pojištěných škod u požárů. Ve své tiskové zprávě za rok 2021 píše, že počet pojistných událostí v souvislosti s požárem nemovitostí se pohybuje kvartálně poměrně stabilně kolem průměrné hodnoty 1242 pojistných událostí. U souvisejícího finančního objemu pojistných událostí platilo, že až do konce druhého čtvrtletí 2021 dosahoval jejich kvartální objem částky většinou v rozmezí mezi 400 až 600 milióny Kč. Ke zcela zásadně odlišnému výsledku došlo v obou čtvrtletích druhého pololetí 2021, kdy objem pojistných událostí z požárů narostl téměř na dvojnásobnou

hodnotu a v obou obdobích překročil částku jedné miliardy korun. V důsledku toho se průměrná škoda z požáru navýšila v druhém pololetí 2021 z dlouhodobě stabilní hodnoty 367 tisíc korun na 860 tisíc korun.

Zajišťovna Swiss Reinsurance company (2022), dále jen Swiss Re, která je jedním z předních světových poskytovatelů zajištění, pojištění a dalších forem převodu rizik založených na pojištění, na svých webových stránkách uvádí, že změna klimatu představuje jedno z nejrozšířenějších rizik pro planetu Zemi a prosperitu jejích obyvatel. Jeho účinky jsou již evidentní a mají dopady na krajinu jako je vyšší průměrné teploty, stoupající hladina moří, delší a častější vlny veder, silné bouře a srážky, více povodní a záplav, lesní požáry a extrémní počasí. Swiss Re (2022) uvádí, že identifikovala hrozbu změny klimatu již v roce 1979, a od té doby analyzuje její dopady na společnost a pojišťovnictví. Dle Swiss Re (2022) jsou dopady změn klimatu viditelné na jejích statistikách o přírodních katastrofách, kdy za poslední tři desetiletí se průměrné výše škod způsobené extrémními povětrnostními událostmi více než zdvojnásobily. Hlavním důvodem dramatického nárůstu škod způsobených přírodními katastrofami je ekonomický a populační růst v exponovaných oblastech, který se dále zhoršuje v měnícím se klimatu. Vzhledem k tomu, že většina škod způsobených přírodními katastrofami není kryta pojištěním, miliony domácností a podniků čelí velkým a zvětšujícím se mezerám v ochraně. Swiss Re v době psaní této diplomové práce ještě nezveřejnila souhrnná čísla za rok 2021, ovšem dle odhadu Swiss Re Institute (2021), globální pojištěné škody z katastrof vzrostou za rok 2021 na celkových 112 miliard dolarů, což je čtvrté nejvyšší číslo od roku 1970. Po seřazení od největších škod, byly větší škody způsobeny jen v letech 2017, 2011 a 2005. V roce 2017 se jednalo o hurikány Harvey, Irma a Maria. V roce 2011 to byly povodně v Thajsku a zemětřesení v Japonsku a na Novém Zélandu. V roce 2005 byly škody způsobeny hurikány Katrina, Rita a Wilma. Dle Swiss Re Institute (2021) škody způsobené přírodními katastrofami budou pravděpodobně nadále růst více než globální HDP vzhledem k nárůstu bohatství, urbanizace a změn klimatu.

Jak je patrné z grafu 3 od Swiss Re Institute, výše škod způsobených přírodními katastrofami a jejich podíl na celkových vzniklých škodách má stoupající tendenci. Naopak škody způsobené člověkem si drží relativně stabilní výši s mírným postupným nárůstem. Uvedená čísla se týkají škod na majetku a nezahrnují nároky související s Covid-19.

Graf 3 Pojištěné škody od roku 1970 (v amerických dolarech a cenách roku 2021)



Zdroj: Swiss Re Institute (2021)

Světová meteorologická organizace (2021), dále jen WMO, ve své komplexní zprávě uvádí, že se katastrofy související s počasím, klimatem nebo vodním nebezpečím za posledních padesát let vyskytovaly v průměru každý den, kdy denně zabily 115 lidí, a způsobily ztráty ve výši 202 milionů dolarů. WMO dále píše, že počet katastrof se za padesát let zvýšil pětinásobně, což je způsobeno změnou klimatu, extrémnějším počasím, ale i lepším podáváním zpráv.

Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění (2019, s. 3), dále jen EIOPA, uvádí, že kybernetické hrozby jsou v posledních letech stále výraznější, a proto jsou stále více považovány za největší globální riziko pro finanční sektor a ekonomiku jako celek. Dle této instituce rostoucí frekvence a sofistikovanost kybernetických útoků, rychlá digitální transformace a rostoucí využívání velkých dat a také služby „cloud computing" nutí pojišťovny stále více vnímat a reagovat na kybernetické hrozby. Pojišťovací skupiny jsou také přirozeným cílem kybernetických útoků, jelikož mají značné množství důvěrných informací o klientech (pojistnících, pojištěných). EIOPA na druhé straně digitální ekonomiku a technologický pokrok vnímá jako příležitosti k úpisu kybernetických rizik. EIOPA (2021) vnímá **souvislost mezi pandemií Covid-19 a kybernetickými riziky**, jelikož pandemie urychlila digitální transformaci. To vysvětluje tak, že nyní se podniky více spoléhají na digitální a vzdálená řešení při provádění svých každodenních operací a poskytování svých služeb zákazníkům. I když to přineslo výhody, rostoucí závislost na digitálních řešeních také zvýšila riziko kybernetických útoků. Banka pro mezinárodní vypořádání (2021, s. 4–6), dále jen BIS, ve své nedávné studii o Covid-19 a kybernetických rizicích ve finančním sektoru odhalila, že finanční sektor zažil největší počet kybernetických událostí souvisejících s Covid-19 po sektoru zdravotnictví. Nejvíce jsou postiženy platební instituce, pojišťovny a družstevní záložny.

Také SPG (2020c) vidí souvislost mezi Covid-19 a narůstajícím počtu kybernetických útoků. Ve svém článku popisuje jak pandemie Covid-19 změnila způsoby, jak lidé nakupují, učí se a pracují, a to má významný vliv na kybernetická rizika. Elektronické obchodování zažívá *„boom"*, kamenní prodejci přecházejí na digitální platformy a školy a kanceláře přijaly online kurzy a práci z domova. Pro organizace to znamenalo přehodnotit strategie digitalizace a zdvojnásobit výdaje na informační technologie, kapacitu cloudu a infrastrukturu s cílem zvýšit šířku pásma, zajistit kontinuitu podnikání a udržet si zákazníky. SPG věří, že tyto trendy digitalizace tu zůstanou a nevyhnutelně povedou k vyšší pravděpodobnosti kybernetických incidentů, protože podniky zvýší svou digitální stopu nebo vůbec poprvé vstoupí do digitálního prostoru. Dále uvádí, že tempo digitalizace a propojení dat se bude jen zvyšovat, to bude řízené trendy, jako je internet věcí, sociální média, mobilní sítě páté generace a Průmysl 4.0. To znamená, že kybernetická bezpečnost, cloud a ochrana dat bude muset být nejvyšší prioritou podniků, aby se vypořádaly s novými sofistikovanými kybernetickými hrozbami. V této souvislosti se SPG domnívá, že stále více podniků bude zvažovat kybernetické pojištění jako doplněk širších strategií řízení kybernetických rizik.

Smejkal (2018, s. 844) do budoucna předpokládá následující vývoj v oblasti kybernetické kriminality (ze seznamu vybrány pouze relevantní pro účely této DP):

- objektem útoků budou v převážné většině nehmotné informace (programy a data), nikoliv hmotné prostředky informačních systémů a technologií,
- nebude klesat objem kriminálního jednání vlastních zaměstnanců (aktivní krádež dat nebo nedbalostní prozrazení či umožnění útoku, ale i krádež zařízení obsahující data.

Dle zprávy **Národního úřadu pro kybernetickou a informační bezpečnost** (2021, s. 3), dále jen NÚKIB, se rok 2020 vyznačoval nárůstem počtu kybernetických útoků proti českým institucím, organizacím a firmám ve všech sektorech. V roce 2020 bylo NÚKIB nahlášeno

468 incidentů oproti 217 incidentům v roce 2019. Téměř třetinu z řešených incidentů nahlásily neregulované subjekty. Za tímto nárůstem stojí velmi pravděpodobně vyšší počet kybernetických útoků i větší povědomí o existenci a aktivitách NÚKIB. Vzrostla také závažnost incidentů, jak ukazují útoky proti Fakultní nemocnici Brno nebo Psychiatrické nemocnici Kosmonosy. Nejčastějšími typy útoků byly v roce 2020 podle NÚKIB spam, phishing a scanning.

2.2 IT hrozby a kybernetické pojištění

Dle Organizace pro hospodářskou spolupráci a rozvoj (2016), dále jen OECD, kybernetická rizika představují skutečnou hrozbu pro společnost a hospodářství, což lze doložit na rostoucí pozornosti věnované této hrozbě ve velkém rozsahu v médiích.

Veber a kolektiv (2021, s. 365) píší, že v souvislosti s rozšiřováním digitalizace a hackerskými útoky vyvstává u řady firem a institucí nutnost aplikovat management rizika směrem k zajištění ICT bezpečnosti.

Pastoráková a kolektiv (2020, s. 17) uvádějí, že informační věk sice umožňuje okamžitý přenos informací a dat, ty se však shromažďují, třídí a přenáší elektronicky. Jejich ochrana je právě proto o mnoho náročnější, a krádež ve fyzické podobě byla vystřídána elektronickou krádeží včetně krádeže identity jako projevu hospodářské kriminality.

Doucek a kolektiv (2019, s. 12) vysvětlují, že informační systémy se v dnešní době poměrně často stávají oběťmi útoků různých druhů lidí, kteří svou lehkomyslností systém poškodí nebo kteří chtějí získat neoprávněnou výhodu z průniku do cizího informačního systému nebo kterým jen stačí pocit, že jsou tak dobří, že jsou schopni překonat ochranná bezpečnostní opatření informačního systému. Jako důvod vidí postupující proces globalizace regionálních ekonomik, i jejich informačních systémů, který usnadňuje takovým lidem možnosti útoků na informační systémy organizací zejména proto, že dochází k neustálému vzájemnému propojování informačních systémů do větších celků a tím roste i jejich zranitelnost vůči hrozbám, které mohou omezit jejich provoz nebo jej dokonce zcela zastavit. Doucek a kolektiv (2019, s. 13) ještě zmiňují digitalizaci světa, kdy stále více dat je předáváno v digitální formě. Dále pak, že stále významnější a důležitější data z pohledu celé společnosti jsou uložena v informačních systémech a v případě jejich výpadku by byla ohrožena větší část společnosti.

Nejedná se ale o zcela nový trend posledních pár let, trvá však již od počátku milénia. Již Janata (2004, s. 9) před téměř 20 lety předpokládal, že vědeckotechnický pokrok v mnohém obohatil život lidí, rozšířil jejich obzory, umožnil prosperitu a růst populace, ale nové objevy a vynálezy přinášejí nová rizika. Jako příklad uvádí informační technologie, které v posledních letech zaznamenaly velký rozvoj. Za nové rizikové faktory, se kterými nikdo nepočítal, považuje viry a počítačové piráty. Uvádí i další příklad, který nikdo nepředpokládal, a to, že zničení počítačového systému nepřítele se stane prvořadým strategickým cílem v případě válečného konfliktu.

2.2.1 Základní pojmy v kontextu IT hrozeb

Aby bylo možné správně pochopit kybernetické pojištění, je nejprve nutné pochopit pojmy s ním spojené, které se mohou vyskytovat v pojistných podmínkách jednotlivých pojistitelů. Jedná se zejména o pojmy jako je kybernetická hrozba, riziko, incident či útok.

Hrozba je potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace (ISO 27000, 2018).

Kybernetický prostor je globálně propojený prostor, který se skládá z internetu a dalších počítačových sítí, digitálních zařízení, systémů, služeb a procesů na nich. Tím poskytuje globální infrastrukturu pro široké spektrum osobních, podnikatelských i správních aktivit a pro jejich propojení (ISO 27100, 2018).

Kybernetická hrozba je hrozba, která se nachází v kybernetickém prostoru (ISO 27100, 2018).

Doucek a kolektiv (2019, s. 24) rozdělují hrozby především na:

- **přírodní a fyzické** – živelné pohromy a nehody jako jsou například poruchy v dodávce elektrického proudu, požáry, povodně, vichřice a podobně,
- **technické a technologické** – poruchy nosičů dat, počítačů nebo jiných technologických komponent IS/ICT, poruchy sítí, poruchy způsobené programy – nesprávná funkčnost, například nedostatečně otestované programové vybavení, viry, trojské koně a podobně,
- **lidské**
    - **neúmyslné**, které vyplývají z neznalosti nebo zanedbání plnění povinností,
    - **úmyslné**, které rozdělujeme na působící:
        - **zvenku systému** – hackeři, teroristé, mezifiremní špionáž a podobně,
        - **zevnitř** – zlomyslní, zneuznaní, chamtivý zaměstnanci, hosté a návštěvníci organizace a podobně.

Kybernetické riziko je riziko způsobené kybernetickou hrozbou (ISO 27100, 2018).

Šulc (2018, s. 10) za **kybernetické riziko** označuje situaci, kdy existuje určitá hrozba, která by mohla zneužít nějaké zranitelnosti a způsobit škodu.

CRO Forum (2019, s. 5) **kybernetické riziko** definuje jako jakékoliv riziko vznikající při používání elektronických dat a jejich přenosu včetně technologických nástrojů, jakými jsou internet a telekomunikační sítě. Dále pak také zahrnuje fyzickou škodu, která může být způsobena kybernetickým incidentem, podvod spáchaný zneužitím dat, odpovědnost vznikající při uchovávání dat a dostupnost, integritu a důvěrnost elektronických informací – může se vztahovat k jednotlivcům, právnickým osobám o státu.

Kybernetický incident je kybernetická událost, která způsobuje ztrátu informační bezpečnosti nebo má dopady na procesní aktivity organizace (ISO 27103, 2018).

Doucek a kolektiv (2019, s. 20) rozlišují zejména 5 typů **kybernetických incidentů**:

- **Závady v systému nebo jeho špatná funkcionalita**. Situace nastane, když napadený systém nebo počítačová síť způsobí škodu systému třetí strany nebo systém dodavatele služeb není funkční, a to má dopad na ostatní činnosti v kybernetickém prostoru.
- **Prolomení ochrany důvěrnosti dat**. Data uložená v systému jsou zcizena nebo kompromitována. Stejná je situace i v případě, že je systém spravován nebo hostován třetí stranou.
- **Byla ztracena dostupnost dat nebo byla porušena jejich integrita**. Data, uložená v systému byla poškozena nebo smazána. Stejná je situace i v případě, že je systém spravován nebo hostován třetí stranou.
- **Poškozující aktivita**. Zneužití technologie za účelem způsobit poškození (jako je například kybernetická šikana na sociálních sítích nebo snaha získat přístup k datům za účelem jejich smazání) nebo získat nezákonný prospěch, např. Kybernetický podvod.

- **Lidská chyba**. Byla-li člověkem provedena nějaká neúmyslná operace, která poškodila systém, počítačovou síť, informaci nebo službu.

Kolouch (2016, s. 55) chápe **kybernetický útok** jako jakékoliv protiprávní jednání útočníka v kybernetickém prostoru, který směřuje proti zájmům jiné osoby. To dále upřesňuje, že tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného, a kybernetický útok může být dokonán, stejně jako může být ve stádiu přípravy či pokusu.

Doucek a kolektiv (2019, s. 184) klasifikují **neveřejné informace** na interní informace, jejichž ohrožení sice může vést k ohrožení zájmů organizace, ale které nenaplňují požadavky na legislativní či smluvní ochranu, a dále pak ostatní informace, u nichž práce s nimi bývá nějakým způsobem regulována, a které popisují následovně.

- **Osobní údaje** jsou informace, jejichž nutnost ochrany vyplývá z Obecného nařízení o ochraně osobních údajů (anglicky General Data Protection Regulation), zkráceně GDPR, plným názvem Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.
- **Obchodní tajemství** jsou informace, u nichž si organizace stanovila nutnost jejich ochrany podle §504 zákona č. 89/2012 Sb., občanský zákoník.
- **Informace smluvní strany** jsou ty informace, jejichž nutnost ochrany vyplývá ze smluvních závazků nebo jiných požadavků.
- Mezi **přísně důvěrné informace** se řadí informace, které mají charakter obchodního tajemství podle §504 zákona č. 89/2012 Sb., občanský zákoník, jejichž ohrožení vede k poškození strategických a klíčových zájmů organizace. Typickým zástupcem kategorie přísně důvěrných informací může být zvláštní kategorie osobních údajů ve smyslu článku 9 Obecného nařízení EU o ochraně osobních údajů č. 2016/679 (GDPR). Někdy se také používá termín citlivé údaje.
- **Informace utajované** se týkají důležitých informací odrážejících klíčové státní zájmy, a proto jsou převážně zpracovávány státními orgány. Obecně lze utajované informace definovat jako informace, podléhající ochraně podle zákona č. 412/2015 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Jedná se o informace, které by v případě zneužití mohly způsobit újmu zájmům České republiky nebo zájmům, k jejichž ochraně se Česká republika zavázala, nebo by mohly být pro tyto zájmy nevýhodné, a které jsou uvedeny v seznamu utajovaných informací.

Zákona č. 412/2015 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti dále utajované informace klasifikuje stupněm utajení na přísně tajné, tajné důvěrné a vyhrazené. Dle AEC (2018, s. 13) si podnik pomocí vnitřního předpisu určí tři až pět tříd/kategorií, do kterých informace klasifikuje. Kritériem pro třídění bývá nejen důvěrnost, ale i přístup. Pro pojmenování tříd se nejčastěji používají označení veřejné (neklasifikované), interní (pro vnitřní potřebu) a chráněné (citlivé, důvěrné).

2.2.2 Předpisy a zákonná úprava

Jak již bylo zmíněno, ochrana osobních údajů v evropském prostoru se řídí GDPR, které začalo platit 25. 5. 2018 a v důsledku toho byla upravena i česká legislativa. To znamená zákon č. 101/2000 Sb., o ochraně osobních údajů byl zrušen a nahrazen zákonem č. 110/2019 Sb., o zpracování osobních údajů, který upřesňuje zavedení nařízení GDPR. Prolomení

ochrany důvěrnosti dat (typ kybernetického bezpečnostního incidentu) může mít za následek porušení GDPR, což může vést k udělení vysokých sankcí.

Kybernetická bezpečnost je upravena zákonem č. 181/2014 Sb. o kybernetické bezpečnosti, který zapracovává příslušné předpisy Evropské unie, konkrétně se jedná o směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

NÚKIB upřesňuje, že zákon o kybernetické bezpečnosti, se nevztahuje plošně na všechny občany a instituce v České republice. Dále uvádí, že zákon je závazný pro všechny subjekty stanovené v § 3 a že zákon nerozlišuje mezi tím, jestli je subjekt soukromou společností nebo státní institucí – podstatné je jen splnění charakteristik nebo kritérií pro určení jednotlivých povinných osob podle § 3. Dodržování zákona probíhá prostřednictvím kontroly NÚKIB, který vedle uložení pokuty může přistoupit také k uložení nápravného opatření, jehož přijetí je oprávněn kontrolovat.

2.2.3 Kybernetické pojištění

Kybernetické pojištění pokrývá nebo redukuje finanční ztráty, které byly způsobeny kybernetickým incidentem (ISO 27103, 2018). Organizace pro hospodářskou spolupráci a rozvoj (2016) uvádí, že pojištění kybernetické bezpečnosti je jedním ze způsobů přenosu rizika spojeného se vznikem finančních nákladů způsobených kybernetickým útokem a zároveň se jím zajišťuje asistence postiženým. Navíc kybernetické pojištění slouží podpůrně k omezení rizika, protože motivuje k vytváření opatření pro snížení škod a jejich předcházení.

Dobiáš (2019, s. 241) tvrdí, že většina pojišťoven na českém pojistném trhu nabízí pojištění kybernetických rizik (někdy nazývané jako pojištění internetových rizik) v rámci svých jiných produktů (např. pojištění domácnosti, nebo připojištění elektronických a strojních zařízení v nemovitostech) nebo umožňuje uzavření pojištění těchto pojistných rizik při uzavření pojištění *"na míru"*. To dále upřesňuje, že pod pojem *"internetové pojištění"* zahrnuje pojištění fyzických osob a případně osob žijící s touto osobou ve společné domácnosti, a pojištěním kybernetických rizik se rozumí pojištění právnických osob, a to zejména obchodních společností.

Zda nebo do jaké míry bude kybernetický útok hrazen pojišťovnou, dle SPG (2020c) závisí na tom, jak podnik řídí kybernetická rizika. Mnoho škod vzniká proto, že strategie kybernetické bezpečnosti v podniku chyběla nebo nebyla dostatečná, aby odolala útoku. Pro podniky může kybernetický incident vést mimo jiné k přerušení provozu, platbám výkupného, poklesu reputace a potenciální pokutě od regulátora. Dle názoru SPG by mělo kybernetické pojištění nabízet více než jen čistou náhradu za potenciální významnou finanční ztrátu. Pojistitelé mohou navíc poskytnout asistenční služby a také pomoct pojistníkům lépe zvládat kybernetická rizika. To by byla pro klienty klíčová výhoda, která by jednotlivým pojistitelům umožnila odlišit se od konkurence a pomohlo by snížit frekvenci a závažnost kybernetických škod. Efektivnější kybernetická prevence a sofistikované řízení rizik silně korelují s nižšími náklady na pojistná plnění, a jsou proto také i pro pojistitele klíčovou výhodou.

Šulc (2018, s. 13) má za to, že typický podnik zpravidla provozuje nějaké webové stránky, používá jeden nebo více počítačů propojených v síti za účelem správy klientského a produktového portfolia, daňové účetní a mzdové evidence a realizace plateb. Šulc uvádí také možné cíle útočníka:

- znepřístupnit informační systém podniku (webové stránky, e-shop), takže jeho klienti se na něj nedostanou,

- smazat, pozměnit nebo zašifrovat data, takže se podnik nedostane k informacím o zaměstnancích, klientech, produktech, postupech a nebude moci včas uspokojit jejich požadavky,
- ukrást citlivé informace o zaměstnancích, klientech, produktech či postupech a prodat je následně na černém trhu nebo je přímo zneužít ve vlastní prospěch, k postavení lepší nabídky nebo k vydírání, že informace budou zveřejněny a případně je i zveřejnit,
- ovládnout systém a zneužít ho k útoku na jiný podnik nebo jeho klienty či k rozšíření malware,
- ovládnout systém, který je užíván k řízení výroby ovládání technologie u klientů a záměrně ho nastavit tak, aby nefungoval, produkoval zmetky či jinak škodil,
- ovládnout systém, pomocí kterého podnik provádí platební operace, a poté provést neautorizované operace jako například v aplikaci internet banking a převést si peníze na svůj účet,
- ovládnout systém, začlenit do něj vlastní škodlivý kód a poté upozornit na chybu a nabídnout, že ji za úplatu zcela odstraní nebo že na její přítomnost upozorní veřejnost, aby věděla, že daný podnik nedokáže spolehlivě ochránit data a raději se mu vyhnuli.

Smejkal (2018, s. 858) píše, že je všeobecně známo, že drtivá většina škod nevzniká v důsledku útoku zvenčí, ale vzniká **na základě interního jednání** – naplnění některé z hrozeb, ohrožujících informační systém, jako jsou technologická a technická rizika, charakteristická pro určitou technologii a způsob jejího používání, rizika vyplývající z poruch a havárií (přerušení dodávky elektrické energie, záplava atd.), ale zejména pak rizika související s lidským faktorem (chybné postupy, nedbalost, zlý úmysl). To dále komentuje, že pokud bude tedy pojištění omezeno pouze na útok zvenčí, lze odhadnout, že 80 % rizika provozovatele IS/IT zůstane nepokryto. Jako alternativu uvádí pojištění, které bylo doposud realizováno jako pojištění pro případ přerušení nebo omezení provozu podniku. Zde se ale obává výluky právě na kybernetické útoky.

Doucek a kolektiv (2019, s. 25) uvádějí, že převážná většina hrozeb, které poškodí IS/ICT organizace (více než 50 % ze všech), patří do **kategorie neúmyslných hrozeb**. Také podíl hrozeb zevnitř organizace je významně vyšší než hrozby z vnějšku. Podle některých statistických zdrojů až 98 % všech bezpečnostních incidentů v organizaci je interního původu – většinou nedbalost pracovníků, která je nejčastěji způsobena jejich neznalostí problematiky bezpečnosti IS/ICT (např. pracovník odejde od svého počítače na oběd a zůstane připojený pod svým uživatelským jménem do informačního systému, pracovník si nahraje seznam zákazníků na flash disk a odnese si jej domů). Mezi **základní hrozby** na informační aktiva patří neoprávněné, náhodné nebo úmyslné:

- **prozrazení** interních informací organizace – dojde k prozrazení dat neautorizovaným, náhodným nebo úmyslným způsobem,
- **upravení** – dojde k porušení integrity dat neautorizovaným, náhodným nebo úmyslným způsobem,
- **zničení** – data systému jsou zničena neautorizovaným, náhodným nebo úmyslným způsobem,
- **bránění** v dostupnosti dat, zdrojů nebo služeb informačního systému autorizovaným uživatelům.

Šulc (2018, s. 12) informuje o možných dopadech kybernetických útoků, které mohou být finanční i nefinanční povahy a jejich závažnost se bude odvíjet od úrovně zavedených

opatření. Píše, že následky těchto útoků se zpravidla vždy negativně projeví na zisku podniku, tempu jeho růstu, a v krajním případě pak takový útok může vést i k jeho krachu a nucené likvidaci. Šulc uvádí také konkrétní příklady a to, že podnik může utrpět okamžitou ztrátu, protože nemůže dočasně poskytovat své služby, dále pak může dojít ke ztrátě tržního podílu, kdy část klientů podnik opustí, neboť ztratí důvěru a nové klienty bude hůř získávat a v neposlední řadě pak podnik může dostat pokutu čelit sankcím a platit soudní výlohy.

Na základě dotazování 41 velkých pojišťovacích a zajišťovacích skupin napříč Evropou, které v součtu reprezentují 75% tržní podíl, EIOPA zjistila (2019, s. 3), že nejčastějšími kybernetickými incidenty postihujícími pojišťovny jsou phishing, malware (ransomware), krádež dat a útoky způsobující zastavení služeb. Hlavní důsledky, které pojistitelé po těchto kybernetických incidentech utrpěli, jsou přerušení provozu a materiální náklady pro pojistníky a třetí strany.

SPG (2020, III.) podrobněji popisuje současné kybernetické hrozby. Ve svém článku píše, že významné incidenty, jako byly ransomwarové útoky WannaCry v květnu 2017 a NotPetya v letech 2016 a 2017, podstatně zvýšily povědomí o kybernetických hrozbách s odhadovanými globálními škodami až čtyři miliardy amerických dolarů. Tyto kybernetické incidenty ukázaly obrovské riziko a potenciál velkých vzájemně souvisejících ztrát vzhledem k šíření ransomwaru po celém světě. Útoky ransomwaru, kdy konkrétní malware (například trojský kůň) zablokuje celé počítačové sítě a hackeři hrozí zveřejněním dat obětí útoku nebo trvalým blokováním přístupu, pokud nebude zaplaceno výkupné, jsou stále častější a čím dál závažnější. Dle SPG je také nepopíratelná rostoucí sofistikovanost kybernetických útoků. Například Advanced Persistent Threats (ADPs) – cílený útok, kdy kybernetický hacker získá přístup k systému s cílem ukrást data nebo narušit síť a zůstane po delší dobu nezjištěn – jsou na vzestupu. Tyto útoky jsou obvykle určeny ke krádeži duševního vlastnictví a citlivých dat za účelem politického nebo ekonomického zisku. Článek od SPG popisuje i další stále populárnější způsoby útoku, kterým je sociální inženýrství, kdy kybernetičtí útočníci manipulují jednotlivci, aby vyzradili citlivé informace. V červenci 2020 se Twitter stal obětí koordinovaného útoku sociálního inženýrství, který se zaměřoval na zaměstnance s přístupem k citlivým interním administrativním systémům. Účty slavných osobností, včetně bývalého prezidenta USA Baracka Obamy, zakladatele Amazonu Jeffa Bezose, generálního ředitele Tesly Elona Muska a rappera Kanye Westa, byly kompromitovány zveřejněním tweetů, které žádaly od milionů sledujících, aby poslali peníze na bitcoinovou adresu jako příspěvek komunity. Mnoho sledujících bylo oklamáno a posílalo bitcoinové platby s očekáváním dvojnásobného výnosu, který nikdy nedorazil. SPG upozorňuje, že kromě nákladů souvisejících se samotným kybernetickým útokem hrozí podnikům případná pokuta, pokud se zjistí, že plně nedodržují předpisy, například tím, že nebudou řádně chránit osobní údaje a proaktivně hlásit porušení jejich ochrany. Implementace obecného nařízení o ochraně osobních údajů (GDPR) dle SPG znamená, že organizace čelí vyšším sankcím za porušení ochrany osobních údajů, přičemž regulační orgány EU ukládají pokuty až do výše 4 % ročního celosvětového příjmu organizace nebo 20 milionů EUR, podle toho, která částka je vyšší, pokud poruší soukromí uživatelů.

2.3 Covid-19 a pojištění přerušení provozu

V posledních dvou letech se v médiích neustále opakuje téma pandemie Covid-19, která zasáhla pravděpodobně celý svět. Otázkou je, zda bylo možné pandemii předvídat a připravit se na ni. Pandemie Covid-19 nebyla první pandemií a co do úmrtnosti ani tou největší. Pandemie Španělské chřipky z let 1918–1919 nakazila polovinu světové populace a způsobila

smrt 40 miliónů lidí (WHO, 2002). Velmi znám je virus ptačí chřipky, konkrétně podtyp H5N1, který je přenosný na člověka.

Strauss, James H. a Strauss, Ellen G. (2008, s. 335) uvádějí, že virus ptačí chřipky, podtyp H5N1, byl poprvé detekován v Číně v roce 1996 a pro zastavení šíření viru bylo nutné v dané době utratit více než 140 miliónů ptáků, a zároveň uvádí, že pokud by virus získal schopnost šířit se přímo z člověka na člověka a pokud by pokračovala vysoká úmrtnost, mohl by tento virus způsobit zničující pandemii.

Riziko přenosu z člověka na člověka je ostatně také důvodem pro mimořádná veterinární opatření k zamezení šíření nebezpečné nákazy – „ptačí chřipky“ na území České republiky, které vydala Státní veterinární správa.

Smil (2008, s. 359–360) již v roce 2008 považoval pandemii chřipky za vysoce pravděpodobnou, dokonce téměř jistou. Jako jeden z argumentů uvádí vysokou hustotu osídlení jižní Číny a neustálý blízký kontakt lidí s drůbeží a prasaty, který činí tento region trvalým zdrojem nových virů (2008, s. 74). Zároveň upozorňoval (2008, s. 360), že nepředvídatelně mutující viry nás budou provázet vždy a upozorňoval na nutnost neustále zdokonalovat svoji připravenost k boji s novou pandemií. Nejednalo se ale o “proroctví” Smila, ale o predikci na základě následujících skutečností. Typická frekvence chřipkových pandemií byla v období let 1700–1889 jednou za 50–60 let (nejdelší známý interval byl 52 let mezi pandemiemi 1729–1733 a 1781–1782) a od roku 1889 jednou za 10–40 let. Interval výskytu vypočítávaný jednoduše jako průměrná doba uplynuvší mezi posledními šesti známými pandemiemi je zhruba 28 let s extrémy 6 a 53 let. Přidáním průměrného a nejvyššího intervalu k roku 1968 se dostáváme k rozmezí let 1996 a 2021 (2008, s. 75).

Pojištění přerušení provozu dle Gmentové (2020, s. 36) kryje následné (finanční) ztráty vzniklé v příčinné souvislosti s celkovým, nebo částečným přerušením provozu v důsledku věcné škody, tj. škody způsobené pojištěným nebezpečím v rámci pojištění majetku (například požárem, povodní), znamená to, že předpokladem pojistného plnění z pojištění přerušení provozu je vznik majetkové škody, která je pojištěna základním živelním pojištěním majetku, a která byla z pojištění majetku likvidní. Autorka dále upřesňuje, že po celou dobu, co dochází k opravě majetku poškozeného pojištěným nebezpečím z pojištění majetku, pojištění přerušení provozu pokrývá náklady, které pojištěný podnik musí vynakládat i přesto, že provoz nefunguje, nevyrábí. Za dobu, kdy nedochází k výrobě či činnosti firmy, ztrácí pojištěný zisk, který je též součástí pojištění přerušení provozu.

Ducháčková (2015, s. 199) řadí pojištění pro **přerušení provozu**, též nazývané „šomážní pojištění“, do kategorie pojištění finančních ztrát. Píše o něm, že úzce navazuje na živelní strojní pojištění a další produkty majetkového pojištění, kdy častou podmínkou pro jeho sjednání ze strany pojišťovny je sjednání majetkového pojištění, na které pojištění provozu navazuje. Prakticky to znamená, že majetková pojištění zabezpečují náhradu přímé věcné škody, a pojištění pro případ přerušení provozu kryje tzv. následné škody, tedy zabezpečuje náhradu finanční újmy, která vzniká v důsledku přerušení provozu, ke kterému dochází na základě poškození pojištěného majetku živelní nebo jinou událostí. K tomu Ducháčková dodává, že objem následných škod často výrazně překračuje přímé věcné škody.

Řezáč (2016, s. 185) popisuje pojištění přerušení provozu jako následnou škodu věcné škody. Za následnou škodu pro účely tohoto pojištění pak považuje náklady specifikované v pojistné smlouvě, které pojištěnému nabíhají i v případě přerušení provozu (stálé náklady) v období přerušení provozu, a také ušlý provozní zisk za období přerušení provozu.

Veber a kolektiv (2012, s. 164) řadí mezi pojištění rizik vyplývající z činnosti podnikatele také pojištění pro případ přerušení nebo omezení provozu, o kterém dále píší, že jej nabízí

většina univerzálních komerčních pojišťoven ke sjednanému majetkovému pojištění a jedná se o připojištění průmyslových rizik. Dle Vebera a kolektivu má majetkové pojištění nahradit poškozený či zničený předmět, ale neřeší důsledky toho, že po kratší či delší dobu nepoběží provozní činnost, přitom podnikatel musí platit například pronájem či leasing, sociální pojištění za své zaměstnance, zálohy na daně a tak dále. Uvádějí, že právě tyto položky a také případně provozní zisk, mohou být hrazeny z pojištění přerušení provozu, a že tento pojistný produkt zpravidla není nabízen ztrátovým firmám nebo firmám v konkurzu či likvidaci.

Česká asociace pojišťoven (2020) dělí přerušení provozu na základní a rozšířené. To základní definuje jako přerušení provozu (podniku) z důvodu požáru, blesku, exploze či pádu letadla. Dále pak, že základní přerušení provozu je předmětem pojištění, a je možné rozšíření o vloupání, vodu z potrubí a tak dále. Rozšířené, či podmíněné, přerušení provozu ČAP definuje mnohem obsáhleji, a to následovně. Pojištění přerušení provozu patří k již běžným podnikatelským pojištěním. V zásadě se dle ČAP jedná o pojištění následných (ekonomických) škod vzniklých v příčinné souvislosti s celkovým nebo částečným přerušením provozu v důsledku věcné škody, kde se za věcnou škodu považuje poškození nebo zničení věcí sloužících pojištěnému provozu v důsledku (základních) živelních rizik. ČAP dále píše, že pojištění přerušení provozu se obvykle váže na pojištění majetku, a proto se sjednává i odpovídající rozsah pojistných nebezpečí. ČAP upozorňuje, že rozsah pojištění se u jednotlivých pojistitelů liší, a proto je třeba se důkladně seznámit s pojistnými podmínkami, kde kromě živelních rizik může být kryta i stávka, vandalismus, terorismus a podobně. ČAP (2020) popisuje, že v anglickém pojišťovacím prostředí se prezentovaný pojem interpretuje například takto: *„Pojistné plnění končí, jakmile podnik opravil nebo vyměnil stroje a zařízení a výroba může znovu začít“*. Ovšem v případě delšího výpadku produkce dle ČAP může podniku nějakou dobu trvat, než se dostane zpět na svůj tržní podíl, který držel před přerušením provozu, a z tohoto důvodu může být dohodnuto, že pojistitel vyplácí pojistné plnění ještě po rozšířené (prodloužené) období, jehož doba trvání se stanovuje v pojistné smlouvě. Dle ČAP produkce podniku může být ale ovlivněna nejen věcnou škodou na jeho majetku, ale také škodou v podniku zákazníka nebo dodavatele. Pokud je totiž podnikatelská činnost například zákazníka přerušena, nemůže pochopitelně nakupovat zboží ani služby od pojištěného podniku, a pokud dodavatel nemůže poskytnout potřebný input, může to vést ke stavu, kdy se produkce pojištěného podniku zastaví. ČAP dále upřesňuje, že přirozeným vývojem tak vznikla potřeba rozšířit na základě dodatečného pojistného pojištění pro případ přerušení provozu, aby jako pojistná událost byla brána i věcná škoda na výrobních prostředcích dodavatele nebo zákazníka. Takové rozšíření je dle ČAP nazváno *„podmíněné pojištění pro případ přerušení provozu“*, tedy pojištění, jež bere v úvahu závislost pojištěného podniku na svých zákaznících a dodavatelích.

Nebolsina (2021, s. 1) uvádí, že většina pojistných smluv, kde je sjednáno pojištění přerušení provozu, poskytuje krytí pouze v případě, že došlo k majetkové újmě (věcné škodě), a tedy škodám na pojištěné budově nebo movitých věcech. Ve většině případů však smlouvy nekryjí škody v důsledku Covid-19, a zdá se tak, že v těchto případech ani nevzniká nárok na úhradu škod vzniklých v důsledku přerušením provozu. Dále píše, že i přesto celosvětově již probíhají tisíce soudních sporů, v nichž pojistníci zastávají názor, že pojem *„věcná škoda“* by měl být vykládán široce a měl by zahrnovat také důsledky pandemie Covid-19, přičemž pojistníci již dosáhli významných úspěchů jak ve Spojených státech, tak v Evropě, včetně vítězství před anglickým vrchním soudem. Nebolsina (2021, s. 2) na základě svých zjištění píše, že pandemie Covid-19 výrazně zvýšila poptávku po pojištění přerušení provozu během prvních šesti měsíců roku 2020 a tento trend může dále trvat, což také může částečně kompenzovat obrovské ztráty, které pojistitelé utrpěli na základě pojistných smluv

s přerušením provozu, které byly vydané před pandemií, a obsahují právě pojištění přerušení provozu v důsledku pandemie.

Dle OECD (2021, s. 1-2) pandemie Covid-19 a opatření přijatá k omezení šíření nemoci významně narušily ekonomickou aktivitu v zemích po celém světě, což má za následek značné ztráty z v důsledku přerušení provozu. Převážnou většinu těchto ztrát pravděpodobně půjde k tíži podniků, protože pokud vlády (nebo soudy) nezasáhnou, jen málo podniků má sjednáno přerušením provozu, které by krylo tyto typy ztrát. OECD píše, že pandemie odhalila významnou mezeru v pojistném krytí přerušení provozu v důsledku pandemie. V reakci na současnou krizi pojišťovny zkoumají dlouhodobější řešení, jak vyřešit mezeru v pojistné ochraně pojištění přerušení provozu v důsledku pandemie. Dle OECD pojišťovny a asociace pojišťoven po celém světě uvedli, že většina pojistných smluv nekryje škody v důsledku přerušení provozu v souvislosti s Covid-19. Ve většině zemí je pojištění přerušení provozu poskytováno jako volitelné a je spojené s pojištěním majetku, kdy přerušení provozu je často (ale ne vždy) kryto pouze v důsledku věcné škody. OECD dále uvádí, že kromě toho mohou pojistné podmínky a smlouvy obsahovat také výluku krytí ztrát způsobených viry, bakteriemi, či konkrétně v souvislosti s pandemií. Někdy naopak může být výslovně pojištěno přerušení provozu v důsledku pandemie formou zvláštního ujednání, ale jen omezeně.

Renomia a.s. (2020), dále jen Renomia, uvádí, že vláda České republiky byla nucena přijmout mnoho opatření proti šíření Covid-19, v důsledku čehož došlo k zásadnímu snížení, omezení nebo dokonce úplnému přerušení podnikatelských aktivit, a je tak těžce zasaženo mnoho odvětví, jako jsou pohostinství, hotely, různé služby a ostatní maloobchodní oblasti. Dle Renomia většina z těchto firem má sjednáno pojištění přerušení provozu, avšak v důsledku Covid-19 neutrpí žádnou hmotnou škodu, což je standardní podmínka pojistné události u pojištění přerušení provozu v majetkovém pojištění. Dle Renomia u standardních programů pojištění majetku s pojištěním přerušení provozu je ve většině případů nepravděpodobné, že by krytí škod v důsledku pandemie bylo pojištěno. Renomia se domnívá, že většina pojistných smluv nikdy nezamýšlela pojišťovat škody vyplývající z pandemie, jelikož se jedná se o riziko, u kterého pojistitelé uznávají, že si nemohou dovolit jej pojistit. Potenciální pojištění pandemie Renomia srovnává s pojištěním válečných rizik, což je typ rizika, které by světový trh plně pojistit nedokázal.

Dle Renomia se podniky zpravidla nejvíce obávají těchto následků spojených s rizikem šíření Covid-19:

- Částečné či zcela úplné omezení provozu podniku (snížení výnosů, zisku a generování stálých nákladů, zásadní snížení cash flow), což může následně vést rovněž ke snížení tržní kapitalizace podniku (dopad na akcionáře).
- Hrozby odpovědnostních nároků třetích stran vůči podnikům a managementu v souvislosti s možným opomenutím/zanedbáním ochrany zákazníků, návštěvníků a zaměstnanců, kteří mohou být neúměrně vystaveni hrozbě Covid-19.
- Zvýšené náklady související s dekontaminací/dezinfekcí.
- Kybernetické hrozby – zvýšený zájem veřejnosti o Covid-19 povede ke zvýšenému počtu phishing útoků směrem na podniky (podvodné e-maily zabývající se problematikou Covid-19).
- Kreditní riziko (zásadní zvýšení doby obratu pohledávek, případně pohledávky zcela neuhrazeny).
- Mobilita firem v návaznosti na rozsah cestovního pojištění, léčení v zahraničí.

Dle průzkumu Allianz Risk Barometr 2022 se riziko přerušení provozu posledních pět let stabilně pohybovalo na prvních dvou příčkách žebříčku nejpodstatnějších rizik. Dle Allianz

(2022) může být přerušení provozu důsledkem mnoha dalších rizik, jako jsou kybernetická rizika a přírodní katastrofy, a jedná se o přetrvávající problém pro podniky po celém světě. Pandemie také odhalila rozsah zranitelnosti v moderních dodavatelských řetězcích, a jak se může sejít více událostí, které způsobí přerušení provozu. V roce poznamenaném přerušením provozu v důsledku pandemie, bouřek, kybernetických útoků a zablokování Suezského průplavu, není žádným překvapením, že přerušení provozu a narušení dodavatelského řetězce stále trvá, a je tak zařazeno mezi rizika, která budí největší obavy. Philip Beblo, kterého průzkum cituje, uvedl, že většina podniků má obavy z toho, že nebude schopna produkovat a dodávat své produkty a služby. Je přitom jedno, zda to je v důsledku kybernetického útoku, povodně nebo požáru, který zasáhne klíčovou oblast podnikání nebo dodavatele. Dle Bebla přerušení provozu může být velmi nákladné a může mít dlouhotrvající účinek s přesahem mimo podnik. Allianz (2022) dále v průzkumu píše, že navzdory přetrvávajícím dopadům Covid-19, nejobávanější **příčinou přerušení provozu** v letošním průzkumu jsou kybernetická rizika (52 %), následovaná přírodními katastrofami (36 %) a až třetí je přerušení provozu z důvodu pandemie (35 %). Z průzkumu Allianz dále vyplynulo, že podniky důvěřují svým pohotovostním plánům a přípravám na budoucí podobné situace. Na otázku, jak se cítí připraveni na budoucí pandemii, 80 % podniků odpovědělo, že jsou připravení adekvátně nebo dobře. Dalších 9 % odpovědělo, že jsou připraveni dokonce velmi dobře, a pouze 11 % odpovědělo, že nejsou dostatečně připraveni.

2.4 Změny klimatu a pojištění přírodních nebezpečí

Českou republiku zasáhly v letech 1997 a 2002 silné povodně. Hovořilo se o stoleté vodě, což může vyvolat mylný dojem, že v současném století již podobná katastrofa nenastane. Statistiky bohužel hovoří jinak. V roce 2021 zasáhla další silná povodeň Německo. Obecně vědci tyto extrémní povětrnostní jevy považují za důsledek změn klimatu. Tou hlavní změnou je nárůst průměrné roční teploty, kterou z velké míry způsobuje rostoucí hladina oxidu uhličitého v atmosféře. Smil (2012, s. 266) zvažuje mnohem více faktorů, které budou mít vliv na oteplování do roku 2050, konkrétně uvádí vlivy jako budoucí radiační působení, budoucí intenzitu spalování fosilních paliv, změny ve využívání půdy, používání hnojiv a objem produkce masa.

Ať už je důvodem změny klimatu cokoliv, nic to nemění na statistikách narůstajícího počtu přírodních katastrof. Ministerstvo životního prostředí České republiky (2021, s. 177) ve své strategii přizpůsobení se změně klimatu v podmínkách ČR pro období 2021-2030 považuje za perspektivní ekonomický nástroj pojištění proti přírodním rizikům, které by mělo hrát významnou úlohu při adaptaci na změnu klimatu. Změnou klimatu se dle ministerstva rozumí kombinace dlouhodobých změn klimatického systému, včetně přirozené variability klimatu a změn způsobených lidskou činností, přičemž přirozenou a antropogenní složku změny klimatu od sebe nelze zcela oddělit. Ministerstvo píše, že změna klimatu se projevuje zejména nárůstem teploty vzduchu (a potažmo povrchové vody), zkracováním délky zimního období, poklesem úhrnu srážek v letním období a nárůstem frekvence a závažnosti extrémních meteorologických jevů, jako jsou dlouhá suchá období, intenzivní srážky, vlny veder a podobně. Dle ministerstva příčinou probíhající změny klimatu je s největší pravděpodobností zesilování přirozeného skleníkového efektu atmosféry v důsledku lidské činnosti a nadměrného zvyšování antropogenních emisí skleníkových plynů.

Ducháčková (2015, s. 192) v rámci majetkového pojištění podnikatelských a průmyslových rizik uvádí jako klasický pojistný produkt **živelní pojištění**, které kryje škody na majetku, způsobené realizací živelního rizika jako je blesk, vichřice, povodeň, záplava, pád stromů a stožárů, krupobití, zřícení skal, zemětřesení, ale také požár, výbuch a jiné. Nejedná se tedy

pouze o samotné pojištění přírodních nebezpečí, ale v jeho rámci bývá kryto i vodovodní pojistné nebezpečí a často má podobu pojištění FLEXA – fire, lightening, explosion, airplane (požár, úder blesku, výbuch, pád letadla). Ducháčková (2015, s. 186) definuje jednotlivá přírodní nebezpeční následovně:

- **Vichřice** = dynamické působení hmoty vzduchu (vítr), který dosahuje v místě pojištění rychlosti minimálně 75 km/hod.
- **Krupobití** = přírodní jev, při kterém kousky ledu vytvořené v atmosféře dopadají na předměty.
- **Úder blesku** = bezprostřední přechod blesku (atmosférického výboje) na pojištěnou věc.
- **Povodeň** = zaplavení větších či menších územních celků vodou, která se vylila z břehů vodních toků nebo nádrží, nebo tyto břehy a hráze protrhla, nebo byla způsobena náhlým a neočekávaným zmenšením průtočného profilu toku.
- **Záplava** = vytvoření souvislé vodní plochy, na které bude voda delší dobu stát, případně po ní proudit.

Janata (2014, s. 48-51) řadí pojištění **FLEXA** mezi základní živelní pojištění, které se uzavírá hromadně pro všechny čtyři rizika. Dle Janaty lze sjednat i rozšířený živel, kde se rizika vybírají individuálně, a patří sem vichřice, povodeň, záplava, krupobití, zemětřesení, sesouvání půdy, zřícení skal nebo zemin, a tíha sněhu nebo námrazy. O **vichřici** pak Janata píše, že bývá podmíněna rychlostí větru minimálně 20,8 metru za sekundu, a to odpovídá devátému stupni Beaufortovy stupnice, silné vichřici, která ničí i správně udržované střechy domů. Janata píše, že kolem tohoto čísla bývají spory, protože meteorologové měří rychlosti u povrchu země, tedy v mezní vrstvě, kdežto střechy jsou podstatně výše, a tam bývají rychlosti vyšší. V celosvětovém měřítku považuje větrné smršť za velmi závažné riziko. Také píše, že podle definice vichřice není příčinou škod, pokud byla budova bez oken a dveří (prováděny stavební práce), v důsledku zchátralých, shnilých nebo jinak poškozených střešních konstrukcí a podobně. Dalším rizikem, které spadá mezi rozšířený živel, patří povodeň. **Povodeň** definuje jako vystoupení vody z břehů u vodních toků a nádrží, popřípadě protržením hrází. Janata upozorňuje, že v současnosti je v celé řadě smluv zavedena výluka dvacetileté vody (kvůli častému opakování). **Záplavu** definuje jako vytvoření souvislé vodní hladiny jiným mechanismem než povodní, například průnikem z kanalizace. **Krupobití** dle Janaty představují kousky ledu, vytvořené v atmosféře, které dopadají na pojištěnou věc a tím dochází k jejímu poškození nebo zničení. Dle Janaty bývají nebezpečné již kousky o průměru dvacet milimetrů, kdy mohou být způsobeny škody na sklenících nebo skleněných částech budov, na automobilech, zraněni mohou být lidé nebo zvířata. Kroupy vznikají několikanásobným průchodem ledových krystalů zvláštními bouřkovými mraky (Cumulonimbus). Janata upozorňuje, že krupobití ale není příčinou škody, pokud je budova bez oken a dveří z důvodu stavebních prací, nebo v důsledku zchátralých, shnilých nebo jinak poškozených střešních konstrukci a podobně. **Zemětřesení** je dle Janaty pojišťovnou hrazeno, jen pokud dosáhlo sily šesti stupňů MSK 1964 (Medveděv, Sponheuer, Kárník), což je již poměrně silné zemětřesení s otřesy dosahujícími třech až sedmi procent tíhového zrychlení. Janata zemětřesení popisuje jako pohyby zemské kůry, vyvolané neustálými pohyby zemských desek podél jejich zlomů. Proto se největší zemětřesení vyskytuji v oblastech, kudy zlomy procházejí, což je západní pobřeží Ameriky, východní Asie (průvodní ostrovy mezi Asií a Austrálií), a dále Kavkaz, Turecko, Írán, Středomoří. Dle Janaty se zemětřesení dělí na:

- **Řítivá** (asi 3 %) – vznikají zřícením stropů podzemních dutin v dolech nebo krasových oblastech.
- **Sopečná** (7 %) – projev vulkanické činnosti.

- **Tektonická neboli dislokační** (90 %) – vznikají náhlým uvolněním nahromaděné energie.

Mezi další rozšířená rizika dle Janaty patří sesouvání půdy, zřícení skal nebo zemin, což je jev, kdy se masa půdy, zeminy nebo skal zřítí působením gravitace. Naopak sesouváním půdy není klesání zemského povrchu směrem ke středu Země v důsledku přírodních sil. Dle Janaty jsou v České republice sesuvy půdy poměrně časté, nemívají však katastrofální následky. Podobně definuje sesuv nebo zřícení lavin, kdy masa sněhu nebo ledu se náhle uvede do pohybu po svazích a řítí se do údolí. Riziko tíhu sněhu nebo námrazy Janata popisuje jako destruktivní působení těchto hmot na střešní krytinu a nosné konstrukce budovy.

Engst a kolektiv (2020, s. 32) také uvádějí, že **FLEXA** je základním pojistným nebezpečím, ale navíc dodává, že bez něj nelze ostatní pojistná nebezpečí sjednat. Autoři používají i další souhrnná označení nebezpečí, jedná se o:

- **Katastrofická nebezpečí** – patří sem především záplava, povodeň, zemětřesení, vichřice a krupobití.
- **Sdružený živel** – zahrnuje pojištění všech pojistných nebezpečí, kde se jejich výčet může u různých pojistitelů lišit.
- **Doplňková živelní nebezpečí** – patří sem všechna ostatní živelní nebezpečí mimo FLEXA, katastrofických nebezpečí a vodovodních škod, kde se opět jejich výčet může u různých pojistitelů lišit.
- **All Risk** – je definován jako všechny události kromě těch, které jsou vyloučeny (je potřeba v pojistných podmínkách každé z pojišťoven nastudovat výčet výluk).

Engst a kolektiv (2020, s. 34) živelní pojištění dělí dle rozsahu na standardní rozsah a All Risk. Do standardního rozsahu dle autorů patří FLEXA, vichřice, krupobití, záplava, povodeň, zemětřesení, tíha sněhu nebo námrazy, pád stromů, stožárů nebo jiných předmětů, sesuv půdy, zřícení skal nebo zemin, sesuv nebo zřícení lavin, a vodovodní škody. All Risk není dle autorů v případě živelního pojištění standardně nabízen. Píší o něm, že se jedná o cenově dražší riziko, ale pro některý typ majetku případně provozů je na makléři, aby doporučil sjednání. Dle autorů je potřeba myslet na to, že v případě All Risk pojištění pojišťovna dokazuje, že nastalá událost je vyloučena, v případě vyjmenovaných rizik pojištěný dokazuje, že nastalá událost spadá do pojištěných nebezpečí, například dokladem z hydrometeorologického ústavu o rychlosti větru.

2.5 Metodika práce

Tato diplomová práce je rozdělena do čtyř hlavních částí, a to jsou konkrétně úvod, teoreticko-metodologická část, analytická část a na konec závěr. Teoreticko-metodologická část se zabývá současnými trendy v oblasti rizik, která nejprve identifikuje dle veřejně a všeobecně známých informací. K tomu byly také využity statistické informace ze zdrojů (včetně zahraničních), jako je například Swiss Re, Allianz Risk Barometr, Český hydrometeorologický ústav, Národní úřad pro kybernetickou a informační bezpečnost. Následně jsou zkoumaná rizika definována a blíže popsána, včetně všech souvisejících pojmů. K tomu bylo potřeba získání teoretických znalostí při využití rešerše sekundárních zdrojů, zejména pak literatury z oblasti pojišťovnictví, informačních technologií a přírodních věd. S ohledem na aktuálnost témat bylo také nutné využít rešerše i zahraničních odborných článků ze zdrojů jako jsou Science Direct, Swiss Re, World Health Organization, World Meteorological Organization, Organisation for Economic Co-operation and Development, European Insurance and Occupational Pensions Authority, nebo S&P Global Inc.

K vyhledávání byla využívána např. klíčová slova insurance, cyber risk, business interruption, covid-19, pandemic, natural catastrophes, natural disasters, a jiné další kombinace. Současně přitom byly zkoumány trendy na pojistném trhu, kdy nelze vyloučit, že pojistný trh krytí některých rizik buď vůbec nenabízí, nebo je třeba postupně přestává nabízet. Získání těchto teoretických znalostí bylo nezbytné pro formulování možností, co lze vůbec pojistit, a tedy proti kterým rizikům se lze pojištěním chránit.

Analytická část zkoumá, zda český trh s pojištěním nabízí krytí zkoumaných rizik a v jakém rozsahu. Práce se zaměřuje pouze na nabídku pojišťoven, které mají významný podíl předepsaného pojistného v podnikatelském pojištění. K tomu bylo využito nejnovějších statistických údajů České asociace pojišťoven, ze kterých vyšlo, že mezi tyto pojišťovny patří Generali Česká pojišťovna a.s., Kooperativa pojišťovna, a.s., Vienna Insurance Group, Allianz pojišťovna a.s., ČSOB Pojišťovna, a.s., člen holdingu ČSOB, a Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group. Přímo z webových stránek vybraných pojišťoven byly staženy pojistné podmínky, které se vztahují k vybraným rizikům. Následně proběhl rozbor těchto pojistných podmínek za účelem zjištění rozsahu pojistného krytí, povinností pojištěného, výluk a dalších ustanovení pojistných podmínek, na které by si pojištěný měl dávat pozor. V analytické části práce se dále nachází případová studie vybraného podniku, který si přeje být anonymizován, a proto je v práci využíván pouze název XYZ. Základní informace o podniku byly získány z volně dostupných informací (např. webových stránek podniku), které však bylo nutné doplnit o informace získané přímo od jednatele podniku XYZ. Pro celkový přehled o daném podniku byly podrobnější informace získány od jednatele prostřednictvím dotazníku (viz příloha 5), který byl elektronicky předán jednateli k vyplnění, a obsahuje dotazy vztahující se přímo k tématu práce. Jedná se například o otázky ohledně fungování provozu, rozsahu opatření, která jsou v podniku zavedena proti možným kybernetickým hrozbám, zda má podnik nějaké možnosti zmírnit dopady uzavření nebo omezení provozu (např. práce z domova), jaká přírodní rizika mohou ovlivnit fungování podniku (např. zda se nachází v povodňové zóně), a jiné další otázky související s tématem práce. Z výsledků dotazníku bylo následně vyhodnoceno, jaká rizika na podnik působí, a jaký je současný stav řízení vybraných rizik v podniku. Jedním z kroků případové studie bylo posouzení všech pojistných smluv podniku XYZ k majetkovému a odpovědnostnímu pojištění, zejména pak zjistit rozsah krytí pro vybraná rizika. Jako závěrečný krok bylo provedeno vyhodnocení na základě všech do té doby zjištěných informací, ke kterým byly přidány znalosti a zkušenosti autora, a podniku bylo uděleno doporučení k řízení rizik.

3 Analytická část práce

Jak již bylo popsáno v metodice, analytická část práce nejprve zkoumá, zda a v jakém rozsahu český pojistný trh nabízí podnikatelské pojištění rizik, která byla předmětem teoretické části. Konkrétně se jedná o pojištění kybernetických rizik, přerušení provozu a přírodních nebezpečí. Ovšem jen samotný výsledek této části zkoumání není jediným rozhodujícím faktorem, zda doporučit podniku XYZ sjednat takové pojištění, a případně u jaké pojišťovny. Neméně podstatnou informací je, zda rozsah pojištění odpovídá konkrétním potřebám daného podniku. K tomu je samozřejmě nutné o podniku zjistit maximum informací, které mohou mít vliv na pojištění, a tedy i na pojistné plnění z případné pojistné události.

Pro přehlednost nejprve krátké shrnutí těch nejdůležitějších zjištění z teoretické části práce, které je nutné zohlednit v té analytické:

- Mezi **kybernetické hrozby** nepatří pouze úmyslný útok hackera zvenčí, ale daleko pravděpodobnější a častější jsou vnitřní hrozby, kam mimo jiné patří úmyslné, či neúmyslné jednání zaměstnance podniku. Jako příklad lze uvést neopatrnost při práci s daty nebo vědomé vynesení a zneužití dat zaměstnancem. V návaznosti na to je pak velmi důležité pojištění odpovědnosti za ztrátu dat, které může vést k porušení GDPR a následnému udělení sankcí, jež pro podnik mohou v krajním případě být i likvidační. Bude tedy velmi důležité u nabídek pojištění sledovat, zda kryje také tyto situace, a v jakém rozsahu (zda je například pojistné plnění omezeno limitem plnění, jinak řečeno, zda jsou plně kryty případné sankce za nedodržení GDPR).
- Pojištění **přerušení provozu** standardně nekryje situace, kdy k přerušení provozu dojde z důvodu pandemie, ale musí k němu dojít v důsledku škody na věci, ke které dojde z pojištěného rizika. Převedením do praktického příkladu, podnik má pojištěné riziko požáru, který v době pojištění nastane v místě pojištění, a dojde ke škodě na budově a movitých věcech. V důsledku této události podnik XYZ přestane být schopen provozovat svou činnost (dodávat své výrobky nebo služby) a vznikají mu tak finanční ztráty, které jsou předmětem pojistného plnění. Některé smlouvy mohou mít sjednáno pojištění přerušení provozu z důvodu pandemie nebo vládního nařízení, nicméně více obávanější je dnes přerušení provozu z důvodu kybernetického útoku nebo přírodní katastrofy. Co se týká přírodních katastrof, lze je považovat za již tradiční příčinu přerušení provozu. To stejné se ale nedá říct o kybernetickém útoku. Bude proto velmi důležité sledovat, zda pojištění obsahuje přerušení provozu i z důvodu kybernetického útoku. Zda kryje i přerušení provozu následkem pandemie bude vhodné ověřit, ale nelze to příliš očekávat.
- Škody vlivem **přírodních událostí** v současnosti nastávají čím dál častěji a způsobují čím dál větší škody. Pojištění přírodních událostí je v dnešní době už spíše samozřejmostí. Je také důležité zmínit provázanost pojištění přírodních nebezpečí a pojištění přerušení provozu. Přestože případná vichřice napáchá relativně malé materiální škody, finanční újma v podobě přerušení provozu může být mnohonásobně větší, a na to je nutné myslet pří řízení rizik v podniku.

3.1 Rozbor pojistných podmínek vybraných pojišťoven

Pro účely práce je nejprve nutné zjistit, které z pojišťoven se zabývají podnikatelským pojištěním, ve kterém by mohlo být obsaženo pojištění vybraných rizik. K tomu je nejvhodnější využít statistiky vývoje pojistného trhu za uplynulý rok, tedy rok 2021, kterou pravidelně publikuje Česká asociace pojišťoven. Příloha 4 ukazuje předepsané smluvní pojistné dle metodiky ČAP v podnikatelském pojištění, které aktuálně má celkem 14 pojišťoven, z nichž 5 pojišťoven má významný podíl na českém trhu. Právě na těchto

5 pojišťoven se bude práce zaměřovat. Jedná se o všeobecné známé pojišťovny, konkrétně to jsou (seřazeno dle výše podílu od nejvyššího po nejmenší):

- Generali Česká pojišťovna a.s.,
- Kooperativa pojišťovna, a.s., Vienna Insurance Group,
- Allianz pojišťovna a.s.,
- ČSOB Pojišťovna, a.s., člen holdingu ČSOB,
- Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group.

To ovšem samo o sobě nemusí znamenat, že uvedené pojišťovny nabízí krytí zkoumaných rizik, jinak řečeno nemusí mít ve svém portfoliu například kybernetické pojištění, které je poměrně novým typem pojištění. Nicméně jedná se o velké, stabilní a kapitálově zajištěné pojišťovny, které dokáží dostát svým závazkům i v případě velkých událostí, což se ukázalo např. při tornádu na Moravě.

3.1.1 Pojištění kybernetických rizik

Odvětví informačních technologií je dynamicky se rozvíjející odvětví, a ruku v ruce s tím jdou i související kybernetický hrozby. Proto i pro pojišťovny musí být nesmírně těžký úkol vytvořit ten správný produkt. Prostým zadáním klíčových slov *„kybernetické pojištění“* do vyhledávače Google se z prvních deseti výskytů zobrazí nabídka pojištění od pojišťoven Kooperativa pojišťovna, a.s., Vienna Insurance Group, ČSOB Pojišťovna, a.s., člen holdingu ČSOB, Colonnade Insurance S.A., Maxima pojišťovna a.s. a INSIA a.s. Velké pojišťovny jako Generali Česká pojišťovna a.s., Allianz pojišťovna a.s. nebo Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group mezi nimi nejsou. Je tak možné, že pojištění kybernetických rizik není v jejich nabídce.

Generali Česká pojišťovna a. s.

Generali Česká pojišťovna a. s. (dále jen GČP) je, co se týká celkového předepsaného pojistného, největší pojišťovnou v České republice. To stejné platí i pro segment podnikatelského pojištění, kde zabírá první pozici. Po důkladném prostudování webových stránek GČP a zejména sekce, kde jsou uloženy pojistné podmínky, tato pojišťovna aktuálně nenabízí na českém trhu možnost sjednání kybernetického pojištění, a to jak pro občany, tak pro podnikatele. GČP (2021) na počátku loňského roku na svých webových stránkách zveřejnila informaci, že připravuje nové pojistné podmínky pro kybernetické pojištění v rámci produktu s názvem *„ProfiPlán“*. Avšak ani po roce k vydání nových pojistných podmínek a možnosti sjednání nového typu pojištění stále nedošlo.

Kooperativa pojišťovna, a.s., Vienna Insurance Group

Obecná specifikace produktu:

Kooperativa pojišťovna, a.s., Vienna Insurance Group (dále jen KOOP) nabízí produkt s názvem *„Pojištění kybernetických rizik“*, který je určen pro všechny podnikatelské subjekty i neziskové organizace, kteří zpracovávají a ukládají osobní i jiná data klientů, zaměstnanců a obchodních partnerů. Může se jednat také o další informace, které jsou zvlášť chráněné, jež mohou například být předmětem obchodního tajemství, a jsou tak pro podnik klíčové. Produkt kryje rizika jako je lidská chyba (zanedbání bezpečnostních procesů, vedoucích k úniku nebo zneužití osobních dat klientů), nefunkčnost počítačových systémů, přerušení provozu a poškození dobrého jména podniku. V případě kybernetického útoku pojištěný musí tento incident nahlásit na infolinku Kooperativy, kde operátor přijme hlášení, a buď poradí ihned,

nebo záležitost předá k dalšímu řešení specializovanou IT firmou. Technický pracovník IT firmy se bezprostředně po nahlášení incidentu spojí s pojištěným a dohodne následný postup. Pojištění kybernetických rizik se řídí zvláštními pojistnými podmínkami s označením P-900/18, které byly vydané v červnu 2020.

Pojištěná rizika:

KOOP z daného pojištění považuje za likvidní pouze takové škody, kdy nastal tzv. *„kybernetický incident“*. Za kybernetický incident pojišťovna považuje tři situace. První situací je poškození, zničení, ztráta nebo odcizení dat v elektronické podobě způsobené úmyslným jednáním, nikoliv však jako důsledek poškození, zničení, odcizení nebo ztráty hardwaru. Úmyslným jednáním je například hackerský útok, malware, ransomware, či nespokojený nebo zhrzený zaměstnanec, který vynese data v elektronické podobě. Druhou situací je nedbalostní pochybení pojištěného nebo osob pro něj činných, vedoucí k poškození či ztrátě dat v elektronické podobě, nikoliv však jako důsledek poškození, zničení, odcizení nebo ztráty hardwaru. Jedná se například o situace, kdy zaměstnanec omylem pošle dokument s citlivými osobními údaji klienta na neoprávněnou osobu, nebo nechá počítač nebo notebook bez dozoru a v nezabezpečeném režimu. Třetí situací je DDoS útok (Denial of Service), kterým je myšleno úmyslné přetížení nebo zahlcení počítačového systému, a které způsobí odepření služby (nefunkčnost, zablokování systému).

Rozsah krytí:

V případě kybernetického incidentu pojišťovna KOOP hradí škody na datech v elektronické podobě, konkrétně jejich poškození, odcizení, ztrátu nebo únik. Dalším typem pojistné události může být nefunkčnost nebo porucha počítačového systému v důsledku kybernetického incidentu. Pojišťovna také hradí náklady na opravu či obnovu (znovupořízení) dat, které byly poškozeny, zničeny, odcizeny nebo ztraceny z počítačového systému pojištěného. Jako další hrazené náklady z pojištění jsou ty, které byly nutné k obnovení funkčnosti vlastního počítačového systému pojištěného do stavu bezprostředně před pojistnou událostí (včetně odstranění případného malwaru). Pojišťovna uvádí, že bude hradit také náklady na IT odborníka, kdy pokud to bude IT odborník určený pojišťovnou, klient nemusí hradit spoluúčast sjednanou v pojistné smlouvě.

Jedna samostatná sekce pojistných podmínek se věnuje nákladům na **regulatorní řízení**, které musí být explicitně ujednané v pojistné smlouvě. Jedná se o náklady na zastupování pojištěného ve správním řízení vedeného Úřadem pro ochranu osobních údajů proti pojištěnému z důvodů porušením zabezpečení osobních údajů o fyzických osobách uložených v počítačovém systému pojištěného, které bylo vyvoláno kybernetickým incidentem. Pojistné podmínky upřesňují, že zahájení regulatorního řízení proti pojištěnému musí nastat v době trvání pojištění, a v oblasti územní platnosti pojištění (tzn. České republice).

Jiná samostatná sekce pojistných podmínek upravuje podmínky pro úhradu nákladů tzv. ***„public relations“***, jinak řečeno obnovu dobrého jména. Tyto náklady také musí být explicitně sjednané v pojistné smlouvě. Podmínky takovou situaci popisují jako ztrátu nebo oslabení důvěryhodnosti pojištěného u jeho zákazníků, dodavatelů či jiných smluvních partnerů (popř. pokud to reálně hrozí). Pojišťovna v takovém případě uhradí náklady na uveřejnění informací ve veřejném sdělovacím prostředku (např. formou tiskové zprávy), včetně informací o případných opatřeních učiněných pojištěným k odstranění nebo zmírnění následků kybernetického incidentu nebo k předcházení nebezpečí jeho opakování. Podmínkou je, že se tyto informace týkají výlučně kybernetického incidentu, musí být uveřejněny do 30 dnů od kybernetického incidentu, a samozřejmě jen pokud se jedná o přiměřené, účelné, hospodárně a prokazatelně vynaložené náklady pojištěným.

Sekce *„**Odpovědnost za újmu**“*, která též musí být ujednána, se věnuje finanční újmě způsobené únikem dat v elektronické podobě z počítačového systému pojištěného, a zároveň nákladům právní ochrany pojištěného. Musí přitom platit, že uniklá data nejsou veřejně přístupná a současně podléhají zákazu zpřístupnění vyplývajícímu z obecně závazného právního předpisu nebo ze smlouvy (např. osobní údaje fyzických osob, informace podléhající zákonné povinnosti mlčenlivosti, obchodní tajemství). Dále pak to musí být v důsledku kybernetické incidentu, a pojištěný je povinen poskytnout náhradu újmy na základě obecně závazných právních předpisů. Odpovědnost za újmu kryje navíc také finanční újmy, způsobenou poškozenému v důsledku nefunkčnosti nebo poruchy funkčnosti vlastního počítačového systému poškozeného, nebo v důsledku zničení, poškození, odcizení nebo ztráty dat z počítačového systému poškozeného za předpokladu, že taková újma vznikla v důsledku kybernetického incidentu v počítačovém systému poškozeného, který byl způsoben kybernetickým incidentem v počítačovém systému pojištěného. Stručněji řečeno a převedením do praktického příkladu, pokud kybernetický incident v podniku XYZ způsobí kybernetický incident u koncového zákazníka, a podnik XYZ za to bude odpovědný, pojišťovna uhradí poškozenému vzniklou škodu. Navíc pojišťovna (pokud pojištěný splní své povinnosti) uhradí náklady související s řízením o náhradě újmy, na právní zastoupení, na obhajobu a mimosoudní projednávání. Výše těchto nákladů je samozřejmě v pojistných podmínkách upravena s ohledem například na jejich účelnost, odměny advokáta stanovené právními předpisy, a spoluvinu poškozeného. Na sekci *„Odpovědnost za újmu“* se kromě společných výluk produktu vztahují také speciální výluky, určené právě jen pro tuto sekci (podrobněji viz dále).

K produktu je navíc možné volitelně sjednat **přerušení provozu**, které kryje následnou škodu v podobě finančních nákladů jako ušlý zisk a stálé náklady. Velmi podstatnou informací v pojistných podmínkách je informace o časové spoluúčasti, která je dohodnutá v pojistné smlouvě. Jedná se o časový úsek ihned po kybernetickém incidentu, který nehradí pojišťovna, ale pojištěný. Pokud doba přerušení provozu nepřesáhne časovou spoluúčast, nevznikne pojištěnému právo na plnění z pojištění přerušení provozu. Pojistná smlouva stanovuje, od jakého dne pojišťovna hradí škodu z přerušení provozu. Pokud tedy ve smlouvě bude uvedeno 2 dny a přerušení provozu bude trvat 2 dny, pojišťovna nic neuhradí. Pokud ve smlouvě bude uveden 1 den a přerušení provozu bude trvat 3 dny, pak pojišťovna uhradí jen poslední 2. Stejně tak pojistné podmínky definují horní hranici jako dobu ručení, a definují také způsob výpočtu přerušení provozu, k čemuž využívají srovnávací období tří kalendářních měsíců předcházejících měsíci, ve kterém vznikla pojistná událost. V případě, že pokles průměrných denních příjmů za dobu částečného přerušení provozu (nejdéle však za dobu ručení) ve vztahu ke srovnávanému období nepřesáhne 20 %, nevznikne pojištěnému právo na plnění z pojištění přerušení provozu. Další podstatnou informací je, že toto pojištění se nevztahuje na přerušení provozu v důsledku zákazu nebo omezení vyplývající z rozhodnutí, nařízení či jiného opatření či zásahu orgánu státní moci nebo veřejné správy. To však logicky není součástí přerušení provozu v důsledku kybernetických rizik, ale pojišťovna to může nabízet až v rámci samostatného pojištění přerušení provozu (viz samostatný oddíl dále). Pojišťovna také není povinna plnit za zvětšení rozsahu následné škody způsobené tím, že pojištěný nevyvíjel plné úsilí pro urychlené obnovení provozu, nebo nezajistil včas obnovu nebo opětovné pořízení prostředků sloužících provozu.

<u>Podmínky pojištění a povinnosti pojištěného:</u>

Podmínkou pro sjednání daného pojištění je, že podnik dbá na určitá bezpečnostní opatření, jako je například používání silných hesel a antivirů, práce v oficiálních a aktuálních verzích programů nebo provádí pravidelné zálohování dat. Pojistné podmínky definují převážně obecné povinnosti, které lze běžně očekávat od podniku, jež odpovědně řídí rizika. Pojišťovna

nejprve požaduje vyplnění dotazníku vztahujícího se ke sjednávanému pojištění, kdy od klienta očekává jejich pravdivé a úplné zodpovězení. Následně je od klienta očekáváno, že stejnou úroveň zabezpečení, kterou uvedl v dotazníku, také po celou dobu pojištění dodržuje. Smysl je celkem jasný, cena pojištění se velmi pravděpodobně odvíjí od úrovně zabezpečení, a klient by neměl uzavření pojištění brát tak, že se již o nic nemusí starat. I nadále pro klienta platí, že musí mít zabezpečení nepřetržitě aktivní a pravidelně jej musí aktualizovat, chránit prvky sloužící k ochraně počítačového systému a dat, zamezit neoprávněnému přístupu k nim (např. používat antivirové programy, firewall, hesla nebo obdobné ochranné prvky), a dodržovat pokyny a doporučení výrobců, dodavatelů či poskytovatelů hardwaru a softwaru. V případě vzniku škody je pojištěný povinen ji nejen neprodleně oznámit pojišťovně, ale také postupovat v souladu se všemi jejími pokyny (resp. jejího smluvního partnera), zejména využít služeb jimi určeného nebo předem odsouhlaseného IT odborníka. Pojištěný je také povinen umožnit přístup do svých počítačových systémů, poskytnout veškerou potřebnou součinnost, uchovat veškerý relevantní hardware, software a data a poskytnout je na žádost pojišťovně (resp. jejímu smluvnímu partnerovi). Další povinnosti pojištěného a důsledky porušení povinností mohou vyplývat z ustanovení pojistné smlouvy, kterou by si klient měl před podpisem důkladně pročíst. Jak se říká *„Přečíst musíš, podepsat můžeš“*.

Výluky z pojištění:

Pojistné podmínky obsahují mimo jiné několik **základních výluk**, jako je například výluka na škody způsobené úmyslně nebo v souvislosti s úmyslným protiprávním jednáním zejména pojistníka, pojištěného nebo člena statutárního či kontrolního orgánu těchto osob. Pojistné podmínky výčet osob, na které se výluka úmyslného jednání vztahuje, rozšiřují o osoby, jejíž počítačový systém pojištěný výlučně užívá, vedoucího zaměstnance v přímé řídící působnosti člena statutárního orgánu, jejich prokuristy nebo osoby pověřené nebo zodpovědné za nastavení, správu nebo zabezpečení jejich počítačového systému a dat v něm uložených. Do výluky spadají také osoby jednající z podnětu či v dohodě s některou z všech uvedených osob. To je poměrně široký výčet, ale obecně se jedná o zcela běžnou výluku, kterou lze vidět i v jiných pojistných podmínkách, nejen v podmínkách kybernetického pojištění, ale třeba i v povinném ručení nebo běžné odpovědnosti. Výluka je svým způsobem i logická.

Mezi další základní výluky patří i výluka na škody vzniklé v souvislosti s požitím alkoholu nebo aplikací omamných či psychotropních látek výše uvedených osob. Opět se jedná o zcela běžnou výluku i pro jiné druhy pojištění. Stejně tak jsou logicky vyloučeny škody vzniklé v důsledku skutečností, které pojistníkovi nebo pojištěnému byly nebo s přihlédnutím ke všem okolnostem mohly být známy v době uzavření pojistné smlouvy.

Naproti tomu pojistné podmínky obsahují mimo jiné **výluky**, které jsou svým charakterem **specifické výhradně pro kybernetické pojištění**, avšak logické, a preventivně vylučují situace, které nejsou v pravém slova smyslu kybernetickými incidenty (resp. útoky). Jedná se například o újmu vzniklou v souvislosti s plánovanými odstávkami, výpadky nebo přerušením fungování počítačových systémů nebo jejich částí, dále pak je vyloučena újma způsobená selháním připojení, výpadkem, přerušením nebo omezením fungování jakékoli sítě (např. internetové, telekomunikační, satelitní, kabelové, elektrické). Z pojištění dále nevzniká právo na náhradu nákladů na jakoukoli aktualizaci, upgrade, rekonfiguraci nebo redesign počítačových systémů nebo dat nad úroveň, která existovala bezprostředně před vznikem pojistné události. Dala by se sem zařadit také výluka na škody vzniklé v důsledku vady nebo chyby ve vývoji, konstrukci, obsahu nebo trochu sporná výluka na nastavení hardwaru nebo softwaru. Otázkou je, co pojišťovna řadí do nastavení softwaru. Bude pojišťovna považovat chybné nastavení antivirového programu za výluku? Stejně tak nejsou hrazeny škody v důsledku stárnutí, opotřebení, koroze nebo eroze, a působení magnetických nebo

elektromagnetických polí. Toto je zatím výčet výluk, které lze (vyjma jedné) relativně očekávat a nemusí být pro pojištěného nikterak překvapující.

Pojistné podmínky dále vylučují **situace, za které si pojištěný podnik může svým způsobem sám**, a kterým bylo možné předejít. Mezi takové výluky patří situace vzniklé v souvislosti s neoprávněným užitím softwaru nebo hardwaru, s užitím neautorizovaného softwaru nebo hardwaru, nebo s neoprávněným zpracováním dat výše uvedenými osobami. Dále pak situace vzniklé v důsledku připojení k nezabezpečené počítačové síti, způsobené porušením práv v oblasti ochrany duševního vlastnictví (např. autorské právo, právo na patent), či způsobené porušením povinnosti pojištěného spolupracovat s příslušnými orgány v rámci šetření nebo řízení týkajícího se kybernetického incidentu a přijmout opatření k dodržení jejich pokynů, rozhodnutí nebo nařízení. Výčet výluk obdobného charakteru tímto nekončí, pojistné podmínky obsahují ještě několik takových, kdy pojišťovna nechce poskytovat plnění. Buď se nejedná o kybernetický incident, nebo jim lze předejít jen tím, že podnik nebude zcela pasivní při práci s daty, a například na žádost klienta odstraní zpracovávaná data o něm. Nad rámec toho pojistné podmínky pojišťovně umožňují přímo do pojistné smlouvy vložit další výluky, na což by si klient při sjednání smlouvy měl dát pozor.

Avšak pojistné podmínky obsahují i **překvapivá ustanovení**, které by pojištěný čekal již méně. Pojištění kybernetických rizik je na webových stránkách KOOP prezentováno jako pojištění, které podnik uchrání i před hrozbou porušení GDPR. KOOP konkrétně na svých webových stránkách uvádí: *„Ztráta dat, důvěry zákazníků a často i finančních prostředků může být pro vaše podnikání fatální. Nové nařízení EU o ochraně osobních údajů (GDPR) navíc přímo ukládá povinnost adekvátně zabezpečit osobní data a v případě podobného útoku a absence zabezpečení hrozí vysoké pokuty. Proto vás proti kybernetickým rizikům pojistíme.“*. To ale dle pojistných podmínek má svá omezení v podobě výluky, která říká, že pojistitel neposkytne pojistné plnění na úhradu sankcí a jiných plateb, které mají represivní, preventivní nebo exemplární charakter (včetně případných sankčních složek náhrady újmy, tzv. punitive damages), bez ohledu na to, komu byly uloženy. Uvedenou výluku lze tedy chápat tak, že pokud podnik nedodrží pravidla GDPR, a bude mu uložena vysoká (až likvidační) pokuta ze strany dozorového orgánu, pojišťovna mu v takové situaci nepomůže. Stejně tak pojišťovna nebude z pojištění hradit výkupné, tj. jakéhokoli plnění požadovaného osobou, která vyvolala nebo hrozí vyvoláním kybernetického incidentu v počítačovém systému pojištěného, za ukončení nebo upuštění od jejího protiprávního jednání, případně za odstranění následků takového jednání. Další překvapující výlukou může pro některé podniky být výluka na škody vzniklé v důsledku kybernetických incidentů v počítačových systémech využívaných v souvislosti s řízením/ovládáním dopravních prostředků. Převedením do praktického příkladu, pokud podnik využívá autonomní dopravní prostředky (v současnosti zatím ne na veřejných komunikacích), pak kybernetický útok na takové dopravní prostředky není krytý pojištěním. To je samozřejmě na dnešní dobu stále málo představitelná situace, ale jak již bylo zmíněno v samotném úvodu práce *„Kolik věcí se považuje za nemožné, dokud se skutečně nestanou?“*. Co je ale mnohem lépe představitelné, že se bude jednat o dopravní prostředek řízený na dálku nebo za pomoci řidiče. Tato výluka by mohla být obzvlášť kritická pro podnik XYZ, který se zabývá vývojem, výrobou a dodáváním automatizační, řídicí a přístrojové techniky. A není to jediná taková výluka. Pojišťovna vylučuje i úhrady škod vzniklých v souvislosti s činností pojištěného spočívající v poskytování software či hardware nebo jakýchkoli jiných činností a služeb (např. prodej, servis, správa, poradenství) v oblasti počítačových systémů a informačních technologií, včetně provozování nebo správy webových portálů, zpracování, správy nebo uchovávání dat (např. poskytování hostingových, cloudových a obdobných služeb). Opět převedením do praktického příkladu to znamená, že pojištění se nevztahuje na situace, kdy podnik XYZ někomu dodá svůj výrobek nebo službu

(např. software), a hacker napadne tento software, který již bude nainstalován u zákazníka (popř. právě bude prováděna instalace).

Poslední z řady překvapivých ustanovení může být výluka na újmu vzniklou v souvislosti s finančními transakcemi, či obchodováním na finančních trzích. Pokud tedy podnik XYZ investuje na finančních trzích, a hacker se naboural do jejich účtu, pojišťovna pravděpodobně nevyplatí pojistné plnění. Výluku lze chápat tak, že pojišťovna neuhradí i jiné škody v souvislosti jakýmikoliv finančními transakcemi.

U připojištění odpovědnosti za újmu je navíc výluka na újmy vzniklé majetkově propojeným osobám s pojištěným (osoby blízké, dceřiné společnosti, jednatelé apod.), právo z vadného plnění (vady, záruky), povinnosti převzaté nad rámec zákona, či pokud pojištěný ujednal delší promlčecí lhůtu, než je ta zákonná.

Další části pojistných podmínek, na které je třeba si dát také pozor:

Náklady na IT odborníka jsou hrazeny pouze za služby poskytnuté IT odborníkem z území České republiky. Pojistné plnění je poskytnuto maximálně do limitu, který je uveden v pojistné smlouvě. Dále je pojistné plnění hrazeno pouze do výše účelně vynaložených nákladů na nejhospodárnější ze způsobů řešení, jinak řečeno ten ze způsobů řešení, který umožní obnovu dat, obnovení funkčnosti počítačového systému nebo řešení jiných případných následků pojistné události při vynaložení nejnižších nákladů.

Hodnocení produktu:

Produkt je určen pro podnikatelské subjekty, a tedy i pro podnik XYZ, avšak ve výsledku nabízí spíše základní ochranu. Rozhodně se nejedná o *„All risk“* pojištění, které by krylo jakýkoliv incident, který může v podniku nastat. Zároveň nekryje velké potenciální škody (např. vysoké sankce za nedodržení GDPR), a vlastně ani ty malé, pokud je ve smlouvě sjednána časová spoluúčast. Pojištění se tak dá považovat spíše za doplněk managementu rizik. Přestože produkt na první pohled nabízí mimořádně široké krytí, po bližším prostudování pojistných podmínek, má i mnoho výluk, z nichž některé mohou být pro tak specializovaný podnik jako je XYZ nepřijatelné, jelikož mohou být v rozporu s předmětem podnikání. Pro rozhodnutí, zda takové pojištění sjednat, jsou pak zcela zásadní otázky ohledně činnosti podniku XYZ, a co od kybernetického pojištění vůbec očekává. V neposlední řadě bude rozhodující i cena pojištění.

Allianz pojišťovna, a. s.

Allianz pojišťovna, a.s. (dále jen AZP) také patří mezi velké hráče v oblasti pojištění podnikatelů, konkrétně na českém pojistném trhu zabírá třetí příčku. AZP má širokou nabídku různých typů pojištění nejen pro menší a střední podnikatele, ale také pro velké korporace. Nabízí mnoho specifických typů pojištění jako je pojištění letadel, plodin, zvířat, profesní odpovědnost mnoha oborů (např. lékařů, právníků, veterinářů, realitních makléřů), silničního dopravce, zásilek, D&O a mnoho dalších. Avšak po důkladném prostudování webových stránek AZP, tato pojišťovna aktuálně nenabízí na českém trhu možnost sjednání kybernetického pojištění, a to ani pro občany, ani pro podnikatele.

ČSOB pojišťovna, a.s., člen holdingu ČSOB

ČSOB Pojišťovna, a.s., člen holdingu ČSOB (dále jen ČSOBP) nabízí podnikatelské pojištění kybernetických rizik. ČSOBP na svých webových stránkách uvádí, že v případě kybernetického útoku nenechá své klienty na holičkách, a bude za ně vše řešit.

Obecná specifikace produktu:

Pojištění kybernetických rizik se řídí dle všeobecných pojistných podmínek s označením VPP CRC 2018 s účinností od 1. listopadu 2018. Kromě toho se kybernetické pojištění řídí všeobecnými pojistnými podmínkami – obecná část VPP OC 2014, kde jsou vymezeny další práva a povinnosti účastníků pojištění kybernetických rizik. ČSOBP o svém produktu píše, že se jedná o komplexní pojištění škod na datech, kdy uhradí náklady na obnovu dat, na IT podporu, která je k dispozici 24/7, právní služby a další náklady. Ve svém reklamním spotu, který je také na webu ČSOBP, pojištění označuje nikoliv jako náhradu antivirového programu, ale jako jeho doplněk. V daném videu mimo jiné potvrzuje rostoucí počet kybernetických útoků na podniky, a formou příkladu upozorňuje na následky takového útoku, jako je třeba nabourání dodavatelsko-odběratelského řetězce, kde podniku může vzniknout odpovědnost za škodu vzniklou jejím obchodním partnerům. Dále to je přerušení provozu podniku (např. kolaps stránek e-shopu), náklady na IT specialistu, PR specialisty, kteří se postarají, aby organizace utrpěla co nejmenší újmu ve vnímání veřejnosti, nebo na právníky.

Pojištěná rizika:

Pojištění kryje riziko kybernetického incidentu, který pojistné podmínky definují jako nezákonné jednání, malware, lidské pochybení, útok typu DoS, odcizení dat, který bude mít dopad na počítačový systém pojištěného nebo počítačový systém jeho providera nebo důvodné podezření na některou z těchto skutečností.

Rozsah krytí:

Do základního rozsahu krytí jsou zařazeny finanční ztráty pojištěného spočívající v přiměřených a nezbytných nákladech na činnost odborníka, který vyšetří kybernetický incident, s cílem dodržet všeobecné závazné právní předpisy vztahující se k ochraně dat, včetně všeobecně závazných právních předpisů upravujících ochranu osobních údajů, zejména informování kompetentního státního orgánu nebo informování subjektů údajů. Dalším pojištěným nákladem jsou náklady na práci zaměstnanců přesčas, na provozování vnitropodnikového centra krizového managementu po dobu prvních 30 dní od oznámení pojistné události, dále pak na zabezpečení služeb na monitorování neoprávněného používání karet (zejména věrnostní karty, přístupové, atd.) a krádeže totožnosti subjektu údajů postihnutých kybernetickým incidentem (toto se hradí pouze se souhlasem pojišťovny). Pojistné podmínky do základního rozsahu řadí také náklady na odborníka, který po pojistné události zabezpečí pojištěnému PR služby, až do uplynutí platnosti doby ochrany dobrého jména, a na právní obhajobu, která vznikne v souvislosti se žalobou vznesenou vůči pojištěnému kompetentním státním orgánem.

ČSOBP oproti KOOP již v základním rozsahu krytí nahradí i náklady pojištěného vynaložené v souvislosti s administrativně-právními sankcemi, zejména pokutami, udělenými kompetentním státním orgánem v přímé souvislosti s porušením ochrany dat (pouze pokud se jedná o pojistnou událost).

Podnik si může sjednat krytí i dalších pěti typů nákladů. Prvním z nich jsou náklady na obnovu dat a softwaru pojištěného po kybernetickém incidentu, do stavu co nejvíce se blížícímu původnímu stavu bezprostředně před kybernetickým incidentem. Druhým typem jsou finanční ztráty pojištěného, vzniklé přerušením (popř. omezením) provozu, které bylo přímo způsobené kybernetickým incidentem, kdy pojišťovna nabízí uhradit ušlý zisk, stálé náklady a vícenáklady po dobu trvání přerušení (popř. omezení) provozu. Třetím typem jsou finanční ztráty pojištěného vzniklé v podobě výkupného, které pojištěný zaplatí, výlučně na základě předcházejícího písemného souhlasu pojišťovny (na rozdíl oproti KOOP, která je

nehradí vůbec), a jakékoli přiměřené a nezbytné náklady na vyřešení kybernetického vydírání. Jako čtvrtý typ je možné sjednat pojištění náhrady jakýchkoli peněžních prostředků, o které přijde pojištěný přímo v důsledku kybernetického zločinu. A posledním typem je možnost pojistit si náhrady jakýchkoli peněžních pokut a sankcí, které vůči pojištěnému uplatní poskytovatel platební karty z důvodu porušení standardů PCI-DSS pojištěným, které bude přímo způsobené kybernetickým incidentem. Pokud to bude poskytovatel platební karty požadovat, pojišťovna uhradí i jakékoli přiměřené a nevyhnutné náklady na forenzního vyšetřovatele v odvětví platebních karet, který prošetří podezření z porušení standardů PCI-DSS, opětovnou certifikaci v oblasti standardů PCI-DSS, nebo opětovné vystavení jakékoli kreditní, debetní nebo předplacené karty z důvodu porušení standardů PCI-DSS pojištěným, které bude přímo způsobené kybernetickým incidentem.

Podmínky pojištění a povinnosti pojištěného:

Jak již bylo dříve uvedeno, povinnosti pojištěného pro kybernetické pojištění jsou uvedeny ve Všeobecných pojistných podmínek – Obecná část VPP OC 2014. V nich jsou uvedeny **obecné povinnosti** pojištěného, které jsou platné napříč mnoha podnikatelských pojištění od ČSOBP. Uvedené pojistné podmínky mimo jiné upravují takové základní povinnosti pojištěného jako je včasné oznámení škody pojišťovně, neměnit stav škody dokud není prohlédnuta pojišťovnou (nejdéle však 10 dnů) vyjma určitých situací (bezpečnostní nebo hygienické důvody), a podobné další. Nicméně zde nejsou žádné speciální povinnosti pro pojištění kybernetických rizik. Zvláštní povinnosti pojištěného, které se přímo vztahují ke kybernetickému pojištění, jsou uvedeny ve všeobecných pojistných podmínkách VPP CRC 2018 pro kybernetické pojištění.

Do těch **základních povinností**, pro pojištěného dosti intuitivních, patří široký výčet povinností. Jedná se o zejména povinnosti dodržovat technické a další normy včetně předpisů vztahujících se na provoz pojistníka nebo pojištěného, vést prokazatelnou dokumentaci, udržovat provoz v dobrém technickém stavu, podat pravdivé vysvětlení o vzniku škody a rozsahu následků, předložit doklady potřebné k posouzení škody, a umožnit pojišťovně získat kopie těchto dokladů. Tímto výčet povinností pojištěného zdaleka nekončí a mezi ty další patří také povinnost oznámit pojišťovně nároky třetích stran, informovat jí o zahájení trestního řízení, postupovat v souladu s jejími pokyny, nezavazovat se bez jejího souhlasu k náhradně promlčené pohledávky, neuzavírat bez jejího souhlasu soudní smír, spolupracovat a poskytovat přiměřenou součinnost, každou opravu nebo odstranění následků škody vykonat přiměřeným způsobem, poskytnout důkaz vzniku škody, zachovat, zpřístupnit a umožnit vykonání šetření jakýchkoli podkladů nebo dokumentů, zejména hardwaru, softwaru a dat, a to všechno samozřejmě pouze v souvislosti se škodou. Tyto a další základní povinnosti pojištěného nejsou žádným překvapením pro klienta. Od pojištěného se v podstatě očekává spolupráce při řešení škody, obezřetnost a uvážlivé chování.

Pojistné podmínky dále obsahují i povinnosti ve smyslu **prevence vzniku škody**. Jedná se o povinnost zálohovat svoje data minimálně jednou za týden. Tato povinnost nemusí být v každém podniku běžná, a je potřeba si na ni zvyknout. Jedná se o relativně splnitelnou povinnost, pokud bude nastaveno automatické zálohování. Každopádně tato povinnost patří k těm velmi důležitým, a bez přečtení pojistných podmínek by ji podnik nemusel zaznamenat.

Jiná preventivní povinnost je nainstalovat, mít nepřetržitě aktivovaný a automaticky aktualizovat přiměřený profesionální software na ochranu proti malware na svých počítačových systémech, chránit svoje počítačové systémy a počítačovou síť před kybernetickými incidenty, jako například aktualizací hesel, konfigurací a firewall, v opačném případě není pojistitel povinný poskytnout pojistné plnění. Tuto povinnost lze předpokládat, že v určité míře dodržuje v dnešní době každý podnik. Ovšem pojistné podmínky nestanovují

přesné parametry zajištění takové bezpečnosti, jako je například typ antivirového programu, frekvence změny hesel, jinak řečeno, co přesně znamená přiměřeně? Ve volném překladu autora to znamená, že si pojišťovna dává prostor pro individuální posouzení každé situace a možnost odmítnout škodu uhradit. Podnik by si tedy zřejmě měl zmapovat aktuální stav zabezpečení a pojišťovnou si nechat odsouhlasit, že se jedná o dostatečné zabezpečení. V opačném případě hrozí, že by pojišťovna nemusela plnit naopak svojí povinnost uhradit škodu.

Výluky z pojištění:

ČSOBP v pojistných podmínkách pro kybernetické pojištění využívá několika podobných výluk jako KOOP. Z těch **základních výluk** to je třeba výluka na škodu způsobenou úmyslným jednáním pojištěného, pojistníka nebo osob jednajících z jejich podnětu. Dále pojišťovna neuhradí ani škody způsobené v důsledku vědomé nedbalosti pojištěného, pojistníka, trestným činem pojištěného, pojistníka nebo osob blízkých. Oproti KOOP, ale již nevylučuje úmyslné jednání dalších osob jako například členů statutárního nebo kontrolního orgánu, a jiné. V této výluce je ČSOBP oproti KOOP mírnější. Pojišťovna má v pojistných podmínkách také výluku na škodu způsobenou pod vlivem alkoholu nebo jiných psychotropních nebo omamných látek nebo léku s varovným symbolem. Opět celkem běžná výluka, která pojišťovnu opravňuje nehradit třeba škody způsobené opilým zaměstnancem. Však také v podniku bývá standardně vnitřním předpisem zakázána práce pod vlivem alkoholu, psychotropních a jiných látek. Pojem léky s varovným symbolem pojišťovna nijak dále neupřesňuje, ale dá se předpokládat, že se jedná třeba o prášky na spaní, a jiné léky ovlivňující pozornost, reakce, úsudek, či kvalitu vidění.

Pojistné podmínky vylučují dále škody, které ve své podstatě ani **nejsou kybernetickým incidentem**, jako jsou škody přímo nebo nepřímo související s jadernou energií, jaderným a jiným zářením jakéhokoliv druhu, magnetickým nebo elektromagnetickým polem, či ionizací. Pojistné podmínky dále vylučují škodu vzniklou v příčinné souvislosti s válečnými událostmi, vyhlášením válečného nebo výjimečného stavu, napadnutím nebo činem vnějšího nepřítele, nepřátelskou akcí bez ohledu na to, či byl válečný stav vyhlášen nebo ne, vzniklou v příčinné souvislosti s revolucí, povstáním, vzpourou, státním nebo vojenským převratem, občanskou válkou, demonstrací, zabavením nebo represívními zásahy státních orgánů, a to vše bez ohledu na jakékoliv další současné nebo v jakémkoliv časovém sledu spolupůsobící příčiny. Stejně tak podmínky vylučují náklady vyplývající z nařízení vlády nebo náklady související s přemístěním nebo modifikováním majetku pojištěného, který nemůže být nadále používaný k původnímu účelu. Podobně také nejsou hrazeny ani škody způsobené v důsledku vypuštění, rozptýlení, prosakování, proudění, uvolnění nebo úniku nebezpečných, znečišťujících nebo škodlivých látek. Dále nejsou hrazeny škody, které vzniknou přímo nebo nepřímo ze selhání, přerušení, zhoršení nebo výpadku infrastruktury dodavatelů následujících služeb: telekomunikačních, internetových, satelitních nebo kabelových služeb, dodávky elektrické energie, plynu nebo vody. Pojistné podmínky obsahují ještě několik výluk podobného charakteru. Jejich smyslem je omezit plnění jen na skutečné kybernetické incidenty.

Všechny prozatím uvedené výluky jsou pochopitelné a dost pravděpodobně by ani pojištěného nenapadlo nahlašovat takovou škodu jako kybernetický incident. Nicméně tu je jedna výluka na škody, které by pojištěný mohl za kybernetický incident považovat a to je výluka na škody v příčinné souvislosti s jakýmkoliv teroristickým činem nebo kybernetickým terorismem. Ne zcela každý kybernetický incident pojištění kryje. Pokud podnik XYZ nepatří do klíčové infrastruktury státu, pak se pravděpodobně nemusí obávat, že bude ve středu zájmu kybernetických teroristů.

Další kategorií výluk jsou výluky na škody, kterým jednak bylo možné předejít, ale především k takovému jednání by v odpovědném podniku ani nemělo docházet. Řeč je o škodách způsobenými v souvislosti s jakoukoli činností vykonávanou pojištěným v rozporu s všeobecně závaznými právními předpisy, včetně škody způsobené v souvislosti s jakoukoli činností vykonávanou pojištěným bez relevantního oprávnění nebo bez požadované odborné kvalifikace, včetně neoprávněného shromažďování dat, neoprávněným užíváním cizí věci nebo zatajením věci, poškozením věci v důsledku jejího využití k jinému účelu, než byla určena, dále pak škody, které vzniknou přímo nebo nepřímo z použití nezákonného nebo nelicencovaného softwaru. Stejně tak nemohou být hrazeny ani škody způsobené porušením pravidel hospodářské soutěže, porušením pravidel veřejné soutěže, porušením práv duševního vlastnictví, zejména autorského práva, patentového práva, či ochranné známky.

Do kategorie výluk, a tedy škod, kterým pojištěný mohl předejít lze zařadit i nedbalost pojištěného jako jsou škody, které vzniknou v případě, že pojištěný neodstraní data na webovém portále nebo na webové stránce pod kontrolou pojištěného po tom, co pojištěný dostane oprávněnou stížnost nebo žádost třetí strany. Podobně nejsou hrazeny ani škody, které vzniknou z uveřejnění na jakémkoli webovém portále, na kterém se obsah může uveřejnit bez registrace vkládající osoby, nebo z jakéhokoli webového portálu nebo jakéhokoli obsahu, nad kterým nemá pojištěný přímou kontrolu. Dále nejsou hrazeny škody, které vzniknou přímo nebo nepřímo ze škodných událostí, které pojištěný zjistí nebo které měl rozumně zjistit před dobou platnosti pojistné smlouvy. Uvedenou výluku lze chápat tak, že se cizí osoba naboural do systému pojištěného už dříve, ještě před počátkem pojištění, ale například krádež dat provede až v době platnosti smlouvy.

Pojistné podmínky ovšem obsahují také výluky pro škody, které pojišťovna evidentně považuje za vysoce rizikové a raději je preventivně vylučuje. Stejně jako KOOP, ani ČSOBP nechce hradit škody, které vzniknou přímo nebo nepřímo v souvislosti s poskytováním „cloudových“ a obdobných řešení pojištěným, a dále pak ty, které vzniknou v důsledku kybernetického incidentu na počítačových systémech pojištěného, které se využívají v souvislosti s řízením dopravních prostředků. Pravděpodobně ze stejného důvodu pojišťovna vylučuje i škody, které vzniknou na datech ve smyslu finančního vyjádření hodnoty těchto dat.

ČSOBP, stejně jako v KOOP, nechce hradit škody, které vzniknou přímo nebo nepřímo ze ztráty nebo poškození hmotného majetku a jakékoliv následné majetkové újmy včetně ztráty možnosti užívání hmotného majetku. Převedením do praxe, fyzické poškození harddisku, který obsahuje důležitá data, byť poškození cizí osobou, není považováno za kybernetický incident. Smyslem této výluky je nehradit škody, které mají být hrazeny z jiného pojištění, a to majetkového. Podnik by pro tyto a podobné případy měl mít navíc pojištěnou krádež, loupež, vandalismus a elektroniku. Jinak řečeno, kybernetické pojištění plně nenahrazuje majetkové pojištění a je potřeba zvolit vhodnou kombinaci různých druhů produktů pro zajištění optimální ochrany.

Další části pojistných podmínek, na které je třeba si dát také pozor:

V případě škody může pojištěný využít odborníka, kterého si po dohodě s poskytovatelem řešení incidentů sám zvolí, avšak tyto náklady budou hrazené jen do výše maximálních hodinových sazeb určených a sdělených právě poskytovatelem řešení incidentů (smluvním partnerem pojišťovny). Proto pokud chce mít pojištěný jistotu, že mu budou náklady pojišťovnou uhrazeny v plné výši, měl by vždy volit cestu aktivní komunikace s pojišťovnou ohledně nákladů na odstranění škody, a ideálně si zvolit IT odborníka doporučovaného pojišťovnou. Pojištěný by si měl také dávat pozor na maximálně počet asistenčních zásahů,

kdy pojistitel poskytne maximálně tři asistenční zásahy v průběhu jednoho pojistného období (pojistného roku) v úhrnné délce nejvýše 180 minut.

Dále by si pojištěný měl dát pozor na výluku na škody, které mají preventivní, represivní nebo sankční charakter, zejména jakékoliv pokuty, penále, či jiné sankční platby, včetně represivních a exemplárních pokut. Ale pozor, tato výluka se vztahuje pouze na situace, kdy podnik přímo sám nedodrží pravidla GDPR a dostane pokutu. Nikoliv však na situace, kdy dojde ke kybernetickému incidentu dle pojistných podmínek, a tedy pojistné události. Tyto dvě situace je potřeba odlišovat.

Hodnocení produktu:

Pojistné podmínky od ČSOBP jsou vůči klientovi mnohem vstřícnější. Přestože na první pohled obsahují opravdu velké množství výluk, smyslem většiny z nich je nehradit škody, které nejsou kybernetickou hrozbou, nebo jim bylo možné předejít běžnou prevencí a obezřetností. Pojištění má doplňující charakter ke stávající ochraně, ale rozhodně ji nenahrazuje. Ve své podstatě jsou pojistné podmínky trochu i návodem, na co by si podnik měl dávat pozor a jaká základní pravidla ochrany by měl dodržovat. Přesto pojistné podmínky dávají pojišťovně prostor pro odmítnutí pojistného plnění. Nestačí jen sjednat pojistnou smlouvu, ale je potřeba také zkontrolovat úroveň zabezpečení, případně ji zlepšit, nastavit vnitropodnikové procesy pro zálohování, prevenci a podobně, které budou v souladu s podmínkami.

Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group

Jak již název napovídá, Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group (dále jen ČPP) patří do stejné pojišťovací skupiny jako Kooperativa pojišťovna, a.s., Vienna Insurance Group. KOOP je nadřazenou organizací nad ČPP, a je tedy možné, že KOOP řídí produktové portfolio ČPP, ve kterém ale chybí pojištění kybernetických rizik pro podnikatele.

3.1.2 Pojištění přerušení provozu

V teoretické části práce bylo zjištěno, že přerušení provozu se váže na pojištěná rizika v majetkovém pojištění (resp. pojištěnou věcnou škoda). Jinak řečeno pokud je pro věcnou škodu sjednáno pouze krytí rizika požáru, pak přerušení provozu musí vzniknout jako důsledek požáru a věcné škody. V tomto konkrétním oddílu bude ověřeno, zda tomu tak skutečně je i v praxi. Pojistné podmínky obvykle bývají rozděleny na všeobecné a zvláštní pojistné podmínky, případně ještě doplňkové. Právě z důvodu úzkého propojení pojištění přerušení provozu a majetkového pojištění, bude vždy kromě zvláštních/doplňkových pojistných podmínek nutné znát i všeobecné podmínky pojištění. Zkoumány budou také konkrétní parametry nabízeného pojištění přerušení provozu od vybraných pojišťoven, jelikož se mohou lišit například v rozsahu poskytovaného krytí.

Generali Česká pojišťovna, a.s.

Obecná specifikace produktu:

Generali Česká pojišťovna, a.s. (dále jen GČP) nabízí pojištění přerušení provozu v rámci dvou téměř identických produktů. Oba mají shodný název *„Pojištění majetku a odpovědnosti podnikatele a právnických osob“*. Rozdíl mezi nimi je v označení pojistných podmínek, dle kterých se řídí, a rozsahu nabízeného krytí. Jinak řečeno se jedná o dvě varianty stejného pojištění. Dále GČP nabízí samostatné pojištění strojů, ke kterému je možné připojistit přerušení provozu z důvodu poškození nebo zničení stroje jakoukoliv nahodilou událostí,

která není v pojistných podmínkách nebo v pojistné smlouvě vyloučena. K samostatnému pojištění elektronických zařízení není nabízeno pojištění pro následné přerušení provozu.

Pojištěná rizika:

První varianta pojištění se řídí všeobecnými pojistnými podmínkami s označením VPPMO-P-01/2020 a doplňkovými pojistnými podmínkami s označením DPPPP-P-01/2020. Tato varianta nabízí možnost sjednání krytí přerušení provozu v důsledku rizik: požár, výbuch, přímý úder blesku, pád letadla (případně jeho části nebo nákladu), povodeň nebo záplava, vichřice nebo krupobití, sesouvání půdy, zřícení skal nebo zemin, sesouvání nebo zřícení sněhových lavin, pád stromů, stožárů nebo jiných předmětů, tíha sněhu nebo námrazy, zemětřesení, voda vytékající z vodovodních zařízení, odcizení krádeží vloupáním nebo loupeží, a úmyslné poškození nebo úmyslné zničení (tj. vandalismus). Pojištění majetku lze navíc sjednat na riziko přetlaku nebo zamrzání vody ve vodovodním potrubí, což ale není nabízeno v rámci pojištění přerušení provozu.

Druhá varianta pojištění, která má navíc i obchodní název produktu „ProfiPlán“, se řídí všeobecnými pojistnými podmínkami s označením VPPMO-P-02/2020 a doplňkovými pojistnými podmínkami s označením DPPPP-P-02/2020. Rozdílem v krytí je, že tato varianta, oproti první, nabízí navíc krytí rizik kouř a aerodynamický třesk.

Rozsah krytí:

Předmětem pojištění pro obě varianty je finanční ztráta, která je specifikovaná v pojistné smlouvě, a je způsobená přerušením nebo omezením provozu **v důsledku věcné škody**. Pod pojmem finanční ztráta je myšlen ušlý zisk, stálé náklady, ušlé nájemné a vícenáklady. Konkrétně se jedná o ušlý zisk z prodeje výrobků nebo zboží, ušlý zisk z poskytovaných služeb, kterého by oprávněná osoba dosáhla během doby trvání přerušení provozu, nejdéle však během doby ručení, pokud by k přerušení nedošlo, a stálé náklady pojištěného provozu, které musí oprávněná osoba během doby trvání přerušení provozu, nejdéle však během doby ručení, bezpodmínečně vynakládat, aby bylo možné po obnovení zařízení co nejdříve uvést provoz do činnosti v původním rozsahu. Za ušlé nájemné je považováno nájemné z pronájmu bytových i nebytových prostor, nikoliv však náklady na technologické energie a jiné náklady, které při přerušení nenabíhají, odvodové a daňové povinnosti, majetkové sankce (např. penále, pokuty, manka a náhrady škod), které je oprávněná osoba povinna zaplatit v důsledku nesplnění, popř. porušení závazků nebo jiných právních povinností. Pojistné podmínky vysvětlují také vícenáklady, které jsou definovány jako zvýšené náklady, jejichž pomocí může oprávněná osoba v době přerušení provozu realizovat svoji činnost v náhradních prostorách jako je například nájem za provizorní provozovny, náklady na úklid a úpravy provizorních provozoven, nájem za provizorní stroje a zařízení, náklady na dopravu zařízení včetně nákladů na přemístění zařízení do provizorních provozoven, zvýšené náklady na zásobování energiemi vlastního provozu, příplatky za přesčasové práce při náhradní činnosti, zvýšené pojistné za provizorní provozovny, zvýšené náklady na ostrahu a vrátné, či ostatní náklady vzniklé v souvislosti s nájmem provizorních provozoven (tj. zvýšené náklady na reklamu, telefony, správní poplatky apod.).

Pojistné podmínky u všech typů finanční újmy používají termín **doba ručení**, kterým se rozumí sjednaný počet po sobě jdoucích měsíců po vzniku věcné škody, po který je pojišťovna povinna plnit za finanční ztrátu, pokud během této doby vznikne. Doba ručení začíná od okamžiku vzniku věcné škody, nejpozději však od okamžiku, od kterého finanční ztráty vznikají. Není-li v pojistné smlouvě ujednáno jinak, doba ručení za finanční ztráty se ujednává **v délce dvanácti měsíců**.

Věcnou škodou se rozumí poškození, zničení nebo ztráta věci sloužící pojištěnému provozu **sjednaným pojistným nebezpečím**. Právo na pojistné plnění za finanční ztrátu vzniká pouze v případě, že věcná škoda je pojistnou událostí z pojištění staveb nebo věcí movitých nastalá z téže příčiny, na stejném místě pojištění a **u téže pojišťovny**. V překladu to znamená, že nelze sjednat samotné přerušení provozu. Zároveň nastavení produktu a pojistných podmínek od GČP potvrzuje informace z teoretické části práce.

Podmínky pojištění a povinnosti pojištěného:

Pojistník, pojištěný nebo oprávněná osoba má povinnost vést průběžné účetnictví v plném rozsahu, vést průkaznou evidenci o výši tržeb, vynaložených nákladech, příjmech a výdajích alespoň jedenkrát týdně nebo jde-li o fyzickou osobu jedenkrát měsíčně. Dále pak mají **povinnost bezpečně, vzájemně odděleně ukládat ve dvou vyhotoveních** inventury, bilance, obchodní knihy, účty, doklady o daňové a odvodové povinnosti, výsledky hospodaření a smlouvy o pronájmu za tři roky předcházející vzniku pojistné události, a tyto v případě pojistné události pojišťovně předložit. Stejně tak musí učinit opatření směřující k tomu, aby se po nastalé pojistné události vzniklá finanční ztráta již nezvětšovala, a v neposlední řadě bezodkladně po nastalé pojistné události informovat pojišťovnu o jakýchkoliv úkonech, krocích či opatřeních zamýšlených k částečnému či úplnému nahrazení v důsledku věcné škody přerušeného nebo omezeného provozu provozem náhradním realizovaným ekonomicky a technicky možným způsobem (např. přesunem činnosti do jiných výrobních prostor, pronájmem náhradních srovnatelných prostor, strojů a zařízení apod.).

Výluky z pojištění:

Stejně jako u ostatních typů pojištění, i zde existují výluky, kterým je třeba věnovat pozornost, a zde obzvlášť. Samotné majetkové pojištění neobsahuje pojištění strojů a elektroniky, a stejně tak je vyloučeno přerušení provozu z důvodu škody na elektronických nebo strojních zařízeních, které vznikly působením elektrického proudu s výskytem ohně nebo bez něho (např. přepětím, izolační chybou, závitovým zkratem, tělesovým nebo zemním spojením, nedostatečnými kontakty, selháním měřicích, regulačních nebo bezpečnostních zařízení), pokud se oheň dále nerozšířil mimo elektronické nebo strojní zařízení, nebo pokud toto poškození nenastalo v příčinné souvislosti se škodami vzniklými požárem nebo výbuchem na ostatním majetku, který slouží pojištěnému provozu. Vzhledem k tomu, že podnik XYZ je technicky zaměřený, je možné, že bude navíc potřebovat pojištění strojů, ke kterému je teprve vázáno přerušení provozu. V případě elektroniky je přerušení provozu nepojistitelné riziko. K tomu bude nutné položit podniku XYZ otázku.

Pozornost je nutné věnovat také výluce na škody spočívající ve zničení, poškození nebo ztrátě peněz na hotovosti, cenin, cenných papírů, listin, plánů, výkresů, jakékoliv nosiče dat a záznamů na něm (záznamy zvukové, obrazové, datové a jiné), softwarové vybavení, obchodní knihy nebo spisy všeho druhu. Pro příklad, pokud požár zničí některou z uvedených věcí, pojišťovna takovou ztrátu neuzná jako důvod pro úhradu finančních ztrát z přerušení provozu.

Ve výlukách je též uvedeno, co není považováno za ušlý zisk a stálé náklady. Jedná se o náklady, které již při přerušení provozu nevznikají, náklady a výdaje závislé na obratu, sankce, příspěvky, poplatky, dotace apod. Ne tedy každá položka finanční újmy je z pojištění hrazena. Z pojištění také nejsou hrazeny finanční ztráty způsobené neobvyklými událostmi vzniklými během přerušení provozu, a úředním zásahem v důsledku hygienických nebo bezpečnostních důvodů. Z logického důvodu jsou vyloučeny plánované odstávky, nebo pokud pojištěný včas neodstraní následky, či provoz obnovuje ve větším rozsahu, než byl původně (např. inovuje technologii). Pojistné podmínky obsahují i další výluky, které ovšem nebudou

příliš relevantní pro podnik XYZ. Jedná se o výluku na škody na letadlech a zařízeních pro létání všeho druhu, a škody na lodích a jiných plavidlech všeho druhu.

Další části pojistných podmínek, na které je třeba si dát také pozor:

Ušlý zisk a stálé náklady se sjednávají na pojistnou částku, vícenáklady se sjednávají na limit plnění, a ve smlouvě se ujednává spoluúčast. Tyto tři položky budou mít vliv na cenu pojištění, a je tedy velmi důležité ještě před sjednáním pojistné smlouvy udělat propočet pro jejich optimální nastavení.

Hodnocení produktu:

GČP nenabízí zcela plnou ochranu proti všem příčinám přerušení provozu v jednom komplexním pojištění. Zároveň je nutnost mít u GČP sjednané i majetkové pojištění. Ve výsledku by si podnik musel sjednat pojištění majetku a s ním související přerušení provozu, a k němu pojištění strojů a s ním související přerušení provozu. K tomu je nutné počítat s tím, že se pojištění přerušení provozu nevztahuje na kybernetické hrozby, pandemie, úřední zásahy, přerušení v dodavatelském řetězci a jiné nestandardní situace. Pojištění přerušení provozu od GČP lze tedy považovat za velmi „tradiční" pojištění, bez větších inovací, a bez ohledu na nové hrozby, se kterými se podnik může potýkat (viz zjištění v analytické části práce). Pro sjednání pojištění od GČP bude samozřejmě rozhodujícím faktorem také cena daného pojištění.

Kooperativa pojišťovna, a.s., Vienna Insurance Group

Obecná specifikace produktu:

Pravděpodobně z důvodu přehlednosti, KOOP sdružuje pojistné podmínky pro všechny typy pojištění podnikatelů do jednoho souhrnného dokumentu s názvem *„Soubor pojistných podmínek pro pojištění podnikatelů"*. V tomto dokumentu se mimo jiné nachází Všeobecné pojistné podmínky pro pojištění majetku a odpovědnosti s označením P-100/14, a také Zvláštní pojistné podmínky pro pojištění přerušení provozu s označením P-405/14. KOOP o pojištění přerušení provozu na svých webových stránkách píše, že kompenzuje finanční ztráty způsobené přerušením nebo omezením provozu podniku, a že se vztahuje na škody v podobě ušlého zisku a fixních výdajů, které musí podnik i při přerušení provozu vynakládat. Dále na stránkách uvádí, že v rámci pojištění za podnik uhradí mzdy a odvody na sociální a zdravotní pojištění, nájemné včetně leasingových splátek, veškeré placené služby, materiálové náklady vynaložené v době odstávky provozu, odpisy, silniční daň a daň z nemovitosti, pojistné, ušlý provozní hospodářský výsledek atd. Naopak předem avizuje, že nejsou pojištěny variabilní výdaje, tj. výdaje pojištěného, které se mění s objemem výkonů nebo výší obratu, splátky úvěrů, zisky a náklady bezprostředně nesouvisející s výrobní nebo obchodní činností, finanční a jiné sankce.

Pojištěná rizika:

Pojištění od KOOP kryje přerušení provozu nejen v důsledku věcné škody, ale navíc také v důsledku úředního zásahu, což je také podstatným rozdílem oproti pojištění od GČP. Podmínky popisují úřední zásah jako rozhodnutí, opatření nebo jiný zásah orgánu státní moci nebo veřejné správy, v jehož důsledku došlo k přerušení provozu pojištěného v místě pojištění.

Co se týká věcné škody, pojistné podmínky ji omezují jen na pojistná nebezpečí pro pojištění majetku, která jsou konkrétně uvedena v pojistné smlouvě v části pojištění pro případ přerušení provozu, s tím že se musí jednat o pojištěné věci příslušnou smlouvou, nebo budovu

v místě pojištění. Lze jen předpokládat, že stejná rizika, která jsou sjednatelná v majetkovém pojištění, budou sjednatelná i v přerušení provozu, ale KOOP to v pojistných podmínkách blíže nevysvětluje. Jak již bylo v práci dříve řešeno, KOOP nabízí pojištění kybernetických rizik, v rámci kterého je možné připojistit také přerušení provozu v důsledku kybernetických rizik.

Rozsah krytí:

Z pojištění přerušení provozu je hrazena následná škoda, kterou se rozumí zisk z činnosti uvedené v pojistné smlouvě, kterého by pojištěný jinak dosáhl za dobu přerušení provozu, a stálé náklady, které pojištěný musel bezpodmínečně vynaložit během přerušení provozu, pokud by je byl povinen vynaložit i kdyby k přerušení provozu nedošlo. Pro obojí platí, že nejdéle za dobu ručení, která se ujednává standardně v délce tří měsíců, ale v pojistné smlouvě lze ujednat i delší doba.

Podmínky pojištění a povinnosti pojištěného:

Pojištěný je zejména povinen vést evidenci o přerušení provozu, která bude obsahovat údaje o příčině a době přerušení provozu a hospodaření v době přerušení provozu (např. o výši tržeb a nákladech na snížení škody), dále pak umožnit pojistiteli kontrolu hospodaření a plnění opatření vedoucích k urychlenému a úplnému obnovení přerušeného provozu, a to po celou dobu přerušení provozu. Povinností pojištěného je také učinit veškerá opatření směřující k předcházení vzniku následné škody, případně k tomu, aby se následná škoda nezvětšovala, zejména vyvíjet plné úsilí pro urychlené obnovení provozu, zajistit včas obnovu nebo opětovné pořízení zničených, poškozených nebo ztracených věcí sloužících provozu. Další povinnosti pojištěného a důsledky porušení povinností mohou vyplývat z ustanovení pojistné smlouvy, jiných pojistných podmínek vztahujících se ke sjednanému pojištění a právních předpisů.

Výluky z pojištění:

Není příliš překvapení, že se pojištění nevztahuje na přerušení provozu, k němuž došlo v důsledku omezení nebo přerušení dodávek elektrické energie, vody, plynu, tepla nebo jiných médií, předem plánovaných prací a akcí (např. rekonstrukce, opravy, úpravy), úředního zásahu v souvislosti s porušením právní povinnosti ze strany pojištěného, či úředního zásahu, který zakazuje nebo omezuje prodej určitých výrobků, poskytování služeb nebo výkon jiné činnosti bez přímé vazby k místu pojištění. Naopak podnik by mohla překvapit výluky na přerušení provozu v důsledku škody vzniklé na dokumentaci, vzorcích, modelech a prototypech. Vzhledem k činnosti podniku se jedná o velmi reálnou příčinu přerušení provozu. Opět konkrétním příkladem, pokud dojde k malému požáru, který nezpůsobí velké škody na budově nebo movitých věcech, ale pouze na důležité dokumentaci, bez které podnik nemůže fungovat, pojišťovna uhradí přerušení provozu pouze po čas opravy budovy a náhrady movitých věcí, nikoliv však po dobu obnovy dokumentace.

Vyloučeny jsou také škody, kdy k přerušení provozu došlo při výkonu činnosti, která není uvedena v pojistné smlouvě, nebo k jejímuž provozování není pojištěný oprávněn na základě obecně závazných právních předpisů. Dost pravděpodobně podnik XYZ vykonává svoji činnost zcela v souladu s legislativou, ale při případném sjednání smlouvy by si měl podnik pečlivě zkontrolovat činnosti uvedené v pojistné smlouvě.

Podmínky obsahují i dosti logickou výluku, kdy se pojištění nevztahuje na přerušení provozu z důvodu, o kterém pojistník nebo pojištěný v době sjednání pojištění věděl nebo mohl vědět.

Tímto tedy odpadá možnost si narychlo sjednat přerušení provozu například těsně před úředním zásahem.

Pojišťovna dále není povinna plnit za zvětšení rozsahu následné škody způsobené tím, že pojištěný nevyvíjel plné úsilí pro urychlené obnovení provozu, a dále pokud pojištěný nezajistil včas obnovu nebo opětovné pořízení zničených, poškozených nebo ztracených věcí sloužících provozu, nebo k tomu nezabezpečil včas dostatek finančních prostředků.

Další části pojistných podmínek, na které je třeba si dát také pozor:

Na pojištění se mohou vztahovat ještě další výluky uvedené v pojistné smlouvě, jiných ustanoveních pojistných podmínek, jiných pojistných podmínkách vztahujících se ke sjednanému pojištění nebo vyplývající z právních předpisů. Na pojistné plnění má vliv kromě doby ručení také časová spoluúčast a limit pojistného plnění, který se sjednává na pojistný rok. Ve smlouvě lze ujednat také denní limit pojistného plnění. To vše má vliv na cenu pojištění. Podnik by si tedy před případným sjednáním měl dobře promyslet a propočítat optimální nastavení.

Hodnocení produktu:

KOOP bezesporu nabízí širší krytí rizik než její největší rival GČP. Příčinou přerušení provozu může být u KOOP také úřední zásah, a navíc je možné sjednat přerušení provozu v důsledku kybernetické hrozby. To jsou dvě velmi aktuální rizika, a proto lze považovat nabídku od KOOP za inovativní a především aktuální. Co se týká povinností pojištěného, a výluk z pojištění, produkt neobsahuje žádné překvapivé ustanovení. Většina povinností a výluk jsou logická a očekávaná u takového produktu. Pokud podnik vykonává svoji činnost v souladu s legislativou, a chová se zodpovědně, nemělo by žádné ustanovení pojistných podmínek u přerušení provozu být překážkou pro výplatu pojistného plnění z případné škody. Pouze snad samotné pojištění kybernetických hrozeb, které má mnoho svých výluk, by mohlo mít vliv i na plnění z přerušení provozu. Na to je třeba si dávat pozor, stejně tak na výluky vztahující se k majetkovému pojištění.

Allianz pojišťovna, a.s.

Obecná specifikace produktu:

AZP má ve své nabídce dva samostatné produkty pro podnikatele, které oba zahrnují pojištění přerušení provozu, jeden starší a druhý novější. Starší produkt se řídí souborem pojistných podmínek, které byly vydány 1. 12. 2018 a skládají se ze všeobecných pojistných podmínek s označením VPP-P 1/17, několika zvláštních pojistných podmínek a doplňkových pojistných podmínek. Přerušení provozu konkrétně řeší zvláštní pojistné podmínky pro pojištění majetku podnikatelů s označením ZPP-MP 1/17. Ostatní zvláštní pojistné podmínky nejsou pro pojištění přerušení provozu relevantní. Dle webových stránek se jedná o pojištění přerušení provozu v důsledku pojistné události, které se vztahuje na ušlý zisk, náklady na opatření na zkrácení doby přerušení provozu, náklady na pronájem náhradních prostor a prostředků, a stálé provozní náklady. Webové stránky AZP dávají také základní přehled pojistných nebezpečí, na která se pojištění přerušení provozu vztahuje. Jedná se o požár a související nebezpečí, živel, voda z vodovodního zařízení, ostatní pojistná nebezpečí a krádež vloupáním. Podrobnější vysvětlení, co vše například patří pod „ostatní nebezpečí“, je součástí pojistných podmínek, které jsou zkoumány podrobněji níže.

Druhý, novější produkt s obchodním názvem *„Moje firma”*, byl vydán v roce 2021. Podnik si dle něj může sjednat pojištění v několika různých variantách (tzv. balíčcích), které se liší nejen názvem, ale i svým rozsahem krytí. Pojištění přerušení provozu obsahují všechny

varianty (Komfort, Plus, Extra a Max), kdy na rozsah krytí škod z přerušení provozu má vliv sjednaná varianta. Na svých webových stránkách pojišťovna píše, že uhradí ušlý zisk, stálé náklady (např. na mzdy) a vícenáklady (např. náklady na zmírnění následků pojistné události, na pronájem náhradních prostor apod.). Nejvyšší varianta, označená jako „Max“, dle webových stránek kryje základní rizika (blíže specifikovaná viz dále), přírodní události, vodovodní škody, krádež a loupež, vandalismus, odpovědnost, skla, rozbití strojů a elektroniky, různé druhy asistencí, přerušení provozu a volitelně také zemětřesení.

Pojištěná rizika:

U staršího produktu zvláštní pojistné podmínky ZPP-MP 1/17 stanovují, že pojištění přerušení provozu se vztahuje pouze na ta pojistná nebezpečí, která jsou ve stejné pojistné smlouvě ujednána pro majetek sloužící k provozované činnosti. Pojištění majetku lze sjednat proti následujícím rizikům: požár a jeho průvodní jevy, výbuch, úder blesku, zřícení letadla, voda z vodovodního zařízení, povodeň, záplava, vichřice, krupobití, zemětřesení, sesuv půdy, lavina, tíha sněhu, náraz vozidla, kouř, rázová vlna, pád stromů, stožárů a jiných věcí, krádež vloupáním, vandalismus, a škody způsobené sprinklerovým hasicím zařízením. Lze předpokládat, že pro všechna uvedená rizika lze sjednat i přerušení provozu. V případě staršího produktu jedinou příčinou přerušení nebo omezení provozu může být škoda na pojištěné věci. Pouze pokud je v pojistné smlouvě ujednáno, vztahuje se pojištění přerušení provozu i na jiná pojistná nebezpečí, pojišťovna je ale dále nespecifikuje (zřejmě jen na přímý dotaz).

V případě nového produktu je rozsah pojištěných rizik rozšířen pouze o riziko atmosférických srážek, ale jinak nenabízí žádná nová rizika jako například kybernetické hrozby. Stejně tak není v rámci nového produktu nabízeno ani přerušení provozu z důvodu úředního zásahu.

Rozsah krytí:

Starší produkt se ujednává na pojistnou částku, která se ujednává na pojistný rok, a také se ujednává doba odškodnění, která může být maximálně 12 měsíců. Pokud si podnik sjedná jen základní pojištění přerušení provozu, to se ujednává na roční limit plnění, kde maximální doba odškodnění činí jen 3 měsíce. Podmínky definují dobu odškodnění jako časové období ujednané v pojistné smlouvě, na které se pojištění přerušení provozu vztahuje. Pojištění kryje vynaložené náklady na opatření směřující ke zkrácení doby přerušení (popř. omezení) provozu, či zmírnění jejich následků. Mezi další hrazené náklady spadají také náklady na pronájem náhradních prostor, náklady nezbytné pro realizaci pojištěné činnosti po dobu přerušení (popř. omezení) provozu, použití náhradních prostředků apod. Pojišťovna hradí i náklady na opatření potřebná k informování klientů, pokud musely být vynaloženy v souvislosti s přerušením provozu v podniku pojištěného. Zde je potřeba ale upozornit, že vícenáklady uhradí pojišťovna maximálně do výše 5% celkové pojistné částky nebo celkového limitu pojistného plnění z pojištění přerušení provozu.

Dále platí, že pojištění přerušení provozu se vztahuje pouze na majetek sloužící k provozování podnikatelské činnosti pojištěného, pro který je ve stejné pojistné smlouvě ujednáno pojištění (věcí movitých nebo/a pojištění budov a vedlejších staveb). Pouze pokud je v pojistné smlouvě ujednáno, vztahuje se pojištění přerušení provozu i na jiný majetek sloužící k provozované činnosti. Převedením do praktického příkladu, pokud má podnik pojištěny pouze movité věci, dojde k požáru, který ale poškodí jen budovu, pak případné přerušení provozu není kryto z pojištění.

V případě **nového produktu** je rozsah krytí téměř totožný jako u starého produktu. Ve stručnosti, i zde pojišťovna hradí ušlý zisk, stálé náklady a účelně vynaložené vícenáklady.

Stejně tak platí základní princip, že aby bylo možné uhradit škodu z přerušení provozu, musí dojít ke škodě na pojištěném majetku, a z pojištěného rizika. Doba, za kterou pojišťovna vyplatí pojistné plnění, je maximálně 90 dní. I zde platí, že pokud je doba přerušení provozu kratší než 90 dní, vyplatí jen poměrnou část. Pojištění se sjednává na limit plnění, a nikoliv pojistnou částku, u které pojišťovna může uplatnit případné podpojištění. Pojistné podmínky neuvádí žádné dílčí limity např. na vícenáklady, jako to bylo u staršího produktu. Rozdílné oproti staršímu produktu je, že v případě přerušení provozu pojišťovna uhradí škodu, jen pokud bude **doba přerušení provozu delší než 3 dny**. Jinak řečeno, jedná se také o tzv. časovou spoluúčast, kterou používá např. Kooperativa, a.s., Vienna Insurance Group.

Podmínky pojištění a povinnosti pojištěného:

U staršího produktu je pojištěný povinen bezodkladně oznámit pojišťovně vznik škody na věci, která má nebo může mít za následek vznik následné škody (přerušení provozu), a vyžádat si pokyny pojistitele ohledně dalšího postupu. Také je pojištěný povinen vést písemnou evidenci o přerušení provozu, která bude obsahovat údaje nezbytné pro prokázání výše následné škody a době trvání přerušení nebo omezení provozu. Také v případě nového produktu je pojištěný povinen vést písemnou evidenci o přerušení provozu. Tato evidence musí obsahovat údaje, kterými pojištěný prokážete výši následné škody a dobu přerušení provozu. Podmínky pojištění a povinnosti pojištěného jsou v obou produktech velmi podobné.

Výluky z pojištění:

Pojištění přerušení (popř. omezení) provozu a vícenákladů se u staršího produktu nevztahuje na náklady, které vzniknou v důsledku úředně nařízených opatření, která omezují obnovu a provoz podniku, nebo tím, že pojištěný nezajistí včas obnovu nebo opětovné pořízení zničeného nebo poškozeného majetku (např. z důvodu nedostatku finančních prostředků). Pojištění se nevztahuje ani na náklady, které vzniknou po ukončení pojištění. Shodně je to uvedeno i v novém produktu, kde je navíc uvedeno, že se nehradí přerušení provozu v důsledku přerušení dodávky vody, plynu, elektrické energie a dalších médií.

Další části pojistných podmínek, na které je třeba si dát také pozor:

U staršího produktu platí, že pokud je doba přerušení nebo omezení provozu kratší než ujednaná doba odškodnění, stanoví se maximální výše pojistného plnění ve stejném poměru k pojistné částce pro přerušení provozu, v jakém je doba přerušení nebo omezení k ujednané době odškodnění. Také je pojišťovna oprávněna přiměřeně snížit pojistné plnění o případné ekonomické výhody, které vzniknou pojištěnému během doby odškodnění jako následek přerušení nebo omezení provozu. Stejným způsobem je to popsáno i v novém produktu, kde je ale navíc uvedeno, že ušlý zisk pojišťovna neuhradí, pokud vyplývá z finančních operací, finančních služeb nebo obchodování s nemovitostmi.

Starší produkt nabízí možnost sjednání na pojistnou částku nebo limit plnění. Pokud je přerušení provozu sjednáno na pojistnou částku, pojišťovna má právo uplatnit podpojištění je-li pojistná částka v době pojistné události nižší než pojistná hodnota přerušení provozu. Pojišťovna má v podmínkách nastavenou toleranci 15 %, nicméně podnik by si přesto měl správně zvolit pojistnou částku, aby se vyhnul krácení pojistného plnění.

Hodnocení produktu:

Oba z nabízených produktů od AZP lze (stejně jako v případě GČP) považovat za velmi tradiční, jelikož neobsahují krytí přerušení provozu z důvodu kybernetické hrozby, ani úředního zásahu, což lze považovat za jejich nevýhodu. Pro oba produkty platí, že rozhodujícím faktorem pro sjednání daného pojištění bude jeho cena. Starší produkt v případě

sjednání na pojistnou částku má i další nevýhodu v případném uplatnění podpojištění, a to z následujícího důvodu. I kdyby podnik na začátku správně nastavil pojistnou částku, není zaručeno, že bude správně nastavená po celou dobu pojištění. Podnikatelské prostředí se dynamicky mění, mění se v čase zisk i náklady, které v poslední době rapidně rostou. Navíc podnik ani tak nemusí mít stálé cashflow vzhledem k typu provozu. Nevýhodou u nového produktu je sjednání časové spoluúčasti, kdy malé škody toto pojištění nekryje.

ČSOB Pojišťovna, a.s., člen holdingu ČSOB

ČSOB Pojišťovna, a.s., člen holdingu ČSOB (dále jen ČSOBP) nabízí podnikatelské pojištění nejen pro živnostníky a menší podniky, ale také pro velké podniky a korporace. O daném pojištění na svých webových stránkách píše jako o komplexním pojištění, které umí pojistit téměř cokoliv včetně pojištění přerušení provozu, které pak dělí na živelní a strojní.

Obecná specifikace produktu:

Pojištění živelního přerušení provozu se řídí dle všeobecných pojistných podmínek – zvláštní část s označením CPP ZPP 2014, a pro strojní přerušení provozu byly vydány všeobecné pojistné podmínky – zvláštní část s označením VPP SPP 2014. Oboje podmínky navazují na všeobecné pojistné podmínky – obecná část s označením VPP OC 2014.

Pojištěná rizika:

Pojištění **živelního** přerušení provozu lze sjednat v základním rozsahu pro rizika požár, výbuch, úder blesku, náraz nebo zřícení pilotovaného letícího tělesa, jeho části nebo nákladu. Uvedený výčet rizik je klasické pojištění FLEXA. Navíc k tomu lze sjednat pojištění i pro další rizika jako je vichřice, krupobití, sesouvání půdy, zřícení skal nebo zemin, lavina, pád stromů, stožárů a jiných předmětů, zemětřesení, tíha sněhu nebo tíha námrazy, náraz vozidla, kouř, nadzvuková vlna (aerodynamický třesk), povodeň, záplava, vodovodní škoda, odcizení a vandalismus. ČSOBP v pojistných podmínkách upřesňuje, že za pojištěné riziko považuje také poškození, zničení nebo pohřešování věci sloužící provozu pojištěného způsobené bouracími, záchrannými či odklízecími pracemi, pokud tyto práce byly realizovány v důsledku pojistných nebezpečí, proti jejichž negativnímu působení bylo pojištění sjednáno. To vše pouze v důsledku věcné škody (poškození, zničení nebo pohřešování věci sloužící provozu pojištěného). Jinak řečeno, pojištění živelního přerušení provozu nekryje situace, kdy k přerušení provozu dojde z důvodu úředního zásahu, pandemie, apod.

Pojištění **strojního** přerušení provozu se sjednává pro případ přerušení nebo omezení provozu z důvodu věcné škody (poškození, zničení nebo pohřešování strojů sloužících provozu) jakoukoliv nahodilou událostí, která není dle pojistných podmínek vyloučena. Ani zde tedy nejsou kryty situace, kdy k přerušení provozu dojde z důvodu úředního zásahu, pandemie, apod. Velmi důležité pro strojní přerušení provozu bude právě výčet výluk.

Rozsah krytí:

Pojištění **živelního** přerušení provozu se vztahuje na finanční ztráty, kterou je myšleno ušlý zisk a stálé náklady. Ušlým ziskem se rozumí zisk vzniklý z realizace výrobní, obchodní, případně jiné činnosti, kterého by pojištěný dosáhl za dobu nepřerušení nebo neomezení provozu. Stálými náklady se rozumí náklady pojištěného, které musí pojištěný bezpodmínečně vynakládat během doby trvání přerušení nebo omezení provozu, aby bylo možné následně co nejdříve obnovit postižený provoz v původním rozsahu. Pokud bylo sjednáno pojištění stálých nákladů, vzniká pojištěnému právo na plnění také za vícenáklady. Vícenáklady se rozumí zvýšené náklady na náhradní zajištění provozu účelně vynaložené

pojištěným, nikoliv na obnovení v důsledku věcné škody přerušeného nebo omezeného provozu, ale na částečné či úplné nahrazení v důsledku věcné škody přerušeného nebo omezeného provozu provozem náhradním realizovaným ekonomicky a technicky nejefektivnějším možným způsobem (např. přesunem činnosti pojištěného do jiných jeho výrobních prostor, nájmem náhradních srovnatelných výrobních prostor, strojů a zařízení outsourcingem činnosti pojištěného, apod.). Pokud jsou sjednány vícenáklady, ty se hradí pouze do ročního limitu pojistného plnění ve výši 5 % z pojistné částky. Avšak vícenáklady jsou hrazeny nad rámec sjednané pojistné částky. Pokud je ušlým ziskem ušlé nájemné, pojišťovna vždy snižuje plnění o částku na údržbu stavby, která je ve výši 10 % ušlého nájemného. Také u ČSOBP je stanovena doba ručení, po kterou pojišťovna hradí finanční ztrátu. Pojistné podmínky ji stanovují na 12 měsíců, ale ve smlouvě lze ujednat i jiná. Pojistné podmínky stanovují i časovou spoluúčast pojištěného v rozsahu 2 dnů, které lze ve smlouvě ujednat odlišně. Znamená to, že pokud doba přerušení provozu nepřesáhne 2 dny, pojišťovna za ně nevyplatí pojistné plnění. Pokud bude přerušení provozu trvat celkem 4 dny, pojišťovna uhradí pouze 2 dny. Pojišťovna pro časovou spoluúčast používá vlastní výraz *„odčetná spoluúčast“*. ČSOBP v pojistných podmínkách dále stanovuje hranici pro uplatnění podpojištění ve výši 15 % rozdílu mezi pojistnou částku pojistnou hodnotou.

Také pojištění **strojního** přerušení provozu se vztahuje na finanční ztráty, kterou je myšleno ušlý zisk a stálé náklady. Jejich definice, včetně definice pro vícenáklady, je totožná jako u živelního přerušení provozu. Shodná je také horní hranice plnění u vícenákladů, časová spoluúčast 2 dny, a pravidla pro uplatnění podpojištění. Ušlý zisk v podobě ušlého nájemného není v podmínkách řešen, zřejmě není pro tento druh pojištění relevantní. Rozdílná je však doba ručení, která u strojního přerušení provozu činí jen 3 měsíce. Ve smlouvě dobu ručení lze sjednat odlišně. Velmi podstatné je vědět, že k finanční ztrátě musí dojít v důsledku věcné škody na stroji, který **je uveden v pojistné smlouvě v seznamu strojů**. Podnik by si měl proto udělat přesný seznam strojů, a v případě nákupu nového stroje v průběhu pojištění oznámit pojišťovně tuto změnu. Samozřejmě platí, že stroj byl v okamžiku uzavření pojistné smlouvy nepoškozen a v provozuschopném stavu nebo byl připraven k předání do trvalého provozu (došlo k úspěšnému zakončení testovacího období).

Podmínky pojištění a povinnosti pojištěného:

Všeobecné podmínky pojištění – obecná část VPP OC 2014 definují skutečně obecné povinnosti pojištěného, které v pojistných podmínkách bývají standardem, jsou logické a pro pojištěného nejsou nijak překvapující. Další povinnosti pojištěného jsou pak definovány zvlášť pro živelní přerušení provozu a zvlášť pro strojní přerušení provozu. A právě některé z nich je potřeba více hlídat.

U **živelního** přerušení provozu je pojištěný povinen pojišťovně oznámit vznik škody nejpozději do pěti dnů od jejího vzniku. Dále je povinen ukládat inventury, bilance a výsledky hospodaření za poslední předcházející dva hospodářské roky ve dvou vyhotoveních bezpečně a vzájemně odděleně na ochranu proti současnému zničení. A v neposlední řadě je pojištěný povinen informovat pojišťovnu o všech zamýšlených krocích pro částečné nebo plné obnovení provozu, všechny kroky konzultovat a postupovat v souladu s pokyny pojišťovny. Jinak řečeno nárok na pojistné plnění nelze uplatnit zpětně, a pouze s předložením celkového účtu za přerušení provozu.

V případě **strojního** přerušení provozu je pojištěný navíc povinen dodržovat technické a další normy vztahující se na provoz a údržbu strojů, a vést průkaznou dokumentaci jejich provozu (provozní deník). Každý stroj také musí splňovat technické normy a obecně závazné právní předpisy pro provozování a užívání v místě pojištění, pojištěný je povinen zabezpečit obsluhu strojů osobami s předepsanou kvalifikací a oprávněním. Pojištěný musí také dbát na to, aby

stroje byly v dobrém technickém stavu, aby byly řádně udržovány a nedocházelo k jejich záměrnému přetěžování nad technicky přípustnou mez stanovenou výrobcem, zajistit, aby stroje, včetně elektroinstalace, byly instalovány oprávněnou osobou s předepsanou kvalifikací a oprávněním či povolením, a zajistit, aby na nich byly oprávněnou osobou prováděny prohlídky, revize a povinná údržba, které stanoví výrobce a příslušné technické normy. K tomu všemu je pojištěný povinen zabezpečit pravidelnou kontrolu (minimálně jednou za 48 hodin) řádné pracovní činnosti strojů pracujících automaticky bez lidské obsluhy. Jinak řečeno, pojištěný musí dodržet všechna preventivní opatření, v opačném případě pojišťovna vzniklou škodu neuhradí.

Výluky z pojištění:

Výluky pro oba produkty přerušení provozu jsou velmi obsáhlé. V případě **živelního** přerušení provozu se převážně jedná buď o výluky, které nějakým způsobem upřesňují definice pojistných nebezpečí, nebo vylučují situace, které ani živelním rizikem nejsou. Jako příklad první kategorie výluk lze uvést třeba výluku na škody způsobené vodou při mytí, sprchování nebo vodou stříkající z kropicích, mycích, zavlažovacích nebo obdobných zařízení. Tato výluka upřesňuje definici vodovodních škod. Podobně je upřesněna i definice rizika požáru, výbuchu, vichřice, krupobití, zemětřesení, odcizení, vandalismu či atmosférických srážek. Obecně tento druh výluk snižuje okruh situací, které mohou nastat a způsobit přerušení provozu. Avšak některá upřesnění rizik, jako například upřesnění rizika atmosférických srážek, může být pro podnik velkým překvapením. Pojistné podmínky vylučují škody vzniklé působením normálních atmosférických podmínek, se kterými je třeba podle ročního období a místních poměrů počítat. To může i znamenat, že v případě větších jarních přeháněk pojišťovna nebude škodu hradit. Nebo pak upřesnění vandalismu, kdy podmínky vylučují škody vzniklé jakýmkoliv znečištěním, zabarvením, kresbami, nápisy apod. V případě podniku XYZ to nutně nemusí být kritická výluka, ale u jiných typů provozu být může.

Do druhé kategorie patří například výluka na škody vzniklé v důsledku nesprávné údržby, nekvalifikované obsluhy, opotřebení, vady projektu, chyby vzniklé programovým vybavením nebo nedodržením technologického postupu. Znamená to, že pokud třeba dojde k požáru v důsledku nesprávné údržby, pojišťovna nemusí vyplatit pojistné plnění. Pojišťovna také specifikuje náklady, které z přerušení provozu nebude hradit, jako jsou výdaje za suroviny, materiál, technologickou energii a za odebrané zboží, pokud se nejedná o výdaje na udržování provozu, odvodové a daňové povinnosti a vývozní cla, odpisy hmotného a nehmotného majetku, který byl v důsledku věcné škody zničen nebo pohřešován, dopravné, náklady spojů, pokud se nejedná o výdaje na udržování provozu, pojistné závislé na obratu, licenční a vynálezecké poplatky závislé na obratu, zisky a stálé náklady, které nesouvisejí s výrobním, obchodním nebo průmyslovým provozem (např. z kapitálových nebo pozemkových obchodů, z prodeje majetku, apod.), majetkové sankce (např. penále, pokuty a náhrady škod), které je pojištěný povinen zaplatit v důsledku nesplnění, popř. porušení svých právních povinností.

Podmínky pro živelní přerušení provozu samozřejmě obsahují i výluky na finanční ztráty způsobené vlivy a událostmi nesouvisejícími se vznikem věcné škody, dále pak tím, že pojištěný nevyvinul plné úsilí pro urychlenou obnovu provozu, že nezajistil včas obnovu nebo opětovné pořízení zničených, poškozených, pohřešovaných nebo odcizených věcí sloužících provozu nebo k tomu nezabezpečil včas dostatek finančních prostředků. Podobně pojišťovna nebude hradit finanční ztráty způsobené tím, že došlo k rekonstrukci (např. inovaci, přestavbě) zničených nebo poškozených věcí sloužících provozu v širším rozsahu, než v jakém sloužily provozu v době vzniku věcné škody. Tyto výluky lze považovat za poměrně logické.

U **strojního** přerušení provozu existuje několik specifických výluk pro stroje, které však mohou být někdy sporné, a umožnují pojišťovně odmítnout mnoho škod. Jedná se o výluku na finanční ztráty vzniklé v důsledku trvalého vlivu provozu, opotřebení, koroze, eroze, kavitace, postupného stárnutí, únavy materiálu, nedostatečného používání, a dlouhodobého uskladnění. Stejně tak pojišťovna vylučuje finanční ztráty v důsledku škod na strojních součástech pro kluzná a valivá uložení pro přímočarý i rotační pohyb (např. ložiska, písty, vložky válců), na součástech nebo příslušenství stroje, které se pravidelně vyměňují při změně pracovního úkonu nebo proto, že podléhají rychlému opotřebení (např. formy, matrice, razidla, ryté a vzorkované válce, řezné nástroje), na součástech nebo příslušenství stroje, kterými jsou hadice, těsnění, pásy, pneumatiky, řemeny, lamely, lana, řetězy, žáruvzdorné vyzdívky a obložení, trysky hořáků, drticí nástroje drticích strojů, součásti ze skla, na činných médiích a provozních kapalinách (např. paliva, chladiva, filtrační hmoty, chemikálie), na nosičích záznamu, snímacích a záznamových prvcích, na záznamech zvukových, obrazových, datových a jiných včetně softwarového vybavení, na základech, rámech, ukotveních a podstavcích strojů, pokud nejsou součástí stroje. Do stejné kategorie ještě patří také přímé dlouhodobé vlivy biologických, chemických nebo tepelných procesů nebo znečištění. Nelze příliš odhadnout jak často, a v jakých případech pojišťovna bude tyto výluky uplatňovat. Nicméně **podmínky dávají pojišťovně poměrně široký prostor neposkytnout pojistné plnění**. Vyloučeny jsou také škody, které mají být uplatněny z živelního či kybernetického pojištění přerušení provozu. Produkty se tedy vzájemně doplňují. A vyloučeny jsou také vybrané druhy finančních ztrát, které jsou téměř totožné jako u živelního přerušení provozu.

Další části pojistných podmínek, na které je třeba si dát také pozor:

V případě živelního přerušení provozu by si podnik měl dávat pozor zejména na jednu konkrétní výluku. Tou je, že za věcnou škodu se nepovažují škody spočívající v tom, že jsou zničeny, poškozeny, nebo pohřešovány věci zvláštní hodnoty, cennosti, **záznamy zvukové, obrazové, datové a jiné, včetně softwarového vybavení, spisy a listiny všeho druhu**. Pro podnik to znamená, že by měl vyjmenované věci uchovávat na velmi bezpečném místě, a v případě záznamů a listin je mít i zálohované, ve více kopiích apod.

Hodnocení produktu:

Živelní přerušení provozu lze považovat za klasický produkt pojištění s celkem očekávatelným rozsahem krytí, podmínkami a výlukami. U tohoto pojištění bude rozhodující hlavně jeho cena. To stejné však nelze říct o strojním přerušení provozu, zejména z pohledu výluk, které jsou nejen obsáhlé, ale dávají pojišťovně možnost odmítnout velké množství potenciálních škod. Tento produkt spíše nelze podniku doporučit, pouze za předpokladu, že podnik disponuje novějšími stroji, které jsou v dobrém technickém stavu, nejsou přetěžované, a je u nich prováděna pravidelná údržba. I zde samozřejmě bude důležitá cena pojištění.

Česká podnikatelská pojišťovna a.s., Vienna Insurance Group

Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group (dále jen ČPP) se na svých webových stránkách chlubí, že je pojišťovnou roku, pojištění pro podnikatele umí, a dodává *„Letos slavíme zlato a bronz v soutěži Zlatá koruna“*. ČPP nabízí pojistnou ochranu nejen pro malé podnikatele a střední podniky (do 100 mil. Kč), ale také pro ty velké a průmysl. Portfolio ČPP mimo jiné obsahuje i produkty jako finanční způsobilost dopravce, stavebně montážní pojištění, pojištění úpadku cestovní kanceláře, či dokonce pojištění proti terorismu pro podnikatele a subjekty veřejné správy. Podnikatelům pojišťovna nabízí možnost sjednání individuálního pojištění, ve kterém si podnik sám přesně určí rozsah pojištění, který bude zohledňovat specifika daného podniku, alespoň tak to na svém webu píše pojišťovna. ČPP má

ve své nabídce celkem tři druhy pojištění pro přerušení provozu. Tím prvním je klasické živelní přerušení provozu, které se řídí dle doplňkových pojistných podmínek s označením DPPŠP MP 1/16. Druhé, spíše ojedinělé pojištění, je kontingentní pojištění přerušení provozu, které se vztahuje na finanční ztráty v důsledku zastavení výroby v důsledku působení pojistného nebezpečí na straně dodavatele podniku. Tento druh pojištění je nabízen pouze v nejvyšším balíčku pojištění na míru. Nicméně ani po důkladném prohledání webových stránek ČPP, a zveřejněných dokumentů, nebylo možné získat k tomuto pojištění více informací. Pravděpodobně se jedná o pojištění pouze na dotaz. A jako třetí má pojišťovna v nabídce pojištění strojního přerušení provozu, které se řídí podmínkami s označením ZPPŠST MP 1/16, a ve kterém je navíc zahrnuta také elektronika. Kromě doplňkových pojistných podmínek příslušných druhů přerušení provozu, se pojištění řídí také dokumentem Všeobecné pojistné podmínky pro pojištění majetku s označením VPPM 1/16, jež upravuje obecné podmínky pojištění.

Jak již jednou bylo uvedeno, ČPP patří do stejné pojišťovací skupiny jako Kooperativa pojišťovna, a.s., Vienna Insurance Group (dále jen KOOP), což se může projevit jednak na obdobném produktovém portfoliu, ale zejména na podobnosti pojistných podmínek. Nemá příliš přínos a smysl znovu opakovat stejná ustanovení pojistných podmínek, a proto bude kladen větší důraz na to, co ČPP, pojišťovna roku, nabízí lepšího a rozdílně oproti jiným pojišťovnám. Zejména pak, zda nabízí krytí aktuálních rizik, která jsou předmětem této práce.

Produkt **živelní** přerušení provozu nabízí krytí pro běžný výčet živelních rizik, a nejedná se o komplexní produkt jako v případě KOOP, který obsahuje pojištění úředního zásahu. ČPP naopak přímo vylučuje finanční ztráty způsobené úředně nařízenými omezeními pro obnovení provozu. Rozsah krytí živelného přerušení provozu je omezen (podobně jako u produktů jiných pojišťoven) dobou ručení 12 měsíců, a časovou spoluúčastí 2 dnů. Většina výluk je obdobných jako u jiných pojišťoven, stejně tak podmínky pojištění a povinnosti pojištěného. Některé výluky jsou však odlišné oproti jiným pojišťovnám, zejména pak výluka vztahující se k riziku povodně. Pojišťovna v podmínkách uvádí, že nebude hradit škody v důsledku povodně, při které nebylo v místě pojištění, které není v pojistné smlouvě přesně specifikováno, dosaženo 10letého maximálního průtoku, tj. průtoku, který je dosažen nebo překročen průměrně jedenkrát za deset let (tzv. 10letá voda), a v důsledku povodně, záplavy na silnicích, mostech, cestách, opěrných zdech, veřejném osvětlení a dopravním značením. Další velmi zajímavou výlukou je výluka na škody v přímém či nepřímém důsledku jakéhokoliv nakládání či manipulací s výbušninami nebo s jakýmikoliv věcmi, jež výbušninu obsahují. V obou případech se jedná o velmi netypické výluky.

Strojní přerušení provozu se přímo váže na Doplňkové pojistné podmínky pro pojištění strojů a elektroniky DPPSE MP 1/16. Na první pohled by se mohlo zdát, že podmínky pro strojní přerušení provozu neobsahují natolik přísné podmínky jako v případě ČSOB Pojišťovny, a.s., člen holdingu ČSOB, která v nich výslovně vylučuje finanční ztráty způsobené opotřebením stroje, únavou materiálu, koroze, apod. Ale není tomu tak. Také v podmínkách ČPP je výluka na běžné nebo předčasné opotřebení a únavu materiálu. Výluka je totiž součástí pojištění strojů a elektroniky, nikoliv podmínek pro strojní přerušení provozu.

Hodnocení produktu:

Produkty od ČPP lze považovat spíše za klasická pojištění přerušení provozu. V nabídce zcela chybí pojištění přerušení v důsledku kybernetického incidentu, úředního zásahu, či pandemie. Celkově podmínky obsahují méně výluk a méně povinností pojištěného, jsou tak pro podnik více pro klientské. Neobsahují žádná zvlášť překvapivá ustanovení, a podmínky jsou relativně

stručné. Velmi záleží na konkrétní nabídce a ceně pojištění, avšak rozhodně se nejedná o komplexní pojištění přerušení provozu, a z pohledu zkoumaných rizik je pojištění spíše nevyhovující.

3.1.3 Pojištění přírodních rizik

Jak již vyplynulo nejen z teoretické části práce, ale také z rozboru pojistných podmínek, pojištění přírodních rizik bývá nabízeno v rámci živelního pojištění, které navíc obsahuje také základní rizika, jakou je požár, výbuch, pád letadla, jeho části nebo nákladu. Nicméně předmětem zkoumání jsou čistě přírodní rizika, kterými jsou vichřice, krupobití, úder blesku, povodeň, záplava, zemětřesení, atmosférické srážky, sesuv půdy, zřícení skal nebo zemin, pád lavin, a tíha nebo tlak sněhu. Pojištění přírodních nebezpečí je tradičním pojištěním, rozhodně není ničím novým, a lze předpokládat, že všechny ze zkoumaných pojišťoven toto pojištění nabízí. Pro účely práce bude nejprve nutné zjistit, zda tomu tak opravdu je, a zda mezi pojišťovnami a jejich produkty existují významné rozdíly, které mohou mít vliv na to, zda pojistit či nikoliv. Nabídku zkoumaných pojišťoven, která vychází ze srovnání jejich pojistných podmínek je přehledně v tabulce 1.

Tabulka 1 Nabídka pojištění přírodních rizik u zkoumaných pojišťoven

Riziko/Pojišťovna	GČP	KOOP	AZP	ČSOBP	ČPP
Vichřice	Ano	Ano	Ano	Ano	Ano
Krupobití	Ano	Ano	Ano	Ano	Ano
Úder blesku	Ano	Ano	Ano	Ano	Ano
Povodeň	Ano	Ano	Ano	Ano	Ano
Záplava	Ano	Ano	Ano	Ano	Ano
Zemětřesení	Ano	Ano	Ano	Ano	Ano
Atmosférické srážky	Ne	Ne	Ano	Ne	Ne
Sesuv půdy	Ano	Ano	Ano	Ano	Ano
Zřícení skal nebo zemin	Ano	Ano	Ano	Ano	Ano
Sesuv a pád lavin	Ano	Ano	Ano	Ano	Ano
Tíha nebo tlak sněhu	Ano	Ano	Ano	Ano	Ano

Zdroj: vlastní zpracování (2022)

Z tabulky je patrné, že nabídka pojišťoven je téměř shodná, ale až na jednu výjimku. Tou výjimkou je pojištění atmosférických srážek, které jako jediná nabízí Allianz pojišťovna a.s. (dále jen AZP).

Kromě samotného výčtu pojištěných rizik může být rozdíl v definici rizik, limitech plnění, spoluúčasti, či jiných podmínkách a povinnostech.

Vichřice

Generali Česká pojišťovna, a.s. (dále jen GČP) definuje vichřici jako dynamické působení hmoty vzduchu, která se pohybuje rychlostí 20,8 m/s (75 km/h) a vyšší. Není-li rychlost pohybu vzduchu v místě pojištění zjistitelná, poskytne pojišťovna pojistné plnění, pokud oprávněná osoba prokáže, že pohyb vzduchu v okolí místa pojištění způsobil obdobné škody na řádně udržovaných stavbách nebo shodně odolných jiných věcech nebo že škoda při bezvadném stavu stavby nebo jiné věci mohla vzniknout pouze v důsledku vichřice. Obdobnou definici používají i ostatní pojišťovny. Kooperativa pojišťovna, a.s., Vienna Insurance Group (dále jen KOOP) se oproti ostatním pojišťovnám odlišuje, konkrétně přidává

navíc následující podmínku. Vznikne-li škodná událost následkem vichřice nebo v přímé souvislosti s vichřicí do 10 dnů po sjednání pojištění, není pojistitel z této škodné události povinen poskytnout pojistné plnění.

Krupobití

GČP krupobitím rozumí jev, při kterém kousky ledu různého tvaru, velikosti, hmotnosti a hustoty vytvořené v atmosféře dopadají na předmět pojištění. Za poškození nebo zničení předmětu pojištění krupobitím se považuje takové poškození nebo zničení předmětu pojištění, k němuž došlo buď přímým působením krupobití, nebo v příčinné souvislosti s tím, že krupobití poškodilo dosud bezvadné a funkční části stavby. ČSOB Pojišťovna, a.s., člen holdingu ČSOB (dále jen ČSOBP) a Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group (dále jen ČPP) používají téměř shodnou definici. KOOP využívá podstatně stručnější definici, ve svém základním významu ale shodnou s GČP. AZP nevysvětluje naopak krupobití vůbec, zřejmě se spoléhá na obecné povědomí o tomto přírodním jevu. Žádná z pojišťoven nepřidává k riziku žádné zvláštní podmínky, povinnosti, či výluky.

Úder blesku

Přestože některé z vybraných pojišťoven používají název rizika *„Přímý úder blesku“* a některé jen *„Úder blesku“*, všechny používají významově shodnou definici. GČP, která užívá první variantu, definuje přímý úder blesku jako přímý zásah blesku (atmosférického výboje) do předmětu pojištění nebo do budovy, v níž se předmět pojištění nacházel a aby vzniklo právo na pojistné plnění, musí být místo přímého úderu blesku do předmětu pojištění nebo do budovy spolehlivě zjištěno podle tepelně mechanických stop. AZP užívá název rizika „Úder blesku“, jež definuje jako přímý zásah blesku, při němž proud blesku prochází pojištěným majetkem a zanechá na něm prokazatelně viditelné stopy. Všechny pojišťovna tak vylučují škody způsobené přepětí v elektrorozvodné nebo komunikační síti, k němuž došlo v důsledku působení blesku na tato vedení (mimo místo pojištění). Pro krytí škod, které způsobí přepětí, je nutné mít pojištění elektroniky, někdy nazývané jako pojištění elektro či přepětí.

Povodeň

AZP za povodeň považuje zaplavení místa pojištění vodou, která vystoupila z břehů vodního toku nebo vodního díla následkem přírodních jevů (např. deště, tání, posunu ledu), či příval vody způsobený poruchou vodního díla (např. protržená hráz přehrady). V principu tuto definici používají i ostatní vybrané pojišťovny.

GČP k definici automaticky přidává navíc také vystoupnutí vody do budovy z kanalizační sítě v důsledku vzniklé povodně v blízkosti místa pojištění, a to na principu spojených nádob s korytem řeky či vodní nádrže. KOOP nepřímo zahrnuje vystoupnutí vody z kanalizace do definice povodně, a u rizika vodovodních škod je explicitně vylučuje, pokud se jedná o důsledek povodně. ČSOBP vystoupnutí vody z kanalizace v souvislosti s povodní nabízí jen formou volitelného připojištění, a AZP má schované vystoupnutí z kanalizace (z jakékoliv příčiny, nejen povodně) v rámci pojištění vodovodních škod, a v rámci rizika povodně přímo vylučuje škody způsobené vystoupnutím vody z odpadního potrubí. ČPP v podmínkách vystoupnutí vody z kanalizace vůbec nezmiňuje, a pravděpodobně jej vůbec nehradí.

Kromě ČSOBP všechny vybrané pojišťovny vylučují škody způsobené povodní, které vznikly do 10 dnů od sjednání pojištění. KOOP ukládá pojištěnému povinnost uložit na pevný podklad o výšce min. 15 cm nad úrovní podlahy zásoby a cizí předměty, které jsou umístěné v podlažích, kde je podlaha pod úrovní okolního terénu. ČPP vylučuje škody v důsledku

povodně, při které nebylo v místě pojištění, které není v pojistné smlouvě přesně specifikováno, dosaženo 10letého maximálního průtoku, tj. průtoku, který je dosažen nebo překročen průměrně jedenkrát za deset let (tzv. 10letá voda). Není zcela jasné, co tím ČPP má přesně na mysli. Avšak velmi pravděpodobně vylučuje škody v oblastech, které jsou zasaženy povodní v intervalu menším než 10 let. AZP to definuje mnohem přesněji, kdy v pojistných podmínkách uvádí, že pojištění proti povodni se nevztahuje na škody způsobené v oblastech, které podle aktuálních povodňových map bývají zaplavovány povodněmi s periodicitou 10 let nebo nižší, resp. záplavových území stanovených nebo navržených úřadem (např. obecním) či správcem vodního toku.

Během povodně může v jejím okolí docházet ke zvýšení hladiny podzemních vod, které se následně projeví v zatopení např. sklepů, které jsou pod úrovní terénu. AZP v rámci rizika povodně vylučuje škody způsobené pronikáním a zvýšením hladiny podzemní vody, a dále pak škody způsobené pronikáním nebo průsakem vody v důsledku předchozího porušení celistvosti konstrukčních prvků (např. hydroizolace). ČPP vzlínáním, pronikáním, prosakováním nebo zvýšením hladiny podzemní vody, které je přímým důsledkem povodně či záplavy, z pojištění hradí. Ostatní pojišťovny se k tomu v podmínkách nevyjadřují, ale dle definice povodně mohou takový nárok odmítnout.

Záplava

Definice záplavy je u všech vybraných pojišťoven velmi obdobná. Pro příklad AZP záplavu definuje jako zaplavení místa pojištění způsobené v důsledku nedostatečného odtoku atmosférických srážek, které vytvoří souvislou vodní plochu, nebo příval vody způsobený deštěm. Ostatní podmínky, jako například výluka na škody vzniklé do 10 dnů od sjednání pojištění, používají všechny pojišťovny shodně pro povodeň i záplavu.

Zemětřesení

Všechny z vybraných pojišťoven kromě KOOP se shodují, že se musí jednat o otřesy zemského povrchu vyvolané pohybem v zemské kůře, které dosahují v místě pojištění alespoň 6. stupně podle makroseizmické stupnice EMS 98 (KOOP používá starší stupnici MSK-64). Jinak řečeno, pokud jsou otřesy slabší, nebo jsou způsobeny např. důlní činnosti nebo výbuchem, nejsou z daného rizika hrazeny. AZP dává navíc možnost prokázání zemětřesení přes Richterovu stupnici, kdy zemětřesení musí dosahovat 5. stupně.

Atmosférické srážky

Toto riziko jako jediná nabízí AZP, která jej v pojistných podmínkách definuje jako vniknutí atmosférických srážek do budovy nebo provozovny, prosakování tajícího sněhu nebo ledu do budovy nebo provozovny, a u pojištění budovy jako rozpínavost ledu v důsledku k zamrznutí dešťových svodů umístěných na obvodovém plášti budovy.

Sesuv půdy, hornin, zemin a zřícení skal

ČSOBP definuje riziko sesuv půdy, zřícení skal nebo zemin jako pohyb hornin svahu z vyšších poloh svahu do nižších, ke kterému dochází působením přírodních a klimatických vlivů. Obdobnou definici používají i ostatní vybrané pojišťovny, avšak KOOP, AZP a ČPP k tomu přidávají sesuv z důvodu lidské činnosti. Pokud tedy bude ve svahu prováděna např. stavba nebo terénní úpravy, pak pouze některé z pojišťoven takovou škodu uhradí, nikoliv každá. Na čem se však pojišťovny shodnou je, že z daného rizika nehradí pokles rovinatého terénu nebo změny základových poměrů staveb (např. promrzáním, sesycháním, podmáčením půdy bez porušení rovnováhy svahu). AZP jako jediná se v pojistných podmínkách nijak nevyjadřuje k riziku zřícení skal.

Sesuv a pád lavin

Definice tohoto rizika není u vybraných pojišťoven (kromě AZP) jen obdobná, avšak dokonce totožná. Vybrané pojišťovny riziko definují jako jev, kdy masa sněhu nebo ledu se náhle po svazích uvede do pohybu a řítí se do údolí. Jediná AZP lavinu popisuje jako pád sněhové nebo ledové vrstvy z přírodních svahů. Pojistné podmínky žádné z vybraných pojišťoven k tomu nepřidávají další podmínky.

Tíha nebo tlak sněhu

GČP tíhou sněhu nebo námrazy rozumí destruktivní působení tíhy vrstvy sněhu nebo námrazy z příčiny jejich nadměrné hmotnosti na střešní krytiny, nosné nebo ostatní **konstrukce střechy**. Za poškození nebo zničení předmětu pojištění tíhou sněhu nebo námrazy GČP považuje takové destruktivní poškození nebo zničení předmětu pojištění, k němuž došlo přímým působením tíhy sněhu nebo námrazy na střešní krytinu nebo ostatní konstrukce střechy budovy, nebo v příčinné souvislosti s tím, že tíha sněhu nebo námrazy poškodila dosud bezvadné a funkční stavební součásti zastřešení budovy. Avšak KOOP, ČSOBP a ČPP neomezují toto riziko jen na střechu, ale rozšiřují jej na všechny konstrukce. AZP nijak toto riziko nedefinuje, nicméně vylučuje škody, které nastanou z daného rizika v období do 10 dnů (včetně) od data sjednání.

3.2 Případová studie vybraného podniku

Vybraný podnik si přeje být anonymizován, a proto je v práci využíván pouze název XYZ. Základní informace o podniku byly získány z volně dostupných informací (např. webových stránek podniku), které však bylo nutné doplnit o informace získané přímo od jednatele podniku XYZ. Na základě všech takto získaných informací je podnik nejprve popsán v oddílu *„Představení podniku XYZ“*. V další pak navazující oddíl *„Aktuální rizika versus podnik XYZ“* je základem provedená kontrola pojistných smluv podniku XYZ, jež byly poskytnuty jednatelem podniku. Na přání jednatele podniku dané smlouvy nejsou přílohou práce, a to ani v anonymizované podobě. Předmětem kontroly pojistných smluv bylo pouze zjistit, na jaká rizika je podnik v současnosti pojištěn a zda mezi pojištěnými riziky jsou také aktuální rizika, která jsou předmětem této práce. Avšak samotné ověření rozsahu krytí pojistné smlouvy nestačí ke správnému posouzení, zda má podnik ideálně nastavené pojištění. Proto v rámci případové studie bylo nezbytné také ověřit, zda vybraná rizika vůbec mohou ohrozit podnik, a zda je opravdu nutné mít proti těmto rizikům sjednané pojištění. Zároveň s tím, pokud tato rizika podnik mohou ohrožovat, zda má podnik nastavená preventivní opatření, a tedy, zda jsou daná rizika v podniku řízena jiným způsobem než pouze pojištěním. Posledním pohledem na věc také je, zda podnik splňuje povinnosti, která vyžaduje pojišťovna, a jsou součástí pojistných podmínek. Pro tyto účely byl vypracován dotazník (viz příloha 5), který byl zodpovězen přímo jednatelem podniku. Dotazník se týká pouze vybraných rizik.

3.2.1 Představení podniku XYZ

Podnik XYZ byl založen na počátku devadesátých let, bez zahraniční účasti, a již od svého založení se zabývá projekty průmyslové automatizace. Podnik nejprve vyvinul vlastní řídicí systém, který nabízel i jiným realizátorům zakázek. Po cca 10 letech, kdy začaly být v České republice cenově dostupné zahraniční řídicí systémy i pro menší zakázky, se podnik soustředil na vývoj a zajišťování výroby zákaznických řešení. Postupným rozvojem podniku, zejména v oblasti služeb, výroby, vývoje a dodávek v oboru automatizační, řídicí a přístrojové techniky, se rozšířil na desítky stálých zaměstnanců, množství odběratelů, subdodavatelů a externích spolupracovníků. Aktuální roční obrat podniku činí cca 1 milion USD. Podnik

disponuje silným softwarovým oddělením, které vyvíjí softwarová řešení pro zákazníky z mnoha oborů, jako je například sklářství, textilní průmysl, polovodičový průmysl, chemický průmysl, strojírenský průmysl, zkušební stroje, teplárenství a klimatizace, drůbežářství. Kromě jiného se podnik zabývá sběrem a přenosem dat, monitoringem a regulací odběru energie. Podnik má zkušenosti i s vývojem jednoúčelových přístrojů. V současné době nabízí:

- vestavné systémy a jiná speciální zákaznická řešení,
- vývoj elektroniky a přístrojové techniky včetně jejich následné výroby, oživení a testování,
- vývoj aplikačního programového vybavení, běžícího jak na PC, tak i vlastních zákaznických systémech,
- vývoj aplikačního programového vybavení, běžícího na standardních řídicích systémech (např. Siemens),
- vypracování projektů a studií automatizace technologií, strojů a výrobních linek,
- montáž a dodávky rozvaděčů s řídicí elektronikou,
- a komplexní dodávky řídicích systémů a pohonů včetně vizualizace a napojení na podnikové řídicí systémy.

Co se týká organizační struktury, podnik je řízen jednateli, kteří jsou odpovědni valné hromadě. Jednatelem je ředitel (volen valnou hromadou) a případně další vedoucí úseků. Ředitel podniku schvaluje přijímání a propouštění zaměstnanců, jmenuje a odvolává vedoucí úseků, řídí a koordinuje vedoucí jednotlivých úseků. Pomocným orgánem ředitele podniku je porada vedení, skládající se z vedoucích jednotlivých úseků. Jedná se o úseky ekonomicko-právní, obchodní, vývojový, výrobní, správa infrastruktury,

Ekonomicko-právní úsek má na starosti vedení účetnictví, personalistiku, právní záležitosti, sledování legislativy, pojištění podniku a školení zaměstnanců. Tento úsek dále vypracovává ekonomické ukazatele, oponuje tvorbu cen, a provádí archivaci účetních, personálních a právních dat. Obchodní úsek má na starosti marketing, udržování dobrých kontaktů se stávajícími zákazníky, vedení databáze zakázek, stanovení cen, koordinaci rozsáhlých zakázek, návrh smluv, prodej, koordinaci zakázek, koordinaci servisu, a archivaci dat.

Vývojový úsek se dělí na úsek vývoje hardware a úsek vývoje software. Má na starosti zpracování projektů na vývoj hardware nebo software dle potřeb obchodního úseku včetně vypracování technického zadání úkolu, vypracovávání podkladů pro cenové kalkulace, tvorbu podkladů pro výrobu funkčních vzorků, prototypů i sériové výroby, tvorbu průběžné a závěrečné oponentury vývoje. Vývojový úsek dále zajišťuje typové zkoušky vyvinutých výrobků v externích zkušebnách, vydává prohlášení o shodě pro nové výrobky, zajišťuje změnové řízení dle potřeb obchodu nebo výroby, a zajišťuje také archivaci veškerých vývojových podkladů.

Výrobní úsek zajišťuje kontrolu výrobních podkladů, plánování externí a interní výroby, zajišťování externí výroby včetně kooperace při zajišťování materiálu, nákup materiálu a dalších dílů potřebných pro zajištění zakázky, interní výrobu funkčních vzorků, nákup materiálu a dílů, u kterých provádí jejich vstupní kontrolu. Výrobní úsek také vede sklad materiálu a kupovaných dílů pro realizaci výroby a jednotlivých zakázek, provádí montáž sestav z dodaných komponent, jejich oživování, zahořování, expedici k zákazníkovi, provádí nákup režijního materiálu a interního vybavení, a také má na starosti archivaci výrobních protokolů.

Správa infrastruktury zajišťuje kontrolu a revizi elektrických spotřebičů, kalibraci měřících přístrojů, opravy přístrojů a kancelářské techniky, servisní prohlídky a opravy automobilů, údržbu a úklid kanceláří, zajišťování BOZP a protipožární ochrany, a správu počítačové sítě

a nakoupeného vybavení. Úsek kontroly kvality zajišťuje údržbu systému ISO 9001, zajištuje interní a externí audit, vede podnikový elektronický archiv, provádí namátkovou kontrolu kvality výroby a nakupovaných dílů, a provádí kontrolu kvality v oblasti EHS.

3.2.2 Aktuální rizika versus podnik XYZ

V minulosti podnik řešil pouze několik škod na vozidle, a to z povinného ručení a havarijního pojištění. Neřešil tedy žádnou škodu ze zkoumaných rizik. Škody byly pojišťovnou uhrazeny v plné výši, nicméně podnik XYZ nebyl spokojen s likvidací škody u Generali České pojišťovny, a.s. (dříve známé jako České pojišťovny a.s.), a proto je od roku 2000 klientem Allianz pojišťovny, a.s. Podnik dlouhodobě hledá model pojištění, které by pokrylo pojištění odpovědnosti za škodu způsobenou jeho výrobky, a pojištění odpovědnosti za škodu způsobenou stroji řízenými jeho řídicími systémy s územním rozsahem Evropy a Severní Ameriky. Nicméně na tento typ pojištění se diplomová práce nezaměřuje.

V současnosti má podnik sjednané majetkové pojištění s krytím pro rizika požár, výbuch, úder blesku, náraz nebo zřícení letadla, krádež vloupáním a pojištění nákladu. Podnik má také odpovědnostní pojištění, kdy smlouva konkrétně kryje provozní odpovědnost (včetně regresů zdravotních pojišťoven), odpovědnost za škodu způsobenou na převzatých věcech a na pronajatých nemovitostech, a odpovědnost za škodu způsobenou stroji, které jsou řízeny výrobky vyrobenými pojištěným. Avšak neobsahuje krytí pro aktuální rizika, kterými jsou kybernetické hrozby, přerušení provozu, vichřice, krupobití, povodeň, záplava, atmosférické srážky, zemětřesení, sesuv půdy hornin, zemin a zřícení skal, sesuv a pád lavin, a také tíha a tlak sněhu.

IT hrozby a kybernetické pojištění

První část dotazníku se věnuje kybernetickým rizikům. Jak vyplynulo z teoretické části práce, většina škod patří do skupiny neúmyslných hrozeb, způsobených na základě interního jednání, tzv. způsobené **interním vlivem**. Pro příklad se jedná buď o nedbalost zaměstnance, nebo jeho úmyslné jednáním (např. vynesení informací, či krádež zařízení, kde jsou informace uloženy). Příkladem nedbalosti může být neopatrnost při práci s informacemi, konkrétně pak třeba zveřejnění informací na webových stránkách, které však nemají být zveřejněny. Podnik provozuje vlastní webové stránky (nikoliv e-shop), které si také sám spravuje, a kromě pracovníků podniku XYZ nemůže nikdo jiný přidávat nebo měnit obsah těchto webových stránek. Riziko možné chyby je tedy čistě na straně interních zaměstnanců. Jak bylo zjištěno, podnik má ale jen desítky stálých zaměstnanců, u kterých lze předpokládat loajalitu a profesionalitu. Rozhodně se nejedná o provoz s vysokou fluktuací neprověřených zaměstnanců. Podnik má navíc nastavena pravidla pro práci s informacemi, jako je podniková směrnice, která nastavuje pravidla klasifikace, označování a ukládání dokumentů, přístup jednotlivých skupin zaměstnanců k informacím a dokumentům, či obecná pravidla nakládání s osobními údaji fyzických osob (GDPR).

Ochrana před **externími kybernetickými hrozbami** je v dnešní době celkem běžnou součástí každého počítačového systému. Antivirové programy a firewally jsou dnes standardem, a u podniku XYZ tomu není jinak. Podnik má na všech zařízeních, která jsou připojena k veřejné síti, nainstalován antivirový program (včetně ochrany pro malware), provádí nebo má nastavenou automatickou aktualizaci počítačových systémů, antivirových programů a firewallů, které má navíc správně nakonfigurované. Zcela samozřejmě pracujete pouze s oficiálními verzemi programů, a na základě platné licence. Naproti tomu, ale nemá nastavena pravidla pro používání silných hesel, které proto v podniku nejsou zavedeným standardem. A co víc nemá procesně nastavenou pravidelnou aktualizaci hesel, což v praxi může znamenat, že některá hesla nebyla změněna roky. Selhání technického zabezpečení, ale

pro podnik nemusí být jedinou slabinou. Tou další může být selhání lidského faktoru, kdy hacker využije metod jako je phishing, scanning nebo jiný typ sociálního inženýrství. Podnik XYZ pro tyto případy proškolil všechny zaměstnance.

Vnější hrozbu mohou představovat také návštěvy, pro které má podnik nastavená pravidla jako je omezení jejich pohybu jen na vyčleněné prostory, omezení jejich přístupu na společnou wi-fi apod. Stejně tak má podnik nastavená další bezpečnostní pravidla, která jsou ukotvena v pracovní směrnici. Jedná se například o povinnost uzamykání obrazovky při odchodu z pracovního místa, uzamknutí místnosti apod.

Podnik XYZ elektronicky zpracovává osobní údaje, uchovává obchodní tajemství a informace smluvních stran. Nedostatečné zabezpečení informací a jejich následná krádež může podniku XYZ způsobit nemalé potíže, někdy to může mít dokonce fatální dopady. Únik informací může pro podnik znamenat třeba udělení sankce od kontrolního orgánu, smluvních pokut, či ztráty důvěry zákazníků apod. Přesto podnik nepoužívá zabezpečenou formu přenosu/předávání informací, jako je například šifrovaná pošta, heslování souborů a předání hesla jiným kanálem (např. SMS zprávou), předávání přes zabezpečená uložiště, apod. Dost pravděpodobně podnik k veškeré komunikaci používá nezabezpečenou emailovou poštu. Cílem hackerů nemusí být jen odcizení informací, ale jak vyplynulo z teoretické části práce, může je také úmyslně poškodit, smazat nebo zablokovat. Prevencí v takových případech je zálohování dat alespoň jednou týdně, což podnik dodržuje.

Z pohledu pojištění je pak výhodou, že podnik neprovozuje činnost, které nejsou kryté pojištěním od žádné z vybraných pojišťoven. Konkrétně příkladem takových činností je provoz nebo správa webových portálů, poskytování hostingových, cloudových a obdobných služeb, obchodování na finančních trzích, či vývoj software pro řízení/ovládání dopravního prostředku. Stejně tak podnik XYZ nepracuje s utajovanými informacemi, které se týkají důležitých informací odrážejících klíčové státní zájmy, není řazen do tzv. kritické infrastruktury státu a nemusí tak být cílem kybernetického terorismu, který dle pojistných podmínek třeba ČSOBP nehradí. Z dotazníku ovšem vyplynulo, že podnik XYZ poskytuje software či hardware, nebo provádí jakékoliv jiné činnosti a poskytuje služby v oblasti počítačových systémů a informačních technologií, kdy hrozí u koncového zákazníka kybernetický incident. Stejně tak mohou být kybernetickým incidentem postiženy finanční transakce podniku.

Covid-19 a pojištění přerušení provozu

Podnik XYZ patří k podnikům, které mají vytvořen plán a opatření pro případnou novou pandemii s cílem minimalizovat potenciální přerušení/omezení provozu. Podnik XYZ je příkladem digitální transformace, kde alespoň polovina zaměstnanců podniku XYZ je schopna plně vykonávat svoji práci z domova. Nejen z tohoto důvodu, ale také vzhledem ke zjištění z teoretické části práce, nebyl příliš důvod věnovat dotazník jen přerušení provozu z důvodu pandemie. Proto se část dotazníku, která se zabývá přerušením provozu, věnuje i dalším příčinám přerušení provozu, kterými jsou přírodní nebezpečí a škody na strojích. Podstatnou otázkou pak také je, jaký dopad by takové přerušení provozu mělo na podnik XYZ. Otázky ohledně konkrétních finančních ztrát (ušlého zisku a nákladů) jsou obsahově širší, než je zvolené téma diplomové práce. Proto jsou dopady přerušení provozu řešeny jen v obecné rovině. Podnik se domnívá, že je schopen obnovit svůj provoz po velké události už za 3 měsíce. Dle informací od jednatele, finanční ztráty v případě přerušená provozu jsou nejvyšší jen během prvních dvou dnů, další dny pak klesají. V případě velké události, která by znemožnila vykonávat činnost v současné budově, podnik je schopen provoz přesunout jinam, a pokračovat tak v činnosti. Další výhodou pro podnik je, že ukládá bezpečně, vzájemně odděleně a ve dvou vyhotoveních inventury, bilance, obchodní knihy, účty, doklady o daňové

a odvodové povinnosti, výsledky hospodaření a smlouvy o pronájmu za poslední tři roky, které jsou nutné k likvidaci případné škody z přerušení provozu. Stejně tak uchovává bezpečně listiny, plány, výkresy, jakékoliv nosiče dat se záznamy na nich (např. zvukové, obrazové, datové a jiné), softwarové vybavení, vzorky, modely, prototypy, obchodní knihy nebo spisy všeho druhu, jejichž poškození, zničení nebo ztráta by mohlo způsobit přerušení provozu. Naproti tomu ale podnik nemá vypracován krizový plán pro velké události, nemá tak připravená konkrétní řešení jako jsou právě např. náhradní prostory, zástupy apod. Co se týká případného přerušení provozu z důvodu škody na stroji, podnik sice provádí pravidelnou revizi a údržbu strojů a zařízení, obává se však zkratu, přepětí nebo poruchy, které by také mohlo způsobit přerušení provozu. Přitom ale nemá všechny stroje a elektroniku chráněny přepěťovou ochranou a vlastně nemá pojištěno ani riziko přepětí a zkratu pro stroje a elektroniku.

Změny klimatu a pojištění přírodních nebezpečí

Podnik vykonává svou činnost v pronajatých prostorách, a žádný nemovitý majetek nevlastní. Pro svoji činnost podnik využívá pouze jednu budovu, ve které má zároveň sídlo, a která prošla v roce 2000 rekonstrukcí. Vzhledem k tomu, že v provozní budově je pouze nájemcem, podnik XYZ má pojištěn jen movitý majetek a náklad v autech, nikoliv však budovu. Součástí movitého majetku jsou stroje, elektronika, zásoby, díly, kancelářská technika, automobily a další vybavení jako nábytek apod. Provozní budova se nachází v místě, kde ji přímo neohrožuje působení žádného z přírodních živlů. Není umístěna ve svahu, ani v blízkosti skály, ani v místech s častějším výskytem silného větru, jako jsou vyšší polohy, kopce, otevřená prostranství, nenachází se v povodňové zóně, ani v blízkosti vodního toku nebo díla, není umístěna v horské oblasti, a nenachází se ani v oblasti s častějším výskytem zemětřesení. Jednatel podniku XYZ dále uvedl, že v místě budovy není zhoršený odtok atmosférických srážek, a při dlouhodobějších deštích nikdy nedošlo k vystoupnutí vody z kanalizace. Podnik má sice uskladněny některé věci v prostorech, které jsou pod úrovní terénu, ale všechny věci jsou na pevném podkladu o výšce min. 15 cm nad úrovní podlahy (tuto povinnost stanovují pojistné podmínky KOOP). Při případnému úderu blesku je budova chráněna hromosvodem, a v případě masivního zasněžení budovy/střechy je podnik schopen sníh ze střechy odklidit.

3.3 Vyhodnocení

Tato část práce využívá a spojuje dohromady informace z teoreticko-metodologické části práce, rozboru pojistných podmínek vybraných pojišťoven, případové studie podniku, z doplňujícího rozhovoru s jednatelem podniku a osobní zkušenosti autora práce. Cílem vyhodnocení je poskytnout podniku XYZ zpětnou vazbu k současnému řízení rizik, která jsou předmětem této práce.

IT hrozby a kybernetické pojištění

Z pěti vybraných pojišťoven nabízí kybernetické pojištění pouze dvě, konkrétně KOOP a ČSOBP. Naopak jiné velké pojišťovny, jako jsou GČP, AZP a ČPP tento typ pojištění v současnosti nenabízí. Není tedy zcela pravdou, že většina pojišťoven na českém pojistném trhu nabízí pojištění kybernetických rizik, což tvrdí Dobiáš (2019, s. 241). Co je ale naopak pojistnými podmínkami pro pojištění kybernetických rizik potvrzeno, je tvrzení SPG (2020c): *„Zda nebo do jaké míry bude kybernetický útok hrazen pojišťovnou, závisí na tom, jak podnik řídí kybernetická rizika.“*. Pojistné podmínky skutečně podmiňují úhradu škody dodržováním různých pravidel bezpečnosti. Stejně tak je potvrzen i názor SPG (2020c), která uvádí, že pro podniky může kybernetický incident vést mimo jiné k přerušení provozu, platbám výkupného, poklesu reputace a potenciální pokutě od regulátora. Dle názoru SPG by mělo kybernetické pojištění nabízet více než jen čistou náhradu za potenciální významnou finanční ztrátu, ale

navíc poskytnout asistenční služby, a také pomoct pojistníkům lépe zvládat kybernetická rizika. Potvrzují to pojistné podmínky ČSOBP, dle kterých z kybernetického pojištění jsou hrazeny náklady na činnost IT odborníka, za PR služby, za právní obhajobu, hradí se také sankce (vyjma ale sankcí za přímé nedodržení pravidel GDPR), náklady na obnovu dat a software, finanční újma spojená s přerušením provozu, výkupné, a jakékoliv peněžní prostředky, o které přijde pojištěný přímo v důsledku kybernetického zločinu. To vše si může klient ČSOBP pojistit.

Hlavní obranou podniku XYZ před **interními vlivy** (nedbalost nebo úmysl zaměstnance) je především správný výběr zaměstnanců a spolupracovníků, a udržení si těch spolehlivých. Tuto strategii by si měl podnik i nadále udržet. Proto je riziko takového incidentu v podniku XYZ nižší než v jiných typech provozů. Pokud by přesto podnik požadoval krytí i tohoto rizika, KOOP a ČSOBP nabízí krytí škod v důsledku chyby nebo úmyslného jednání zaměstnance, avšak s omezeními (podrobněji viz oddíl 3.1.1). Pojištění na tento typ rizika je tak spíše jen doplňkem, nikoliv nutnou ochranou pro podnik XYZ. Podniku je ale silně doporučeno nezanedbat prevenci, a udržovat aktualizovaná pravidla, která budou ukotvena v pracovní směrnici. Zejména pak je doporučeno i **nadále věnovat pozornost GDPR**, kdy pracovní směrnice je pro zaměstnance návodem jak s osobními údaji fyzických osob nakládat. Podnik navíc může pomocí směrnice lépe vymáhat dodržování pravidel.

Z teoretické části dále vyplynulo, že **vnější kybernetické hrozby** se stále vyvíjí a jsou čím dál více sofistikovanější. Nejčastějšími typy útoků je phishing, malware (ransomware) s cílem zablokování systému, znepřístupnění webových stránek nebo e-shopu, smazání, změna nebo zašifrování dat, a následné požadování výkupného, či krádež informací a duševního vlastnictví s úmyslem je prodat. Tyto a jiné útoky jsou stále na vzestupu, tzn., zvyšuje se jejich četnost, intenzita a míra jejich dopadů. Přestože jsou u podniku XYZ základní prvky ochrany splněny, nelze tyto útoky brát na lehkou váhu. Současná opatření nikdy nezaručí 100% ochranu, jelikož i zkušeného pracovníka lze nachytat, a sebelepší prvky ochrany lze překonat. **Pojištění je vhodným doplňkem ochrany**, ale kromě něj je nutná opět prevence. Většinu prevenčních povinností, které stanovují pojistné podmínky, podnik splňuje, kromě **pravidelné aktualizace hesel a nastavení používání jen silných hesel**, což podnik v současnosti nedělá. Pokud by se podnik rozhodl sjednat kybernetické pojištění třeba u ČSOBP, které se jeví jako více pro klientské, musel by zavést i tato opatření nad rámec současných. V rámci prevence je podniku XYZ doporučeno zavést i některá další opatření. Možnou prevencí je testování pozornosti zaměstnanců. K takovému testování lze použít fiktivní emailové zprávy, které vypadají jako firemní pošta, či email od věhlasné společnosti, ale ve skutečnosti nejsou (odesílatelem je někdo jiný), a adresát je nabádán na kliknutí na odkaz. Podnik sice uvádí, že zaměstnance proškolil na možné kybernetické útoky, ale jednorázové proškolení není dostatečným opatřením. Podniku je **doporučeno provádět pravidelná školení a časté opakování pravidel bezpečnosti**. Pravidla bezpečnosti by měly být také k dispozici v písemné podobě. Vůči dalším vnějším hrozbám, které mohou představovat třeba návštěvníci budovy je podnik chráněn dalšími pravidly bezpečnosti. Naopak podstatnou slabinou podniku je absence zabezpečeného přenosu informací. Zde by měl podnik zvážit nápravu, a alespoň ty **nejcennější informace (např. obchodní tajemství) posílat bezpečnější formou** než je email.

Z pohledu pojištění je výhodou, že si podnik sám spravuje obsah webových stránek. Je ale také důležité, aby si podnik **dával pozor, které informace zveřejňuje na svých webových stránkách**, jelikož vybrané pojišťovny by takový typ kybernetické incidentu z pojištění nehradily. Příkladem takové situace může být prezentace referencí, které by obsahovaly až příliš podrobné informace o zákaznících (např. osobní údaje fyzických osob).

Covid-19 a pojištění přerušení provozu

Přerušení provozu je druhým rizikem v pořadí, kterému se celosvětově věnuje největší pozornost. Ale není tomu jen z důvodu pandemie, přestože až teprve díky Covid-19 si některé podniky začali uvědomovat, o jak závažné riziko se jedná. Jak již bylo řečeno, pandemie urychlila digitální transformaci, ale také naučila podniky novým způsobům jak v případě další pandemie předejít přerušení provozu. Pandemie Covid-19 nebyla první a pravděpodobně, ani nebude poslední pandemií, a nemusí to být jen viry typu Covid-19, SARS či MERS, ale ohrožují nás také baktérie. Jak vyplývá z teoretické části práce, pojištění přerušení provozu je obecně koncipováno pro úhradu následných (finančních) ztrát vzniklých v příčinné souvislosti s přerušením provozu v důsledku věcné škody. Což potvrzuje také analytická část práce, kdy navíc jak ukazují pojistné podmínky většiny z vybraných pojišťoven, věcná škoda musí vzniknout z pojištěného nebezpečí u stejné pojišťovny. V překladu to znamená, že riziko pandemie není běžně u přerušení provozu krytou příčinou. Není to ale pravidlo, výjimky se přeci jen najdou. Tou výjimkou je KOOP, která pojištění přerušení provozu z důvodu pandemie nabízí. Pro podnik XYZ však přerušení provozu z důvodu pandemie není tolik závažné riziko, jelikož v podniku jsou již nastavena pravidla a připravené nástroje, které pravděpodobně odolají další vlně pandemie. Nutnost sjednání pojištění přerušení provozu z důvodu pandemie je tak spíše na uvážení podniku.

Jak ale ukázal dotazník, přerušení provozu podniku XYZ může nastat i z jiných příčin. A potvrzuje to i teoretická část práce. Kybernetická rizika, přírodní události a přerušení provozu mají k sobě velmi blízko. Nejobávanější příčinou přerušení provozu jsou právě kybernetická rizika, následovaná přírodními katastrofami, a až na třetím místě žebříčku nejobávanějších příčin je přerušení provozu z důvodu pandemie. Pravděpodobným důvodem tohoto seřazení je, že většina podniků je na pandemii mnohem lépe připravena než na kybernetický útok nebo přírodní katastrofu. Nelze ani zapomínat, že přerušení provozu může způsobit také porucha některého ze strojů, kterými podnik disponuje. Na českém trhu lze pojistit i přerušení provozu z důvodu škody na stroji nebo elektronice. KOOP a ČSOBP nabízí k pojištění kybernetických rizik také pojištění přerušení provozu. Jiné z vybraných pojišťoven nenabízí pojištění kybernetických rizik, a logicky tak nemohou nabídnout pojištění přerušení provozu ze stejné příčiny. GČP, AZP a ČPP nabízí pouze tradiční krytí pro přerušení provozu, jako jsou přírodní události a škody na strojích.

Podnik XYZ je doporučeno nejprve zvážit, jak vysoké finanční ztráty podniku reálně hrozí v případě nenadálého přerušení provozu, a to porovnat s cenou daného pojištění. Jinak řečeno, pro rozhodnutí, zda sjednat či nesjednat bude především cena pojištění. Je přitom důležité dávat pozor na časovou spoluúčast, která u některých pojišťoven je nastavena právě na dva dny, kdy má podnik XYZ nejvyšší finanční ztráty. Dále pak na dobu ručení, která znamená maximální hrazenou dobu přerušení provozu. Podnik XYZ dokáže obnovit svůj provoz do 3 měsíců, a není tedy důvod mít dobu ručení sjednanou v délce 12 měsíců. Velmi zásadní informací také je, že pojištění přerušení provozu se přímo váže na majetkové pojištění sjednané u stejné pojišťovny. Pokud by se tedy podnik rozhodl pro sjednání strojního přerušení provozu, pak musí zároveň s ním sjednat i pojištění strojů. Stejně tak v případě kybernetických rizik a přírodních událostí. V případě, že se podnik rozhodne nepojistit své stroje proti rizikům jako je přepětí, měl by zvážit alternativní možnost ochrany v podobě přepěťové ochrany na všech provozovaných zařízeních (stroje a elektronika).

Změny klimatu a pojištění přírodních nebezpečí

Analytická část práce pouze potvrdila to, co si už mnoho lidí myslí. Přírodní katastrofy, které zahrnují extrémní přírodní události celosvětově, nastávají s čím dál větší frekvencí, a právem se tak umístily na druhém místě žebříčku nejzávažnějších a nejčastějších celosvětových

podnikatelských rizik, kterým je potřeba věnovat pozornost. Není to však jen ve světovém měřítku, ale riziko je i lokální. V českých statistikách škod za poslední 3 roky je vidět, že vichřice, atmosférické srážky a povodně patří k těm nejčetnějším a nejzávažnějším. Jedná se o informace, které nezávisle na sobě potvrzuje mnoho institucí a statistik, ale to není ani tolik překvapující. Zajímavým zjištěním je ale informace, že nepojištěné škody z přírodních nebezpečí rostou rychleji než ty pojištěné. Nastává tedy mnohem častěji situace, že vzniklou škodu si poškození musí uhradit z vlastních zdrojů. Mnoho subjektů si pravděpodobně pojištění buď nemůže vůbec dovolit, nebo riziko podceňují. Přitom třeba z vybraných pojišťoven nabízí krytí přírodních událostí všechny. V současnosti v rámci pojištění se jedná o již tradiční pojištění, kdy definice jednotlivých rizik od různých pojišťoven se vzájemně příliš neliší. Snad jediným podstatným rozdílem v nabídce je, že AZP nabízí navíc pojištění atmosférických srážek.

Přesto podnik XYZ nemá sjednáno pojištění přírodních nebezpečí. Dle všech získaných informací, ale nic nenasvědčuje tomu, že by podnik nutně potřeboval pojištění přírodních nebezpečí, které v současnosti nemá. Jednak je to kvůli umístění budovy, ale zároveň také tím, že není ani jejím vlastníkem. Pojištění přírodních nebezpečí by se tak týkalo pouze movitých věcí, které tomuto riziku ani nejsou přímo vystaveny. I přes všechna tato zjištění je však potřeba mít na paměti, a potvrzuje to i teoretická část práce, že je každým rokem více škod, které napáchají přírodní události. Zvyšuje se nejen jejich četnost, ale také síla. Tornádo, které udeřilo na Moravě, je toho důkazem. Z tohoto důvodu by podnik neměl považovat rizika přírodních událostí za zcela vyloučená, a **minimálně by měl zvážit nejhorší možné scénáře**. Extrémní chování počasí, lze očekávat i v budoucnosti, a proto pojištění vichřice, záplavy, tíhy sněhu, či zemětřesení se může jednoho dne vyplatit.

4 Závěr

Hlavní trendy v oblasti podnikatelských rizik, která lze pojistit, jsou minimálně pro následujících několika let jasné. Na globální úrovni se na tom shodují nejen odborníci z oblasti pojišťovnictví, ale i samotné podniky a známe organizace. Nejobávanějším podnikatelským rizikem jsou kybernetické hrozby, následované rizikem přerušením provozu a přírodními událostmi. Každý podnik, nejen podnik XYZ, by toto měl zohlednit v rámci procesu řízení rizik. Pro daná rizika sice podnik XYZ aktuálně nemá sjednané pojištění, avšak soudě dle nastavených preventivních opatření v tomto podniku, je si těchto rizik vědom. Management rizik v podniku XYZ není tak jen prázdný pojem, ale k řízení rizik skutečně dochází. Zejména vůči kybernetickým rizikům podnik přistupuje velmi zodpovědně. Aby ne, když se jedná o podnik, který působí na poli automatizační techniky. Podnik XYZ by přesto neměl zapomínat, že doba je rychlá, a měl by adaptovat na nové podmínky. Opatření, která ještě před pár lety byla nadstandardní, dnes jsou zcela běžná a je potřeba udělat víc. V opačném případě může přijít nemilé překvapení. Počty hackerských útoků neustále rostou, a dopady těchto událostí jsou rok od roku větší, nemluvě o sofistikovanosti kybernetických útoků. To vše je podrobně rozebráno v analytické části práce. A kromě věcných škod mohou podniku vzniknout i finanční škody v podobě přerušení provozu, sankcí, výkupného, nákladů na IT, právních nebo PR služeb atd. Z chybějícího pojistného krytí je tak podniku XYZ doporučeno zvážit zejména sjednání pojištění kybernetických rizik, které nabízí ČSOBP. Nicméně samotné sjednání pojištění je pouze doplňkem ochrany, a proto je podniku XYZ především doporučeno zavést další opatření v oblasti prevence rizik nad rámec těch současných. Mezi taková opatření patří pravidelné aktualizace hesel, nastavení povinnosti používání jen silných hesel, provádět pravidelná školení v oblasti bezpečnosti, časté opakování pravidel bezpečnosti, alespoň ty nejcennější informace (např. obchodní tajemství) posílat bezpečnější formou než je email, raději však i další citlivé informace. Stejně tak by si podnik měl dávat pozor, které informace zveřejňuje na svých webových stránkách, zejména pak s ohledem na GDPR, kterému je nutné nadále věnovat pozornost. Dále pak každým rokem přibývá množství přírodních katastrof, ať jsou již důvodem klimatické změny způsobené člověkem či nikoliv, statistická čísla potvrzují, že škod každým rokem přibývá. Oproti kybernetickým rizikům ale podnik není natolik ohrožen přírodními vlivy nejen umístěním provozní budovy, ale také proto, že není jejím vlastníkem. Přesto by se měl podnik minimálně zamyslet a vytvořit krizový plán pro případ, že by nastala velká událost typu tornádo, či zemětřesení. Obsahem krizového plánu by pak mělo například být konkrétní řešení v podobě možných náhradních prostorů, či plán zástupů apod. A co se týká přerušení provozu, podnik by neměl podcenit ani toto riziko. Přestože nemusí být nutně ohrožen případnou další pandemií, příčinou přerušení provozu mohou být právě i kybernetické hrozby, které s rizikem přerušení provozu velmi úzce souvisí. Pro tyto případy je doporučeno zvážit pojištění přerušení provozu z důvodu kybernetického incidentu. Ať už se jedná o výše uvedená nebo jiná rizika, podnik XYZ by měl mít stále na paměti, že klíčem k úspěšnému podnikání je připravenost i na nenadálé situace, a neměl by příliš věřit, že k některým událostem nemůže dojít, podobně jako je psáno v citátu z úvodu práce.

Literatura

Primární zdroje

ČASTORÁL, Z. *Management rizik v současných podmínkách.* Praha: Univerzita Jana Amose Komenského Praha, 2017. ISBN 978-80-7452-132-4.DOBIÁŠ, P. *Pojištění podnikatelů ve vztazích s mezinárodním prvkem.* Praha: Leges, 2019. ISBN 978-80-7502-348-3.

DOUCEK, P. a kolektiv *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

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

JANATA, J. *Pojištění a management majetkových podnikatelských rizik.* Praha: Professional Publishing, 2004. ISBN 80-86419-64-9

JANATA, J. *Principy pojištění podnikatelů a právnických osob.* Praha: Professional Publishing, 2014. ISBN 978-80—7431-140-6.

JURKOVIČOVÁ, M., ONDRUŠKA, T., PASTORÁKOVÁ, E. Dejiny poisťovnictva. Praha: Wolters Kluwer ČR, a.s., 2020. ISBN 978-80-7598-998-7

KOLOUCH, J. *Cybercrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7. Dostupné z WWW: <https://knihy.nic.cz/files/edice/cybercrime.pdf >

KRULIŠ, J. *Jak vítězit na riziky: aktivní management rizik – nástroj řízení úspěšných firem.* Praha: Linde, 2011. ISBN 978-80-7201-835-2.

PACÁKOVÁ V. a kolektiv *Aplikovaná pojistná statistika*. Pardubice: Univerzita Pardubice, 2019. ISBN 978-80-7560-259-6

FOJTÍKOVÁ, I. a kolektiv *Pojištění občanů.* Praha: Eva Gmentová, 2020. ISBN 978-80-906748-6-8.

ENGST, P. a kolektiv *Pojištění v kostce*. Praha: Eva Gmentová, 2020. ISBN 978-80-906748-7-5.

RAMNATH, S., et al. *What is Business Interruption Insurance and How is it Related to the Covid-19 Pandemic?*. Chicago Fed Letter, 2020, vol.1, no.440, p.1-5. ISSN 0895-0164.

ŘEZÁČ, F. *Řízení rizik v pojišťovnictví.* Brno: Masarykova univerzita, 2016. ISBN 978-80-210-8179-6

SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.

SMIL, V. *Global Catastrophes and Trends. The Next Fifty Years*. Cambridge, Massachusetts: MIT Press, 2012. ISBN 10: 0262518228 ISBN 13: 9780262518222

STRAUSS, J., H., STRAUSS E., G., Viruses and Human Disease. California, Pasadena: Elsevier, 2008. ISBN 978-0-12-373741-0

ŠULC, V. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

VEBER, J. a kolektiv *Management: základy, přístupy, soudobé trendy*. I. vydání. Praha: Ekopress, 2021. ISBN 978-80-87865-69-9.

VEBER, J. a kolektiv *Podnikání malé a střední firmy.* Praha: Grada, 2012. ISBN 978-80-247-4520-6.

Normy, nařízení a legislativa

ČSN ISO 31000 (010351) Management rizik – Principy a směrnice. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018

ISO/IEC 27000:2018 *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC TS 27100:2020 *Information technology – Cybersecurity – Overwiew and concepts.* International Organization for Standardization

ISO/IEC TS 27103:2018 Information technology – Security techniques – Cybersecurity and ISO and IEC standards. International Organization for Standardization

Zákon č. 412/2015 Sb., o ochraně utajovaných informací a o bezpečnostní

Internetové zdroje

AEC, *Klasifikace informací v korporátním prostředí* [online]. 2018 Dostupné z WWW: <https://www.aec.cz/cz/ztisku/matej-kacic-klasifikace-informaci-v-korporatnim-prostredi-dsm-2018.pdf>

Allianz Global Corporate & Specialty SE, Risk Barometer 2022 [online]. 18. 1. 2022 Dostupné z WWW: <https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html>

Allianz pojišťovna a.s., *Pojištění pro firmy* [online]. 2022 Dostupné z WWW: <https://www.allianz.cz/cs_CZ/pro-firmy.html>

Allianz pojišťovna a.s., *Dokumenty a formuláře* [online]. 2022 Dostupné z WWW: <https://www.allianz.cz/cs_CZ/pojisteni/pro-klienty/dokumenty-a-formulare.html#dokumenty-pro-firmy>

Allianz pojišťovna a.s., *Smluvní dokumentace Allianz podnikání* [online]. 2018 Dostupné z WWW: <https://apps.allianz.cz/file/45275/predsmluvni_info_Podnikatele_12._2018_v9_spojene_nove_podminky_FINAL3.pdf>

Allianz pojišťovna a.s., *Průvodce pojištěním Moje Firma* [online]. 2021 Dostupné z WWW: <https://www.allianz.cz/content/dam/onemarketing/cee/azcz/dokumenty-a-formulare/pro-firmy/moje-firma/BG_MOJEFIRMA_A5_10_21_v27.pdf>

Banka pro mezinárodní vypořádání, *Covid-19 and cyber risk in the financial sector* [online]. 14.1.2021 Dostupné z WWW: < https://www.bis.org/publ/bisbull37.pdf>

CRO Forum, *The Cyber Risk Challenge and the Role of Insurance* [online]. 2014, s. 5. Dostupné z WWW: <https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf>

Česká asociace pojišťoven, *Tisková zpráva – Vývoj pojistného trhu v roce 2021* [online]. Praha: 2022 Dostupné z WWW: <https://www.cap.cz/tiskove-centrum/tiskove-zpravy/104867-vyvoj-pojistneho-trhu-v-roce-2021-rust-trhu-o-4-4-zejmena-diky-nezivotnimu-pojisteni-narust-skod-je-v-pojisteni-majetku>

Česká asociace pojišťoven, *Statistiky* [online]. Praha: 2019-2021. Dostupné z WWW: <https://www.cap.cz/statistiky-prognozy-analyzy/skody-z-pojisteni-majetku>

Česká asociace pojišťoven, *Slovník pojmů* [online]. Praha: 2020. Dostupné z WWW: < https://www.cap.cz/odborna-verejnost/odborne-slovniky>

Česká asociace pojišťoven, *Vývoj pojistného trhu* [online]. Praha: 2022. Dostupné z WWW: <https://www.cap.cz/statistiky-prognozy-analyzy/vyvoj-pojistneho-trhu>

Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group *Pojištění podnikatelů* [online]. Praha: 2022. Dostupné z WWW: < https://www.cpp.cz/pojisteni-podnikatelu>

Česká podnikatelská pojišťovna, a.s, Vienna Insurance Group *Pojištění podnikatelů a průmyslu na míru* [online]. Praha: 2022. Dostupné z WWW: <https://www.cpp.cz/pojisteni-podnikatelu/pojisteni-podnikatelu-a-prumyslu-na-miru>

Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group *Doplňkové pojistné podmínky pro pojištění přerušení nebo omezení provozu DPPŠP MP 1/16* [online]. Praha: 2016. Dostupné z WWW: <https://www.cpp.cz/file/edee/dokumenty/pojisteni-podnikatelu/spolecne-dokumenty/pp0372016unp_p3_dppsp-mp-1_16.pdf>

Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group *Doplňkové pojistné podmínky pro pojištění strojů a elektroniky DPPSE 1/16* [online]. Praha: 2016. Dostupné z WWW: <https://www.cpp.cz/file/edee/dokumenty/pojisteni-podnikatelu/spolecne-dokumenty/pp0372016unp_p6_dppse-mp-1_16.pdf>

Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group *Všeobecné pojistné podmínky pro pojištění majetku VPPM 1/16* [online]. Praha: 2016. Dostupné z WWW: <https://www.cpp.cz/file/edee/dokumenty/nezivotni-pojisteni/vppm-1_16.pdf>

Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group *Zvláštní pojistné podmínky pro pojištění přerušení nebo omezení provozu poškozením nebo zničením stroje a elektroniky ZPPŠST MP 1/16* [online]. Praha: 2016. Dostupné z WWW: <https://www.cpp.cz/file/edee/dokumenty/pojisteni-podnikatelu/pojisteni-podnikatelu-a-prumyslu/pp0372016unp_d2_p_zppsst-mp-1_16.pdf>

Český hydrometeorologický ústav, *Souhrnná zpráva k vyhodnocení tornáda na jihu Moravy 24. 6. 2021* [online]. Praha: 2021, s. 3. Dostupné z WWW: <https://www.chmi.cz/files/portal/docs/tiskove_zpravy/2021/Souhrnna_zprava_tornado_24.6.2021.pdf>

ČSOB Pojišťovna, a.s., člen holdingu ČSOB *Všeobecné pojistné podmínky – zvláštní část VPP CRC 2018 Pojištění kybernetických rizik* [online]. 01.11.2018. Dostupné z WWW: <https://www.csobpoj.cz/documents/10332/32946/10N9059+VPP_CRC_2018_10-2018.pdf/dc55ba8d-b5e3-17c8-0954-63591b631e67?t=1576162606907>

ČSOB Pojišťovna, a.s., člen holdingu ČSOB *Všeobecné pojistné podmínky – Obecná část VPP OC 2014* [online]. 28.04.2018. Dostupné z WWW: <https://www.csobpoj.cz/documents/10332/474974/VPP_OC_2018_GDPR.pdf/08df5d15-3a77-4aa8-bacc-2b42317dded5>

Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění [online]. Frankfurt am Main: 2019. ISBN 978-92-9473-213-2 Dostupné z WWW: <https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf>

Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění [online]. Frankfurt am Main: 15.10. 2021. Dostupné z WWW: <https://www.eiopa.europa.eu/media/feature-article/cyber-risks-what-impact-insurance-industry_en?source=search>

Generali Česka pojišťovna a.s., *ProfiPlán - pojištění pro podnikatele a právnické osoby – významně navyšuje pojistné limity u klíčových rizik* [online]. 12.01.2021 Dostupné z WWW: <https://www.generaliceska.cz/-/profiplan-pojisteni-pro-podnikatele-a-pravnicke-osoby-vyznamne-navysuje-pojistne-limity-u-klicovych-rizik>

Generali Česka pojišťovna a.s., *Dokumenty ke stažení – Firemní produkty* [online]. 2022. Dostupné z WWW: <https://www.generaliceska.cz/firemni-dokumenty>

Generali Česka pojišťovna a.s., *Všeobecné pojistné podmínky pro pojištění majetku a odpovědnosti podnikatele a právnických osobVPPMO-P-01/2020* [online]. 2020. Dostupné z WWW: <https://www.generaliceska.cz/documents/20183/63226/8.40.014_01-20_v01_KLIK_k1-11-19_ren.pdf/06f5d678-feea-481e-9db0-11964f9e361a>

Generali Česka pojišťovna a.s., *Všeobecné pojistné podmínky pro pojištění majetku a odpovědnosti podnikatele a právnických osob VPPMO-P-02/2020* [online]. 2020. Dostupné z WWW: <https://www.generaliceska.cz/documents/20183/63226/Poji%C5%A1t%C4%9Bn%C3%AD+majetku+a+odpov%C4%9Bdnosti+podnikatele+a+pr%C3%A1vnick%C3%BDch+osob/2eded3b3-5820-4014-98df-71b89e4fd6c1>

Generali Česka pojišťovna a.s., *Doplňkové pojistné podmínky pro pojištění přerušení provozu DPPPP-P-01/2020* [online]. 2020. Dostupné z WWW: <https://www.generaliceska.cz/documents/20183/63226/8.40.018_01-20_v01-k19-8-19.pdf/03cc9d9a-7071-408e-b3ca-fad987eaab61>

Generali Česka pojišťovna a.s., *Doplňkové pojistné podmínky pro pojištění přerušení provozu DPPPP-P-02/2020* [online]. 2020. Dostupné z WWW: <https://www.generaliceska.cz/documents/20183/63226/99.8.60.113+10-20+v01.pdf/a1b63292-195b-4d5b-b864-62e348dc2893>

Generali Česka pojišťovna a.s., *Doplňkové pojistné podmínky pro pojištění strojů DPPST-P-01/2020* [online]. 2020. Dostupné z WWW: <https://www.generaliceska.cz/documents/20183/63226/8.20.009_01-20_v01_FINAL_nahled.pdf/bb34b342-317c-4e5a-b885-06590f52fc1c>

Generali Česka pojišťovna a.s., *Doplňkové pojistné podmínky pro pojištění strojů DPPST-P-02/2020* [online]. 2020. Dostupné z WWW: <https://www.generaliceska.cz/documents/20183/63226/99.8.60.114+10-20+v01.pdf/328923e3-826c-48a2-973e-ed60f097aab5>

Generali Česka pojišťovna a.s., *Doplňkové pojistné podmínky pro pojištění elektronických zařízení DPPEZ-P-01/2020* [online]. 2020. Dostupné z WWW: <

https://www.generaliceska.cz/documents/20183/63226/8.20.010_01-20_v01_nahled.pdf/c4c335e7-7225-4b0c-ab58-c6aeeff89e8c>

Generali Česka pojišťovna a.s., *Doplňkové pojistné podmínky pro pojištění elektronických zařízení DPPEZ-P-02/2020* [online]. 2020. Dostupné z WWW: <https://www.generaliceska.cz/documents/20183/63226/99.8.60.115+10-20+v01.pdf/8969511a-950c-402b-8b10-b1546ee1ed08>

Kooperativa pojišťovna, a.s., Vienna Insurance Group *Pojištění kybernetických rizik* [online]. 2018. Dostupné z WWW: <https://www.koop.cz/pojisteni/pojisteni-malych-a-strednich-podnikatelu/pojisteni-kybernetickych-rizik>

Kooperativa pojišťovna, a.s., Vienna Insurance Group *Soubor pojistných podmínek pro pojištění podnikatelů* [online]. 2020. Dostupné z WWW: <https://www.koop.cz/file/edee/dokumenty/podnikatele-prumysl/KOOP_Soubor_pojistnych_podminek_pro_pojisteni_podnikatelu.pdf>

Ministerstvo životního prostředí Strategie přizpůsobení se změně klimatu v podmínkách ČR – 1. aktualizace pro období 2021–2030 [online]. 2021. Dostupné z WWW: < https://www.mzp.cz/cz/zmena_klimatu_adaptacni_strategie>

Národní úřad pro kybernetickou a informační bezpečnost, *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* [online]. Praha: 2021, s. 3. Dostupné z WWW: <https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf>

Národní úřad pro kybernetickou a informační bezpečnost, *Regulace a kontrola / FAQ* [online] Dostupné z WWW < https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/>

NEBOLSINA, E. The impact of the Covid-19 pandemic on the business interruption insurance demand in the United States. [online] Heliyon, 2021. ISSN 2405-8440. Dostupné z WWW: < . https://www.sciencedirect.com/science/article/pii/S2405844021024609#bib44>

OECD *Cyber risk insurance* [online]. 18. 04. 2016 Dostupné z WWW: <https://www.oecd.org/finance/insurance/cyber-risk-insurance.htm>

OECD *Responding to the COVID-19 and pandemic protection gap in insurance* [online]. 16. 3. 2021 Dostupné z WWW: < https://www.oecd.org/coronavirus/policy-responses/responding-to-the-covid-19-and-pandemic-protection-gap-in-insurance-35e74736/>

Renomia, *Pojištění a koronavirus – Co Vás nejvíce zajímá* [online]. Praha: 2020. Dostupné z WWW: < https://www.renomia.cz/koronavirus-co-vas-nejvice-zajima>

S&P Global Inc., *European Insurance In Transition: Plotting A Course In A Chaotic World* [online]. 2020a, 3. 12. 2020 Dostupné z WWW: <https://www.spglobal.com/ratings/en/research/articles/201203-european-insurance-in-transition-plotting-a-course-in-a-chaotic-world-11758026?utm_campaign>

S&P Global Inc., *COVID-19 Highlights Global Insurance Protection Gap On Climate Change* [online]. 2020b, 28. 9. 2020 Dostupné z WWW: <https://www.spglobal.com/ratings/en/research/articles/200928-covid-19-highlights-global-insurance-protection-gap-on-climate-change-11617761?utm_campaign>

S&P Global Inc., *Cyber Risk In A New Era: Insurers Can Be Part Of The Solution* [online]. 2020c, 2. 9. 2020 Dostupné z WWW: <https://www.spglobal.com/ratings/en/research/articles/200902-cyber-risk-in-a-new-era-insurers-can-be-part-of-the-solution-11590046?utm_campaign=corporatepro&utm_medium=contentdigest&utm_source=Insurance>

Státní veterinární správa, *Nařízení státní veterinární správy – mimořádná veterinární opatření k zamezení šíření nebezpečné nákazy – vysoce patogenní influenzy ptáků (aviární influezy, tzv. „ptačí chřipky") na území České republiky* [online]. Praha: 2021. Dostupné z WWW: <https://eagri.cz/public/web/file/690193/MZE_66362_2021_18140.pdf>

Swiss Re [online]. Curych: 2022. Dostupné z WWW: <https://www.swissre.com/risk-knowledge/mitigating-climate-risk.html>

Swiss Re Insitute [online]. Curych: 2021. Dostupné z WWW: <https://www.swissre.com/media/news-releases/nr-20211214-sigma-full-year-2021-preliminary-natcat-loss-estimates.html>

World Health Organization, *Severe Acute Respiratory Syndrome (SARS)* [online]. Ženeva: 2021a Dostupné z WWW: <https://www.who.int/health-topics/severe-acute-respiratory-syndrome#tab=tab_1>

World Health Organization, *Middle East respiratory syndrome coronavirus (MERS-CoV)* [online]. Ženeva: 2021b. Dostupné z WWW: <https://www.who.int/health-topics/middle-east-respiratory-syndrome-coronavirus-mers#tab=tab_1>

World Health Organization, *WHO urges an increase in influenza vaccination* [online]. Ženeva: 2002. Dostupné z WWW: <https://www.who.int/news/item/26-09-2002-who-urges-an-increase-in-influenza-vaccination>

World Meteorological Organization, *Weather-related disasters increase over past 50 years, causing more damage but fewer deaths* [online] 31. 8. 2021. Dostupné z WWW: <https://public.wmo.int/en/media/press-release/weather-related-disasters-increase-over-past-50-years-causing-more-damage-fewer>

Přílohy

Příloha 1

Česká asociace pojišťoven

Předběžné údaje ČAP – škody z pojištění majetku 1-12/2019

Ukazatel	1-12/2018	1-12/2019	Index 1-12/2019 k 1-12/2018
Počet pojistných událostí		ks	
Počet pojistných událostí celkem	**244 900**	**265 821**	**108,5**
- škody z tíhy sněhu	1 531	7 951	519,3
- škody z povodní	5 090	7 041	138,3
- škody z vichřice	24 677	41 605	168,6
- škody z krupobití	5 204	15 383	295,6
- škody z požáru	5 995	5 189	86,6
- škody z úderu bleskem	5 602	4 908	87,6
- škody z výbuchu	473	297	62,8
- škody ze sesuvu / poklesu půdy	556	390	70,1
- vodovodní škody	48 395	43 929	90,8
- škody z atmosférických srážek	6 504	8 708	133,9
- poškození nebo zničení skla	9 722	10 053	103,4
- poškození nebo zničení stroje	8 259	7 805	94,5
- škody z pádu letadle nebo jiných předmětů	8 210	5 430	66,1
- škody z nárazu dopravního prostředku	3 091	2 806	90,8
- škody z přepětí v elektrické síti	9 946	10 593	106,5
- škody ze zkratu elektromotoru	2 265	2 100	92,7
- ostatní poškození elektroniky	23 701	23 895	100,8
- škody z vandalismu	10 288	8 204	79,7
- škody z krádeží	14 950	13 559	90,7
- ostatní škody z pojištění majetku (bez pojištění vozidel)	50 441	45 974	91,1
Pojistné události		tis. Kč	
Pojistné události celkem	**9 526 498**	**9 545 567**	**100,2**
- škody z tíhy sněhu	19 852	192 305	968,7
- škody z povodní	187 534	288 816	154,0
- škody z vichřice	576 675	1 040 812	180,5
- škody z krupobití	515 198	1 252 164	243,0
- škody z požáru	3 090 884	1 811 541	58,6
- škody z úderu bleskem	114 036	95 998	84,2
- škody z výbuchu	83 978	33 944	40,4
- škody ze sesuvu / poklesu půdy	12 379	18 525	149,6
- vodovodní škody	1 282 455	1 214 355	94,7
- škody z atmosférických srážek	91 194	134 904	147,9
- poškození nebo zničení skla	73 334	74 336	101,4
- poškození nebo zničení stroje	894 076	851 254	95,2
- škody z pádu letadle nebo jiných předmětů	97 778	95 441	97,6
- škody z nárazu dopravního prostředku	76 403	75 780	99,2
- škody z přepětí v elektrické síti	167 564	181 463	108,3
- škody ze zkratu elektromotoru	31 258	33 510	107,2
- ostatní poškození elektroniky	144 817	154 749	106,9
- škody z vandalismu	109 459	104 991	95,9
- škody z krádeží	334 855	392 602	117,2
- ostatní škody z pojištění majetku (bez pojištění vozidel)	1 622 770	1 498 079	92,3

Zdroj: Česká asociace pojišťoven (2020)

Příloha 2

Česká asociace pojišťoven

Předběžné údaje ČAP – škody z pojištění majetku 1-12/2020

Ukazatel	1-12/2019	1-12/2020	Index 1-12/2020 k 1-12/2019
Počet pojistných událostí		ks	
Počet pojistných událostí celkem	**287 815**	**262 449**	**91,2**
- škody z tíhy sněhu	8 046	246	3,1
- škody z povodní	7 343	14 006	190,7
- škody z vichřice	43 023	50 127	116,5
- škody z krupobití	15 953	5 593	35,1
- škody z požáru	5 943	4 960	83,5
- škody z úderu bleskem	5 092	3 768	74,0
- škody z výbuchu	320	314	98,1
- škody ze sesuvu / poklesu půdy	426	399	93,7
- vodovodní škody	46 968	43 240	92,1
- škody z atmosférických srážek	9 032	13 245	146,6
- poškození nebo zničení skla	11 794	10 210	86,6
- poškození nebo zničení stroje	8 460	8 430	99,6
- škody z pádu letadle nebo jiných předmětů	5 814	4 112	70,7
- škody z nárazu dopravního prostředku	3 208	2 545	79,3
- škody z přepětí v elektrické síti	11 210	11 221	100,1
- škody ze zkratu elektromotoru	2 194	2 263	103,1
- ostatní poškození elektroniky	24 248	22 445	92,6
- škody z vandalismu	10 301	8 196	79,6
- škody z krádeží	15 246	12 859	84,3
- ostatní škody z pojištění majetku (bez pojištění vozidel)	53 193	44 270	83,2
Pojistné události		tis. Kč	
Pojistné události celkem	**10 137 112**	**10 872 909**	**107,3**
- škody z tíhy sněhu	193 745	5 988	3,1
- škody z povodní	306 396	789 237	257,6
- škody z vichřice	1 082 439	1 412 340	130,5
- škody z krupobití	1 303 072	572 592	43,9
- škody z požáru	1 872 619	1 997 051	106,6
- škody z úderu bleskem	95 653	83 808	87,6
- škody z výbuchu	33 685	645 523	1916,4
- škody ze sesuvu / poklesu půdy	20 096	26 166	130,2
- vodovodní škody	1 301 159	1 200 309	92,2
- škody z atmosférických srážek	129 212	189 848	146,9
- poškození nebo zničení skla	80 566	80 462	99,9
- poškození nebo zničení stroje	930 928	859 490	92,3
- škody z pádu letadle nebo jiných předmětů	109 172	93 030	85,2
- škody z nárazu dopravního prostředku	87 432	95 142	108,8
- škody z přepětí v elektrické síti	182 815	191 375	104,7
- škody ze zkratu elektromotoru	43 904	37 815	86,1
- ostatní poškození elektroniky	159 263	144 791	90,9
- škody z vandalismu	110 116	116 116	105,4
- škody z krádeží	383 738	337 136	87,9
- ostatní škody z pojištění majetku (bez pojištění vozidel)	1 711 104	1 994 693	116,6

Zdroj: Česká asociace pojišťoven (2021)

Příloha 3

Česká asociace pojišťoven

Předběžné údaje ČAP – škody z pojištění majetku 1-12/2021

Ukazatel	1-12/2020	1-12/2021	Index 1-12/2021 k 1-12/2020
Počet pojistných událostí		ks	
Počet pojistných událostí celkem	**250 061**	**266 190**	**106,5**
- škody z tíhy sněhu	409	4 969	1214,9
- škody z povodní	14 351	10 371	72,3
- škody z vichřice	51 788	33 153	64,0
- škody z krupobití	5 826	15 643	268,5
- škody z požáru	5 438	4 749	87,3
- škody z úderu bleskem	3 956	5 236	132,4
- škody z výbuchu	339	340	100,3
- škody ze sesuvu / poklesu půdy	424	434	102,4
- vodovodní škody	45 879	43 621	95,1
- škody z atmosférických srážek	13 510	13 355	98,9
- poškození nebo zničení skla	11 172	11 380	101,9
- poškození nebo zničení stroje	9 477	8 383	88,5
- škody z pádu letadle nebo jiných předmětů	4 484	4 745	105,8
- škody z nárazu dopravního prostředku	3 089	2 655	86,0
- škody z přepětí v elektrické síti	11 732	13 847	118,0
- škody ze zkratu elektromotoru	2 200	2 186	99,4
- ostatní poškození elektroniky	22 872	16 207	70,9
- škody z vandalismu	6 786	7 590	111,8
- škody z krádeží	12 586	11 300	89,8
- ostatní škody z pojištění majetku (bez pojištění vozidel)	23 743	56 026	236,0
Pojistné události		tis. Kč	
Pojistné události celkem	**11 274 427**	**19 582 020**	**173,7**
- škody z tíhy sněhu	7 268	125 140	1721,8
- škody z povodní	771 592	558 698	72,4
- škody z vichřice	1 398 653	4 076 715	291,5
- škody z krupobití	571 488	1 469 006	257,0
- škody z požáru	1 932 559	2 867 949	148,4
- škody z úderu bleskem	85 304	170 714	200,1
- škody z výbuchu	577 225	2 589 389	448,6
- škody ze sesuvu / poklesu půdy	15 798	33 170	210,0
- vodovodní škody	1 236 269	1 355 849	109,7
- škody z atmosférických srážek	191 234	224 376	117,3
- poškození nebo zničení skla	80 606	94 655	117,4
- poškození nebo zničení stroje	878 105	857 560	97,7
- škody z pádu letadle nebo jiných předmětů	100 640	133 577	132,7
- škody z nárazu dopravního prostředku	77 919	95 908	123,1
- škody z přepětí v elektrické síti	190 327	241 230	126,7
- škody ze zkratu elektromotoru	38 230	37 240	97,4
- ostatní poškození elektroniky	152 399	141 593	92,9
- škody z vandalismu	117 258	116 022	98,9
- škody z krádeží	327 473	309 155	94,4
- ostatní škody z pojištění majetku (bez pojištění vozidel)	2 524 079	4 084 072	161,8

Zdroj: Česká asociace pojišťoven (2022)

Příloha 4

Česká asociace pojišťoven

Neživotní pojištění dle metodiky ČAP – indexy 1-12/2021

	Pojišťovna	Podnikatelská pojištění		
		Předepsané smluvní pojistné (tis. Kč)		
		1-12/2020	1-12/2021	Index
1	GČP	6 884 753	7 147 027	**103,8**
2	KOOP	5 342 335	5 118 143	**95,8**
3	ALLIANZ	2 490 375	2 637 624	**105,9**
4	ČPP	1 713 091	1 917 465	**111,9**
5	ČSOBP	1 839 703	2 077 517	**112,9**
6	UNIQA	897 933	890 999	**99,2**
7	CARDIF			
8	DIRECT	169 514	143 894	**84,9**
9	COLONNADE	696 599	767 341	**110,2**
10	SLAVIA	186 476	190 435	**102,1**
11	HVP	424 019	386 525	**91,2**
12	ERV	4 961	4 339	**87,5**
13	KP			
14	MAXIMA	111 629	127 425	**114,2**
15	HDI	410 045	470 837	**114,8**
16	ERGO			
17	D.A.S.			
18	METLIFE			
19	HALALI	6 155	9 100	**147,8**
20	YOUPLUS			
21	ČKP			
	CELKEM	**21 177 588**	**21 888 671**	**103,4**

Zdroj: Česká asociace pojišťoven (2022)

Příloha 5 Dotazník včetně odpovědí jednatele společnosti (odpovědi tučně zvýrazněny)

1) Má podnik XYZ aktuálně sjednané majetkové pojištění? Pokud ano, u jaké pojišťovny?
    a) **ano: Allianz pojišťovna, a.s.**
    b) ne
2) Má podnik XYZ aktuálně sjednané odpovědnostní pojištění? Pokud ano, u jaké pojišťovny?
    a) **ano: Allianz pojišťovna, a.s. (od roku 2000)**
    b) ne
3) Řešili jste v minulosti nějakou škodu s kteroukoliv pojišťovnou? Pokud ano, jakou?
    a) **ano: párkrát škoda na vozidle z titulu povinného ručení resp. havarijního pojištěni**
    b) ne
4) Jak byla škoda pojišťovnou vyřešena?
    a) **uhrazena v plné výši**
    b) uhrazena částečně
    c) zamítnuta
5) Pokud byla škoda zamítnuta, uveďte důvod:

    ……..
6) Splňuje současné pojištění všechny požadavky podniku XYZ? Pokud ne, uveďte, v čem by pojištění mělo být jiné?
    a) ano
    b) **ne: Podnik dlouhodobě hledá model pojištění, které by pokrylo pojištění odpovědnosti za škodu způsobenou jejími výrobky, a pojištění odpovědnosti za škodu způsobenou stroji řízenými jejími výrobky s územním rozsahem Evropy a Severní Ameriky.**

<u>Kybernetická rizika:</u>

7) Máte vlastní webové stránky?
    a) **ano**
    b) ne

8) Pokud máte vlastní webové stránky, kdo všechno má možnost přidávat/měnit jejich obsah? (pozn. lze vybrat i více možností)
    a) podnik XYZ
    b) externí dodavatel
    c) někdo jiný
9) Provozujete nebo spravujete webové portály?
    a) ano
    b) ne
10) Provozujete vlastní e-shop?
    a) ano
    b) ne
11) Zpracováváte, spravujete nebo uchováváte data ve smyslu například poskytování hostingových, cloudových a obdobných služeb? (pozn. vylučuje KOOP a ČSOBP)
    a) ano
    b) ne
12) Které druhy informací jsou v podniku zpracovávány? (pozn. lze vybrat více možností zároveň, bližší popis druhů informací viz oddíl 2.2.1)
    a) Osobní údaje (pozn. GDPR)
    b) Obchodní tajemství
    c) Informace smluvní strany
    d) Přísně důvěrné informace
    e) Informace utajované (pozn. státní zájmy)
13) Má podnik nastavena nějaká pravidla pro práci s informacemi? Příkladem může být podniková směrnice, která nastavuje pravidla klasifikace, označování a ukládání dokumentů, přístup jednotlivých skupin zaměstnanců k informacím a dokumentům, či obecná pravidla nakládání s osobními údaji fyzických osob (GDPR)?
    a) ano
    b) ne
14) Používáte zabezpečenou formu přenosu/předávání informací, jako je například šifrovaná pošta, heslování souborů a předání hesla jiným kanálem (např. SMS zprávou), předávání přes na zabezpečená uložiště, apod.? Jinak řečeno, posíláte osobní údaje fyzických osob a citlivé informace bezpečněji než jen prostým emailem?
    a) ano
    b) ne

15) Je podnik XYZ řazen do tzv. kritické infrastruktury státu a může tak být cílem kybernetického terorismu? (pozn. ČSOBP vylučuje kybernetický terorismus)
    a) ano
    b) ne
16) Nabízí, používá nebo se podnik zabývá vývojem software pro řízení/ovládání dopravního prostředku? (pozn. vylučuje KOOP)
    a) ano
    b) ne
17) Zálohujete data alespoň jednou za týden? (pozn. vyžaduje zejména ČSOBP)
    a) ano
    b) ne
18) Máte na všech zařízeních, která jsou připojena k veřejné síti, nainstalován antivirový program?
    a) ano
    b) ne
19) Máte nepřetržitě aktivovaný přiměřený profesionální software na ochranu proti malware? (pozn. vyžaduje zejména ČSOBP)
    a) ano
    b) ne
20) Používáte firewall a máte ho správně nakonfigurovaný? (pozn. vyžaduje zejména ČSOBP)
    a) ano
    b) ne
21) Provádíte pravidelné aktualizace veškerého software, zejména počítačových systémů, antivirů a firewallů? Případně máte nastavené automatické aktualizace?
    a) ano
    b) ne
22) Pracujete pouze s oficiálními verzemi programů, a na základě platné licence?
    a) ano
    b) ne
23) Má podnik nastavena pravidla pro používání silných hesel, která se v podniku opravdu v praxi používají?
    a) ano
    b) ne

24) Máte procesně nastavenou pravidelnou aktualizaci hesel? (pozn. vyžaduje zejména ČSOBP)
    a) ano
    b) ne
25) Poskytuje software či hardware, nebo provádí jakékoliv jiné činnosti a poskytuje služby v oblasti počítačových systémů a informačních technologií, kdy hrozí u koncového zákazníka kybernetický incident?
    a) ano
    b) ne
26) Máte nastavení pravidla pro návštěvy jako je omezení jejich pohybu jen na vyčleněné prostory, omezení jejich přístupu na společnou wi-fi apod.?
    a) ano
    b) ne
27) Má podnik nastavená další bezpečnostní pravidla, která jsou ukotvena v pracovní směrnici jakou je povinnost uzamykání obrazovky při odchodu z pracovního místa, uzamknutí místnosti apod.?
    a) ano
    b) ne
28) Byli zaměstnanci proškolení jak odhalit a ubránit se nejčastějším kybernetickým útokům jako je phishing, scanning nebo jiným typům sociálního inženýrství?
    a) ano
    b) ne
29) Mají zaměstnanci k dispozici manuál jak odhalit a ubránit se nejčastějším kybernetickým útokům jako je phishing, scanning nebo jiným typům sociálního inženýrství?
    a) ano
    b) ne
30) Obchodujete a provádíte transakce na finančních trzích?
    a) ano
    b) ne
31) Mohou být kybernetickým útokem ohroženy finanční transakce podniku?
    a) ano
    b) ne

Přerušení provozu:

32) Za jak dlouho je schopen podnik obnovit svůj provoz po velké události?
    - **a) 3 měsíce**
    - b) 12 měsíců
33) V případě přerušená provozu, finanční ztráty jsou:
    - **a) nejvyšší jen během prvních dvou dnů, pak klesají**
    - b) stejné každý den po celou dobu přerušení provozu
34) Obáváte se poškození nebo zničení strojů z důvodu zkratu, přepětí nebo poruchy, které by mohlo způsobit přerušení provozu?
    - **a) ano**
    - b) ne
35) Provádíte pravidelnou revizi a údržbu strojů a zařízení?
    - **a) ano**
    - b) ne
36) Máte vytvořen plán a opatření pro případnou novou pandemii s cílem minimalizovat potenciální přerušení/omezení provozu?
    - **a) ano**
    - b) ne
37) Je alespoň polovina zaměstnanců podniku XYZ schopna plně vykonávat svoji práci z domova?
    - **a) ano**
    - b) ne
38) V případě velké události, která by znemožnila vykonávat činnost v současné budově, je možné provoz přesunout jinam, a pokračovat tak v činnosti?
    - **a) ano**
    - b) ne
39) Má podnik vypracován krizový plán pro velké události, nebo dokonce připravená konkrétní řešení jako např. náhradní prostory, zástupy apod.?
    - a) ano
    - **b) ne**
40) Ukládáte bezpečně, vzájemně odděleně a ve dvou vyhotoveních inventury, bilance, obchodní knihy, účty, doklady o daňové a odvodové povinnosti, výsledky hospodaření a smlouvy o pronájmu za poslední tři roky, které jsou nutné k likvidaci případné škody z přerušení provozu?

a) ano

b) ne

41) Uchováváte bezpečně také listiny, plány, výkresy, jakékoliv nosiče dat se záznamy na nich (např. zvukové, obrazové, datové a jiné), softwarové vybavení, vzorky, modely, prototypy, obchodní knihy nebo spisy všeho druhu, jejichž poškození, zničení nebo ztráta by mohlo způsobit přerušení provozu?

a) ano

b) ne

Přírodní události:

42) Budova, ve které podnik vykonává svoji hlavní činnost je:

a) ve vlastnictví podniku XYZ

b) pouze v pronájmu

43) Využívá podnik pro svoji činnost i další budovy? Pokud ano, uveďte, zda jsou ve vlastnictví podniku, nebo v pronájmu?

a) ano

b) ne

44) Vlastní podnik XYZ nějaký jiný nemovitý majetek?

a) ano

b) ne

45) Vlastní podnik XYZ movitý majetek? Pokud ano, jaký?

a) ano: stroje, elektroniku, zásoby, díly, kancelářskou techniku, automobily a další vybavení jako nábytek apod.

b) ne

46) Nachází se provozní budova ve svahu a může tak být ohrožena sesuvem půdy?

a) ano

b) ne

47) Nachází se provozní budova v blízkosti skály, kde hrozí zřícení skal?

a) ano

b) ne

48) Nachází se provozní budova v místech s častějším výskytem silného větru (např. vyšší polohy, kopce, otevřená prostranství)?

a) ano

b) ne

49) Nachází se provozní budova ve vyhlášené povodňové zóně? (pozn. oblasti, kde podle aktuálních povodňových map bývají zaplavovány povodněmi s periodicitou 10 let nebo nižší, resp. záplavových území stanovených nebo navržených úřadem, např. obecním, či správcem vodního toku)

a) ano

b) ne

50) Nachází se provozní budova v blízkosti a na úrovni nějakého vodního toku nebo díla?

a) ano

b) ne

51) Nachází se provozní budova v místě s horším odtokem atmosférických srážek? Při velkých deštích zůstávají v místě souvislá vodní plocha?

a) ano

b) ne

52) Nastalo někdy při dlouhodobějších deštích v provozní budově vystoupnutí vody z kanalizace?

a) ano

b) ne

53) Nachází se provozní budova v horských oblastech, kde hrozí riziko pádu lavin?

a) ano

b) ne

54) Nachází se provozní budova v oblastech s častějším výskytem zemětřesení? (např. Moravskoslezský nebo Karlovarský kraj)

a) ano

b) ne

55) Uveďte přibližné stáří budovy, nebo dobu od poslední rekonstrukce. Zaměřte se jen na stáří střechy, oken, dveří a pláště budovy. (pozn. nutné pro posouzení možnosti zatékání do budovy a odolnosti budovy vůči povětrnostním podmínkám)

Odpověď: poslední rekonstrukce proběhla v roce 2000

56) Má provozní budova prostory, které jsou umístěny pod úrovní terénu, a mohou být tak zasaženy zvýšenou hladinou podzemních vod jako důsledku vydatných dešťů?

a) ano

b) ne

57) Pokud podnik má prostory, které jsou umístěny pod úrovní terénu, jsou v takových prostorech uloženy věci na pevném podkladu o výšce min. 15 cm nad úrovní podlahy? (pozn. zejména zásoby a cizí věci)
    a) ano
    b) ne
58) V případě masivního zasněžení budovy/střechy, máte prostředky a možnosti jak sníh ze střechy odklidit? (pozn. zvažte přístupnost střechy, schopnosti pracovníků, vybavení, atd.)
    a) ano
    b) ne
59) Je provozní budova opatřena ochranou před bleskem? (např. aktivním či pasivním hromosvodem)
    a) ano
    b) ne
60) Jsou všechny stroje a elektronika chráněny přepěťovou ochranou?
    a) ano
    b) ne

Zdroj: vlastní zpracování (2022)

VŠEM VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Pojištění jako nástroj řízení aktuálních podnikatelských rizik ve vybrané společnosti

Miloš Bednář, KEMMA01

Řešená problematika

úvod

Co má společného kybernetický útok, Covid-19 a přírodní živel?

Odpověď: Jedná se o nejzávažnější podnikatelská rizika pro rok 2022, kterým je věnována největší pozornost.

problém

Mohou tato rizika ohrožovat podnik XYZ?

Lze tato rizika na českém trhu pojistit?

Je podnik proti těmto rizikům chráněn pojištěním, případně řídí tato rizika jinak?

přístup

Ověřit, zda má podnik XYZ sjednáno pojištění v rozsahu, které dostatečně chrání jeho podnikatelské aktivity proti rizikům, kterým je v současnosti věnována světově i regionálně největší pozornost. Poskytnout podniku zpětnou vazbu.

Postup řešení

zdroj	získávání	zpracování
Odborné literární zdroje Odborné články Internetové zdroje Instituce Statistiky Pojistné podmínky vybraných pojišťoven Informace získané od podniku XYZ	Knihovna ČNB Science Direct Internet obecně Webové stránky institucí a vybraných pojišťoven	Získání teoretických znalostí Rozbor pojistných podmínek Kontrola současných pojistných smluv Dotazník pro podnik XYZ Vyhodnocení Udělení doporučení

Výsledky práce

Z výsledků práce vyplynulo, že:

- →Kybernetické pojištění nabízí z vybraných pěti pojišťoven pouze dvě
  - →Kybernetické pojištění kryje mimo jiné také náklady na IT specialisty, PR a právní služby, přerušení provozu, výkupné, obnovu dat a software, sankce za porušení GDPR
  - →Podnik XYZ využívá téměř všech prvků základních ochrany, ne však úplně všechny
- →Pojištění přerušení provozu z důvodu pandemie není na českém trhu nabízeno. Jediná Kooperativa nabízí přerušení provozu z důvodu úředního zásahu.
  - →Standardně pojištění kryje finanční ztráty pouze z důvodu věcné škody z pojištěného rizika u stejné pojišťovny
  - →Podnik má nastavenu opatření pro případ další vlny pandemie
- →Nabídka pojištění přírodních události je na českém trhu již velmi standardizovaná
  - →Podnik XYZ provozuje činnost v pronajaté budově, která není ohrožena přírodními vlivy
- →Podnik XYZ není pojištěn na žádné z daných rizik

Doporučení

Na základě výsledků jsou podniku XYZ doporučeny následující kroky:

1. **Zvážení sjednání kybernetického pojištění a pojištění přerušení provozu z důvodu kybernetického incidentu**

2. **Zavedení dalších preventivních opatření proti kybernetickým hrozbám**

3. **Nadále věnovat pozornost dodržování nařízení GDPR**

Závěr

Práce přinesla zejména nový pohled na řízení rizik v podniku XYZ. Současné řízení rizik v podniku XYZ je na vysoké úrovni, přesto je tu ale prostor pro další zlepšení. Podniku XYZ proto byla udělena konkrétní doporučení, která by měl podnik zvážit.

Novým řešením je více se při řízení rizik zaobírat hlavními trendy v oblasti podnikatelských rizik, která lze pojistit, a která jsou minimálně pro následujících několika let jasné. Každý podnik, nejen podnik XYZ by toto měl zohlednit v rámci svého procesu řízení rizik.


VŠEM
VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU
DĚKUJI ZA POZORNOST