Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Návrh algoritmu pro stanovení pojistné hodnoty z pohledu kybernetické bezpečnosti

Design of Algorithm for the Determination of Insurance Value from the Perspective of Cyber Security

Disertační práce

Autor:	Ing. Lukáš Pavlík
Studijní program:	Inženýrská informatika
Studijní obor:	Inženýrská informatika
Školitel:	doc. Ing. Luděk Lukáš, CSc.

Zlín, září 2019

PROHLÁŠENÍ

Prohlašuji, že jsem disertační práci na téma Návrh algoritmu pro stanovení pojistné hodnoty z pohledu kybernetické bezpečnosti vypracoval samostatně pod vedením pana docenta Luďka Lukáše za použití literatury a zdrojů, které jsou k dispozici v seznamu použité literatury a zdrojů na konci disertační práce.

ABSTRAKT

Disertační práce je zaměřena na problematiku informační bezpečnosti z pohledu pojištění proti kybernetickým hrozbám. Hlavní částí práce je návrh algoritmu pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví a jeho následné ověření. Navržený algoritmus je založen na principu ocenění identifikovaných ohrožených prvků organizace a analýzy vybraných scénářů kybernetických hrozeb, včetně určení nejzávažnějšího scénáře. Výstupem tohoto algoritmu je stanovení finančních dopadů na vybrané ohrožené prvky organizace, které mohou být použity pro výpočet pojistné hodnoty. Vyjádření potenciálních dopadů kybernetických hrozeb je také založeno na analýze informačního prostředí organizace, statistických ukazatelích a pravděpodobnostních modelech.

Klíčová slova: riziko, pojistná hodnota, hrozba, scénář, informační systém, ohrožený prvek, kybernetický incident.

ABSTRACT

The thesis is focused on the issue of information security from the perspective of insurance against cyber threats. The main part of the thesis is a proposal of an algorithm for determining the insurance value resulting from the impact of selected cyber threats on the organization from the perspective of insurance and its subsequent verification. The proposed algorithm is based on the valuation principle of identified vulnerable elements of the organization and analysis of selected cyber threat scenarios, including determining the most serious scenario. The output of this algorithm is to determine the financial impact on selected vulnerable elements of the organization that can be used to calculate the insurance value. The expression of potential impacts of cyber threats is also based on an analysis of the organization's information environment, statistical indicators, and probabilistic models.

Keywords: risk, insurance value, threat, scenario, information system, endangered element, cyber incident.

OBSAH

ÚVOD

Ochrana informačních systémů, dat a organizací je aktuálním problémem kybernetické bezpečnosti především z pohledu společenského a ekonomického dopadu. Vznik a realizace kybernetických incidentů může narušit nejen informační systém a jeho prvky, ale také jiné oblasti organizace, které úzce souvisí se zajištěním její činnosti. K řešení vzniku a dopadů těchto nežádoucích událostí je možné aplikovat pojištění, které je zaměřeno na kompenzaci škod a obnovu související s kybernetickými incidenty. Klíčovou částí celého pojišťovacího procesu je stanovení pojistného plnění, tedy pojistné hodnoty. Pro stanovení výše pojistné hodnoty je nezbytné využít jak přístupů typických pro oblast pojišťovnictví, tak také např. pro oblasti informačních technologií nebo bezpečnosti. A právě tento přístup ke stanovení výše pojistné hodnoty se jeví jako zásadní problém v současné oblasti pojištění.

Pro stanovení výše pojistné hodnoty pro jednotlivé organizace je využíváno především matematického aparátu. Tento přístup je také doplněn o dotazníky, které jsou vyplňovány samotnou organizací, a také statistickými údaji o dané problematice. V disertační práci je navržen a rozvíjen přístup pro stanovení výše pojistné hodnoty, který je koncipován na principu oceňování vybraných prvků organizace. Tyto prvky představují důležité oblasti, jejichž narušení vlivem kybernetického incidentu může způsobit ochromení nebo výrazné narušení informačního systému organizace a dalších významných aktiv. Další částí navrhovaného algoritmu je charakteristika vybraných kybernetických scénářů, které jsou ve vzájemných interakcích porovnávány s identifikovanými ohroženými prvky organizace. Pro tyto účely je využíváno analytických metod, prostřednictvím kterých je prováděno modelování této interakce. Výsledkem celého procesu je identifikace nejzávažnějšího scénáře kybernetické hrozby pro organizaci, a to na základě dopadů na vybrané ohrožené prvky. Posledním krokem je stanovení možné výše finančních škod v případě jeho realizace. Výstupy algoritmu je poté možné aplikovat v procesu stanovení výše pojistné hodnoty pro jednotlivé organizace.

Navržený algoritmus v rámci své funkce propojuje problematiku informačních a komunikačních technologií, oblasti bezpečnosti a ochrany dat a také právních a ekonomických aspektů, které v současné době v oblasti pojištění kybernetických hrozeb absentují. Navrhovaný algoritmus, který je určen primárně pro pojišťovny, lze také využít pro samotné organizace, které mohou pomocí jeho aplikování zjistit svou bezpečnostní úroveň a možný dopad případného kybernetického incidentu. Uplatnění může najít také v agenturách, které poskytují služby v oblasti analýzy informačního prostředí pro pojišťovny a zajišťovny. V neposlední řadě lze práci doporučit akademické a vědecké sféře nebo také laické veřejnosti, která se zajímá o danou problematikou.

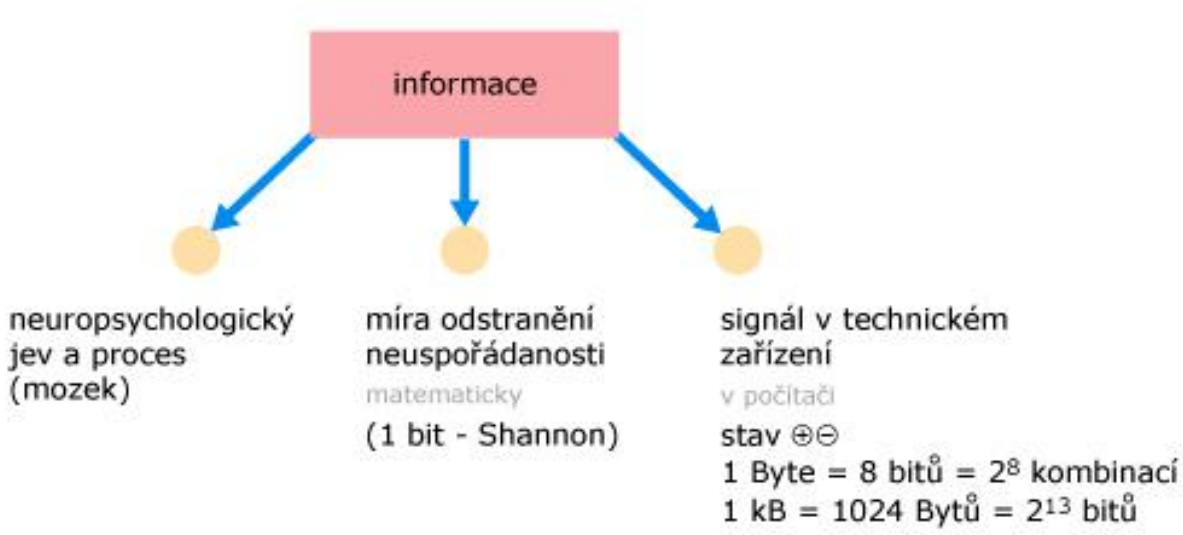
1. ZHODNOCENÍ SOUČASNÉHO STAVU

V této kapitole je analyzována základní problematika, která souvisí s pojištěním kybernetických hrozeb v organizaci. Jsou zde popsány základní pojmy z oblasti informačních systémů a kybernetické bezpečnosti. Dále je zde charakterizován současný stav v oblastí pojištění kybernetických hrozeb a také legislativní rámec, který úzce souvisí s danou problematikou.

1.1 Informační systém a jeho význam pro organizaci

1.1.1 Informace

Pojem informace lze charakterizovat jako údaje, které jsou specifikovány a organizovány za účelem prezentace v kontextu, který má konkrétní význam a smysl. Informace snižuje entropii (tedy neurčitost) a je součástí všech komunikačních procesů. U informací je rovněž důležitá obsahová charakteristika (formát, přesnost a význam pro danou aplikaci, důvěrnost, dostupnost a integrita), (Kolouch, 2016; Šilerová a kol. 2016).



Obr. 1.1: Znázornění pojmu informace (Skokan a Šedinová, 2008)

Tento výklad pojmu informace je zúžený, v širším pojetí lze informaci chápat také jako sociálně psychologický jev a proces.

1.1.2 Informační systém

Definic, které charakterizují informační systém, je mnoho. Lze říci, že se jedná o personálně technický systém, jehož prvky jsou subjekty (informatici, uživatelé), technické prostředky (počítače, servery), data a metody (software), které koordinovaně zabezpečují funkce systému s využitím technologií. Informační

systém lze charakterizovat také jako celek složený z hardwaru a softwaru, k němuž patří také lidé, kteří tento hardware a software také využívají, a činnosti a procesy, které při tom vykonávají, a to za účelem šíření potřebných informací k plánování, řízení a rozhodování. Z hlediska pozice informačního systému v řídicí soustavě se rozlišuje, na jaké úrovni informační pyramidy se nachází. Na nejnižším stupni pyramidy se nacházejí informační systémy, které zpracovávají konkrétní údaje organizace na úrovni úloh, tj. jsou známé přesné algoritmy řešení. Na nejvyšším stupni pyramidy jsou takové informační systémy, které řeší problémy organizace, u nichž je potřeba znalostí externích odborníků. Tyto problémy jsou řešeny pomocí znalostního modelování s využitím expertních modelů (Čandík, 2016).

Informační pyramidu zpravidla tvoří tyto informační systémy:

- transakční systémy,
- informační systémy pro řízení,
- systémy pro podporu rozhodování,
- informační systémy pro vrcholové řízení,
- strategické informační systémy,
- prognostické systémy.

1) **Transakční systémy** (TPS – Transaction Processing System)

Jedná se o pokračovatele klasických dávkových systémů, které měly za úkol mechanizovat konkrétní úlohy agendy, jako např. účetnictví, evidenci, skladové systémy apod. Převážná práce s daty je vykonávána ihned po jejich vložení. Velká část informačních systémů, které jsou běžnými uživateli využívány v každodenním životě, jsou právě tohoto typu (Janíček a Jíša, 2013).

2) **Informační systémy pro řízení** (MIS – Management Information System)

Svůj původ mají v ekonomických a účetních systémech. Jejich hlavním úkolem je zpřístupnit různé součtové sestavy nebo přehledy (počty objednávek, zisk v jednotlivých měsících, přehledy o provozu dílen apod.), (Janíček a Jíša, 2013).

3) **Systémy pro podporu rozhodování** (DSS Decision IS)

Jsou určitou nadstavbou pro MIS. Jejich posláním je umožnit různé analýzy, aby řídící pracovníci mohli přijímat důležitá rozhodnutí (Janíček a Jíša, 2013).

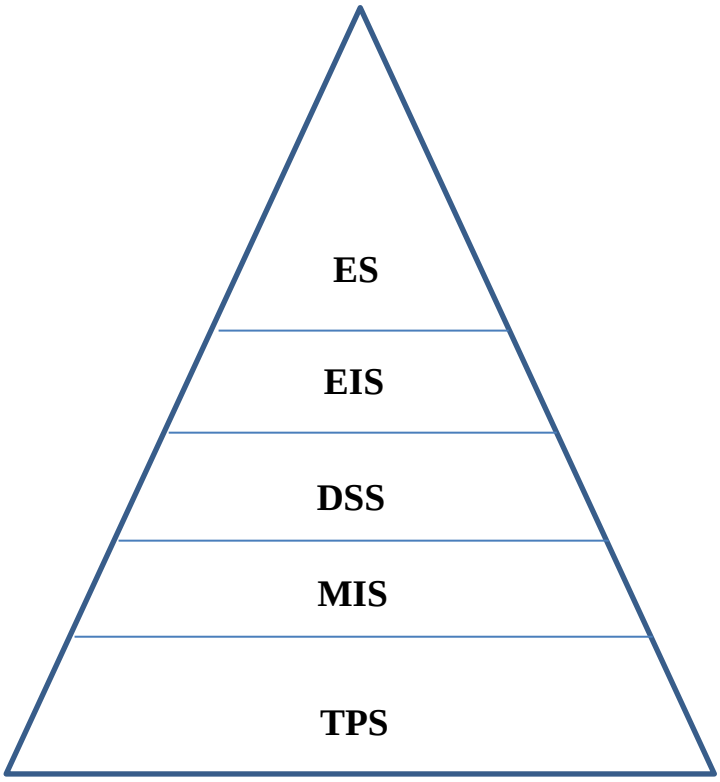
4) **Informační systémy pro vrcholové řízení** (EIS – Executive IS)

Jejich hlavním úkolem je poskytovat řídícím pracovníkům informace, které jsou nezbytné pro rozhodování na strategické úrovni, pro budoucnost a vývoj podniku a schopnost řešit tak úlohy diagnostického charakteru (Janíček a Jíša, 2013).

5) **Expertní systémy** (ES)

Tyto systémy jsou tvořeny nástroji, které dovolují provádět analýzu typu „co když“ a tím vytvářet prognózy. Patří sem např. expertní systémy, které jsou často považovány za zvláštní druh informačních systémů (Janíček a Jíša, 2013).

Na následujícím obrázku je znázorněna pyramida s jednotlivými informačními systémy.



Obr. 1.2: Informační pyramida (vlastní zdroj)

Informačních systémy v podnikovém prostředí můžeme rozdělit do několika skupin. Tyto skupiny jsou navrženy z hlediska úlohy IS a typu uživatelů, kteří s nimi pracují. Na každé úrovni řízení organizace je nutné zpracovávat odpovídající data a informace, které zaměstnanci potřebují pro realizaci své práce. Výše uvedené informační systémy jim tuto úlohu mohou usnadnit a přispět tak k zlepšení a zkvalitnění podnikových procesů.

Dále je možné členit informační systémy z holisticko-procesního pohledu (podle jejich uplatnění) na:

ERP (Systémy pro plánování podnikových zdrojů)

- jedná se o jádro informačního systému obsluhující interní podnikové procesy,
- tento typ informačních systémů je zaměřen především na zajišťování podnikových procesů, jako je např. plánování, zásobování, marketing, finance, personalistika apod.
- pojem ERP označuje zároveň také software, který tyto činnosti zajišťuje.

CRM (Systémy pro řízení vztahu se zákazníky)

- systém pro obsluhu procesů se zaměřením na komunikaci se zákazníky,
- jedná se o databázi, která slouží pro zpracovávání, shromažďování a ukládání informací o zákaznících,
- tyto informace se mohou týkat např. zvyklosti a potřeby konkrétních zákazníků.

SCM (Systémy pro správu dodavatelského řetězce)

- systém pro řízení dodavatelského řetězce,
- SCM systémy umožňují vytvářet prostor pro sdílení informací týkajících se marketingu, technologií nebo obchodních postupů,
- součástí tohoto systému může být i APS (Advanced Planning and Scheduling), systém určený pro rozvrhování a plánování výroby (Pohanka, 2013; Bruckner a kol., 2012).

Systémy typu ERP, SRM a SCM jsou definovány jako podnikové informační systémy, které jsou určeny pro zajišťování procesů v organizaci. Každý z těchto typů IS je schopen pokrýt široké množství operací, které lze zařadit mezi klíčové činnosti pro zajištění základních funkcí podniku. Narušení funkce těchto informačních systémů může mít velké dopady na fungování celé organizace ve všech jejich oblastech.

1.1.3 Informační systém a jeho bezpečnost v prostředí organizace

Informační systém tvoří základní páteř pro řízení organizace. Všechny organizace, které chtějí budovat svou pozici v oblasti, ve které působí, musí především dosahovat svých hlavních cílů, jako např. zisku. Pro zajištění dosažení těchto cílů, je nutné věnovat dostatečnou pozornost rozvoji svých informačních systémů. Faktory, které podněcují k rozvíjení a inovování podnikových informačních systémů, jsou vyvolány charakterem současného podnikatelského prostředí a významem informací v tomto prostředí (Basl a Blažíček, 2012).

Informace a znalosti se staly jedním z nejcennějších podnikových aktiv. Tato skutečnost je dána také tím, že se velmi dynamicky mění segmenty trhů, mění se obchodní komodity a také se objevuje nová konkurence. Využívání informací v této sféře je jedním ze základních předpokladů udržitelnosti a konkurenceschopnosti. Oblastí, která úzce souvisí se zajištěním fungování informačních systémů a ochrany dat, je informační bezpečnost. Informační bezpečnost je již nedílnou součástí bezpečnostní politiky moderních organizací, a proto je tomuto druhu bezpečnosti věnována velká pozornost (Smejkal 2018; Kolouch 2016).

Informace z pohledu významnosti v prostředí organizací představuje určité „know-how“, které je třeba chránit. Pro zneužití a získání informací v konkurenčním podnikovém prostředí je využívána řada technik, jako např. špionáž, hacking nebo sociální inženýrství. Tyto techniky slouží k získání citlivých informací od subjektů (např. know-how), které mohou mít pro útočníka důležitý význam. Prostřednictvím získání specifických citlivých informací může být poškozena nejen dobrá pověst organizace, ale také obchodní vztahy. Tato skutečnost je pro každou organizaci tou nejhorší variantou.

Samozřejmě to, jak je riziko napadení informačního systému organizace vysoké, závisí na několika faktorech, kterými jsou:

a) zranitelnost informačního sytému,
b) úroveň ochrany bezpečnostního systému,
c) druh napadení informačního systému (Smejkal 2018, Kolouch 2016).

ad a) Zranitelnost informačního systému

Zranitelnost informačních systémů představuje jejich nejslabší místo. Jedná se v podstatě o zranitelná místa těchto systémů především z pohledu funkčnosti. Velkým nedostatkem bývá nedokonalost organizačního zázemí, tzn. dokumentování (formalizace) všech procedur a informačních toků. Lze také predikovat, že většina správců a administrátorů informačních sítí nemá k dispozici havarijní plány. Stejně tak málo institucí má k dispozici kvalifikovaný bezpečnostní management (Varadzin, 2011).

Specifickou oblastí posuzování zranitelnosti organizačního prostředí je personální management. Této oblasti ale není zatím věnována dostatečná pozornost, a to i navzdory kriminálním událostem posledních několika let. Pozornost je v této oblasti zatím věnována především logickému prostředí. Bezpečnostní manažeři by měli brát v úvahu, že některá hardwarová vybavení mají vlastnosti Fault Tolerant System, některá jsou certifikována, budují se např. i záložní výpočetní centra apod. (Varadzin, 2011).

Začínají se také aplikovat řízené přístupy k objektům a začíná se projevovat odklon od přístupových hesel směrem k využívání personálních inteligentních čipových karet (Smart Cards). Ve vztahu k minimalizaci zranitelnosti komunikačního prostředí (z pohledu dostupnosti) dnes řada organizací využívá

záložních přenosových cest. Některé z organizací také do své bezpečnostní politiky zavádějí šifrování datových přenosů (Varadzin, 2011).

Ad b) Úroveň ochrany informačního systému

Některé z organizací uplatňují odborně provedenou výstavbu bezpečnostního systému jako jedno z bezpečnostních hledisek. Takový zásadní krok vyžaduje ze strany managementu zájem o řešení problematiky informační bezpečnosti na straně jedné a na straně druhé přijetí dlouhodobého plánu rozvoje v této oblasti (Čermák, 2009).

Realizace tohoto plánu předpokládá v první fázi především provedení analýzy, na jejímž základě by měla být navržena bezpečnostní politika, popř. vypracován bezpečnostní projekt. Výstavba navrženého bezpečnostního systému se pak provádí buď na základě projektu, nebo podle závěrů bezpečnostní analýzy. Kvalitní ochrana informací a informačních systémů je nejen vizitkou dané organizace, ale také předpokladem bezproblémových auditů prováděných např. s cílem získat ISO 9001 (Čermák, 2009).

Ad c) Druhy napadení informačního systému

V současné době dochází k rozšiřování technického a programového vybavení a také ke stále častějšímu výskytu bezpečnostních děr. Velmi alarmující jsou výsledky statistik, podle kterých až 90 % realizovaných útoků na informační systém, pochází zevnitř organizace. V současnosti je popsáno více než 800 způsobů, kterými lze napadnout informační systém. Tyto útoky se liší cílem a použitými prostředky (Kolouch, 2016).

Jedná se např. o:

d) sociální inženýrství,
e) červy,
f) viry typu trojan,
g) code injections attack,
h) botnet,
i) zamezení přístupu ke službě (denial of service),
j) phishing,
k) vishing,
l) smishing,
m) rogueware,
n) hoax,
o) cracking,
p) spam,
q) fyzický útok zloděje,
r) ukradení identity apod. (Kolouch, 2016)

Graf. 1.1: Nejčastější typy kybernetických hrozeb na SME organizace (CIO & Leader, 2017)

1.1.4 Shrnutí

Informace je v současném světě chápána jako aktivum, které má pro jednotlivce, organizace nebo celou společnost velký význam. Z tohoto důvodu je kladen velký důraz na jejich ochranu a bezpečnost. V organizacích lze nalézt mnoho typů informačních systémů, jejichž účel a funkce se významně liší. Z tohoto důvodu se také rozvíjí možnosti a druhy útoků na informační systémy.

Každý informační systém se skládá z několika prvků, které tvoří jeho platformu pro zajištění funkce a dosahování předem stanovených cílů. Každý z těchto prvků plní svoji funkci a jakákoliv porucha nebo znemožnění jeho fungování by mohlo ohrozit zajištění funkce celého informačního systému. Na informační systém a jeho architekturu se lze dívat ze dvou možných pohledů, a to z horizontálního pohledu a vertikálního. Každý z těchto pohledů může umožnit organizaci lepší pochopení svého informačního prostředí a může se tak lépe chránit před možnými kybernetickými hrozbami.

Informační systémy jsou nezastupitelným článkem struktury organizace. Jejich napadení nebo oslabení základních funkcí může způsobit narušení základních procesů a mechanismů v organizaci. Tuto skutečnost již vnímá většina organizací, a proto je této problematice věnována náležitá pozornost.

Ochrana informačního systému se stává jednou z priorit efektivního řízení a fungování organizace. Druhy útoků a napadení informačních systémů a jejich částí se neustále vyvíjí, a proto je nutné také vyvíjet nové metody a nástroje ochrany. Jedním z takových způsobů, jak řešit dopady kybernetických hrozeb na informační prostředí organizace, může být jejich pojištění proti těmto typům nežádoucích situací.

1.2 Problematika kybernetické bezpečnosti z pohledu pojišťovnictví

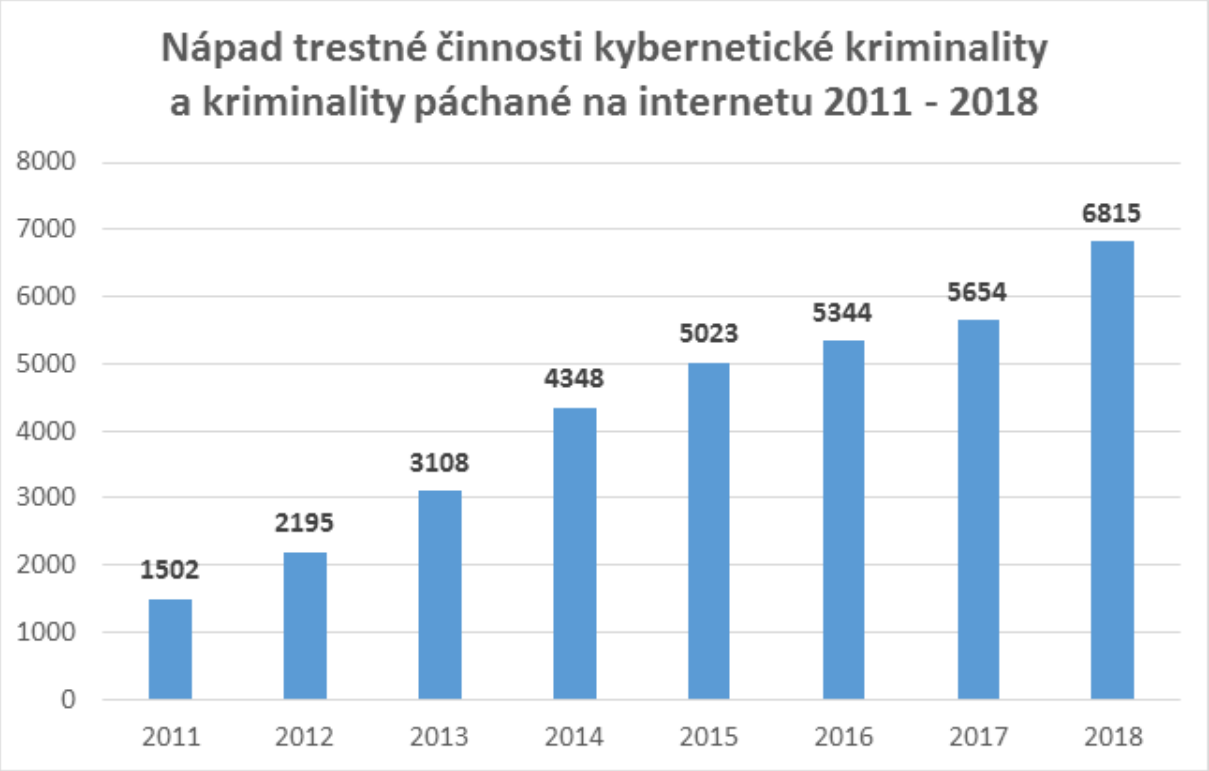
Kybernetické hrozby jsou v současném světě problematikou, která vyvolává mnoho otázek a diskusí. Z pohledu pojišťovnictví se jedná o poměrně novou oblast, která je na vzestupu. Pojistné produkty pojišťoven jsou v současné době nastaveny na několik typů hrozeb, které by měly pokrýt. Nejprve je ale důležité charakterizovat některé pojmy, které s touto problematikou souvisí (Kreuzer, 2018; Marotta et al., 2017).

1.2.1 Kybernetický prostor

Kybernetický prostor podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů je charakterizován jako digitální prostředí, v němž probíhá zpracování a výměna informací prostřednictvím ICT technolgií. Toto prostředí je tvořeno informačními systémy, ale také jinými elektrotechnickými a telekomunikačními zařízeními, které mohou být cíleně napadnuty nebo poškozeny (Zákon č. 181/2014 Sb.).

1.2.2 Kybernetická kriminalita

Kybernetická rizika jsou v současném světě problematikou, která vyvolává mnoho otázek a diskusí. Velmi často je kybernetická kriminalita považována za nový druh kriminality, nicméně značná část kybernetické kriminality využívá či přenáší již známé druhy protiprávního jednání (např. podvody, porušování práv autorských, krádeže, šikanu aj.) do prostředí informačních a komunikačních technologií, ve kterém je lze aplikovat „lépe, rychleji, efektivněji“ než ve světě reálném. Mezi ryze kybernetické útoky by pak bylo možné zařadit např. hacking, DoS a DDoS útoky, botnety aj. (Kolouch, 2016). Na následujícím obrázku můžeme vidět nárůst činnosti kybernetické kriminality a kriminality páchané na internetu od roku 2011 do roku 2018 na území České republiky (Smejkal, 2018).



Graf 1.2: Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu 2011 – 2018 (Policie ČR - Národní centrála proti organizovanému zločinu SKPV, 2019)

1.2.3 Kybernetické riziko

Obecně lze říci, že riziko vyjadřuje míru ohrožení sledovaného aktiva, tj. míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku, který vede ke vzniku škody. Výše rizika je určena cenou sledovaného aktiva, resp. následkem pro jeho vlastníka nebo celou organizaci, zranitelností aktiva a pravděpodobností vzniku hrozby (Smejkal a Rais, 2013, Tichý 2006).

Na riziko v oblasti kybernetické bezpečnosti lze nahlížet z různých úhlů pohledu. Je možné jej chápat obecně jako riziko, které je vlastní všem aktivitám v kyberprostoru. Touto definicí bychom narušili všechny hranice mezi jednotlivými druhy rizik, jelikož musíme zohledňovat při výpočtu i ostatní rizika (provozní, pojistně-technické riziko apod.). Je to z toho důvodu, že téměř všechny operace v současných organizacích probíhají v digitálním světě. Tento pohled je velmi technický a odvíjí se od zaměření na základní funkční principy informačních systémů. Na základě této úvahy pak lze odvodit, že kybernetické riziko je rizikem ovlivňujícím svým následkem neporušenost, diskrétnost, prokazatelnost, nepopíratelnost, dostupnost, důvěrnost a integritu informace (Smejkal a Rais, 2013).

1.2.4 Kybernetická hrozba

Pojmem kybernetická hrozba můžeme označit negativní událost kybernetického charakteru, která může ohrozit určitý druh aktiva. Kybernetickým charakterem je myšlena podstata hrozby, která vychází z kybernetického prostoru a je realizována prostřednictvím nástrojů informačních a komunikačních technologií. Každá kybernetická hrozba může způsobit ztrátu, kterou lze vyjádřit finančními prostředky (např. poškození technických komponent informačního systému). Základní charakteristikou kybernetické hrozby je její úroveň, která určuje míru schopnosti hrozby způsobit škodu (Čermák, 2009).

1.2.5 Pojištění organizací proti kybernetickým hrozbám – charakteristika pojištění

Kybernetické útoky již v dnešní době nejsou cíleny pouze na internetové firmy. V ohrožení je v podstatě kdokoliv, kdo pracuje s daty. Významnost kybernetické bezpečnosti pro úspěšnost podnikání je srovnatelná s fyzickou bezpečností. Zatímco proti krádeži nebo poškození se firmy mohou pojistit, tak v případě vlastních zákaznických dat je situace složitější (Ponemon study, 2018; Čermák, 2009).

V České republice nebyl produkt týkající se pojištění kybernetických hrozeb do roku 2013 nabízen. Od roku 2013 jej začala nabízet pobočka americké pojišťovny AIG v Praze v podobě produktu Cyber Edge. S platností legislativy GDPR (General Data Protection Regulation) byl v České republice zaznamenán nárůst tohoto typu pojištění pro malé a střední organizace (tzv. SME). Mezi pojišťovny, které mají ve svém portfoliu tento typ pojistného produktu na tuzemském trhu, patří také společnosti Renomia nebo Kooperativa (Moláček a Konečný, 2017).

V zahraničí je ale situace jiná. V USA, Německu a Velké Británii je množství takových nabízených pojistných produktů vyšší a stejně tak i počet firem, které si jej sjednají. Poměrně velkým problémem je nepoměr částek, ve kterých se vyplácí pojistné krytí. Dohromady tato částka v USA činí 2,45 mld. dolarů, což je 68,2 mld. korun. I tato částka je ale ve skutečnosti nedostatečná. Podle poradenské společnosti PWC totiž 90 % pojistného připadá na americké firmy. Přitom má pojištění proti škodám jen třetina firem v USA (PWC – Insurance 2020 & beyond, 2015; Franke, 2017).

1.2.6 Rozsah krytí a kompenzace škod pojištění proti kybernetickým hrozbám

Pojištění kybernetických hrozeb je ve své podstatě kombinací **majetkového** pojištění (tzn. poskytování pojistného plnění za škody způsobené pojištěnému) a pojištění **odpovědnosti za škodu**, kdy jsou hrazeny škody způsobené třetím osobám.

Pojištění poskytuje pojistnou ochranu před:

- únikem osobních údajů, informací a dat z informačního systému firmy, ať již náhodného charakteru nebo z nedbalosti,
- cíleným napadnutím informačního systému třetími osobami nebo zaměstnanci za účelem získání přístupu k citlivým informacím (Smejkal, 2018. AIG 2018).

Škody, které lze z pojištění proti kybernetickým hrozbám hradit

Současné pojistné produkty jsou nastaveny na krytí následujících škod:

- škody pojištěného způsobené únikem citlivých korporátních dat a informací,
- náklady pojištěného na oznámení úniku osobních údajů, informací a dat dozorovým orgánům a veřejnosti a komunikace s postiženými klienty sloužící k ochraně dobré pověsti společnosti,
- náklady pojištěného na identifikaci úniku osobních údajů a informací, zabezpečení běžného provozu informačního systému firmy a realizace opatření k nápravě nedostatků, které způsobily únik,
- škody třetích stran v souvislosti s únikem,
- náklady pojištěného na jednání s dozorovými orgány a jimi udělené pokuty,
- ztráty zisku pojištěného v důsledku webových nebo síťových služeb a úniku osobních údajů a dat (Smejkal, 2018; AIG, 2018).

1.2.7 Možnosti sjednání pojištění proti kybernetickým hrozbám

Pojištění proti kybernetickým hrozbám je řešeno pojistnou smlouvou, stejně jako jiné druhy pojištění, ve které jsou stanoveny podmínky a rozsah pojistného krytí. Podle přání pojistníka je možné sjednat i smluvní ujednání, které se liší od pojistných podmínek tak, aby pojistné krytí reagovalo na konkrétní situaci a jeho potřeby. Při sjednání pojištění je samozřejmě klíčové rozpoznání hrozeb, se kterými se zájemci o pojištění kybernetických hrozeb mohou setkat (AIG, 2018).

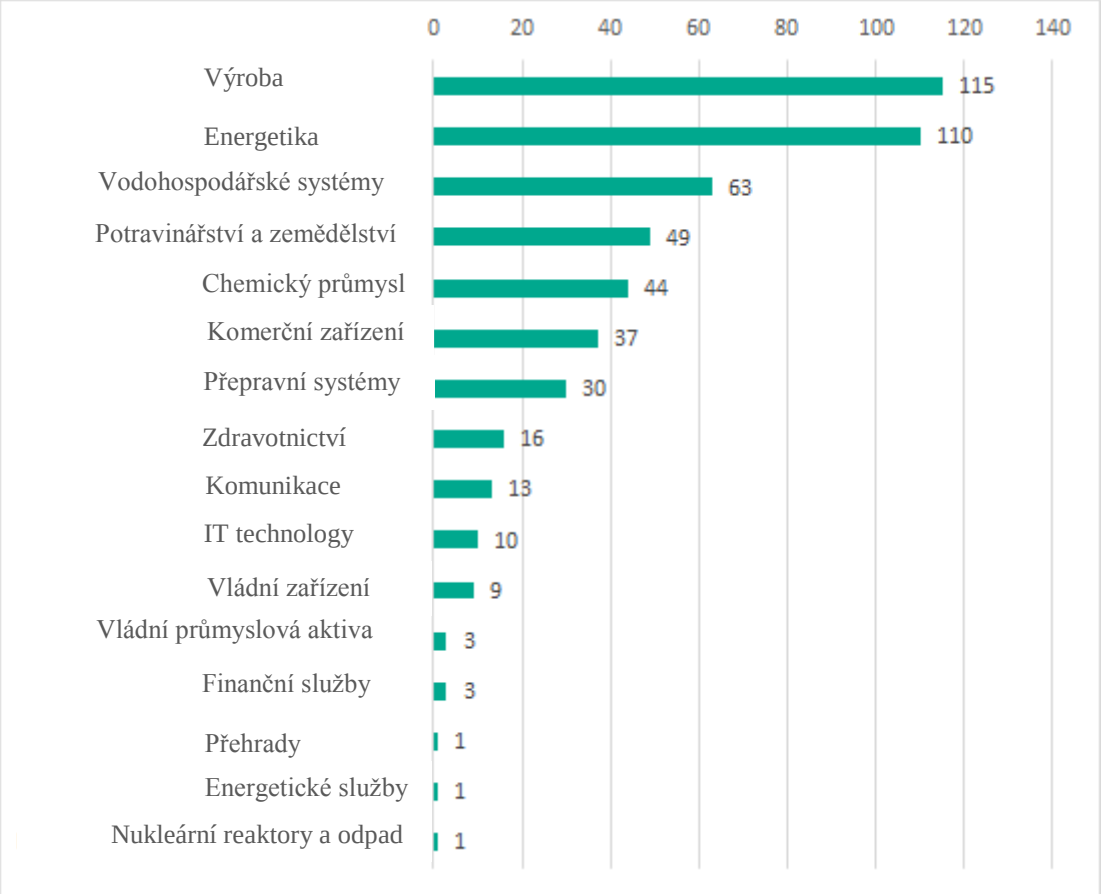
Velmi důležitou roli hraje dotazník pojistitele, který zájemce o pojištění vyplňuje. V dotazníku jsou uvedeny informace týkající se oboru činnosti pojistníka, údajů a typů dat, se kterými společnost pracuje a které shromažďuje o svých klientech. Pojistitel také úzce spolupracuje s IT společností, která přispívá k vyjasňování určitých specifik na straně zájemce o pojištění (AIG, 2018).

Pojistit společnost proti kybernetickým hrozbám je v současné době velmi riskantní. Zatímco potenciálně vzniklé škody jsou podle pojišťoven a jejich měřítek srovnatelné s velkými přírodními katastrofami, výskyt kybernetických incidentů je v tomto případě mnohem vyšší. V České republice se této skutečnosti pojišťovny obávají, tudíž zde není nabídka tohoto typu pojištění na trhu tak velká.

Na druhou stranu lze konstatovat, že jistý zájem ze strany firem zde existuje, ale obvykle k němu dochází až po zveřejnění nějaké mediální kauzy spojené s únikem nebo zneužitím dat. Organizace si uvědomují, že je zde určitá hrozba v podobě cíleného kybernetického útoku, ale většinou pod nátlakem další operativy tuto skutečnost odsouvají na neurčito. Danou oblast většinou řeší až tehdy, když nastane vážný bezpečnostní problém (AIG, 2018; Moláček a Konečný, 2018).

1.2.8 Charakteristika pojišťovaných subjektů

Pojištění proti kybernetickým hrozbám lze poskytnout jakékoliv organizaci, bez ohledu na obor jejího podnikání nebo fungování. Nechat si pojistit svá data tedy může jak výrobní podnik, tak např. univerzita nebo krajský úřad. Je důležité poznamenat, že pojištění proti kybernetickým hrozbám se vztahuje na pojištění dat třetích stran. Tato skutečnost znamená, že mohou být pojištěna data týkající se např. osobních údajů o zákaznících nebo studentech, nikoliv samotné „know-how“ organizace (Ponemon study, 2018). Tento typ pojištění nachází své uplatnění také ve veřejném sektoru. V grafu 1.3 jsou uvedeny sektory podle počtu zranitelných prvků z hlediska napadení kybernetickými hrozbami. Jak můžeme vidět, oblast výroby, energetiky nebo vodohospodářství patří mezi nejvíce zranitelné cíle vůči kybernetickým útokům, a proto pojištění proti kybernetickým hrozbám může pomoci dopady těchto nežádoucích událostí snížit (Kaspersky Lab ICS CERT, 2019).



Graf 1.3: Počet zranitelných prvků, používaných v různých průmyslových odvětvích (Kaspersky Lab ICS CERT, 2019)

1.2.9 Shrnutí

Pojišťování informačních systémů proti kybernetickým hrozbám v organizaci je novou oblastí, která se postupně rozvíjí. Jak již bylo řečeno v předchozích podkapitolách, možnosti napadení informačních systémů se neustále rozvíjí, a proto bylo identifikováno několik hrozeb, na které se může pojištění kybernetických hrozeb vztahovat. Předmětem pojištění kybernetických hrozeb může být jakákoliv organizace, jako např. výrobní podnik, univerzita, mobilní operátor apod. Pro splnění pojistitelnosti konkrétní organizace musí být dodrženy minimální požadavky na zabezpečení informačních systémů a jejich prvků, jako je např. používání antivirové ochrany, provádění zálohování, pravidelná změna hesel nebo šifrování dat.

1.3 Pojištění kybernetických hrozeb z pohledu legislativy

Z pohledu legislativy je oblast pojištění proti kybernetickému riziku transdisciplinární oblastí. V rámci řešení této problematiky dochází ke kombinaci legislativy jak z oblasti pojišťovnictví, tak z oblasti bezpečnosti a ochrany dat. Můžeme zde nalézt např. nařízení a směrnice z Evropské unie a také legislativu jednotlivých států, která tuto problematiku reguluje.

Mezi nejvýznamnější dokumenty v oblasti pojištění proti kybernetickému riziku patří:

- Nařízení Evropské unie 2016/679,
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů,
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti,
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148,
- Zákon č. 110/2019 Sb. o zpracování osobních údajů.

1.3.1 Nařízení Evropské unie 2016/679

Jedná se o nejnovější legislativní opatření v oblasti bezpečnosti a ochrany dat. Tato direktiva je oficiálně platná od května 2018 v Evropské unii, ale většina organizací se na její zavedení začíná připravovat až teď. GDPR klade větší důraz na ochranu dat, které mohou sloužit k identifikaci jednotlivce. Může se tedy jednat o bankovní účet, fotografie, e-mail apod. (Nařízení Evropské unie 2016/679).

Hlavním cílem tohoto nařízení je zajistit větší kontrolu a zodpovědnost za data, se kterými organizace pracuje.

V rámci GDPR jsou navrhována tato opatření:

- údaje musí být anonymizovány nebo zašifrovány,
- musí být zajištěny řádné procesy kontrol nad tím, jak jsou data jednotlivých klientů chráněna (tyto procesy musí být kdykoliv doložitelné),
- organizace musí být, v případě mimořádné události, schopna svůj systém a data rychle obnovit,
- organizace musí pravidelně testovat efektivitu a odolnost informačního systému (Nařízení Evropské unie 2016/679).

Problematika GDPR také zavádí mnohem vyšší sankce, než které byly doposud ze strany státu požadovány. V případě, že organizace nebude vyhovovat požadavkům tohoto nařízení, může dostat pokutu ve výši 4 % z obratu nebo 20 mil. €. Z důvodu takto vysokých sankcí pojistný trh předpokládá, že po zavedení této legislativy dojde k rapidnímu nárůstu poptávky po pojištění kybernetických rizik. Jelikož budou hrozit takto vysoké pokuty, lze předpokládat, že většina

organizací se nebude vystavovat těmto sankcím, a proto své informační systémy budou nechávat pojišťovat (Nařízení Evropské unie 2016/679; Moláček a Konečný 2018).

1.3.2 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

S problematikou kybernetických rizik v České republice také souvisí zákon o kybernetické bezpečnosti. V této legislativě jsou charakterizovány orgány, které mají povinnosti v oblasti kybernetické bezpečnosti. Jsou zde také charakterizována bezpečnostní opatření, která by měly organizace dodržovat. Je zde rovněž charakterizován kybernetický incident, evidence těchto událostí apod. (Zákon č. 181/2014 Sb.).

Ze zákona o kybernetické bezpečnosti tedy vycházejí všechny pojišťovny, jejichž cílem je poskytovat pojištění proti kybernetickým hrozbám. Jelikož je v tomto zákoně přesně definována problematika kybernetické bezpečnosti, alespoň v jejich základních principech, je tento zákon rovněž zařazen mezi základní legislativu týkající se kybernetické bezpečnosti (Zákon č. 181/2014 Sb.).

1.3.3 Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti

Tento zákon stanovuje zásady pro nakládání s utajovanými informacemi, dále pak podmínky pro přístup k utajovaným informacím a požadavky na jejich ochranu. Jsou zde také vymezeny základní pojmy v oblasti utajovaných informací, personální bezpečnost a požadavky na způsobilost týkající se přístupu k utajovaným informacím (Zákon č. 412/2005 Sb.).

1.3.4 Směrnice Evropského parlamentu a Rady (EU) 2016/1148

Tato evropská směrnice je ve své podstatě novelizovaný zákon o kybernetické bezpečnosti. Tato legislativa je zaměřena na tzv. poskytovatele základních služeb a jejich informační systémy, což mohou být instituce v oblastech energetiky, bankovnictví, dopravy, zdravotnictví, veřejné správy apod. V tomto dokumentu jsou také definováni poskytovatelé digitálních služeb nebo dopadová kritéria a jejich podmínky naplnění.

V rámci české legislativy související s kybernetickou bezpečností došlo na základě směrnice NIS k úpravě zákona o kybernetické bezpečnosti tak, aby byl v souladu s touto směrnicí. Pokuty, které mohou být uděleny za naplnění některého z dopadových kritérií ve vybraných oblastech poskytování služeb, mohou dosahovat až výše 5 000 000 Kč (Směrnice Evropské unie 2016/1148).

1.3.5 Zákon č. 110/2019 Sb., o zpracování osobních údajů

Tento zákon, který vešel v platnost 24. dubna 2019, upravuje zpracování osobních údajů podle nařízení Evropského parlamentu a Rady (EU) 2016/679. Jsou zde definovány postupy pro zpracovávání osobních údajů příslušnými orgány za účelem odhalování nebo předcházení trestné činnosti, dále pak pro zajišťování obranných a bezpečnostních zájmů České republiky nebo postavení Úřadu pro ochranu osobních údajů. V této legislativě je také upravena výše možných finančních sankcí pro území ČR. Tyto sankce mohou být do 1 000 000 Kč, do 5 000 000 Kč nebo do 10 000 000 Kč (Zákon č. 110/2019 Sb.).

1.3.6 Shrnutí

Legislativa v oblasti bezpečnosti tvoří významnou část při návrhu a realizaci pojistných produktů. V oblasti pojišťování kybernetických hrozeb je možné vycházet z několika právních zdrojů, které by měly být brány v úvahu při zavádění tohoto typu pojištění na pojistný trh. V rámci České republiky a Evropské unie je možné zmínit několik legislativních pramenů. Za velmi důležitý pramen lze považovat směrnici GDPR (General Data Protection Regulation), která vešla v platnost dne 25. května 2018. Dle současných odhadů analytických firem lze predikovat, že zájem o pojištění kybernetických hrozeb bude stoupat, a to především v souvislosti se zavedením směrnice GDPR. Rovněž je velmi důležité brát v úvahu zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve kterém jsou definovány základní pojmy z oblasti kybernetické bezpečnosti.

1.4 Závěr teoretických východisek a kritické zhodnocení současného stavu

Na základě provedených rešerší a analýz současných poznatků a oborných textů týkajících se problematiky pojištění informačních systémů proti kybernetickým hrozbám lze konstatovat, že:

- zájem o tento typ pojištění u malých a středních organizací stoupá a tento růst bude nadále pokračovat (Kreuzer, 2018),
- se jedná o novou transdisciplinární oblast kybernetické bezpečnosti, do které vstupují i jiné vědní disciplíny, jako je např. ekonomie, bezpečnost, informační technologie nebo právo,
- správné posouzení kybernetických hrozeb a jejich dopadů na organizaci je jednou z klíčových činností celého procesu pojištění,
- v současné době jsou používány metody aktuárské matematiky, které jsou velmi přínosné z pohledu pojišťovnictví a matematických výpočtů, nicméně do tohoto procesu nevstupuje problematika informačních systémů nebo bezpečnosti,

- pro přesnější vyjádření potenciálních škod v informačním prostředí organizace je nezbytné tyto skutečnosti do procesu stanovení pojistné hodnoty zahrnout, což potvrzuje i současná odborná komunita, která se touto problematikou zabývá (Kreuzer, 2018),
- postupy a matematické metody, které se v současné době používají v rámci pojištění organizací proti kybernetickým hrozbám, neutváří ucelený algoritmus nebo metodiku (jedná se o nezávislé a oddělené přístupy stanovení pojistné hodnoty, které jsou pro běžné pojistitele velmi komplikované),
- došlo k rozvoji modelů pro tvorbu pojistných cen, nicméně pokročilá tvorba ceny vycházející z ověřených historických dat a pojistně matematických modelů z oblasti pojištění kybernetických hrozeb nebyla zatím dostatečně ověřena (Kreuzer, 2018),
- pojištění informačních systémů proti kybernetickým hrozbám by mělo společně s pojistiteli především přispět k ochraně malých a středních organizací před likvidačními škodami, a to komplexně v souladu s danou rizikovou situací (Kreuzer, 2018).

Na základě výše uvedených skutečností lze konstatovat, že v oblasti pojištění absentuje postup, který by umožňoval stanovit výši ekonomických dopadů na organizaci z pohledu kybernetických hrozeb. Je proto potřebné vytvořit algoritmus, který by umožňoval stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví.

Hlavním přínosem navrhovaného algoritmu by mělo být:

- vyjádření finanční hodnoty ohrožených prvků organizace, které představují oblasti informačního prostředí, jež mohou být nejvíce zasaženy dopadem kybernetické hrozby,
- modelování dopadů vybrané kybernetické hrozby, která může na sledovaných ohrožených prvcích organizace způsobit nejzávažnější finanční škody,
- vyjádření těchto finanční škod a stanovení optimální pojistné hodnoty.

2. CÍLE DISERTAČNÍ PRÁCE

Cíle disertační práce vychází z kritického zhodnocení současného stavu v oblasti pojištění proti kybernetickým hrozbám. Na základě provedených analýz dostupných odborných materiálů, legislativního rámce a ICT nástrojů, autor dospěl k názoru, že ve zkoumané oblasti absentuje ucelený metodický postup a algoritmus, jehož aplikace v oblasti pojišťovnictví by umožňovala stanovení výše pojistné hodnoty pro organizaci vůči kybernetickým hrozbám. Tento metodický postup nebo algoritmus by měl umožnit stanovení výše potenciálních finančních škod v informačním prostředí organizace s ohledem na problematiku bezpečnosti, ekonomiky, legislativy a informačních technologií.

Pro vytvoření takového algoritmu musí autor disertační práce vyřešit tyto otázky:

a) Jaké oblasti organizace mohou být nejvíce zasaženy dopadem kybernetických hrozeb?
b) Jak stanovit finanční škody ve sledovaných oblastech ve vztahu ke kybernetickým hrozbám, které mohou organizaci ohrozit?
c) Jak vyjádřit pojistnou hodnotu, která by reflektovala dopady kybernetických hrozeb na dané oblasti?
d) Je navržený algoritmus aplikovatelný pro praxi?

Vyřešením těchto otázek je autor schopen splnit hlavní cíl disertační práce, tedy **vytvoření algoritmu pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví.**

K dosažení hlavního cíle, bude nutné splnit tyto dílčí cíle:

- identifikace kybernetických hrozeb, které mohou být součástí pojištění proti kybernetickým hrozbám,
- specifikace ohrožených prvků, které jsou ovlivněny dopadem kybernetických hrozeb a ve kterých mohou organizaci vznikat finanční náklady,
- definování způsobu ocenění specifikovaných ohrožených prvků v organizaci,
- stanovení výše finančních dopadů vybraných kybernetických hrozeb na jednotlivé ohrožené prvky na základě jejich vzájemné interakce,
- vytvoření algoritmu pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví a jeho ověření na vybraných referenčních objektech.

Omezení disertační práce:

- z důvodu rozsahu bude navrhovaný algoritmus aplikován pouze na organizace, které se nacházejí v soukromém sektoru,
- z důvodu rozsahu řešeného tématu bude výsledkem navrhovaného algoritmu stanovení pojistné hodnoty, tzn. že nebude stanoven konečný pojistný limit pro organizaci.

3. ZVOLENÉ METODY ZPRACOVÁNÍ

Pro zjištění aktuálního stavu řešené problematiky byla provedena rešerše zahraničních i tuzemských informačních zdrojů, které jsou v této problematice klíčovým zdrojem informací. K řešení disertační práce bylo použito vědeckých metod, které jsou obvyklou součástí vědeckých prací.

Využity byly především tyto metody:

- metoda analýzy a syntézy,
- metoda indukce a dedukce,
- metoda srovnávání (komparace),
- metoda analogie,
- metoda modelování,
- metoda multikriteriálního hodnocení.

a) Metoda analýzy

Analýza je jednou ze základních metod poznání, pomocí níž je konkrétní objekt rozložen na dílčí části a jsou zjišťovány vazby mezi jednotlivými částmi a celkem. Na základě analýzy můžeme vyslovit obecné závěry o určitém objektu nebo jevu. Metoda analýzy byla aplikována při identifikaci ohrožených prvků organizace.

b) Metoda syntézy

Syntéza spojuje jednotlivé části daného objektu, jevu nebo systému do jednoho celku. Jedná se o proces, kdy je vytvářen strukturovaný objekt z jeho jednotlivých prvků a jejich vzájemných vazeb. Metoda syntézy byla v disertační práci využita pro spojování jednotlivých oblastí organizace do celku, který bude dále systematicky posuzován. Tato metoda zde byla využita k vytvoření uceleného algoritmu pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví.

c) Metoda indukce

Tuto vědeckou metodu lze rovněž označit jako párovou a patří rovněž do kategorie logických metod. Pomocí indukce jsou vytvářeny obecné závěry na základě zjištěných poznatků o jednotlivých objektech nebo jevech. Induktivní úsudky umožňují dojít k podstatě zkoumaných jevů a stanovit jejich zákonitosti. Tato metoda byla v disertační práci využita především pro stanovení ohrožených prvků organizace na základě provedeného dotazníkového šetření.

d) Metoda dedukce

Prostřednictvím dedukce jsou vyvozována nová tvrzení. Jedná se tedy o opak indukce. Tyto metody byly v disertační práci použity pro stanovení závěrů na základě provedeného výzkumu a dosažených výsledků.

e) Metoda srovnávání

Tato metoda patří mezi empirické metody. Při porovnávání se posuzují shodné nebo rozdílné stránky zkoumaných objektů nebo jevů a na základě zjištěných výsledků se provádějí korekce. Tato metoda byla aplikována v disertační práci ve fázi modelování a stanovení výše pojistné hodnoty.

f) Metoda analogie

Jedná se o myšlenkový postup, při němž jsou zjišťovány shody vybraných znaků objektu nebo jevu zkoumaného celku. Tato vědecká metoda byla v disertační práci aplikována při porovnávání scénářů kybernetických hrozeb a ohrožených prvků organizace.

g) Metoda modelování

Modelování je metodou často používanou ve vědecké praxi v mnoha oborech. Cílem použití této metody je napodobit chování zkoumaného systému a ovlivnit jeho chování požadovaným způsobem. Model je vždy pouze přiblížením reálnému objektu, který může být na rozdíl od modelu mnohem složitější. Metoda modelování byla v disertační práci aplikována ve fázi porovnávání scénářů kybernetických hrozeb s ohroženými prvky organizace.

h) Metoda multikriteriálního hodnocení

Multikriteriální hodnocení je metoda, která se používá pro rozhodování mezi více variantami, přičemž se nepřipouští existence více variant řešení. Výsledkem by měla být pouze jedna varianta řešení. Předpokladem použití této metody je větší počet kvantifikovatelných kritérií, která jsou zahrnuta do hodnocení. Tato metoda byla použita pro stanovení vah u nejzávažnějších kybernetických hrozeb v organizaci.

4. TEORETICKÝ ROZBOR MOŽNOSTÍ POJIŠTĚNÍ PRO OCHRANU ORGANIZACE VŮČI KYBERNETICKÝM HROZBÁM

Ze zhodnocení současného stavu lze dedukovat, že za významný aspekt v rámci stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb z pohledu pojišťovnictví lze pokládat ocenění vybraných ohrožených prvků organizace. Tyto ohrožené prvky představují významné oblasti informačního prostředí, ve kterých mohou vlivem realizace kybernetické hrozby vzniknout organizaci vysoké náklady. V souvislosti s platností nařízení Evropské unie 2016/679 (General Data Protection Regulation) a četností kybernetických hrozeb na malé a střední organizace, se zde vytváří prostor pro rozvoj kybernetické bezpečnosti v oblasti pojistných produktů. Vzhledem k tomu, že oblast pojištění organizací proti kybernetickým hrozbám je transdisciplinární oblastí, je nutné na tento problém pohlížet také z pohledu ekonomie, práva, informačních systémů a bezpečnosti.

Na základě propojení těchto vědních disciplín je možné navrhnout algoritmus, který může být aplikován pro vyjádření potenciálních finančních škod v organizaci. Tento algoritmus může být aplikován jak v oblasti pojišťovnictví pro stanovení optimální pojistné hodnoty, tak také pro samotné organizace, které mají být proti kybernetickým hrozbám pojištěny. Organizace si mohou nechat ohodnotit svá informační prostředí a stanovit si tak možné finanční dopady pro své podnikání. Výstupem tohoto procesu je také identifikace nejzávažnější kybernetické hrozby, kterou může být konkrétní organizace zasažena.

4.1 Pojištění jako způsob ochrany a jeho podstata

Podstatou pojištění je vytvářet z finančních příspěvků zájemců o pojištění rezervy, které slouží k úhradě potřeb nebo náhradám škod, které vzniknou pojištěným vlivem nahodilých událostí. Základním účelem pojištění je kompenzovat náklady spojené s obnovou činnosti organizace a nastolením rovnovážného stavu. Pojištění jako takové neovlivňuje riziko výskytu události nebo případnou škodu a vztahuje se pouze na předem dohodnuté nežádoucí události, které se mohou vyskytnout s určitou pravděpodobností. Tyto události jsou definovány v pojistné smlouvě, která je uzavřena mezi pojistitelem a pojistníkem. Běžné formy pojištění mohou krýt např. podnikatelská rizika, živelní pohromy, nemoc, úmrtí nebo také výdaje na nutnou zdravotní péči ve stáří apod. (Ducháčková, 2009).

4.1.1 Členění pojištění

Odborná literatura uvádí nejčastěji následující členění pojištění:

a) povinné pojištění,
b) nepovinné pojištění (které lze dále rozdělit na životní a neživotní pojištění).

ad a) Povinné pojištění

Ze zákona je toto pojištění uloženo firmám a osobám, které mají povinnost účastnit se vymezeného druhu pojištění. Povinná účast na pojištění má za úkol především zajištění sociálních jistot lidí a zabezpečení proti škodám způsobených jinými osobami při provozu motorových vozidel (Ducháčková, 2009).

Do této kategorie můžeme zařadit:

- zákonné zdravotní pojištění osob dle zákona o zdravotním pojištění,
- zákonné pojištění pracovních úrazů a nemoci z povolání zaměstnanců,
- zákonné pojištění odpovědnosti za škodu z provozu motorového vozidla,
- zákonné sociální pojištění osob dle zákona o sociálním pojištění.

ad b) Nepovinné pojištění

Toto pojištění není povinné a můžeme jej členit na:

1) životní pojištění,
2) neživotní pojištění.

ad 1) Životní pojištění

Tento typ pojištění je sjednán vždy pro fyzické osoby za účelem ochrany těchto osob a rodinných příslušníků proti rizikům těžkých úrazů, jejich trvalých následků, vážných nemocí nebo úmrtí.

Mezi druhy životního pojištění patří:

- úrazové pojištění,
- pojištění pobytu v nemocnici,
- pojištění závažných onemocnění,
- penzijní pojištění apod. (Ducháčková, 2009).

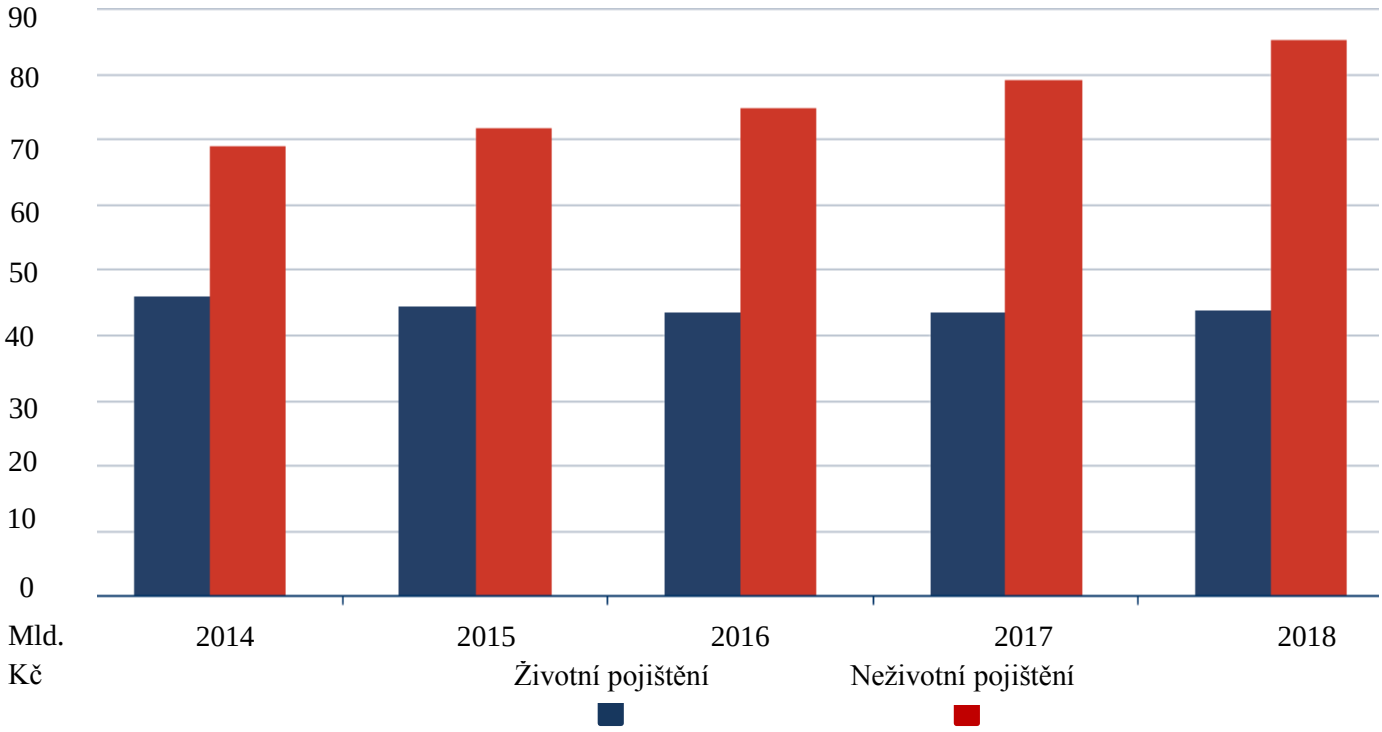
ad 2) Neživotní pojištění

Jedná se především o pojištění movitého a nemovitého majetku. Do této kategorie lze např. zařadit:

- cestovní pojištění (ambulantní lékařské ošetření apod.),

- pojištění nemovitosti (rodinný dům, bytový dům, garáž apod.),
- pojištění domácnosti (klenoty, ceniny, cenné papíry, elektronika apod.),
- pojištění proti přerušení provozu,
- pojištění podnikatelských rizik,
- pojištění kybernetických rizik,
- pojištění odpovědnosti za škodu (Ducháčková, 2009).

Trh s neživotním pojištěním, do kterého lze zařadit i pojištění organizací proti kybernetickým hrozbám, v posledních letech narůstá, jak lze vidět v následujícím grafu.



Graf 4.4: Vývoj pojistného trhu v České republice (Zdroj: Česká asociace pojišťoven, 2019)

4.1.2 Základní terminologie

Oblast pojišťovnictví je charakterizována několika základními pojmy, které vystihují podstatu této oblasti finančnictví.

Běžné pojistné

Pojistné, které je placeno v pravidelně dohodnutých časových obdobích. Může se jednat např. o měsíc, rok apod. Dohoda, která specifikuje počátek a délku období, musí být součástí pojistné smlouvy (Ducháčková, 2015).

Mimořádné pojistné

Jedná se o pojistné, které je uhrazeno pojistníkem jednorázově nad rámec běžného pojistného nebo platby. Mimořádné pojistné je možné vložit kdykoliv během trvání pojištění (Ducháčková, 2015).

Pojištěný

Podle občanského zákoníku tento termín označuje osobu, na jejíž život, zdraví, majetek, zodpovědnost nebo jinou hodnotu pojistného zájmu se pojištění vztahuje (Nový občanský zákoník, 2019).

Pojistník

Jedná se o fyzickou nebo právnickou osobu, která uzavřela s pojišťovnou (tj. pojistitelem) pojistnou smlouvu. Pojistník a pojištěný bývá často tatáž osoba, není to ale pravidlem pojistné smlouvy (Ducháčková, 2015).

Pojistitel

Pojistitel je osoba fyzická nebo právnická, která se za úplatu zavazuje převzít sjednaná rizika pojistníka při vzniku možné škody. Pojistitel je zpravidla pojišťovna, která se řídí zákonem č. 277/2009 Sb., o pojišťovnictví. Pojistitel v případě vzniku pojistné události poskytuje určitou finanční náhradu pojistníkovi na základě sjednané pojistné smlouvy (Ducháčková, 2015).

Pojistná částka

Částka pojistného plnění, která je splatná pojišťovnou při splnění určitých podmínek a okolností stanovených v pojistné smlouvě. V praxi se jedná o částku, která je určena k výplatě v případě pojistné události (Ducháčková, 2015).

Pojistná doba

Jedná se o dobu, na kterou je uzavřena pojistná smlouva. Pokud během této doby dojde k realizaci pojistné události, je pojišťovna povinna vyplatit dohodnutou výši plnění (Ducháčková, 2015).

Pojistná hodnota

Tento pojem označuje nejvyšší možnou finanční újmu na majetku, která může v důsledku realizace pojistné události nastat (Ducháčková, 2015).

Pojistná událost

S výjimkou dožití se jedná o nahodilou skutečnost, se kterou je spojen vznik povinnosti pojišťovny vyplatit dohodnutou výši plnění (např. nemoc, úraz nebo úmrtí), (Ducháčková, 2015).

Pojistné krytí

Jedná se o rozsah sjednaných rizik, která jsou zahrnuta v pojistné smlouvě. V této smlouvě jsou v přiložených podmínkách detailně popsána pravidla, za kterých je pojišťovna povinna uskutečnit plnění a při kterých ne (Ducháčková, 2015).

Pojistné plnění

Částka, která může být vyplacena jednorázově nebo postupně a kterou podle pojistné smlouvy poskytne pojišťovna v případě vzniku a realizace pojistné události (Ducháčková, 2015).

Pojistné podmínky

Podmínky, které obsahují především vymezení vzniku, trvání a zániku pojištění, stejně tak pojistné události a stanovení podmínek, za kterých nevzniká pojistiteli povinnost poskytnout pojistné plnění. Dále pak způsob určení rozsahu pojistného plnění a jeho splatnost (Ducháčková, 2015).

Pojistný zájem

Pojistným zájmem je označována potřeba ochrany před následky pojistných událostí. Pojišťovna je tedy povinna pojistný zájem zajistit. Pokud však pojistný zájem pomine, má klient právo zrušit pojistnou smlouvu (Nový občanský zákoník, 2019).

Pojištění

Pojištění slouží ke kompenzaci vzniklých nákladů, které jsou spojeny s realizací nežádoucí události na subjektu, který je předmětem pojištění (Ducháčková, 2015).

Pojišťovnictví

Pojišťovnictví lze charakterizovat jako specifický ekonomický obor řešící minimalizaci rizik v oblastech ekonomických i neekonomických činností člověka (Ducháčková, 2015).

Výluka

Jedná se o případy nebo situace uvedené v pojistných podmínkách, při nichž není pojišťovna povinna pojistné plnění vyplatit (Ducháčková, 2015).

Zajištění pojišťovny

Jedná se o převod části rizika, které převede pojistitel od pojištěných na jiný subjekt pojištění, označovaného jako zajistitel (pojištění pojišťoven). Zajistitel nemá k pojištěným žádný smluvní vztah. Jedná se pouze o ochranu pojistitele v případě velkých pojistných událostí, kdy se zpravidla podílí na výplatě pojistného plnění (Ducháčková, 2015).

4.1.3 Typy pojištění a jejich vhodnost pro ochranu vůči kybernetickým hrozbám

Pojištění organizací a jejich informačních systémů proti kybernetickým hrozbám je kombinací majetkového pojištění a pojištění odpovědnosti za škodu. V rámci vývoje pojišťovnictví bylo doposud navrženo několik kategorií pojistných produktů, které svou podstatou mohou krýt škody a mírnit dopady kybernetických hrozeb na organizaci.

Mezi tyto kategorie pojistných produktů lze zařadit:

a) Pojištění majetku – pojištění technických rizik

V rámci tohoto typu pojištění může být předmětem pojistné smlouvy stroj nebo elektronické zařízení, které je nedílnou součástí výrobního nebo pracovního procesu. Tento typ pojištění tedy může krýt škody způsobené chybou obsluhy nebo výrobcem, dále pak škody způsobené mrazem a ledem, škody způsobené provozem zařízení nebo finanční újmy způsobené přerušením provozu. Pro potřeby pojištění kybernetických hrozeb může být toto pojištění využito pro kompenzaci škod způsobených na hmotném majetku (Martinovičová, 2006).

b) Pojištění přerušení provozu

Jedná se o typ pojištění, které kompenzuje ztráty, které jsou způsobené omezením nebo přerušení provozu organizace. Vztahuje se také na kompenzaci ušlého zisku a fixních nákladů, které musí pojištěná organizace při přerušení provozu vynakládat.

Jedná se např. o:

- nájemné včetně leasingových splátek,
- mzdy a odvody sociálního a zdravotního pojištění za zaměstnance,
- veškeré placené služby,
- odpisy,
- materiálové náklady vynaložené v době odstávky provozu,
- ušlý provozní hospodářský výsledek atd.

Z pohledu pojištění kybernetických hrozeb je možné z tohoto typu pojistných produktů hradit finanční náklady na zaměstnance v době přerušení provozu činnosti. Dále pak kompenzovat ušlý hospodářský výsledek, popř. materiálové náklady vynaložené v době odstávky provozu (Zvláštní pojistné podmínky pro pojištění pro případ přerušení nebo omezení provozu – Kooperativa, 2019). Tyto typy pojištění nelze použít na kompenzaci škod vynaloženou na obnovu dobrého jména organizace, nákladů na rekonstrukci nebo obnovu dat a na kompenzaci udělených pokut od dozorových orgánů (Kooperativa, 2019).

4.1.4 Pojistná hodnota a stanovení její výše

Pojistná hodnota představuje nejvyšší možnou finanční škodu, která může být způsobena nežádoucí událostí. Podle zákona č. 37/2004 Sb., o pojistné smlouvě a o změně souvisejících zákonů (dále jen zákon o pojistné smlouvě) je pojistná hodnota definována jako *„nejvyšší možná majetková újma, která může v důsledku pojistné události nastat“*[1]. Obecně lze stanovit pojistnou hodnotu třemi základními způsoby. Cenu pojišťovaného subjektu si může pojištěný stanovit sám nebo je cena subjektu stanovena podle cenového odhadu (Zákon č. 37/2004 Sb.). Pojistná hodnota může být interpretována několika typy cen:

a) Nová cena

[1] *Některé části tohoto zákona byly k 1. 1. 2014 zrušeny.*

Dle zákona o pojistné smlouvě se novu cenou rozumí *„cena, za kterou lze v daném místě a v daném čase věc stejnou nebo srovnatelnou znovu pořídit jako věc stejnou nebo novou, stejného druhu a účelu“*.

a) Časová cena

Dle zákona o pojistné smlouvě se časovou cenou rozumí *„cena, kterou měla věc bezprostředně před pojistnou událostí; stanoví se z nové ceny věci, přičemž se přihlíží ke stupni opotřebení nebo jiného znehodnocení anebo k zhodnocení věci, k němuž došlo její opravou, modernizací nebo jiným způsobem“*.

b) Dohodnutá cena

Tuto cenu lze definovat jako finanční částku, kterou je za daných okolností ochoten kupující zaplatit a konkrétní prodávající ochoten získat, aby provedli danou transakci (Němeček a Janata, 2010).

V občanském zákoníku je také uvedeno, že *„není-li při pojištění majetku ujednána pojistná hodnota, představuje pojistnou hodnotu obvyklá cena, kterou má majetek v době, ke které se určuje jeho hodnota“*.

4.1.5 Shrnutí

Pojištění je chápáno jako nástroj, který slouží pro kompenzaci finančních škod, které vznikly vlivem nežádoucích událostí na konkrétní subjekt nebo objekt. Pojišťovnictví je chápáno jako oblast finančnictví, jejímž úkolem je ochránit určité hodnoty včetně života a zdraví. Pojistné produkty lze rozdělit do několika kategorií. Každá z těchto kategorií zahrnuje specifický typ pojistných produktů, které jsou určeny pro rozdílné subjekty nebo objekty. S těmito subjekty nebo objekty jsou také spojeny odborné pojmy, jejichž charakteristika je nezbytná pro pochopení pojištění a jeho podstaty.

Mezi tyto pojmy lze např. zařadit *pojistnou hodnotu*, která představuje nejvyšší možnou majetkovou újmu, jež může vlivem náhodné události nastat. Pojistná hodnota je jedním z klíčových ukazatelů při stanovení limitu pojištění. V odborné literatuře není uveden obecný matematický postup pro stanovení výše pojistné hodnoty, a proto je tento problém jedním z hlavních cílů disertační práce.

V oblasti pojistných produktů, které jsou zaměřeny na pojištění organizací proti dopadům kybernetických hrozeb, je stanovení pojistné hodnoty velmi problematické. Je to především z důvodu obtížného finančního vyjádření sledovaných oblastí organizace (v této disertační práci označovaných jako „ohrožené prvky“).

4.2 Kybernetické hrozby a jejich dopady na prostředí organizace

V rámci návrhu algoritmu, který je zaměřen na stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví, je nezbytné charakterizovat kybernetické hrozby a jejich možné dopady na prostředí organizace. Dopady kybernetických hrozeb mohou narušit funkci organizace v různých oblastech řízení. Tyto oblasti (v disertační práci uvedeny jako „ohrožené prvky“) mohou být jak technického, tak netechnického charakteru. Mezi tyto prvky můžeme zařadit např. hardware, dobré jméno organizace, výrobní zařízení, vybrané segmenty počítačové sítě. Pokud dojde k realizaci některé z kybernetických hrozeb, dopady na organizaci a její fungování mohou být dlouhodobé.

Mezi takové dopady můžeme zařadit např. obnovu dobrého jména organizace. Pokud dojde k narušení tohoto ohroženého prvku, obnova a náprava může trvat velmi dlouho. Mezi možné projevy poškození dobrého jména organizace můžeme zařadit např. narušení vztahů se zákazníky, odběrateli, dodavateli nebo zaměstnanci. Mezi další prvky, které mohou být narušeny a jejichž obnova nebo rekonstrukce může být velmi nákladná a dlouhodobá, patří data. Z pohledu kybernetické bezpečnosti se jedná o nejcennější aktivum, jehož hodnota je velmi obtížně stanovitelná. Pokud dojde ke zkopírování nebo smazání citlivých dat, může být organizace výrazně poškozena nejen v konkrétním okamžiku, kdy došlo ke zneužití těchto dat, ale také v budoucím vývoji v daném podnikatelském odvětví. Pro stanovení pojistné hodnoty je proto nezbytným krokem definovat možné kybernetické hrozby a stanovit jejich možné dopady na různé oblasti organizace ve vztahu k zajištění základních funkcí.

V rámci znázornění vzniku, průběhu a dopadu jednotlivých kybernetických hrozeb na informační prostředí vybraného referenčního objektu, je popis každé hrozby rozdělen do několika fází:

a) charakteristika,
b) ohrožené prvky,
c) dopady.

Mezi vybrané kybernetické hrozby lze zařadit:

- útok na informační systém prostřednictvím ransomware,
- úmyslnou trestnou činnost prováděnou hackerem,
- neoprávněný přístup do informačního systému,
- napadení informačního systému prostřednictvím malware,
- únik dat vlivem nedbalosti zaměstnance,
- DDoS útok,
- fyzickou ztrátu nosiče dat (ztráta notebooku),

- ztrátu dat a narušení funkce informačního systému organizace vlivem bleskového výboje,
- selhání systému.

1) Útok na informační systém prostřednictvím ransomware

Charakteristika: Ransomware je vyděračský typ malwaru, který brání uživateli v běžném užívání informačního systému do doby, než dostane útočník zaplaceno výkupné. Obecně můžeme rozlišovat dva typy ransomware podle toho, jak mohou zasáhnout do chodu počítačového systému. Prvním typem je ransomware, který omezí funkčnost celého počítačového systému a neumožní uživateli tento systém využívat (např. zabráněním spuštění operačního systému). Druhým typem pak je ransomware, jenž ponechá počítačový systém funkční, avšak dochází k uzamčení a znepřístupnění citlivých dat, které jsou pro uživatele nezbytné (Kolouch, 2016).

Některé formy ransomware šifrují soubory na pevném disku (kryptovirální vydírání), jiné jen uzamknou systém a výhrůžnou zprávou se snaží donutit uživatele k zaplacení výkupného (Kolouch, 2016).

Ohrožené prvky: servery, software, data, dodavatelsko-odběratelské vztahy, segmenty sítě, dobré jméno organizace.

Dopady: V případě útoku typu ransomware, kdy dojde k zamezení přístupu uživatele k potřebným datům, mohou být dopady fatální. V případě nedostupnosti dat může být ohroženo celé podnikání dané organizace, včetně ohrožení jejích dodavatelských a odběratelských vztahů.

Pokud jsou nedostupná klíčová data, která slouží k zajištění základních činností a chodu organizace, pak tato organizace nemůže plnit své závazky vůči jiným subjektům. Z této skutečnosti také vyplývají pokuty, které mohou být organizaci uděleny na základě nedostupnosti informací, především těch, které jsou povinni zveřejňovat na svých webových stránkách.

2) Úmyslná činnost trestná prováděna hackerem

Charakteristika: Hacking: (hackovat, hack) „Nestandardní použití systému či aplikace, při němž uživatel uplatňuje neobvyklé a nekomentované funkce systému a může tak využít některých jeho jinak nepřístupných schopností“. Při hackování se často zasahuje přímo do struktury programových souborů, což vyžaduje jistou znalost formátu těchto souborů (Kolouch, 2016).

Hacking znamená „průnik do systému jinou nežli standardní cestou, tedy obejití či prolomení jeho bezpečnostní ochrany“.

Hacker: Existuje několik definicí tohoto termínu:

a) Hacker je „člověk, kterého baví zkoumat detaily programovatelných systémů a hledat metody, jak je vylepšit“.
b) Policejní definice popisuje hackera jako osobu, která proniká do chráněných systémů, přičemž jejím cílem je prokázat vlastní kvality bez toho, aby měli zájem na získání nebo zničení informací v systému obsažených.

Ohrožené prvky: servery, software, data, dodavatelsko-odběratelské vztahy, segmenty sítě, dobré jméno organizace, hardware.

Dopady: Škody, které může způsobit hacker v dané organizaci, mohou být opravdu velmi širokého a závažného charakteru. Cílem hackera je získat konkrétní typ dat, která nejsou přístupná veřejnosti. Je důležité zmínit, že se v případě hackingu nejedná nutně o smazání dat, ale o jejich kopírování nebo modifikování. V případě smazání dat by byla hackerova činnost ve velmi krátké době identifikována, což pro tento typ útočníka není žádoucí.

Právě tato skutečnost může způsobit pozdější odhalení škod, které byly hackingem způsobeny, což může prohloubit dopad škodlivé události. Čím později je hackerský útok detekován, tím rozsáhlejší charakter mohou škody mít. Dopady takového jednání mohou samozřejmě narušit celkovou funkci organizace a její struktury.

Podobně jako u předchozího typu útoku může dojít k narušení obchodních vztahů, a to nenávratně. Takové dopady mohou také ohrozit dobré jméno organizace, které je zásadním faktorem úspěšného fungování každé organizace. Dalším dopadem je ztráta citlivých dat, ať už se jedná o data vytvořená danou organizací během své činnosti nebo osobní data zaměstnanců. V těchto případech mohou být dopady z pohledu finančního charakteru katastrofální. Skutečnost, že data vlastní také někdo jiný než samotná organizace, může přispět k přerušení činnosti nebo ohrožení její funkce.

Pokud jsou data smazána ze serverů v dané organizaci, jejich obnova a rekonstrukce může být často nejen nákladným procesem, ale také nemusí být vůbec tento proces realizovatelný. V případě úniku osobních dat vznikají také náklady na oznámení této ztráty příslušnému úřadu.

V souvislosti se zajištěním rovnováhy dané organizace, která je důležitá pro obnovení její činnosti, je třeba vynaložit určité finanční prostředky také na právní služby, které jsou s únikem dat spojeny. Dalším faktorem je náprava škod v samotném informačním systému organizace, který bude muset být opraven, a to především v těch částech, které jsou díky hackerskému útoku narušeny.

3) Neoprávněný přístup do informačního systému

Charakteristika: U neoprávněného přístupu se nejedná o útok v pravém slova smyslu, ale o přístup uživatele informačního systému k datům, ke kterým oficiálně nemá povolení přístupu. U této kybernetické hrozby jde především o přístup k datům, která jsou chráněna konkrétním režimovým opatřením a mají pro organizaci velký význam. Jejich zneužití neoprávněnou osobou by tedy mohlo organizaci způsobit značné finanční škody.

Ohrožené prvky: data, uživatelé, zákazníci, dobré jméno, pokuty ze strany dodavatelů a odběratelů.

Dopady: I když se nejedná o cílený útok, dopady mohou být stejně závažné, jako v případě hackerského útoku. Pokud informace o zákaznících, obchodních partnerech, zaměstnancích apod. uvidí někdo nepovolaný, zneužití těchto informací může mít velmi závažné důsledky. Může se jednat o poškození dobrého jména, poškození identity dotčených zaměstnanců a vyzrazení jejich osobních údajů, narušení podnikatelské činnosti apod.

4) Napadení informačního systému prostřednictvím malware

Charakteristika: Malware představuje škodlivý software, určený k poškození nebo vniknutí do počítačového systému. Výraz malware vznikl složením anglických slov „malicious“ (zlovolný, zlomyslný) a „software“ a popisuje záměr autora takového programu spíše než jeho specifické vlastnosti. Pod souhrnné označení malware se zahrnují počítačové viry, počítačoví červi, trojské koně, crimeware, špehovací software (spyware), vyděračský software (ransomware) a reklamní software (adware). V právní terminologii je malware někdy nazýván počítačová nečistota (angl. „computer contaminant“).

Větší hrozbu představují programy navržené tak, aby poškozovaly nebo zcela mazaly data. Mnoho virů pro DOS bylo napsáno tak, aby smazaly soubory na pevném disku nebo aby poškodily souborový systém zapsáním nesmyslných dat. Síťoví červi, jako například Code Red nebo Ramen, také patří do této kategorie, protože byly napsány, aby vandalizovaly webové stránky.

Motivem pro vznik škodlivého softwaru může být někdy pomsta. Programátor nebo správce systému, který byl propuštěn ze zaměstnání, může v systému zanechat zadní vrátka (angl. „backdoors“) nebo softwarovou „časovanou bombu“, která mu umožní poškodit v budoucnu systémy bývalého zaměstnavatele nebo zničit jeho vlastní dřívější práci.

Ohrožené prvky: servery, software, data, dodavatelsko-odběratelské vztahy, segmenty sítě, dobré jméno organizace.

Dopady: Malware je podobný typ útoku jako je hacking, nicméně se tak neděje prostřednictvím lidského faktoru, ale prostřednictvím infekce nebo viru, který má za úkol napadnout konkrétní informační systém a smazat nebo modifikovat určitý typ dat. Data, která jsou prostřednictvím malware smazána, jsou často nenávratně ztracena a jejich obnova již nemusí být možná. Záleží, zda organizace provádí pravidelné zálohování dat a jejich obnovu nebo nikoliv.

Pokud se jedná pouze o modifikaci dat, mohou být data za určitých okolností obnovena. Tato obnova může být ale časově náročná a finančně nákladná. Škody, které mohou být malwarem způsobeny, se týkají tedy především samotných dat, popř. fyzických zařízení jako jsou servery, počítačové sestavy apod. Modifikován může být také samotný software, který zajišťuje funkci informačního systému organizace.

Dalšími dopady, které z tohoto typu hrozby vyplývají, je poškození dobrého jména. V případě ztráty dat se může stát organizace nesolventní vůči svým obchodním partnerům atd.

5) Únik dat vlivem nedbalosti zaměstnance

Charakteristika: Tento únik nebo ztráta dat, která souvisí s rizikovou činností zaměstnance, je velmi častým způsobem, jakým se data ocitnou mimo organizaci. Toto jednání může být neúmyslné a bývá způsobeno nedodržováním bezpečnostních zásad týkajících se nakládání s interními a citlivými daty organizace. Mezi takové situace může patřit cílený prodej citlivých dat organizace jinému subjektu s cílem zvýšit jeho konkurenceschopnost (úmyslné jednání) nebo poskytnutí citlivých údajů organizace prostřednictvím e-mailu jinému subjektu (neúmyslné jednání).

Ohrožené prvky: data, dobré jméno organizace, dodavatelsko-odběratelské vztahy.

Dopady: Pokud se data, která jsou spojena s organizací a jejími interními procesy, ocitnou mimo organizaci nebo se dostanou k nepovolaným osobám, může v případě jejich zneužití k jiným účelům, než ke kterým byla vytvořena, způsobit opět škody velkého rozsahu. Pokud se navíc tento únik dat stane veřejnou záležitostí, může být opět poškozeno dobré jméno organizace, vyzrazena její bezpečnostní opatření a bezpečnostní systém apod.

V případě úniku dat způsobeného nedbalostí zaměstnance, bude velmi důležité posoudit, jestli uniklá data byla zkopírována nebo zda se jedná o ztrátu dat bez možnosti jejich obnovy. Ve druhém případě budou organizaci vznikat další náklady se zajištěním obnovy dat a jejich znovuzískání, stejně jako možnost

postihnutí organizace pokutami od správních úřadů nebo pokutami vyplývajícími z dodavatelsko-odběratelských vztahů.

Samozřejmě i v tomto případě může být způsobeno poškození dobrého jména. Pokud bude kybernetický incident medializován, může dojít k narušení reputace a obchodní značky dané organizace. Mezi další dopady lze zařadit také náklady, které jsou spojeny s rekonstrukcí nebo obnovou ztracených dat, náklady na oznámení ztráty nebo úniku dat apod.

6) **DDoS útok** (Denial of Service)

Charakteristika: Tento typ útoku je zaměřen na zamezení přístupu uživatele informačního systému ke konkrétní službě. DDoS útok je založen na organizovaném zahlcení určitého operačního systému nebo internetové stránky, která se pod vlivem množství velkého počtu připojených uživatelů zhroutí nebo omezí svou činnost.

DDoS útok lze rozdělit na následující druhy:

a) zaplavení provozu na síti náhodnými daty, které zabraňují protékání skutečných dat,
b) zabránění nebo přerušení konkrétnímu uživateli v přístupu k webové službě,
c) narušení konfiguračního nastavení,
d) extrémní zatížení CPU cílového serveru,
e) vsunutí chybových hlášení do sekvence instrukcí, které můžou vést k selhání systému,
f) selhání samotného operačního systému.

Ohrožené prvky: servery, software, data, dodavatelsko-odběratelské vztahy, segmenty sítě, dobré jméno organizace.

Dopady: Škody, které DDoS útoky způsobují, jsou v principu dvojího charakteru. Kromě přímých finančních ztrát, které lze snadno vyčíslit a které se případ od případu mohou pohybovat v závislosti na délce a intenzitě útoku od několika set tisíc až po stovky milionů korun, může být poškozeno také dobré jméno organizace. Jako důsledek této situace může být neuskutečnění obchodů, které probíhají v daný moment útoku.

Zákazníci předpokládají, že poskytovatel on-line služby, kterou využívají, věnuje maximální pozornost zabezpečení své síťové infrastruktury. V případě, že je výrazným způsobem ohrožena dostupnost služby, často odcházejí ke konkurenci. Odolnost proti DDoS útokům se z tohoto hlediska jeví jako nesporná konkurenční výhoda.

7) Fyzická ztráta nosiče dat (ztráta notebooku)

Charakteristika: Jako fyzická ztráta nosiče dat může být označena ztráta notebooku, na kterém jsou uložena data, která mají pro organizaci velký význam. Tato situace může být způsobena cílenou krádeží (zloděj). V tomto případě bývá uskutečnění této situace obtížně prokazatelné.

Při dokazování obou možných způsobů ztrát lze vycházet z kamerových záznamů, které jsou instalovány v místech, kde ke ztrátě došlo, popř. ze svědectví očitých svědků. Pokud nejsou tyto skutečnosti přítomny, je velmi náročné tento typ události uznat jako pojistnou událost.

Ohrožené prvky: data, hardware, software, dobrá pověst organizace.

Dopady: Tento typ kybernetické hrozby bude mít dopady především na dobré jméno organizace. Pokud není organizace schopna zajistit svá data proti fyzické krádeži, bude tato skutečnost vnímána potenciálními zákazníky. Další skutečností, která může mít pro organizaci fatální následky, je ztráta dat. V tomto případě se nejedná o zkopírování dat nebo poškození nosiče dat, ale o fyzické odcizení zařízení, na kterém jsou data uložena.

Tato situace může znamenat pro organizaci velkou zátěž v podobě ztráty know-how, a tím také konkurenceschopnosti.

Rekonstrukce dat může nastat v případě, že:

a) jsou data zálohována na serveru,
b) jsou data zálohována na externím harddisku,
c) jsou data zálohována na cloudu.

V případě rekonstrukce je možné ztracená data obnovit do původního stavu, protože jejich kopie (záloha) je vytvořena na jiném nosiči. U obnovy dat se jedná o závažnější případ, kdy není možné ztracená data již obnovit ze záložního zdroje a organizace je tak nucena vynaložit náklady, které jsou spojeny se znovu pořízením ztracených dat.

Tyto náklady by měly být kompenzovány v pojištění kybernetických hrozeb, pod položkou „náklady na rekonstrukci a obnovu dat“. V případě rekonstrukce dat, není potřeba stanovit výši nákladů, protože žádné nevznikají. Data jsou zálohována na externím nosiči a jsou tedy k dispozici. V případě obnovy dat budou náklady vyšší. Organizace bude muset vynaložit finanční prostředky na znovuzískání dat, což může být časově velmi náročné. Některá data nemusí být možné znovu získat, tudíž jejich ztráta je pro firmu nevyčíslitelná.

8) Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje

Charakteristika: Blesk je silný elektrostatický výboj přírodního charakteru, který je produkován během bouřky a je doprovázen emisí světla. Proti jeho působení je možné se chránit přepěťovou ochranou nebo hromosvodem. Působení blesku a jeho prokazování je velmi složité. Blesk má při každém jeho působení jinou sílu a také škody, které jsou jím způsobeny, mohou mít proměnlivý charakter.

Tento typ hrozby, vzhledem k povaze a potenciálním škodám, které může způsobit, lze zahrnout do kybernetických hrozeb. Pojišťovna tedy může tuto hrozbu zahrnout do pojištění kybernetických hrozeb, nicméně prokazování působení blesku je velmi náročné a ve většině případů jej pojišťovna v rámci tohoto typu pojištění neuzná.

Ohrožené prvky: servery, software, hardware, data, segmenty sítě, hardware.

Dopady: Mezi nejzávažnější dopady patří především narušení funkce a integrity informačního systému organizace. To může mít za následek také vyhoření zdroje informačního systému nebo poškození hlavního serveru. Vlivem těchto okolností může dojít k úplné ztrátě dat nebo k částečnému poškození dat. V případě narušení funkce informačního systému v organizaci může také dojít k přerušení výrobního procesu. Tato situace může nastat tehdy, pokud je fungování informačního systému přímo spojeno s výrobním procesem a existuje zde tedy určitá závislost.

Při přerušení výrobního procesu dochází k vzniku ušlého zisku a vznikají závazky vůči odběratelům, které organizace není schopna za dané situace plnit. V případě přerušení výrobního procesu nemohou odběratelé odebírat od organizace výrobky, které by dále prodávali, a tím jim také vznikají škody v podobě ušlého zisku. Mezi další dopady lze také zařadit poškození dobrého jména organizace, poškození hardwaru, modifikace softwaru apod.

9) Selhání systému

Charakteristika: Selhání systému bývá většinou způsobeno technickou závadou na hardwaru nebo softwaru, která způsobí jeho nefunkčnost. V případě této kybernetické hrozby je vždy důležité vyšetřit příčinu selhání prvku informačního systému v organizaci. Tuto skutečnost musí zajistit technický pracovník pojišťovny, která pojištění proti kybernetickým hrozbám poskytuje.

Ohrožené prvky: servery, software, hardware, data, dodavatelsko-odběratelské vztahy, segmenty sítě, dobré jméno organizace, počítačové sestavy.

Dopady: V případě selhání systému mohou být dopady velmi podobné jako u předcházející hrozby. Může se jednat o narušení funkce informačního systému organizace, a tím také zajištění základních procesů v organizaci. Tyto základní procesy mohou být spojeny se zajištěním funkce organizace jako celku a lze mezi ně zařadit správu ekonomické agendy, účetnictví apod. Pokud není organizace schopna zajišťovat svou výrobu, mohou být uděleny opět sankce ze strany dodavatelů a odběratelů. Dále zde může nastat poškození dobrého jména, i když v tomto případě se nemusí jednat o tak velké škody jako v případě cílených kybernetických útoků způsobených hackerem. Vlivem selhání informačního systému může také dojít k částečné nebo úplné ztrátě dat. Pokud nejsou data pravidelně zálohována na serveru, který je umístěn mimo budovu, externím harddisku, cloudu nebo datovém skladu, mohou být nenávratně ztracena. Obnova těchto dat pak může být velmi časově i finančně náročná. Mezi další dopady lze zařadit nefunkčnost hardwarových komponent, modifikaci softwaru, ušlý zisk z nevyrobených výrobků apod.

4.3 Shrnutí

Pro stanovení pojistné hodnoty organizace, která je předmětem pojištění proti kybernetickým hrozbám, je jednou z klíčových činností celého procesu také charakteristika možných kybernetických hrozeb a jejich dopadů. Současné hrozby, které se vyskytují v kybernetickém světě, se liší nejen svou podstatou, ale také dopady, které mohou v případě jejich realizace nastat. Dopady těchto vybraných kybernetických hrozeb mohou významným způsobem narušit nebo nevratně poškodit sledované ohrožené prvky organizace. Každá z těchto hrozeb je zde popsána z pohledu jednotlivých fází realizace. Jednotlivé fáze obsahují popis narušení definovaných ohrožených prvků organizace a detekci okamžiku vzniku finančních nákladů na těchto prvcích.

5. VÝSLEDKY VÝZKUMU – STAV ORGANIZACÍ Z HLEDISKA POJIŠTĚNÍ PROTI KYBERNETICKÝM HROZBÁM

Empirická část disertační práce navazuje na část teoretickou a prezentuje výsledky kvantitativního šetření. Nástrojem pro ověření hlavního cíle disertační práce, bylo dotazníkové šetření, jehož cílem je zmapovat a ověřit stav organizací z pohledu pojištění proti kybernetickým hrozbám. Cílem dotazníkového šetření k disertační práci byla především **analýza referenčních objektů a dále ověření stanovených cílů, které jsou předpokladem pro návrh algoritmu.**

Vzhledem k tomu, že v oblasti pojištění proti kybernetickým hrozbám není doposud zpracováno dostatečné množství odborné literatury nebo vědeckých prací, je tento dotazník unikátním nástrojem pro sběr požadovaných dat.

5.1 Metodologie výzkumu

Dotazníkové šetření probíhalo ve 20 organizacích na území České republiky. Tyto organizace lze vzhledem k jejich velikosti a počtu zaměstnanců zařadit mezi malé, popř. střední podniky. Jednalo se výhradně o organizace ze soukromé sféry, které se liší svou podstatou podnikání i informačním prostředím. Vzhledem k tomu, že dotazník je zaměřen na oblast kybernetické bezpečnosti, nebyly některé organizace ochotny spolupracovat, a to především z důvodu sdílení citlivých dat o svých informačních systémech.

Dotazník je široce používanou metodou pro oslovení vybraných cílových skupin, v tomto případě referenčních subjektů. V dotazníku je konstruováno celkem 26 otázek. Tyto otázky jsou rozděleny do šesti kategorií podle jejich odborného zaměření.

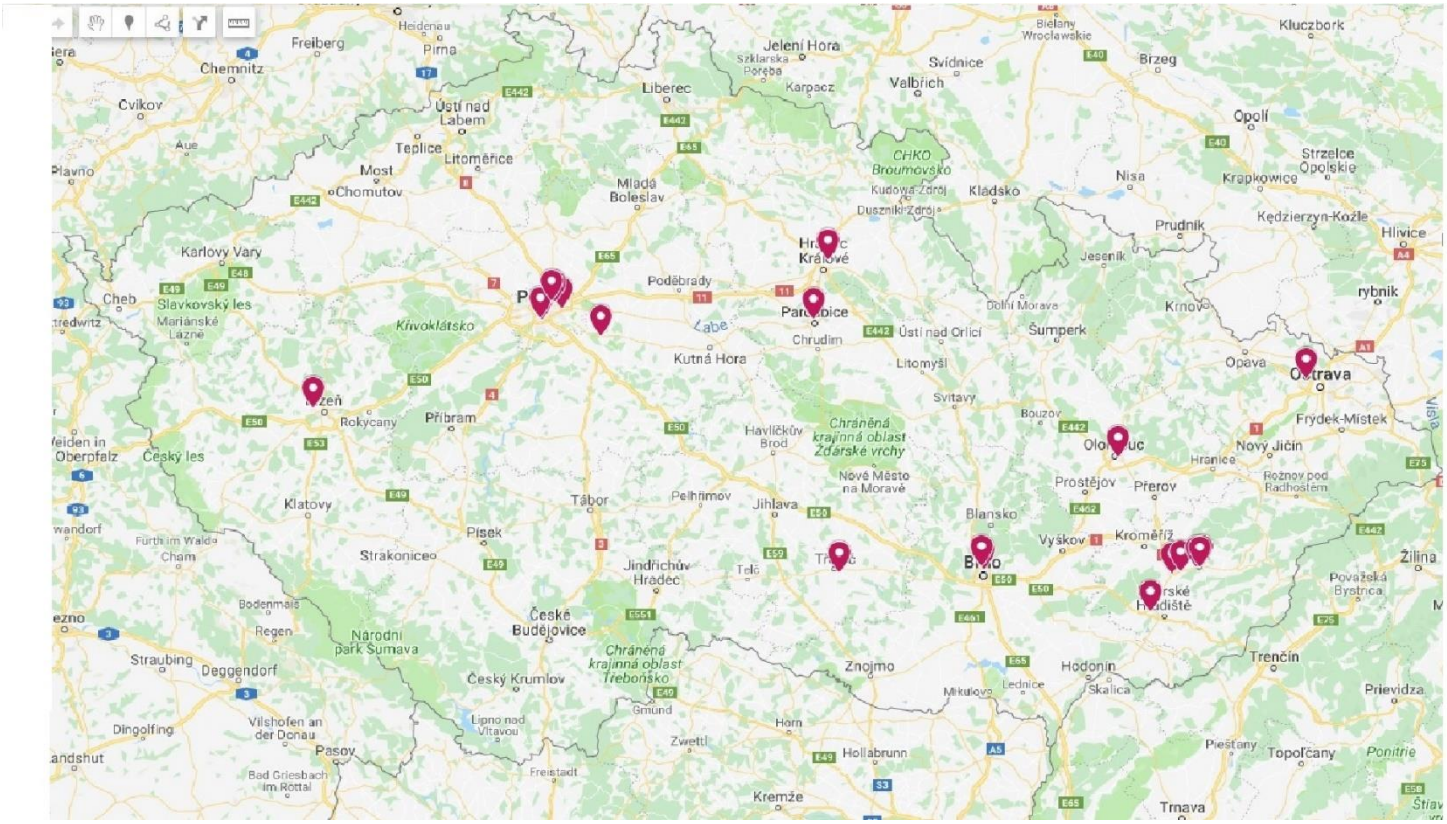
Jedná se o kategorie:

- informace o organizaci, která je předmětem dotazníkového šetření,
- informační systém organizace,
- datová bezpečnost a obnovitelnost funkce organizace,
- typy kybernetických hrozeb,
- připravenost organizace v oblasti kybernetické bezpečnosti,
- předpokládaný rozsah krytí proti kybernetickým hrozbám.

Dotazník byl vypracován na základě studia odborné literatury. Šetřené oblasti se vztahovaly především k problematice pojištění organizací proti kybernetickým hrozbám. Každá kategorie je zaměřena na jinou část této problematiky s cílem získat ucelený přehled o vnímání tohoto typu pojištění u malých a středních podniků v České republice. Otázky jsou konstruovány tak, aby bylo možné určit, které oblasti informačního prostředí mohou být nejvíce zasaženy dopadem

kybernetických hrozeb a jestli je pojištění proti těmto hrozbám pro organizace vhodným řešením.

Níže je uvedena mapa, ve které je vyznačeno umístění dotazovaných referenčních objektů.



Obr. 5.3: Mapa umístění organizací, které byly předmětem dotazníkového šetření (vlastní zdroj)

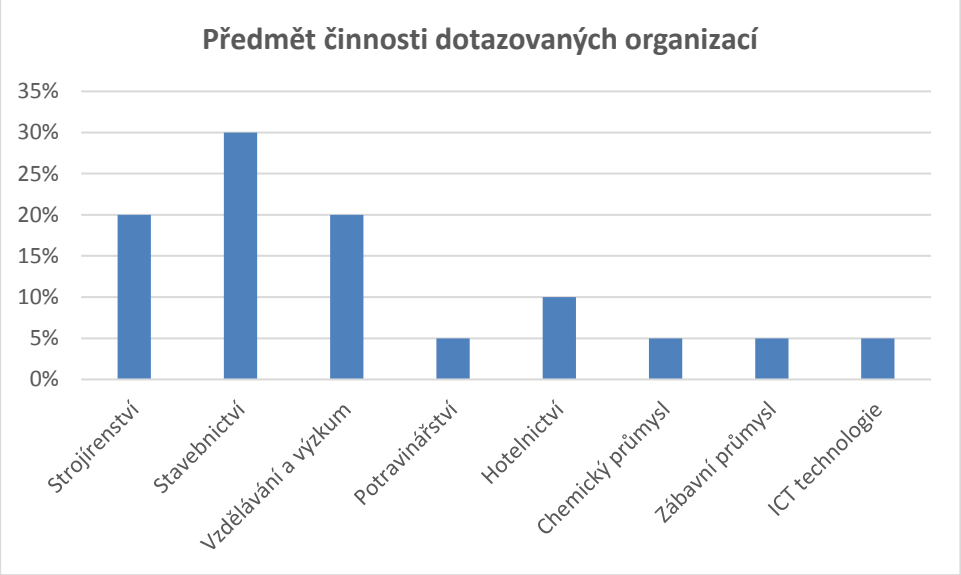
Při realizaci dotazníkového šetření byli vedoucí zaměstnanci oslovených referenčních objektů seznámeni s tím, že se jedná o výzkum k disertační práci a že jména dotazovaných organizací ani jednotlivých zaměstnanců nebudou zveřejněna. Vedoucím zaměstnancům byl dotazník předložen se slovním doplněním. Pokud některý ze zaměstnanců dal najevo neporozumění některé z předložených otázek, byla mu tato otázka slovně vysvětlena. Průměrná doba trvání rozhovoru a vyplnění výzkumných otázek byla 50 minut. Při vyhodnocování provedeného výzkumu bylo použito procentuálního vyjádření, jehož výsledky jsou uvedeny v následujících grafech. Výsledky dotazníkového šetření jsou rozděleny do šesti samostatných kategorií podle zaměření otázek.

Pro přesnější charakteristiku dotazovaných subjektů jsou zde popsány jejich základní atributy, které zahrnují:

- předmět činnosti,
- počet zaměstnanců,
- roční obrat,
- počet jednotek.

Názvy dotazovaných organizací zde nejsou z důvodu zachování anonymity a dobrého jména uvedeny.

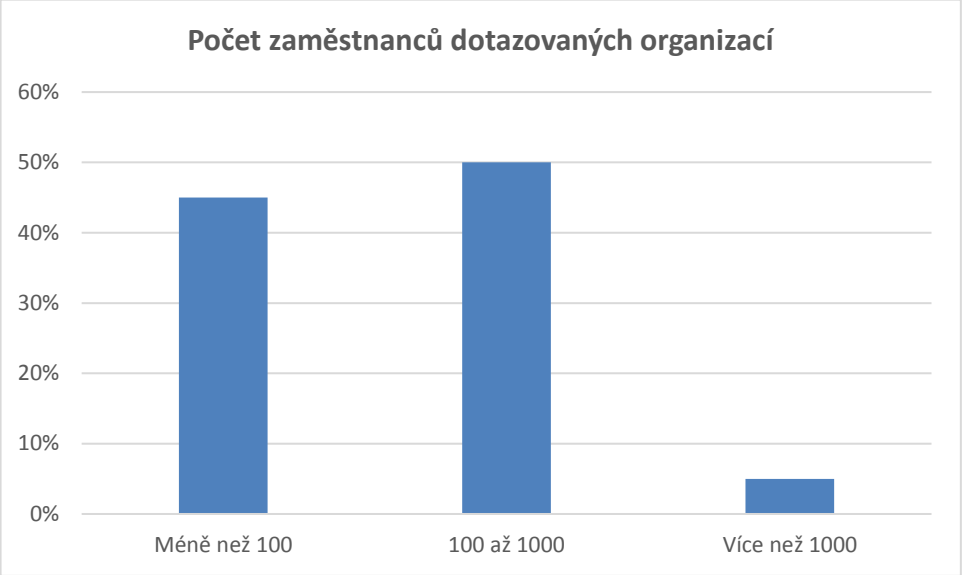
a) Předmět činnosti



Graf 5.5: Předmět činnosti dotazovaných organizací (vlastní zdroj)

Celkem 20 % organizací bylo vybráno z oblasti strojírenské výroby. Je to z důvodu častých kybernetických útoků na organizace se zaměřením na tento segment trhu. Dále pak byly do dotazníkového šetření zahrnuty organizace z oblasti stavebnictví, které tvoří 30 % dotazovaných respondentů. Oblast vzdělávání a výzkumu je zde zastoupena s 20 %, oblast potravinářství reprezentuje 5 %, hotelnictví 10 % a chemický průmysl 5 %. Do výzkumného šetření byla vybrána také jedna organizace, kterou lze podle předmětu její činnosti zařadit do zábavního průmyslu (5 %) a jedna organizace, která je zaměřena na ICT technologie a IT řešení (také 5 %).

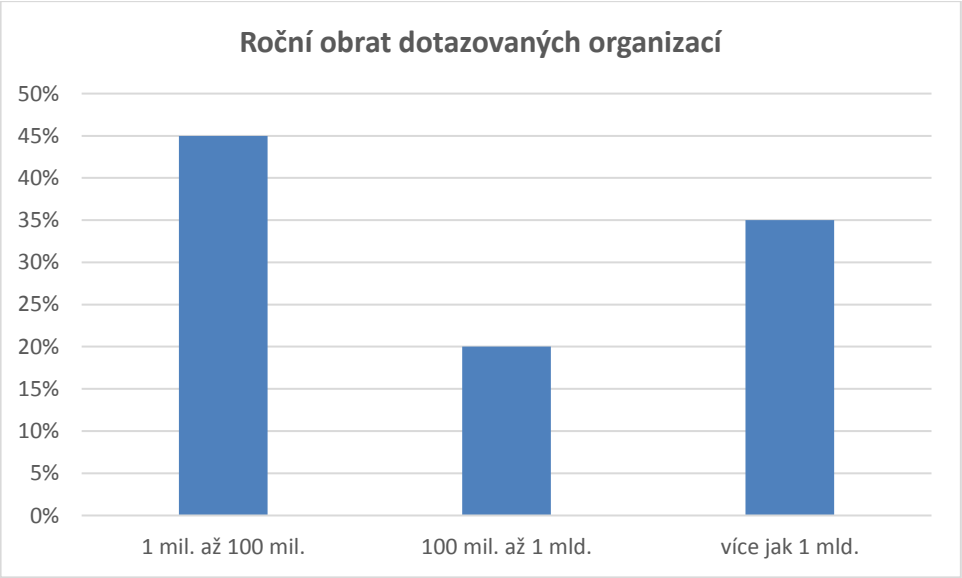
b) Počet zaměstnanců



Graf 5.6: Počet zaměstnanců dotazovaných organizací (vlastní zdroj)

V rámci realizace dotazníkového šetření byly vybrány organizace, které lze zařadit mezi malé a střední podniky. Oblast malých organizací reprezentuje celkem 9 objektů (45 %) a oblast středních organizací reprezentuje celkem 10 objektů (50 %). Jedna z dotazovaných organizací má více než 1000 zaměstnanců (5 %).

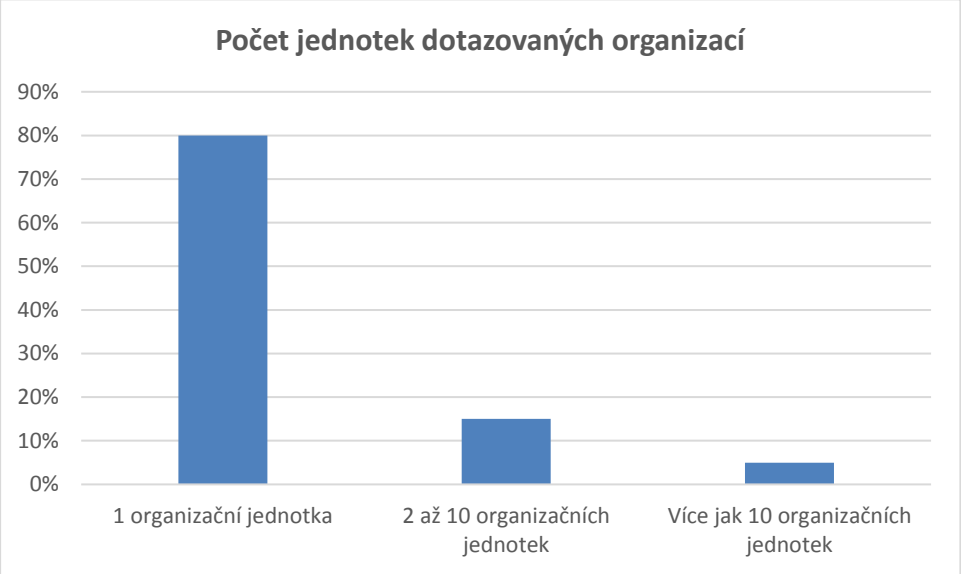
c) Roční obrat



Graf. 5.7: Roční obrat dotazovaných organizací (vlastní zdroj)

Z dotazovaných organizací celkem 45 % má roční obrat v rozmezí 1 mil. až 100 mil. Kč. Druhou nejvíce zastoupenou kategorií jsou organizace s obratem více jak 1 mld. Kč. Nejmenší počet organizací má roční obrat v rozmezí 100 mil. až 1 mld. Kč.

d) Počet jednotek



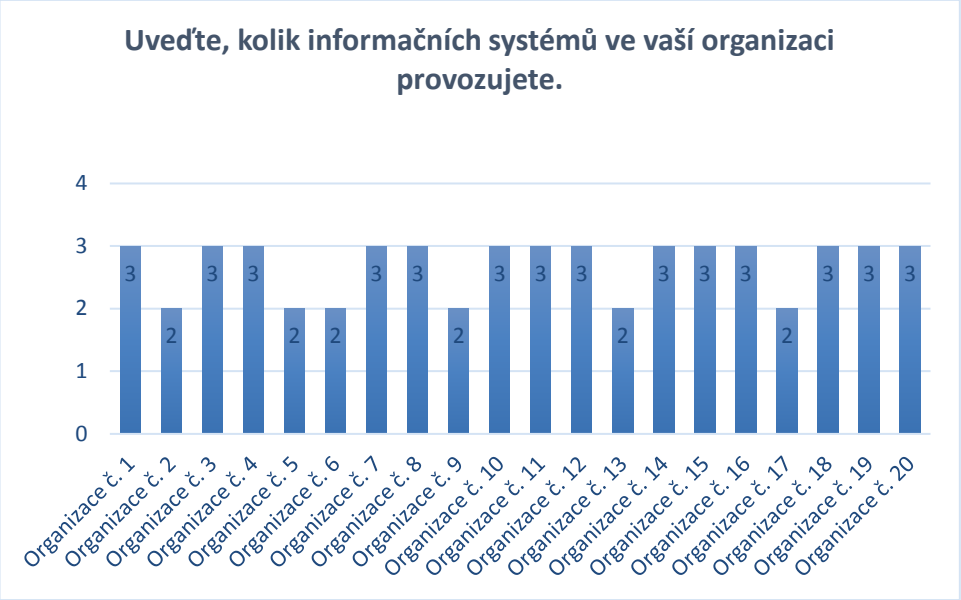
Graf 5.8: Počet jednotek dotazovaných organizací (vlastní zdroj)

Z oslovených organizací má celkem 80 % pouze jednu organizační jednotku. Z této skutečnosti lze konstatovat, že velká část organizací, které lze zařadit mezi malé a střední organizace má pouze jednu mateřskou jednotku. Celkem 15 % pak provozuje dvě a více organizačních jednotek (maximálně však deset). Nejmenší počet organizací (5 %) pak provozuje 10 organizačních jednotek.

Informační systémy organizace

Otázka č. 1

Uveďte, kolik informačních systémů v organizaci provozujete.

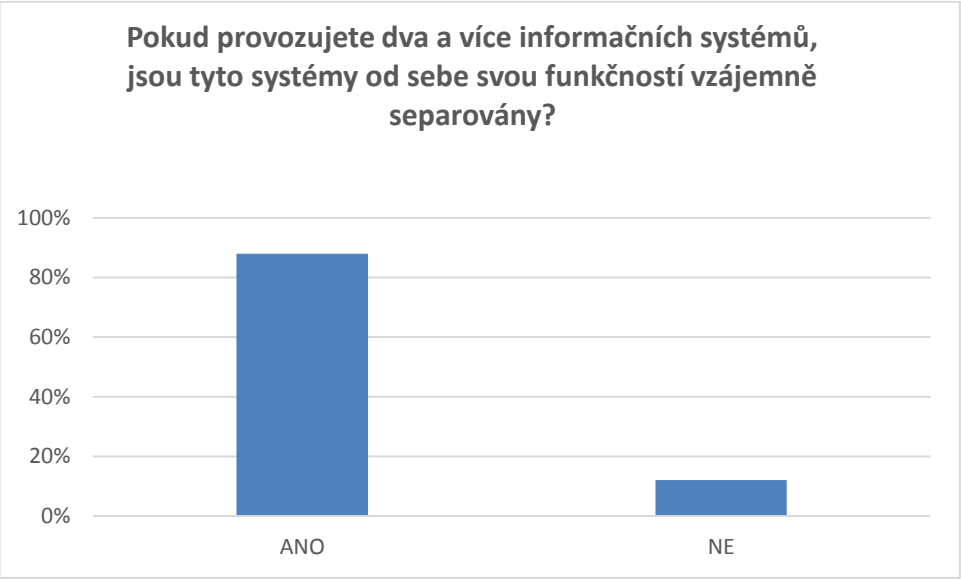


Graf 5.9: Otázka č. 1 a odpovědi jednotlivých respondentů (vlastní zdroj)

Nejvíce respondentů (70 %) uvedlo, že v organizaci používají tři informační systémy. Tato otázka je v dotazníku zařazena z důvodu charakteristiky informačního prostředí organizace.

Otázka č. 2

Pokud provozujete dva nebo více informačních systémů, jsou tyto systémy od sebe svou funkčností vzájemně separovány?



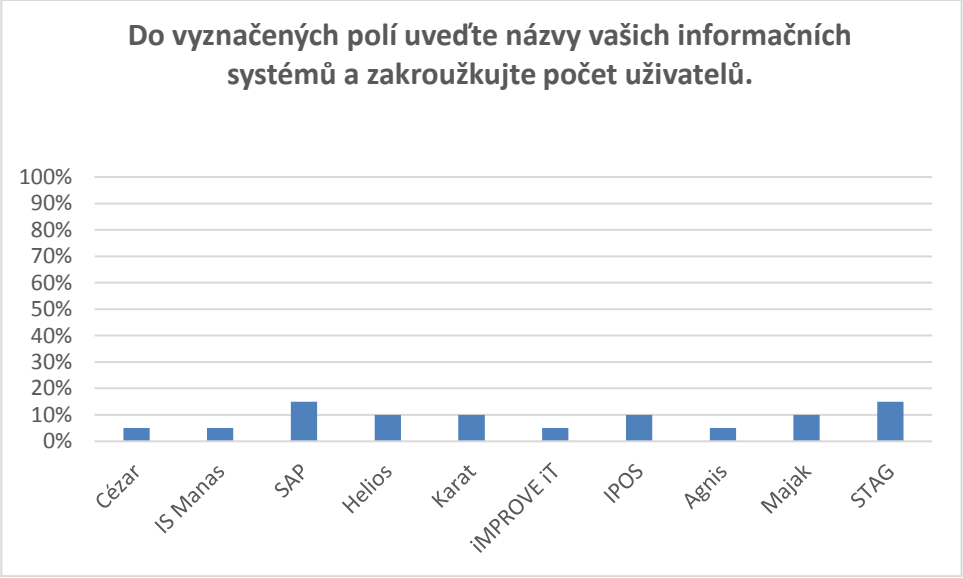
Graf 5.10: Otázka č. 2 a odpovědi jednotlivých respondentů (vlastní zdroj)

Celkem 85 % uvedlo, že jsou jejich informační systémy z pohledu funkčnosti vzájemně separovány. Pokud by byla výrazně omezena funkce jednoho z těchto informačních systémů, organizace by byla schopna bez výraznějších problémů fungovat dál. U tohoto typu organizací nehrozí vznik domino efektu. V případě výpadku dvou nebo tří informačních systémů by zajištění fungování organizace již představovalo velký problém. Zajištění základních funkcí by bez podpory ICT technologií nebylo možné.

Zbylých 15 % pak uvedlo, že jsou jejich informační systémy vzájemně provázány a funkce jednoho systému může ovlivnit funkce jiných informačních systémů. U tohoto typu organizací můžeme mluvit o případném vzniku domino efektu, který by se mohl šířit z jednoho nefunkčního IS na další informační systémy.

Otázka č. 3

Do vyznačených polí uveďte názvy vašich informačních systémů.



Graf 5.11: Otázka č. 3 a odpovědi jednotlivých respondentů (vlastní zdroj)

Pro upřesnění významu jednotlivých informačních systémů pro organizaci jsou zde uvedeny základní funkce každého IS.

1) Cézar

Jedná se o ekonomický informační systém, který je určen především pro vedení skladového hospodářství, provádění inventur, vedení marketingových kampaní,

provádění hromadných fakturací apod. Jeho základní funkcí je zajistit ekonomický chod organizace.

2) IS Manas

Informační systém Manas je používán v obchodní sféře jako pokladní systém. V rámci dotazníkového šetření je tento systém používán jednou organizací, která je zaměřena na distribuci a prodej potravinářského a nepotravinářského zboží. IS Manas je tedy využíván především pro evidenci zboží, tvorbu objednávek a jejich odesílání, evidenci faktur nebo tvorbu uzávěrky pokladny.

3) SAP

Informační systém SAP je určen pro správu ekonomické agendy. Jedná se o ERP systém, který slouží např. pro vedení finančního účetnictví, controlling, evidenci majetku, plánování dlouhodobých projektů, řízení lidských zdrojů, plánování výroby, podpory prodeje, řízení toku dokumentů apod. Jedná se o nejběžnější ERP systém na českém trhu. Z dotazovaných organizací je využíván 15 % organizací.

4) Helios

Jedná se o ekonomický informační systém, který slouží pro správu fakturace, účetnictví, mezd, skladu, business intelligence nebo objednávek. Informační systém Helios lze pořídit v podobě několika modulů, které se liší svými funkcemi. Z dotazovaných respondentů používá tento informační systém 10 % organizací.

5) Karat

Informační systém Karat, který je používán v 10 % procentech dotazovaných organizací, je svou podstatou zaměřen především na správu výrobních a obchodních procesů. Tento informační systém disponuje širokou škálovatelností, flexibilitou a modularitou a je certifikován podle normy ČSN ISO 9001:2008.

6) IMPROVE IT

Jedná se o výrobní informační systém, který je určen pro řízení výrobních zakázek, provádění analýz a navrhování řešení problematických jevů, vyhodnocování parametrů výroby konkrétního výrobku, sledování aktivit jednotlivých operátorů, zajištění správného toku informací s jinými informačními systémy apod. Tento informační systém používá celkem 5 % dotazovaných organizací.

7) IPOS

Tento informační systém je určen pro stavební organizace. Jeho primárním cílem je poskytovat potřebné údaje pro snižování nákladů s využitím principu procesního nákladového řízení. Informační systém IPOS je rozdělen na výrobní a ekonomickou část. Mezi dotazovanými organizacemi je tento systém používán v 10 % případů.

8) Agnis

Informační systém Agnis je určen pro oblast hotelnictví. Jedná se o ubytovací a pokladní systém. Tento informační systém umožňuje provádět on-line rezervace, řízení skladování potravin, řízení časových aktivit jednotlivých hostů, vést přehled obsazenosti daného hotelu apod. V rámci dotazníkového šetření je tento informační systém využíván jednou organizací (5 %).

9) Majak

Jedná se o ekonomický, obchodní a výrobní informační systém. Mezi základní funkce tohoto informačního systému patří evidence majetku, skladového hospodářství, personalistiky, mezd, faktur nebo skladového hospodářství. Systém lze konfigurovat a nastavit různá pracovní prostředí. Tento informační systém používá celkem 10 % z dotazovaných organizací.

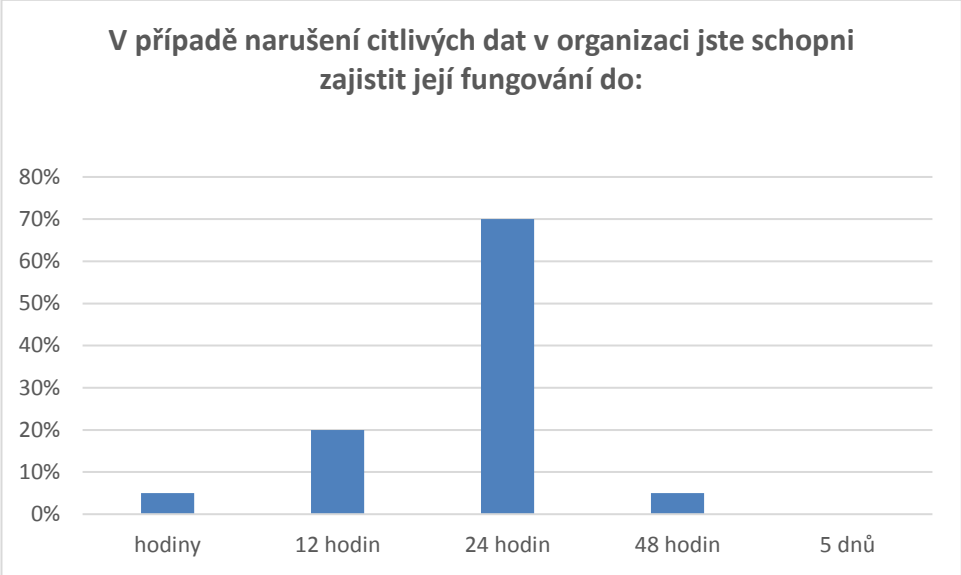
10) STAG

Informační systém STAG je používán především ve vysokoškolském prostředí a jeho hlavní funkcí je evidence studentů, správa kvalifikačních prací, prezentace rozvrhů, správa studijních oborů a programů, zadávání a evidence známek nebo obsazenost jednotlivých učeben. Při realizaci dotazníkového šetření bylo zjištěno, že tento informační systém je využíván třemi organizacemi (vysokými školami).

Datová bezpečnost a obnovitelnost funkce organizace

Otázka č. 4

V případě narušení citlivých dat v organizaci jste schopni zajistit její fungování do:

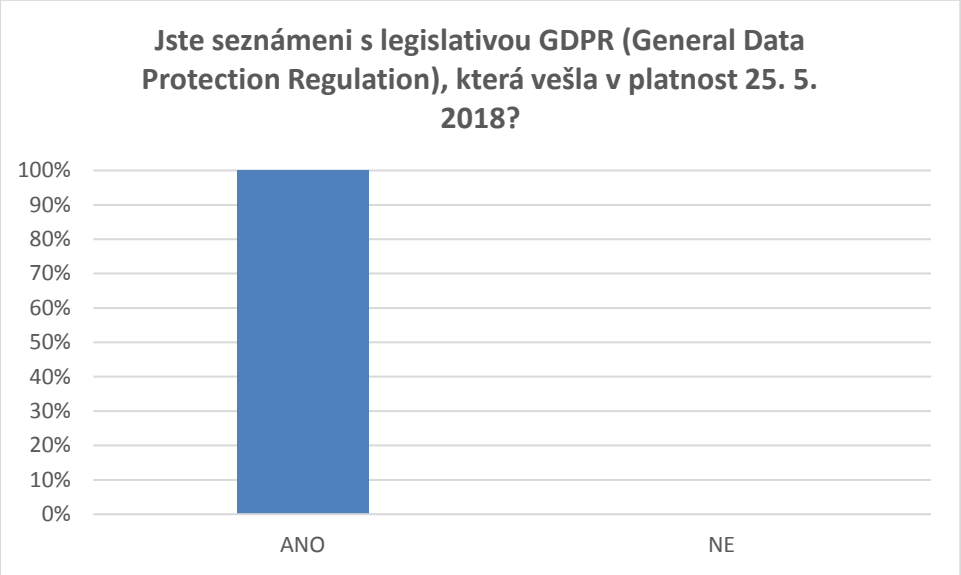


Graf 5.12: Otázka č. 4. a odpovědi jednotlivých respondentů (vlastní zdroj)

Z dotazovaných respondentů odpovědělo celkem 70 %, že je v případě realizace kybernetické hrozby schopno zajistit fungování své organizace do 24 hodin. Druhou nejčastější odpovědí byla obnova fungování do 12 hodin. Možnosti do jedné hodiny a 48 hodin pak získaly 5 %. Odpověď do 5 dnů neoznačil žádný z referenčních objektů. Odpovědi na tuto otázku budou v rámci návrhu algoritmu použity pro stanovení doby, po kterou by měl být kompenzován ušlý obrat organizace.

Otázka č. 5

Jste seznámeni s legislativou GDPR (General Data Protection Regulation), která vešla v platnost 25. května 2018?

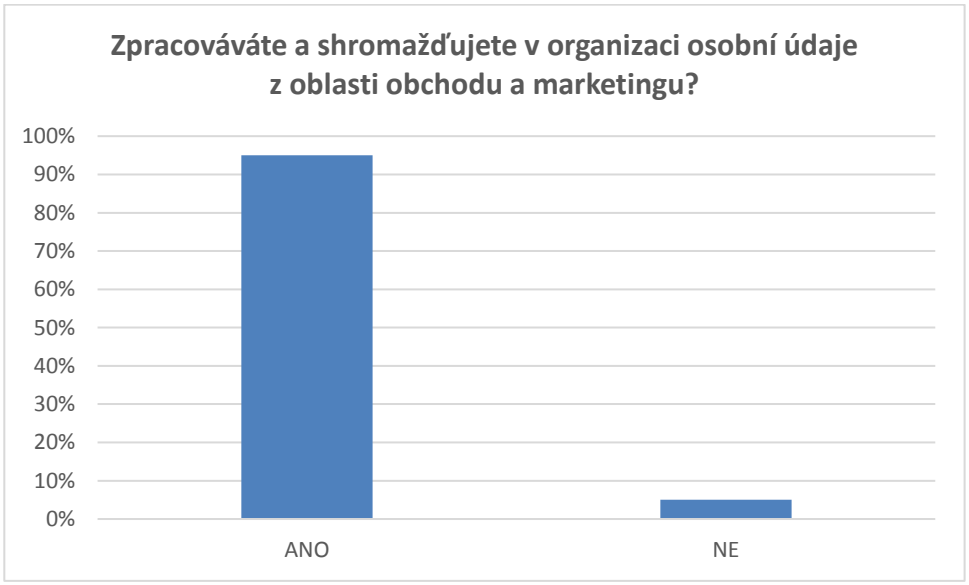


Graf 5.13: Otázka č. 5 a odpovědi jednotlivých respondentů (vlastní zdroj)

Na otázku č. 5 odpověděli všichni respondenti, že jsou s legislativou GDPR seznámeni. Dotazovaní také uvedli, že znají obsah tohoto nařízení a popis implementace v organizaci. Všechny organizace také mají zřízeného pověřence pro zajištění ochrany osobních údajů.

Otázka č. 6

Zpracováváte a shromažďujete v organizaci údaje z oblasti obchodu a marketingu?

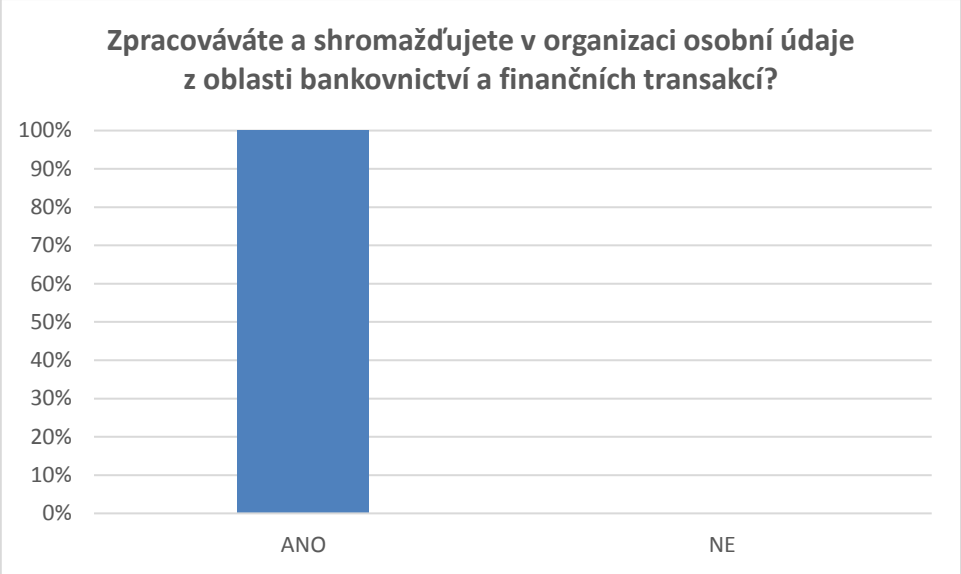


Graf 5.14: Otázka č. 6 a odpovědi jednotlivých respondentů (vlastní zdroj)

Z dotazovaných respondentů 95 % uvedlo, že zpracovává a shromažďuje v organizaci údaje z oblasti obchodu a marketingu. Pouze 5 % uvedlo (jedná se o jednu organizaci), že tyto údaje nezpracovává ani neshromažďuje. Tato otázka byla zařazena do dotazníkového šetření z důvodu identifikace citlivých informací, které souvisí s dobrým jménem organizace.

Otázka č. 7

Zpracováváte a shromažďujete v organizaci osobní údaje z oblasti bankovnictví a finančních transakcí?

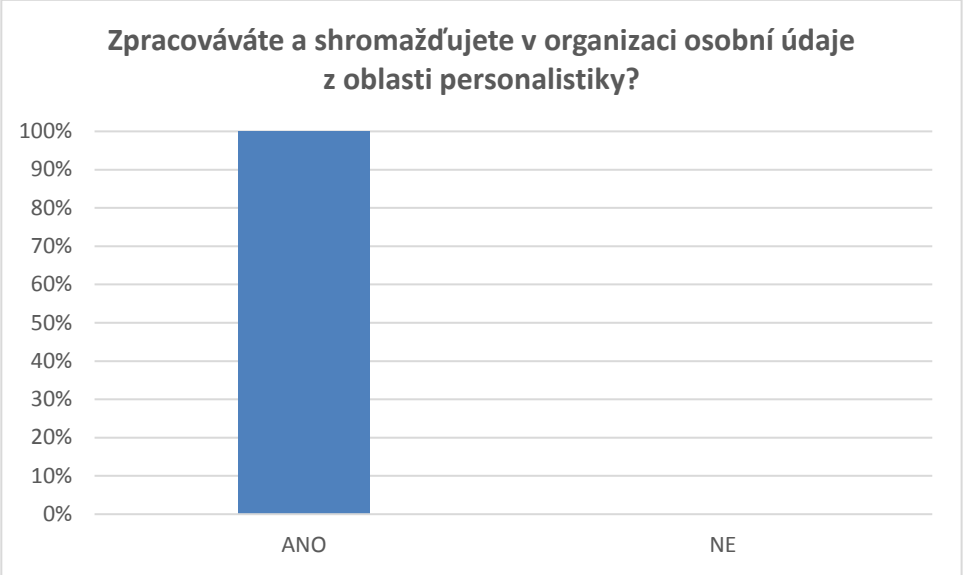


Graf 5.15: Otázka č. 7 a odpovědi jednotlivých respondentů (vlastní zdroj)

Na otázku č. 7 odpovědělo 100 % respondentů, že ve své organizaci zpracovává a shromažďuje osobní údaje (tj. údaje týkající se konkrétních osob) z oblasti bankovnictví a finančních transakcí. Tato otázka zde byla zařazena z důvodu zjištění významnosti osobních údajů pro pojištění proti kybernetickým hrozbám. Na základě tohoto typu údajů mohou být organizaci uděleny pokuty, které by také měly být kompenzovány tímto typem pojištění.

Otázka č. 8

Zpracováváte a shromažďujete v organizaci osobní údaje z oblasti personalistiky?

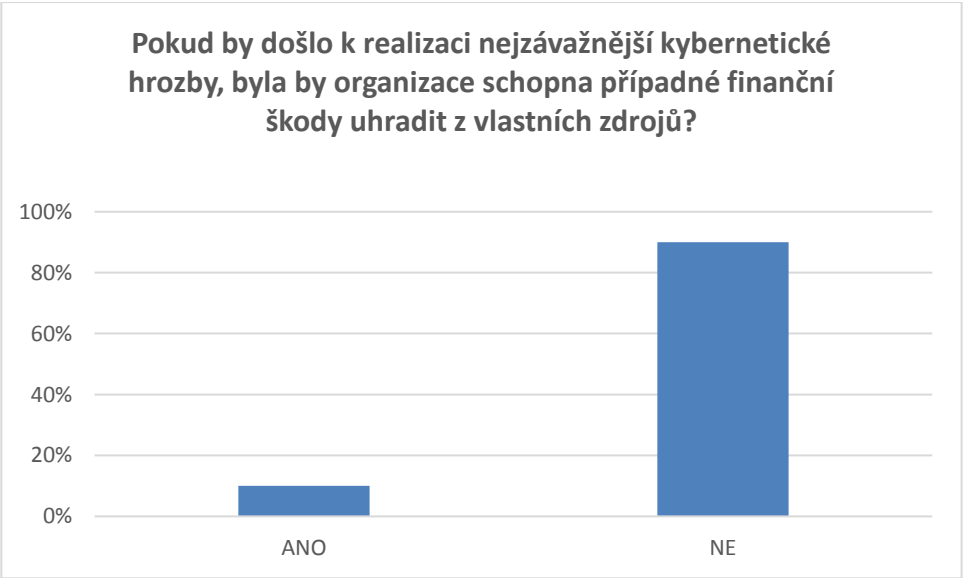


Graf 5.16: Otázka č. 8 a odpovědi jednotlivých respondentů (vlastní zdroj)

Z dotazovaných organizací uvedlo celkem 100 %, že zpracovává pro své vnitřní potřeby osobní údaje z oblasti personalistiky. Tyto údaje se týkají především zaměstnanců a zákazníků. Tato otázka zde byla zařazena z důvodu zjištění významnosti osobních údajů pro pojištění proti kybernetickým hrozbám.

Otázka č. 9

Pokud by došlo k realizaci nejzávažnější kybernetické hrozby, byla by organizace schopna případné finanční škody uhradit z vlastních zdrojů?



Graf 5.17: Otázka č. 9 a odpovědi jednotlivých respondentů (vlastní zdroj)

Na otázku č. 9 odpovědělo celkem 90 % dotazovaných organizací, že by jejich vedení nebylo schopno vlastními finančními prostředky zvládnout dopady kybernetické hrozby na fungování organizace. Pouze 10 % uvedlo, že by se s takovou nežádoucí situací dokázali vyrovnat pomocí vlastních peněžních prostředků. Vzhledem k tomu, že počet organizací, které by nebyly schopny zvládnout dopady kybernetických hrozeb vlastními finančními prostředky, tvoří 90 % dotazovaných, mohlo by být pojištění proti kybernetickým hrozbám aplikováno jako vhodný nástroj pro kompenzaci vzniklých nákladů.

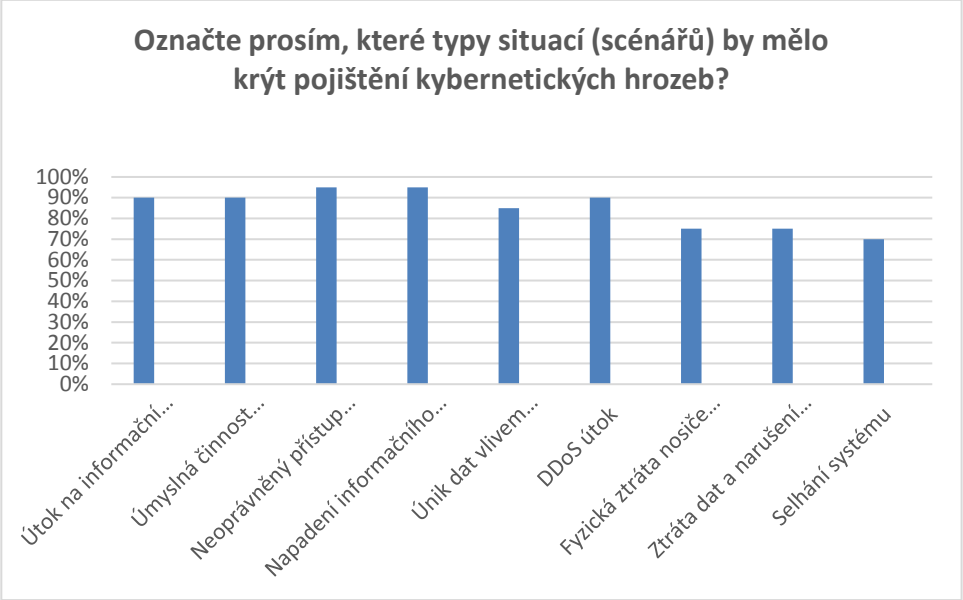
Typy kybernetických hrozeb

Otázka č. 10

Označte prosím, které typy situací (scénářů) by mělo krýt pojištění kybernetických hrozeb.

Mezi možné odpovědi lze zařadit následující scénáře kybernetických hrozeb:

- útok na informační systém prostřednictvím ransomware,
- úmyslná činnost trestná prováděna hackerem,
- neoprávněný přístup do informačního systému,
- napadení informačního systému prostřednictvím malware,
- únik dat vlivem nedbalosti zaměstnance,
- DDoS útok,
- fyzická ztráta nosiče dat (ztráta notebooku),
- ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje,
- selhání systému.



Graf 5.18: Otázka č. 10 a odpovědi jednotlivých respondentů (vlastní zdroj)

Na otázku č. 10 odpovědělo:

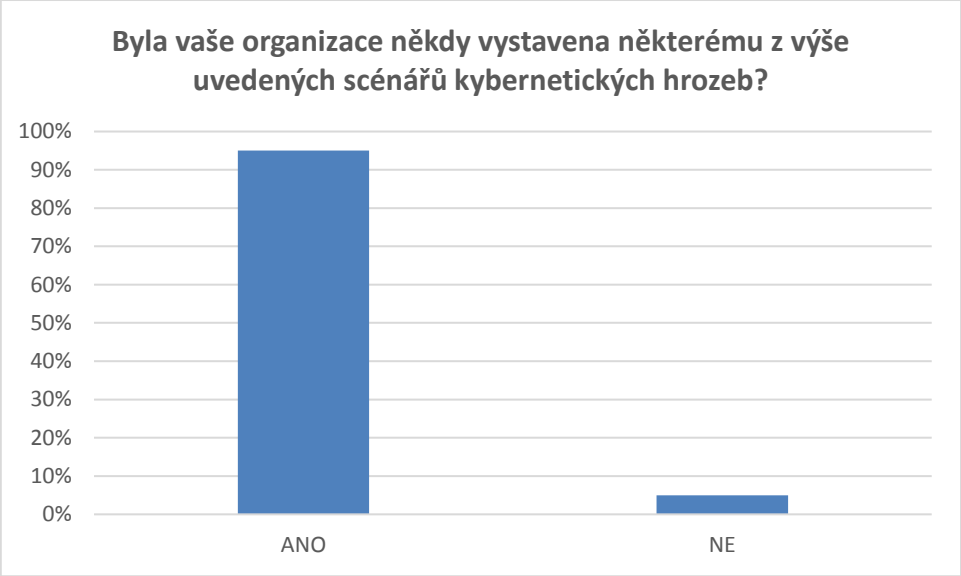
- 90 % dotazovaných respondentů, že pojištění proti kybernetickým hrozbám by mělo krýt útok na informační systém prostřednictvím ransomware,
- 90 % dotazovaných respondentů, že pojištění proti kybernetickým hrozbám by mělo krýt úmyslnou trestnou činnost prováděnou hackerem,
- 95 % dotazovaných respondentů, že pojištění proti kybernetickým hrozbám by mělo krýt neoprávněný přístup do informačního systému,
- 95 % dotazovaných respondentů, že pojištění proti kybernetickým hrozbám by mělo krýt napadení informačního systému prostřednictvím malware,
- 85 % dotazovaných respondentů, že pojištění proti kybernetickým hrozbám by mělo krýt únik dat vlivem nedbalosti zaměstnance,
- 90 % dotazovaných respondentů, že pojištění proti kybernetickým hrozbám by mělo krýt DDoS útok,
- 75 % dotazovaných respondentů, že pojištění proti kybernetickým hrozbám by mělo krýt fyzickou ztrátu nosiče dat (ztráta notebooku),
- 75 % dotazovaných respondentů, že pojištění proti kybernetickým hrozbám by mělo krýt ztrátu dat a narušení funkce informačního systému organizace vlivem bleskového výboje,
- 70 % dotazovaných respondentů uvedlo, že by pojištění proti kybernetickým hrozbám mělo krýt selhání systému, které nastalo z jiných příčin, než které jsou uvedeny v předchozích bodech.

Podle odpovědí dotazovaných respondentů lze usoudit, že uvažované scénáře kybernetických hrozeb jsou vnímány jako velmi závažné. Velká část organizací, které byly předmětem dotazníkového setření by uvítaly, aby v případě pojištění byly proti těmto typům kybernetických hrozeb chráněny.

Otázka č. 11

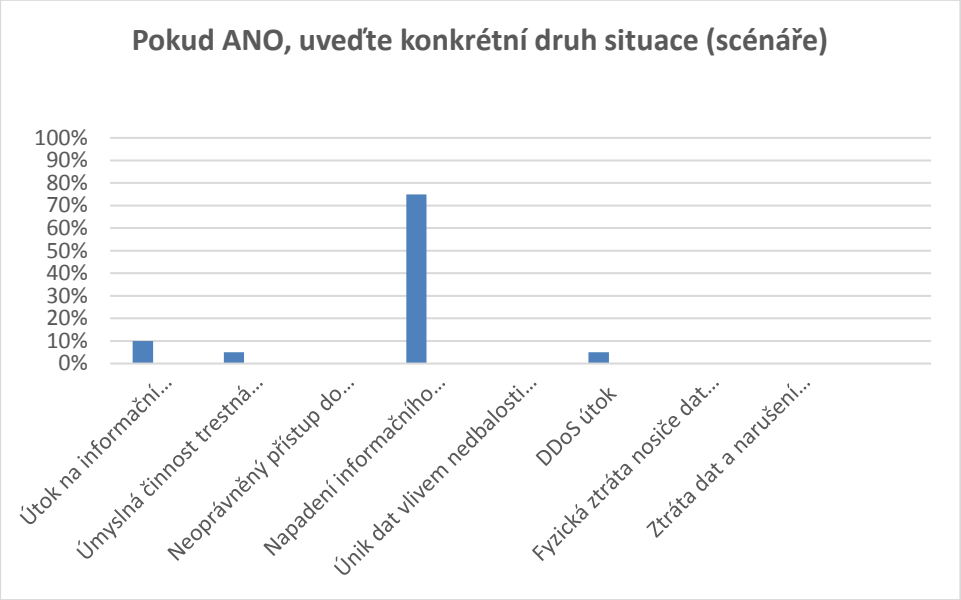
Byla vaše organizace někdy vystavena některému z výše uvedených scénářů kybernetického rizika? Pokud ANO, uveďte konkrétní druh situace (scénáře).

Tato otázka je zde z důvodu složitosti rozdělena do dvou grafických zpracování. První graf zobrazuje část otázky, která je zaměřena na to, jestli byly dotazované organizace vystaveny některému z výše uvedených typů kybernetických hrozeb.



Graf 5.19: Otázka č. 11.1 a odpovědi jednotlivých respondentů (vlastní zdroj)

Celkem 95 % organizací uvedlo, že někdy v minulosti bylo napadeno některým typem z výše uvedených kybernetických hrozeb. Následující graf je pak zaměřen na druhou část otázky, ve které v případě kladné odpovědi měli dotazovaní respondenti uvést konkrétní příklady kybernetických hrozeb, kterým byli vystaveni.



Graf 5.20: Otázka č. 11.2 a odpovědi jednotlivých respondentů (vlastní zdroj)

Nejvíce organizací uvedlo, že bylo napadeno některým typem škodlivého softwaru malware. Tato hrozba byla uvedena v 75 % případů. Druhou nejčastější hrozbou, které byly dané organizace vystaveny, byl ransomware, který získal 10 %. Třetí kybernetickou hrozbou pak byla úmyslná trestná činnost prováděna hackerem (5 %) a DDoS útok (5 %).

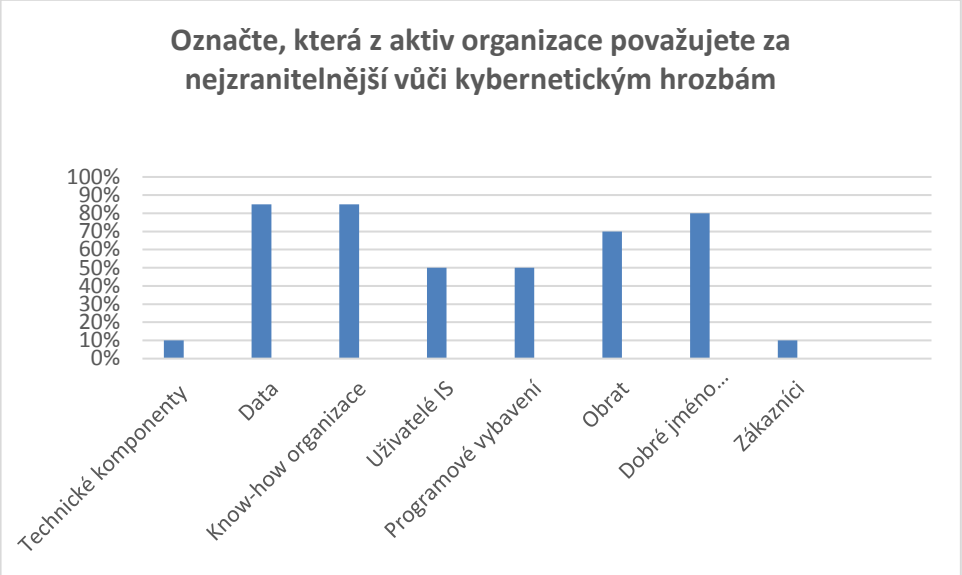
Připravenost organizace v oblasti kybernetické bezpečnosti

Otázka č. 12

Označte, která z aktiv organizace považujete za nejzranitelnější vůči kybernetickým hrozbám?

Mezi možné odpovědi lze zařadit:

- technické komponenty IS,
- data,
- know-how organizace,
- uživatelé IS,
- programové vybavení,
- obrat,
- dobré jméno organizace,
- zákazníci.

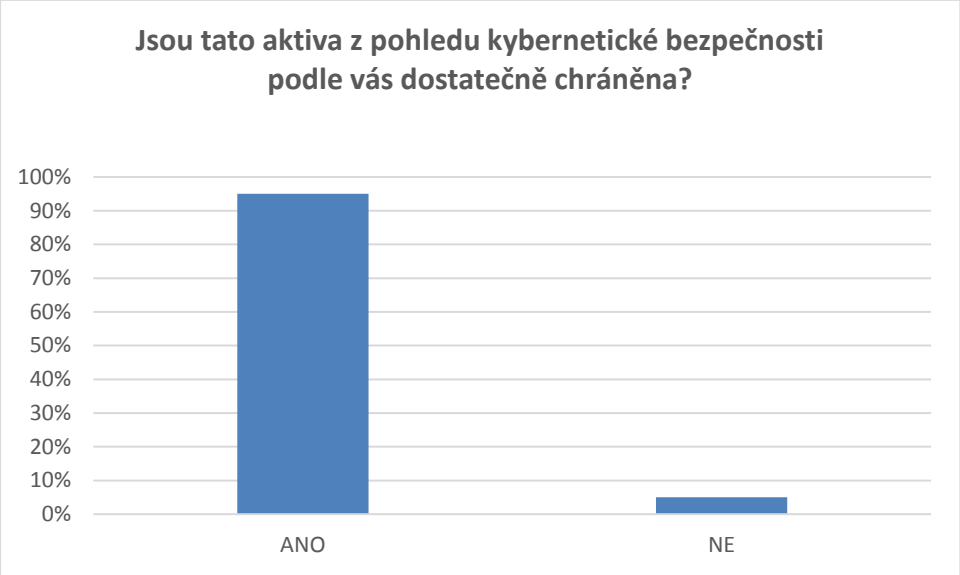


Graf 5.21: Otázka č. 12 a odpovědi jednotlivých respondentů (vlastní zdroj)

Na otázku č. 12 odpovědělo 85 % dotazovaných respondentů, že za nejzranitelnější aktiva považují data a know-how organizace. Dobré jméno organizace získalo 80 %. Dalším důležitým aktivem je podle vybraných organizací obrat. Uživatelé IS a programové vybavení získali celkem 50 %. Posledními aktivy z pohledu zranitelnosti byly technické komponenty a zákazníci, které získali 10 %.

Otázka č. 13

Jsou tato aktiva z pohledu kybernetické bezpečnosti podle vás dostatečně chráněna?

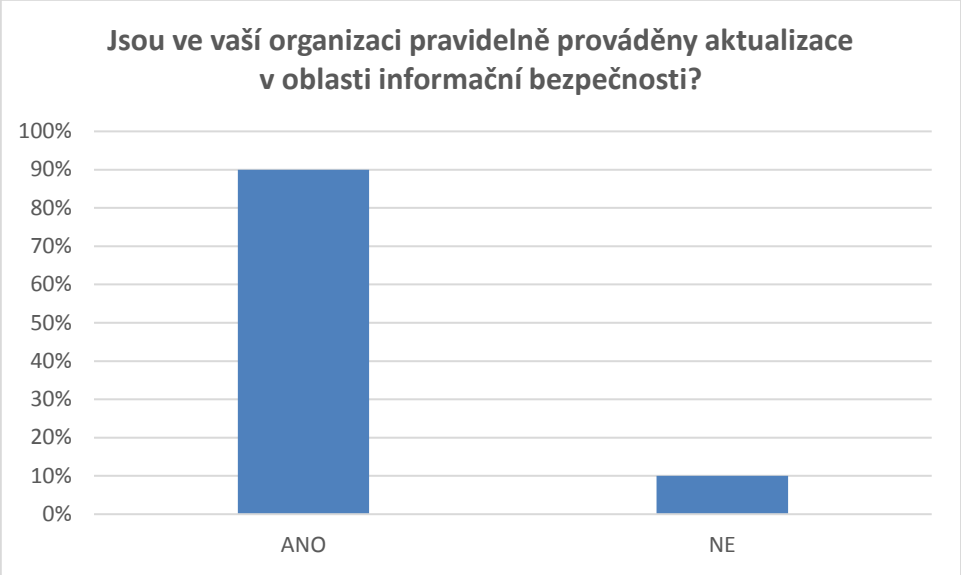


Graf 5.22: Otázka č. 13 a odpovědi jednotlivých respondentů (vlastní zdroj)

Na otázku č. 13 odpovědělo 95 % organizací, že jsou tato vybraná aktiva dostatečně chráněna. Jako efektivní způsob zajištění ochrany těchto aktiv považují tyto organizace hardwarové a softwarové prvky (především antivirus, režimová bezpečnostní opatření apod.). Pouze jedna organizace (5 %) uvedla, že by zabezpečení těchto aktiv mohlo být z jejich pohledu na vyšší úrovni.

Otázka č. 14

Jsou ve vaší organizaci pravidelně prováděny aktualizace v oblasti informační bezpečnosti? (pravidelné kontroly komponent informačního systému, zálohování dat, aktualizace software, změna hesel, aktualizace dokumentu bezpečnostní politiky apod.)

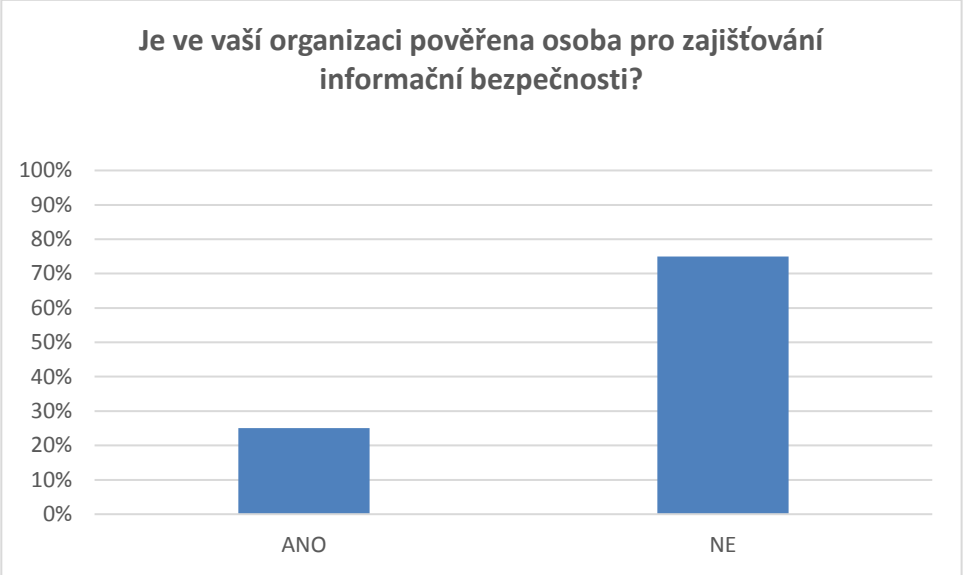


Graf 5.23: Otázka č. 14 a odpovědi jednotlivých respondentů (vlastní zdroj)

V případě otázky č. 14 odpovědělo 90 % dotazovaných, že jsou v jejich organizaci prováděny pravidelné aktualizace v oblasti informační bezpečnosti. Tyto aktualizace zahrnují především pravidelné kontroly komponent informačního systému, zálohování dat, aktualizace software, změnu hesel, aktualizace dokumentu bezpečnostní politiky apod. Celkem 10 % pak uvedlo, že tyto aktualizace nejsou prováděny v pravidelných periodách.

Otázka č. 15

Je ve vaší organizaci pověřena osoba pro zajišťování informační bezpečnosti?

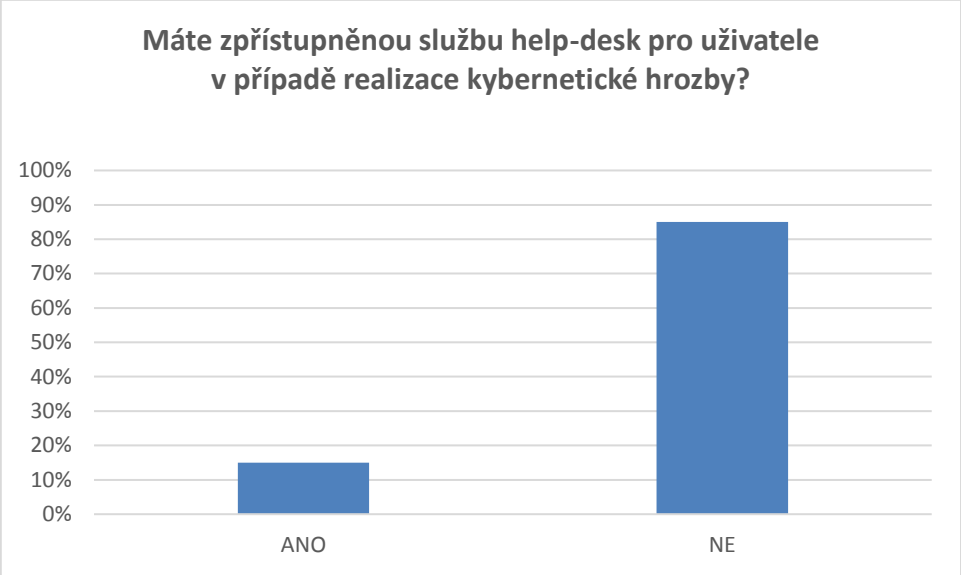


Graf 5.24: Otázka č. 15 a odpovědi jednotlivých respondentů (vlastní zdroj)

Celkem 75 % dotazovaných respondentů odpovědělo, že v jejich organizaci není pověřena osoba pro zajišťování bezpečnosti. Tato skutečnost je vnímána jako velmi nestandardní, obzvláště v případech, kdy se jedná o organizace, ve kterých je bezpečnost informačních systémů vnímána jako jedna z priorit politiky organizace. Absence osoby pro zajišťování informační bezpečnosti může být použita jako argument pro nepojištění dané organizace proti kybernetickým hrozbám. Zbylých 25 % odpovědělo, že pro zajištění informační bezpečnosti je v jejich organizaci pověřena konkrétní osoba.

Otázka č. 16

Máte zpřístupněnou službu help-desk pro uživatele v případě realizace kybernetické hrozby?

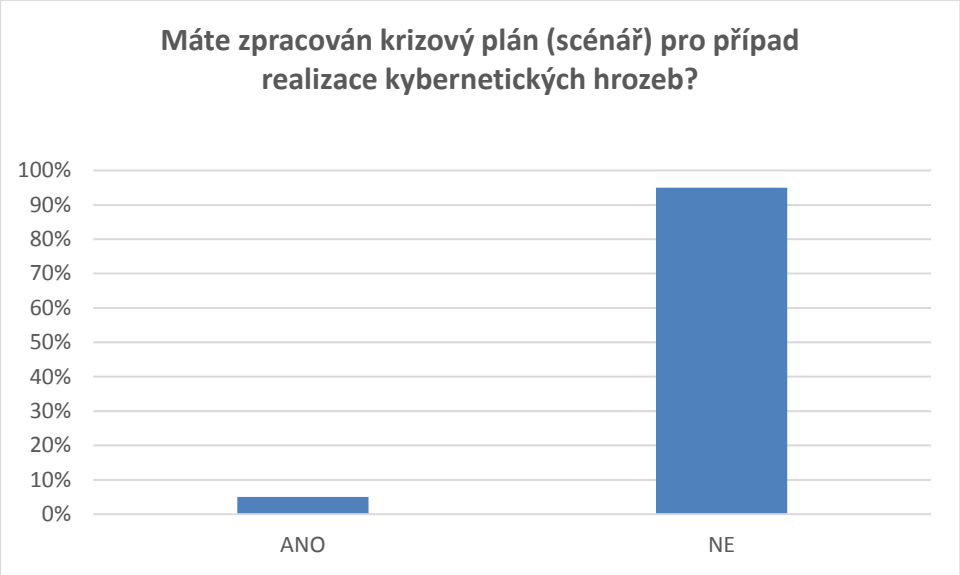


Graf 5.25: Otázka č. 16 a odpovědi jednotlivých respondentů (vlastní zdroj)

Na otázku č. 16, která byla zaměřena na přístupnost služby help-desk, odpovědělo 85 % z dotazovaných organizací, že tuto službu nemá zpřístupněnou. Pouze 15 % uvedlo, že uživatelé mohou využít službu help-desk v případě realizace kybernetické hrozby v jejich organizaci. Tato otázka je do dotazníkového šetření zařazena z důvodu zjištění využitelnosti a případných nákladů na zajištění této služby.

Otázka č. 17

Máte zpracován krizový plán (scénář) pro případ realizace kybernetických hrozeb?



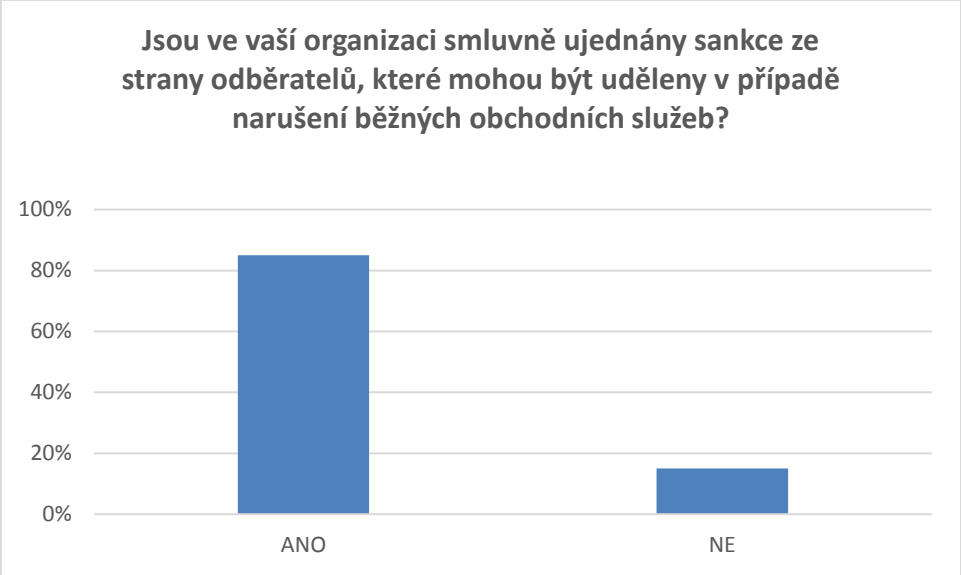
Graf 5.26: Otázka č. 17 a odpovědi jednotlivých respondentů (vlastní zdroj)

Z dotazovaných respondentů odpovědělo 95 %, že pro případ realizace kybernetické hrozby nemá zpracován žádný krizový plán nebo dokument, ve kterém by byl popsán přesný postup řešení takové situace. Tato skutečnost je velmi překvapivá, protože některé organizace vzhledem k jejich velikosti a druhu podnikání by takové krizové scénáře měli mít zpracovány.

Tento faktor může být brán potenciální pojišťovnou, která poskytuje pojištění proti kybernetickým hrozbám, jako negativní ukazatel nedostatečného zabezpečení organizace. Pouze jeden referenční objekt měl v rámci své bezpečnostní politiky zpracován plán, jak postupovat v případě takové události.

Otázka č. 18

Jsou ve vaší organizaci smluvně ujednány sankce ze strany odběratelů, které mohou být uděleny v případě narušení běžných obchodních služeb?



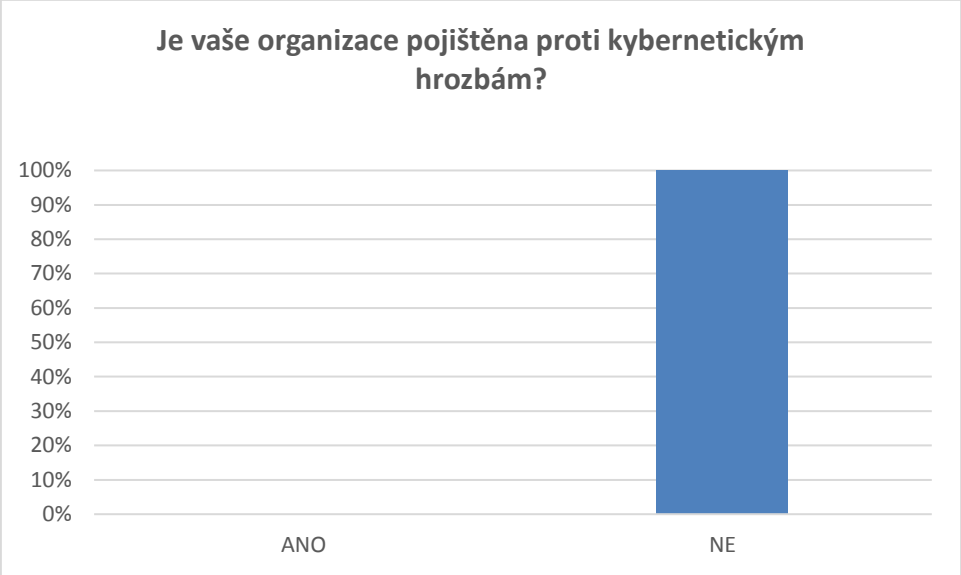
Graf 5.27: Otázka č. 18 a odpovědi jednotlivých respondentů (vlastní zdroj)

Na otázku č. 18 odpovědělo celkem 85 % organizací, že v případě narušení obchodních vztahů mohou být ze strany odběratelů uděleny pokuty. Tyto pokuty mohou být uděleny za nedodávání zboží nebo materiálu v určitém časovém období, které je smluvně ujednáno mezi oběma obchodními partnery. Celkem 15 % odpovědělo, že možnost sankcí ze strany odběratelů u nich sjednána není.

Rozsah krytí proti kybernetickým hrozbám

Otázka č. 19

Je vaše organizace pojištěna proti kybernetickým hrozbám?



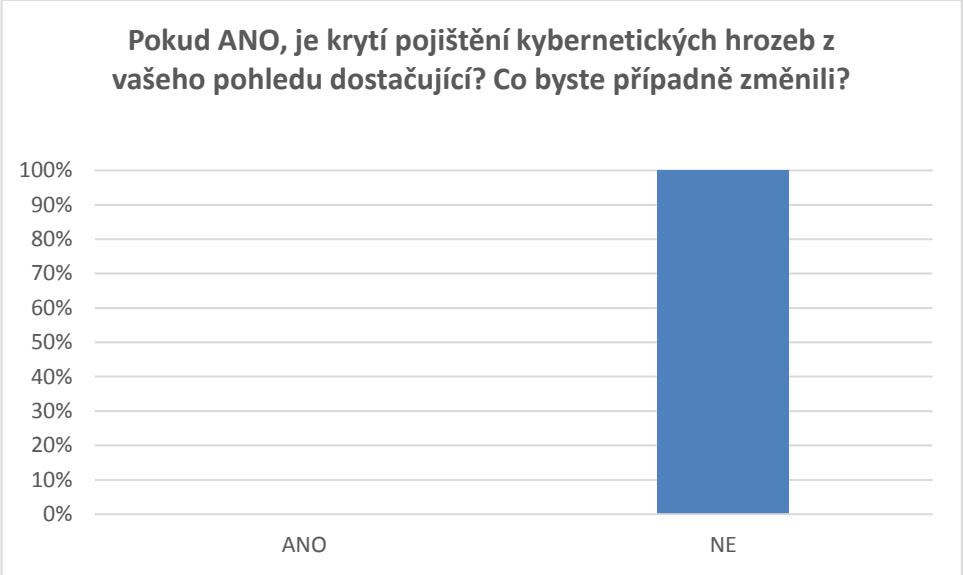
Graf 5.28: Otázka č. 19 a odpovědi jednotlivých respondentů (vlastní zdroj)

Z dotazovaných respondentů 100 % uvedlo, že nemá sjednané pojištění proti kybernetickým hrozbám. Tato otázka zde byla zařazena z důvodu zjištění zájmu o pojištění proti kybernetickým hrozbám na českém trhu. Podle odpovědí jednotlivých respondentů lze konstatovat, že tento typ pojištění není v České republice příliš rozšířen, což potvrzují také jiné informační zdroje (Moláček a Konečný, 2017)

O problematice pojištění proti kybernetickým hrozbám nicméně všichni z dotazovaných subjektů alespoň slyšeli a mají tak základní informace o této oblasti.

Otázka č. 20

Pokud ANO, je krytí pojištění kybernetických hrozeb z vašeho pohledu dostačující? Co byste případně změnili?

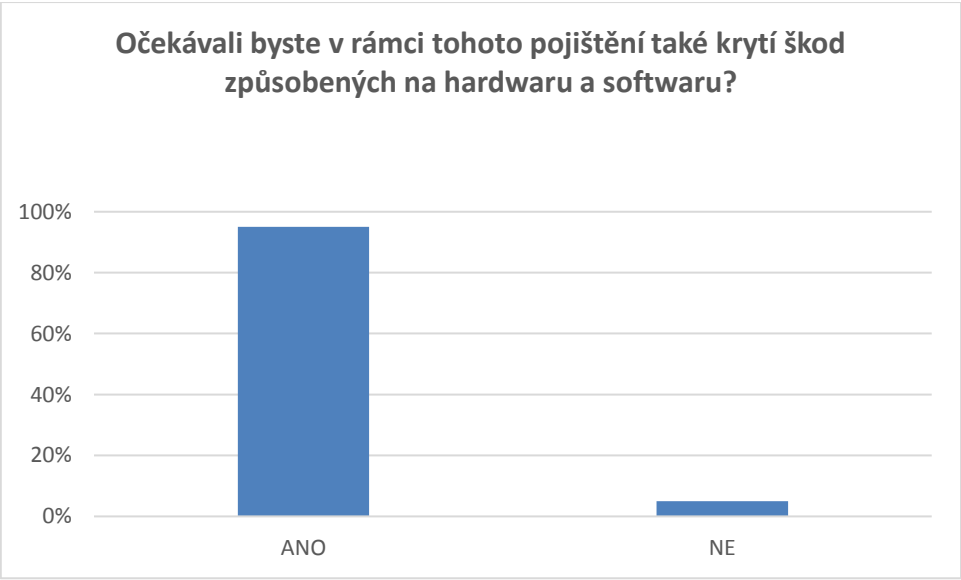


Graf 5.29: Otázka č. 20 a odpovědi jednotlivých respondentů (vlastní zdroj)

Na otázku č. 20 odpovědělo 100 % dotazovaných NE. Žádná z organizací, které byly předmětem dotazníkového šetření, nemá sjednáno pojištění proti kybernetickým hrozbám. Tato otázka zde nebyla, vzhledem k odpovědím na předchozí otázku, více komentována.

Otázka č. 21

Očekávali byste v rámci tohoto pojištění také krytí škod způsobených na hardwaru a softwaru?

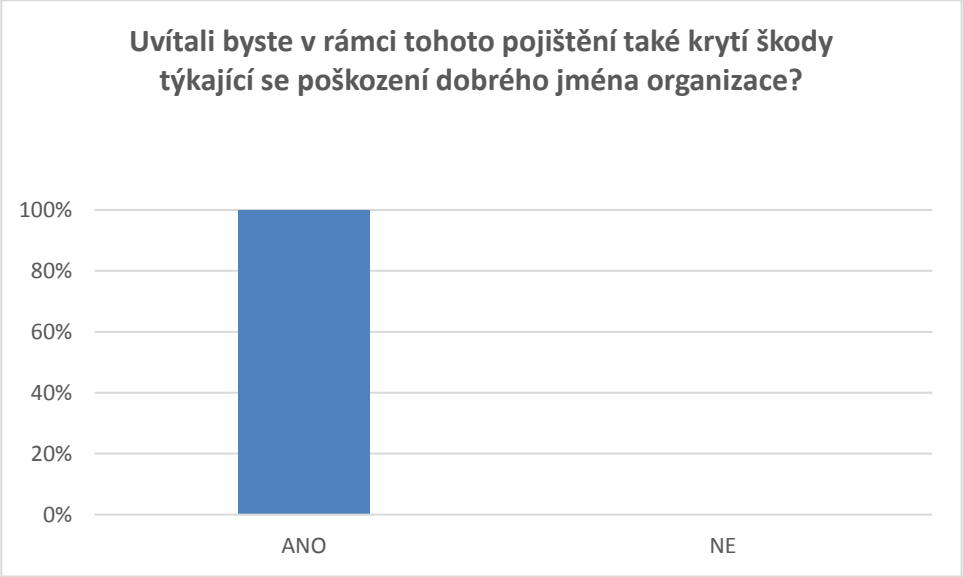


Graf 5.30: Otázka č. 21 a odpovědi jednotlivých respondentů (vlastní zdroj)

Celkem 95 % organizací odpovědělo, že by v rámci pojištění proti kybernetickým hrozbám očekávalo krytí a kompenzaci škod způsobených na hardwaru a softwaru. Tato otázka zde byla zařazena z důvodu ověření potřebnosti hardwaru a softwaru v pojištění proti kybernetickým hrozbám. Pouze 5 % uvedlo, že by tyto škody na hardware a software být kompenzovány nemusely.

Otázka č. 22

Uvítali byste v rámci tohoto pojištění také krytí škody týkající se poškození dobrého jména organizace?

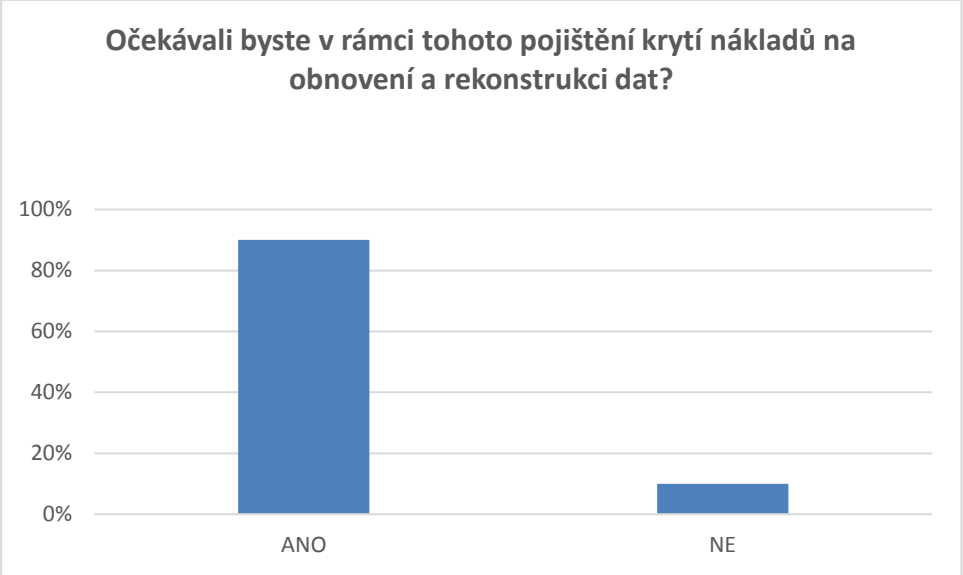


Graf 5.31: Otázka č. 22 a odpovědi jednotlivých respondentů (vlastní zdroj)

V rámci dotazníkového šetření byla tato otázka hodnocena prostřednictvím oslovených respondentů jako nejzásadnější. Dobré jméno organizace je téměř u všech organizací, které byly předmětem dotazníkového šetření, vnímáno jako jedno z nejcitlivějších aktiv. Celkem 100 % dotazovaných respondentů uvedlo, že náklady na případné obnovení dobrého jména by měly být kompenzovány pojištěním proti kybernetickým hrozbám. Tato otázka zde byla zařazena z důvodu ověření významnosti tohoto aktiva v rámci stanovení možných dopadů kybernetických hrozeb na organizaci.

Otázka č. 23

Očekávali byste v rámci tohoto pojištění krytí nákladů na obnovení a rekonstrukci dat?

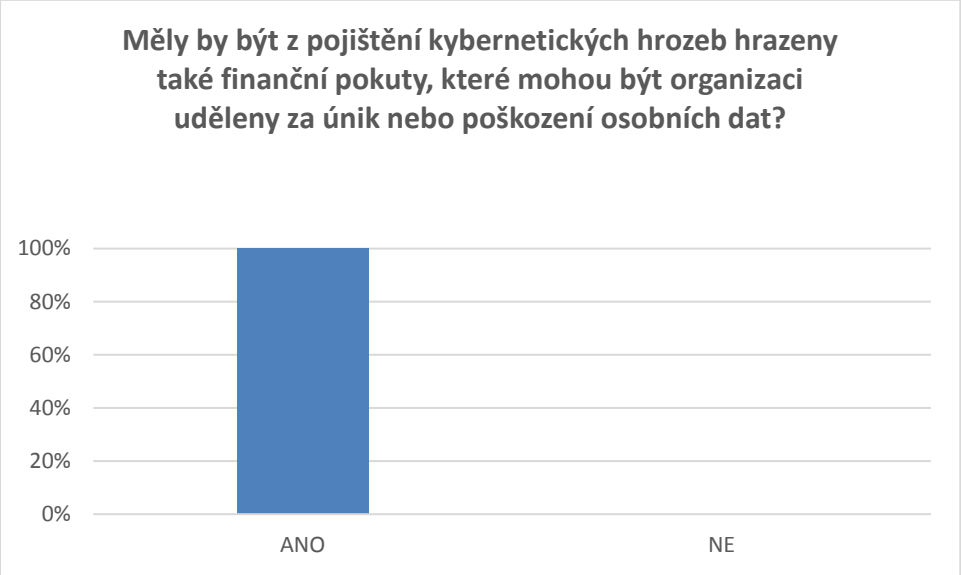


Graf 5.32: Otázka č. 23 a odpovědi jednotlivých respondentů (vlastní zdroj)

Na otázku č. 23 odpovědělo celkem 85 %, že by pojištění proti kybernetickým hrozbám mělo kompenzovat také náklady na obnovení a rekonstrukci dat. Tato otázka zde byla zařazena z důvodu ověření významnosti tohoto prvku v rámci stanovení možných nákladů v rámci pojištění. Pouze 15 % uvedlo, že tyto náklady nemusí být kompenzovány tímto typem pojištěním.

Otázka č. 24

Měly by být z pojištění kybernetických hrozeb hrazeny také finanční pokuty, které mohou být organizaci uděleny za únik nebo poškození osobních dat?

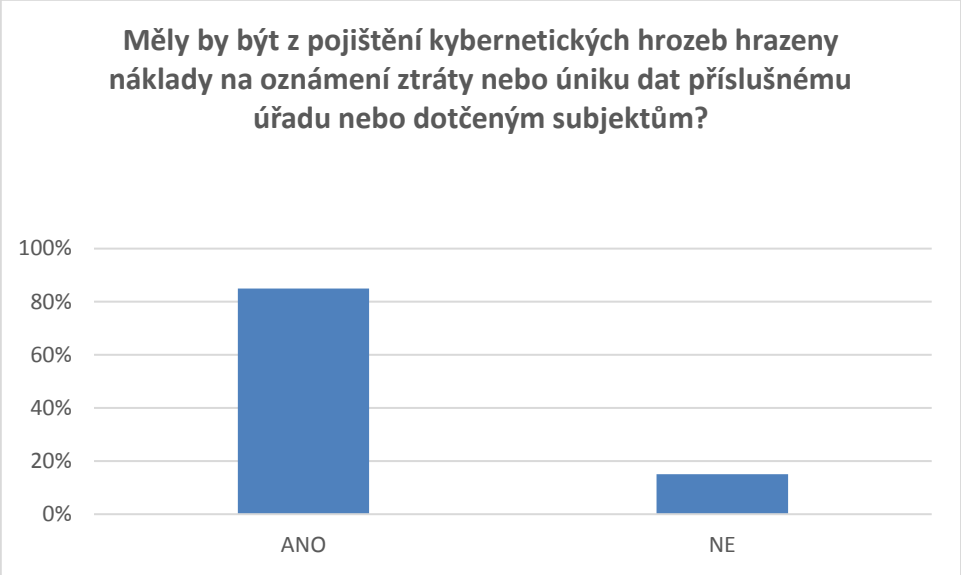


Graf 5.33: Otázka č. 24 a odpovědi jednotlivých respondentů (vlastní zdroj)

Celkem 100 % dotazovaných respondentů uvedlo, že by pojištění kybernetických hrozeb mělo také kompenzovat možné pokuty, které mohou být uděleny na základě porušení bezpečnosti osobních údajů nebo narušení obchodních vztahů ze strany odběratelů. S touto skutečností souvisí platnost Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 (GDPR), kde je stanovena výše pokut, které mohou být organizaci uděleny za únik nebo porušení zabezpečení osobních údajů. Výše těchto pokut je upravena v zákoně č. 110 /2019 Sb., o zpracování osobních údajů.

Otázka č. 25

Měly by být z pojištění kybernetických hrozeb hrazeny náklady na oznámení ztráty nebo úniku dat příslušnému úřadu?

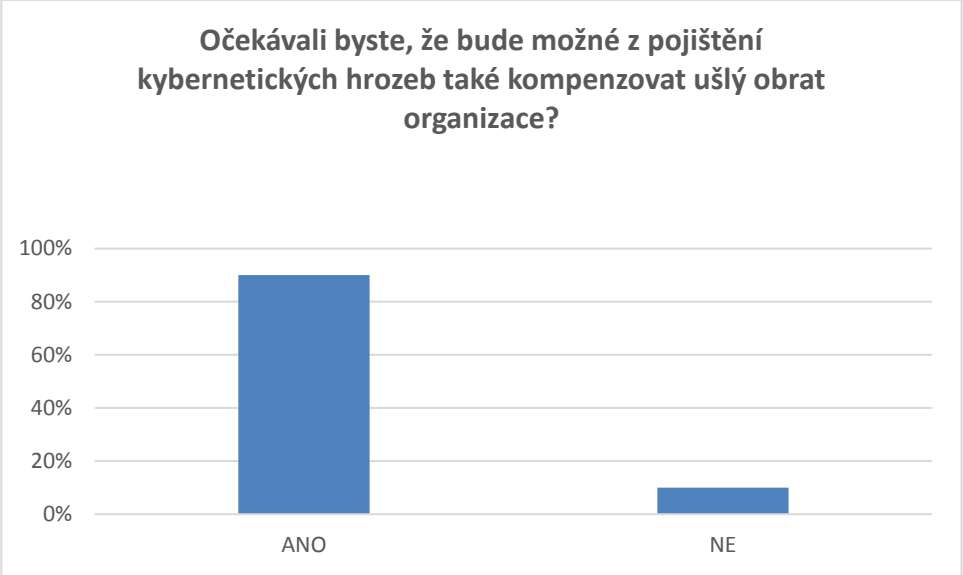


Graf 5.34: Otázka č. 25 a odpovědi jednotlivých respondentů (vlastní zdroj)

Na otázku č. 25 odpovědělo celkem 85 % dotazovaných, že by pojištění proti kybernetickým hrozbám mělo také kompenzovat náklady na oznámení ztráty nebo úniku dat dozorovým orgánům nebo dotčeným subjektům. Tato otázka zde byla zařazena kvůli Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 (GDPR), ve kterém je ukládána povinnost oznámení úniku osobních údajů do 72 hodin příslušenému úřadu a dotčeným subjektům. Zbylých 15 % odpovědělo, že by tyto náklady v rámci tohoto typu pojištění hrazeny být nemusely.

Otázka č. 26

Očekávali byste, že bude možné z pojištění kybernetických hrozeb také kompenzovat ušlý obrat organizace?



Graf 5.35: Otázka č. 26 a odpovědi jednotlivých respondentů (vlastní zdroj)

Podle 85 % z dotazovaných organizací by mělo být pojištění proti kybernetickým hrozbám zaměřeno na kompenzaci ušlého obratu, který může nastat v případě omezení funkce organizace. Celkem 15 % dotazovaných organizací uvedlo, že by ušlý obrat v rámci tohoto typu pojištění být kompenzován neměl.

5.2 Shrnutí

Primárním cílem dotazníkového šetření, které bylo aplikováno v rámci výzkumu k disertační práci, bylo zjistit stav a vnímání organizací, které lze zařadit mezi malé a střední podniky, vůči problematice pojištění kybernetických hrozeb.

Z dostupných informací, které byly během tohoto dotazníkového šetření zjištěny, lze stanovit následující závěry:

- dotazovaní respondenti mají alespoň základní znalosti z oblasti pojištění, které je zaměřeno na kompenzaci nákladů vzniklých realizací některé z vybraných kybernetických hrozeb,
- všechny z oslovených organizací (tedy 100 %) zpracovává citlivé osobní údaje, týkající se třetích stran (tj. zaměstnanců, dodavatelů, odběratelů apod.),
- 90 % z oslovených organizací odpovědělo, že by v případě realizace kybernetické hrozby, nebyly schopny z vlastních zdrojů pokrýt náklady, které by vlivem takové situace vznikly,
- 85 % z oslovených organizací považuje za nejzranitelnější aktiva své organizace data a know-how,

- více jak 80 % z oslovených organizací uvedlo, že by uvítaly, kdyby v rámci pojištění proti kybernetickým hrozbám byla kompenzace vzniklých nákladů u hardwaru, softwaru, dobrém jménu organizace, na rekonstrukci a obnovu dat, pokuty udělených za únik nebo poškození osobních údajů, nákladů na oznámení ztráty nebo úniku dat a kompenzaci ušlého zisku.

Na základě provedeného výzkumu lze konstatovat, že pojištění proti kybernetickým hrozbám, je nástrojem, který může poskytnout pojištěné organizaci dostatečné možnosti pro řešení nežádoucích dopadů kybernetických incidentů. Tato řešení mohou v případě realizace kybernetické hrozby pomoci k překonání nežádoucí situace a nastolení postupné rovnováhy, která je výchozím stavem pro zajištění všech základních funkcí organizace. Pro návrh algoritmu, který je určen pro stanovení pojistné hodnoty, plynoucí z dopadu vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví, jsou z dotazníkového šetření aplikovány především poznatky, týkající se možných kybernetických hrozeb a oblastí, které mohou být nejvíce zasaženy dopadem těchto hrozeb.

V rámci konstrukce dotazníku, bylo potvrzeno, že uvažované scénáře kybernetických hrozeb jsou vnímány dotazovanými organizacemi jako velmi významné pro jejich fungování a měly by být tak součástí krytí pojištění proti dopadu kybernetických hrozeb. Mezi nejvýznamnější zjištění provedeného výzkumu lze zařadit stanovení oblastí, ve kterých mohou organizaci vzniknout největší náklady, spojené s dopadem kybernetické hrozby. Tyto oblasti jsou dále nazývány jako ohrožené prvky a jejich finanční vyjádření, je jedním ze základních ukazatelů možných dopadů na informační prostředí organizace.

Dalším důležitým krokem, který by měl být nezbytnou součástí navrhovaného algoritmu, je pak vyjádření interakce mezi uvažovanými kybernetickými hrozbami a sledovanými ohroženými prvky. Tato interakce by měla vést k identifikaci nejzávažnější kybernetické hrozby pro konkrétní organizaci a ke stanovení pojistné hodnoty, která vyjadřuje možné finanční škody v informačním prostředí organizace.

6. NÁVRH ALGORITMU PRO STANOVENÍ POJISTNÉ HODNOTY Z HLEDISKA POJIŠTĚNÍ PROTI KYBERNETICKÝM HROZBÁM

Hlavním účelem **algoritmu pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví** (dále jen algoritmus) je poskytnout rámec pro vyjádření potenciálních finančních škod, které mohou v organizaci nastat vlivem realizace kybernetické hrozby. Nástroj nebo postup, který by umožňoval dosáhnout tohoto cíle, v současné době absentuje a přitom je zřejmé, že v nejbližších letech bude potřeba. Algoritmus sjednocuje různé pohledy a oblasti, které jsou pro vyjádření pojistné hodnoty v oblasti pojištění proti kybernetickým hrozbám nezbytné. Jedná se především o hlediska ekonomická a informaticko-bezpečnostní.

Navržený algoritmus je rozdělen do následujících fází:

a) Fáze 1: Definování ohrožených prvků organizace a jejich ocenění
b) Fáze 2: Hodnocení významnosti jednotlivých ohrožených prvků organizace
c) Fáze 3: Hodnocení závažnosti vybraných kybernetických hrozeb
d) Fáze 4: Modelování interakce mezi vybranými kybernetickými hrozbami a definovanými ohroženými prvky
e) Fáze 5: Identifikace nejzávažnější kybernetické hrozby
f) Fáze 6: Určení pojistné hodnoty

Na základě Fáze 1 jsou určeny tzv. ohrožené prvky organizace, které představují oblasti, které mohou být zasaženy dopadem kybernetických hrozeb. Finanční škody, které mohou v těchto oblastech vzniknout, mohou významným způsobem zatížit fungování organizace.

Fáze 2 je zaměřena na stanovení významnosti jednotlivých ohrožených prvků pro organizaci. Toto ohodnocení je prováděno na základě semikvantitativní stupnice.

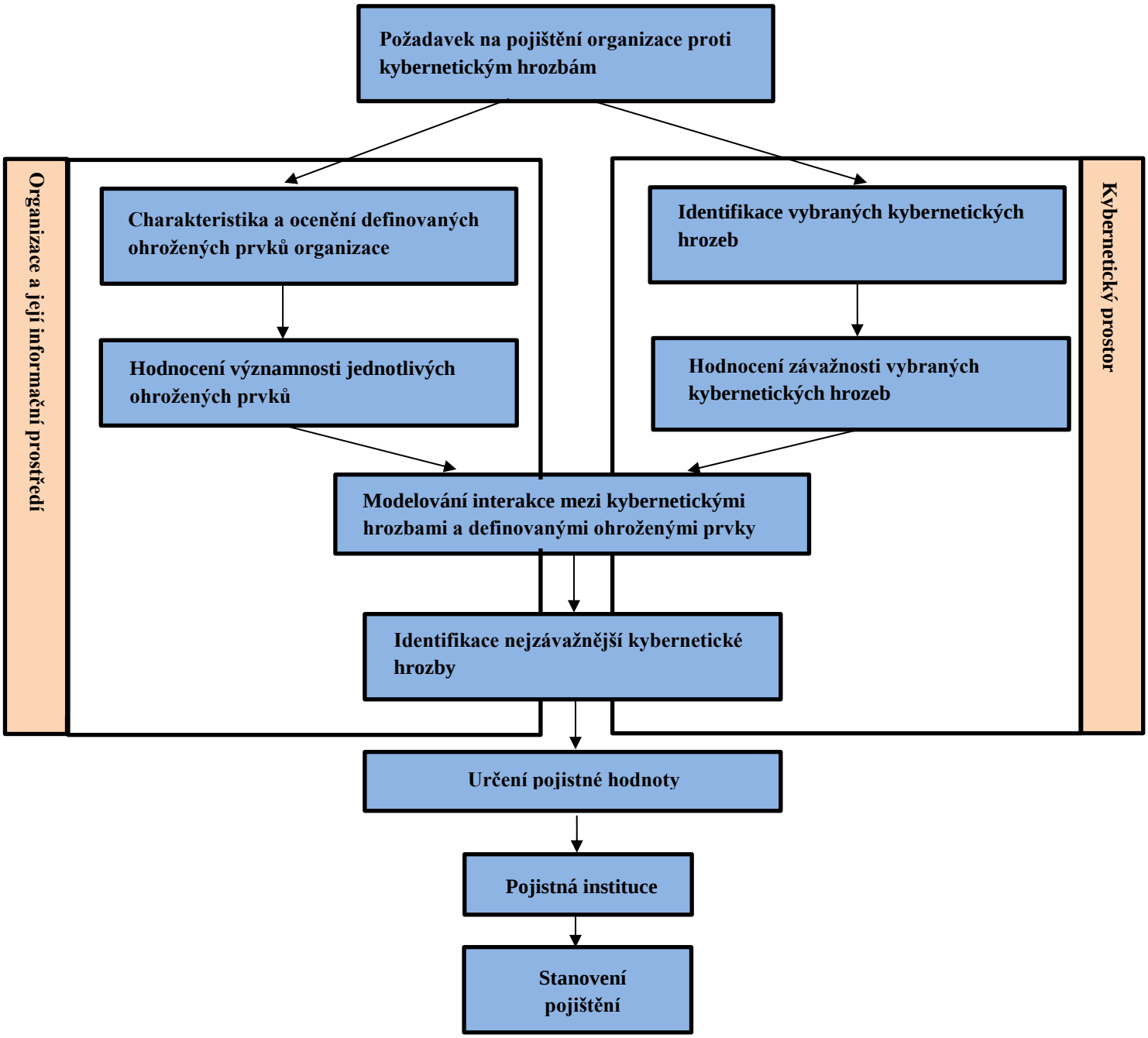
Fáze 3 je určena ke stanovení významnosti uvažovaných kybernetických hrozeb, které mohou být uvažovány v rámci pojištění organizace. Stanovení významnosti těchto kybernetických hrozeb je prováděno na základě semikvantitativní stupnice.

Fáze 4 představuje modelování interakce mezi vybranými kybernetickými hrozbami a ohroženými prvky. Pro tyto účely je zde použito vybraných metod analýzy rizik, které slouží pro vyjádření dopadu jednotlivých kybernetických hrozeb na dané ohrožené prvky.

Fáze 5 je zaměřena na určení nejzávažnější kybernetické hrozby pro organizaci na základě pořadí zjištěných rizik. Tato skutečnost je zjištěna jednak na základě výsledků provedené analýzy rizik, ale také prostřednictvím Saatyho metody.

Fáze 6 pak představuje stanovení pojistné hodnoty na základě navržené semikvantitativní stupnice, pomocí které lze odvodit možné finanční dopady na organizaci a její informační prostředí.

Schéma navrhovaného algoritmu je zobrazeno na obrázku 6.4.



Obr. 6.4: Schéma navrhovaného algoritmu (vlastní zdroj)

6.1 Definování ohrožených prvků organizace a způsoby jejich ocenění

V této části disertační práce jsou charakterizovány ohrožené prvky organizace, které jsou klíčovými oblastmi informačního prostředí organizace z pohledu kybernetického pojištění. Tyto ohrožené prvky byly definovány na základě výsledků dotazníkového šetření a konzultací, které byly absolvovány pojistných institucích. Každý prvek organizace je doplněn vývojovým diagramem, který slouží pro znázornění průběhu a dopadu kybernetických hrozeb na vybrané ohrožené prvky.

Mezi tyto ohrožené prvky lze zařadit:

- hardware,
- software,
- ušlý obrat,
- pokuty,
- dobré jméno organizace,
- náklady na rekonstrukci a obnovu dat,
- náklady na oznámení ztráty nebo úniku dat.

6.1.1 Hardware

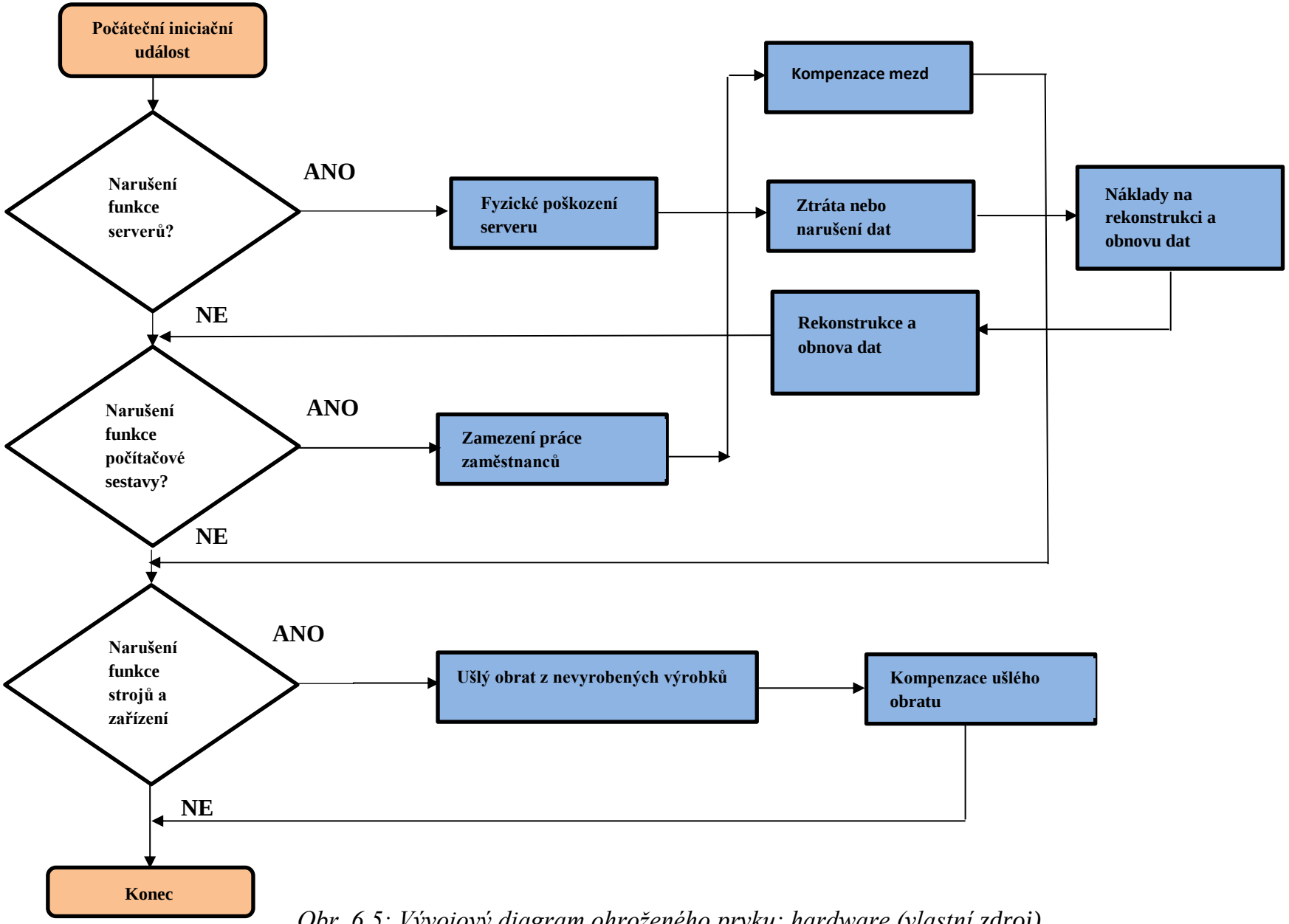
Do oblasti hardware lze zařadit v tomto případě nejen počítače a jejich příslušenství, ale také jakékoliv technické vybavení, které souvisí s informačním systémem organizace.

Tato kategorie je oceněna na základě následujících možných přístupů:

Ocenění pořizovací cenou – u majetku úplatně pořízeného (součástí ceny jsou taktéž náklady s pořízením související – např. přeprava a instalace, licence a patenty, průzkumné, geologické a jiné práce; součástí pořizovací ceny mohou být i úroky z úvěru, pokud se tak účetní jednotka rozhodne).

Ocenění reprodukční pořizovací cenou – cena, za kterou by byl majetek pořízen v době, kdy se o něm účtuje – dlouhodobý hmotný majetek (DHM) získaný darováním, nově zjištěný a dosud nezachycený v účetnictví, vklad DHM za předpokladu, že se tento vklad dle společenské smlouvy neoceňuje jinak; DHM nabytý bezúplatně na základě finančního leasingu; reprodukční pořizovací cena se použije v případech, kdy nelze zjistit vlastní náklady na vytvoření majetku.

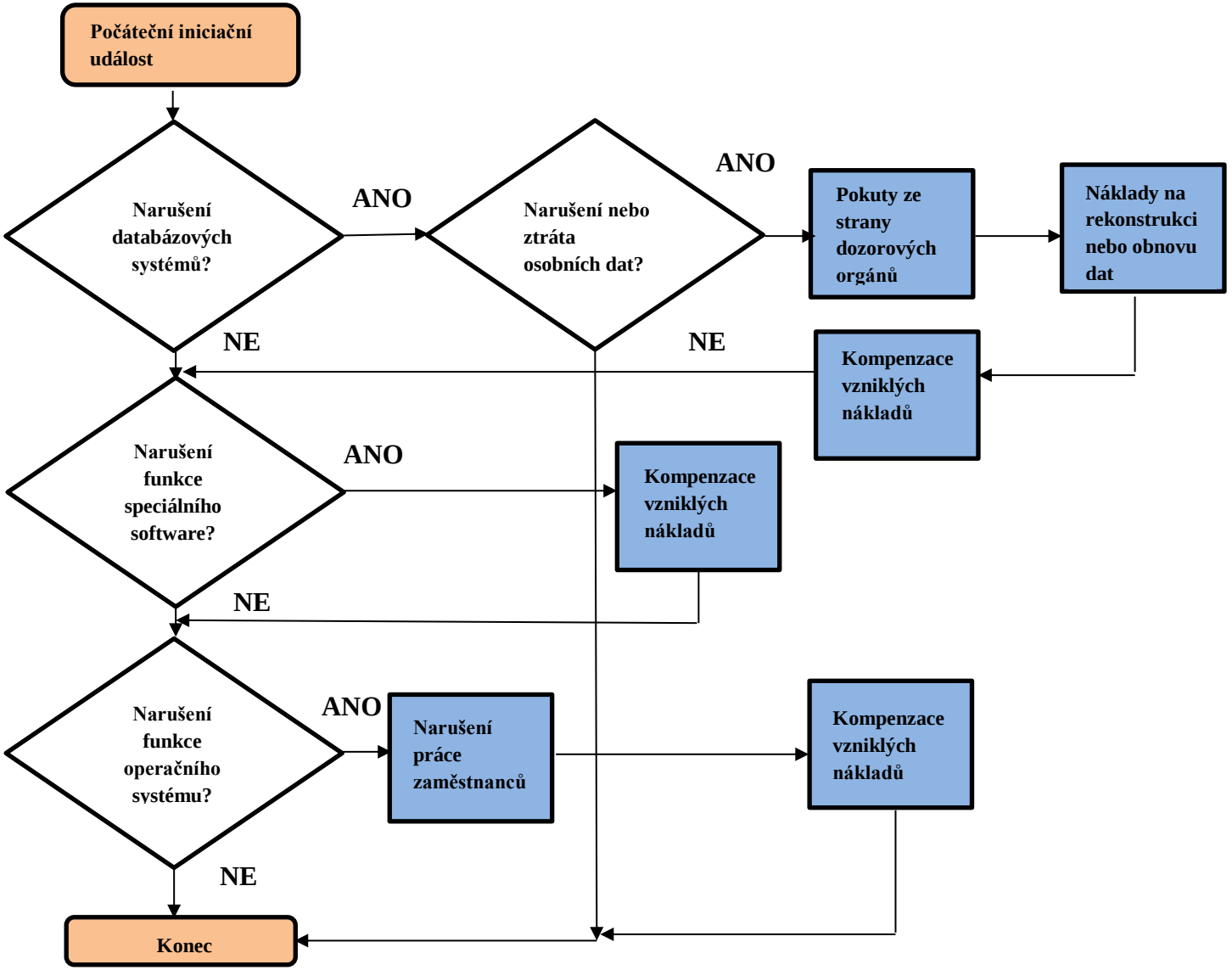
Vlastními náklady – DHM vytvořený vlastní činností. Jedná se o přímé náklady vynaložené na výrobu nebo jinou činnost a nepřímé náklady, které se k výrobě nebo jiné činnosti vztahují; (nelze-li vlastní náklady zjistit, použije se reprodukční pořizovací cena).



Obr. 6.5: Vývojový diagram ohroženého prvku: hardware (vlastní zdroj)

6.1.2 Software

Pro účely této disertační práce bude použita výše nákladů, která by musela být vynaložena na reinstalaci softwaru v případě jeho narušení. Vzhledem k tomu, že organizace vlastní licenci na provoz softwarových nástrojů, není nutné tento software znovu pořizovat za novou cenu. Může také nastat situace, kdy je software pořízen a vázán na hardware, se kterým byl zakoupen, nicméně tato možnost není v případě malých a středních podniků příliš pravděpodobná.



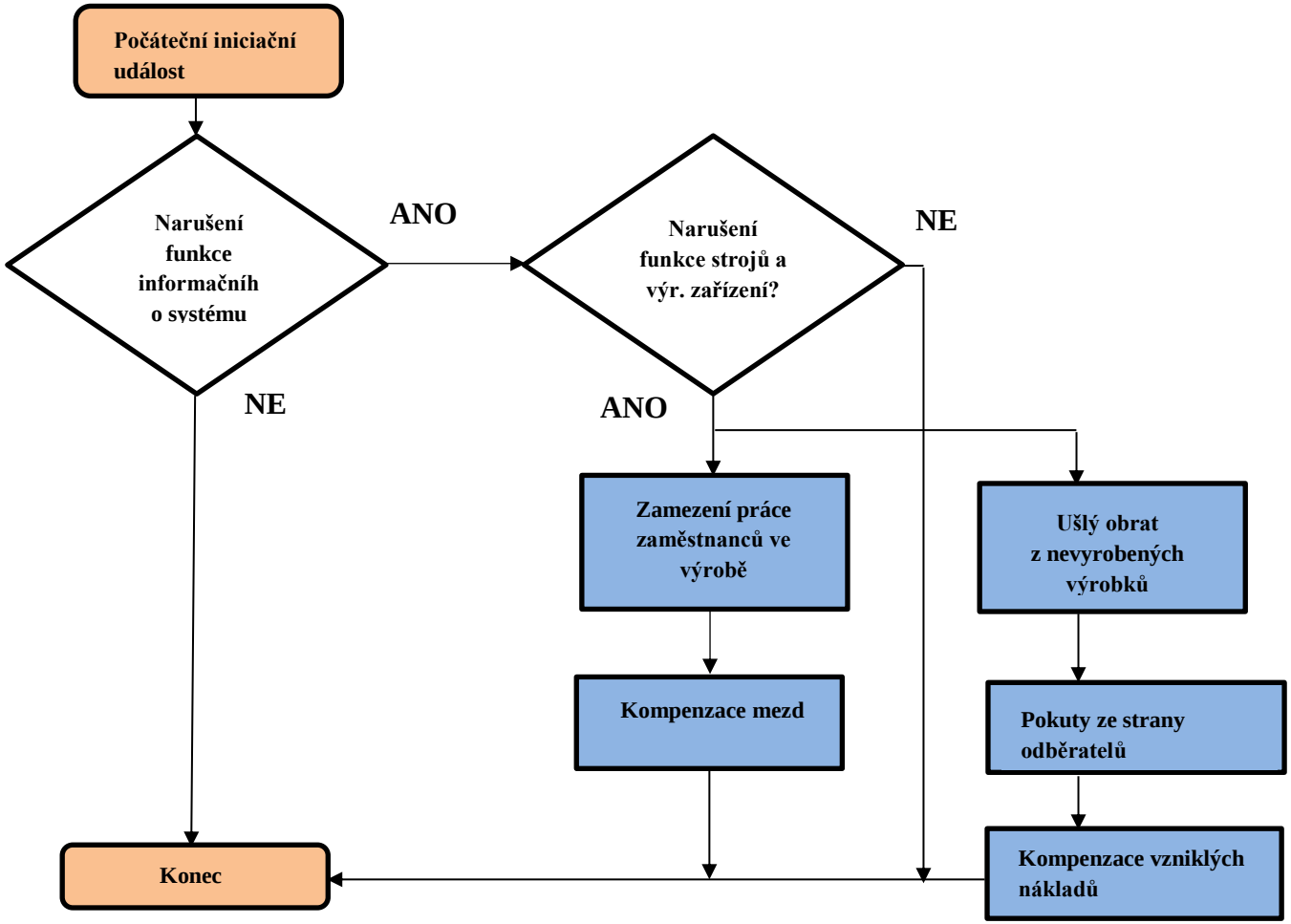
Obr. 6.6: Vývojový diagram ohroženého prvku: software (vlastní zdroj)

6.1.3 Ušlý obrat

Pokud realizace kybernetické hrozby naruší výrobní proces organizace (pokud v organizaci nějaký probíhá) nebo základní funkce a činnosti podnikání, je nutné v procesu stanovení pojistné hodnoty zohlednit také možný ušlý obrat. Za ušlý obrat se považuje množství finančních prostředků, které jsou přijaty ekonomickým subjektem za určité časové období. Pro účely disertačním práce je zde navržen následující vzorec:

$$\boldsymbol{U_z = \frac{O_f}{M_r} * M_t} \tag{6.1}$$

U_z = ušlý obrat
O_f = obrat organizace za rok
M_r = počet dnů za rok
M_t = počet dnů, které jsou vyhrazeny na kompenzaci ušlého obratu



Obr. 6.7: Vývojový diagram ohroženého prvku: ušlý obrat (vlastní zdroj)

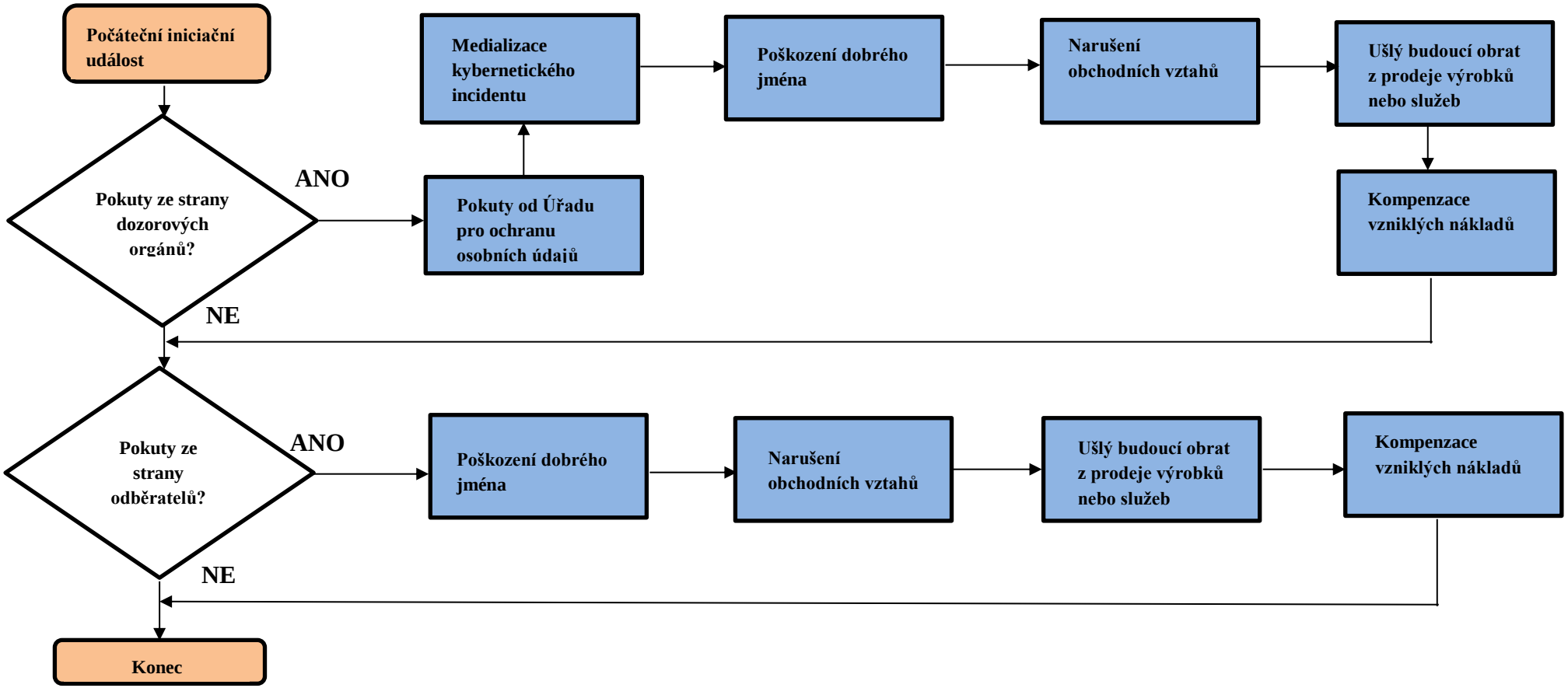
6.1.4 Pokuty

Pro ocenění této kategorie nelze použít předem stanovený vzorec. Výše pokut je individuální záležitostí a záleží na posouzení subjektů, které mohou pokutu dle platné legislativy uložit. Při stanovování výše pokuty je brána v úvahu povaha, závažnost a délka porušení ochrany dat. Dále pak jestli se jedná o ojedinělou událost, nebo o systematické porušování, jestli došlo k porušení úmyslně, nebo z nedbalosti apod. Všechny skutečnosti, které vstupují do procesu stanovení výše pokuty, jsou definovány v nařízení GDPR, které je pro území České republiky upraveno zákonem č. 110/2019 Sb., o zpracování osobních údajů.

Pro přesnější vyjádření udělování pokut a stanovení jejich výše je navržena následující hodnotící škála, která je uvedena v tabulce 6.1. Rozmezí pokut je definováno na základě stupně narušení důvěrnosti, integrity a dostupnosti osobních dat. Je nutné zdůraznit, že pokuty mohou být uděleny již na základě nedodržení základních bezpečnostních předpisů. Nemusí tedy dojít k úniku nebo narušení osobních údajů, které jsou v organizaci uchovávány. Pro exaktnější vyjádření výše pokut je rozdělen typ uvažované situace podle velikosti organizace na malou (méně než 50 osob), střední (méně než 250 osob) a velkou (více než 250 osob).

Tabulka 6.1: Stupně narušení a rozmezí udělovaných pokut (vlastní zdroj)

Stupeň narušení	**Popis situace**	**Velikost organizace**	**Rozmezí pokut**
1	Jsou narušeny základní bezpečnostní prvky informačního systému, jako je např. antivirus, síťové prvky apod. K narušení ochrany, důvěrnosti, integrity a dostupnosti údajů nedochází.	Malá	0 – 5 00 000 Kč
		Střední	0 – 1 000 000 Kč
		Velká	0 –2 000 000 Kč
2	Dochází k narušení a prolomení bezpečnostní bariéry informačního systému organizace. Jako důsledek této situace je narušení integrity, důvěrnosti a dostupnosti menšího počtu osobních údajů (do 25 % datových položek).	Malá	5 00 000 – 1 000 000 Kč
		Střední	1 000 000 – 2 000 000 Kč
		Velká	2 000 000 – 2 500 000 Kč
3	Dochází k narušení struktury většího počtu osobních dat (do 50 % datových položek). Důsledkem nežádoucí události může být únik těchto osobních dat nebo jejich narušení.	Malá	1 000 000 – 1 500 000 Kč
		Střední	2 000 000 – 3 500 000 Kč
		Velká	2 500 000 – 5 000 000 Kč
4	Osobní data jsou narušena ve větším množství (více jak 75 % datových položek). Dochází k jejich masivnímu úniku mimo organizaci a její informační systém	Malá	1 500 000 – 2 000 000 Kč
		Střední	3 500 000 – 5 000 000 Kč
		Velká	5 000 000 – 10 000 000 Kč



Obr. 6.8: Vývojový diagram ohroženého prvku: pokuty (vlastní zdroj)

6.1.5 Dobré jméno organizace

Pro potřeby finančního vyjádření dobrého jména organizace je nutné charakterizovat, co je pod tímto pojmem uvažováno. V rámci pojištění proti kybernetickým hrozbám je „poškozením dobrého jména“ myšlena budoucí finanční újma, která vznikne realizací kybernetické hrozby v určitých oblastech organizace. Těmito oblastmi jsou dodavatelé, odběratelé, zákazníci a sponzoři. Jedná se tedy o finanční prostředky, o které vlivem nežádoucí události může organizace přijít v určitém časovém rozmezí.

Dobré jméno organizace (v oblasti ekonomie nazýváno také jako goodwill), lze finančně vyjádřit pomocí matematického aparátu. Pro jeho aplikaci je ale nutné definovat, co je zde nazýváno dobrým jménem organizace a co lze do této kategorie zahrnout. V tomto případě se jedná především o reklamu a image organizace.

V oblasti reklamy a image je organizace hodnocena jako celek, nikoliv pouze na základě určitých oblastí. Pro vyjádření finanční částky, která reflektuje oblast reklamy a image, je nutné změřit výnosnost investic do této kategorie. Dále je třeba zohlednit synergii, kterou podnik vytváří za účelem oslovení trhu.

V každé organizaci investují zaměstnanci a vedoucí pracovníci svůj čas, peníze a energii do vytváření image organizace. Tento proces je zaměřen především na oslovení nových zákazníků, dodavatelů, odběratelů a udržení stávajících kontaktů. Z tohoto důvodu jsou výpočty v této kategorii zaměřeny na tento bod. Pro tyto účely je nutné změřit průměrný výdělek z každého uzavřeného obchodu, dále průměrné přírůstky a úbytky klientů v posledních pěti letech. Od toho odečteme průměrné náklady vložené do reklam podniku a prostřednictvím sestaveného vzorce můžeme ocenit tuto kategorii dobrého jména organizace.

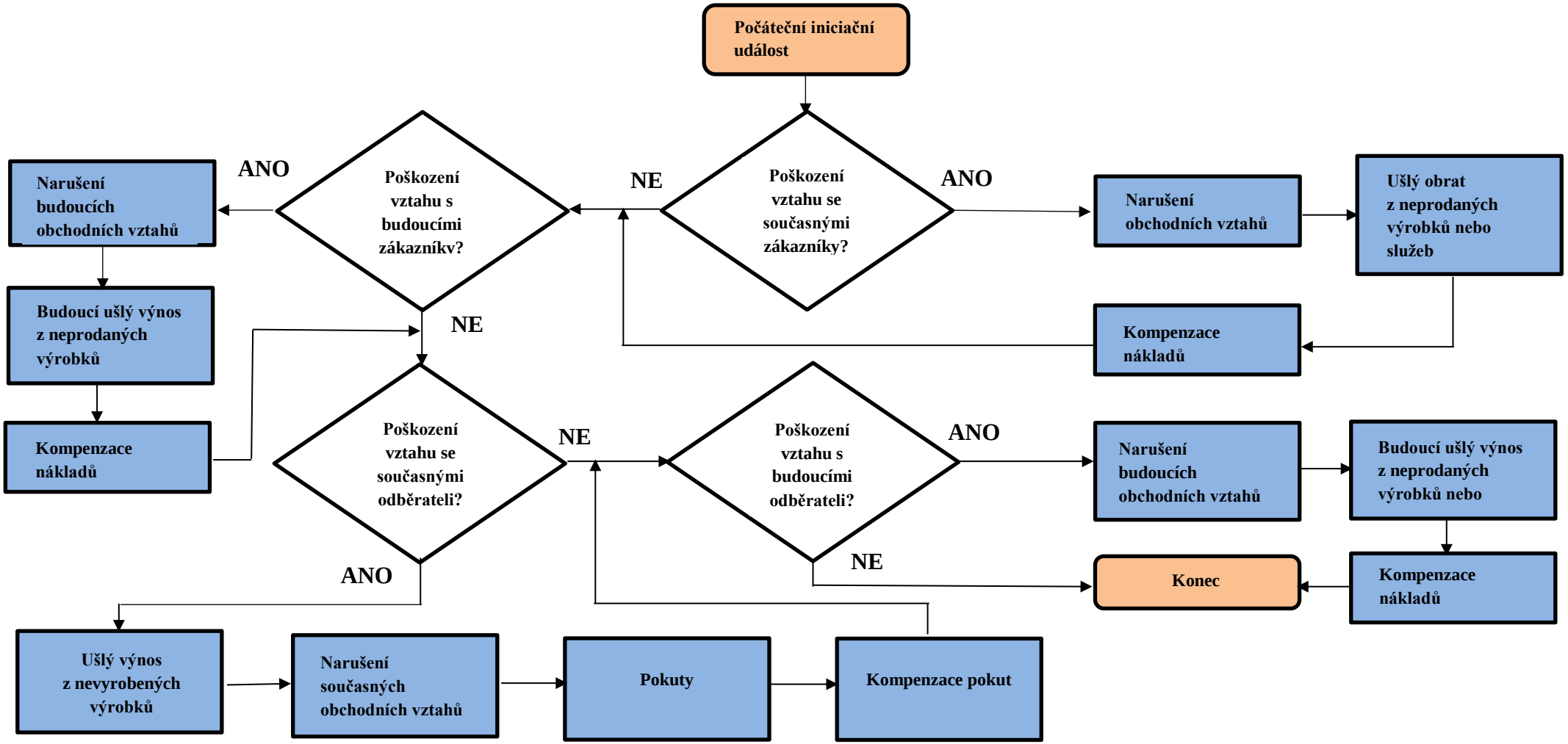
$$\boldsymbol{RI} = \left(\boldsymbol{PPK} * \frac{\sum_{i=1}^{n} \boldsymbol{N_{ki}}}{\boldsymbol{n}} - \boldsymbol{PPK} * \frac{\sum_{i=1}^{n} \boldsymbol{Z_{ki}}}{\boldsymbol{n}}\right) - \frac{\sum_{i=1}^{n} \boldsymbol{N_{ir}}}{\boldsymbol{n}} \qquad (6.2)$$

RI = reklama a image
PPK = průměrný příjem na klienta
N_{ki} = noví klienti za rok
Z_{ki} = ztracení klienti za rok
N_{ir} = náklady na reklamu za rok
n = hodnota sledovaného období

Pro úplnost vyjádření tohoto ukazatele je nutné přidat ještě faktor času, tedy diskontování pro další rok. Vzorec pro diskontování je následující:

$$\boldsymbol{PPK} = \frac{\sum_{i=1}^{n} \boldsymbol{X_i}}{\sum_{i=1}^{n} \boldsymbol{N_{ki}}} \tag{6.3}$$

PPK = průměrný příjem na klienta
X_i = roční příjem z obchodů
N_{ki} = počet klientů za rok



Obr. 6.9: Vývojový diagram ohroženého prvku: dobré jméno organizace (vlastní zdroj)

6.1.6 Náklady na rekonstrukci a obnovu dat

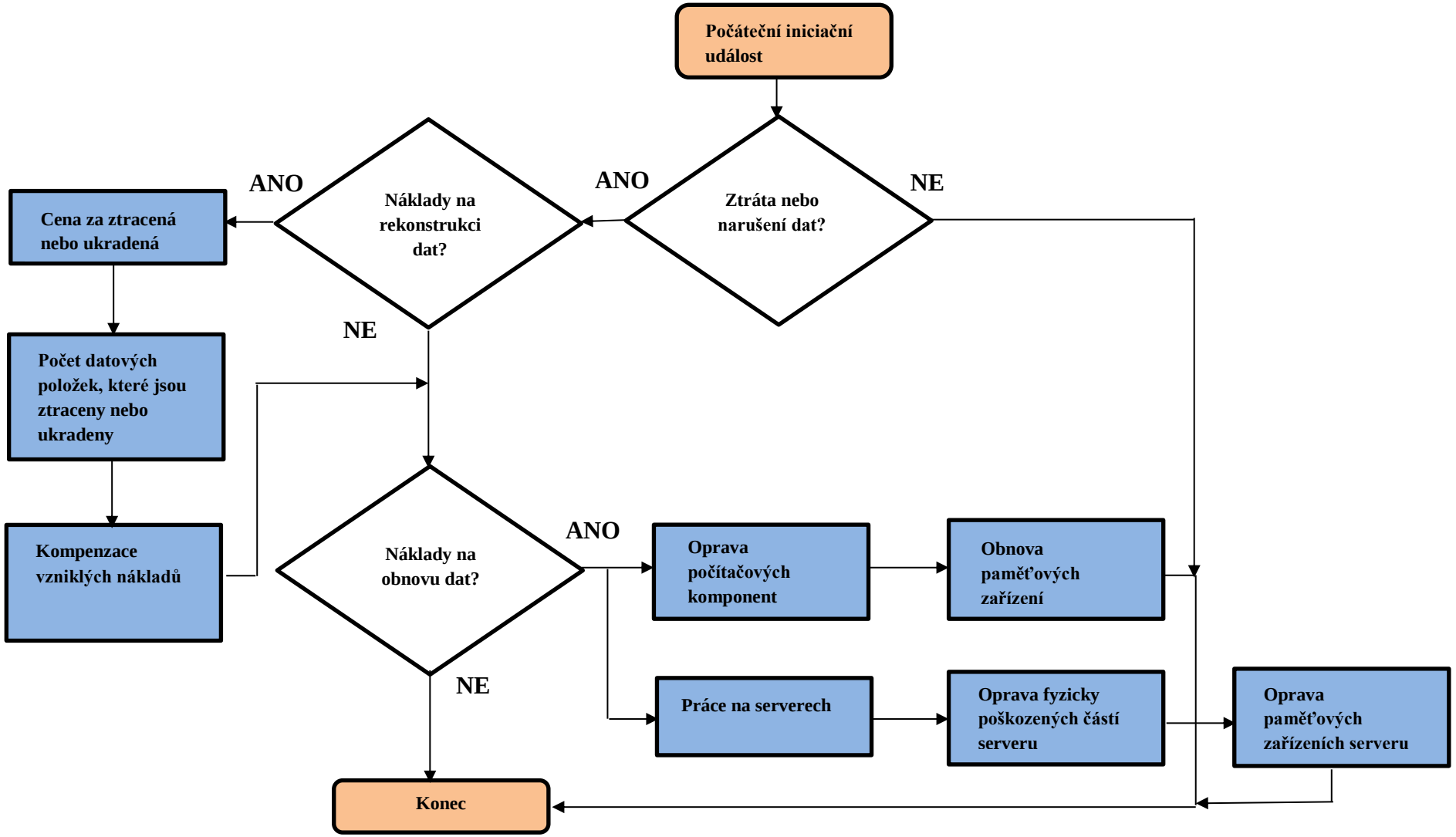
Náklady na rekonstrukci a obnovu dat lze definovat jako účelně vynaložené náklady na obnovu a znovuzískání dat z hardwarových a softwarových prostředků. Ztráta dat může nastat tedy v případě, že je narušen zdroj nebo nosič, na kterém jsou data uložena nebo zálohována.

Z dostupných statistických údajů lze také stanovit průměrnou cenu za ztracená nebo ukradená data na jednu osobu. Tato statistická hodnota, která je uvedena v Ponemon study 2017, činí 141 USD na osobu (v české měně 3 223 Kč). Tato hodnota může být využita pro stanovení nákladů na rekonstrukci dat. Lze použít následující vzorec:

$$\boldsymbol{N_R = C_D * \sum_{i=1}^{n} P_D} \tag{6.4}$$

N_r = náklady na rekonstrukci dat
C_D = cena za ztracená data na jednu osobu
P_D = počet datových položek, které mohou být ztraceny[2]

[2] *Jedná se o přibližný počet datových položek, které mohou být ztraceny nebo poškozeny. Tyto datové položky se týkají osob třetí strany (zákazníci, dodavatelé, odběratelé apod.).*



Obr. 6.10: Vývojový diagram ohroženého prvku: náklady na rekonstrukci a obnovu dat (vlastní zdroj)

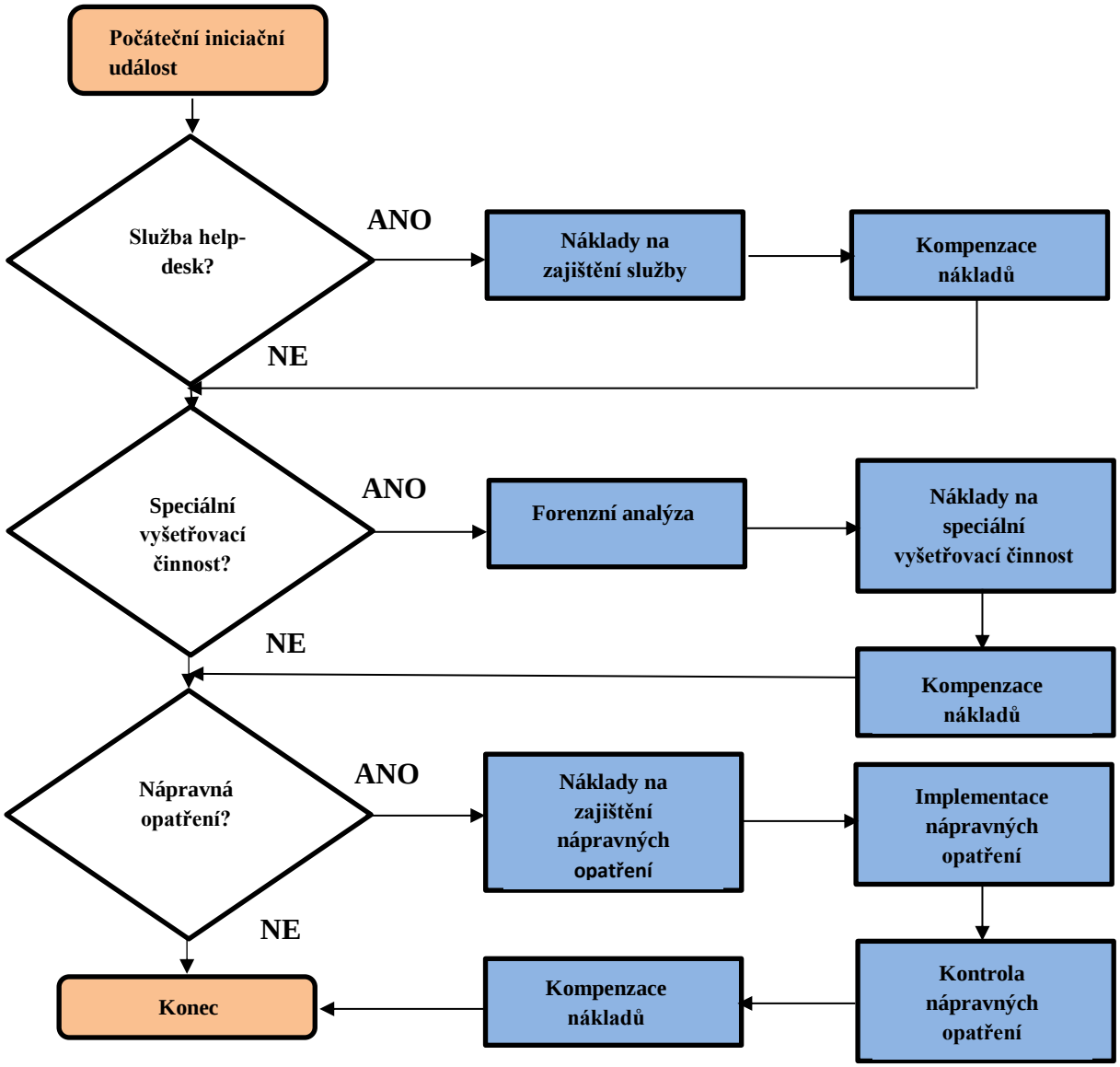
6.1.7 Náklady na oznámení ztráty nebo úniku dat

V rámci pojistného krytí by měly být brány v úvahu také náklady na oznámení ztráty nebo úniku dat dozorovým orgánům. Do této kategorie je zahrnuto také informování dalších poškozených stran, které jsou kybernetickým incidentem dotčeny, komunikace s těmito dotčenými subjekty apod. Tato problematika souvisí částečně se zachováním dobrého jména organizace. Pro účely vyjádření tohoto ohroženého prvku je možné použít následující vzorec:

$$\boldsymbol{N_U = M_Z * H_Z * T_Z} \tag{6.5}$$

N_U = náklady na oznámení ztráty nebo úniku dat
M_Z = počet zaměstnanců, kteří zajišťují kontaktování dotčených subjektů
H_Z = hodinová mzda zaměstnanců, kteří budou kontakt s dotčenými subjekty realizovat
T_Z = počet hodin vynaložených na kontaktování dotčených subjektů[3]

[3] *Jedná se o přibližný počet pracovních hodin, které mají zaměstnanci vyčleněny na kontaktování subjektů, které mohou být ztrátou nebo únikem dat dotčeny.*



Obr. 6.11: Vývojový diagram ohroženého prvku: náklady na oznámení ztráty nebo úniku dat dozorovým orgánům (vlastní zdroj)

6.2 Aplikace a ověření algoritmu na referenčním objektu

Následující podkapitoly jsou zaměřeny na praktické výsledky použití navrhovaného algoritmu na třech vybraných organizacích. Ověření algoritmu na referenčních objektech poskytuje tvrzení o jeho aplikovatelnosti, funkčnosti a možných přínosech pro oblasti pojišťovnictví a kybernetické bezpečnosti. Algoritmus byl ověřen na organizacích, které se liší svou podstatou fungování i informačním prostředím.

Vybrané organizace lze zařadit do kategorie malých a středních podniků, které provozují svou činnost na území České republiky. V každé organizaci byly hodnoceny vždy definované ohrožené prvky organizace a vybrané kybernetické hrozby, které mohou být v rámci pojištění informačních systémů proti kybernetickým hrozbám uvažovány. Výsledkem tohoto procesu je stanovení pojistné hodnoty pro každou organizaci.

V tomto praktickém ověření **algoritmu pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví** byly použity matematické a analytické metody s ohledem na jejich časovou a ekonomickou náročnost. Pro lepší interpretaci výsledků je u každé organizace aplikace algoritmu rozdělena na ekonomickou část a informaticko-bezpečnostní část.

6.2.1 Případová studie č. 1

Organizace č. 1 je soukromou vysokou školou, která byla založena v roce 2005 a svou právní formou je obecně prospěšnou společností. Svou odborností ve vzdělávání a vědeckém výzkumu je tato organizace zaměřena na oblasti ekonomie, managementu a informačních a komunikačních technologií. Pracuje zde celkem 52 stálých zaměstnanců. Organizace spolupracuje se zahraničními partnery v oblasti vědy a výzkumu od evropských států až po Čínu. V současnosti má tato organizace 28 klíčových partnerství, která otevírají další možnosti spolupráce po celém světě.

Studenti i akademičtí pracovníci vyjíždějí za zkušenostmi do zahraničí, v rámci výuky či na mezinárodních konferencích na půdě školy diskutují se zahraničními partnery a podílejí se na řešení mezinárodních mezioborových projektů. V organizaci studuje celkem 722 studentů, kteří studují dva bakalářské studijní programy se zaměřením na ekonomiku a management. Je možné zde studovat nově také navazující magisterský studijní program.

V organizaci jsou zavedeny dva informační systémy. Jedná se o systém STAG, se kterým pracují zaměstnanci i studenti, a o informační systém SAP, který slouží pro správu ekonomické agendy. Se systémem SAP pracují pouze zaměstnanci vysoké školy.

1) Ekonomická část

V této části je stanovena cena vybraných ohrožených prvků organizace, které mohou být ohroženy dopadem kybernetické hrozby.

a) Hardware

Servery: 230 000 Kč (celkem dva servery, které jsou umístěny v hlavním sídle firmy za přibližně 115 000 Kč / jeden kus)

Počítačové sestavy: cca 4 825 000 Kč (počítačová skříň, monitor, klávesnice, myš, tiskárna)

V rámci stanovení ceny hardware byla použita pořizovací cena majetku.

b) Software

Software by oceněn na základě možných nákladů na jeho přeinstalaci. Celková cena obnovy software činí cca **35 000 Kč.**

c) Ušlý obrat

V případě této organizace je ušlý obrat stanoven na základě školného, které je přijímáno od studentů. Za jeden školní rok platí každý student školné ve výši 40 000 Kč. Lze uvažovat situaci, kdy v případě realizace kybernetické hrozby v organizaci může být narušena důvěra studentů a veřejnosti k této instituci. Tato skutečnost se může projevit jako absence přihlášených uchazečů ke studiu a tím také pokles příjmu finančních prostředků v podobě školného.

V uplynulých 13 letech byly v nabídce dva studijní programy. Do těchto studijních programů bylo průměrně každý rok přihlášeno 78 studentů. Z těchto údajů lze při uvažování nejzávažnějšího scénáře tedy stanovit, že narušení informačního systému organizace vlivem kybernetické hrozby může odradit ke studiu průměrně 78 studentů.

Pro výpočet ušlého obratu je použit následující vzorec:

$$\boldsymbol{U_z = \frac{O_f}{M_r} * M_t} \qquad (6.6)$$

U_z = ušlý obrat
O_f = obrat organizace za rok
M_r = počet dnů za rok
M_t = počet dnů, které jsou vyhrazeny na kompenzaci ušlého obratu

Po dosazení do vzorce, bude výpočet následující:

$$\boldsymbol{U_Z = \frac{7\,360\,000}{365} * 3 = 60\,493\ Kč} \quad (6.7)$$

Výše ušlého obratu, který může být kompenzován v pojištění proti kybernetickým hrozbám, je **60 493 Kč.**

d) Pokuty

Organizace č. 1 patří svým počtem mezi malé organizace (přibližně 52 zaměstnanců). Vzhledem k tomu, že je organizace zaměřena na oblast vzdělávání a výzkumu, existuje zde středně silné zabezpečení informačních systémů a jejich komponent. Ze zjištěných skutečností lze predikovat, že zde může nastat dle výše uvedené tabulky maximální stupeň č. 2 v rámci narušení nebo zcizení osobních dat.

Výše možných pokut je tedy stanovena na **1 000 000 Kč**.

e) Dobré jméno organizace

V případě vyčíslení dobrého jména je uvažována kategorie reklama a image.

Reklama a image

$$\boldsymbol{RI = \left(PPK * \frac{\sum_{i=1}^{n} N_{ki}}{n} - PPK * \frac{\sum_{i=1}^{n} Z_{ki}}{n}\right) - \frac{\sum_{i=1}^{n} N_{ir}}{n}} \quad (6.8)$$

RI = reklama a image
PPK = průměrný příjem na klienta
N_{ki} = noví klienti za rok
Z_{ki} = ztracení klienti za rok
N_{ir} = náklady na reklamu za rok
n = hodnota sledovaného období

V následující tabulce jsou uvedeny údaje, které jsou potřebné pro finanční vyjádření dobrého jména organizace.

Tabulka 6.2 Finanční údaje k vyjádření nákladů na reklamu a image (vlastní zdroj)

Rok	Příjem z činnosti (přijato od studentů)	Počet nových klientů/studentů	Počet ztracených klientů/studentů	Náklady na reklamu v korunách
2014	7 360 000	78	24	45 962
2015	7 200 000	75	15	43 251
2016	7 240 000	78	19	41 658
2017	7 360 000	76	12	46 985
2018	7 360 000	78	18	46 935

$$\mathbf{PPK} = \frac{\mathbf{36\,520\,000}}{\mathbf{385}} = \mathbf{94\,857}\ \boldsymbol{K}\text{č / studenta} \qquad (6.9)$$

$$\mathbf{RI} = \left(\mathbf{94\,857} * \frac{\mathbf{385}}{\mathbf{5}} - \mathbf{94\,857} * \frac{\mathbf{88}}{\mathbf{5}}\right) - \frac{\mathbf{224\,791}}{\mathbf{5}} = \mathbf{5\,589\,548}\ \boldsymbol{K}\text{č} \qquad (6.10)$$

Jako další krok je použita opět diskontní sazba:

$$\mathbf{DCF_1} = \frac{\mathbf{5\,589\,548}}{(\mathbf{1+0{,}05})^{\mathbf{1}}} = \mathbf{5\,323\,379}\ \mathbf{K}\text{č} \qquad (6.11)$$

f) Náklady na rekonstrukci a obnovu dat

Z dostupných statistických údajů lze také stanovit průměrnou cenu za ztracená nebo ukradená data na jednu osobu. Tato statistická hodnota, která je uvedena v Ponemon study 2017, činí 141 USD na osobu (v české měně 3 223 Kč). Tato hodnota může být využita pro stanovení nákladů na rekonstrukci dat. Lze použít následující vzorec:

$$\boldsymbol{N_R = C_D * \sum_{i=1}^{n} P_D} \tag{6.12}$$

N_r = náklady na rekonstrukci dat
C_D = cena za ztracená data na jednu osobu
P_D = počet datových položek, které mohou být ztraceny

$$\mathbf{N_R = 3\ 223 * 232 = 747\ 736\ Kč} \tag{6.13}$$

g) Náklady na oznámení ztráty nebo úniku dat

$$\boldsymbol{N_U = M_Z * H_Z * T_Z} \tag{6.14}$$

N_U = náklady na oznámení ztráty nebo úniku dat
M_Z = počet zaměstnanců, kteří zajišťují kontaktování dotčených subjektů
H_Z = hodinová mzda zaměstnanců, kteří budou kontakt s dotčenými subjekty realizovat
T_Z = počet hodin vynaložených na kontaktování dotčených subjektů

$$\mathbf{N_U = 4 * 134 * 24 = 12\ 864\ Kč} \tag{6.15}$$

Finální vyjádření ohrožených prvků organizace ve vztahu k informačnímu prostředí organizace

Hardware: 5 055 000 Kč
Software: 35 000 Kč
Ušlý obrat: 60 493 Kč
Pokuty: 1 000 000 Kč
Dobré jméno organizace: 5 323 379 Kč
Náklady na rekonstrukci a obnovu dat: 747 736 Kč
Náklady na oznámení ztráty nebo úniku dat: 12 864 Kč

Ohrožené prvky organizace jsou oceněny celkovou částkou: 12 234 472 Kč.

2) Informaticko-bezpečnostní část

Pro modelování dopadu jednotlivých kybernetických hrozeb, je použito vybraných metod analýzy rizik. Tato část se skládá z ohodnocení jednotlivých ohrožených prvků organizace podle jejich důležitosti. Tyto prvky jsou zde ohodnoceny konkrétní hodnotou podle jejich stupně významu pro organizaci. Hodnotící škála byla zvolena v rozmezí hodnot 1 až 5, přičemž číslo 5 označuje nejdůležitější ohrožený prvek a číslo jedna označuje nejméně důležitý ohrožený prvek. Dále jsou identifikovány scénáře kybernetických hrozeb a míra zranitelnosti vůči těmto hrozbám. Na závěr jsou výsledky celého procesu vyjádřeny v matici rizik.

Seznam ohrožených prvků a jejich významu pro organizaci, je uveden v tabulce 6.3.

Tabulka 6.3 Identifikace ohrožených prvků organizace a stanovení jejich významnosti

Ohrožený prvek	Identifikovaný ohrožený prvek	Hodnota ohroženého prvku
Hardware	Servery	5
	Počítačové sestavy	4
	Tiskárny	2
	Stroje a výrobní zařízení	5
Ušlý obrat	Ušlý obrat	5
Pokuty	Pokuty ze strany dozorových orgánů	5
	Pokuty ze strany odběratelů	4
Software	Databázové systémy	5
	Speciální software (technologické postupy, výrobní postupy)	4
	Operační systémy	4

Ohrožený prvek	Identifikovaný ohrožený prvek	Hodnota ohroženého prvku
Náklady na rekonstrukci a obnovu dat	Náklady na rekonstrukci dat	4
	Náklady na obnovu dat	5
Poškození dobrého jména	Poškození vztahů se současnými zákazníky	5
	Poškození vztahů s potenciálními budoucími zákazníky	5
	Poškození vztahů se současnými dodavateli a odběrateli	5
	Poškození vztahů s potenciálními budoucími dodavateli a odběrateli.	5
Náklady na oznámení ztráty nebo úniku dat dozorovým orgánům	Náklady na službu help-desk	3
	Speciální vyšetřovací činnost kybernetického incidentu	4
	Nápravná opatření	5

Druhým krokem je identifikace kybernetických hrozeb a zranitelnosti. Pro prvky, které byly identifikovány v předchozím kroku, byly definovány možné příčiny zranitelnosti. Pro určení závažnosti kybernetické hrozby je zde opět použita číselná škála od 1 do 5, která je uvedena v tabulce č. 6.4. Číslem 5 je označena nejpravděpodobnější kybernetická hrozba a číslem 1 nejméně pravděpodobná kybernetická hrozba. V tomto případě je použito u každé číselné hodnoty následující desetinné rozmezí.

Tabulka 6.4 Číselné vyjádření pravděpodobnosti

Pravděpodobnost hrozby	Číselné vyjádření
1	0 – 0,25
2	0,3 – 0,45
3	0,5 – 0,65
4	0,7 – 0,85
5	0,9 - 1

Přiřazení závažnosti konkrétní kybernetické hrozbě je prováděno na základě dotazníkového šetření, ve kterém organizace vyplní údaje o pravděpodobnosti realizace vybraných kybernetických hrozeb. Vybrané kybernetické hrozby a jejich pravděpodobnost realizace pro organizaci, je uvedena v následující tabulce.

Tabulka 6.5 Kybernetické hrozby a určení jejich pravděpodobnosti

Kybernetická hrozba	Pravděpodobnost hrozby	Příklad zranitelnosti
Ransomware	3	Nedostatečná antivirová ochrana informačního systému, nekvalitní bezpečnostní software, nedostatečné zabezpečení e-mailu, nedostatečně vzdělaný zaměstnanec.
Úmyslná trestná činnost prováděna hackerem	4	Nedostatečná antivirová ochrana informačního systému, nekvalitní bezpečnostní software, nedostatečné zabezpečení e-mailu, nedostatečně vzdělaný zaměstnanec.
Neoprávněný přístup	3	Nedostatečné zabezpečení informačního systému (nepravidelná aktualizace hesel, snadný přístup k informačnímu systému).

Kybernetická hrozba	Pravděpodobnost hrozby	Příklad zranitelnosti
Malware	2	Nedostatečná antivirová ochrana informačního systému, nekvalitní bezpečnostní software, nedostatečné zabezpečení e-mailu, nedostatečně vzdělaný zaměstnanec.
Únik dat vlivem nedbalosti zaměstnance	5	Nedodržování bezpečnostních zásad, týkajících se nakládání s interními a citlivými daty organizace.
DDoS útok	2	Nedostatečná kapacita a odolnost počítačové sítě, nedostatečná síťová ochrana,
Fyzická ztráta nosiče dat (ztráta notebooku)	2	Nedostatečné zabezpečení objektu, ve kterém se nosič dat nachází, rizikové chování zaměstnance.
Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje	1	Nedostatečná ochrana proti úderu blesku (absence bleskosvodu, bleskojistek apod.)
Selhání systému	1	Nedostatečná technická údržba zařízení, selhání lidského faktoru.

Třetí krok představuje provedení analýzy rizik. Při tomto postupu zde bude využíváno čtyř tabulek. První dvě z nich (tabulky 6.6 a 6.7) zobrazují ohrožené prvky a identifikované hrozby s jejich přiřazenými hodnotami.

Tabulka 6.6 Matice zranitelnosti 1

Matice zranitelnosti 1	**Popis ohrožené ho prvku**	Servery	Počítačové sestavy	Tiskárny	Stroje a výrobní zařízení	Ušlý obrat	Pokuty ze strany dozorových orgánů	Pokuty ze strany odběratelů	Databázové systémy	Speciální software
	Hodnota ohrožené ho prvku (H)	5	4	2	5	5	5	4	5	4
Kybernetická hrozba	**Pravděp odobnost hrozby (T)**									
Ransomware	3	1	5	1	1	2			5	5
Úmyslná trestná činnost prováděna hackerem	4	5	5				3	3		
Neoprávněný přístup	3	1	5	4					5	5
Malware	2	5	5	2	4	4	4	4	5	5
Únik dat vlivem nedbalosti zaměstnance	5						4	4		
DDoS útok	2	4	5	3			4		5	5

Fyzická ztráta nosiče dat	2		5				4	4	3	3
Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje	1	4	4	1	4	4	4	4	5	5
Selhání systému	1	4	5	2	4	4		3	4	4

Tabulka 6.7 Matice zranitelnosti 2

Matice zranitelnosti 2	**Popis ohroženého prvku**	Operační systémy	Náklady na rekonstrukci dat	Náklady na obnovu dat	Poškození vztahů se současnými zákazníky	Poškození vztahů s potenciálními budoucími zákazníky	Poškození vztahů se současnými dodavateli a odběrateli	Poškození vztahů s potenciálními budoucími dodavateli a odběrateli.	Náklady na službu help-desk	Speciální vyšetřovací činnost kybernetického incidentu	Nápravná opatření
	Hodnota ohroženého prvku (H)	4	4	5	5	5	5	5	3	4	5
Kybernetická hrozba	**Pravděpodobnost hrozby (T)**										
Ransomware	3	5	3	3	1	1	1	1	3	3	4
Úmyslná trestná činnost prováděna hackerem	4	3	5	5	4	4	4	4	4	4	5
Neoprávněný přístup	3	5	4	4	4	4	4	4		4	4
Malware	2	5	5	5	4	4	4	4	4	5	5
Únik dat vlivem nedbalosti zaměstnance	5		5	5	5	4	5	4	4	4	4
DDoS útok	2	5	2	2	4	3	4	3	1	2	3

Fyzická ztráta nosiče dat	2		5	5	5	4	5	4	4	4	4
Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje	1	5	4	4	3	3	3	3			
Selhání systému	1	4	3	3	3	3	3	3	2	2	5

Dalším krokem je výpočet míry rizika. Tato hodnota je vypočítána pomocí vzorce.

$$\boldsymbol{R = T * H * V} \tag{6.16}$$

R = míra rizika
T = pravděpodobnost hrozby
H = hodnota ohroženého prvku (dopad)
V = zranitelnost ohroženého prvku vůči kybernetické hrozbě

Prostřednictvím tohoto vzorce je vypočítána matice rizik, která je uvedena v následujících dvou tabulkách (6.9 a 6.10). V případě, kdy nedochází k interakci kybernetické hrozby s příslušným ohroženým prvkem, zůstává toto pole prázdné.

Opět je zde použita stupnice od 1 do 5, kdy číslem 5 je označena nejpravděpodobnější interakce mezi kybernetickou hrozbou a daným ohroženým prvkem a číslem 1 nejméně pravděpodobná interakce mezi kybernetickou hrozbou a daným ohroženým prvkem. Pro upřesnění a přehlednost výsledků rizik je níže vytvořena stupnice, kde jsou hodnoty rozděleny do tří kategorií, podle jejich závažnosti a dopadu na daný ohrožený prvek. Tyto kategorie jsou také pro lepší přehlednost barevně rozlišeny (tabulka 6.8).

Tabulka 6.8 Stupnice rizikovosti

Riziko	**Rozmezí hodnot**	**Barva**
Nízké riziko	1 až 30	
Střední riziko	31 až 65	
Vysoké riziko	66 až 125	

Tabulka 6.9 Matice rizikovosti 1

Matice rizikovosti 1	**Popis ohrožené ho prvku**	Servery	Počítačové sestavy	Tiskárny	Stroje a výrobní zařízení	Ušlý obrat	Pokuty ze strany dozorových orgánů	Pokuty ze strany odběratelů	Databázové systémy	Speciální software
	Hodnota ohrožené ho prvku (H)	5	4	2	5	5	5	4	5	4
Kybernetická hrozba	**Pravděp odobnost hrozby (T)**									
Ransomware	3	**15**	**60**	**6**	**15**	**30**			**75**	**60**
Úmyslná trestná činnost prováděna hackerem	4	**100**	**80**				**60**	**48**		
Neoprávněný přístup	3	**15**	**60**	**24**					**75**	**60**
Malware	2	**50**	**40**	**8**	**40**	**40**	**40**	**32**	**50**	**40**
Únik dat vlivem nedbalosti zaměstnance	5						**100**	**80**		
DDoS útok	2	**40**	**40**	**12**			**40**		**50**	**40**

Fyzická ztráta nosiče dat	2		**40**				**40**	**32**	**30**	**24**
Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje	1	**20**	**16**	**2**	**20**	**20**	**20**	**16**	**25**	**20**
Selhání systému	1	**20**	**20**	**4**	**20**	**20**		**12**	**20**	**16**

Tabulka 6.10 Matice rizikovosti 2

Matice rizikovosti 2	**Popis ohroženého prvku**	Operační systémy	Náklady na rekonstrukci dat	Náklady na obnovu dat	Poškození vztahů se současnými zákazníky	Poškození vztahů s potenciálními budoucími zákazníky	Poškození vztahů se současnými dodavateli a odběrateli	Poškození vztahů s potenciálními budoucími dodavateli a odběrateli.	Náklady na službu help-desk	Speciální vyšetřovací činnost kybernetického incidentu	Nápravná opatření
	Hodnota ohroženého prvku (H)	4	4	5	5	5	5	5	3	4	5
Kybernetická hrozba	**Pravděpodobnost hrozby (T)**										
Ransomware	3	**60**	**36**	**45**	**15**	**15**	**15**	**15**	**27**	**36**	**60**
Úmyslná trestná činnost prováděna hackerem	4	**48**	**80**	**100**	**80**	**80**	**80**	**80**	**48**	**64**	**100**
Neoprávněný přístup	3	**60**	**48**	**60**	**60**	**60**	**60**	**60**		**48**	**60**
Malware	2	**40**	**40**	**50**	**40**	**40**	**40**	**40**	**24**	**40**	**50**
Únik dat vlivem nedbalosti zaměstnance	5		**100**	**125**	**125**	**100**	**125**	**100**	**60**	**80**	**100**
DDoS útok	2	**40**	**16**	**20**	**40**	**30**	**40**	**30**	**6**	**16**	**30**

Fyzická ztráta nosiče dat	2		**40**	**50**	**50**	**40**	**50**	**40**	**24**	**32**	**40**
Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje	1	**20**	**16**	**20**	**15**	**15**	**15**	**15**			
Selhání systému	1	**16**	**12**	**15**	**15**	**15**	**15**	**15**	**6**	**8**	**25**

Posledním krokem navrhovaného algoritmu je identifikace nejzávažnějšího scénáře kybernetické hrozby a finanční vyjádření možných dopadů této hrozby na informační prostředí organizace. Pro dosažení tohoto cíle je zde aplikována Saatyho metoda. Pro použití této metody a vyjádření preferencí jednotlivých kritérií je zde uvedena následující tabulka.

Tabulka 6.11 Kritéria a jejich preference

Počet bodů	Deskriptor
1	Kritéria jsou stejně vzájemná
3	První kritérium je slabě významnější než druhé
5	První kritérium je dosti významnější než druhé
7	První kritérium je prokazatelně významnější než druhé
9	První kritérium je absolutně významnější než druhé

Výsledkem tohoto kroku je získání pravé horní trojúhelníkové části matice velikostí preferencí (někdy se též tato matice označuje jako Saatyho matice, resp. matice relativních důležitostí). Jestliže tuto matici označíme S, pak její další prvky (na diagonále a v levé dolní trojúhelníkové části) získáme podle vztahů:

$$\boldsymbol{S_{ii} = 1} \qquad \text{pro všechna i,} \tag{6.17}$$

$$\boldsymbol{S_{ji} = \frac{1}{S_{ji}}} \qquad \text{pro všechna i a j.} \tag{6.18}$$

V následující tabulce jsou porovnávány vybrané scénáře kybernetických hrozeb, u kterých se v matici zranitelnosti objevuje největší riziko z pohledu dopadu a finančních ztrát. Účelem této analýzy je identifikace jedné nejzávažnější

kybernetické hrozby, která může mít na organizaci a její informační systém největší dopad.

Tabulka 6.12 Kybernetické hrozby a stanovení jejich významnosti

Kybernetická hrozba	Ransomware	Úmyslná trestná činnost prováděna hackerem	Neoprávněný přístup	Únik dat vlivem nedbalosti zaměstnance	Geometrický průměr
Ransomware		2	5	1	1.96798967127
Úmyslná trestná činnost prováděna hackerem			7	3	4.58257569496
Neoprávněný přístup				1/2	1.41421356237
Únik dat vlivem nedbalosti zaměstnance					

Hodnoty vah kritérií stanovíme pomocí geometrických průměrů řádků Saatyho matice (tyto hodnoty jsou uvedeny v posledním sloupci). Jestliže tyto řádkové geometrické průměry znormujeme, dostaneme normované váhy našeho souboru kritérií.

$$V_i = \frac{G_i}{\sum_{i=1}^{n} G_i} \tag{6.19}$$

V_i = normovaná váha i-tého kriteria
G_i = geometrický průměr i-tého kriteria
n = počet kriterií

Z výsledků analýzy, která byla provedena Saatyho metodou, lze identifikovat, že nejzávažnější hrozbou, která může mít pro organizaci největší dopady, je **úmyslná trestná činnost prováděna hackerem.**

Dalším krokem je vyjádření finančních dopadů na organizaci a její informační prostředí, které je charakterizováno definovanými ohroženými prvky. Pro účely vyjádření finančních škod bude použita hodnotící škála, která vychází z matice zranitelnosti, která byla uvedena v předchozích krocích. Finanční škody jsou zde vypočítány podle tabulky 6.13.

Tabulka 6.13 Klasifikace závažnosti kybernetické hrozby

Stupeň závažnosti hrozby	Procentní podíl z celkové částky
66 – 70	10
71 – 76	20
77 - 82	30
83 – 88	40
89 - 94	50
95 - 100	60
101 - 106	70
107 - 112	80
113 - 118	90
119 - 125	100

V tabulce jsou uvedeny stupně závažnosti hrozby, které vychází z rozmezí nejzávažnějšího rizika, které je uvedeno v tabulce u matice zranitelnosti.

Nejmenší hodnota, které může být dosaženo, je 66 a nejvyšší, která může v této kategorii rizikovosti být udělena, je 125. Postup pro stanovení stupně závažnosti je následující:

a) V matici zranitelnosti je vybrána hrozba, která byla identifikována v analýze Saatyho metodou jako nejvíce závažná.
b) U této hrozby je proveden součet všech hodnot, které se v dané matici objevují (tj. interakce ohroženého prvku a hrozby).
c) Celkový součet se vydělí počtem interakcí.
d) Hodnotě, která byla touto matematickou operací získána, je přiřazeno určité rozmezí hodnot v tabulce s příslušným procentním podílem.
e) Tento procentní podíl je vypočítán z částky, která byla stanovena na začátku celého procesu, tj. ocenění organizace.
f) Výsledná částka by měla pokrýt náklady a finanční škody, které mohou být touto kybernetickou hrozbou způsobeny.

Výpočet:

Průměr hodnot u kybernetické hrozby **„úmyslná trestná činnost prováděna hackerem“** je: **780**

Počet interakcí (ohrožený prvek x hrozba) je: **9**

Průměrná hodnota závažnosti hrozby je: 780 / 9 = 86,66 = **87**

Z uvedené tabulky vyplývá, že škody, které mohou být touto kybernetickou hrozbou způsobeny, by měly tvořit 40 % z celkové částky, která vyjadřuje cenu organizace a jejího informačního systému.

V tomto případě tato částka činí: 12 234 472 * 0,40 = **4 893 789 Kč.**

6.2.2 Případová studie č. 2

Organizace č. 2 provozuje 422 maloobchodních prodejen po celé České republice a její hlavní sídlo je v Ostravě. Byla založena v roce 1991 a svou činnost provozuje až do současnosti. Za tuto dobu si tato společnost zajistila pevné místo na tuzemském trhu, o čemž svědčí roční obrat firmy, který za uplynulý rok činil přes 7 miliard korun. Základní kapitál, který je rozdělen mezi tři společníky, činí 78 000 000 Kč. Svou specializací se firma zaměřuje především na potravinářské zboží (tvoří cca 70 % sortimentu), ale také zboží nepotravinářského charakteru (tvoří cca 30 % sortimentu), jako je drogerie, domácí a kancelářské potřeby. Druhá hlavní pobočka této společnosti se nachází v Uherském Brodě, ze kterého je zásobována jižní a východní Morava.

V organizaci č. 2 pracuje celkem 2 532 zaměstnanců, kteří jsou rozmístěni na různých pracovištích po celé ČR. Všichni zaměstnanci pracují s ekonomickým systémem Manas, který slouží pro objednávání zboží, zadávání nového zboží do katalogu, komunikaci prostřednictvím e-mailového klienta s ostatními zaměstnanci firmy, provádění pokladní uzávěrky, navrhování a tisk cenovek a poutačů ke zboží.

1) Ekonomická část

Z důvodu rozsahu aplikace algoritmu na tomto příkladu organizace jsou v ekonomické a informaticko-bezpečnostní části prezentovány pouze konečné výsledky celého procesu.

Finanční vyjádření ohrožených prvků organizace ve vztahu k informačnímu systému

Hardware: 7 646 000 Kč
Ušlý obrat: 20 547 945 Kč
Pokuty: 5 000 000 Kč
Software: 141 500 Kč
Náklady na rekonstrukci a obnovu dat: 6 446 000 Kč
Poškození dobrého jména: 36 589 123 Kč
Náklady na oznámení ztráty nebo úniku dat: 14 112 Kč

Ohrožené prvky organizace jsou oceněny celkovou částkou: 76 384 680 Kč.

2) Informaticko-bezpečnostní část

Prvním krokem je identifikace ohrožených prvků v organizaci, které jsou uvedeny v tabulce č. 6.14.

Tabulka 6.14 Identifikace ohrožených prvků organizace a stanovení jejich významnosti

Ohrožený prvek	Identifikovaný ohrožený prvek	Hodnota ohroženého prvku
Hardware	Servery	4
	Počítačové sestavy	4
	Tiskárny	2
	Stroje a výrobní zařízení	4
Ušlý obrat	Ušlý obrat	5
Pokuty	Pokuty ze strany dozorových orgánů	4
	Pokuty ze strany dodavatelů	4
	Pokuty ze strany odběratelů	4
Software	Databázové systémy	4
	Speciální software (technologické postupy, výrobní postupy)	4
	Operační systémy	5
Náklady na rekonstrukci a obnovu dat	Náklady na rekonstrukci dat	4
	Náklady na obnovu dat	4
Poškození dobrého jména	Poškození vztahů se současnými zákazníky	5
	Poškození vztahů s potenciálními budoucími zákazníky	5

Ohrožený prvek	Identifikovaný ohrožený prvek	Hodnota ohroženého prvku
	Poškození vztahů se současnými dodavateli a odběrateli	5
	Poškození vztahů s potenciálními budoucími dodavateli a odběrateli.	5
Náklady na oznámení ztráty nebo úniku dat dozorovým orgánům	Náklady na službu help-desk	2
	Speciální vyšetřovací činnost kybernetického incidentu	4
	Nápravná opatření	4

Druhým krokem je identifikace kybernetických hrozeb a pravděpodobnosti jejich vzniku pro organizaci. K tomuto kroku je opět použita stupnice pravděpodobnosti (tabulka 6.15). Seznam vybraných kybernetických hrozeb je uveden v tabulce 6.16.

Tabulka 6.15 Číselné vyjádření pravděpodobnosti

Pravděpodobnost hrozby	Číselné vyjádření
1	0 – 0,25
2	0,3 – 0,45
3	0,5 – 0,65
4	0,7 – 0,85
5	0,9 - 1

Tabulka 6.16 Kybernetické hrozby a určení jejich pravděpodobnosti

Kybernetická hrozba	Pravděpodobnost hrozby	Příklad zranitelnosti
Ransomware	4	Nedostatečná antivirová ochrana informačního systému, nekvalitní bezpečnostní software, nedostatečné zabezpečení e-mailu, nedostatečně vzdělaný zaměstnanec.
Úmyslná trestná činnost prováděna hackerem	4	Nedostatečná antivirová ochrana informačního systému, nekvalitní bezpečnostní software, nedostatečné zabezpečení e-mailu, nedostatečně vzdělaný zaměstnanec.
Neoprávněný přístup	3	Nedostatečné zabezpečení informačního systému (nepravidelná aktualizace hesel, snadný přístup k informačnímu systému).
Malware	3	Nedostatečná antivirová ochrana informačního systému, nekvalitní bezpečnostní software, nedostatečné zabezpečení e-mailu, nedostatečně vzdělaný zaměstnanec.
Únik dat vlivem nedbalosti zaměstnance	4	Nedodržování bezpečnostních zásad, týkajících se nakládání s interními a citlivými daty organizace.
DDoS útok	3	Nedostatečná kapacita a odolnost počítačové sítě, nedostatečná síťová ochrana,

Kybernetická hrozba	Pravděpodobnost hrozby	Příklad zranitelnosti
Fyzická ztráta nosiče dat (ztráta notebooku)	2	Nedostatečné zabezpečení objektu, ve kterém se nosič dat nachází, rizikové chování zaměstnance.
Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje	1	Nedostatečná ochrana proti úderu blesku (absence bleskosvodu, bleskojistek apod.)
Selhání systému	1	Nedostatečná technická údržba zařízení, selhání lidského faktoru.

Třetí krok představuje provedení analýzy rizik s cílem vyjádřit interakci jednotlivých kybernetických hrozeb s definovanými ohroženými prvky.

Tabulka 6.17 Matice zranitelnosti 3

Matice zranitelnosti 3	**Popis ohrožené ho prvku**	Servery	Počítačové sestavy	Tiskárny	Stroje a výrobní zařízení	Ušlý obrat	Pokuty ze strany dozorových orgánů	Pokuty ze strany dodavatelů	Pokuty ze strany odběratelů	Databázové systémy	Speciální software
	Hodnota ohrožené ho prvku (H)	4	4	2	4	5	4	4	4	4	4
Kybernetická hrozba	**Pravděp odobnost hrozby (T)**										
Ransomware	4	2	5	1	1	3				5	5
Úmyslná trestná činnost prováděna hackerem	4	5	5				3	3	3		
Neoprávněný přístup	3	1	4	1	1		4	4	4	5	4
Malware	3	5	5	1	1	2	3	3	3	5	5
Únik dat vlivem nedbalosti zaměstnance	4						5	5	5		
DDoS útok	3	4	5	3			1	1	1	5	5

Fyzická ztráta nosiče dat	2		5				4	4	4	4	4
Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje	1	4	4	1	4	4	3	3	3	4	4
Selhání systému	1	4	5	1	4	4		3	3	4	4

Tabulka 6.18 Matice zranitelnosti 4

Matice zranitelnosti 4	**Popis ohroženého prvku**	Operační systémy	Náklady na rekonstrukci dat	Náklady na obnovu dat	Poškození vztahů se současnými zákazníky	Poškození vztahů s potenciálními budoucími zákazníky	Poškození vztahů se současnými dodavateli a odběrateli	Poškození vztahů s potenciálními budoucími dodavateli a odběrateli.	Náklady na službu help-desk	Speciální vyšetřovací činnost kybernetického incidentu	Nápravná opatření
	Hodnota ohroženého prvku (H)	5	4	4	5	5	5	5	2	4	4
Kybernetická hrozba	**Pravděpodobnost hrozby (T)**										
Ransomware	4	5	3	3	3	3	3	3	2	3	4
Úmyslná trestná činnost prováděna hackerem	4	3	4	4	5	5	5	5	3	4	5
Neoprávněný přístup	3	3	4	4	4	4	4	4		4	4
Malware	3	5	4	4	4	4	4	4	4	5	5
Únik dat vlivem nedbalosti zaměstnance	4		5	5	5	5	5	5	3	5	5
DDoS útok	3	5	2	2	3	3	3	3	1	3	2

Fyzická ztráta nosiče dat	2		5	5	5	4	5	4	4	4	4
Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje	1	5	4	4	3	3	3	3			
Selhání systému	1	4	3	3	3	3	3	3	1	2	5

Tabulka 6.19 Matice rizikovosti 3

Matice rizikovosti 3	**Popis ohrožené ho prvku**	Servery	Počítačové sestavy	Tiskárny	Stroje a výrobní zařízení	Ušlý obrat	Pokuty ze strany dozorových orgánů	Pokuty ze strany dodavatelů	Pokuty ze strany odběratelů	Databázové systémy	Speciální software
	Hodnota ohrožené ho prvku (H)	4	4	2	4	5	4	4	4	4	4
Kybernetická hrozba	**Pravděp odobnost hrozby (T)**										
Ransomware	4	**32**	**80**	**8**	**16**	**60**				**80**	**80**
Úmyslná trestná činnost prováděna hackerem	4	**80**	**80**				**48**	**48**	**48**		
Neoprávněný přístup	3	**12**	**48**	**6**	**12**		**48**	**48**	**48**	**60**	**48**
Malware	3	**60**	**60**	**6**	**12**	**30**	**36**	**36**	**36**	**60**	**60**
Únik dat vlivem nedbalosti zaměstnance	4						**80**	**80**	**80**		
DDoS útok	3	**48**	**60**	**18**			**12**	**12**	**12**	**60**	**60**

Fyzická ztráta nosiče dat	2		**40**				**32**	**32**	**32**	**32**	**32**
Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje	1	**16**	**16**	**2**	**16**	**20**	**12**	**12**	**12**	**16**	**16**
Selhání systému	1	**16**	**20**	**2**	**16**	**20**		**12**	**12**	**16**	**16**

Tabulka 6.20 Matice rizikovosti 4

Matice rizikovosti 4	**Popis ohroženého prvku**	Operační systémy	Náklady na rekonstrukci dat	Náklady na obnovu dat	Poškození vztahů se současnými zákazníky	Poškození vztahů s potenciálními budoucími zákazníky	Poškození vztahů se současnými dodavateli a odběrateli	Poškození vztahů s potenciálními budoucími dodavateli a odběrateli.	Náklady na službu help-desk	Speciální vyšetřovací činnost kybernetického incidentu	Nápravná opatření
	Hodnota ohroženého prvku (H)	5	4	4	5	5	5	5	2	4	4
Kybernetická hrozba	**Pravděpodobnost hrozby (T)**										
Ransomware	4	**100**	**48**	**48**	**60**	**60**	**60**	**60**	**16**	**48**	**64**
Úmyslná trestná činnost prováděna hackerem	4	**60**	**64**	**64**	**100**	**100**	**100**	**100**	**24**	**64**	**80**
Neoprávněný přístup	3	**45**	**48**	**48**	**60**	**60**	**60**	**60**		**48**	**48**
Malware	3	**75**	**48**	**48**	**60**	**60**	**60**	**60**	**24**	**60**	**60**
Únik dat vlivem nedbalosti zaměstnance	4		**80**	**80**	**100**	**100**	**100**	**100**	**24**	**80**	**80**
DDoS útok	3	**75**	**24**	**24**	**45**	**45**	**45**	**45**	**6**	**36**	**24**

Fyzická ztráta nosiče dat	2		**40**	**40**	**50**	**40**	**50**	**40**	**16**	**32**	**32**
Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje	1	**25**	**16**	**16**	**15**	**15**	**15**	**15**			
Selhání systému	1	**20**	**12**	**12**	**15**	**15**	**15**	**15**	**2**	**8**	**20**

Z výsledků analýzy, která byla provedena Saatyho metodou, lze identifikovat, že nejzávažnější hrozbou, která může mít pro organizaci největší dopady, je **únik dat vlivem nedbalosti zaměstnance.**

Výpočet:

Průměr hodnot u kybernetické hrozby **„únik dat vlivem nedbalosti zaměstnance“** je: **960**

Počet interakcí (ohrožený prvek x hrozba) je: **11**

Průměrná hodnota závažnosti hrozby je: 960 / 11 = 87,27 = **87**

Z uvedené tabulky vyplývá, že škody, které mohou být touto kybernetickou hrozbou způsobeny, by měly tvořit 40 % z celkové částky, která vyjadřuje cenu organizace a jejího informačního systému.

V tomto případě tato částka činí: 76 384 680 * 0,40 = **30 553 872 Kč.**

7. PŘÍNOS PRO VĚDU A PRO PRAXI

V rámci této kapitoly je popsán význam a přínos navrhovaného výsledku disertační práce pro vědu a praxi. Jsou zde popsány hlavní výstupy výzkumu, které jsou uvedeny v následujících dvou podkapitolách.

7.1 Přínos pro vědu

Výsledky disertační práce jsou přínosné pro vědeckou komunitu především z pohledu kvantifikace definovaných ohrožených prvků a stanovení možných finančních dopadů na organizaci a její informační systém. Jelikož se jedná o transdisciplinární oblast zájmu, výsledky disertační práce mohou najít své uplatnění především v oblastech, jako je ekonomika, informační a komunikační technologie nebo bezpečnost. Navržený algoritmus může přinést nový pohled do oblasti kybernetické bezpečnosti, a to především pro popis a zkoumání možných dopadů kybernetických hrozeb na organizaci a její informační prostředí. Tento nový pohled může najít své uplatnění ve vědecké komunitě především z důvodu zachycení vzájemných vztahů mezi ohroženými prvky a kybernetickými hrozbami a tím zpřesnění stanovení potenciálních finančních škod v organizaci.

Hlavním výsledkem navrženého algoritmu je stanovení významných oblastí informačního prostředí, jejichž ohrožení nebo významné narušení prostřednictvím kybernetické hrozby může způsobit organizaci významné finanční škody. Tyto oblasti jsou zde charakterizovány prostřednictvím definovaných ohrožených prvků a jejich ocenění. Tyto prvky mají hmotný a nehmotný charakter a proto může být jejich matematické vyjádření, které je v této disertační práci navrženo, velmi přínosné pro vědeckou komunitu. Výsledky disertační práce jsou přínosné také pro rozvoj vědních oborů kybernetická bezpečnost a pojišťovnictví, a to především z pohledu stanovení potenciálních finančních škod v definovaných oblastech informačního prostředí, které nelze vyjádřit prostřednictvím metod pojistné matematiky.

Algoritmus pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví byl navržen na základě analýzy dosavadních knižních a publikačních výstupů. V rámci výzkumu byly rovněž provedeny konzultace s vybranými institucemi, jejichž zaměření úzce souvisí s řešenou problematikou. Jedná se např. o vysoké školy, pojišťovny, malé a střední organizace nebo uzavřené pracovní skupiny. Na základě zjištěných skutečností byl sestaven algoritmus, jehož cílem je integrovat a sjednotit postup stanovení pojistné hodnoty organizace s ohledem na transdisciplinární rozměr problematiky pojištění organizací proti kybernetickým hrozbám.

Výsledky výzkumu byly v průběhu řešení disertační práce publikovány v řadě odborných příspěvků v rámci recenzovaných časopisů, mezinárodních konferencí a odborných časopisů, které jsou evidovány v databázích SCOPUS nebo Web of Science.

7.2 Přínos pro praxi

Hlavní výsledky práce bude možné uplatnit především v oblasti pojišťovnictví a kybernetické bezpečnosti jako analytický nástroj pro posouzení bezpečnostní stránky organizace, která má být pojištěna proti dopadům kybernetických hrozeb. Jelikož současné přístupy k řešení této problematiky nezohledňují vždy všechny aspekty, které mohou mít zásadní vliv na výši pojistné hodnoty, může navrhovaný algoritmus poskytnout přehled o možných dopadech v různých oblastech organizace, které jsou ovlivňovány funkcí informačního systému. Z tohoto důvodu je navrhovaný algoritmus velmi přínosný pro odborníky v oblasti kybernetické bezpečnosti, pojistitele, pojistné makléře a také pro analytiky v oboru pojišťovnictví. Využít tento nástroj mohou také ratingové agentury nebo specializované firmy, které zajišťují odborné poradenství pro pojišťovny v oblasti informačních technologií a bezpečnosti.

Uplatnění navrhovaného algoritmu lze ale také nalézt na straně samotných organizací, které uvažují o takovém typu pojištění. Konkrétní organizace si tedy může provést analýzu svého vlastního informačního prostředí a posoudit tak, jakými kybernetickými hrozbami a s jakou rizikovostí může být zasažena. Výstupem tohoto procesu je pak stanovení možných finančních škod, které mohou být kritériem pro sjednání pojistné smlouvy. Zjištěné výsledky mohou také přinést nový pohled na bezpečnostní situaci v organizaci, což může vést k zavedení a zlepšení bezpečnostních mechanismů.

Velký přínos může tato práce nalézt také v brzké budoucnosti. Vlivem vzrůstající frekvence kybernetických útoků na organizace a jejich informační systémy lze predikovat, že zájem o tento typ pojištění bude narůstat. Vzhledem k legislativě, která souvisí s ochranou osobních dat a sankcemi, které s touto problematikou souvisí, lze rovněž předpokládat, že organizace budou v rámci ochrany svých aktiv vyvíjet větší zájem o pojištění tohoto typu. Dalším významným aspektem jsou také samotné finanční škody, které v oblastech jako je např. dobré jméno, ušlý obrat nebo náklady na rekonstrukci nebo obnovu dat mohou být pro organizaci likvidační. Finanční částka na obnovu těchto oblastí by mohla být pro poškozenou organizaci rovněž velmi zatěžující, a proto by pojištění proti kybernetickým hrozbám mohlo být vhodným nástrojem, jak tuto negativní událost a její dopady zmírnit a umožnit tak organizaci dosáhnout opět stavu rovnováhy.

8. ZÁVĚR

Současná společnost je čím dál více orientována na informační a komunikační technologie. Komunikační prostředky a nástroje se staly nedílnou součástí nejen lidských životů, ale také pracovního prostředí, ve kterém přispívají ke zkvalitňování podnikových procesů. Je zřejmé, že organizace využívající těchto informačních a komunikačních prostředků mohou být předmětem kybernetických útoků. Tyto útoky mohou mít za cíl nejen organizaci poškodit, ale také zamezit její funkci a obnově činnosti.

Předložená disertační práce je zaměřena na tuto oblast s cílem navrhnout algoritmus pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví. V rámci kompenzace a snižování potenciálních škod, které mohou vlivem některé z kybernetických hrozeb nastat, může být aplikován jako účinný nástroj pojištění organizace proti kybernetickým hrozbám. Navržený algoritmus je výsledkem nejen rešerší dostupných informačních zdrojů z této oblasti, ale také strukturovaných rozhovorů a konzultací se zástupci v oblastech pojišťovnictví, bezpečnosti a informačních a komunikačních technologií. Rešerše a konzultace byly provedeny jak v českém, tak zahraničním prostředí. Disertační práce vychází z předpokladu, že do procesu stanovení pojistné hodnoty organizace, která má být pojištěna proti kybernetickým hrozbám, by měly být zahrnuty také jiné oblasti, jejichž funkce ovlivňuje činnost celé organizace. Výzkum realizovaný v rámci řešení disertační práce tento předpoklad potvrdil. Došlo k identifikaci a zpřesnění ohrožených prvků organizace, které je nutno do stanovení výše pojistné hodnoty zahrnout.

Hlavním přínosem této práce z pohledu novosti je návrh algoritmu pro stanovení pojistné hodnoty, který je založen na definování a ocenění vybraných ohrožených prvků organizace, které představují z pohledu významnosti důležité oblasti organizace. Dále se jedná o stanovení vybraných kybernetických hrozeb včetně vyjádření interakce těchto hrozeb vůči stanoveným ohroženým prvkům, identifikaci nejzávažnější kybernetické hrozby pro danou organizaci a vyjádření potenciálních finančních dopadů na její informační prostředí.

V následujících letech bude tento algoritmus zpřesňován na větším množství organizací, které se budou významným způsobem lišit svou velikostí i předmětem činnosti. Cílem bude ověření funkcionality a konfigurace stanovených ohrožených prvků, což by mělo vést k přesnějšímu vyjádření finančních škod v organizaci, které mohou být způsobeny negativním dopadem kybernetické hrozby. Hlavním záměrem bude nabídnout tento algoritmus pojistným institucím s cílem poskytnout jim analytický nástroj pro zkvalitnění procesu stanovení pojistné hodnoty v rámci pojištění organizací proti kybernetickým hrozbám. Na základě dosažených výsledků lze konstatovat, že cíle disertační práce byly splněny.

SEZNAM POUŽITÉ LITERATURY

Kniha

BASL, Josef a Roman BLAŽÍČEK. *Podnikové informační systémy*. 3. aktualizované a doplněné vydání. Praha: Grada, 2012, 328 s. Management informační bezpečnosti. ISBN 978-80-247-4307-3.

BRUCKNER, Tomáš, Jiří VOŘÍŠEK, Alena BUCHALCEVOVÁ, et al. *Tvorba informačních systémů: principy, metodiky, architektury*. 1. vyd. Praha: Grada, 2012, 357 s. Management v informační společnosti. ISBN 978-80-247-4153-6.

ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009, 138 s. ISBN 978-80-7399-731-1.

DUCHÁČKOVÁ, Eva. *Pojištění a pojišťovnictví*. Praha: Ekopress, 2015, 306 s. ISBN 978-80-87865-25-5.

DUCHÁČKOVÁ, Eva. *Principy pojištění a pojišťovnictví*. 3. vydání. Praha: Ekopress, 2009, 224 s. ISBN 978-80-86929-51.

NĚMEČEK, Alojz a Jiří JANATA. *Oceňování majetku v pojišťovnictví*. Praha: C. H. Beck, 2010, 192 s. ISBN 978-80-7400-114-7.

SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4. aktualizované a rozšířené vydání. Praha: Grada, 2013, 488 s. ISBN 978-80-247-4644-9.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Praha: Aleš Čeněk, 2018, 936 s. ISBN 978-80-7380-720-7.

ŠILEROVÁ, Edita, Klára HENNYEYOVÁ a N.N. BALASHOVA. *Informační systémy v podnikové praxi*. Praha: Poweprint, 2016, 163 s. ISBN 978-80-87994-78-8.

TICHÝ, Milík. *Ovládání rizika: analýza a management*. Vyd. 1. Praha: C.H. Beck, 2006, xxvi, 396 s. Beckova edice ekonomie. ISBN 80-717-9415-5.

VARADZIN, František. *Řízení bezpečnosti informací*. 2. vydání. Praha: Professional publishing, 2012, 180 s. ISBN 978-80-7431-050-8.

E-kniha

JANÍČEK, Přemysl a Marek JÍŠA. *Expertní inženýrství v systémovém pojetí*. Praha: Grada, 2013, 592 s. ISBN 978-80-247-4127-7

KOLOUCH, Jan. *CyberCrime* [online]. Praha: CZ.NIC, z.s.p.o., 2016, 511 s. [cit. 2019-04-29]. CZ.NIC. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

Skriptum

MARTINOVIČOVÁ, Dana. *Pojišťovnictví*. Brno: Akademické nakladatelství CERM, 2006, 124 s. ISBN 80-214-3257-8.

Kvalifikační, disertační a habilitační práce

POHANKA, M. *Analýza informačního systému výrobní firmy a návrh změn.* Brno: Vysoké učení technické v Brně, Ústav soudního inženýrství, 2013. 102 s. Vedoucí diplomové práce doc. Ing. Miloš Koch, CSc.

Článek v elektronickém časopise

FRANKE, Ulrik. The cyber insurance market in Sweden. *Computers & Security* [online]. USA: Elsevier, 2017, (68), 130 - 144 [cit. 2018-12-02]. ISSN 0167-4048. Dostupné z: https://www.sciencedirect.com

KREUZER, Martin. Pojištění kybernetických rizik – od rizik k příležitostem. *Pojistný obzor* [online]. Praha: Česká asociace pojišťoven, 2018, **96**(4/2018), 34 - 36 [cit. 2019-02-18]. ISSN 2464-7381. Dostupné z: https://www.pojistnyobzor.cz/archiv

MAROTTA, Angelica, Fabio MARTINELLI, Stefano Nannia NANNIA, Albina ORLANDO a Artsiom YAUTSIUKHIN. Cyber-insurance survey. *Computer Science Review* [online]. Netherlands: Elsevier, 2017, (24), 35 - 61 [cit. 2019-02-28]. ISSN 1574-0137 Dostupné z: https://www.iit.cnr.it/sites/default/files/MARO-17-CSR.pdf

Internetové zdroje

AIG - Cyber Edge: End-to-End Cyber Risk Management Solutions [online]. USA: AIG, 2015, 12 s. [cit. 2018-11-08]. Dostupné z: https://www.aig.com/content/dam/aig/canada/us/documents/brochure/aig-cyber-edge-0418-final-single.pdf

CIO and Leader. Cyber Attack Disrupting Critical Infrastructure In 2016 A Likelihood, Say Security Professionals. IT Next [online]. 2016 [cit. 2017-01-23]. Dostupné z: http://www.itnext.in/article/2016/01/14/cyber-attack-disrupting-critical-infrastructure-2016-likelihood-say-security

Čandík Marek. Informační bezpečnost. [online]. 19.12.2016 [cit. 2018-12-19]. Dostupné z: http://www.cybersecurity.cz/data/candik2.pdf

Insurance 2020 & beyond: Necessity is the mother of reinvention [online]. United Kingdom: PWC, 2015, 28 s. [cit. 2019-01-27]. Dostupné z: https://www.pwc.com/gx/en/insurance/publications/assets/pwc-insurance-2020-and-beyond.pdf

KASPERSKY LAB ICS CERT. *Threat landscape for industrial automation systems. H2 2018* [online]. Rusko, 2019 [cit. 2019-05-06]. Dostupné z: https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/#_Toc4416091

Kyberkriminalita: Národní centrála proti organizovanému zločinu SKPV. *Policie ČR* [online]. 2019 [cit. 2019-05-05].
Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

MOLÁČEK, Petr a Daniel KONEČNÝ. Kybernetická rizika jsou pro české pojišťovny téma. *Cyberinsurance.cz* [online]. Praha, 2017, 31. 3. 2017 [cit. 2019-04-28]. Dostupné z: http://www.cyberinsurance.cz/?p=534

MOLÁČEK, Petr a Daniel KONEČNÝ. Role pojišťovnictví v kyber prostředí. *Cyberinsurance.cz* [online]. Praha, 2018, 17. 5. 2018 [cit. 2019-03-15]. Dostupné z: http://www.cyberinsurance.cz/?p=698

Ponemon study 2018 [online]. USA: Ponemon Institute, 2018, 47 s. [cit. 2019-04-28]. Dostupné z : https://databreachcalculator.mybluemix/assets/2018

SKOKAN, Jindřich a Jana ŠEDINOVÁ. *ČVUT - PRAŽSKÁ SÍŤ PODPORY ELEKTRONICKÉHO VZDĚLÁVÁNÍ. Informační gramotnost jako kognitivní systém* [online]. Praha, 2008 [cit. 2019-05-02]. Dostupné z: http://pspev.cvut.cz/PSPEV_CD/V5/main.html?ID=15

STATISTICKÉ ÚDAJE DLE METODIKY ČAP 1–3/2019 – GRAFY [online]. Praha: Česká asociace pojišťoven, 2019 [cit. 2019-04-30]. Dostupné z: https://www.opojisteni.cz/res/archive/104/011301.pdf

Zvláštní pojistné podmínky pro pojištění pro případ přerušení nebo omezení provozu [online]. Kooperativa Vienna Insurance Group, 2019 [cit. 2019-03-30]. Dostupné z: https://www.koop.cz/dokumenty/podnikatele-prumysl/file-1034-general-pdf/file_1034_GENERAL.pdf

Legislativní zdroje

ČR. Zákon č. 110/2019 Sb. o zpracování osobních údajů. In: *Sbírka zákonů - Česká republika 2019*. Ministerstvo vnitra, p.o. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

ČR. *Nový občanský zákoník: (ve znění účinném k 1.7.2018)*. In: . Tošovský – advokátní kancelář, 2019.
Dostupné také z: http://www.pracepropravniky.cz/zakony/novy-obcansky-zakonik-2014-uplne-zneni

ČR. *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In: 181/2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

ČR. *Zákon č. 37/2004 Sb. o pojistné smlouvě a o změně souvisejících zákonů (zákon o pojistné smlouvě)*. In: 37/2004. Dostupné také z: https://www.zakonyprolidi.cz/cs/2004-37

ČR. *Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti*. In: 412/2005. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

EU. *Nařízení Evropské unie 2016/679 (General Data Protection Regulation)*. In: 2016/679 Dostupné také z: https://www.uoou.cz/assets/File.ashx?id

EU. *Směrnice 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*. In: 2016/1148. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016L1148

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM POUŽITŽÝCH ZKRATEK

AIG	American International Group, Inc.
APS	Advanced Planning and Scheduling
CPU	Centrální procesorová jednotka
CRM	Customer Realtionship Management
DDoS	Denial of Distributed Service
DHM	Dlouhodobý hmotný majetek
DoS	Denial of Service
ERP	Enterprise Resource Planning
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IS	Informační systém
IT	Informační technologie
PWC	PricewaterhouseCoopers
SAP	Systeme, Anwendungen, Produkte in der Datenverarbeitung
SCM	Supply Chain Management
SME	Small and Medium Enterprise
STAG	Studijní agenda
USD	Americký dolar

PUBLIKAČNÍ ČINNOST AUTORA

Články v recenzovaných časopisech evidovaných v databázi SCOPUS, WoS

PAVLÍK, Lukáš. Modeling the Impact of Cyber Threats on an Organization's Information System in the Framework of Cyber-Risk Insurance. *International Journal of Mathematical Models and Methods in Applied Sciences* [online]. USA: North Atlantic University Union, 2019, 5 s., **13**(13) [cit. 2019-04-26]. ISSN 1998-0140. Dostupné z: http://naun.org/cms.action?id=20232

PAVLÍK, Lukáš. Modeling the Impact of Selected Cyber Threats on the Organization's Parameters in the Framework of Cyber Risk Insurance. WSEAS Transactions on Business and Economics [online]. 2018, 7 s., **10** (Vol. 15) [cit. 2018-11-15]. ISSN 1109-9526. Dostupné z: http://www.wseas.org/multimedia/journals/economics/2018/b025107-669.pdf

Články ve vědeckých nebo odborných časopisech neevidovaných v databázích WoS, SCOPUS

PAVLÍK, Lukáš, Tomáš KLÍMA a Krerk PIROMSOPA. *The Issue of Cyber-Risk Insurance from the Point of View of the Valuation of the Information System in the Organization* [online]. Vol. 11. North Atlantic University Union, 2017, 6 s. [cit. 2017-11-26]. ISSN 1998-4308. Dostupné z: http://naun.org/cms.action?id=16148

PAVLÍK, Lukáš. POSTERUS.SK. *Metrics for Evaluating Information Systems* [online]. Slovensko, 2017, 10 s. [cit. 2017-05-17]. ISSN 1338-0087.

PAVLÍK, Lukáš. Quantitative and Qualitative Assessment Tools for Information Systems Security. Posterus.sk [online]. 2016, 9(5), 8 s. [cit. 2016-06-30]. ISSN 1338-0087. Dostupné z: http://www.posterus.sk/?p=18519

Články ve sborníku konference evidovaných v databázi SCOPUS, WoS

PAVLÍK, Lukáš. Design Methodology for Determining the Financial Damage caused by Cyber Threats in the Field of Insurance. In: *ICMT 2019*. Brno: Univerzita obrany, 2019.

FICEK, Martin, Lukáš PAVLÍK, Rui Miguel SOARES SILVA a Michaela MILKULIČOVÁ. *Influence of distance to depth shot of a CO2-powered airsoft gun with lead shot ammunition and shape of the temporary and permanent cavity in ballistic gelatin*. Athens, Greece: 23 rd INTERNATIONAL CONFERENCE ON CIRCUITS, SYSTEMS, COMMUNICATIONS AND COMPUTERS (CSCC 2019), 2019, 7 s.

Článek je přijat na konferenci, prezentován bude v červenci 2019.

VEČEŘA, Filip a Lukáš PAVLÍK . *The finding of the queuing theory models for evaluation throughput of the IRS radio network in the Czech Republic*. Athens, Greece: 23 rd INTERNATIONAL CONFERENCE ON CIRCUITS, SYSTEMS, COMMUNICATIONS AND COMPUTERS (CSCC 2019), 2019, 6 s.

Článek je přijat na konferenci, prezentován bude v červenci 2019.

PAVLÍK, Lukáš. *Possibilities of modelling the impact of cyber threats in cyber risk insurance*. 22 nd INTERNATIONAL CONFERENCE ON CIRCUITS, SYSTEMS, COMMUNICATIONS AND COMPUTERS (CSCC 2018). Majorca, Spain, 2018, 4 s.

ŠAUR, David a Lukáš PAVLÍK. *Comparison of accuracy of forecasting methods of convective precipitation*. Majorca, Spain: INTERNATIONAL CONFERENCE ON CIRCUITS, SYSTEMS, COMMUNICATIONS AND COMPUTERS (CSCC 2018), 2018, 6 s.

GRACLA, Michal a Lukáš PAVLÍK. *Preparation of experimental measurements using a firearm.* Majorca, Spain: INTERNATIONAL CONFERENCE ON CIRCUITS, SYSTEMS, COMMUNICATIONS AND COMPUTERS (CSCC 2018), 2018, 6 s.

PAVLÍK Lukáš. *Identifying and Modeling the Impact of Cyber Threats in the Field of Cyber Risk Insurance*. INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN SCIENCES AND INDUSTRY 2018. Corfu, Greece: IEEE, 4 s. [cit. 2018-04-30].

PAVLÍK, Lukáš. *Mathematical Method as a Tool for the Identification of Assets within the Organization Providing Insurance against Cyber Risk.*

INTERNATIONAL CONFERENCE KNOWLEDGE FOR MARKET USE 2017. Univerzita Palackého, Filozofická fakulta, Olomouc, 2017, 9 s. ISBN 978-80-244-5233-3

KLÍMA, Tomáš, Krerk PIROMSOPA a Lukáš PAVLÍK. *Designing model for calculating the amount of cyber risk insurance*. INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN SCIENCES AND INDUSTRY 2017. Corfu, Greece: IEEE, 5 s.

PAVLÍK, Lukáš a Luděk LUKÁŠ *Pareto Analysis as a Tool for the Identification of Assets within the Organization Providing Insurance against Cyber Risk*. INTERNATIONAL CONFERENCE ON MILITARY TECHNOLOGIES 2017. Univerzita obrany, Brno, 2017, 5 s. ISBN 978-1-5386-1988-9 [cit. 2017-05-17]

PAVLÍK, Lukáš a Roman JAŠEK. *Possibilities Pricing of the Information System by Providng Insurance against Cyber Risk: International Scientific Conference: Knowledge for Market Use 2016* [online]. Univerzita Palackého, Olomouc, 2016, 8 s. [cit. 2016-10-26]. ISBN 978-80-87533-14-7.

LUKÁŠ, Luděk, Martin HROMADA a Lukáš PAVLÍK.. *The Key Theoretical Models for the Safety and Security Ensuring*. INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN SCIENCES AND INDUSTRY 2016. Chania, Crete: IEEE, 2016, 5 s.

Články ve sborníku konference neevidovaných v databázi SCOPUS, WoS

PAVLÍK, Lukáš a Martin FICEK. *Identifikace aktiv ovlivňujících cenu informačního systému organizace v rámci poskytování pojištění proti kybernetickým hrozbám.* Mezinárodní Konference Bezpečnostní Technologie Systémy a Management. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2017, 6 s. ISBN 978-80-7454-696-9.

PAVLÍK, Lukáš. *Specifikace faktorů ovlivňujících cenu informačního systému v rámci poskytování pojištění proti kybernetickému riziku: XXV. ročník mezinárodní konference Požární ochrana 2016*. Ostrava, 2016, 7 s. ISBN 978-80-7385-177-4. ISSN 1803-1803.

VEČEŘA, Filip a Lukáš PAVLÍK. *Možnost zvyšování odolnosti radiokomunikační sítě PEGAS jako prvku kritické infrastruktury*. Mezinárodní Konference Bezpečnostní Technologie Systémy a Management. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2015, 8 s. ISBN 978-80-7454-559-7

ŠAUR, David a Lukáš PAVLÍK. *Využití programu SFERA pro účely ochrany kritické infrastruktury*. Mezinárodní Konference Bezpečnostní Technologie Systémy a Management. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2015, 7 s. ISBN 978-80-7454-559-7

PROFESNÍ ŽIVOTOPIS AUTORA

Osobní údaje:

Jméno a příjmení, titul:	Ing. Bc. Lukáš Pavlík
Datum narození:	15. 1. 1987
Stav:	svobodný
Adresa:	Třída Tomáše Bati, 1276, 760 01, Zlín
Kontaktní telefon:	724 589 193
E-mail:	lukas.pavlik87@gmail.com

Pracovní zkušenosti, praxe:

Organizace:	Crissis Consulting, s.r.o.
Náplň práce:	zpracovávání povodňových plánů, placená praxe
Doba trvání:	květen 2013 – září 2013
Organizace:	Principal engineering, s.r.o.
Náplň práce:	spolupráce na tvorbě metodických postupů v oblasti analýzy rizik
Doba trvání:	říjen 2016 – září 2018
Organizace:	Moravská vysoká škola Olomouc, o.p.s.
Náplň práce:	odborný asistent – pedagogická a výzkumná činnost
Doba trvání:	září 2017 - současnost

Vzdělání:

Škola:	Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, Zlín

Rok nastoupení a ukončení:	2015- současnost
Obor:	Inženýrská informatika – Inženýrská informatika (Ph.D.)
Škola:	Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, Zlín
Rok nastoupení a ukončení:	2013 - 2015
Obor:	Inženýrská informatika – Bezpečnostní technologie, systémy a management (Ing.)
Škola:	Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a Krizového řízení, Uherské Hradiště
Rok nastoupení a ukončení:	2010 – 2013
Obor:	Procesní inženýrství – Ovládání rizik (Bc.)

Znalosti a dovednosti:

PC:	MS WINDOWS, MS OFFICE, RISKAN, TERREX, INTERNET – úroveň znalostí pokročilá
Významné aktivity:	V roce 2013 absolvování SVOČ na Fakultě logistiky a krizového řízení v oblasti Krizové řízení a ochrana obyvatelstva. Obhájení druhého místa s prací na téma „Analýza rizik obchodu s potravinami ve Zlíně“.
Jazykové znalosti:	Anglický jazyk – pokročilá znalost
	Německý jazyk – základní úroveň
	Ruský jazyk – mírně pokročilý
Řidičský průkaz:	Skupiny B

Vlastnosti a zájmy: Zodpovědnost, spolehlivost, preciznost, komunikativnost, sport.

PŘÍLOHA A: Dotazník

1. Informace o organizaci, která je předmětem dotazníkového šetření	
Název organizace, typ (právní forma) organizace, adresa organizace	
Předmět činnosti	
Počet zaměstnanců	
Roční obrat	
Počet jednotek organizace	

2. Informační systémy organizace			
Otázka	**ANO**	**NE**	**Poznámka**
Uveďte, kolik informačních systémů ve vaší organizaci provozujete.			
Pokud provozujete dva a více informační systémů, jsou tyto systémy od sebe svou funkčností vzájemně separovány?			
Do vyznačených polí uveďte názvy vašich informačních systémů a zakroužkujte počet uživatelů. IS č. 1…….. IS č. 2……. IS č. 3……. IS č. 4……			

3. Datová bezpečnost a obnovitelnost funkce organizace

Otázka
V případě narušení citlivých dat v organizaci jste schopni zajistit její fungování do: *hodiny *12 hodin *24 hodin *48 hodin *5 dnů

Otázka	**ANO**	**NE**	**Poznámka**
Jste seznámeni s legislativou GDPR (General Data Protection Regulation), která vešla v platnost 25. 5. 2018?			
Zpracováváte a shromažďujete v organizaci osobní údaje z oblasti obchodu a marketingu? Pokud ANO, uveďte do pole POZNÁMKA počet datových položek.			
Zpracováváte a shromažďujete v organizaci osobní údaje z oblasti bankovnictví a finančních transakcí? Pokud ANO, uveďte do POZNÁMKA počet datových položek.			
Zpracováváte a shromažďujete v organizaci osobní údaje z oblasti personalistiky? Pokud ANO, uveďte do POZNÁMKA počet datových položek.			
Pokud by došlo k realizaci nejzávažnější kybernetické hrozby, byla by organizace schopna případné finanční škody uhradit z vlastních zdrojů?			

4. Typy kybernetických hrozeb			
Otázka	**ANO**	**NE**	**Poznámka**
Označte prosím, které typy situací (scénářů) by mělo krýt pojištění kybernetických hrozeb.			
1. Útok na informační systém prostřednictvím ransomware.			
2. Úmyslná činnost trestná prováděna hackerem.			
3. Neoprávněný přístup do informačního systému.			
4. Napadení informačního systému prostřednictvím malware.			
5. Únik dat vlivem nedbalosti zaměstnance.			
6. DDoS útok.			
7. Fyzická ztráta nosiče dat (ztráta notebooku).			
8. Ztráta dat a narušení funkce informačního systému organizace vlivem bleskového výboje.			
9. Soudní řízení založené na porušení nařízení o ochraně osobních údajů (GDPR).			
Byla vaše organizace někdy vystavena některému z výše uvedených scénářů kybernetického rizika? Pokud ANO, uveďte konkrétní druh situace (scénáře).			

5. Připravenost organizace v oblasti kybernetické bezpečnosti

Otázka
Označte, která z aktiv organizace považujete za nejzranitelnější vůči kybernetickým hrozbám? *technické komponenty IS *data *know-how organizace *uživatelé IS *programové vybavení *obrat *dobré jméno organizace *zákazníci

Otázka	ANO	NE	Poznámka
Jsou tato aktiva z pohledu kybernetické bezpečnosti podle vás dostatečně chráněna?			
Jsou ve vaší organizaci pravidelně prováděny aktualizace v oblasti informační bezpečnosti? (pravidelné kontroly komponent informačního systému, zálohování dat, aktualizace software, změna hesel, aktualizace dokumentu bezpečnostní politiky apod.)			
Je ve vaší organizaci pověřena osoba pro zajišťování informační bezpečnosti?			
Máte zpřístupněnou službu help-desk pro uživatele v případě realizace kybernetické hrozby?			
Máte zpracován krizový plán (scénář) pro případ realizace kybernetických hrozeb?			

Jsou ve vaší organizaci smluvně ujednány sankce ze strany odběratelů, které mohou být uděleny v případě narušení běžných obchodních služeb?			

6. Rozsah krytí proti kybernetickým hrozbám

Otázka	ANO	NE	Poznámka
Je vaše organizace pojištěna proti kybernetickým hrozbám?			
Pokud ANO, je krytí pojištění kybernetických hrozeb z vašeho pohledu dostačující? Co byste případně změnili?			
Očekávali byste v rámci tohoto pojištění také krytí škod způsobených na hardwaru a softwaru?			
Uvítali byste v rámci tohoto pojištění také krytí škody týkající se poškození dobrého jména organizace?			
Očekávali byste v rámci tohoto pojištění krytí nákladů na obnovení a rekonstrukci dat?			
Měly by být z pojištění kybernetických hrozeb hrazeny také finanční pokuty, které mohou být organizaci uděleny za únik nebo poškození dat?			
Měly by být z pojištění kybernetických hrozeb hrazeny náklady na oznámení ztráty nebo úniku dat příslušnému úřadu?			

Očekávali byste, že bude možné z pojištění kybernetických hrozeb také kompenzovat ušlý obrat organizace?			

PŘÍLOHA B: STANOVISKO K PŘÍPADOVÉ STUDII Č. 1

Odborné stanovisko k Případové studii č. 1

Účel vypracování odborného stanoviska

Předmětem tohoto stanoviska, je ověřit reálnost algoritmu a jeho výsledků, který byl předložen Ing. Lukášem Pavlíkem. Tento algoritmus byl vytvořen v rámci disertační práce Ing. Pavlíka a byl aplikován na naši organizaci a její informační strukturu. Cílem této aplikace je stanovení potenciálních finančních škod, které mohou být způsobeny kybernetickými hrozbami a jejich posouzení našimi pracovníky, kteří zajišťují provoz informačních systémů. Odborné stanoviska k jednotlivým zjištěným výsledkům jsou uvedeny níže.

I. Finanční dopady na hardware

Na základě výsledků, které byly získány aplikací algoritmu a byly porovnávány se skutečným stavem hardwarových zařízení a jejich komponent lze konstatovat, že tyto výsledky jsou shodné se skutečnou hodnotou z 85 %. Možné škody způsobené kybernetickými hrozbami mohou dosáhnout podobných hodnot, nicméně záleží na jejich průběhu a také fázi, ve které jsou detekovány.

II. Finanční dopady na software

V oblasti software byla stanovena jeho finanční škoda na základě nákladů, které by museli být vynaloženy na jeho reinstalaci. V tomto případě předložena finanční částka souhlasí s možnou reálnou situací z 90 %.

III. Finanční dopady v podobě ušlého obratu (příjmu)

V případě ušlého obratu je v naší organizaci uvažována možnost ušlého příjmu, který představuje nepřijaté finanční prostředky od studentů. Jelikož se jedná o soukromou vysokou školu, je příjem studentů jediným zdrojem finančních prostředků, které však vzhledem k právní formě této organizace, nemůže být vykazován jako zisk. Pokud by byla narušena činnost naší organizaci vlivem kybernetické hrozby, lze předpokládat, že během 72 hodin by tato činnost byla obnovena, Důsledkem této situace může dojít ke ztrátě a nepřijímaní finančních prostředků. Tato skutečnost nicméně závisí na průběhu

situace a více faktorech. Získané výsledky, které nám pan Ing. Pavlík předložil, by podle našich odhadů korespondovali s možnou realitou na 70 %.

IV. Pokuty

Na základě aplikace algoritmu, který nám byl předložen, lze také odhadovat finanční částku ve formě pokut, které by mohli být na základě problematiky GDPR uděleny. Pro stanovení pokut je navržena v disertační práci Ing. Pavlíka tabulka, která umožňuje tuto částku stanovit. Vzhledem k tomu, že se jedná spíše o právní záležitost, z našeho pohledu nejsme příliš kompetentní, tuto skutečnost posoudit. Nicméně výše možných pokut byla konzultována s pověřencem pro ochranu osobních údajů a ten rozhodl, že předložená částka by mohla souhlasit z 80 %.

V. Dobré jméno organizace

Problematika stanovení dobrého jména organizace je z našeho pohledu velmi složitou záležitostí. Pan Ing. Pavlík ve své práci předložil návrh stanovení dobrého jména s ohledem na jeho podstatu a charakteristiku. Dobré jméno z našeho pohledu lze definovat různými způsoby, které podle našeho názoru poté určují způsob jeho stanovení a finančního vyjádření. Pan. Ing. Pavlík pojal dobré jméno organizace jedním z možných a logických způsobů, jak tento problém uchopit. Způsob výpočtu a stanovení dobrého jména je založen na reálných ukazatelích. Odhad budoucích škod v této oblasti, které mohou být způsoben kybernetickými hrozbami a jejich dopady je velmi složitý, nicméně podle našich ukazatelů a analýz, jak by tato situace mohla probíhat i s možným vývojem finančních dopadů, lze předložené výsledky, které byly zkoumány našimi odborníky, považovat za reálné z 65 %.

VI. Náklady na rekonstrukci nebo obnovu dat

V případě narušení dat v organizace, jsou z našeho pohledu reálné dva různé scénáře vývoje. V prvním případě může dojít ke ztrátě dat, která již nemohou být obnovena a musí dojít k jejich nové rekonstrukci, tzn. novému sběru. Druhým možným scénářem je v rámci např. napadení IS hackerem, pouze zkopírování dat, kdy data jsou vlastněna také jinou osobou, která k nim nemá žádná oprávnění, nicméně tato data také zůstávají v organizaci. V případě uvažování jejich rekonstrukce je v disertační práci Ing. Pavlíka navržen vzorec, který je založen na ceně za ztracená data na jednu osobu, která je stanovena na základě statistických ukazatelů. Tento krok má z našeho pohledu logickou

souvislost, nicméně je otázkou, jakým způsobem byla cena dat na jednu osobu stanovena a jestli se tato cena nemůže lišit např. podle demografického prostředí. Výpočet, který je navržen na stanovení finanční částky, která by měla být vynaložena na rekonstrukci dat, nicméně považujeme za jednu z možných a správných cest. Podle našich odhadů je tato částka reálná ze 70 %.

VII. Náklady na oznámení ztráty nebo úniku dat

Finanční náklady na oznámení ztráty nebo úniku dat dotčeným orgánům jsou v algoritmu Ing. Pavlíka opět stanoveny na základě sestaveného vzorce a výsledků, které nám byly předloženy lze konstatovat, že výsledná částka by mohla odpovídat realitě ze 70 %. Podle našeho odborného úsudku si nejsme vědomi, že by existoval způsob, jak stanovit tyto náklady v obecné rovině, nicméně navržený způsob Ing. Pavlíka přichází v úvahu jako jedna z možností, jak tuto položku určit.

Stanovení finančních dopadů v případě kybernetické hrozby

Pro stanovení finančních dopadů (v práci Ing. Pavlíka označovaných jako „pojistná hodnota") jsou z našeho pohledu použity standardní metody analýzy rizik, na základě kterých je odvozena finanční škoda (pojistná hodnota) na sledovaných oblastech (označovaných jako „ohrožené prvky"). Navržený algoritmus, jehož součástí jsou výše uvedené postupy lze brát jako logický postup, jak možné finanční dopady kybernetických hrozeb v prostředí organizace stanovit. Z našeho pohledu se jedná o nový postup v této oblasti, který má zcela jistě potenciál uplatnění. Jako návrh ke zlepšení aplikace tohoto algoritmu, bychom doporučili do budoucna ověření na větším množství organizací a zvážení zařazení dalších oblastí, které mohou být dopadem kybernetických hrozeb zasaženy.

Závěr

Naše závěrečné stanovisko je, že tento algoritmus umožňuje stanovit reálnost potenciálních škod na 75 %.

V Olomouci dne: 3. 6. 2019

Ing. Martin Turovský

Vedoucí odboru ICT

PŘÍLOHA C: STANOVISKO K PŘÍPADOVÉ STUDII Č. 2

Odborné stanovisko – Případová studie č. 2

Odborné stanovisko, které je vypracováno na základě výsledků disertační práce pana Ing. Lukáše Pavlíka má především za úkol zhodnotit možnosti a reálnost výsledků, které získal na základě aplikace svého algoritmu v naší organizaci. Pro posouzení adekvátnosti jednotlivých ukazatelů, které by mohly mít vliv na možné finanční škody, způsobené kybernetickými hrozbami, byly použity stanoviska odborníků, kteří se zabývají příslušnými oblastmi. V rámci hodnocení správnosti a uplatnitelnosti získaných výsledků byl také provedeno porovnání se situací, kdy došlo ke kybernetickému útoku v naší organizaci. Při srovnávání s podobnou situací, jaká byla nastíněna v disertační práci pana Ing. Lukáše Pavlíka byly zjištěny následující skutečnosti:

1) Na základě aplikace algoritmu v naší organizaci, bylo dosaženo podobnosti se skutečným stavem přibližně na 70 %.
2) Některé oblasti (např. hardware, software) jsou z našeho pohledu dobře vyčíslitelné. Jiné oblasti (např. dobré jméno, náklady na rekonstrukci a obnovu dat), jsou podle našeho úsudku obtížněji stanovitelné. Pro ověření těchto skutečností byla provedena konzultace s odborníky na ekonomiku a finance v naší organizaci. Podle jejich názoru předložené výsledky odpovídají možným skutečnostem, které by mohli nastat v případě kybernetické hrozby.
3) Ze zhodnocení výsledků, kterých bylo dosaženo na základě aplikace tohoto algoritmu, lze usoudit, že práce pana Ing. Lukáše Pavlíka přináší nový pohled na stanovování finančních dopadů v rámci kybernetických hrozeb. Tuto práci vnímáme jako inovativní a v budoucnu snad i uplatnitelnou v běžné praxi.

Odborný posudek byl vydán na základě žádosti pana Ing. Lukáše Pavlíka a slouží pouze jako součást jeho disertační práce. Tento posudek nesmí být využit k jiným účelům, než k výše uvedenému.

V……Ostravě…… dne…… 6.6. 2014 ……..

……
manažer pro oblast ICT