VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATIC

METODIKA HODNOCENÍ ÚROVNĚ KYBERNETICKÉ BEZPEČNOSTI
METHODOLOGY FOR ASSESSING THE LEVEL OF CYBER SECURITY

TEZE DISERTAČNÍ PRÁCE
DISSERTATION THESIS

AUTOR PRÁCE — **Ing. Lukáš PODEŠVA**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Miloš KOCH, CSc.**
ADVISOR

BRNO 2024

ABSTRAKT

V dnešní digitální éře je zajištění kybernetické bezpečnosti klíčové pro ochranu podnikových aktiv. Přestože existuje mnoho nástrojů, metodik a vědeckých přístupů pro hodnocení kybernetické bezpečnosti, chybí metodika, která by implementovala nejvýznamnější vědecké ekonomické modely a zároveň by zohledňovala velikost organizace a sektor ve kterém působí.

Tento výzkum je zaměřen právě na nalezení takové metodiky, která stanovuje výkon kybernetické bezpečnosti a hodnotí úroveň klíčových vnitřních procesů v oblasti kybernetické bezpečnosti. Součástí je také ekonomický model pro hodnocení návratnosti investic do kybernetické bezpečnosti na základě dosažených výsledků jednotlivých procesů. Výkon kybernetické bezpečnosti využívá tří mikroekonomické charakteristiky firem (roční obrat, počet koncových bodů v síti a počet zaměstnanců v kyberbezpečnosti). Výhodou těchto charakteristik je, že je díky nim možné zohlednit motivaci útočníku.

Navrhovaná metodika byla sestavena na základě rozsáhlé literární rešerše a vstupů od expertů z oboru kybernetické a informační bezpečnosti. Byly definovány nejvýznamnější ekonomické modely a zásadní procesy v oblasti kybernetické bezpečnosti. Váhy používané v rámci navržené metodiky byly stanoveny na základě kvantitativního výzkumu a následně verifikovány odbornými konzultacemi s experty z oboru. Pro validaci celé metodiky byl vytvořen nástroj, který sloužil pro kvalitativní výzkum ve vybraných firmách a simulaci dopadů investic.

Vývoj této metodiky má významný přínos pro oblast kybernetické bezpečnosti tím, že poskytuje spolehlivý nástroj pro hodnocení a srovnání bezpečnostní výkonnosti. Umožňuje organizacím lépe pochopit své bezpečnostní slabiny a posiluje jejich schopnost reagovat na potenciální hrozby. Navíc, díky jeho škálovatelnému a flexibilnímu designu, může být snadno přizpůsoben různým průmyslovým odvětvím a velikostem organizací. Tato metodika je určená především pro malé a střední firmy, které nedisponují významnými prostředky pro investice do oblasti kybernetické bezpečnosti, ale chtějí tuto oblast systematicky řídit.

KLÍČOVÁ SLOVA

kybernetická bezpečnost, informační bezpečnost, výkon kybernetické bezpečnosti, řízení rizik, návratnost investic, Gordon-Loeb, ROSI, výrobní sektor

Obsah

1. Úvod

V současném digitálním věku je kybernetická a informační bezpečnost jeden z nejvýznamnějších aspektů pro všechny organizace, bez ohledu na jejich velikost či obor činnosti, jak ukazuje graf 1.1. Bez správných informací a jejich smysluplného zpracovávání a vyhodnocování si podnikání umíme už jen těžko představit. Již v roce 1993 Peter Drucker prohlásil, že „informace jsou jediným smysluplným zdrojem podnikání a ostatní výrobní faktory (práce, půda, kapitál) jsou až druhořadými“. (Drucker, 1993)

S rychlým technologickým pokrokem a rostoucím počtem zařízení připojených k internetu se kybernetické hrozby stávají stále sofistikovanějšími a nebezpečnějšími. Firmy čelí širokému spektru rizik, od krádeže citlivých dat a finančních podvodů, po útoky na infrastrukturu a narušení provozu. V tomto dynamickém a vysoce rizikovém prostředí je nezbytné, aby organizace měly efektivní nástroje a metody pro hodnocení a zlepšování své kybernetické a informační bezpečnosti. (Lackner et al., 2018)

Na evropské úrovní řeší problematiku kybernetické bezpečnosti uvnitř organizací evropská směrnice NIS 2 (Network and Information Security Directive 2). Do právního prostředí České republiky je směrnice NIS 2 implementována prostřednictvím nového zákona o kybernetické bezpečnosti. Z důvodu rozsahu transponované směrnice dojde k přinejmenším patnáctinásobnému nárůstu regulovaných subjektů, což přinese značné ekonomické a finanční dopady na podnikatelské prostředí v ČR. Nově se tak podle současných odhadů navrhovaná úprava dotkne přibližně 6000 subjektů, z čehož asi 5000 bude regulováno v režimu nižších povinností. Většina těchto subjektů budou střední podniky. (“Závěrečná zpráva z hodnocení dopadů regulace (RIA)”, 2024)

Problematika kybernetické bezpečnosti se také promítá do vědeckého výzkumu. Například Douglas Kelly ve svém článku The Economics of Cybersecurity," pojednává o motivačním dilematu a dalších mikroekonomických principech kybernetické bezpečnosti, které mají pomoci zvýšit úroveň kybernetického průmyslu na společensky optimální. V tomto článku uvádí, že kybernetické útoky stály v roce 2017 podniky celosvětově více než 500 miliard dolarů ročně a zamýšlí nad velmi naléhavou otázkou: Kolik investic do kybernetické bezpečnosti je dostatečné, aby se minimalizovala hrozba úspěšného útoku? (Kelly, 2017)

Jedním z nejvýznamnějších dopadů na tuto oblast z pohledu ekonomie měl však článek "The Economics of Information Security Investment" od Lawrence A. Gordona a Martina P. Loeba, který představuje ekonomický model pro optimalizaci investic do informační bezpečnosti. Gordon-Loebův model analyzuje, jaké množství prostředků by mělo být vynaloženo na ochranu informačních aktiv, aby byly minimalizovány celkové náklady spojené s bezpečnostními incidenty. Autoři demonstrují, že maximální investice do bezpečnosti by neměly přesáhnout přibližně 37 % očekávané ztráty způsobené potenciálním bezpečnostním incidentem. (Gordon & Loeb, 2002)

2. Formulace výzkumného problému a definice mezery ve vědeckém poznání

Literární Rešerše odhalila, že současné modely se zaměřují především na hodnocení jednotlivých informačních aktiv v organizaci, přičemž každé aktivum je hodnoceno samostatně z hlediska rizik a zranitelností. Tato individualizace aktiv je výhodná v kontextu organizací s jasně definovanými a oddělenými systémy, avšak nevýhodná v případech, kdy jsou aktiva a procesy navzájem silně propojené a kde je riziko přenositelné mezi různými částmi organizace.

Kritická analýza současných přístupů ukázala, že existuje nedostatek metodik, které by umožnily holistické hodnocení bezpečnosti firmy jako celku. Zatímco Gordon-Loebův model poskytuje užitečný rámec pro optimalizaci investic do kybernetické bezpečnosti, postrádá

dimenzi, která by zohledňovala procesně orientovaný přístup k hodnocení bezpečnosti napříč celou organizací.

Zároveň je zřejmé, že ve vědecké literatuře chybí propojení ekonomických modelů s praktickými metodami auditu a identifikace zranitelností na úrovni procesů. To znamená, že firmy, které se snaží řídit kybernetickou bezpečnost na úrovni jednotlivých procesů, postrádají integrovaný nástroj, který by jim umožnil jak identifikaci rizik, tak kvantifikaci návratnosti investic do bezpečnostních opatření. Na základě těchto zjištění byla mezera vědeckého poznání definována takto:

„V současné době čelí organizace zvyšujícím se hrozbám v oblasti kybernetické a informační bezpečnosti, přičemž tradiční metody hodnocení bezpečnosti často nezohledňují ekonomické aspekty, které jsou klíčové pro rozhodování na úrovni managementu. Tento nedostatek vede k tomu, že organizace nejsou schopny efektivně hodnotit svou bezpečnostní úroveň a alokovat zdroje tak, aby dosáhly optimální úrovně ochrany při minimálních nákladech.“

Z definovaného výzkumného problému vyplývá návrh nové metodiky, která by efektivně poskytovala organizacím komplexní pohled na jejich úroveň kybernetické a informační bezpečnosti. Nejprve je nezbytné stanovit jasně definovat mezeru vědeckého poznání, která byla definována takto:

Mezera ve vědeckém poznání spočívá v absenci jednotného metodického přístupu, který by kombinoval procesně orientované hodnocení kybernetické bezpečnosti s ekonomickými modely optimalizace investic. Konkrétně, neexistuje metodika, která by umožňovala pohlížet na firmu jako na jedno komplexní aktivum, kde jsou zranitelnosti identifikovány a hodnoceny na úrovni jednotlivých procesů, a zároveň by poskytovala kvantitativní rámec pro hodnocení efektivity bezpečnostních opatření a návratnosti investic v oblasti kybernetické bezpečnosti.

Tato mezera je významná z několika důvodů:

1. **Nedostatečné pokrytí propojených rizik**: Současné metody často ignorují skutečnost, že rizika plynoucí z hrozeb se část vážou k několika aktivů současně a spíše, než na aktiva je efektivnější se soustředit na procesy, které reflektují různé vektory útoku.
2. **Omezená schopnost kvantifikovat návratnost investic na úrovni procesů**: Ačkoli existují modely pro výpočet ROSI, nejsou běžně aplikovány na úrovni procesů, což brání firmám v efektivní alokaci zdrojů na opatření s nejvyšším dopadem.
3. **Chybějící praktické nástroje pro malé a středně velké firmy**: Většina existujících modelů je buď příliš obecná, nebo příliš složitá pro praktické použití v menších organizacích, které nemají rozsáhlé bezpečnostní týmy nebo pokročilé analytické kapacity.

3. Cíle výzkumu a výzkumné otázky

Na základě jasně definované mezery vědeckého poznání byly definován hlavní cíl, dílčí cíle a relevantní výzkumné otázky. Tyto cíle a otázky pomohly zaměřit výzkum a zajistit, že výsledná metodika bude plně odpovídat potřebám a výzvám, kterým čelí moderní organizace v oblasti kybernetické bezpečnosti.

<u>Hlavní cíl</u>

Navrhnout komplexní metodiku pro hodnocení úrovně kybernetické bezpečnosti v organizacích, která integruje nejnovější vědecké poznatky a nejlepší praxe v oblasti kybernetické bezpečnosti, která bude efektivně identifikovat a řešit slabá místa v procesech řízení kybernetické bezpečnosti.

Vedlejší cíle

Stanovení vedlejších cílů v rámci výzkumu pomáhá rozdělit hlavní cíl na menší, konkrétnější úkoly, které jsou snáze zvládnutelné a měřitelné. Zde jsou uvedeny vedlejší cíle pro návrh nové metodiky:

1. ***Rešerše existujících metodik:*** Provést důkladnou analýzu a syntézu stávajících metodik hodnocení kybernetické bezpečnosti, včetně mezinárodních standardů a průmyslových praxí, aby byly identifikovány jejich silné a slabé stránky.
2. ***Identifikace klíčových bezpečnostních procesů:*** Definovat klíčové procesy kybernetické bezpečnosti, které jsou kritické pro hodnocení a ochranu informačních systémů
3. ***Návrh nové metodiky:*** Vyvinout novou metodiku, která zahrnuje jak kvantitativní, tak kvalitativní hodnotící nástroje a metody, a která je dostatečně flexibilní, aby umožnila přizpůsobení specifickým potřebám různých organizací.
4. ***Validace metodiky:*** Ověřit účinnost navrhované metodiky pro vybraný typ organizací (sektor) a srovnat výsledky s existujícími metodikami

Výzkumné otázky

Výzkumné otázky hrají klíčovou roli v každém výzkumném projektu a pomáhají přesně vymezit, na co se výzkum zaměřuje. Přestože cíl výzkumu poskytuje obecný směr, výzkumné otázky jdou do větší hloubky a specifikují konkrétní aspekty problému, které budou zkoumány. V rámci tohoto výzkumu jsou výzkumné otázky definovány takto:

1. ***Jak metodologicky postupovat při návrhu nové metodiky, tak aby byla validní splnila stanovený cíl?***
2. ***Jaké jsou nejvýznamnější vědecké ekonomické modely a přístupy v oblasti kybernetické bezpečnosti, které budou reflektovat aktuální stav vědeckého poznaní v navrhované metodice?***
3. ***Jaké jsou klíčové bezpečnostní procesy, které by měly být zahrnuty do metodiky, aby adekvátně pokryla všechny aspekty kybernetické a informační bezpečnosti v organizaci?***
4. ***Jaká je mezera ve vědeckém poznání, která bude reflektována v rámci navrhované metodiky?***
5. ***Jaké váhové modely by měl být použity pro hodnocení významu jednotlivých domén a metrik v rámci celkového metodiky?***
6. ***Jakým způsobem bude prezentována úroveň kvality kybernetické bezpečnosti?***
7. ***Jaké specifické ukazatele by měly být využity pro objektivní posouzení celkového kontextu organizace ve vztahu ke kybernetické bezpečnosti?***
8. ***Je navržená metodika vhodná pro využití v praxi a dává relevantní výstupy?***
9. ***Jaké jsou potenciální výzvy a omezení při implementaci a používání metodiky a jak mohou být tyto problémy řešeny?***

Tyto cíle a otázky jsou základem pro vývoj ucelené a efektivní metodiky, která pomůže organizacím lépe rozumět a řídit svá kybernetická rizika.

4. Popis metodiky hodnocení úrovně kybernetické bezpečnosti

V této práci je kybernetická bezpečnost pojata jako dynamický střet mezi dvěma protichůdnými silami, motivací útočníků a schopností organizací čelit těmto hrozbám. Toto chápání zdůrazňuje, že bezpečnostní opatření a strategie nejsou statické, ale vyvíjejí se v reakci na neustále se měnící taktiky a techniky útočníků. Tento přístup podtrhuje nutnost organizací nejen reagovat na bezprostřední hrozby, ale také aktivně rozvíjet svou obranyschopnost v předvídavý a adaptivní způsob, který zohledňuje jak současné, tak budoucí bezpečnostní výzvy.

Z uvedeného pojetí kybernetické bezpečnosti jako neustálého střetu mezi motivací útočníků a obranyschopností organizací vyplývá kritický význam pravidelných auditů a hodnocení úrovně kybernetické a informační bezpečnosti. Tyto aktivity jsou nezbytné pro udržení kroku s rychlým vývojem a sofistikovaností kybernetických hrozeb. Audity a hodnocení umožňují organizacím systematicky revidovat a posilovat své bezpečnostní strategie, identifikovat slabiny v obraně a implementovat potřebná zlepšení. Tímto způsobem mohou organizace proaktivně reagovat na změny v tomto rizikovém prostředí a zajistit, že jejich obranné mechanismy jsou vždy aktuální a efektivní.

Efektivní auditní procesy a pravidelné hodnocení nejenže pomáhá minimalizovat rizika kybernetických útoků, ale také podporuje vytváření důvěry u zákazníků a partnerů tím, že demonstrují závazek organizace k vysokým standardům bezpečnosti. Pravidelné hodnocení v této oblasti je základním předpoklad pro udržení kontinuity činnosti, minimalizace právních a finančních rizik a zachování dobré pověsti firmy v digitálně propojeném světě.

Navrhovaná metodika pro hodnocení kybernetické bezpečnosti firem představuje inovativní přístup k řešení tohoto problému. Cílem této metodiky je poskytnout malým a středně velkým firmám ucelený nástroj, který umožní systematicky hodnotit různé aspekty jejich bezpečnosti, identifikovat slabá místa, navrhnout konkrétní kroky pro zlepšení a určit návratnost těchto investic.

Metodika definuje klíčové procesy kybernetické bezpečnosti jako jsou například inventarizace a kontrola hardwarových aktiv, nebo správa síťové infrastruktury. U každého takto definovaného procesu se měří procentuální shoda s nejlepšími praktikami, přičemž celkové skóre, nazvané jako ***Výkon kybernetické bezpečnosti***, je průměrnou hodnotou všech těchto procesů a teoreticky může nabývat hodnot od 0 do 100. Toto skóre poskytuje celkový pohled na úroveň kybernetické a informační bezpečnosti organizace. Výsledky mohou být prezentovány vedení společnosti spolu s interpretací, která vysvětluje význam skóre v kontextu dané organizace. Na základě těchto výsledků jsou formulovány doporučení pro zlepšení.

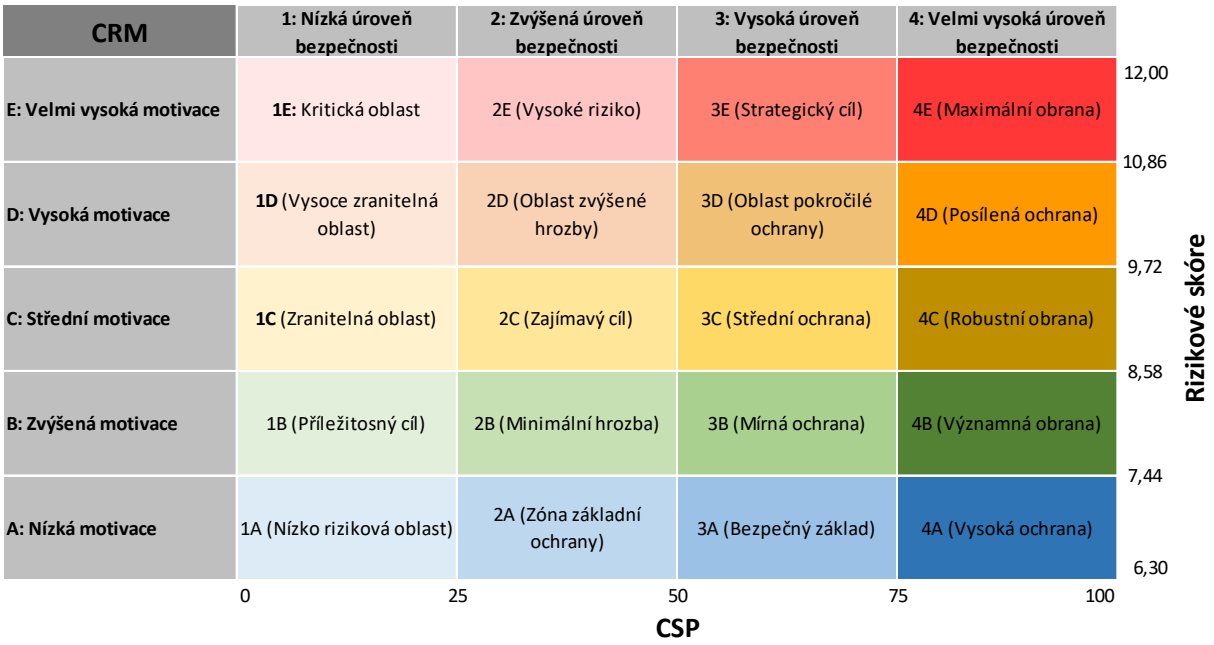
Součástí této metodiky je také ekonomický model, který vychází z modelu navrženého Gordonem a Loebem (Gordo, Loeb, 2002) a návratnosti investic do kybernetické bezpečnosti ROSI (Davis, 2005). Každý proces má proto přiřazenou váhu podle vlivu na aktuálně definované hrozby. Každá hrozba má potom definovaný dopad a pravděpodobnost výskytu. V rámci této metodiky je na firmu, nebo organizaci pohlíženo jako na jedno aktivum. To umožňuje kvantifikovat a hodnotit účinnost (návratnost) implementovaných bezpečnostních opatření proti každé definovaní hrozbě.

Kromě výkonu kybernetické bezpečnosti je každá organizace hodnocena podle dalších výkonnostních metrik, které vychází ze tří základních mikroekonomických veličin v oblasti kybernetické bezpečnosti (roční obrat, počet koncových bodů v síti a počet úvazků pracovníku kyberbezpečnosti):

- ***Technologická efektivita****:* měří, jak efektivně firma využívá svou síťovou infrastrukturu ke generování obratu, což poskytuje přehled o tom, jak technologie přispívají k finančnímu výkonu společnosti.
- ***Produktivita kyberbezpečnosti****:* udává, kolik obratu generuje firma na jednoho zaměstnance v oblasti kybernetické bezpečnosti, což odráží finanční efektivitu a výkonnost týmu zabezpečení.
- ***Intenzita kybernetické zátěže****:* vypočítává, kolik koncových bodů v síti připadá na jednoho zaměstnance kybernetické bezpečnosti, čímž poskytuje ukazatel pracovní zátěže a kapacitního vytížení personálu v kybernetické bezpečnosti.

Nakonec byla, na základě empirických zjištění z dotazníkového šetření, navržena Matice kybernetického rizika uvedená na obrázku č. 1. Tato matice poskytuje podrobný pohled na

rizikové profily různých organizací na základě úrovně jejich kybernetické bezpečnosti a motivace útočníků. Umožňuje organizacím lépe pochopit jejich rizikovou pozici a efektivně plánovat a implementovat bezpečnostní opatření. Mapa poskytuje firmě pohled na to, kde se vzhledem k riziku kybernetického útoku a úrovně vnitřních zabezpečovacích procesů nachází v rámci sektoru, ve kterém podniká.



Obrázek 1: Matice kybernetického rizika

Společně tyto metriky poskytují ucelený pohled na prostředí kybernetické a informační bezpečnosti organizace a umožňují lepší porozumění a řízení kybernetické bezpečnosti.

V kontextu současného kybernetického prostředí je nezbytné mít komplexní a agilní nástroje pro hodnocení bezpečnosti, které jsou schopny reagovat na nové hrozby a výzvy. Navrhovaná metodika poskytuje organizacím nejen kvantitativní hodnocení jejich bezpečnostní úrovně, ale také doporučení pro zlepšení. Tento přístup umožňuje firmám lépe porozumět jejich aktuálnímu stavu bezpečnosti a efektivněji řídit rizika ve vztahu ke konkrétním hrozbám. V konečném důsledku přispívá k posílení celkové odolnosti organizací vůči kybernetickým útokům a zvyšuje jejich schopnost rychle a účinně reagovat na bezpečnostní incidenty.

5. Metodologie výzkumu

Tento výzkum lze charakterizovat jako empirický aplikovaný výzkum s přesně stanoveným cílem vývoje a správného nastavení nové metodiky včetně její validace v oblasti hodnocení úrovně kybernetické bezpečnosti. Základem byla klasifikace a analýza dané oblasti a následné hledání příčinných souvislostí. Zde jsou hlavní charakteristiky tohoto výzkumu:

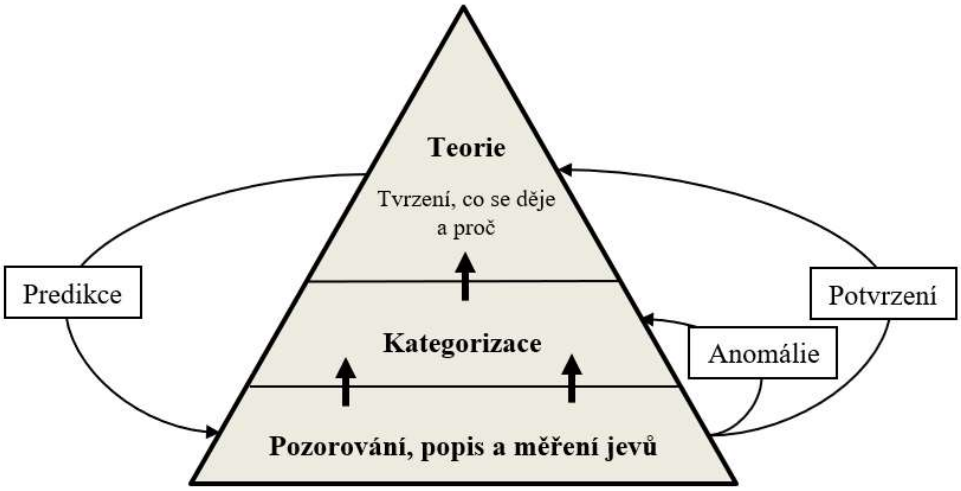
- **Aplikovaný výzkum:** Cílem je vyvinout prakticky použitelnou metodiku pro hodnocení kybernetické bezpečnosti malých a středně velkých firem. Aplikovaný výzkum se zaměřuje na řešení konkrétních problémů s přímým využitím v praxi, což přesně odpovídá záměru vytvořit ucelený nástroj pro zlepšení kybernetické bezpečnosti organizací.
- **Metodologický výzkum:** Výzkum je zaměřen na vývoj nové metodiky, což zahrnuje návrh, implementaci a validaci systému hodnocení. Tento typ výzkumu se často zaměřuje na vytvoření nových nástrojů, postupů nebo modelů, které lze aplikovat v konkrétních situacích nebo oborech.
- **Kombinace kvantitativního a kvalitativního přístupu:** Výzkum kombinuje kvantitativní analýzy (např. výpočet Výkonu kybernetické bezpečnosti, analýza

ekonomických modelů) s kvalitativním výzkumem (např. expertní rozhovory, validace na základě zpětné vazby od pracovníků kybernetické bezpečnosti). Tento smíšený přístup umožňuje hloubkovou analýzu a porozumění jak numerickým údajům, tak kvalitativním aspektům bezpečnosti.

- **Deskriptivní a explorativní výzkum:** Výzkum je deskriptivní v tom smyslu, že popisuje a měří úroveň kybernetické bezpečnosti v organizacích pomocí nově vyvinutého nástroje. Zároveň má explorativní povahu, protože zkoumá nové přístupy a integruje ekonomické modely a nejlepší praktiky, což je inovativní krok v oblasti kybernetické bezpečnosti.
- **Empirický výzkum:** Výzkum je empirický, jelikož se opírá o data získaná z reálného prostředí (např. sekundární data, simulace, zpětná vazba z řízených rozhovorů). Empirické přístupy jsou klíčové pro validaci nových metodik a jejich praktickou aplikovatelnost.

Na hledání nové metodiky můžeme pohlížet jako na hledání nové teorie v oblasti ekonomie a managmentu. Teorii můžeme popsat jako možné tvrzení o tom, co se děje. Výzkum v této oblasti (ekonomie a managementu) probíhá obvykle ve 3 krocích, tak jak to popsal prof. Molnár s kolektivem v díle „Pokročilé metody vědecké práce". (Molnár, 2012)

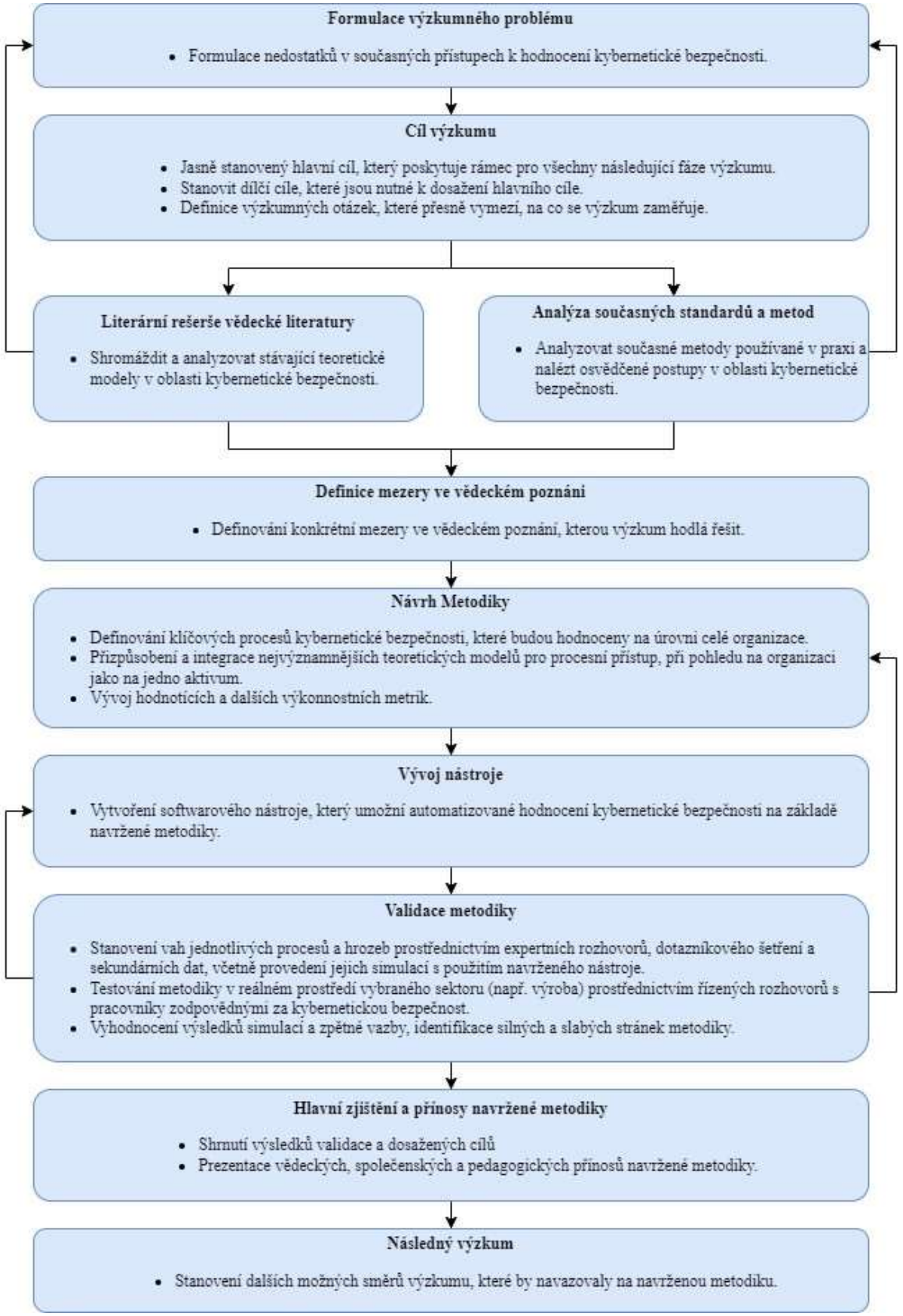
1. **Pečlivé pozorování popisování a měření toho co se děje** – sledované situace (které jsou někdy náhodně vytvořené) se popisují jednoduchými pojmy a dokumentují se.
2. **Seskupení výsledků do kategorií** – Jednotlivé kategorie se liší svými atributy a je hledáno vysvětlení, jak určitá množina atributů vede k určitým výsledkům.
3. **Vytvoření teorie** – nejprve se ovšem bude jednat pouze o počáteční teorii.
4. Tento postup je vlastně založen na principu indukce a po vytvoření výchozí teorie je potřeba se vrátit na spodek pyramidy, jak je znázorněno na obrázku 2. Teorie se využije k predikci jevů, které mohou nastat v různých situacích.



Obrázek 2.: Pyramida tvorby teorie v ekonomii a managementu (Molnár, 2012)

Následně bylo vytvořeno konceptuální schéma výzkumu, které znázorňuje hlavní komponenty výzkumného procesu a vztahy mezi nimi. Toto schéma zahrnuje klíčové fáze výzkumu, jako jsou formulace výzkumného problému, stanovení cílů, výběr metodologie, sběr a analýza dat, a interpretace výsledků.

Konceptuální schéma výzkumu pro vývoj a validaci nové metodiky hodnocení kybernetické bezpečnosti firem lze znázornit jako diagram, který ukazuje hlavní fáze výzkumu a jejich vzájemné vztahy. Na obrázku 3 jsou jasně znázorněné jednotlivé kroky a komponenty výzkumu, které přispívají k dosažení hlavního cíle.



Obrázek 3: Konceptuální schéma vědeckého výzkumu

Zde jsou popsány jednotlivé kroky vývoje, které popisují, jak bylo k vývoji a validaci nové metodiky přistupováno:

1. Analýza stávajících modelů a nejlepších praktik

Prvním krokem ve vývoji metodiky je důkladná literární rešerše zaměřená na stávající ekonomické modely a nejlepší praktiky v oblasti hodnocení kybernetické bezpečnosti. Cílem této fáze je identifikovat klíčové ekonomické modely a další důležité prvky, které lze přizpůsobit a integrovat do nové metodiky, která by efektivně sloužila potřebám malých a středně velkých firem. Hlavním výstupem je tedy identifikace klíčových prvků a mezer ve vědeckém poznání, které budou začleněny do nové metodiky.

2. Návrh procesně orientovaného přístupu

Na základě formulovaného výzkumného problému navrhnout metodiku jako procesně orientovaný přístup, kde je na celou firmu pohlíženo jako na jedno komplexní aktivum, tak aby umožňoval systematicky identifikovat zranitelnosti v klíčových procesech kybernetické bezpečnosti, jako jsou inventarizace a kontrola hardwarových aktiv nebo správa síťové infrastruktury. Každý proces se následně ohodnotí procentuální shodou s nejlepšími praktikami, což umožní vytvořit celkové skóre nazvané Výkon kybernetické bezpečnosti.

3. Integrace ekonomického modelu

Rozšíření metodiky o nejvýznamnější ověřené ekonomické modely, tak aby nová metodika umožňovala kvantifikovat účinnost implementovaných bezpečnostních opatření na základě definovaných hrozeb, jejich dopadu a pravděpodobnosti výskytu. Každému procesu se přiřadí váha podle jeho vlivu na celkovou bezpečnostní úroveň organizace, což umožní efektivní alokaci zdrojů.

4. Návrh klíčových hodnotících metrik

Stanovení výkonnostních metrik, které budou vycházet ze základních mikroekonomických ukazatelů hodnocených firem a organizací, tak aby bylo celkové hodnocení firmy zasadit do širšího kontextu a aby tyto metriky bylo možné využít pro benchmarking.

5. Vývoj nástroje pro validaci metodiky

Návrh softwarového nástroje pro testování a validaci navržené metodiky, tak aby umožňoval automatizované hodnocení jednotlivých procesů na základě definovaných kritérií a metrik, což umožní rychlou a efektivní analýzu úrovně kybernetické bezpečnosti v organizaci.

6. Stanovení a vah a příprava simulací

Stanovení vah pro jednotlivé procesy a hrozby na základě expertních rozhovorů, dotazníkového šetření a analýzy sekundárních dat. Tyto váhy se následně implementují do softwarového nástroje, který se použije k provádění simulací bezpečnostních scénářů.

7. Kvalitativní validace

Testována a validace ve vybraných výrobních firmách (dle klasifikace CZ-NACE se jedná o označení C), prostřednictvím řízených rozhovorů s pracovníky zodpovědnými za oblast kybernetické bezpečnosti. Cílem bude získání zpětné vazby ohledně funkčnosti, praktické využitelnosti a účinnosti navržené metodiky, včetně porovnání výsledků této metodiky s aktuálně používanými metodikami v těchto organizacích.

6. Interpretace a diskuze výsledků

Interpretace výsledků navrhované metodiky hodnocení úrovně kybernetické bezpečnosti, je prezentována pomocí výstupů simulovaných na fiktivní firmě. Tato simulace proběhla v softwarovém nástroji navrženém na základě této metodiky, který byl zároveň použit pro její validaci ve vybraných firmách.

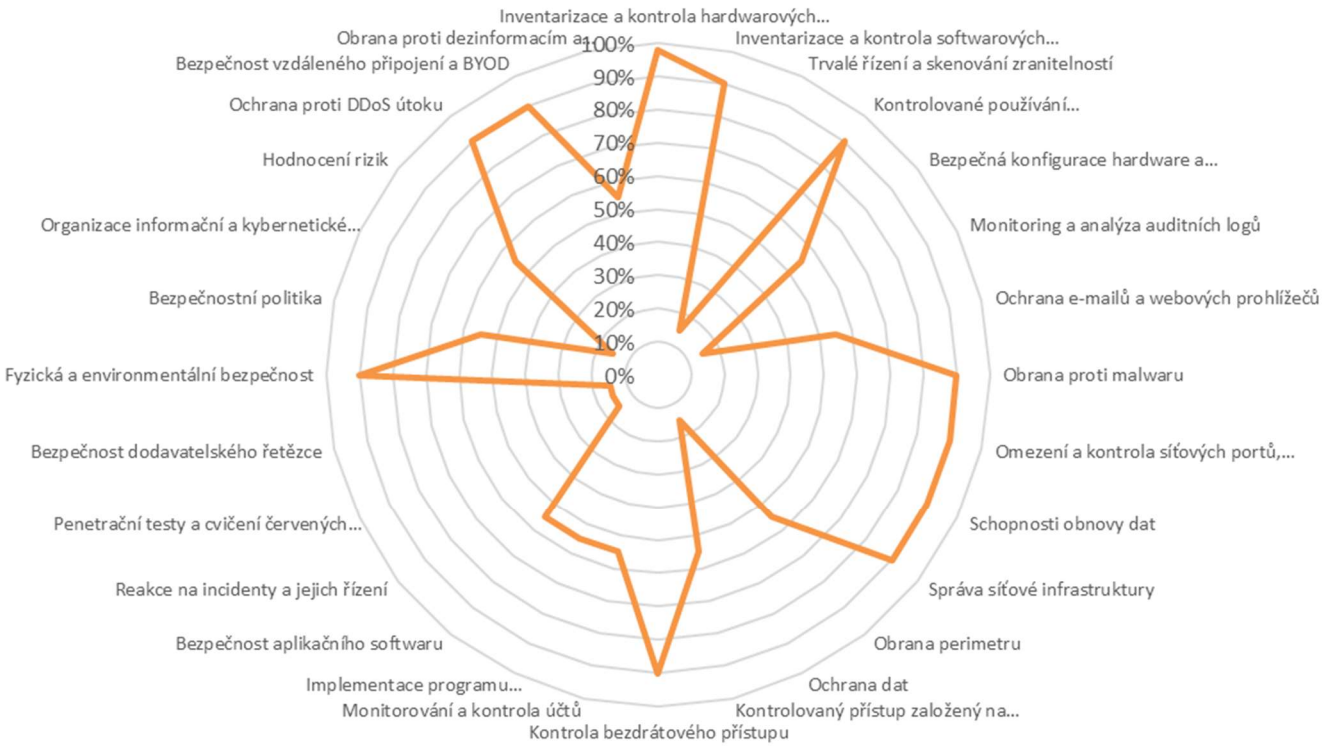
Navržená metodika má dvě úrovně, nejprve proběhne zjištění skutečného stavu a poté může proběhnout posouzení návratnosti investice do určitého procesu.

Vstupní parametry fiktivní firmy pro simulaci:

- Sektor: Výroba
- Roční obrat: 4000000 €
- Počet koncových bodu v síti: 300 ks
- Počet úvazků v kybernetické bezpečnosti: 0,2 (Tato forma má pouze jedno zaměstnance oddělení IT, jehož pracovní náplní je z 20 % kybernetická bezpečnost)

V rámci simulace dosáhla fiktivní firma úrovně kybernetického výkonu **59,4 %**.

Grafické znázornění úrovně jednotlivých vnitřních procesů dodává celkový pohled na kybernetickou bezpečnost hodnocené firmy (graf 1). Velmi jednoduchým způsobem lze identifikovat kritické procesy.



Graf 1: Grafické znázornění úrovně vnitřních procesů

Pro lepší pochopení celé problematiky jsou všechny procesy rozděleny do pěti hlavních kategorií, podle jejich funkce vzhledem ke kybernetické bezpečnosti. U těchto kategorií je také uveden jejich stručný popis pro lepší srozumitelnost výsledků (tabulka 1).

Tabulka 1: Dosažená úroveň výkonu jednotlivých funkcí vnitřních procesů

Typ	Popis	Index
Identifikace:	Tato funkce se zaměřuje na pochopení podnikových prostředí, identifikaci aktiv, rizik a bezpečnostních požadavků. Organizace musí rozpoznat, co potřebuje chránit, jaké hrozby na ni číhají a jaké jsou její zákonné povinnosti.	**65%**
Ochrana:	Tato funkce zahrnuje opatření a kontroly, které minimalizují nebo eliminují rizika identifikovaná v rámci funkce „Identifikace“. Cílem je zajistit ochranu kritických služeb a systémů před hrozbami.	**62%**
Detekce:	Tato funkce se zaměřuje na včasné detekování bezpečnostních incidentů. Organizace musí mít schopnost včas odhalit kybernetické útoky nebo narušení.	**44%**
Reakce:	Tato funkce zahrnuje kroky a procesy pro efektivní reakci na kybernetické incidenty. Organizace by měly mít plány a procesy pro řízení a zmírňování dopadů incidentů.	**15%**
Obnova:	Tato funkce se zaměřuje na obnovení běžných operací po kybernetickém incidentu. Organizace musí mít plány a postupy pro rychlé zotavení po bezpečnostním incidentu.	**90%**

Z výše uvedených výstupů leze konstatovat, že firma spoléhá především na zálohy a obnovu systému, kterou pravidelně testuje. Kompletně jí však chybí plán reakce na incidenty (případně plán kontinuity činnosti), což může být zásadní problém při obnově dat při skutečném kybernetickém útoku.

Záleží však vždy na vedení společnosti, jak si dané výsledky interpretuje a vyhodnotí vliv těchto procesů a jejich funkci na bezproblémový provoz společnosti. V tomto rozhodování ji můžou pomoci další výstupy z této metodiky:

- Rizikové skóre RSMA: 9,08
- Pravděpodobnost útoku: 71 %
- Oblast matice kybernetického rizika: 3C (obrázek 1)

Ekonomické zhodnocení kybernetické bezpečnosti pomáhá firmám kvantifikovat riziko ztráty a očekávanou potenciální ztrátu pro jednotlivé hrozby, tyto hodnoty jsou uvedeny v tabulce 2. To firmě umožní zaměřit se na procesy které souvisí s hrozbami, které mají nejvyšší očekávanou ztrátu.

Tabulka 2: Ekonomická analýza současného stavu

Aqnalýza současného stavu	Očekávaná max. ztráta	Pravděpodobnost hrozby	Zranitelnost vůči hrozbě	Rizko ztráty	Očekávaná ztráta
Ransomware	800 000 €	19,56%	36,18%	7,08%	56 614 €
Malware	400 000 €	3,32%	36,18%	1,20%	4 812 €
Sociální inženýrství	40 000 €	5,17%	52,80%	2,73%	1 092 €
Hrozby proti datům	40 000 €	6,55%	41,46%	2,72%	1 086 €
Hrozby proti dostupnosti služeb	40 000 €	4,28%	45,59%	1,95%	780 €
Webové hrozby	4 000 €	1,25%	52,37%	0,66%	26 €
Manipulace a dezinformace	4 000 €	0,00%	53,40%	0,00%	0 €
Útok na dodavatelský řetězec	40 000 €	6,27%	45,41%	2,85%	1 139 €
Zero-Day zranitelnosti	400 000 €	24,59%	46,80%	11,51%	46 034 €
Celkem	1 768 000 €				111 584 €

Z tabulky 2 plyne, že nejvyšší očekávaná ztráta hrozí v případě Ransomwaru a Zero-day zranitelnosti. Procesy s největším dopadem na mitigaci rizik spojených s těmito hrozbami jsou:

- Trvalé řízení a skenování zranitelností
- Reakce na incidenty a jejich řízení
- Monitoring a analýza auditních logů

Vzhledem k vysoké očekávané ztrátě u Ransomware a Zero-day zranitelnosti a výsledků z měření úrovně kvality jednotlivých procesů (graf 2) a jejich funkce (tabulka 1), byly proces Reakce na incidenty a jejich řízení vyhodnocen jako nejkritičtěji. Firma se rozhodla investovat do vytvoření plánu řízení incidentů v oblasti kybernetických hrozeb. Protože s tímto fiktivní firma nemá zkušenosti, rozhodlo se vedení společnosti oslovit externí firmu, která jim tyto procesy nastaví.

Posouzení návratnosti investice

Cenová nabídka externí firmy na vytvoření plánu řízení incidentů a v oblasti kybernetických hrozeb je 2000 €. K tomu je potřeba připočíst další investice, která s implantací tohoto plánu souvisí (úprava vnitřních směrnic, procesů a školení zaměstnanců), toto bylo odhadnuto na dalších 1000 €. Celková investice fiktivní firmy do procesu Reakce na incidenty a jejich řízení je tedy 3000 €.

V části ekonomického posouzení návratnosti investic je uveden vliv této investice na klíčové ukazatele.

Zvýšení Kybernetického výkonu z **59,4 %** na **60,46 %**, tedy zlepšení o **1,43 %**

Tabulka 3: Posouzení investice do vybraného procesu

Vliv investic na jednotlivé hrozby	Iinvestice na hrozbu	Snížení zranitelnosti	Zranitelnost vůči hrozbě	Rizko ztráty	Očekávaný Přínos	Čistý očekávaný přínos
Ransomware	214 €	2,00%	34,18%	6,69%	3 130 €	2 915 €
Malware	214 €	2,00%	34,18%	1,14%	266 €	52 €
Sociální inženýrství	429 €	4,00%	48,80%	2,52%	83 €	-346 €
Hrozby proti datům	171 €	1,60%	39,86%	2,61%	42 €	-130 €
Hrozby proti dostupnosti služeb	514 €	4,80%	40,79%	1,75%	82 €	-432 €
Webové hrozby	429 €	4,00%	48,37%	0,61%	2 €	-427 €
Manipulace a dezinformace	343 €	3,20%	50,20%	0,00%	0 €	-343 €
Útok na dodavatelský řetězec	343 €	3,20%	42,21%	2,65%	80 €	-263 €
Zero-Day zranitelnosti	343 €	3,20%	43,60%	10,72%	3 148 €	2 805 €
Celkem	**3 000 €**				**6 832 €**	**3 832 €**

Investice se podle tabulky 3 rozpočítá na jednotlivé hrozby, podle toho, jaký má vybraný proces vliv na tyto hrozby, to je uvedeno. V tabulce 3 je dále uvedeno procentuální snížení zranitelnost procesů proti všem hrozbám a nová úroveň zranitelnosti procesů v procentech.

Z tabulky 3 také vyplývá, že investice má pro kritické hrozby (Ransomware a Zero-Day zranitelnosti) vysoký očekávaný přínos (sloupec: očekávaný přínos) i čistý očekávaný přínos ENBIC (sloupec: čistý očekávaný přínos). Přestože u ostatních hrozeb je tento přínos spíše záporný. To znamená, že vzhledem k očekávané ztrátě způsobené těmito hrozbami tato investice není efektivní. Celkový součet všech jednotlivých čistých očekávaných přínosů je však kladný a dosahuje 3832 €, což vyjadřuje čistou peněžní ztrátu způsobenou kybernetickými hrozbami, které investice do procesu Reakce na incidenty a jejich řízení zabránila.

Tento ekonomický model je odvozen z modelu Gordon-Loeb (Gordon & Loeb, 2002), který v případě kladného Čistého očekávaného přínosu doporučuje investici realizovat. Zároveň tento model uvádí, že maximální částka investice do kybernetické bezpečnosti ve sledovaném období (rok) nemá překročit 37 % celkové očekávané ztráty (tabulka 2). Optimální investice za období (rok) by tedy neměla překročit: 41286 €.

Stanovení návratnosti investice do kybernetické bezpečnosti na základě navrženého ekonomického modelu, který je dovozený z modelu Return On Security Investment (Davis, 2005), udává návratnost investice **1,3**. Protože návratnost kladné číslo, investice přináší pozitivní návratnost, a tudíž se vyplatí.

Na základě zkušeností z praktického testování ve vybraných firmách, je čas potřebný na analýzu současného stavu a posouzení investice přibližně 1,5 hodiny. To vychází z předpokladu, že známe velikost investice a nemusí se například čekat na cenovou nabídku.

Validace výzkumné metody pro hodnocení úrovně kybernetické bezpečnosti probíhala prostřednictvím strukturovaných rozhovorů s pracovníky zodpovědnými za kybernetickou bezpečnost, během nichž byly položeny předem definované otázky rozdělené do pěti tematický oblastí:

- Aplikovatelnost metodiky
- Důvěra v metodiku a přesnost výsledků
- Srovnání výstupů s používanými metodikami
- Identifikace silných a slabých stránek metodiky

Pro zajištění důvěryhodnosti a relevance výsledků byla metodika nejprve otestována ve vybrané firmě a její výstupy byly následně porovnány s výsledky, které firma dosahuje pomocí vlastních, zavedených metod hodnocení kybernetické bezpečnosti. Tento přístup umožnil nejen ověřit přesnost a praktickou použitelnost nové metodiky, ale také identifikovat její potenciální výhody nebo nedostatky ve srovnání s existujícími postupy.

Významným aspektem tohoto výzkumu byla problematika získávání dat v oblasti kybernetické bezpečnosti. Firmy často nechtějí sdílet citlivé informace o svých bezpečnostních opatřeních a rizicích, což představuje významnou překážku při validaci nových metodik. Tato neochota je většinou motivována obavami o ochranu obchodního tajemství a minimalizaci rizik spojených s potenciálním únikem citlivých dat. V tomto kontextu bylo klíčové vybudovat důvěru mezi zástupci vybraných firem, aby bylo možné získat nezbytná data pro validaci a zároveň respektovat potřebu zachování důvěrnosti informací. Jedním z požadavků byla naprostá anonymita a možnost zveřejnit pouze odpovědi na validační otázky. Výsledky získané praktickým použitím této metodiky v jednotlivých firmách proto v práci uvedeny nejsou.

Pro analýzu byla použita takzvaná tematická analýza, která je jednou z nejčastěji používaných metod obsahové analýzy. Tento přístup zahrnuje identifikaci a analýzu hlavních témat (tematických oblastí) v odpovědích, které byly následně kategorizovány a porovnány napříč třemi firmami. Výsledkem je strukturovaný přehled, který umožňuje vyhodnotit hlavní tendence, shody a rozdíly mezi firmami v každé tematické oblasti. (Hendl, 2023)

Aplikovatelnost metodiky

Tento tematický okruh zkoumá, jak snadno mohou firmy implementovat novou metodiku ve svém prostředí a jaké jsou její časové a zdrojové nároky.

- ***Analýza:*** Metodika byla obecně hodnocena jako aplikovatelná ve všech firmách, avšak její aplikovatelnost byla velmi ovlivněná vyvinutým softwarovým nástrojem a kvalitou definovaných odpovědí jednotlivých otázek. Všechny firmy se shodly, že hodnocení bylo přizpůsobeno konkrétním specifikům jejich firmy.
- ***Závěr:*** Aplikovatelnost metodiky je vysoká, avšak úspěšnost její implementace závisí na kvalitě softwarového nástroje.

Důvěra v metodiku a přesnost výsledků

Tento okruh se snaží zjistit, do jaké míry firmy důvěřují výsledkům získaným pomocí nové metodiky a zda považují její výstupy za přesné a spolehlivé.

- ***Analýza:*** Ve všech firmách byla důvěra ve výsledky metodiky vysoká. Firmy ocenily, že metodika poskytla detailní analýzu, která odpovídala reálnému stavu, což zvýšilo jejich důvěru v použité postupy a výstupy. Všechny firmy považují za vhodnou pro dlouhodobé využití.
- ***Závěr:*** Metodika je vnímána jako důvěryhodný a přesný nástroj pro hodnocení kybernetické bezpečnosti, přičemž její výsledky jsou považovány za reálné a spolehlivé.

Srovnání výstupů s používanými metodikami

Cílem je porovnat výsledky nové metodiky s výstupy stávajících metod hodnocení kybernetické bezpečnosti, aby se zjistilo, zda přináší nové poznatky, nebo potvrzuje existující závěry.

- ***Analýza:*** Ve všech třech firmách metodika odhalila hlavní rizika, které byly identifikovány pomocí stávajících metod. Firmy A a B dokonce uvedly, že metodika poskytuje lepší výsledky než jejich současné postupy.
- ***Závěr:*** Metodika je schopna identifikovat rizika spojené s jednotlivými hrozbami. V některých případech dokonce lépe než stávajícími postupy, což zvyšuje její hodnotu při hodnocení kybernetické bezpečnosti.

Identifikace silných a slabých stránek metodiky

Tento okruh se zaměřuje na identifikaci konkrétních výhod, nedostatků, nebo omezení, spojené s použitím nové metodiky.

- ***Analýza:*** Firmy obecně vnímaly metodiku jako přínosnou, zejména kvůli její schopnosti vypočítat návratnost investic a zlepšení komunikace s vedením společnosti. Hlavním nedostatkem je srozumitelnost některých odpovědí v části hodnocení jednotlivých procesů a stanovení očekávané maximální ztráty jednotlivých hrozeb. Doporučení pro zlepšení se týkaly především softwarového nástroje, možnosti reportingu a změně formy odpovědí během hodnocení jednotlivých procesů.
- ***Závěr:*** Metodika přináší významné přínosy v oblasti identifikace rizik a poskytuje cenné informace pro zlepšení kybernetické bezpečnosti, což z ní činí hodnotný nástroj pro firmy různé velikosti.

7. Závěr

Navržená metodika navrhuje inovativním způsobem obecný rámec pro hodnocení kybernetické bezpečnosti, definuje výkon kybernetické bezpečnosti a díky integrovanému ekonomickému modelu je schopna posoudit návratnost investic do kybernetické bezpečnosti. V rámci této práce byla metodika empirickým způsobem nastavena a validována pro sektor výroby. Dále byla stanovena mapa kybernetických rizik, která dělí sektor výroby do oblastí podle stejné motivace útočníka v závislosti na ročním obratu firmy a počtu koncových bodů ve firemní síti. Zde jsou uvedeny hlavní výhody navržené metodiky:

- Reflektuje specifickou pozici firmy, tedy sektor, ve kterém působí a zohledňuje motivaci útočníků vzhledem k její velikosti.
- Využít empiricky ověřené váhy, které popisují aktuální stav kybernetického bezpečnostního okolí firmy.
- Umožňuje pravidelnou aktualizaci nastavených vah, tak aby mohla reagovat na měnící se kybernetické prostředí a vývoj jednotlivých hrozeb.
- Hodnocení úrovně kybernetické bezpečnosti se zaměřuje na nejvýznamnější hrozby a konkrétní bezpečnostní procesy.
- Je přizpůsobena potřebám bezpečnostních manažerů a pracovníků zodpovědných za kybernetickou bezpečnost, tedy, že hodnotící proces je jednoduchý, rychlý a dává okamžité měřitelné výsledky.

- Integruje dva nejvýznamnější ekonomické modely popsané ve vědecké literatuře, které slouží pro podporu rozhodování (a obhájení) investic do kybernetické bezpečnosti
- Stanoví výkonnostní charakteristiky, které mohou být využity pro benchmarking.

Navržená metodika má však také několik omezení a kritických míst, jedná se především o tyto:

- Motivace útočníka vychází pouze z touhy po finančním a útoku a nízké náklady na útok (snadnost útoku). Ostatní motivace jako ideologické a politické důvody, konkurenční boj nebo zvědavost, nejsou v tomto modelu uvažovány.
- Stanovení reálných částek pro jednotlivé úrovně dopadů hodnotícím týmem je zásadní pro správné ekonomické zhodnocení návratnosti investic do kybernetické bezpečnosti.
- Objektivita hodnotícího týmu při stanovování úrovně jednotlivých procesů může mít také dopad na kvalitu výsledků.

Vědecký přínos

Na základě provedené systematické literární rešerše, kde byly definovány nedostatky současných norem a metodik v oblasti hodnocení kybernetické bezpečnosti. Dále byly identifikovány hlavní trendy v současných přístupech ve vědeckém poznání. Na základě analýzy odborné a vědecké literatury byl nalezen prostor pro vytvoření obecného rámce pro hodnocení kybernetické bezpečnosti, který je možno přizpůsobit na základě empirického zjištění váhových koeficientů pro vybraný sektor. Metodika je zaměřená na konkrétní hrozby vztahující se na hodnocenou firmu na základě sektoru, ve kterém působí a její velikosti.

Hlavními přínosem v oblasti vědy jsou:

- Pokrok v metodologii: metodika přináší inovace v metodologii měření a hodnocení kybernetické bezpečnosti, kdy se využívá procesního přístupu a na organizaci je pohlíženo jako na jedno aktivum. Propojuje teoretické koncepty s praktickými aplikacemi a nejlepší praktikami, což umožňuje hlubší porozumění dynamikám bezpečnostních opatření a jejich efektivity.
- Modelování a simulace bezpečnostních rizik: metodika pomáhá v rozvoji modelů, které simulují různé bezpečnostní scénáře. To umožňuje lepší predikci výsledků různých bezpečnostních strategií a zvyšuje porozumění rizikovým faktorům v digitálním prostředí.
- Interdisciplinární integrace: Metodika integruje poznatky z informatiky, ekonomie, managementu a sociologie, což přináší komplexní pohled na kybernetickou bezpečnost a její socio-ekonomické důsledky.

Společenský přínos

Společenský přínos navrhovaného metodiky se projevuje v několika klíčových oblastech, které mají široký dopad na celou společnost. Zásadním přínosem je zvýšení celkové bezpečnosti digitálních systémů a infrastruktur. Toto zvýšení bezpečnosti přímo zvyšuje důvěru veřejnosti ve využívání digitálních služeb, což je zvláště důležité v éře, kdy se digitální technologie stávají nezbytnou součástí každodenního života. Nejdůležitější společenské přínosy jsou především:

- Zvýšení bezpečnosti a důvěry: Implementace metodiky může vést ke zvýšení celkové bezpečnosti organizací a firem, což má přímý dopad na důvěru veřejnosti v digitální systémy a služby.
- Ochrana osobních a citlivých dat: Zlepšení kybernetické bezpečnosti organizaci a firem přispívá k ochraně osobních a citlivých dat, což je zásadní pro ochranu práv a svobod jednotlivců.
- Prevence kyberkriminality: Efektivní využití metodiky může předcházet kybernetickým útokům a tím omezit ekonomické škody a další negativní dopady kyberkriminality.

Pedagogický přínos

Data a nová zjištění získaná tímto výzkumem budou dále sloužit pro další rozvoj osnov studijních oborů, protože základní znalosti v oblasti informační a kybernetické bezpečnosti jsou v dnešní době nezbytnou znalostí pro budoucí manažery a majitele firem. Výsledky výzkumu bude také možné využít jako podklad pro další výzkum (možnost získání grantů na další projekty) a zadávání závěrečných prací (bakalářských, diplomových a disertačních). Zde jsou přehledně shrnuty hlavní pedagogické přínosy:

- Vzdělávání a osvěta: Metodika může být využit jako vzdělávací nástroj pro studenty, pedagogy a profesionály, což pomáhá šířit povědomí o důležitosti a metodách kybernetické bezpečnosti.
- Vývoj výukových plánů: Shromažďování výstupů z metodiky může sloužit jako základ pro vývoj nových nebo aktualizovaných studijních plánů, které zahrnují kybernetickou bezpečnost ve větším detailu pro konkrétní sektory.
- Podpora celoživotního vzdělávání: Metodika může inspirovat profesionální vývojové a školicí programy, které podporují aktuální znalosti v rychle se vyvíjejícím oboru kybernetické bezpečnosti.

Návrhy na pro další výzkum a inovace navržené metodiky

Tato práce představuje pouze začátek dlouhodobého výzkumného úsilí v oblasti kybernetické bezpečnosti. Vývoj této metodiky je dynamickým a neustále se vyvíjející proces, který vyžaduje pravidelné aktualizace a inovace, aby dokázal účinně reagovat na neustálé změny v technologickém prostředí. S rychlým pokrokem nových technologií, objevováním nových hrozeb a zranitelností je zásadní, aby se tato metodika neustále vyvíjela a byla aktualizována. To zahrnuje nejen revizi a zlepšení stávajících nástrojů procesů a stanovených vah, ale také integraci nových poznatků a technik, které mohou poskytnout lepší ochranu a obranu proti kybernetickým hrozbám. Tento neustálý vývoj zajišťuje, že metodika zůstane relevantní a efektivní nástroj v ochraně organizací v proměnlivém kybernetickém prostředí. Rozvoj a zdokonalení navrhované metodiky hodnocení úrovně kybernetické bezpečnosti poskytne mnoho možností pro další výzkum. Níže jsou některé návrhy, jak by mohl být tento výzkum rozšířen a prohlouben:

Validace a Kalibrace Metodiky

- Empirická validace pro další sektory: Provést rozsáhlé empirické studie s cílem získat data pro další vybrané sektory.
- Kalibrace: Průběžně kalibrovat a upravovat metriky a vah metodiky na základě zpětné vazby a výsledků z praxe, což umožní metodice lépe odrážet dynamické kybernetické prostředí.

Integrace Nových Technologií a Trendů

- Zahrnutí nových technologií: Začlenit nové technologické trendy, jako je umělá inteligence, strojové učení a blockchain, které mohou ovlivnit kybernetickou bezpečnost. To umožní automatizovanou analýzu velkých objemů dat v reálném čase, což může vést ke zvýšení přesnosti nastavení vah, rychlosti detekce nových hrozeb a zranitelností v kybernetické bezpečnosti.
- Reakce na nové hrozby: Aktualizovat metodiku tak, aby zahrnovala nové typy kybernetických útoků a hrozeb.

Dlouhodobé Studie Dopadu

- Provést dlouhodobé studie, které by sledovaly vliv implementace metodiky na bezpečnostní výkonnost organizací. Tyto studie by poskytly cenné informace o trvalých dopadech metodiky na zlepšení kybernetické bezpečnosti.

Vytvoření specializovaného softwaru

- Vytvoření speciálního softwaru, nebo webového rozhraní, které bude uživatelsky příjemné a bude umožňovat jednodušší aktualizace s ohledem na vývoj technologií hrozeb a zranitelností.

Odstranění kritických míst

- Nalezení závislosti mezi hrozbou a jejím finančním dopadem na organizaci, při její úspěšné realizaci. Tím by se tato částka vzhledem k velikosti firmy a počtu zařízení v síti doplňovala automaticky a minimalizovalo riziko špatného posouzení investice do kybernetické bezpečnosti.
- Lepší specifikace odpovědí pro hodnocení jednotlivých procesů, tak aby byly srozumitelnější, například přidáním více praktických příkladů, check listu, nebo dodatečnými kontrolními otázkami.

Tyto závěry a doporučení zdůrazňují potenciál metodiky jako nástroje pro posílení kybernetické bezpečnosti ve firmách a naznačují cesty, jak tento potenciál plně využít. Implementací těchto doporučení mohou organizace nejen zlepšit svou bezpečnost, ale také lépe řídit svá rizika a reagovat na nové hrozby v dynamickém digitálním prostředí.

Seznam použitých literárních zdrojů

Davis, A. (2005). Return on security investment – proving it's worth it. Network Security, 2005(11), 8-10. https://doi.org/10.1016/S1353-4858(05)70301-9

Drucker, P. F. (1993). Postkapitalistická společnost: (Post-Capitalist Society). Management Press.

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. ACM Transaction on Information and System Security, 5(4), 438-457.

Hendl, J. (2023). Kvalitativní výzkum: základní teorie, metody a aplikace (Páté, přepracované vydání). Portál.

Kelly, D. (2017). The economics of cybersecurity. In 12th International Conference on Cyber Warfare and Security (pp. 522-528). Academic Conferences and Publishing International Limited.

Lackner, M., Markl, E., & Aburaia, M. (2018). Cybersecurity Management for (Industrial) Internet of Things: Challenges and Opportunities. Journal of Information Technology & Software Engineering, 08(05). https://doi.org/10.4172/2165-7866.1000250

Molnár, Z. (2012). Pokročilé metody vědecké práce. Profess Consulting.

Závěrečná zpráva z hodnocení dopadů regulace (RIA) (2024). Ministerstvo financí. https://www.mfcr.cz/cs/kontrola-a-regulace/legislativa/legislativni-dokumenty/2023/zaverecna-zprava-ria-51775