VYSOKÁ ŠKOLA POLYTECHNICKÁ JIHLAVA

Katedra technických studií

Kybernetická bezpečnost kritických infrastruktur: analýza a znalostní model

bakalářská práce

Autor práce: Michaela Purkertová

Vedoucí práce: doc. Dr. Ing. Jan Voráček, CSc.

Jihlava 2020

Vysoká škola polytechnická Jihlava

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Autor práce:	**Michaela Purkertová**
Studijní program:	Elektrotechnika a informatika
Obor:	Aplikovaná informatika
Název práce:	**Kybernetická bezpečnost kritických infrastruktur: analýza a znalostní model**
Cíl práce:	Seznamte s vymezením pojmů kritická infrastruktura a kybernetická bezpečnost. Analyzujte současné způsoby datového zabezpečení kritických infrastruktur a to zejména z pohledu firemního prostředí a bezpečnostních politik. Přitom zohledněte i nejnovější technologické trendy (Internet věcí, 5G sítě, digitální ekonomika, RIS3 apod.). Získané poznatky zpracujte formou znalostního modelu, reprezentujícího bezpečnostní politiku firmy. K analýze i implementaci modelu využijte on-line platformy InsigtMaker a/nebo AnyLogic.

doc. Dr. Ing. Jan Voráček, CSc.
vedoucí bakalářské práce

doc. Ing. Zdeněk Horák, Ph.D.
vedoucí katedry
Katedra technických studií

Abstrakt

Osvojení si pojmů kybernetická bezpečnost a kritická infrastruktura. Následná analýza nynějších způsobů datového zabezpečení kritických infrastruktur a zohlednění novějších technologických trendů. Získané poznatky se zpracují formou znalostního modelu, reprezentujícího bezpečnostní politiku firmy. K analýze a implementaci se využijí online platformy InsightMaker, Forio nebo AnyLogic, případně některá ze systémově dynamických knihoven zvoleného programovacího jazyka.

Klíčová slova

Kyberprostor; kybernetická bezpečnost; kritická infrastruktura; hrozby; nové technologie

Abstract

Adoption of concepts cyber security and critical infrastructure. Subsequent analysis of current ways of data security of critical infrastructures and consideration of newer technological trends. Acquired knowledge will be processed in the form of knowledge model representing company security policy. For analysis and implementation will be utilized online platforms as InsightMaker, Forio or AnyLogic, eventually some of systemically dynamic libraries of the selected programming language.

Key words

Cyberspace; cyber security; critical infrastructure; threats; new technology

Prohlašuji, že předložená bakalářská práce je původní a zpracoval/a jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil/a autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v platném znění, dále též „**AZ**“).

Souhlasím s umístěním bakalářské práce v knihovně VŠPJ a s jejím užitím k výuce nebo k vlastní vnitřní potřebě VŠPJ.

Byl/a jsem seznámen/a s tím, že na mou mé bakalářskou práci se plně vztahuje **AZ**, zejména § 60 (školní dílo).

Beru na vědomí, že VŠPJ má právo na uzavření licenční smlouvy o užití mé bakalářské práce a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

Jsem si vědom/a toho, že užít své bakalářské práce či poskytnout licenci k jejímu využití mohu jen se souhlasem VŠPJ, která má právo ode mne požadovat přiměřený příspěvek na úhradu nákladů, vynaložených vysokou školou na vytvoření díla (až do jejich skutečné výše), z výdělku dosaženého v souvislosti s užitím díla či poskytnutím licence.

V Jihlavě dne 21. února 2020

…….
Podpis studenta/ky

Poděkování

Tímto bych ráda poděkovala svému vedoucímu bakalářské práce doc. Dr. Ing. Janu Voráčkovi, CSc. za profesionální rady, věcné připomínky, individuální přístup a trpělivost při vypracovávání této bakalářské práce. Dále bych chtěla poděkovat rodině a přátelům, kteří mě po celou dobu podporovali.

Obsah

Seznam obrázků

Seznam grafů

Seznam použitých zkratek

5G	- Pátá generace bezdrátových systémů
AI	- Artificial Intelligence (umělá inteligence)
BSC	- Balanced scorecard
CERT	- Computer Emergency Response Teams
CIA	- confidentiality (důvěrnost), integrity (integrita), availability (dostupnost)
COBIT	- Control Objectives for Information and related Technology
cPPP	- Cybersecurity Public-Private Partnership
CPS	- Cyber-Physical systems (kyber-fyzikální systémy)
CSIRT	- Computer Security Incident Response Team
ČR	- Česká republika
DAD	- Disclosure, Alteration, Destruction (odhalení, modifikace, zničení)
DDoS	- Distributed Denial of Service
DoS	- Denial of Service (odepření služby)
ECSO	- European Cyber Security Organisation
ENISA	- European Network and Information Security Agency (Evropská agentura pro bezpečnost sítí a informací)
ETSI	- European Telecomunications Standarts Institute (Evropský ústav pro telekomunikační normy)
EU	- Evropská Unie
HR	- Human resource (lidské zdroje)
ICT	- Informační a komunikační technologie
IoT	- Internet of Things (Internet věcí)
IoTSI	- Internet of Things Security Institute
IP	- Internet Protocol
ISACA	- Information Systems Audit and Control Association
ISMS	- Information Security Management System (Systém řízení bezpečnosti informací)
ITIL	- Information Technology Infrastructure Library
KB	- Kybernetická bezpečnost
KI	- Kritická infrastruktura
KII	- Kritická informační infrastruktura
MITM	- Man in the middle (člověk uprostřed)

NCKB	- Národní centrum kybernetické bezpečnosti
NGFW	- next-generation firewall
NÚKIB	- Národní úřad pro kybernetickou a informační bezpečnost
PDCA	- Plan, Do, Check, Act (naplánuj, proveď, ověř, jednej)
PESTLE	- Political, Economical, Social, Technological, Legal, Ecological (politické, ekonomické, sociální, technologické, legislativní, ekologické)
RIS3	- Research and Innovation Strategy for Smart Specialisation (Výzkumná a inovační strategie pro inteligentní specializaci)
SBOP	- Společná bezpečnostní a obranná politika
SQL	- Structured Query Language
SWOT	- Strengths, Weaknesses, Opportunities, Threats (silné stránky, slabé stránky, příležitosti, hrozby)
USA	- United States of America (Spojené státy americké)
WHO	- World Health Organization (Světová zdravotnická organizace)

Úvod

Neustále vyvíjející se technologie přinesly pro lidi velké množství benefitů. Nicméně s nástupem internetu a moderních technologií je stále složitější uchovávat informace tak, aby se k nim nedostaly nepovolané osoby, které by je mohly zneužít. S novými technologiemi a větším množství zařízení připojených k internetu, se navyšuje i počet míst, odkud lze provést případný kybernetický útok (Saravanan and Bama, 2019). Proto se poslední dobou stále častěji řeší otázka kybernetické bezpečnosti, která zvedá zájem u koncových uživatelů, v průmyslu či ve výzkumech (Lezzi et al., 2018; Pala and Zhuang, 2019; Sánchez et al., 2019). Každé další zařízení připojené k internetu, je zkrátka dalším rizikem a možným vstupem pro kybernetický útok.

Ačkoliv jsou si strategičtí manažeři vědomi kybernetických hrozeb, mají často potíže se zavedením efektivních řešení. Často jim totiž chybí technické vzdělání a mají tak větší tendenci přijmout strategie, které nejsou ve směru kybernetické bezpečnosti nejvhodnější. To pak může vyústit ve špatně zabezpečený nebo někdy naopak příliš zabezpečený podnik. V obou případech se takové rozhodnutí negativně projeví na financích podniku.

Jednou z částí této práce je tedy snaha o implementaci kybernetické bezpečnosti do BSC (Balanced scorecard) frameworku, a tedy i pozvednutí kybernetické bezpečnosti na vyšší úroveň než na úroveň rizika, jak je tomu do teď. Mohlo by to tak pomoct překlenout problémy mezi IT oblastí a managementem.

Protože jsem byla členkou projektu Česko-německé přeshraniční kritické infrastruktury, použila jsem v práci některé výstupy projektu. Moje práce pak zahrnovala převážně rozsáhlou rešerši a tvorbu modelu pro testování vzniklých dynamických hypotéz. Při tvorbě této bakalářské práce jsem kromě části výstupů projektu využila i některé poznatky obsažené v práci Barbory Skalické, jež mi byly nápomocné.

Motivace

V této práci se budu věnovat tomu, jak zvýšit kybernetickou bezpečnost kritických infrastruktur podniku. I přes stálý vývoj informačních technologií je kybernetická

bezpečnost u nás často podceňována. S novými technologiemi přichází totiž i nové hrozby, které je třeba brát v potaz a musí se na ně adekvátně reagovat.

Jedním z důvodů, proč jsem se rozhodla pro práci na toto téma je ten, že chci pomoct k lepšímu přiblížení této problematiky.

Cíl práce

Dílčí cíle bakalářské práce:

- Literární průzkum v oblasti kybernetické bezpečnosti a kritických infrastruktur (ten se bude týkat čtyř oblastí, konkrétně: právního prostředí, kybernetické bezpečnosti podniků, co nabízí trh a výzkumu v oblasti kybernetické bezpečnosti)
- Vytvoření myšlenkové mapy ze získaných poznatků
- Vytvoření systémového diagramu a diagramu kauzálních smyček (CLD diagramu)
- Vytvoření zjednodušené simulace v některé z dostupných platforem

1 Úvod do problematiky

V této části postupně projdu jednotlivé pojmy související s kybernetickou bezpečností, které je lepší pro pochopení problému znát. Také zde uvedu nejčastější druhy kybernetických útoků a základní právní rámec.

1.1 Kyberprostor

Pro lepší pochopení kybernetické bezpečnosti, je vhodné si nejprve definovat kyberprostor. První zmínky o termínu kyberprostor pochází z povídky „Jak vypálit Chrom“ od Williama Gibsona, ten ho následně více proslavil ve svém románu „Neuromancer“. Nicméně do všeobecného povědomí se dostává až v roce 1996 vydáním deklarace od Johna Barlowa (Kolouch and Bašta, 2019, s. 35).

Samotný kyberprostor pak lze interpretovat různě, jednoznačně daná definice v podstatě neexistuje. Ottis a Lorents jej kupříkladu definují jako množinu vzájemně provázaných informačních systémů závislých na čase a jejich uživatelích (Peeter Lorents, Rain Ottis, 2010).

Kyberprostor je vlastně pomocí technologií vytvořený virtuální svět, kde dochází ke vzájemné komunikaci. Můžeme zde sdílet informace a nápady, podnikat, hrát hry a další. Lze jej využít jak k obchodu, tak i k zábavě (“What is Cyberspace?,” 2020). V dokumentu Cyberspace Operations: Concept Capability Plan 2016-2018 je kyberprostor rozdělen na tři vrstvy: fyzická, logická a sociální. Ty jsou tvořeny celkem pěti komponenty: geografická část, fyzická síť, logická síť, osoba a kyberosobnost (“Cyberspace Operations Concept Capability Plan 2016-2028,” 2020).

1.2 Kybernetická bezpečnost

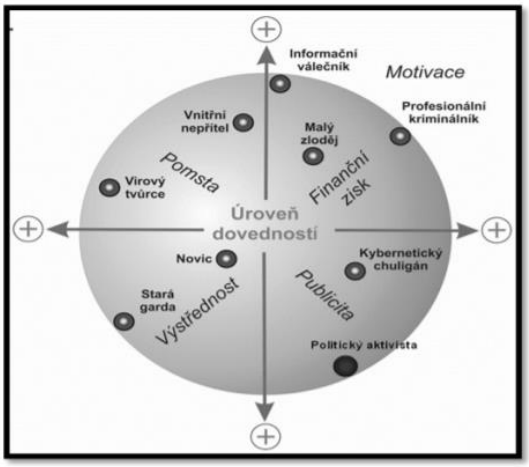
Pojem „kybernetická bezpečnost“ by se pak dal definovat jako souhrn postupů a opatření vedoucích ke specifickému zabezpečení informací v kyberprostoru. Cílem je primárně ochrana těchto informací před zneužitím a krádeží neboli zabránění nechtěnému chování počítačů. Nicméně bez fyzických částí by tyto cenné informace neexistovaly. Je tedy třeba chránit i tyto části proti vnějším rizikům jako jsou například přírodní katastrofy, aby nebyly informace poškozeny či zcela zničeny.

Pro uplatnění kybernetické bezpečnosti se používají principy, označované také jako triády. Nejpoužívanější je důvěrnost (confidentiality), integrita (integrity) a dostupnost (availability) označované jako CIA triáda. Většinou se usiluje o přiměřenou míru CIA (Kolouch and Bašta, 2019, s. 45). Naopak pokud by se někdo snažil tato data získat, pak se snaží o co nejefektivnější DAD (odhalení – disclosure, modifikace – alteration, zničení – destruction) ("CISSP – the CIA Triad and its opposites.," 2017).

Co se bezpečnosti týče, jsou tu i další potencionální rizika. Jedno z těch závažnějších a hůře ovlivnitelných je chování samotných uživatelů. Ti se bohužel velmi často a taky mylně domnívají, že se kybernetická bezpečnost týká jen oddělení informačních a komunikačních technologií. Proto mohou svým chováním v práci i doma značně zvýšit riziko jak vzniku, tak i následky kybernetických útoků. Tuto skutečnost stručně pronesl i americký odborník na počítačovou bezpečnost a kryptografii Bruce Schneier, který napsal, že *„Lidé často představují nejslabší článek v bezpečnostním řetězci a jsou chronicky zodpovědní za selhání bezpečnostních systémů"* ("Bruce Schneier Quote," 2000).

1.3 Kybernetické útoky

Kybernetický útok by se dal definovat jako útok způsobený zločinci využívajících jeden či více počítačů proti jednomu a více počítačů nebo sítí. Úspěšný kybernetický útok pak může vést k přerušení činnosti počítačů, krádeži dat, nebo využití narušeného počítače pro další útok. Útočníci mohou použít různé způsoby pro zahájení kybernetického útoku. Jedná se například o malware, phishing („rhybaření"), DoS (Denial of service – odepření služby) a další ("What is a Cyber Attack?," 2020). V každém případě se vždy jedná o hrozby ze strany konkrétních útočníků, ty lze členit z různých hledisek. Asi nejobecnější rozdělení útočníků je podle jejich motivace (Kolouch, 2007).



Obrázek 1 - Možné členění útočníků v kyberprostoru dle motivace (Kolouch, 2007, s. 2)

Celkově by problematika kybernetických útoků byla velmi obsáhlá. Pro zachování jednoduchosti, uvedu v této kapitole jen některé druhy kybernetických útoků.

1.3.1 Malware

Jedná se v podstatě o jakýkoliv škodlivý software určený k infikování digitálních zařízení. Často se využívá k získání osobních informací napadených osob a následně k jejich vydírání za účelem finančního zisku. Nicméně takto získaná data nemusí být čistě osobní informace jednotlivých uživatelů. Může se také jednat o zdravotní záznamy, údaje k internetovému bankovnictví a v případě napadení většího množství počítačů je lze využít k následným DoS útokům. Konkrétními typy malware jsou různé viry, červi (Worms), vyděračský software (Ransomware), špehovací software (Spyware), trojský kůň (Trojans), reklamní software (Adware) nebo bezsouborový malware (Fileless malware). Pokud dojde k napadení počítače, lze Malware rozpoznat několika způsoby. Obvyklým projevem je zpomalení počítače, přesměrovávání na jiné než požadované stránky nebo časté vyskakování reklam. (“What is malware,” 2020).

1.3.2 SQL Injection

SQL injection se snaží využít chyb v dotazech, které mohou být způsobené špatným vývojem. K útoku může dojít vložením SQL kódu do neošetřeného vstupního pole, jako je třeba login. Pokud je útok úspěšný, útočník získá kontrolu nad daty v databázi aplikace. Může tak přidat svůj vlastní pozměňující či jinak škodlivý příkaz. Hlavním cílem se tedy

stávají především databáze s citlivými údaji a čísly bankovních karet uživatelů (“SQL Injection,” 2008).

1.3.3 Phishing („rhybaření“)

Phishing je druh útoku, kde se snaží o oklamání lidí tak, aby sami sdíleli citlivé informace jako hesla nebo číslo kreditní karty. I tady existuje několik způsobů, jak toho lze dosáhnout, nejčastěji však jde o škodlivé emaily (malspam) nebo textové zprávy. Ty se mohou jevit jako neškodné, ale obsahují odkaz na útočníkem vytvořenou stránku, která ho požádá o zadání přihlašovacích údajů. Po potvrzení jsou tyto údaje odeslány útočníkovi. I přesto, že se jedná o jeden z nejjednodušších způsobů útoku, tak se bohužel zároveň jedná i o jeden z nejnebezpečnějších. Je to z toho důvodu, že tento typ útoku se nezaměřuje na technické nedostatky nebo jiné chyby v zabezpečení. Spoléhá čistě na selhání lidského faktoru, kdy se uživatel často nezdržuje kontrolou emailu a jeho původu (“What is Phishing?,” 2020).

V souvislosti s phishingem je známý případ „Operation Phish Phry“ z roku 2009, kdy bylo po dvouletém vyšetřování obviněno téměř 100 osob z USA a Egypta a které takto převedly na falešné účty okolo 1.5 milionu dolarů. V rámci tohoto případu bylo upozorněno i na to, že phishingové útoky v takové míře mohou sloužit jako sbírka pro případný teroristický útok (“FBI — Operation ‘Phish Phry,’” 2009).

1.3.4 DoS (Denial of Service – „odepření služby“)

Tyto útoky se zaměřují na znepřístupnění či vyřazení zařízení nebo sítě tak, aby nebyla dostupná předpokládaným uživatelům. DoS útoky toho mohou dosáhnout zahlcením cíle dotazy nebo odesláním informace, která způsobí pád. Většina útoků se týká významných organizací jako jsou banky, vláda nebo obchodní organizace. Přestože DoS útoky obvykle nevedou ke krádeži nebo ztrátě podstatných informací, tak mohou oběť stát nemalé množství času a peněz. Podtypem DoS útoku je i známý DDoS útok (Distributed Denial of Service). O ten se jedná ve chvíli, kdy je útok na cíl veden z více než jednoho místa, což útočníkovi dává jisté výhody. Hlavní výhody zahrnují obtížnější určení pozice útočníka, stejně tak jako vyřazení většího množství zařízení najednou (“What is a denial of service attack (DoS) ?,” 2020). Za jeden z největších DDoS útoků se považuje výpadek

služby GitHub z února 2018. Během útoku byl datový provoz o síle až 1.35 Tb/s (126.9 milionu paketů za sekundu) (“February 28th DDoS Incident Report,” 2018).

1.3.5 MITM (Man in the Middle – „člověk uprostřed“)

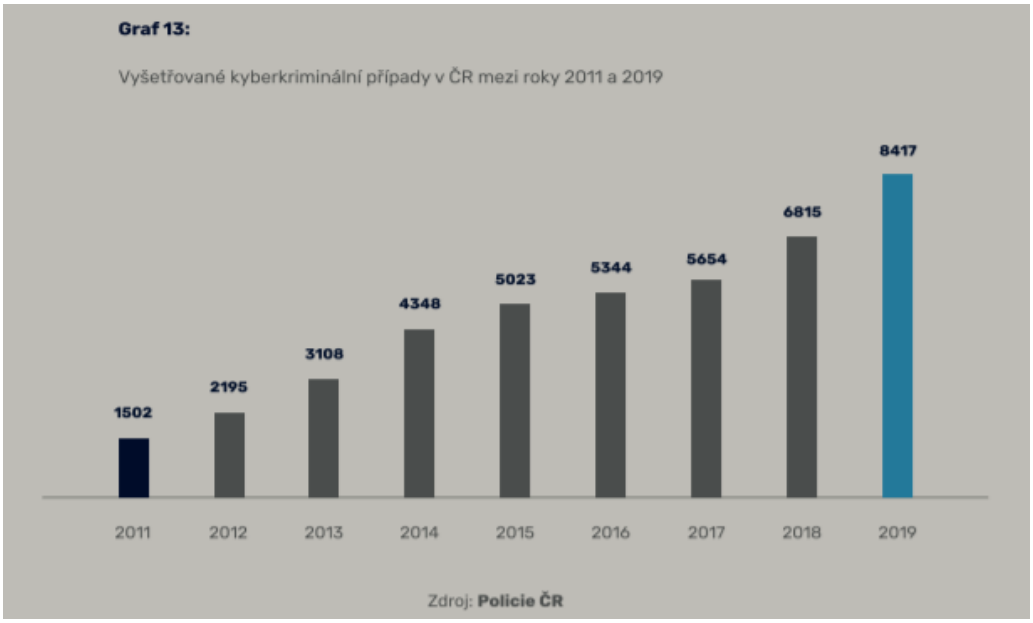
MITM útok je vlastně všeobecný termín pro osobu, která se umístí do konverzace mezi uživatele a aplikaci ať už kvůli odposlechu nebo vydávání se za jednu ze stran, což pak vypadá jen jako běžná výměna informací. Cílem takového útoku je krádež osobních informací jako jsou přihlašovací údaje nebo číslo kreditní karty. Útočníci se tak zaměřují na uživatele finančních aplikací, stránky elektronického obchodu a dalších stránek, kde je potřeba se přihlásit pomocí údajů (“What is MITM Attack | Imperva,” 2020).

1.3.6 Útoky na dodavatelské řetězce

I přesto, že útok na dodavatelské řetězce nepatří mezi nejčastější typ útoku, v případě úspěchu může mít rozsáhle následky. Jedním z takových útoků byl útok na antivirovou společnost Avast v druhé polovině roku 2019. Předpokládá se, že cílem útočníků byl produkt CCleaner. Tehdy to byl již druhý pokus o poškození softwaru, první proběhl v září 2017, ten byl však úspěšný (Zpráva o stavu kybernetické bezpečnosti ČR – 2019, s. 13).

1.3.7 Kybernetické útoky v ČR

Tak jako jinde ve světě, i v České republice dochází ke kybernetickým útokům. Statistika, kterou zveřejnil NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) potvrzuje nemilou skutečnost, že se každoročně nejen zvyšuje počet kyberkriminálních případů, ale jejich nárůst je oproti předchozímu roku o to vyšší. Mezi roky 2018 a 2019 došlo k nárůstu vyšetřovaných případů o 24%. Kyberkriminalita se stává stále více oblíbeným druhem kriminální činnosti, protože zajišťuje relativně snadný zisk a zároveň poskytuje anonymitu, díky které je nižší šance na odhalení (Zpráva o stavu kybernetické bezpečnosti ČR – 2019, s. 9).



Obrázek 2 - Vyšetřované kyberkriminální případy v CR (https://nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf)

Nárůst kybernetických útoků je patrný i na množství úspěšných útoků na nemocnice. Ty jsou totiž velmi lákavým držitelem obrovského množství osobních údajů. Útoky na nemocnice mívají kromě toho i rozsáhlé dopady. V česku je jedním z nejznámějších případů útok na nemocnici v Benešově, ke kterému došlo v prosinci 2019. V tomto případě se jednalo o napadení pomocí ransomware. Nemocnice tak musela omezit lékařské zákroky, včetně plánovaných operací. Proti útoku pomáhali jak pracovníci NCOZ (Národní centrála proti organizovanému zločinu), tak zaměstnanci NÚKIB a společnosti ESET. Do plného provozu se nemocnice vrátila 30. prosince a způsobené škody se odhadují na více než 59 milionů korun ("Kyberútok na nemocnici v Benešově," 2019; "Útok na Nemocnici Benešov způsobil škodu 59 milionů," 2020).

Jedním z relativně nedávných závažných kybernetických útoků je například i útok, který byl vedený proti americké společnosti SolarWinds. Problém tak představovali některé aplikace, přesněji aplikace z platformy Orion. Od března do června 2020 byly aktualizace těchto aplikací modifikovány a opatřeny backdoorem, v případě SolarWinds označeného názvem SUNBURST. Pomocí automatických aktualizací tak došlo k distribuci upraveného softwaru. Zákazníci, kteří používali tyto aplikace, měli velmi vysokou šanci na narušení sítě zmiňovaným backdoorem. Mezi organizace, které byly tímto backdoorem zasaženy, patří například Microsoft, Cisco, Visa, Ford, Siemens, Yahoo, americká ministerstva obrany a spravedlnosti, řada letišť, nemocnic, tajných služeb

a dalších. Zákazníkům bylo doporučeno provést aktualizaci aplikací podle návodu na stránkách SolarWinds. Jako reakci na tento závažný útok vydal NÚKIB dne 16. prosince 2020 reaktivní opatření, které řešilo kybernetický bezpečnostní incident a mělo tak zajistit co nejrychlejší zabezpečení konkrétních systémů. Tyto systémy spadaly pod zákon o kybernetické bezpečnosti. Díky přípravě, která na tento útok musela proběhnout a taky kvůli dopadům na infrastrukturu panují domněnky, že se mohlo jednat o státem sponzorovaný útok ("NÚKIB - reaktivní opatření," 2020; "Security Advisory | SolarWinds," 2021; "Útok na SolarWinds," 2020).

1.4 Právní rámec

Hlavním důvodem pro vznik práva v kybernetické bezpečnosti je to, aby nedocházelo k narušení kybernetické bezpečnosti prostřednictvím kybernetických incidentů. V jednotlivých zemí jsou si sice některé zákony podobné, ale mohou se do jisté míry lišit. Každá země totiž začala s řešením problematiky kybernetické bezpečnosti v jinou dobu a s jiným přístupem.

1.4.1 Česká republika

V ČR se začala otázka kybernetické bezpečnosti řešit více kolem roku 2000, tehdy vznikla koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření. Vznik tohoto dokumentu byla reakce na čím dál tím větší přechod společnosti na informační technologie. Předpokládalo se, že moderní technologie budou častěji zneužity k trestné činnosti. Cílem byla hlavně analýza současného stavu a vývoje trestné činnosti v této oblasti.

Dne 19. října 2011 byla zřízena rada pro kybernetickou bezpečnost ("Rada pro kybernetickou bezpečnost," 2011) a vláda ČR schválila vznik národního centra kybernetické bezpečnosti (NCKB). To se zabývá jak prevencí před kybernetickými hrozbami vůči prvkům kritické informační infrastruktury, tak i řešením případných kybernetických incidentů u prvků kritické infrastruktury. Zároveň se zapojuje do výzkumu a vývoje v kybernetické bezpečnosti nebo do osvěty a vzdělávání v oblasti kybernetické bezpečnosti ("Národní centrum kybernetické bezpečnosti," 2020).

Jedním ze zásadnějších kroků pro zvýšení kybernetické bezpečnosti v ČR bylo vytvoření strategie pro oblast kybernetické bezpečnosti České republiky na období 2012-2015.

Účelem této strategie bylo zlepšení úrovně kybernetické bezpečnosti pro vládní instituce, kritickou infrastrukturu ale i pro obyvatele České republiky. Toho se chtělo dosáhnout splněním několik cílů. Mezi dva hlavní patřilo vytvoření legislativního rámce v kybernetické bezpečnosti a vybudování Národního centra kybernetické bezpečnosti a vládního pracoviště CERT.

Skrze tuto strategii byl přijat zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) (“Legislativa,” 2014). Hlavními cíli tohoto zákona je stanovení základní úrovně bezpečnostních opatření, zlepšení detekce kybernetických incidentů či zavedení hlášení kybernetických incidentů. Později došlo k významné novelizaci a to zákonem č. 104/2017 s účinností od 1. července a zákonem č. 205/2017 Sb. s účinností od 1. srpna 2017. Tato novelizace zahrnovala požadavky směrnice EU. Později došlo ještě k další novelizaci (“nukib - Legislativa,” 2020).

K zákonu o kybernetické bezpečnosti patří několik vyhlášek, například 317/2014 Sb. vyhláška ze dne 15. prosince 2014 o významných informačních systémech a jejich určujících kritérií, dále pak vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby (“Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby,” 2017) a vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

1.4.2 Legislativa v Evropě

Jedním ze základních dokumentů, který zajistil řešení problémů s kybernetickou bezpečností v Evropské unii, je nejspíše Strategie kybernetické bezpečnosti z roku 2013.(EUR-Lex, 2013) Ta uvádí, že jedním z hlavních cílů je ochrana základních práv, svobody projevu, osobních údajů a soukromí. V této strategii je popsáno pět strategických priorit. Jedná se konkrétně o: dosažení kybernetické odolnosti, výrazné omezení kyberkriminality, rozvoj politik a kapacit kybernetické obrany v souvislosti se společnou bezpečnostní a obranou politikou (SBOP), rozvoj průmyslových a technologických zdrojů pro kybernetickou bezpečnost, zavedení soudržné mezinárodní politiky Evropské unie týkající se kyberprostoru a podpora základních hodnot EU.

Dalo by se říci, že na tuto strategii navazuje poměrně důležitá 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 (EUR-Lex, 2016). Jedním z cílů této směrnice je podpora spolupráce a výměny informací mezi členskými státy. Za tímto účelem ustavuje síť bezpečnostních týmů typu CSIRT. Směrnice je v našem právním systému zavedena pomocí již zmiňované vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. Na tuto směrnici přímo navazuje prováděcí nařízení komise (EU) 2018/151 ze dne 30. ledna 2018 (*Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018*, 2018). Nařízení blíže specifikuje povinnosti poskytovatele digitálních služeb.

2 Kybernetická bezpečnost podniků

S rozšířením využití informačních technologií se otázka kybernetické bezpečnosti týká takřka všech uživatelů internetu.

V rámci této kapitoly se pokusím lépe objasnit pojem kritické infrastruktury a uvedu způsoby jejich zabezpečení. Současně zde uvedu některé novější způsoby datového zabezpečení kritických infrastruktur.

2.1 Kritická infrastruktura

Z definice kritické infrastruktury vyplývá, že kritickou infrastrukturou se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva (Zákon č. 240/2000 Sb.).

Směrnice rady 2008/114/ES jasně stanovuje odvětví, které se svojí funkcionalitou řadí pod kritickou infrastrukturu. Jedná se o energetiku, dopravu, zdravotní péči, vodní hospodářství, potravinářství, zemědělství, komunikační a informační systémy, bankovní a finanční sektor, nouzové služby a veřejnou správu (*Směrnice Rady 2008/114/ES*, 2008; "Vzdělávání členů SH ČMS," 2014).

Průřezová kritéria pro určení prvku kritické infrastruktury jsou tři hlediska s mezními hodnotami. Jedná se o hlediska (nařízení vlády č. 432/2010 Sb.):

1) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,
2) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo
3) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

Narušení kritické infrastruktury by mohlo mít rozsáhlé dopady jak hospodářské, tak i politické, sociální, psychologické či na životní prostředí. Například útok na zařízení pro tekutý zemní plyn by mohl způsobit nejen majetkovou škodu, ale i velké ztráty na

životech. Značné problémy by mohl zapříčinit i případný kaskádový efekt způsobený provázaností infrastrukturních odvětví (“EUR-Lex - 52004DC0702 - CS,” 2004). V takovém případě by selhání jedné části kritické infrastruktury vedlo k selhání dalších částí. Jedním ze známějších případů je kaskádová jaderná katastrofa ve Fukušimě. Zde došlo nejprve k zemětřesení o síle 9,0 stupně. Při něm nezemřelo více než sto lidí. Nicméně na následky způsobené vlnou tsunami vyvolanou tímto zemětřesením zemřelo přibližně 18 000 lidí (Alexander, 2018).

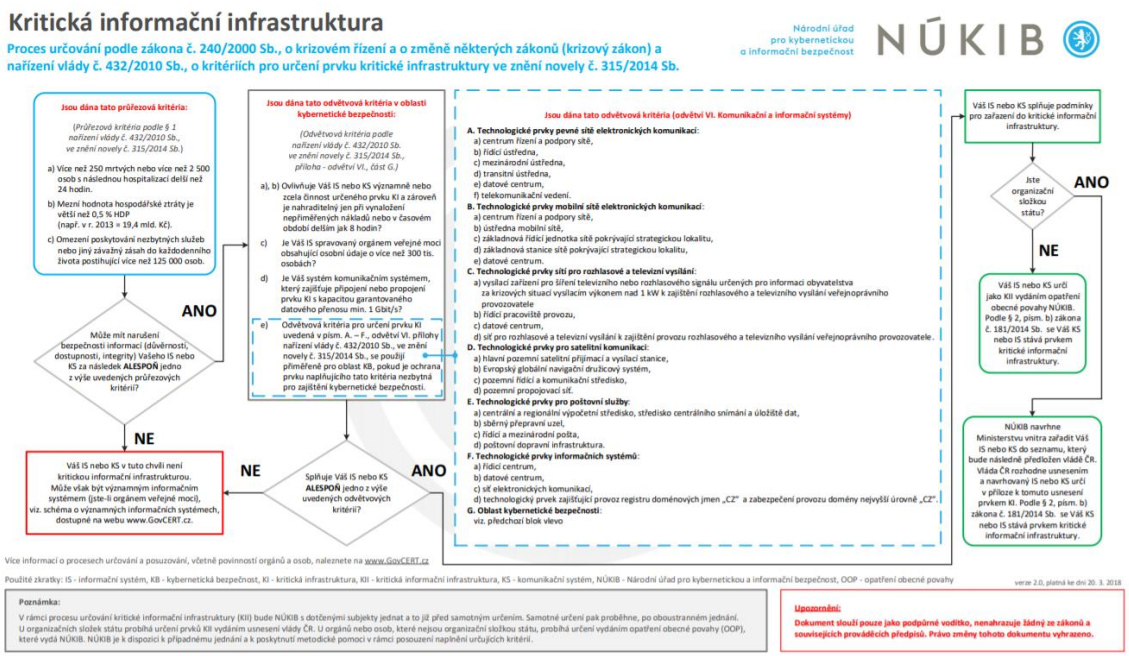
Kritickou infrastrukturu ohrožuje kromě mimořádných událostí i řada rizik. Ohrožení objektů lze rozdělit podle příčin narušení a místa vzniku na vnitřní a vnější problémy.

V případě vnitřních problémů to mohou být příčiny narušení funkcí na objektech a v systémech kritické infrastruktury, které nemusí být přímo ovlivněny příslušným subjektem nebo subjekty. V takovém případě se může jednat o různé technické poruchy, havárie, nedostatek náhradních dílů, výpadky dodávky energie, vody, surovin pro výrobu nebo poskytování služeb, případně kolaps počítačových sítí. Může se taky jednat o vnitřní problémy, kde jsou příčiny narušení funkcí přímo nebo nepřímo ovlivněny příslušným subjektem nebo subjekty. Jedná se o rizika jako krach firmy, stávka zaměstnanců subjektu kritické infrastruktury nebo změny orientace poskytování výrobků a služeb.

V případě vnějších problémů se pak jedná o rizika jako narušení objektu kritické infrastruktury z důvodu živelní pohromy, průmyslové havárie v sousedním objektu, narušení objektu člověkem, nedostatek pracovních sil včetně zvýšené nemocnosti a stávka zaměstnanců subjektů zajišťujících služby (Svoboda, 2010).

2.1.1 Kritická informační infrastruktura

Jedná se o prvek nebo prvky kritické infrastruktury, které podle zákona č. 240/2000 Sb., krizového zákona patří do odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti. Spadají zde pouze ty prvky, které splňují kritéria pro určení prvků KII (Kolouch and Bašta, 2019, s. 150 - 153). Za kritickou informační infrastrukturu se dají považovat všechny IT systémy tedy hardware i software, které jsou použity pro správu systémů kritické infrastruktury.

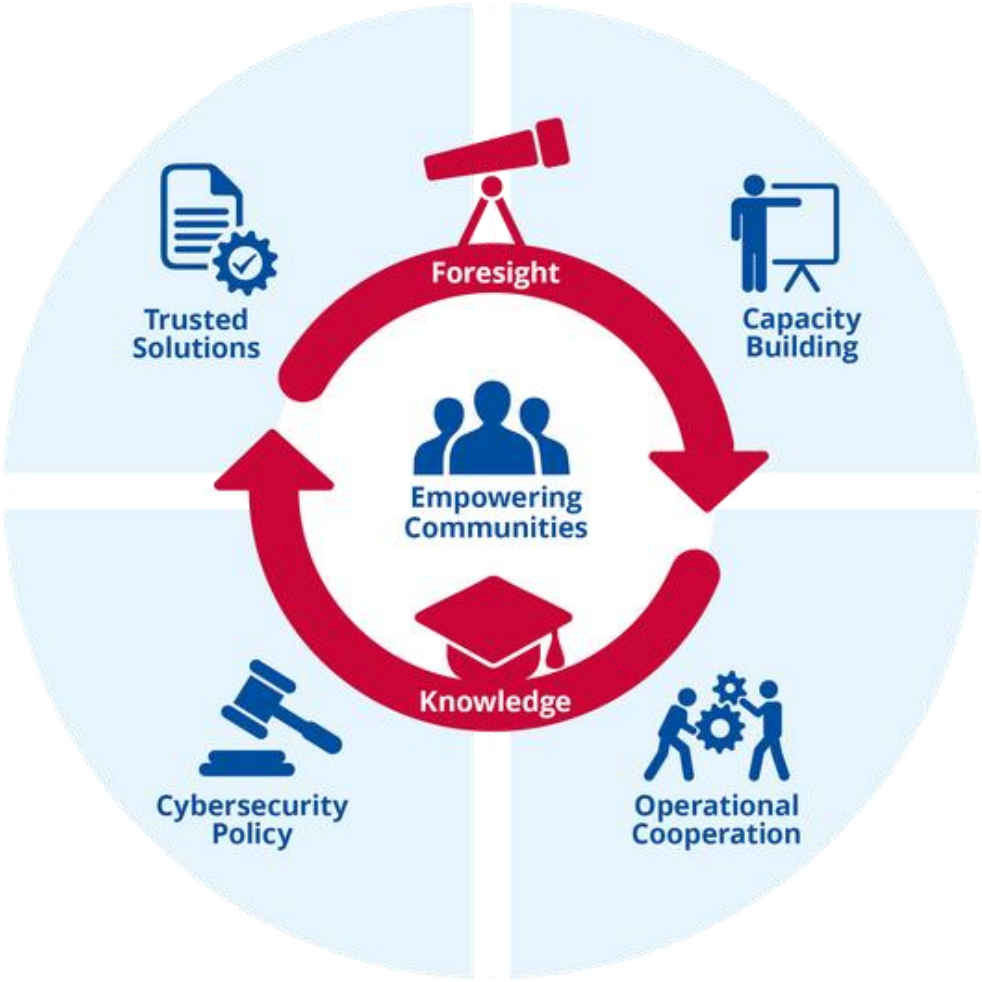


Obrázek 3 - Proces určování kritické informační infrastruktury (NÚKIB, 2018)

2.2 Důležité organizace

V Evropské unii působí například agentura ENISA, která byla zřízena roku 2004 skrze Nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ("EUR-Lex - 02004R0460-20110625 - EN - EUR-Lex," 2004). Jejím hlavním úkolem je dosáhnutí vysoké úrovně kybernetické bezpečnosti v Evropě. Přispívá tak třeba zvyšováním důvěryhodnosti ICT produktů, ale i spoluprací s členskými státy. Díky této spolupráci, sdílení znalostí a zvyšování povědomí pomáhá spolu se zainteresovanými stranami s posílením odolnosti evropské infrastruktury a také s digitálním zabezpečením občanů Evropy. Podílí se také na návrzích právních předpisů evropské kybernetické politiky. ENISA poskytuje různé druhy aktivit v zemích EU a pro orgány EU. Jedná se o nácviky řešení krizových situací

v oblasti kybernetické bezpečnosti, pomoc při národních strategií kybernetické bezpečnosti a další. Agentura vytvořila také síť zainteresovaných stran, ta se zaměřuje na odborné znalosti, politická opatření, kapacity a spolupráci (“About ENISA - The European Union Agency for Cybersecurity,” 2020).



Obrázek 4 - aktivity agentury ENISA (https://www.enisa.europa.eu/about-enisa)

Další v Evropě působící organizací je pak kupříkladu nezisková organizace ECSO (European Cyber Security Organisation). Ta je partnerem Evropské komise pro implementaci cPPP (Cybersecurity Public-Private Partnership) (“ECSO - European Cyber Security Organisation,” 2021).

2.3 Technologické trendy

Rychlý rozvoj technologických trendů, jako jsou například IoT, 5G sítě, digitální ekonomika a další, způsobuje i mnohem vyšší potřebu rozvoje kybernetické bezpečnosti. Zde tedy zohledním některé technologické trendy, jejich využití, výhody a nevýhody.

2.3.1 IoT

IoT nebo také „internet věcí“ je systém vzájemně propojených počítačových zařízení, mechanických a digitálních přístrojů, objektů, zvířat a lidí, kde má každý svůj unikátní identifikátor a schopnost přenosu dat po síti. Může se jednat prakticky o jakýkoliv živý organismus nebo předmět, kterému lze přiřadit vlastní IP adresu a je schopen přenosu dat. Příkladem může být třeba osoba se srdečním implantátem nebo biočipové senzory na zvířecích farmách.

IoT poskytuje podnikatelům pohled v reálném čase na to, jak jejich systémy opravdu fungují, poskytuje přehled jak o výkonu strojů, tak o dodavatelských řetězcích a logistických operací. IoT umožňuje firmám automatizaci procesů, snižuje množství odpadu a zlepšuje poskytování služeb, čímž se výroba a doručení zboží stává levnější. Všeobecně poskytuje výhody jako úsporu času a peněz, zlepšuje zákaznickou zkušenost, zvyšuje produktivitu zaměstnanců, pomáhá generovat více příjmů a další. Avšak i zde se lze potýkat s řadou nevýhod, mezi něž patří například mnohem větší množství připojených zařízení a informací sdílených mezi nimi. Více připojených zařízení může být lákavé pro případné hackery. Podniky se navíc mohou potýkat s příliš velkým množstvím vygenerovaných dat, jejichž sběr a následná údržba nemusí být jednoduchá. Příliš vzájemně propojených zařízení zkrátka vytváří širší prostor pro hackerské útoky (“What is IoT?,” 2016).

Pro zlepšení bezpečnosti IoT zařízení tak začali vznikat různé organizace. Například IoTSI (Internet of Things Security Institute) tvoří frameworky a podporuje vzdělávací služby, aby pomohl se správou bezpečnosti v rámci ekosystému internetu věcí. Vydává tak IoT Security Framework pro chytrá města a kritickou infrastrukturu. Ten má za cíl vytvořit rozsáhlý soubor pokynů každému z účastníků dodavatelského řetězce. IoTSI jim chce touto cestou pomoct se specifikací, bezpečnou instalací, integrací a údržbou IoT v budovách a chytrých městech (Cities and Things, 2019). Se zlepšením bezpečnosti zařízení IoT má pomoct i projekt Brain-IoT, jež se zaměřuje na vytvoření frameworku

a metodiky, která podporuje IoT platformy úzce spolupracující s CPS (kyber-fyzikální systémy) (“Home - BRAIN-IoT,” 2018).

2.3.2 Sítě 5G

Jedním z témat poslední doby je také zavádění 5G sítí. Hlavní výhodou je přibližně desetinásobná přenosová rychlost a znatelné snížení doby odezvy proti 4G. To vede k jejich využití v IoT a konceptu chytrých měst. Na nové síti tak poběží provoz městské infrastruktury, dopravních systémů, vodohospodářství, odpadového hospodářství, e-government nebo krizové řízení (“Role jednotlivých subjektů v procesu zavádění 5G sítě,” 2020). Pomocí 5G sítí dojde k propojení miliardy předmětů a systémů i v kriticky významných odvětvích, zejména pak v energetice, dopravě, bankovnictví nebo zdravotnictví. Právě ve zdravotnictví se tato technologie uplatní například při prevenci díky možnosti sledování zdravotního stavu pacienta v reálném čase. S pomocí mikroskopických kamer a dalších zdravotních zařízení půjde vzdáleně určit diagnózu. Takový způsob kontroly by mohl zároveň snížit náklady na případnou diagnózu nebo léčbu, protože pacient nemusí být osobně přítomen. To uvítají zejména osoby, které se kvůli zdravotnímu stavu nebudou moci dostavit osobně na kontrolu, případně ti, kteří nechtějí absolvovat zdlouhavou cestu (Neumuth et al., 2020; Siriwardhana et al., 2020).

Nicméně 5G přináší i jisté potíže. Hardware jako routery nebo síťové přepínače řešily velké množství různých procesů, které jsou v případě 5G vykonávány za pomoci software. Zároveň kvůli menšímu dosahu potřebují více antén. To vše bohužel vytváří více možností ke kybernetickému útoku. Protože bude na 5G sítích záviset mnoho kritických prvků, je kvalitní zajištění jejich bezpečnosti nesmírně důležité (CADEK, 2020). Přepokládá se, že by jedním z větších rizik mohli být samotní dodavatelé. Od těch jsou nezbytné například antény formující paprsky signálu, bez nichž se 5G sítě neobejdou. Ty však vyžadují vysoký výpočetní výkon. Není moc pravděpodobné, že by stát dokázal zajistit dostatečnou kontrolu všech těchto zařízení, a tudíž spoléhá prakticky jen na důvěru v dodavatele. Druhým podstatným problémem je chybějící dělení na periferii a jádro. To sice umožnilo značné snížení odezvy, bohužel tak odpadla i možnost odchycení podezřelých dodavatelů na periferii a znemožnění jejich přístupu do jádra. Citlivá data jsou tak vedena takřka jakoukoliv částí 5G (“Implementace a rozvoj sítí 5G v České republice | MPO,” 2020).

Kvůli provázanosti jednotlivých systémů by narušení mohlo mít dopady až za hranicemi jednotlivých států. Evropská rada tak vyzvala ke koordinovanému přístupu k bezpečnosti sítí 5G a vydává doporučení Evropské komise 2019/534. Členské státy tak mají s podporou Komise a agentury ENISA vzájemně spolupracovat a realizovat dohodnutá opatření (Union, 2020).

2.3.3 RIS3

Nebo taky Národní výzkumné a inovační strategie pro inteligentní specializaci České republiky (Research and Innovation Strategy for Smart Specialisation) je dokument, jehož cílem je efektivní využití finančních prostředků z různých zdrojů pro rozvoj inovací v perspektivních oblastech. V rámci Národní RIS3 strategie jsou podporovány různé aktivity, jako například podnikavost, spolupráce, ambice, kreativita, udržitelnost ale i odolnost. Skrze odolnost je za pomoci nových řešení a technologií snaha o posílení odolnosti nosných odvětví, infrastruktury a kybernetické bezpečnosti. Podporuje mezinárodní spolupráci ve zvládání rizik a výzev pro posílení odolnosti společnosti.

Rozvoj digitálních technologií bere jednak jako příležitost ale také jako podmínku pro lepší fungování nejen jednotlivých institucí, ale i hospodářství jako celku. Jedná se o některé již zmíněné technologie jako rozvoj 5G sítí, využití IoT, umělé inteligence, modelování, simulací a další. Udává, že Česko je ve využívání novějších technologií pozadu a hrozí tak neudržení konkurenceschopnosti, což by mohlo mít negativní dopad na ekonomiku. Považuje tak za nutné zvýšit úroveň digitalizační transformace, ale také odstranění neochoty k inovacím u veřejného sektoru. (“Národní RIS3 strategie | MPO,” 2021).

2.3.4 Digitální ekonomika

Digitální ekonomika je vlastně ekonomika značně využívající internet, počítače a další elektronická zařízení. Na začátku 21. století dochází s nástupem ICT ke změnám v různých odvětvích včetně toho, jakým způsobem se lidé vzdělávají, nebo jak tráví svůj volný čas (ManagementMania, 2017). Původně se digitální ekonomika týkala hlavně transakcí. Časem došlo k vybudování digitální infrastruktury a tím i k rozvoji e-business. Cílem e-business bylo hlavně zabezpečit převod peněz a zabránit falšování elektronických podpisů (“Digitální ekonomika,” 2017).

Protože digitální ekonomika stálé přináší nové změny a tím i nové příležitosti, je v zájmu jednotlivých zemí těchto možností využít. Vláda tak přišla s programem pro digitalizaci České republiky zastřešující tři pilíře, které tvoří jeden celek. Konkrétně: Česko v digitální Evropě, Informační koncepce České republiky a Koncepce digitální ekonomika a společnost. Tyto pilíře pak mají za úkol naplnit několik cílů. Jedním z těchto cílů je například zajištění bezpečnosti a důvěry v prostředí digitální ekonomiky a společnosti. Toho se chce dosáhnout efektivním zajišťováním kybernetické bezpečnosti prvků kritické informační infrastruktury a dalších subjektů, které pomohou zvednout konkurenceschopnost ČR a ochrání její digitální ekonomiku. Zmiňuje také to, že je potřeba zvednout celkové povědomí, protože se digitální ekonomika dotýká i obyčejných uživatelů, jejichž chování má, byť nevědomě, dopad na bezpečnost ("Digitální Česko," 2020; "Hlavní cíle koncepce Digitální ekonomika a společnost | MPO," 2019).

2.3.5 Gartner a AI (umělá inteligence)

Gartner je americká výzkumná a poradenská společnost poskytující informace, nástroje a rady pro lídry v oblasti IT, financí, HR (Human resource), zákaznického servisu a podpory, výzkumu a vývoje a další. Kromě výzkumů a konzultací také pořádá konference ("Gartner," 2021).

Jedno z populárních zasedání bylo o strategických předpovědí pro rok 2020. Top 10 technologických trendů se soustředilo kolem dvou témat – chytrá prostředí a přístupy zaměřené na lidi. Obě tato témata pak zahrnovala pět trendů. Pod přístupy zaměřené na lidi byla zařazena hyperautomatizace, mnohozážitek, demokratizace dovedností, rozšíření lidských možností, a nakonec transparentnost a dohledatelnost. Mezi chytrá prostředí pak spadal výkonný edge, distribuovaný cloud, autonomní věci, praktický bookchain a AI bezpečnost ("Gartner's 2020 Trends," 2019).

Právě využívání umělé inteligence je stále častějším jevem, který dokáže značně pomoct s řešením kybernetické bezpečnosti. AI bezpečnost se pak snaží o zahrnutí využití umělé inteligence pro identifikaci a zastavení kybernetických útoků s menším lidským zásahem, než jaký je potřebný u běžných bezpečnostních přístupů. Nástroje pro AI bezpečnost mají objevovat, předpokládat, zdůvodnit a učit se o potencionálních hrozbách pro kybernetickou bezpečnost, aniž by byl potřeba značný lidský zásah. Běžně tyto nástroje zahrnují schopnost se učit z předchozích chování a na jejich základě pak rychle reagují

na neznámé chování. Kromě toho dokážou přijít s konkrétním závěrem založeném i na nekompletní podmnožině dat. Zároveň mohou posílit bezpečnostní týmy tím, že prezentují různá řešení na známý problém a vybere tak nejvhodnější řešení pro možnou nápravu (“AI Security Definition & Examples,” 2021).

Rozhodně se tedy jedná o důležitý trend, který bude hrát čím tím větší roli v oblasti kybernetické bezpečnosti. Avšak stejně jako u ostatních technologických trendů, i zde se se sice investuje, nicméně tato problematika opět není napojena do managementu.

2.4 ISMS podle norem ISO řady 27000

ISMS (Information Security Management System – Systém řízení bezpečnosti informací) je soubor pravidel, které pomocí aplikování procesu řízení rizik zachovávají důvěrnost, integritu a dostupnost. Organizace postupně odstraní případná rizika na základě jejích obchodních potřeb, platné legislativy a norem, které se zavazují splnit. Díky ISMS jsou chráněna aktiva, řízena rizika bezpečnosti informací a zavedená opatření jsou kontrolována. Zavádění ISMS se aplikuje v souladu s normou ISO/IEC 27001 a provádí se podle cyklu PDCA (Plan, Do, Check, Act). Díky opakování tohoto cyklu postupně dochází ke zlepšení služeb, dat či kvality procesů.

Přínosy implementace ISMS dle normy ISO/EIC 27001 jsou:

- Sladění potřeb bezpečnosti se strategií a cíli organizace
- Systémové řešení bezpečnosti
- Stanovení jasných bezpečnostních pravidel a postupů pro zaměstnance a dodavatele
- Ochrana aktiv
- Řízení a redukce rizik
- Naplnění požadavků partnerů a právních norem
- Zajištění souladu bezpečnosti s ostatními ISO normami (např. ISO 90001)
- Zkvalitnění řídících procesů
- Zvýšení důvěrnosti a vnímání v očích zákazníků

2.5 ITIL

Pro zlepšení kvality konkrétně IT služeb je vhodný například ITIL (Information Technology Infrastructure Library), který je dnes prakticky standart pro řízení a správu IT služeb. Jedná se v podstatě o knižní souhrn doporučení a osvědčených praktik v oblasti IT. Díky těmto postupům pomáhá ITIL zkvalitňovat složku firemních informačních technologií. Kromě své knižní formy je ITIL šířen i pomocí odborných konzultací a školení. Jedna z výhod je například to, že společnosti řídící se procesy ITIL požívají stejné termíny, což usnadňuje komunikaci s partnery i se zákazníky. Dále například sníží množství potencionálních potíží, protože se hledají příčiny problémů. Z ITIL vychází i norma ISO 20000, která se soustředí na všeobecné zefektivnění IT procesů.

2.6 COBIT

COBIT je framework, určený ke správě a řízení IT. Jedná se o soubor praktik a postupů, které mají pomoct organizaci s minimalizací IT rizik a dosáhnutím strategických cílů. Ten byl vyvinut mezinárodní profesní asociací ISACA, která se zaměřuje na oblast auditu, řízení, kontroly a bezpečnosti informačních systémů. COBIT byl navržen jakožto podpůrný nástroj pro manažery. Umožňuje překlenutí zásadní mezery mezi technickými problémy, obchodními riziky a kontrolními požadavky. Celkově COBIT zajišťuje kvalitu, kontrolu a spolehlivost informačních systémů v organizaci (ManagementMania, 2015; “What is COBIT?,” 2012).

COBIT definuje procesy IT rozdělené do čtyř domén:

- Plánování a organizace
- Akvizice a implementace
- Dodávka a podpora
- Monitoring a evaluace

3 Zajištění kybernetické bezpečnosti

Pro odstranění, a především prevenci bezpečnostních hrozeb je k dispozici několik různých nástrojů. K tomuto účelu lze využít konkrétní hardware a software. Jedná se například o zařízení na filtrování DDoS útoků, počítačové systémy, sítě, firewall, aplikace na šifrování, ale i aktualizaci software. Nicméně často tyto nástroje k zabezpečení nestačí, a dokonce se někdy považují za „méně důležité“. Je to z toho důvodu, že výše zmíněné způsoby zabezpečení chrání pouze před známými typy útoků. Nicméně jak se oblast kybernetické bezpečnosti rychle vyvíjí, tak se stejně rychle ne-li rychleji vyvíjí i útočníci a jejich způsoby, jak bezpečnost obejít. Pro efektivní prevenci je třeba reagovat na vyvíjející se kyberkriminalitu. K tomu slouží různé druhy školení, analýz či dokumentací.

3.1 Poskytovatelé

Přestože problematiku kybernetické bezpečnosti musí z větší části řešit konkrétní organizace či osoba, je vhodné využít i některých bezpečnostních prvků a služeb od společností zabývajících se kybernetickou bezpečností. Na českém i zahraničním trhu existuje několik dodavatelů poskytujících hardware, software ale i služby jako jsou například školení zaměstnanců. Uvedu alespoň pár příkladů.

3.1.1 Cisco

Tato společnost byla založena roku 1984, u nás působí od roku 1995 a patří mezi světové špičky v oblasti síťových prvků. Vyrábí a prodává hardware i software, ale nabízí také různé druhy služeb. Jedná se třeba o poradenství nebo optimalizace. Součástí jejího portfolia jsou i nástroje pro týmovou spolupráci a jednání na dálku, jako jsou WebEx nebo TelePresence (“Cisco - Global Home Page,” 2020). Cisco se může také chlubit velkým množstvím nových patentů a dlouholetými zkušenostmi v oblasti IT služeb.

Cisco Networking Academy pak nabízí různé druhy kurzů a školení jak pro vzdělávací instituce, tak pro jednotlivce. Příkladem mohou být kurzy programování, IoT (Internet of Things – Internet věcí) nebo i kyberbezpečnosti. Kupříkladu v kurzu Cybersecurity Essentials se lze naučit lépe chápat problematiku kybernetické kriminality, bezpečnostní zásady, technologie a postupy potřebné pro zajištění sítě. Absolvování kurzu je také vhodné i jako příprava pro získání Cisco CyberOps Associate certifikací (“Cybersecurity Courses,” 2018).

3.1.2 IBM

Dalším z významných poskytovatelů je společnost IBM. Vznikla již v roce 1911 jako akciová společnost a svou první pobočku založila v tehdejším Československu roku 1932. Patří mezi největší a nejstarší poskytovatele služeb informačních technologií na světě. Uvádí na trh jak systémy pro ukládání dat, tak i software či poradenské služby. Kromě prodeje technologií se zabývá i výzkumem, jenž vedl například k miniaturizaci paměťových médií. Společnost se člení na divize podle poskytovaných služeb, kdy například divize IBM GTS (Global Technology Services) poskytuje IT služby a řešení v oblasti návrhu, vývoje, implementace, bezpečnosti či správy IT. Divize IBM GBS (Global Business Services) pak poskytuje převážně konzultační služby ("IBM - Czech Republic," 2020).

3.1.3 Oracle

Jedná se o nadnárodní společnost založenou roku 1977 a známou hlavně vývojem relační databáze. Oracle navrhuje, tvoří a prodává jak hardware, tak software. Zároveň nabízí dodatečné služby jako konzultace nebo hostingové služby. V roce 2019 byla podle tržeb druhou největší softwarovou společností ("Oracle," 2020).

3.1.4 Palo Alto Networks

Oproti ostatním relativně mladá společnost působící na světovém trhu od roku 2005. Zaměřuje se na realizaci NGFW (next-generation firewall), který dokáže například detekovat neznámé hrozby za pomoci analytických metod, včetně statické analýzy se strojovým učením a dynamickou analýzou. Mezi další známé produkty patří taky WildFire, což je cloudová služba analýzy hrozeb, kde jsou přijaté soubory a URL spouštěny a analyzovány ve virtuálním prostředí v cloudu ("Palo Alto Networks," 2020). Skrze napadení počítačů virem WannaCry dne 12.5.2017 byla 17.5.2012 do anti-mallware databáze přidána signatura viru ("UPDATED," 2018).

3.1.5 Micro Focus

Jedna z největších softwarových společností na světě založená roku 1976 ve Velké Británii. Produkuje software pro správu a zabezpečení dat, zároveň nabízí poradenství ("Micro Focus," 2020). Na českém a slovenském trhu funguje společnost DNS jako

distributor společnosti Micro Focus. Do jejich portfolia patří jak nástroje pro monitoring a trackování aplikací, tak zálohovací softwary nebo nástroje pro monitoring a vyladění infrastruktury. Konkrétními produkty jsou například SiteScope, Data Protector, VM Explorer, Cloud optimizer a další (“Micro Focus | DNS a.s.,” 2020).

3.1.6 Kaspersky Lab

Kaspersky je mezinárodní společnost zajišťující kybernetickou bezpečnost založená roku 1997. Cílem společnosti Kaspersky je vývoj bezpečnostních služeb pro ochranu podniků, kritické infrastruktury, vlády a spotřebitelů po celém světě. Mezi hlavní produkty patří například antivirus Kaspersky nebo software Kaspersky Internet Security (“Kaspersky,” 2020).

3.1.7 Fortinet

Fortinet – nadnárodní společnost vyvíjející software a spotřebiče pro zajištění kybernetické bezpečnosti. Jeho hlavními produkty jsou například FortiGate, FortiAnalyzer nebo FortiManager.

4 Průzkum v oblasti KB a KI

Pro úspěšné zajištění kybernetické bezpečnosti, je třeba si nejprve ujasnit, proti čemu se vlastně brání. Na čem se výzkumníci shodují je to, že s narůstajícím využitím informačních technologií, se zvyšuje potřeba vyššího zabezpečení. To vede k rozvoji technologií zabezpečení. Mezi ty patří třeba deception technologies (Bushby, 2019). Ke zlepšení přispívá i sdílení informací ohledně kybernetických útoků, které mohou být použity pro zpracování analýzy a následné zvýšení obrany proti daným útokům. (W Chadwick, et al., 2020)

Aby docházelo k útokům co nejméně, je dobré se na tuto problematiku zaměřit již při vývoji. K tomu lze využít například metody modelování hrozeb (threat-modeling methods). Toto opatření umožňuje identifikovat případné hrozby, vytvořit profil potencionálního útočníka a jeho cílů. Jedna z populárnějších variant je metoda STRIDE. (Shevchenko, 2018)

Existuje několik výzkumů, které se zabývají tím, co vše může vést k narušení kybernetické bezpečnosti v podniku. Různé průzkumy kladou větší důraz na různé typy zabezpečení. Všeobecně se ale shodují na několika zásadnějších problémech, které je třeba mít pod kontrolou (Nimesh, 2019).

V takřka všech případech je kladen důraz na narušení bezpečnosti zevnitř podniku, konkrétně skrze zaměstnance firmy. (Kemper, 2019), (Gratian, et al., 2018). Například společnost Clearswift uvádí, že za posledních 12 měsíců měli zaměstnanci na svědomí 52% útoků v organizacích, které čelili úniku dat. (Bunker, 2020) Jedním z problémů je tedy nedostatečná informovanost a proškolení zaměstnanců ohledně problematiky kybernetické bezpečnosti. Jon Fielding též zmiňuje ve své práci, že na základě dotazníků se organizace přiznali k úniku dat způsobeného zaměstnanci. Výsledkem bylo, že 34% dotazovaných organizací uvedlo jako příčinu úniku informací zaměstnance, kteří neúmyslně ohrozily data. Dalších 24% uvedlo jako příčinu zaměstnance, kteří únik dat způsobili záměrně. (Fielding, 2020).

Částečně by tudíž problémy s bezpečností v podniku mohla řešit motivace k aktivnímu podílení na zvýšení bezpečnosti a správná školení zaměstnanců. Ta by je měla seznámit nejen s tím, jak s daty nakládat, ale taky jak se chovat v případě, že mají podezření na nějaký problém.

Mezi další, často zmiňované předměty zkoumání, patří i prevence proti malware, bezpečné uložení vyměnitelných zařízení nebo ochrana proti napadení pomocí SQL injection. (M. Nema, 2019)

Relativně novým pojmem a předmětem zájmu se stal „Cyber hygiene“ (Vishwanath, et al., 2020), který pojednává o návycích koncových uživatelů. S tím souvisí i snaha o zvýšení povědomí ohledně problému kybernetické bezpečnosti.

V rámci kritických infrastruktur se řeší třeba to, jakým způsobem narušení jedné části ovlivní další aspekty kritických infrastruktur (Wróbel, 2019). Kvůli zlepšení odolnosti kritických infrastruktur byla navržena například metoda CIERA (Rehak, et al., 2019). Ta řeší v případě napadení i schopnost obnovení funkčnosti prvků kritických infrastruktur a jejich možnost přizpůsobit se předchozím potížím. Zároveň identifikuje slabá místa.

4.1 Situační povědomí

Do této kapitoly bych chtěla zahrnout i problematiku situačního povědomí. Nedostatečné situační povědomí se totiž považuje za jeden z hlavních prvků, které způsobují nehody vyvolané lidským faktorem.

Situační povědomí či povědomí o situaci je definováno jako vnímání prvků v prostředí uvnitř času a prostoru, pochopení jejich významu a projekce jejich postavení v blízké budoucnosti. Může být tak stručně chápáno jako schopnost vnímání toho, co se děje kolem nás (“Situational Awareness - SKYbrary Aviation Safety,” 2020; “Situational awareness,” 2015). Veškeré naše znalosti, zkušenosti a výchova nám umožňují rozumět tomu, co se děje v naší blízkosti a pomáhá nám rozhodnout, zda je pro nás situace bezpečná.

O tom, jak se v různých situacích zachováme, rozhodují tři prvky situačního povědomí, konkrétně vnímání, porozumění a projekce. Nejdříve dojde k posouzení situace pomocí vnímání a pozornosti. Následuje interpretace posouzení situace, tedy její porozumění. Vědění, jak se situace nejspíše vyvine, je projekce. Na základě těchto prvků dojde k celkovému vyhodnocení situace a vytvoření základu pro správné rozhodnutí.

Důležitost situačního povědomí se odrazila i v legislativě. Za relativně nedávný příklad lze považovat koronavirovou epidemii. Kvůli ní vzniklo například Společné sdělení evropskému parlamentu, evropské radě, radě, hospodářskému a sociálnímu výboru

a výboru regionů jakožto boj proti dezinformacím o COVID-19 (“EUR-Lex - 52020JC0008 - EN - EUR-Lex,” 2020). Kromě vzájemnému sdílení informací mezi členskými státy se navrhly i možnosti, jak zlepšit povědomí o situaci u občanů. V relativně nové situaci se totiž začalo šířit obrovské množství zpráv z pochybných zdrojů, které byly v některých případech až nebezpečné. Jednalo se o zprávy, že mytí rukou nepomáhá, nebo že 5G způsobuje COVID, což vedlo k útokům na vysílače a k všeobecně horšímu potlačení epidemie.

V běžném životě se například bezpečnostní analytik stará o kybernetickou bezpečnost. U něj se zkrátka předpokládá, že má značné povědomí o situaci. Je zodpovědný za to, že neustále studuje oblast hrozeb a dává pozor na případné hrozby vůči organizaci. Současně stále řeší otázky jako „Probíhá tu v tuto chvíli nějaký útok?“, „Pokud ano, jaký je momentální stupeň narušení a kde je útočník?“. Nicméně zrovna v případě kybernetické bezpečnosti je stále složitější, aby fyzické osoby udržovaly dostatečné povědomí. Není tedy neobvyklé využívat umělou inteligenci, či různé frameworky, které mohou do jisté míry značně pomoci (“(PDF) An Integrated Framework for Cyber Situation Awareness,” 2017; “(PDF) Autonomy in use for space situation awareness,” 2019; “(PDF) Cyber Situational Awareness,” 2015).

Ve světě lze najít poměrně velké množství různých studií, které buď charakterizují situační povědomí či ho v různých směrech aplikují tak, aby se v konkrétních případech dosáhlo lepších výsledků. Velmi často se aplikuje v boji, což je logické už jen z důvodu, že jedny z prvních zmínek o situačním povědomí pocházejí z období první světové války (“Povědomí o situaci - Situation awareness - qwe.wiki,” 2020). Byla to totiž jedna z nutných dovedností u posádky vojenských letadel. Život pilotů letadel jasně závisel na tom, jak moc dobře pozorují nepřátelská letadla a jak dobře odhadnou jejich příští pohyb (“(PDF) A Visualization Technique to Improve Situational Awareness,” 2018; “(PDF) Situation awareness,” 1999). Později bylo situační povědomí popsáno jako tři za sebou jdoucí úrovně, konkrétně již zmíněné vnímání, porozumění a projekce.

Zlepšení situačního povědomí se vyplatilo i u studentů v Anglii studujících medicínu. Ti se během prvních dvou týdnů naučili klinickým dovednostem. I WHO (Světová zdravotnická organizace) souhlasila s přístupem, kdy se od začátku tréninku studenti věnují znalostem a dovednostem v lidských faktorech. Věří se tomu, že pokud se již ze začátku naučí lépe vnímat a chápat co se děje kolem nich, mohou lépe plánovat dopředu,

případně mohou přijmout opatření ke zmírnění nebo dokonce odstranění možných rizik. Při testování studentů se výsledky potvrdily a celková zpětná vazba byla velmi pozitivní (“(PDF) Innovative teaching in situational awareness,” 2015; Schulz et al., 2013).

5 Praktická část

Po bližším vysvětlení různých prvků kybernetické bezpečnosti, se budu dále zabývat tím, jakým způsobem jednotlivé faktory ovlivňují celkovou kybernetickou bezpečnost podniku.

5.1 Metodika

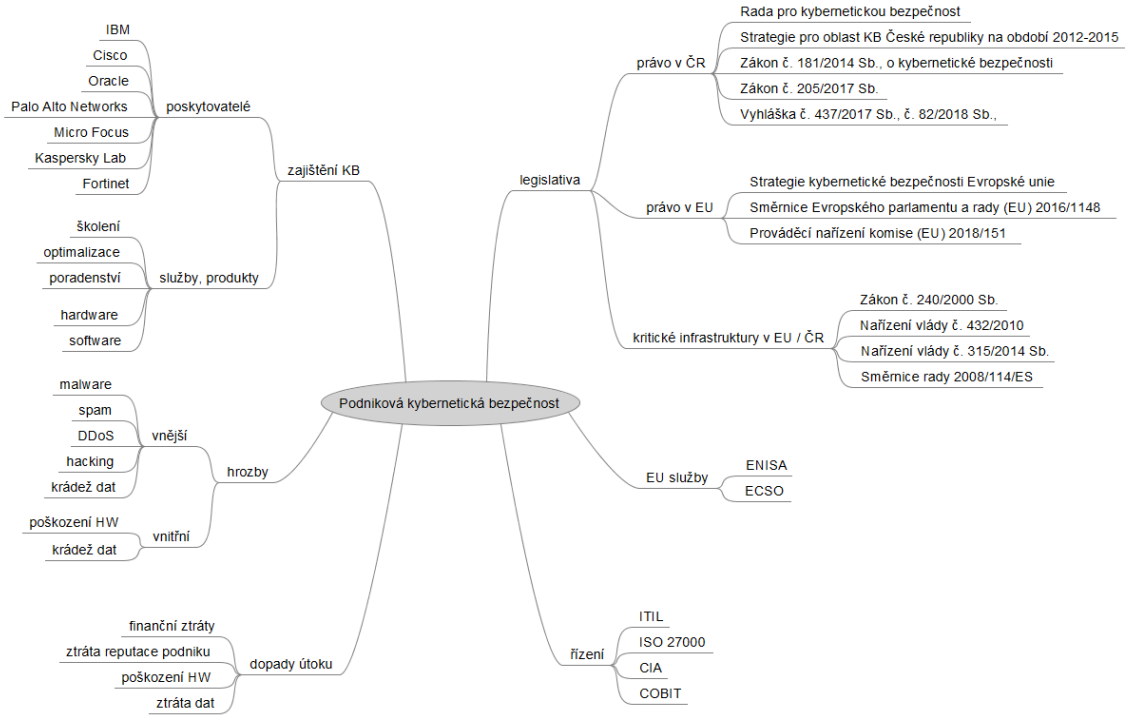
Součástí metodiky byla rozsáhla literární rešerše, která umožnila získat dostatek informací potřebných pro vytvoření jednotlivých částí praktické práce. Díky této rešerši jsem mohla postupně zformulovat kvalitativní modely, tedy dynamické hypotézy a CL diagram. Některé hypotézy jsem pak ověřila kvantitativně za pomoci modelu.

Začala jsem s myšlenkovou mapou, která jednoduchým grafickým znázorněním shrnuje získané poznatky z rešerše. Na tu jsem navázala rozdělením faktorů ovlivňujících podnik na vnitřní a vnější. Zde už se objevují smyčky, které určují zpětnou vazbu mezi jednotlivými prvky podniku.

Dále jsem pokračovala tvorbou systémového diagramu. V něm jsem se pokusila implementovat kybernetickou bezpečnost do nástroje BSC (Balanced scorecard). Určité předpoklady jsem pak začlenila do dynamických hypotéz. Na hypotézy jsem navázala diagramem kauzálních smyček (CL diagram), který je obohacenou variantou systémového diagramu. Zároveň zahrnuje podmínky vycházející z dynamických hypotéz. Nakonec jsem pravdivost dynamických hypotéz ověřila za pomoci zjednodušeného modelu vytvořeného díky simulačnímu nástroji InsightMaker.

5.2 Myšlenková mapa

Pro lepší přehled jsem ze získaných informací zpracovala myšlenkovou mapu. Ta obsahuje hlavní složky kybernetické bezpečnosti podniku. Součástí jsou jak různé druhy hrozeb, tak jejich hlavní dopady. Aby se podnik dokázal co nejlépe ubránit těmto hrozbám, či minimalizovat jejich dopady, je potřeba využít různých způsobů zabezpečení. Na tuto mapu jsem pak navázala tvorbou diagramu. Myšlenkovou mapu by šlo jistě rozšířit o další komponenty, avšak z důvodu přehlednosti jsem ji již dále nerozšiřovala.



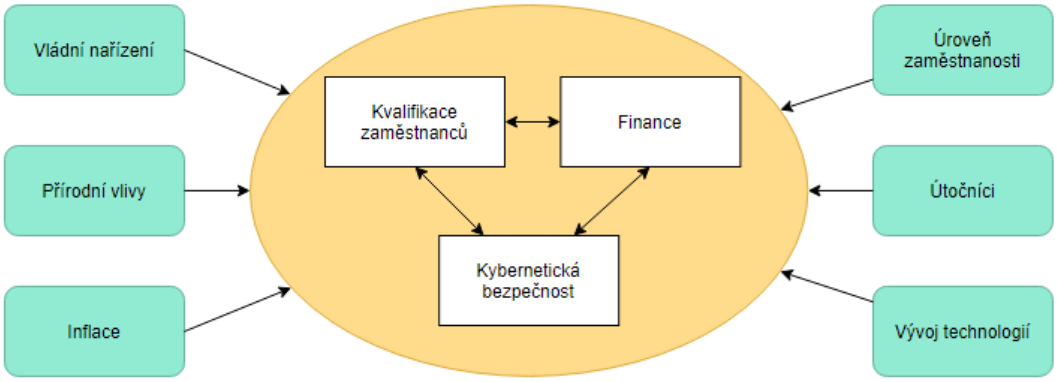
Obrázek 5 - Myšlenková mapa kybernetické bezpečnosti podniku (vlastní tvorba)

5.3 Vnější a vnitřní faktory

Aby se snáze chápal vliv jednotlivých faktorů působících na podnik, určila jsem vnější a vnitřní faktory. Vnější faktory tak na podnik působí a ovlivňují jeho fungování, ale sám o sobě je podnik nemá jak ovlivnit. Naproti tomu vnitřní faktory jsou podnikem ovlivnitelné. Takových faktorů může být mnoho, avšak vybrala jsem jen některé. Konkrétně ty, které mají z mého pohledu největší vliv. Pro určení převážně vnějších faktorů jsem využila PESTLE analýzu. Tu jsem částečně využila spolu se SWOT analýzou pro určení i vnitřních faktorů.

- Zelenou barvou jsem označila faktory vnější, tedy ty, které podnik nemůže přímo ovlivnit. Mohou to tak být různí útočníci, přírodní katastrofy, státem vydaná nařízení a další.

- Oranžovou barvou jsem pak vyznačila samotný podnik. Ten se skládá z několika vnitřních faktorů. Podnik je může přímo ovlivnit a jednotlivé vnitřní faktory mají na sebe vzájemný vliv. Například dostatečná kvalifikace zaměstnanců povede ke zlepšení kybernetické bezpečnosti. Ta pak může zamezit případným útokům, které by vedly k finančním ztrátám.



Obrázek 6 - Vnější a vnitřní faktory podniku (vlastní tvorba)

5.4 Systémový diagram

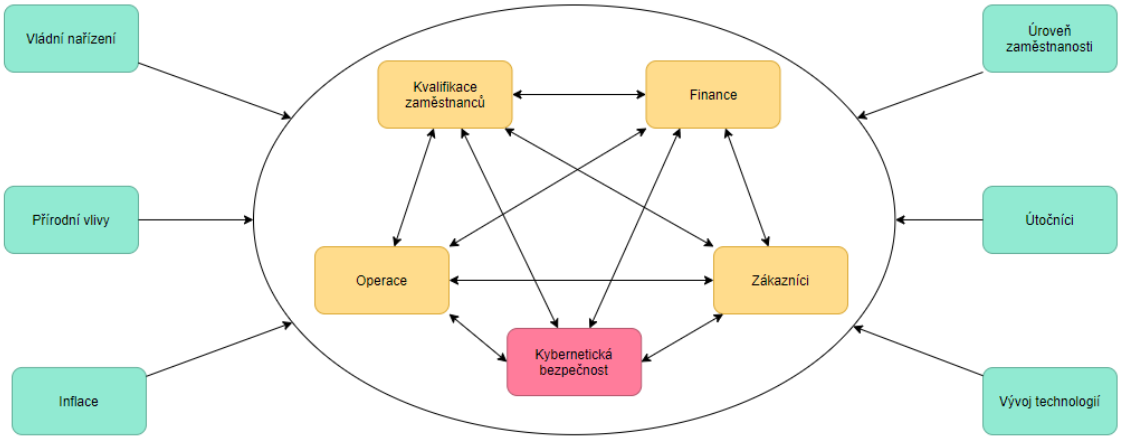
Pro další práci jsem vycházela z balanced scorecard (BSC), což je nástroj pro řízení výkonnosti firmy. Ten posuzuje výkonnost podniku podle čtyř sektorů. Těmi jsou finance (Financial), zákazník (Customer), interní a podnikové procesy (Internal Process) a nakonec učení se a růst (Learning and Growth).

Obrázek 7 - Čtyři sektory nástroje BSC (https://balancedscorecard.org/bsc-basics-overview/)

V rámci projektu se došlo k tomu, že by do těchto sektorů měla být zahrnuta i kybernetická bezpečnost místo toho, aby byla pouze součástí řízení rizik, jak je tomu do teď. Jedním z důvodů je skutečnost, že kybernetická bezpečnost značně ovlivňuje části

zmíněných sektorů BSC. Vytvořila jsem tedy zjednodušenou formu systémového diagramu, který implementuje kybernetickou bezpečnost k ostatním sektorům BSC.

K vyznačení subsystémů spadajících do BSC jsem použila oranžovou barvu. Červenou jsem pak zvýraznila samostatně kybernetickou bezpečnost, implementovanou do BSC. Všechny tyto sektory mezi sebou vzájemně komunikují a působí na ně již zmiňované vnější vlivy.



Obrázek 8 - Systémový diagram (vlastní tvorba)

5.5 Dynamické hypotézy

Dále jsem vytvořila konkrétní dynamické hypotézy. Zde mě zajímá *produktivita*, kterou berou jako souhrn kvalitativních a kvantitativních ukazatelů ze čtyř zmíněných sektorů BSC. Předpokladem je, že v ideálním případě se postupně zvyšuje produktivita podniku a snaží se tak dosáhnout maximální hodnoty 100%. Čím víc se blíží této hodnotě, tím obtížněji se navyšuje. V praxi ale k útokům dochází a ty pak tuto produktivitu nepříznivě ovlivňují.

V rámci hypotéz předpokládám, že pokud je míra zabezpečení dostatečná, pak se podnik s útokem vypořádá rychleji a případné dopady budou minimalizovány. Naopak, pokud bude míra zabezpečení velmi nízká či nulová, útok o dostatečné síle značně ovlivní produktivitu podniku, případně může být pro něj fatální.

- Hypotéza 1 (H1) – Podnik kybernetickou bezpečnost prakticky neřeší nebo do ní neinvestuje systematicky. Takřka jakýkoliv úspěšný útok bude mít velmi negativní dopad, ze kterého se podnik bude jen těžko vzpamatovávat. Pokud se

jedná o silnější útok, pak jsou jeho následky natolik vážné, že může dojít i k zániku podniku.

- Hypotéza 2 (H2) – Alespoň drobná míra zabezpečení pomůže zmírnit dopady útoku natolik, že se z něj podnik vzpamatuje. Případně alespoň zabrání dalšímu klesání produktivity a tím i zániku podniku.
- Hypotéza 3 (H3) – Přiměřená míra zabezpečení dokáže relativně snadno eliminovat případný útok a jeho následky. S útokem se vypořádá rychle a zanedlouho se obnoví i jeho původní produktivita.
- Hypotéza 4 (H4) – Teoreticky může dojít k „přezabezpečení“ podniku. Tato hypotéza počítá s tím, že podnik je maximálně zabezpečen a ze všech případů se s hrozbou vypořádá nejrychleji. Avšak taková míra zabezpečení je už příliš nákladná, což může o něco zpomalit nárůst produktivity.

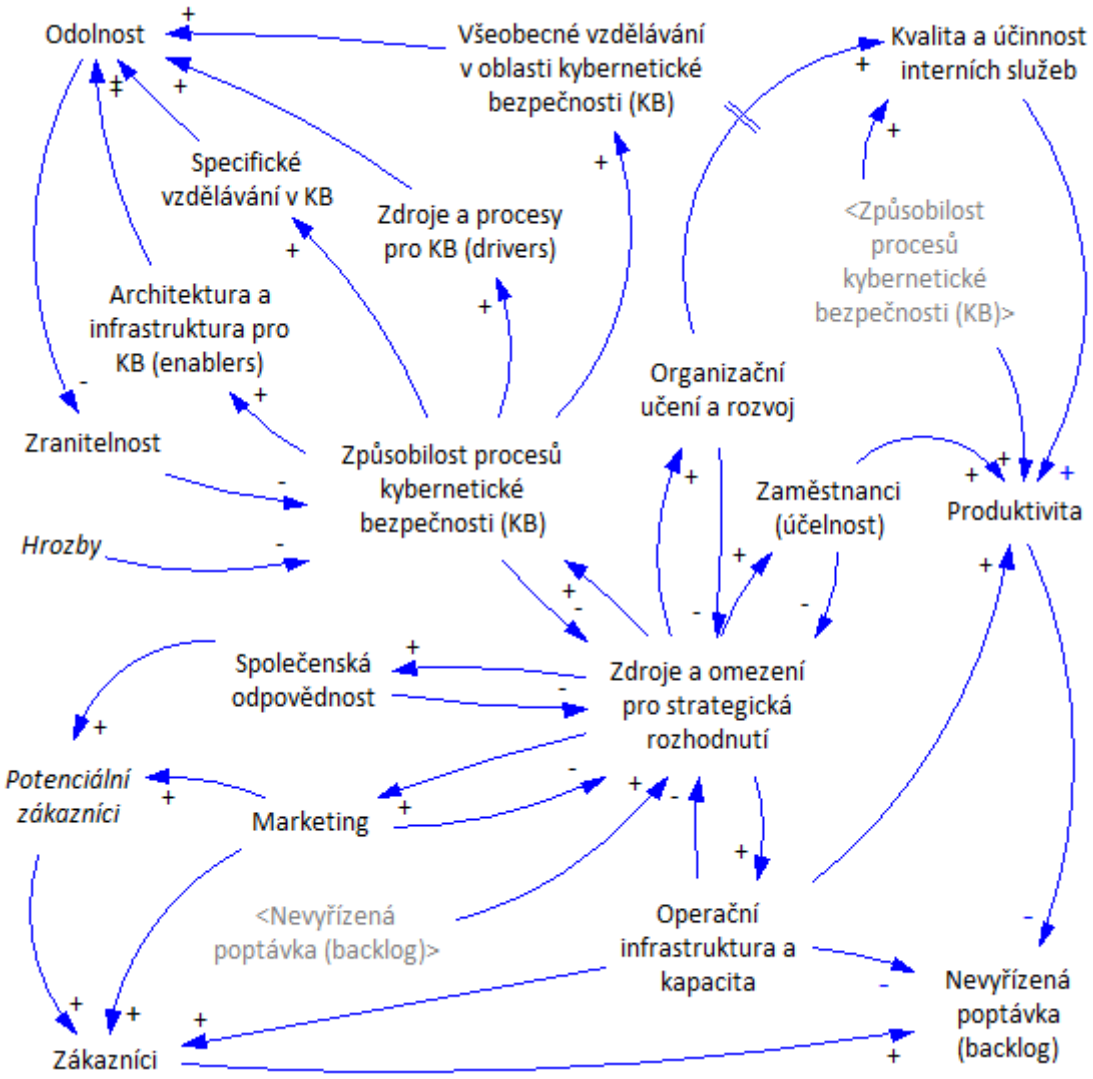
5.6 CL diagram

Následovala tvorba diagramu kauzálních smyček (CL diagramu), jenže je rozšířenou variantou systémového diagramu a zároveň navrhuje podmínky pro dynamické hypotézy zmíněné výše. Výsledný CL diagram je převzat ze závěrečné zprávy projektu.

Konkrétní hodnoty jednotlivých kritérií se vzájemně liší podle dostupných financí, získaných z nevyřízených poptávek (backlog). Zároveň jsou ovlivněny konkrétní kombinací objednávek, technologií a produktivitou. Produktivita se skládá z kvalitativní a kvantitativní části, kde kvalitativní část zahrnuje efektivitu získanou díky celkovému vzdělávání a rozvoji týmové spolupráce. Kvantitativní část pak zahrnuje zaměstnance a změny v infrastruktuře.

Celkově lze diagram teoreticky rozdělit do několika sektorů. Mezi ně patří například marketing. Ten se sám o sobě zabývá pouze přilákáním dalších zákazníků. Naproti tomu společenská odpovědnost zahrnuje společenské aspekty ovlivňující jak podnik, tak zákazníky, a to ve formě politických, ekonomických, sociálních, technologických, legislativních a ekonomických faktorů (PESTLE). Společenská odpovědnost má tak všeobecně široký vliv jak na podnik samotný, tak na jeho stakeholdery a veřejnost. Tato forma udržování dobrých vztahů s veřejností a stakeholdery vede ke zlepšení reputace a důvěryhodnosti podniku. A tím i k jeho ziskovosti.

Dalším takovým sektorem je způsobilost procesů kybernetické bezpečnosti. Ta má své vlastní smyčky, které určují konkrétní míru odolnosti a zranitelnosti podniku.



Obrázek 9 - Diagram kauzálních smyček (CL diagram)

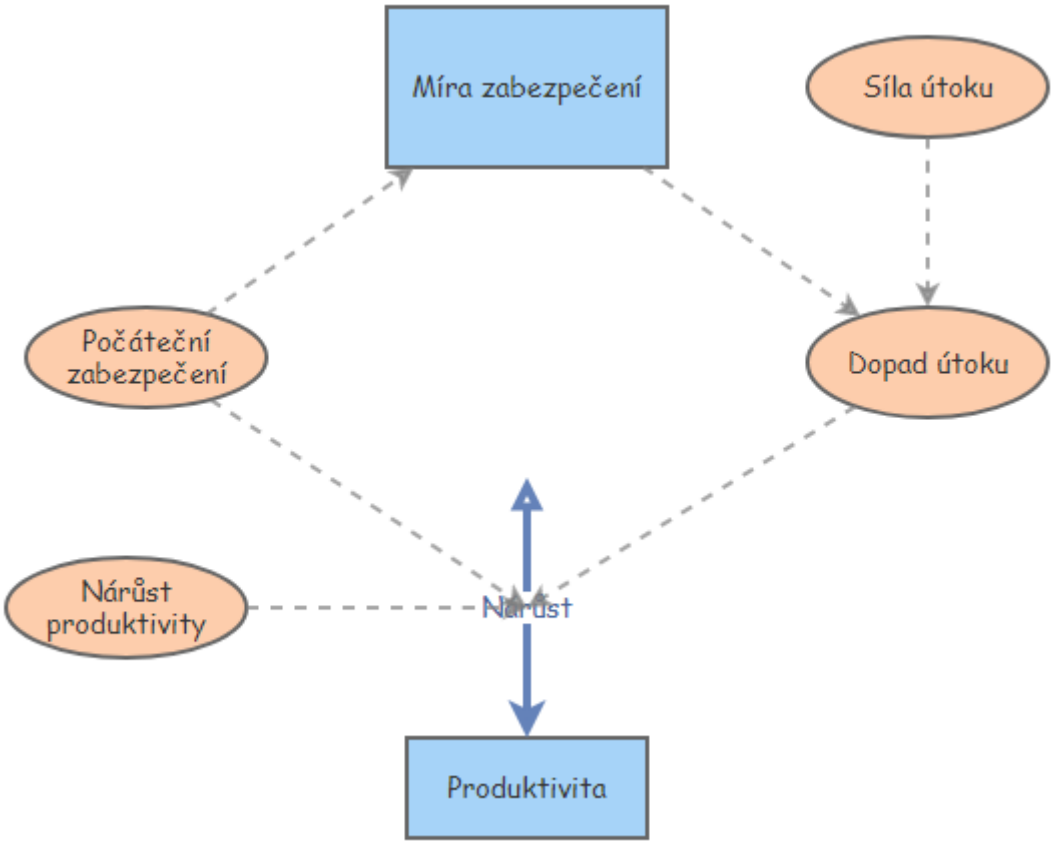
Samotná kybernetická bezpečnost tak tvoří celkem několik smyček:

- KB → Zdroje a omezení pro strategická rozhodnutí → KB
- KB → Specifické vzdělávání v KB → Odolnost → Zranitelnost → KB
- KB → Všeobecné vzdělávání v oblasti KB → Odolnost → Zranitelnost → KB
- KB → Zdroje a procesy pro KB (drivers) → Odolnost → Zranitelnost → KB
- KB → Architektura a infrastruktura pro KB (enablers) → Odolnost → Zranitelnost → KB

- KB → Kvalita a účinnost interních služeb → Produktivita → Nevyřízená poptávka (backlog) → Zdroje a omezení pro strategická rozhodnutí → KB

5.7 Výsledky

Protože je CL diagram čistě kvalitativní model, pokusila jsem se dynamické hypotézy ověřit i kvantitativně za pomoci modelu vytvořeného v nástroji InsightMaker.



Obrázek 10 - Model (vlastní tvorba)

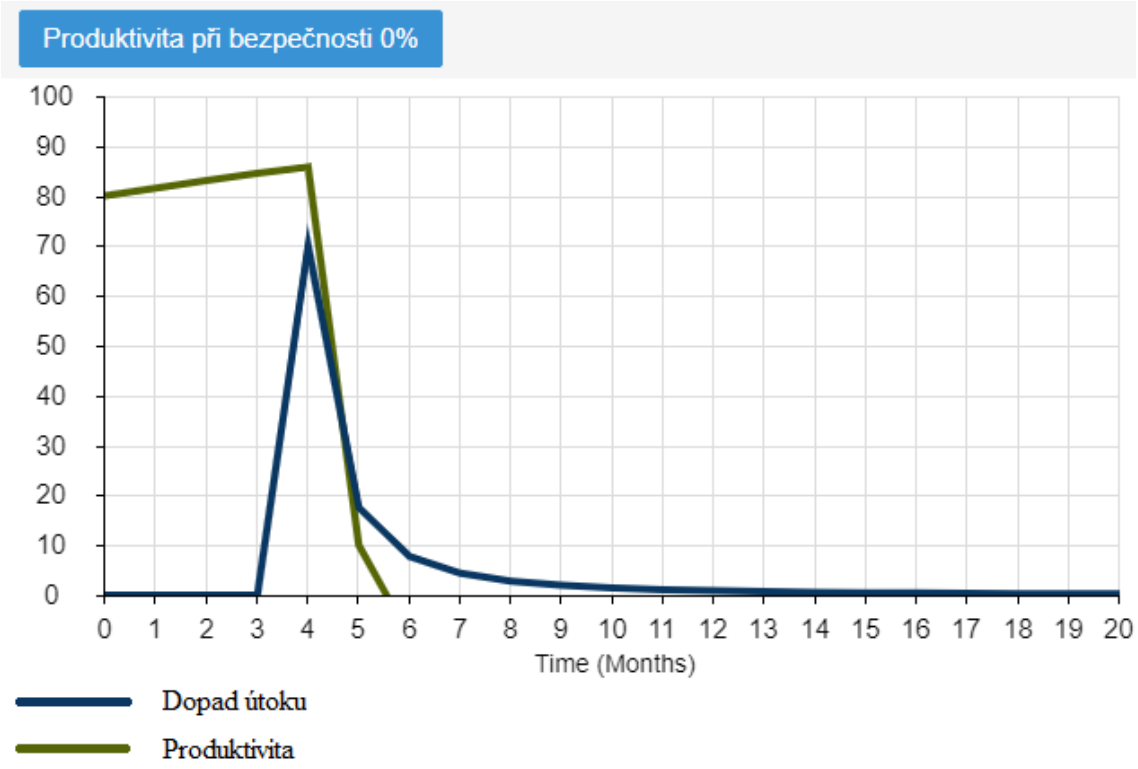
Tento model se skládá z několik prvků, v mém případě z míry zabezpečení a produktivity podniku a z několik dalších proměnných. Míra zabezpečení je dána nastavenou hodnotou, která se odvíjí od množství a úrovně využitých bezpečnostních prvků. Těmi mohou být například zaměstnanci vzdělaní v oblasti kybernetické bezpečnosti, využití moderních technologií, pravidelná údržba HW a SW a další.

Produktivita se za optimálních okolností pomalu navyšuje. V případě útoku je produktivita ovlivněna mírou zabezpečení a dopadem útoku. Dopad útoku se pak mění

v závislosti na jeho celkové síle a na míře zabezpečení. Síla útoku může být ovlivněna například jeho druhem či celkovou komplexností. Kvůli zachování jednoduchosti simulace jsem nezahrnula možnou proměnnou finance, která by podle míry využití limitovala nárůst produktivity. Zahrnutí využití financí vychází z předpokladu že podniky, které prakticky do bezpečnosti neinvestují, sice jednorázově ušetří, ale v případě úspěšného útoku pak mnohem víc ztrácí kvůli rozsáhlejším následkům a naopak. V zjednodušené formě jsem tedy tuto skutečnost zahrnula jen jako součást rovnice pro výpočet produktivity. Pro přehlednější zobrazení jsem nechala v grafech viditelné dvě hodnoty, konkrétně dopad útoku a produktivitu.

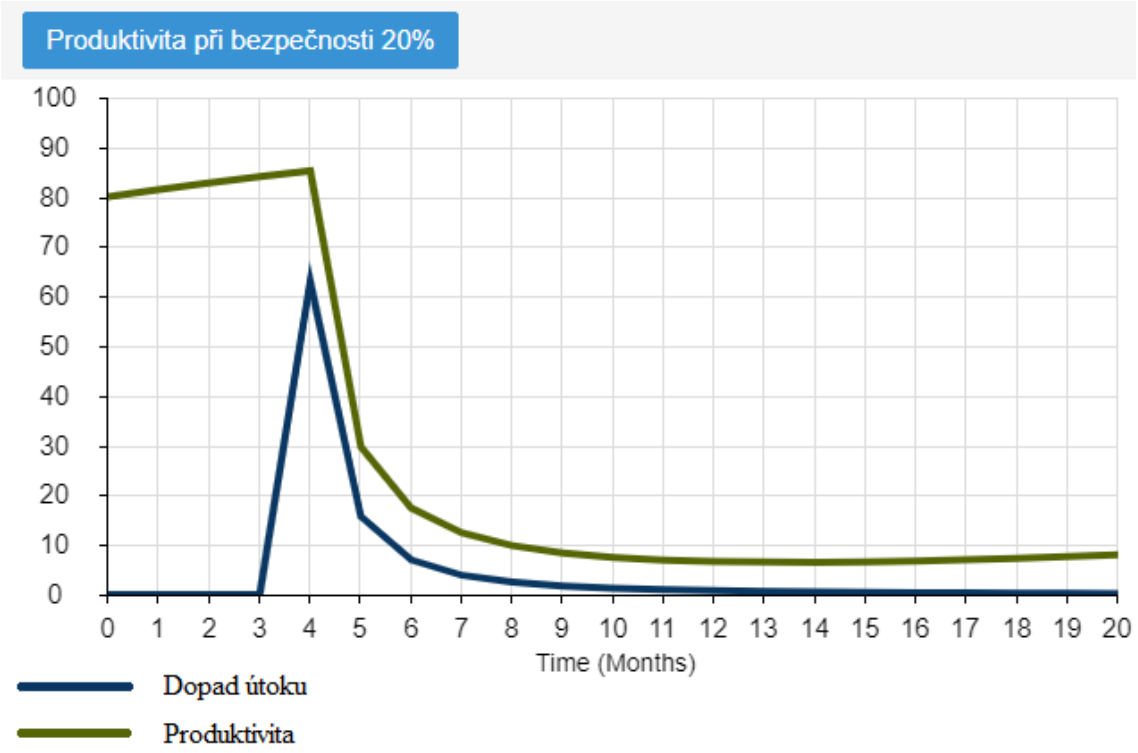
Při všech simulacích mám použitý identický časový horizont – 20 měsíců. V každé z hypotéz podnik začíná na produktivitě 80%. Ve všech případech mám také nastavený stejně silný útok, který proběhne ve 4. měsíci simulace a jeho následky postupně odeznívají. Jak se během této doby s útokem podnik vypořádá, to je ovlivněno mírou zabezpečení a silou útoku.

- V případě H1 se počítá s bezpečností na hodnotě 0. Dokud neproběhl útok, produktivita narůstala nejrychleji ze všech případů. Avšak úspěšný útok měl kvůli nulovému zabezpečení obrovské dopady, a než zcela odezněl, podniku kvůli příliš rozsáhlým dopadům klesla produktivita na 0, čímž by podnik v praxi zanikl.



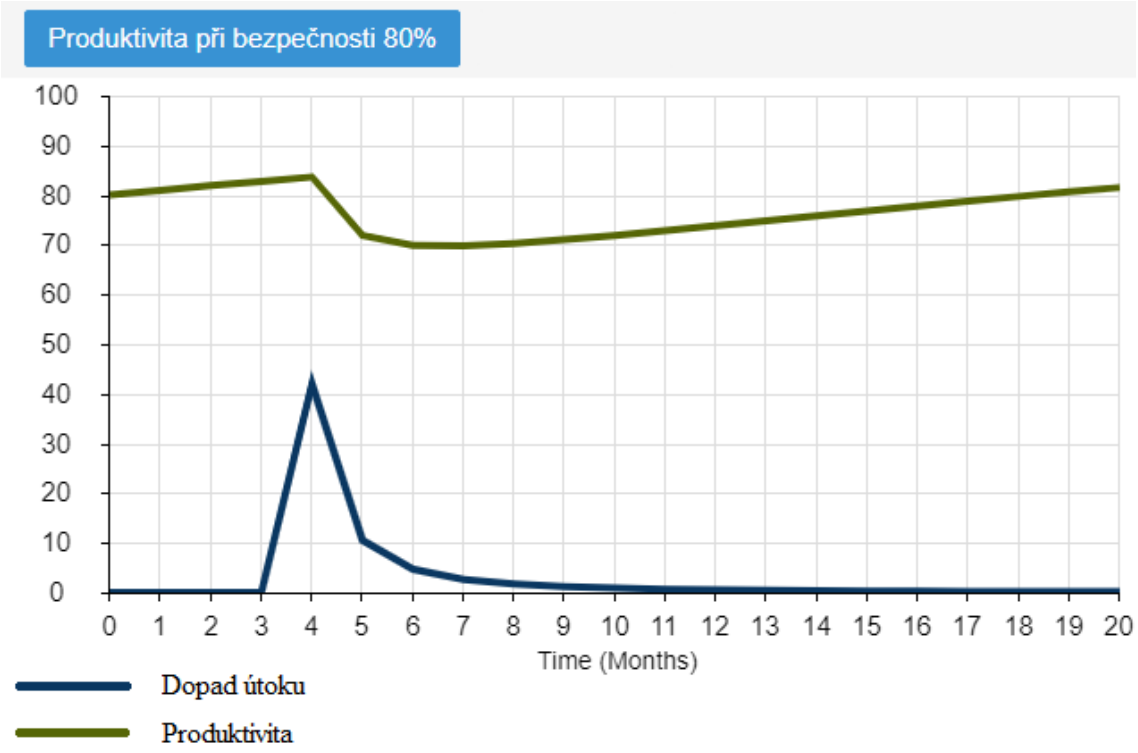
Graf 1 - Hypotéza 1

- V případě H2 se počítá s bezpečností na hodnotě 20. Dokud neproběhl útok, produktivita narůstala. Nicméně i zde měl úspěšný útok rozsáhlé dopady, avšak díky alespoň mizivému zabezpečení se produktivita stabilizovala a po dostatečně dlouhé době, by se podnik mohl i vzpamatovat. Avšak další podobně rozsáhlý útok by mohl být i zde fatální. Taková forma zabezpečení je tedy sice lepší než žádná, ale rozhodně není optimální.



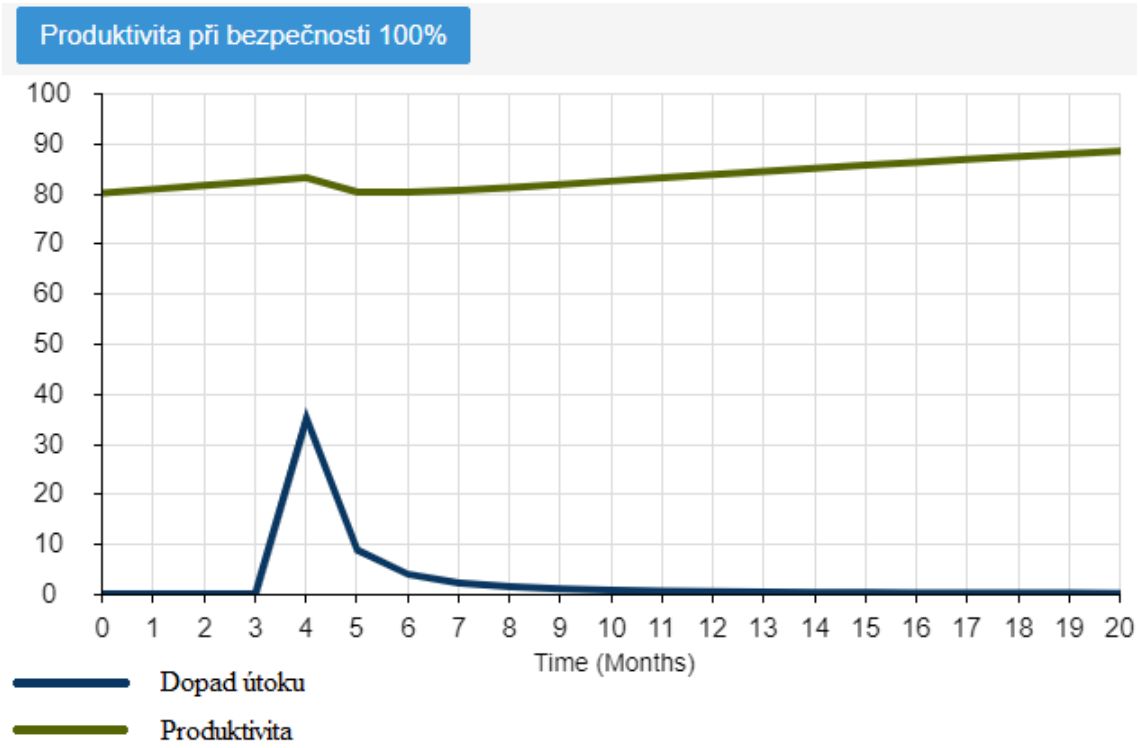
Graf 2 - Hypotéza 2

- V případě H3 se počítá s bezpečností na hodnotě 80. Zde je již vidět značný rozdíl oproti předchozím hypotézám. Dopad útoku byl o hodně menší, což způsobilo, že produktivita nebyla tak negativně ovlivněna, jako tomu bylo v ostatních případech. Podnik se tedy s útokem vypořádal velmi dobře. Produktivita brzy přestala klesat a začala se pomalu vracet do původních hodnot.



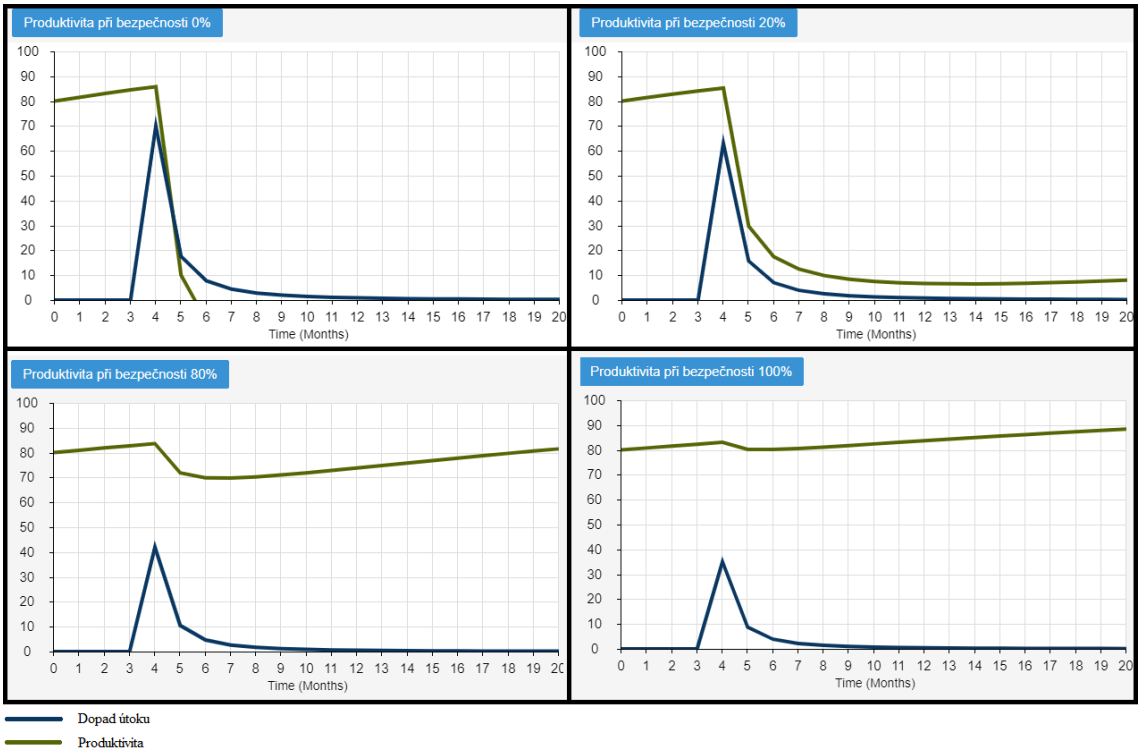
Graf 3 - Hypotéza 3

- V případě H4 se počítá s bezpečností na hodnotě 100. Ačkoliv to z počáteční hodnoty produktivity 80 není nejzřetelnější, v tomto případě sice také produktivita narůstá, avšak nejpomaleji ze všech hypotéz. To je dáno předpokladem, že si podnik udržuje bezpečnost na skoro až zbytečně vysoké úrovni, což zpomaluje jeho celkový růst. Nicméně ze všech případů se zde podnik vyrovnal s útokem a jeho dopady nejlépe. Začal se tak nejdřív vracet do původních hodnot produktivity.



Graf 4 - Hypotéza 4

Pro přehlednější porovnání jednotlivých výsledků přikládám obrázek s výsledky všech čtyř hypotéz najednou.



Obrázek 11 - Srovnání výsledků hypotéz

6 Diskuze

Výsledky z vytvořených modelů podle mě z větší části potvrdili přepokládané výsledky hypotéz. Tedy že v případě úspěšného útoku se podnik s vyšší mírou zabezpečení dokáže mnohem lépe vyrovnat s jeho případnými následky. Podniky s dostatečným zabezpečením se s úspěšným útokem vypořádaly rychleji než podniky se zabezpečením žádným nebo minimálním. Dopad útoku byl také o hodně menší a celkově se na produktivitě podniku neprojevil tak markantně, jako tomu bylo v případech nedostatečného zabezpečení.

Pokud by se tedy mizivá bezpečnost týkala podniku, který je prvkem kritické infrastruktury, následky by mohly být fatální. Úspěšný útok by mohl v některých případech podnik zcela vyřadit z provozu. Problematické jsou tak bohužel občas nemocnice, které mají někdy značně zastaralé způsoby zabezpečení a v případě útoku trvá příliš dlouho, než se s ním vypořádají, nemluvě o způsobených komplikacích.

Kromě zastaralých způsobů zabezpečení, která mnohdy nejsou adekvátní vůči možným hrozbám a jejich následkům, stále zůstává jedním z největších problémů nedostatečné proškolení zaměstnanců podniku. Moderní technologie se týkají nás všech a již dávno není jen a pouze na IT oddělení, aby se starali o kybernetickou bezpečnost. Zvyšování povědomí o problematice kybernetické bezpečnosti je tedy na místě jak mezi zaměstnanci podniku, tak mezi běžnými občany.

I když nové technologie sice v mnoha směrech zlepšují kvalitu života a chod podniku, s jejich využitím přichází stále více příležitostí k útoku z různých směrů. Nicméně kybernetická bezpečnost se často řeší tak, že podnik použije nějakou část financí, například 5% rozpočtu a dál se nestará, jestli to stačí, jak je s těmito financemi naloženo apod. Skrze využívání technologií by se ale kybernetická bezpečnost měla dostat na stejnou úroveň, jako je třeba marketing, výroba a další, poněvadž se stává neméně důležitou součástí podniku a její zanedbání může podnik vyřadit ze dne na den. Tomu by šlo pomoct právě zahrnutím kybernetické bezpečnosti do standartních podnikových architektur.

Závěr

Jedním z cílů bakalářské práce bylo upozornění na následky z úspěšného útoku na podnik, jenž je prvkem kritické infrastruktury. Zároveň jsem chtěla poukázat na možná řešení, která by pomohla těmto následkům předejít nebo alespoň zmírnila dopady. Toho jsem postupně dosáhla nejprve důkladnějším seznámením s problematikou kybernetické bezpečnosti celkově. Ta se skládala z několik částí, mezi něž patřilo rozebrání některých typů útoků, klady a zápory nových technologií či legislativa související s danou problematikou.

Z průzkumu se také potvrdila skutečnost, že jedním z nejčastějších zdrojů úspěšného útoku je skrze zaměstnance podniku. Jejich školení a vzdělávání v této problematice je nezbytnou součástí prevence útoku a jeho včasné identifikace. Podnik se díky tomu stane celkově odolnějším vůči kybernetickým útokům. Dokáže na ně včas reagovat a zmenšit tak případné následky, které plynou z narůstajících pokusů o narušení kybernetické bezpečnosti ať zevnitř nebo z vně podniku.

Systematickým procházením různých zdrojů a výzkumných prací, jsem se dozvěděla dostatek informací potřebných k tvorbě diagramu a následného modelu, použitého pro simulaci konkrétních situací. Myslím si, že stanovené cíle se mi z větší části povedlo splnit.

Za pozitivní vliv této práci považuji to, že jsem se mnohem lépe seznámila s problematikou kybernetické bezpečnosti kritických infrastruktur. Zároveň jsem si vyzkoušela modelaci dynamických hypotéz. Protože se u mě jednalo o poměrně novou zkušenost, tak je sice model řešen poněkud zjednodušeně, ale pro demonstraci doufám postačil.

Seznam použité literatury

About ENISA - The European Union Agency for Cybersecurity [WWW Document], 2020. URL https://www.enisa.europa.eu/about-enisa/about-enisa (accessed 12.6.20).

AI Security Definition & Examples, 2021. . Awake Secur. URL https://awakesecurity.com/glossary/ai-security/ (accessed 4.27.21).

Alexander, D., 2018. A magnitude scale for cascading disasters. Int. J. Disaster Risk Reduct. 30, 180–185. https://doi.org/10.1016/j.ijdrr.2018.03.006

Bruce Schneier Quote [WWW Document], n.d. . -Z Quotes. URL https://www.azquotes.com/quote/570039 (accessed 10.28.20).

CADEK, M., 2020. Zabezpečení sítí 5G: Evropská komise připravuje nová opatření [WWW Document]. Czech Repub. - Eur. Comm. URL https://ec.europa.eu/czech-republic/news/200129_5g_cs (accessed 11.28.20).

Cisco - Global Home Page [WWW Document], n.d. . Cisco. URL https://www.cisco.com/c/en/us/index.html (accessed 1.15.20).

CISSP – the CIA Triad and its opposites., 2017. . ThorTeaches CISSP CISM PMP Train. URL https://thorteaches.com/cissp-the-cia-triad-and-its-opposites/ (accessed 10.28.20).

Cities, P.T.I. has released an I.S.F. for S., Things, C.I.| iotosphere-Internet of, 2019. IoT Security Framework. Create Cult. Innov. IIoT World. URL https://iiot-world.com/industrial-iot/connected-industry/the-iotsi-has-released-an-iot-security-framework-for-smart-cities-and-critical-infrastructure/ (accessed 12.1.20).

Cybersecurity Courses [WWW Document], 2018. . Netw. Acad. URL https://www.netacad.com/courses/cybersecurity (accessed 11.25.20).

Cyberspace Operations Concept Capability Plan 2016-2028, n.d. 77.

Digitální Česko [WWW Document], 2020. URL https://www.digitalnicesko.cz/zakladni-informace/ (accessed 12.3.20).

Digitální ekonomika [WWW Document], 2017. URL https://docplayer.cz/38026055-1-digitalni-ekonomika.html (accessed 12.2.20).

ECSO - European Cyber Security Organisation [WWW Document], n.d. . ECSO - Eur. Cyber Secur. Organ. URL https://ecs-org.eu/about (accessed 4.6.21).

EUR-Lex, 2016. 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, 194.

EUR-Lex, 2013. EUR-Lex - 52013JC0001 - EN - EUR-Lex [WWW Document]. URL https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=JOIN:2013:0001:FIN (accessed 2.22.20).

EUR-Lex - 02004R0460-20110625 - EN - EUR-Lex [WWW Document], n.d. URL https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A02004R0460-20110625 (accessed 12.6.20).

EUR-Lex - 52004DC0702 - CS [WWW Document], n.d. URL https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52004DC0702&from=EN (accessed 9.8.20).

EUR-Lex - 52020JC0008 - EN - EUR-Lex [WWW Document], n.d. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1599057203265&uri=CELEX:52020JC0008 (accessed 9.2.20).

FBI — Operation “Phish Phry” [WWW Document], n.d. URL https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709 (accessed 11.12.20).
February 28th DDoS Incident Report, 2018. . GitHub Blog. URL https://github.blog/2018-03-01-ddos-incident-report/ (accessed 11.13.20).
Gartner [WWW Document], 2021. . Gartner. URL https://www.gartner.com/en (accessed 4.27.21).
Gartner’s 2020 Trends [WWW Document], 2019. . Solace. URL https://solace.com/blog/event-driven-architecture-gartner-top-tech-trends/ (accessed 4.27.21).
Hlavní cíle koncepce Digitální ekonomika a společnost | MPO [WWW Document], 2019. URL https://www.mpo.cz/cz/podnikani/digitalni-spolecnost/hlavni-cile-koncepce-digitalni-ekonomika-a-spolecnost--243491/ (accessed 12.3.20).
Home - BRAIN-IoT, 2018. URL http://www.brain-iot.eu/ (accessed 12.1.20).
IBM - Czech Republic [WWW Document], n.d. URL https://www.ibm.com/cz-en (accessed 1.15.20).
Implementace a rozvoj sítí 5G v České republice | MPO [WWW Document], 2020. URL https://www.mpo.cz/cz/e-komunikace-a-posta/elektronicke-komunikace/koncepce-a-strategie/narodni-plan-rozvoje-siti-nga/implementace-a-rozvoj-siti-5g-v-ceske-republice-_-cesta-k-digitalni-ekonomice--252026/ (accessed 11.30.20).
Kaspersky [WWW Document], n.d. URL https://www.kaspersky.com/ (accessed 1.15.20).
Kolouch, J., 2007. kyberneticke_utoky.pdf [WWW Document]. URL https://csirt.cesnet.cz/_media/cs/documents/kyberneticke_utoky.pdf (accessed 11.9.20).
Kolouch, J., Bašta, P., 2019. CyberSecurity.
Kyberútok - Nemocnice Benešov, n.d. URL https://centrumkyberbezpecnosti.cz/kyberutok-na-nemocnici-v-benesove-nefunguji-zadne-pristroje/ (accessed 4.9.21).
Legislativa [WWW Document], 2014. URL https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/ (accessed 2.28.20).
Lezzi, M., Lazoi, M., Corallo, A., 2018. Cybersecurity for Industry 4.0 in the current literature: A reference framework. Comput. Ind. 103, 97–110. https://doi.org/10.1016/j.compind.2018.09.004
ManagementMania, 2017. Digitální Ekonomika (Digital Economy) [WWW Document]. ManagementMania.com. URL https://managementmania.com/cs/digitalni-ekonomika-digital-economy (accessed 12.2.20).
ManagementMania, n.d. COBIT 5 [WWW Document]. ManagementMania.com. URL https://managementmania.com/cs/cobit-control-objectives-for-information-and-related-technology (accessed 4.13.21).
Micro Focus | DNS a.s. [WWW Document], n.d. URL https://www.dns.cz/vyrobci/micro-focus (accessed 1.15.20).
Micro Focus [WWW Document], n.d. URL https://www.microfocus.com/en-us/home (accessed 1.15.20).
Národní centrum kybernetické bezpečnosti [WWW Document], n.d. URL https://nukib.cz/cs/kyberneticka-bezpecnost/ (accessed 11.26.20).
Národní RIS3 strategie | MPO [WWW Document], n.d. URL https://www.mpo.cz/cz/podnikani/ris3-strategie/dokumenty/narodni-ris3-

strategie-pomuze-lepe-zacilit-financni-podporu-do-vyzkumu--vyvoje-a-inovaci-v-perspektivnich-oblastech-ekonomiky-cr---259162/ (accessed 4.8.21).
Neumuth, T., Bulitta, C., Hamm, S., Edelmann, F., Mittermaier, A., Rockstroh, M., Thümmler, C., 2020. 5G Health - The need for 5G technologies in healthcare. https://doi.org/10.13140/RG.2.2.10915.27687
nukib - Legislativa [WWW Document], 2020. URL https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/ (accessed 11.26.20).
NÚKIB - reaktivní opatření [WWW Document], n.d. URL https://nukib.cz/cs/infoservis/aktuality/1667-nukib-vydal-v-souvislosti-se-solarwinds-reaktivni-opatreni/ (accessed 4.8.21).
Oracle [WWW Document], n.d. URL https://www.oracle.com/index.html (accessed 1.15.20).
Pala, A., Zhuang, J., 2019. Information Sharing in Cybersecurity: A Review. Decis. Anal. 16, 172–196. https://doi.org/10.1287/deca.2018.0387
Palo Alto Networks [WWW Document], n.d. URL https://www.paloaltonetworks.com/ (accessed 1.15.20).
(PDF) A Visualization Technique to Improve Situational Awareness [WWW Document], n.d. . ResearchGate. URL https://www.researchgate.net/publication/325763452_A_Visualization_Technique_to_Improve_Situational_Awareness (accessed 8.19.20).
(PDF) An Integrated Framework for Cyber Situation Awareness [WWW Document], n.d. . ResearchGate. URL https://www.researchgate.net/publication/318255963_An_Integrated_Framework_for_Cyber_Situation_Awareness (accessed 8.19.20).
(PDF) Autonomy in use for space situation awareness [WWW Document], n.d. . ResearchGate. URL https://www.researchgate.net/publication/334752405_Autonomy_in_use_for_space_situation_awareness (accessed 8.19.20).
(PDF) Cyber Situational Awareness [WWW Document], n.d. . ResearchGate. URL https://www.researchgate.net/publication/273145856_Cyber_Situational_Awareness (accessed 8.18.20).
(PDF) Innovative teaching in situational awareness [WWW Document], n.d. . ResearchGate. URL https://www.researchgate.net/publication/278044947_Innovative_teaching_in_situational_awareness (accessed 8.19.20).
(PDF) Situation awareness [WWW Document], n.d. . ResearchGate. URL https://www.researchgate.net/publication/232562661_Situation_awareness (accessed 8.18.20).
Peeter Lorents, Rain Ottis, n.d. CCDCOE [WWW Document]. URL https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/ (accessed 10.22.20).
Povědomí o situaci - Situation awareness - qwe.wiki [WWW Document], n.d. URL https://cs.qwe.wiki/wiki/Situation_awareness (accessed 9.2.20).
Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, 2018. , OJ L.
Rada pro kybernetickou bezpečnost [WWW Document], 2011. URL https://www.govcert.cz/cs/rkb/rada-pro-kybernetickou-bezpecnost/ (accessed 3.1.20).
Role jednotlivých subjektů v procesu zavádění 5G sítě [WWW Document], 2020. URL https://www.pravniprostor.cz/clanky/ostatni-pravo/role-jednotlivych-subjektu-v-procesu-zavadeni-5g-site (accessed 11.28.20).

Sánchez, H.S., Rotondo, D., Escobet, T., Puig, V., Quevedo, J., 2019. Bibliographical review on cyber attacks from a control oriented perspective. Annu. Rev. Control 48, 103–128. https://doi.org/10.1016/j.arcontrol.2019.08.002

Saravanan, A., Bama, S.S., 2019. A Review on Cyber Security and the Fifth Generation Cyberattacks. Orient. J. Comput. Sci. Technol. 12, 50–56.

Schulz, C.M., Endsley, M.R., Kochs, E.F., Gelb, A.W., Wagner, K.J., 2013. Situation Awareness in AnesthesiaConcept and Research. Anesthesiol. J. Am. Soc. Anesthesiol. 118, 729-742-729–742. https://doi.org/10.1097/ALN.0b013e318280a40f

Security Advisory | SolarWinds [WWW Document], n.d. URL https://www.solarwinds.com/sa-overview/securityadvisory (accessed 4.8.21).

Siriwardhana, Y., Gür, G., Ylianttila, M., Liyanage, M., 2020. The Role of 5G for Digital Healthcare against COVID-19 Pandemic: Opportunities and Challenges. ICT Express.

Situational Awareness - SKYbrary Aviation Safety [WWW Document], n.d. URL https://www.skybrary.aero/index.php/Situational_Awareness (accessed 8.19.20).

Situational awareness [WWW Document], n.d. . R. Coll. Obstet. Amp Gynaecol. URL https://www.rcog.org.uk/en/guidelines-research-services/audit-quality-improvement/each-baby-counts/ebc-2015-report/human-factors-nontechnical-skills/situational-awareness/ (accessed 8.19.20).

Směrnice Rady 2008/114/ES, 2008. , 345.

SQL Injection [WWW Document], 2008. . PCWorld. URL https://www.pcworld.com/article/146048/article.html (accessed 11.12.20).

Svoboda, Z., 2010. Kritická infrastruktura a její ochrana. Vysoká škola báňská - Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství.

Union, P.O. of the E., 2020. Bezpečné zavádění sítí 5G v EU [WWW Document]. URL http://op.europa.eu/cs/publication-detail/-/publication/a9099bfd-435d-11ea-b81b-01aa75ed71a1/language-cs (accessed 11.28.20).

UPDATED: Palo Alto Networks Protections Against WanaCrypt0r Ransomware Attacks, 2018. . Palo Alto Netw. Blog. URL https://blog.paloaltonetworks.com/2018/01/palo-alto-networks-protections-wanacrypt0r-attacks/ (accessed 11.23.20).

Útok na Nemocnici Benešov způsobil škodu 59 milionů [WWW Document], n.d. URL https://www.ceskenoviny.cz/zpravy/utok-na-nemocnici-benesov-zpusobil-skodu-59-milionu/1922928 (accessed 4.9.21).

Útok na SolarWinds [WWW Document], n.d. URL https://www.aec.cz/cz/cdc-info/Stranky/utok-na-solarwinds.aspx (accessed 4.8.21).

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby [WWW Document], n.d. URL https://www.govcert.cz/cs/vyhlaska-c-437-2017-sb-o-kriteriich-pro-urceni-provozovatele-zakladni-sluzby/ (accessed 2.28.20).

Vzdělávání členů SH ČMS [WWW Document], n.d. URL https://www.vzdelavani-dh.cz/publicCourse?id=59&head=124&subhead=316 (accessed 9.8.20).

What is a Cyber Attack? [WWW Document], n.d. . Check Point Softw. URL /cyber-hub/cyber-security/what-is-cyber-attack/ (accessed 11.9.20).

What is a denial of service attack (DoS) ? [WWW Document], n.d. . Palo Alto Netw. URL https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos (accessed 11.13.20).

What is COBIT? [WWW Document], 2012. . Simplilearn.com. URL https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article (accessed 4.13.21).

What is Cyberspace? - Definition from Techopedia [WWW Document], n.d. . Techopedia.com. URL http://www.techopedia.com/definition/2493/cyberspace (accessed 10.22.20).

What is IoT? [WWW Document], 2016. . IoT Agenda. URL https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (accessed 11.30.20).

What is malware [WWW Document], n.d. . McAfee. URL https://www.mcafee.com/en-us/antivirus/malware.html (accessed 11.12.20).

What is MITM Attack | Imperva, n.d. . Learn. Cent. URL https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/ (accessed 11.13.20).

What is Phishing? [WWW Document], n.d. . Malwarebytes. URL https://www.malwarebytes.com/phishing/ (accessed 11.12.20).