Hodnocení rizik obce s rozšířenou působností

Bc. Michaela Snopková

Diplomová práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Michaela Snopková**
Osobní číslo:	**L21323**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Hodnocení rizik obce s rozšířenou působností**

Zásady pro vypracování

1. Zpracujte literární rešerši k problematice hodnocení kybernetických rizik.
2. Proveďte posouzení vybrané obce s rozšířenou působností s důrazem na oblast kybernetické bezpečnosti.
3. Identifikujte dopady vybraných kybernetických hrozeb na obec s rozšířenou působností.
4. Vyhodnoťte aktuální situaci v oblasti kybernetické bezpečnosti v obci s rozšířenou působností a uveďte, jaké změny v této oblasti přinese zavedení nové směrnice NIS2.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. European Union Agency for Cybersecurity. *ENISA THREAT LANDSCAPE 2023*. Brusel: European Union Agency for Cybersecurity (ENISA), 2023. ISBN: 978-92-9204-645-3.
2. NONNEMANN, František; ČERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. Právní monografie. Praha: Wolters Kluwer, 2022. ISBN 978-80-7676-515-3.
3. SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN: 978-80-7623-068-2.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Lukáš Pavlík, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2023**
Termín odevzdání diplomové práce: **26. dubna 2024**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 26.04.2024

Jméno a příjmení studenta: Bc. Michaela Snopková

.....
podpis studenta

ABSTRAKT

Diplomová práce s názvem Hodnocení rizik obce s rozšířenou působností je rozdělena do dvou částí. V teoretické části je práce zaměřena na teoretická východiska řešené problematiky kybernetické bezpečnosti, kyberprostoru, kybernetických hrozeb a analýzu rizik. Praktická část obsahuje popis vybrané obce s rozšířenou působností, statistickou analýzu oblastí kybernetických útoků, výběr konkrétní organizace sídlící ve vybrané obci s rozšířenou působností a hodnocení jejích kybernetických rizik.

Klíčová slova: kybernetická bezpečnost; kyberprostor; kybernetické hrozby; riziko; hodnocení rizik

ABSTRACT

The master's thesis entitled Risk assessment of municipalities with extended competence is divided into two parts. In the theoretical part, the thesis focuses on the theoretical background of the addressed issues of cybersecurity, cyberspace, cyber threats and risk analysis. The practical part includes a description of the selected municipality with extended competence, statistical analysis of cyber attack areas, selection of a specific organization located in the selected municipality with extended competence and cyber risk assessment.

Keywords: cyber security; cyberspace; cyber threats; risk assessment

Na tomto místě bych ráda poděkovala vedoucímu mé diplomové práce, Ing. Lukáši Pavlíkovi, PhD., za ochotu, trpělivost, konzultace a cenné rady, které mi v průběhu zpracování diplomové práce poskytl.

Velké poděkování patří také celé mé rodině, která mi vytvořila prostor pro studium a po celou dobu studia mi byla nepostradatelnou oporou.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Rychlý rozvoj v oblasti informačních a komunikačních technologií typický pro posledních několik desetiletí s sebou přinesl digitalizaci celé společnosti. Spousta aktivit je díky těmto technologiím a Internetu výrazně snadnější a rychlejší, neomezuje nás časově a ani prostorově. Jednání v bance, bankovní převody, zařizování na úřadech, pracovní pohovory, nákupy a mnoho dalších činností lze dnes zvládnout z pohodlí domova, prostřednictvím svého počítače, tabletu nebo chytrého telefonu. Využívání těchto benefitů plynoucích z technického pokroku je bezesporu příjemné, méně příjemnou stránkou věci jsou však rizika, která s sebou záliba v informačních a komunikačních technologiích nese.

Počítače a telefony se staly běžnou výbavou každého člověka. Pro nemalé procento lidí je prostředí počítače, telefonu a Internetu druhým domovem. A s našim pobytem a působením v tomto virtuálním světe, sdílíme technologiím, a tím často i celému světu, informace o nás samých, o našich zájmech, naší práci, nákupních preferencích, vztazích a dalších zajímavostech, aniž bychom si mnohdy uvědomovali, co takové informace ve vlastnictví jiné osoby mohou způsobit. Informace se postupně staly tou nejcennější komoditou.

Na oblíbenost digitálního prostředí spoléhají také společnosti, organizace, nebo stát a uzpůsobují své služby tomuto trendu. Je to rychlejší, levnější a efektivnější. Co se ale děje, když se státní správa stane cílem kybernetických útoků? Jak takové útoky vypadají a jak se takovým útokům bránit a zajistit, aby nedošlo k ochromení poskytovaných služeb?

Uvedenými otázkami se zabývá tato diplomová práce. Zároveň se autor práce snaží zjistit, jakým způsobem oblast kybernetické bezpečnosti ovlivní nová Směrnice Evropské unie o kybernetické bezpečnosti.

I. TEORETICKÁ ČÁST

CÍL PRÁCE A POUŽITÉ METODY

Hlavním cílem této diplomové práce je analýza zjištěného stavu kybernetické bezpečnosti ve vybrané obci s rozšířenou působností, návrh změn vedoucích k případnému zlepšení stávající situace a vyjádření změn, které pro obec s rozšířenou působností přinese zavedení nové směrnice NIS2.

K dosažení hlavního cíle práce byly stanoveny dílčí cíle:

- zpracovat literární rešerši k problematice hodnocení kybernetických rizik,
- provést posouzení vybrané obce s rozšířenou působností s důrazem na oblast kybernetických rizik,
- identifikovat dopady vybraných kybernetických rizik na obec s rozšířenou působností,
- vyhodnotit aktuální situaci v oblasti kybernetické bezpečnosti v obci s rozšířenou působností a uvést, jaké změny v této oblasti přinese zavedení nové směrnice NIS2.

Ke splnění výše uvedených cílů byly použity metody:

- literární rešerše,
- analýza,
- logická indukce,
- dedukce,
- komparace,
- desk research a
- strukturovaný rozhovor.

Omezení práce

Praktická část diplomové práce je omezena na vybranou obec s rozšířenou působností. V rámci této vybrané obce je na základě teoretických poznatků k problematice kybernetický útoků a jejich nejčastějších cílů zvolena organizace, u které je provedeno hodnocení kybernetických rizik.

1 KYBERNETICKÁ BEZPEČNOST V LITERATUŘE, ELEKTRONICKÝCH ZDROJÍCH A DALŠÍCH DOKUMENTECH

Téma kybernetické bezpečnosti je v posledních letech čím dál více diskutované a aktuální. Státní správa, obchody, podniky, banky i běžné domácnosti jsou závislé na fungování informačních a komunikačních technologií rok od roku větší měrou. Tyto technologie urychlují tok informací, peněz, zvyšují kapacity, zkracují vzdálenosti, a mnoho dalších benefitů, ale zároveň se díky jejich používání můžeme stát zranitelnějšími, pokud je nevyužíváme dostatečně bezpečně. Následky kybernetických útoků mohou mít hluboký dopad.

Problematice bezpečnosti v kyberprostoru a kyber kriminality se věnuje řada literárních i elektronických zdrojů v České republice i v zahraničí. Úvodní kapitola diplomové práce je věnována základním pojmům z této oblasti a nahlédnutí do několika odborných literárních a elektronických zdrojů, do právních předpisů, norem a koncepčních dokumentů.

1.1 Základní pojmy

V oboru informačních a komunikačních technologií (dále jen „ICT“) lze u řady zdrojů narazit na rozlišný výklad jednotlivých pojmů. Snahy o sjednocení tohoto názvosloví se vyskytují již delší dobu a proudí také ze strany Úřadu pro normalizaci, měření a zkušebnictví (dále jen „ÚNMZ“). (Sedlák a Konečný, 2021)

Hrozba

Jakýkoliv fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je daná velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby. (Bezpečnostní strategie České republiky 2003, 2004)

Kybernetická bezpečnost

Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru. (Sedlák a Konečný, 2021)

Kybernetická bezpečnostní událost

Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. (Richter, 2018)

Kybernetický bezpečnostní incident

Analytický bezpečnostní incident je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetických bezpečnostních událostí. (Richter, 2018)

Kybernetická kriminalita

Ta činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti jejímž předmětem jsou popsána zařízení jako věci movité) nebo jako prostředí (objekt). nebo jako nástroj trestné činnosti. (Jirásek, Novák a Požár, 2015)

Kybernetická obrana

Obrana proti kybernetickému útoku a zmírňování jeho následků. Nebo rezistence subjektu na útok a schopnost se účinně bránit. (Sedlák a Konečný, 2021)

Kybernetická strategie

Obecný postup k rozvoji a využití schopnosti pracovat v kybernetickém prostoru, integrovaný a koordinovaný s ostatními operačními oblastmi k dosažení nebo podpoře dosažení stanovených cílů pomocí identifikovaných prostředků, metod a nástrojů v určitém časovém rozvrhu. (Sedlák a Konečný, 2021)

Kybernetická špionáž

Získávání strategicky citlivých či strategicky důležitých informací od jednotlivců nebo organizací za použití či cílení prostředků IT. Používá se nejčastěji v kontextu získávání politické, ekonomické nebo vojenské převahy. (Sedlák a Konečný, 2021)

Kybernetická válka

Použití počítačů a Internetu k vedení války v kybernetickém prostoru. Soubor rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků. (Sedlák a Konečný, 2021)

Kybernetický prostor

Kybernetickým prostorem se rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací tvořené informačními systémy a službami a sítěmi elektronických komunikací. (Richter, 2018)

Kybernetický útok

Útok na ICT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu s politicky či vojensky motivovanými útoky. (Sedlák a Konečný, 2021)

Kyberterorismus

Trestná činnost páchaná za primárního využití či cílení prostředků IT s cílem vyvolat strach či neadekvátní reakci. Používá se nejčastěji v kontextu extrémisticky, nacionalisticky a politicky motivovaných útoků. (Sedlák a Konečný, 2021)

Riziko

Rizikem se rozumí pravděpodobnost vzniku nežádoucího specifického účinku, ke kterému dojde během určité doby nebo za určitých okolností. (Richter, 2018)

Veřejná infrastruktura

Veřejnou infrastrukturou se rozumí pozemky, stavby, zařízení, a to:

1. dopravní infrastruktura, například stavby pozemních komunikací, drah, vodních cest, letišť a s nimi související zařízení,
2. technická infrastruktura, kterou jsou vedení a stavby a s nimi provozně související zařízení technického vybavení, například vodovody, vodojemy, kanalizace, čistírny odpadních vod, stavby ke snižování ohrožení území živelními nebo jinými pohromami, stavby a zařízení pro nakládání s odpady, trafostanice, energetické vedení, komunikační vedení veřejné komunikační sítě a elektronické komunikační zařízení veřejné komunikační sítě, produktovody a zásobníky plynu,

3. občanské vybavení, kterým jsou stavby, zařízení a pozemky sloužící například pro vzdělávání a výchovu, sociální služby a péči o rodiny, zdravotní služby, kulturu, veřejnou správu, ochranu obyvatelstva,
4. veřejné prostranství zřizované nebo užívané ve veřejném zájmu. (Richter, 2018)

1.2 Kybernetická bezpečnost v literárních zdrojích

Monografie ***Teorie bezpečnosti I.*** pojednává o vývoji bezpečnostního prostředí v souvislosti s vývojem a potřebami společnosti. Autor dělí bezpečnost do kategorií: vnitřní bezpečnost, energetická bezpečnost, ropná bezpečnost, potravinová bezpečnost, bezpečnost silničního provozu, kybernetická bezpečnost, bezpečnost personální, bezpečnost environmentální, bezpečnost fyzická, bezpečnost mezinárodní, bezpečnost surovinová, bezpečnost výrobku, požární bezpečnost, zdravotnická bezpečnost atd. a upozorňuje, že zajištění jednotlivých druhů bezpečnosti má tvořit mozaiku bezpečnosti celkové. Teorie bezpečnosti má stejný metodologický základ a cíl, různé bezpečnostní problémy lze řešit stejným přístupem a způsobem. (Lukáš, 2017)

Publikace ***Kybernetická (ne)bezpečnost – Problematika bezpečnosti v kyberprostoru*** se zaměřuje na problematiku kybernetické bezpečnosti a s tím související záležitosti. Upozorňuje na dílčí aspekty kybernetické bezpečnosti a nabízí pohled na řešení bezpečnosti v kyberpostoru v rámci širších souvislostí pomocí vývoje nových technologií. (Sedlák a Konečný, 2021)

V knize ***Kybernetická bezpečnost*** poukazuje autor na ekonomickou stránku kybernetických útoků. Útočníkem získaná data jsou poté používána jako běžná obchodní komodita s cílem jejího prodeje s odpovídajícím ziskem (výnos z prodeje – náklady spojené se získáním dané komodity). Cílem kybernetických útoků je narušení základních atributů bezpečnosti, tzn. ohrožení dostupnosti počítačů a počítačových sítí, důvěrnosti a integrity dat v počítačích a na sítích uložených. (Šulc, 2018)

Praktický náhled na kyberkriminalitu, jak z pohledu zabezpečení počítačů a sítí, tak z pohledu vyšetřování útoků v tomto prostředí a popis právního systému, norem a procesů z oblasti kyberkriminality v prostředí Spojených států amerických nabízí kniha ***Cybercrime and information technology: theory and practice – the computer network infrastructure and computer security, cybersecurity laws, Internet of Things (IoT), and mobile devices***.

Kniha věnuje pozornost také novým bezpečnostním výzvám, které se objevují v souvislosti s novými technologiemi a trendy v oblasti IT. (Alexandrou, 2022)

Praktického průvodce kybernetických rizik pro moderní podniky lze nalézt v příručce ***The cyber rick handbook: creating and measuring effective cybersecurity capabilities***. Jedná se o autoritativní návod, jak postupovat v reálných situacích v boji proti kybernetickým rizikům, jak kybernetická rizika řídit a jak integrovat nástroje a opatření, aby se na míru uzpůsobili individuálním potřebám jednotlivých podniků. (Antonucci, 2017)

V knize ***Bitzkrieq: the new challenge of cyberwarfare*** autor nahlíží na nynější dobu, která je spjata s nejmodernější IT technikou z pohledu válečného. Dále poukazuje také na fakt, že vojenské a bezpečnostní záležitosti, stejně jako fungování domácností a podniků je dnes již obvykle založeno na desítkách „chytrých" zařízení a spotřebičů, softwarů a aplikací, které člověku zjednodušují život, ale zároveň mohou tvořit významné bezpečnostní riziko, které přináší nepříjemné hrozby. (Arquilla, 2021)

Publikace **Cybercrime anvestigations: a comprehensive resource for everyone** poukazuje na problematiku kyberkriminality a jejího vyšetřování. Počet zločinů spáchaných v kyberprostoru roste a osob, které jsou skutečně kompetentní ji vyšetřovat je málo. Jedná se o příručku určenou převážně pro policisty, vyšetřovatele, státní zástupce, právníky, orgány trestního řízení a odborníky na informační bezpečnost.

(Bandler a Merzon, 2022)

Publikace ***Cyber security*** zaznamenává problematiku jak kyberkriminality, tak kybernetické bezpečnosti. V knize lze najít základní principy, které by měly být všeobecně respektovány a zaužívány při práci s ICT a komentář k právním normám souvisejícím bezprostředně s problematikou kybernetické bezpečnosti. Kybernetickou bezpečnost zde autoři popisují jako neustále se vyvíjející a měnící se proces závislý na řadě proměnných. (Kolouch a Bašta, 2019)

The hacker and the state: cyber attacks and the new normal of geopolitice je monografií, která poodhaluje svět vůlí a zájmů moderních států a zabývá se kým jak se v mocenském boji tyto státy navzájem hackersky napadají. Kniha vychází z rozhovoru, odtajněných spisů a forenzních analýz firemních zpráv, odděluje fantazie o kybernetických incidentech a zkoumá soutěž digitálního věku z geopolitického hlediska. (Buchanan, 2020)

V monografii ***Kybernetický bezpečnostní incident 3D*** se autoři intenzivně věnují problematice kybernetických incidentů z pohledu ICT. Kniha poskytuje komplexní a praktický pohled na kybernetické incidenty a nabízí rady, jak takovým incidentům předcházet, nebo jak je alespoň minimalizovat. (Nonnemann, Červený a Vítek, 2022)

1.3 Kybernetická bezpečnost v elektronických zdrojích a závěrečných pracích

Ve sborníku z konference ***Interdisciplinary Information Management Talks 2022*** se autoři Romanovská a Pitner zabývají rostoucím počtem kybernetických útoků ve společnosti, se zaměřením na útoky směřující proti veřejnému sektoru jako zdravotnictví, výzkumné instituce, vláda, veřejná správa a poskytovatelé kritické infrastruktury. Dle autorů lze očekávat zvýšení počtu pokusů o útoky na veřejnou správu a vládu, z čehož plyne nutnost zavedení vhodných opatření a technologií k prevenci. Je zde také poukazováno na skutečnost, že veřejná správa je rozdělena do několika úrovní, ale kybernetická bezpečnost ne, ač by rozdělení řízení kybernetické bezpečnosti do více úrovní mělo nesporné výhody. (Romanovská a Pitner, 2022)

Předmětem článku uveřejněném v časopise Pakistan Journal of Criminology - ***Criminological Aspeckts od Behaviour of Victims of Cyberattacks*** bylo zkoumání aspektů viktimologického chování obětí hackerských útoků, přičemž cílem hackerů byly státní organizace, které zajišťují státní bezpečnost země. K výzkumu byla použita analýza dat a syntéza. (Kanybekova et al., 2023)

Autor článku ***The collective security dilemma of preemptive strikes*** pojednává o strategii reakce na kybernetické útoky. Výsledky jsou kromě kybernetické kriminality, mezinárodního terorismu a vojenských hrozeb relevantní i v mnoha jiných kontextech. V textu je rozvíjena použitelnost logiky preventivního útoku jako obrany před napadením. (Konrad, 2024)

Článek ***Resillience against IT attacks in hospitals: Results from exercise in a German university hospital*** se zabývá v posledních letech velmi aktuální tématikou kybernetických útoků na nemocnice. Takové kybernetické útoky pak paralyzují chod celé nemocnice, čímž je částečně narušena kritická infrastruktura v dotčené lokalitě. Autoři prezentují výsledky cvičení simulující první tři dny po kybernetickém útoku, který způsobil úplné selhání IT systémů. Cvičení se odehrálo ve Fakultní nemocnici v sousedním Německu. (Pfenninger et al., 2023)

Bakalářská práce na téma ***Kybernetická bezpečnost vybrané obce*** velmi dobře shrnuje problematiku kybernetické bezpečnosti ve vybrané obci a za pomoci vybrané metody analýzy rizik …. Včetně doporučení opatření ke zlepšení stávajícího stavu. (Hájek, 2021)

Již zmíněný autor Hájek se věnoval oblasti kybernetické bezpečnosti i v diplomové práci na téma ***Aplikovaná kybernetická bezpečnost***. Autor se tentokrát zaměřil na vybranou obchodní společnost, u které posoudil kybernetická rizika a v aplikační části práce navrhl vhodná opatření, jejichž účinnost prostřednictvím vybraných softwarů závěrem vyhodnotil. (Hájek, 2023)

1.4 Kybernetická bezpečnost v právních normách a dalších významných dokumentech

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) (dále jen „ZoKB“)

Zákon o kybernetické bezpečnosti (dále jen „ZoKB“) vstoupil v platnost 29. srpna 2014 s účinností od 1. ledna 2015. ZoKB upravuje práva a povinnosti osob, pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti a upravuje zajišťování bezpečnosti sítí elektronických komunikací a IS. Jedná se o transpozici předpisů Evropské unie, konkrétně směrnice NIS.

Tento zákon byl dosud novelizován prostřednictvím těchto zákonů:

- zákona č. 104/2017 Sb. (s účinností od 1. července 2017),
- zákona č. 205/2017 Sb. (s účinností od 1. srpna 2017),
- zákona č. 183/2017 Sb. (s účinností od 1. července 2017),
- zákona č. 35/2018 Sb. (s účinností od 07. března 2018),
- zákonem č. 111/2019 Sb. (s účinností od 24. dubna 2019),
- zákonem č. 12/2020 Sb. (s účinností od 01. února 2020),
- zákonem č. 261/2021 Sb. (s účinností od 01. února 2022) a
- zákonem č. 226/2022 Sb. (s účinností od 6. srpna 2022).

Další novelizace tohoto zákona je plánována na rok 2024 v souvislosti s novou evropskou směrnicí týkající se kybernetické bezpečnosti.

Účelem tohoto zákona je stanovení základní úrovně bezpečnostních opatření, zlepšení detekce kybernetických bezpečnostních incidentů, zavedení hlášení kybernetických bezpečnostních incidentů, zavedení systému opatření k reakci na kybernetické bezpečnostní incidenty a úprava činnosti dohledových pracovišť. (NÚKIB ČR, 2024)

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022

Zprávu o stavu kybernetické bezpečnosti za uplynulý rok vydává od roku 2014 Národní úřad pro kybernetickou a informační bezpečnost České republiky. Cílem této zprávy je shrnutí činnosti NÚKIB za daný rok, zveřejnění statistiky kybernetické bezpečnosti v České republice, přehled kybernetických hrozeb a jejich aktérů za daný rok, definování nejčastějších cílů kybernetických útoků, přijatá opatření, legislativní ukotvení dané problematiky a její změny a přehled dalších dílčích činností NÚKIB včetně informací o mezinárodní spolupráci. (NÚKIB, 2023)

Národní strategie kybernetické bezpečnosti České republiky 2021 – 2025

Dokument popisuje hlavní principy, na nichž stojí kybernetická bezpečnost České republiky, stanovuje její strategické směřování v dalším období v oblasti kybernetické bezpečnosti a popisuje vize České republiky v oblasti kybernetické bezpečnosti. Národní strategii kybernetické bezpečnosti zpracovává Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) a předkládá ji vládě ke schválení. Tato strategie aktualizována nejméně každých 5 let, jak ukládá zákon o kybernetické bezpečnosti. (Národní úřad pro kybernetickou a informační bezpečnost, 2023)

Akční plán k národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025

Jedná se o dokument, který vychází z Národní strategie kybernetické bezpečnosti České republiky. Akční plán definuje podrobněji jednotlivé vize a převádí je do konkrétních úkolů, které mají vést k naplnění těchto vizí. Akční plán obsahuje implementační část určující odpovědnost a harmonogram realizace. Stejně jako u Národní strategie kybernetické bezpečnosti, i Akční plán zpracovává NÚKIB, schvaluje jej vláda a aktualizuje se nejméně jednou za 5 let. (Národní úřad pro kybernetickou a informační bezpečnost, 2023)

Nová 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)

Tato nová vyhláška od 28.05.2018 nahradila vyhlášku č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti. Jedná se o prováděcí předpis k ZoKB. Tato vyhláška stanovuje obsah a strukturu bezpečnostní dokumentace, obsah a rozsah bezpečnostních opatření, tipy kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku, vzor oznámení kontaktních údajů a jeho formu a způsob likvidace dat provozních údajů informací a jejich kopii. Touto vyhláškou je zapracována směrnice evropského parlamentu a rady 2016/1148 ze dne 06. července 2016 o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informačních systémů v Unii do tuzemské legislativy. (ČESKO, 2018)

Směrnice Evropského parlamentu a Rady EU 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informačních systémů v Unii – Směrnice NIS

Cílem této evropské směrnice je harmonizace právní úpravy členských států v oblasti bezpečnosti sítí a informačních systémů a zavedení jednotného standardu úrovně kybernetické bezpečnosti. Účelem směrnice je zlepšení fungování vnitřního trhu. Úkolem moci zákonodárné v České republice je implementace Evropských směrnic a právních předpisů do našeho právního systému. Obsah směrnice NIS byl v tuzemsku již částečně řešen novelizací ZoKB. Aktuálně se EU snaží o prohloubení a rozšíření rámce kybernetické bezpečnosti, který byl zaveden směrnicí NIS. Konec platnosti směrnice NIS je určen na 17.10.2024. Tento nový rámec má přinést směrnice NIS2, která by měla na směrnici NIS navázat. (Evropský parlament a rada EU, 2016)

Směrnice Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (jasné nařízení o ochraně osobních údajů) – GDPR (General Data Protection Regulation)

Toto Obecné nařízení působí jako nový právní rámec ochrany osobních údajů v evropském prostoru, tím, že přímo určuje pravidla pro zpracování osobních údajů. Nařízení bylo univerzálně vytvořeno tak, aby bylo použitelné ve všech státech Evropské unie. Tím je dosaženo sjednocujícího účinku. Cílem nařízení je uzpůsobení právního rámce v oblasti ochrany osobních údajů dnešní době. Nařízení určuje adresátům práva povinnosti, ale na rozdíl od zákona obsahuje preambuli s recitály, které jsou výkladem vlastního textu nařízení. (MV ČR, 2023)

Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 – Akt o kybernetické bezpečnosti

Akt o kybernetické bezpečnosti zavedl v Evropské unii nová pravidla pro certifikaci kybernetické bezpečnosti. V tomto rámci bylo vytvořeno několik režimů pro různé kategorie produktů, služeb a procesů. Každý z režimů má stanoveny bezpečnostní standardy, které musí být splněny, metody hodnocení a uvedenou dobu platnosti vydaných certifikátů. Hlavním dozorovým orgánem pro kontrolu certifikací je agentura ENISA (agentura Evropské unie pro bezpečnost sítí a informací). Akt o kybernetické bezpečnosti spolu se směrnicí NIS a GDPR jsou důležitými mezníky na cestě k informační a kybernetické bezpečnosti. (VDT technology a. s., 2021)

Směrnice Evropského parlamentu a Rady (EU) č. 2022/2555, o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 – Směrnice NIS2

NIS2 je novou směrnicí EU o kybernetické bezpečnosti. Aktuálně probíhá příprava k implementaci směrnice NIS 2 do českého právního řádu. Tato směrnice navazuje na výše zmíněnou směrnici NIS, přijatou v roce 2016, jejíž platnost končí k 17. říjnu 2024 a směrnice NIS2 by na ni měla plynule navázat.

Tím že nové znění směrnice NIS vejde v platnost nevzniká dotčeným subjektům, jež spadají do její působnosti, povinnost okamžitého plnění určených povinností. S ohledem na skutečnost, že oficiální znění směrnice bylo v Úředním věstníku Evropské unie zveřejněno 27. prosince 2022, a směrnice vstoupila v platnost 16. ledna 2023, konec transpoziční lhůty pro Českou republiku, která činí 21 měsíců, vychází na 16. října 2024. Subjekty, kterých se dosud ZoKB netýkal pak budou mít stanovenu zvláštní lhůtu pro zahájení plnění nových povinností.

Směrnice NIS nastavila rámec k zajištění vysoké úrovně bezpečnosti sítí a informačních systémů v celé unii, cílem směrnice NIS 2 je rozšíření a prohloubení tohoto rámce. Česká republika má v této oblasti výhodu, protože značná část změn, které nová směrnice do EU přinese je již zakotvena v ZoKB. Přesto NIS2 přináší řadu změn.

Subjekty, které budou dotčeny změnami, které přinese směrnice NIS2, a splňují podmínky pro zařazení do kategorie „velký podnik“ dle doporučení Komise (EU) 2003/361/EC jsou graficky znázorněný v příloze I. Subjekty z těchto kategorií budou zařazeny v režimu essential.

V příloze II. Jsou vyjmenovány subjekty, které dle výše uvedeného doporučení splňují podmínku „velký podnik“ a „střední podnik“, ale bude na ně kladen nižší nárok z pohledu bezpečnostních opatření, tzn. Budou zařazeny v režimu important.

Mimo tyto dva režimy jsou postaveny subjekty, které shromažďují a udržují přesnou a úplnou registraci názvu domén. Takovým subjektům plynou povinnosti z NIS2, ale nejsou zařazeny v uvedených režimech.

Shrnutí kapitoly

Literární rešerše na téma kybernetické bezpečnosti napovídá, že toto téma je vysoce aktuální po celém světě. S vyspělostí jednotlivých zemí dlouhodobě roste obliba IT techniky a Internetu, a zároveň roste také riziko kybernetických hrozeb a tím také potřeba jim účinně čelit a především předcházet. Tato problematika je nesporně s vysokou důležitostí řešena i v rámci České republiky, jak plyne z uvedených právních předpisů a dalších důležitých dokumentů zaměřených na toto téma.

2 KYBERPROSTOR, KYBERNETICKÁ BEZPEČNOST KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT A KYBERNETICKÉ HROZBY

Posun v myšlení člověka jde ruku v ruce s technologickým pokrokem a digitalizací. Se zapojením používání digitálních technologií do svého života se člověk stal součástí kyberprostoru. Informační a komunikační technologie dokážou překonat vzdálenosti, zkrátit čas, zpřístupnit informace a služby. S důvěrou, kterou vkládáme do přístrojů a sítí, souvisí také jisté riziko. Při pohybu v kyberprostoru lze snadno zapomenout, že bezpečnost a opatrnost musí stát na prvním místě.

2.1 Kyberprostor

Pod pojmem kyberprostor si lze představit virtuální prostor, který nemá konec ani začátek, je tedy prakticky neomezený. Proti zákonné definici uvedené v kapitole 1, Kolouch a Bašta dále rozvíjejí, že: *„Kyberprostor je tvořený prvky informačních a komunikačních technologií, které vytvářejí pomocí protokolu TCP/IP celosvětovou, globální počítačovou síť, a jednotlivými počítačovými systémy, které jsou do této sítě připojeny a které v ní interagují. Vlastní interakce uvedených systémů není možná bez zásahu jednotlivých uživatelů (administrátorů či koncových uživatelů). Tím je vytvořen dynamický, neustále se měnící a vyvíjející systém vázaný na hardware, avšak zároveň vytvářející těžko definovatelný a prakticky neomezený kyberprostor.“* (Kolouch a Bašta, 2019)

Pro specifičnost a neomezenost v kyberprostoru je třeba očekávat, že zde nebudou platit stejná pravidla, jako platí v běžné realitě. Kyberprostor je charakteristický svou decentralizovaností, globálností, otevřeností, informační nasyceností a interaktivností.

V souvislosti s kyberprostorem je také potřeba definovat pojem Internet, který je nezbytnou materiální podstatou kyberprostoru. Internet je celosvětový systém propojených počítačových sítí, ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů TCP/IP. Používá se ke sdílení a výměně dat a komunikaci.

Často se můžeme setkat také s velmi zjednodušenou laickou definicí: KYBERPROSTOR = INTERNET = WEB. Tato definice není úplně šťastná, protože jak už je uvedeno výše, součástí kyberprostoru jsou například také lokální počítačové sítě LAN, které nemají přístup k Internetu, jedná se především o intranetové sítě.

Zároveň se kyberprostor netýká jenom webových stránek, ale zahrnuje celou řadu počítačových systémů, uživatelů a dat. Pro řadu běžných uživatelů jsou výrazy Internet a web synonymy.

Dále se můžeme setkat s definováním kyberprostoru a jeho dělením z pohledu dostupnosti a dohledatelnosti dat pro běžné uživatele, do tří kategorií:

1. Surface Web - Služby a data dostupná pomocí Internetu,
2. Deep Web - Služby a data dostupná pouze v rámci konkrétních sítí a zařízení a
3. Dark Web - Služby a data záměrně skrytá a dostupná pouze s využitím speciálních nástrojů. (Kolouch a Bašta, 2019), (Kolouch, 2016),

2.2 Kybernetická bezpečnost

Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, prezentuje výraz bezpečnost jako: *„Zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejich demokratických základů a ochrana životů, zdraví a majetkových hodnot je základní povinností státu.“* (ČESKO, 1998)

Jiný náhled nabízí *Terminologický slovník pojmů krizového řízení*, který definuje bezpečnost jako stav, kdy je systém schopen odolávat vnějším i vnitřním hrozbám charakteru předpokládaného i nenadálého s cílem zachování struktury systému, stability, spolehlivosti a chování v souladu s daným záměrem. (Ministerstvo vnitra České republiky, 2016)

Obecným cílem bezpečnosti je ochránit chráněný zájem před zničením, poškozením nebo zcizením. V souvislosti s kyberprostorem ale nehovoříme o zničení, poškození, nebo zcizení, jako v reálném životě při ochraně hmotných statků. V této souvislosti mluvíme o narušení základních atributů bezpečnosti, konkrétně o ohrožení dostupnosti počítačů a počítačových sítí, důvěrnosti a integrity dat uložených a zpracovávaných počítačích nebo přes ně přenášených. (Šulc, 2018)

V souvislosti s pojmem kybernetické bezpečnosti lze narazit na názory, že kybernetická bezpečnost je pouze věcí odborníků a specialistů na ICT. Opak je ale pravdou, kybernetická bezpečnost by měla být vlastní každému, kdo se vyskytuje v kyberprostoru, ať soukromě či pracovně. Kybernetická bezpečnost je klíčová a měla by být řešena dlouhodobě a systematicky. (Kolouch a Bašta, 2019)

2.2.1 Organizace zabývající se kybernetickou bezpečností

Agentura ENISA

Agentura Evropské unie pro kybernetickou bezpečnost (dále jen „ENISA“) byla zřízena v roce 2004. Hlavním cílem této organizace je dosažení vysoké společenské úrovně kybernetické bezpečnosti v celé Evropě. Sdílením znalostí, budováním kapacit a zvyšováním informovanosti v oblasti kybernetické bezpečnosti usiluje ENISA o posílení základního principu unie, důvěry ve společné fungování.

Mezi hlavní úkoly agentury ENISA patří podílení se na tvorbě politiky Evropské unie v oblasti kybernetické bezpečnosti. Vytváření systému certifikace kybernetické bezpečnosti a zajištění silnější důvěry v digitální produkty, služby a procesy. Spolupráce se zeměmi a orgány Evropské unie a pomoc s přípravou na kybernetické výzvy. Činnost agentury je směřována především ve prospěch veřejnoprávních organizací, tzn. spolupráce s orgány členských zemí a jejich úřady, institucemi, decentralizovanými subjekty a agenturami, a orgány, institucemi a ostatními subjekty EU. Činnost agentury ENISA je prospěšná také pro odvětví ICT, odborníky na kybernetickou bezpečnost, akademické obce, podniky, ale i pro širokou veřejnost.

ENISA poskytuje na svých webových stránkách řadu volně dostupných publikací týkajících se kybernetické bezpečnosti v Evropské unii. (Europen Union Agency for Cybersecurity, 2024)

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB je ústředním správním orgánem pro oblast kybernetické bezpečnosti včetně ochrany utajovaných informací v oblasti informačních a komunikačních sytémů a kryptografické ochrany. Vznikl 1. srpna 2017 na základě zákona č. 205/2017 Sb, kterým se měnil ZoKB. V čele NÚKIB je ředitel, který se účastní jednání Bezpečnostní rady státu (dále jen „BRS“) a je členem Výboru pro kybernetickou bezpečnost (pracovní orgán BRS). (NÚKIB, 2024)

Národní centrum kybernetické bezpečnosti (NCKB)

NCKB je výkonnou sekcí NÚKIB, jejímž úkolem je zajišťovat prevenci před kybernetickými hrozbami proti prvkům kritické informační infrastruktury, IS základní služby, proti významným informačním systémům a vybraným informačním systémům veřejné správy.

Dále NCKB zajišťuje řešení a koordinaci řešení kybernetických bezpečnostních incidentů u subjektů kritické infrastruktury, provozovatelů základní služby a orgánů veřejné správy, zabezpečuje osvětovou a vzdělávací činnost v oblasti kybernetické bezpečnosti, spolupráci s národními i mezinárodními organizacemi podílejícími se na bezpečnosti v kyberprostoru, pořádání a účast na kybernetických cvičeních na národní i mezinárodní úrovni. Tato sekce se zabývá také výzkumem a vývojem v oblasti kybernetické bezpečnosti, zastupování České republiky v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti (ve spolupráci s kabinetem ředitele), vyhodnocováním rizik v oblasti kybernetické bezpečnosti a přijímání příslušných nápravných a preventivních opatření. V neposlední řadě zabezpečuje činnost týmu tzv. „Vládního CERT České republiky“ (dostupné na webové stránce GovCERT.cz), stanovuje komunikační strategii Úřadu v dotčené oblasti (ve spolupráci s ostatními celky Úřadu) a rozsahu své působnosti zajišťuje bezpečnostní politiku úřadu, plnění mezinárodních závazků a spoluprací na mezinárodní úrovni při realizaci předpisů vyplývajících z členství České republiky v NATO a členství v EU a jiných mezinárodních organizacích.

NCKB lze pomocí elektronického formuláře, nebo aplikace ohlásit kybernetický bezpečnostní incident. Odborníci tohoto vládního týmu jsou připraveni poskytnout pomoc po technické stránce a doporučit preventivní opatření, případně vyhodnotit, zda hlášený incident může cílit i na jiné subjekty a zavést případná opatření. (NÚKIB, 2024)

2.2.2 Kybernetická bezpečnost v České republice

V České republice došlo v průběhu roku 2022 ke snížení kybernetických incidentů hlášených NUKIV konkrétně ze 157 na 146. Přesto dle statistik Policie České republiky vzrostl počet kyberkriminálních aktivit, a to téměř dvojnásobně. Největší hrozbou pro kybernetickou bezpečnost České republiky jsou aktivity státem sponzorovaných kybernetických aktérů a činnost kyberkriminálních skupin.

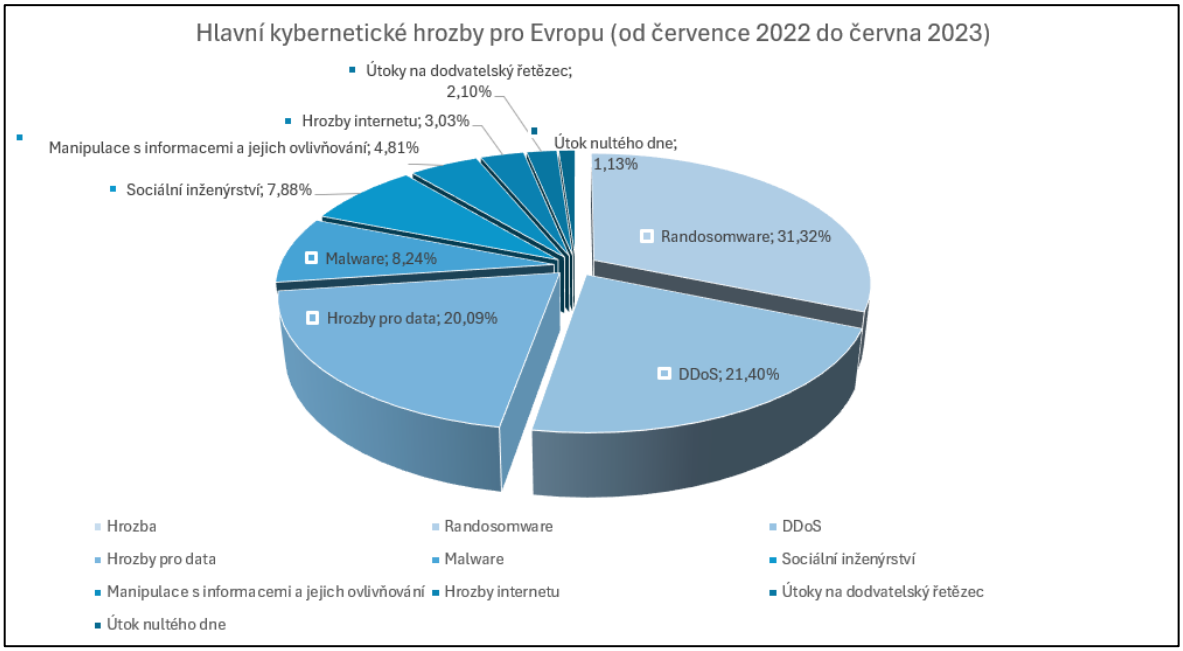
Nejčastějšími typy útoků byli různé druhy phishingu, spear – phishingu, vishingu a podvodných mailů či útoky na dostupnost, zejména ve formě DDoS útoku. Méně často byl zaznamenán výskyt zneužívání zranitelnosti a ransomwarové útoky. Kybernetické incidenty se udály převážně v rámci veřejného sektoru, následovalo zdravotnictví a soukromý sektor. (NÚKIB, 2023)

2.2.3 Kybernetická bezpečnost v Evropě

Agentura ENISA zveřejnila v říjnu 2023 zveřejnila zprávu za sledované období od července 2022 do června 2023, kde sledovala výrazný nárust jak v rozmanitosti, tak v množství kybernetických útoků v Evropské Unii. Tato čísla byla ovlivněna také trvající válkou mezi Ruskem a Ukrajinou, kde manipulace s informacemi hraje významnou roli.

Dle těchto posledních informací je evropský kybernetický prostor ohrožen zejména:

- Randsomware,
- Malware,
- Sociálním inženýrstvím,
- Hrozbami proti datům,
- Hrozbami proti dostupnosti: Odmítnutí služby,
- Hrozbami proti dostupnosti: Hrozby na internetu,
- Manipulací s informacemi a jejich ovlivňováním,
- Útoky na dodavatelský řetězec.



Obrázek 1 – Hlavní kybernetické hrozby pro Evropu od července 2022 do června 2023 Zdroj: ENISA, 2023)

Dále se tato zpráva zmiňuje o nejčastějších cílech kybernetických útoků, kdy útoky na veřejný sektor tvoří až 19 % celkového počtu útoků. V 11 % případů šlo o útoky cílené na konkrétní osoby, v 8 % případů na zdravotnictví a v 7 % případů na digitální infrastrukturu. Významně vzrostl zájem kyberzločinců o cloudové infrastruktury. Díky umělé inteligenci byl zaznamenán také významný nárust útoků sociálního inženýrství. (European Union Agency for Cybersecurity, 2023)

2.3 Kybernetický bezpečnostní incident

Kybernetická bezpečnost je podmnožinou informační bezpečnosti. Oba druhy bezpečnosti mají však stejný cíl. Předmětem ochrany kybernetické bezpečnosti jsou informace, které se vyskytují v digitální podobě, zpracovávané prostřednictvím informačních systémů případně komunikované prostřednictvím komunikačních sítí. Řízení kybernetických bezpečnostních incidentů vychází z obecných principů řízení informační bezpečnosti. Tyto principy definují bezpečnostní standardy a normy.

Kybernetický bezpečnostní incident v organizaci lze chápat jako událost, jejíž dopady mohou ochromit fungování celé organizace, nebo její část. Může se jednat například o neoprávněný přístup k informacím apod.). Zároveň se tímto pojmem označuje i událost, jejíž důsledky zásadně ovlivní fungování celých států (např. útoky zaměřené na kritickou infrastrukturu) a jejichž řešení je velmi náročné a nákladné.

Událost bezpečnosti informací je jakoukoliv potenciální možností narušení bezpečnosti informací (např. doručení podvodného e-mailu, který uživatel nahlásil). Incidentem bezpečnosti informací pak označujeme, pokud tato situace reálně nastala (např. otevření odkazu v podvodném mailu a zadání přihlašovacích údajů). (Nonnemann, Červený a Vítek, 2022)

2.4 Kybernetické hrozby

Hrozbou je chápán potenciální jev, nebo situace, kdy dojde k události, incidentu, nebo události, která bude mít negativní dopad na naše zájmy nebo chráněné hodnoty. Hrozbou je označován jakýkoliv fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míru hrozby lze vyjádřit jako velikost možné škody a časovou vzdáleností možného uplatnění této hrozby, tzn. pravděpodobností, nebo rizikem. (MZV ČR, 2003)

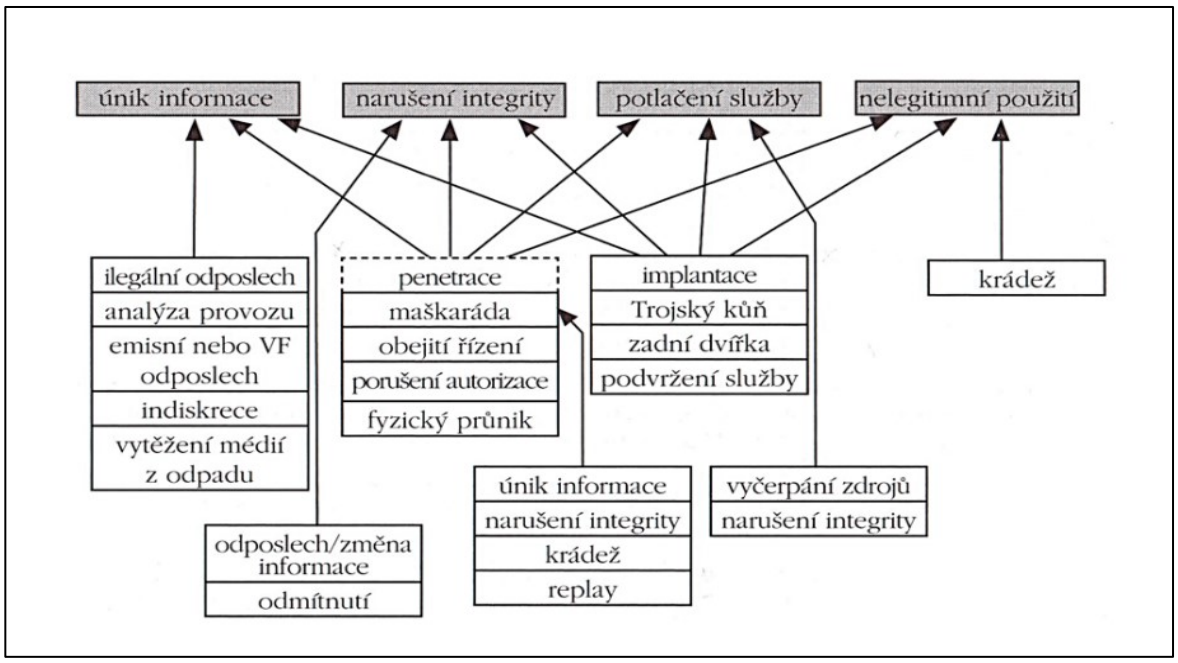
Výkladovém slovníku kybernetické bezpečnosti nalezneme definovaný také s tím související pojem bezpečnostní hrozby (Information Security Threat), jako *„potenciální příčinu nežádoucích událostí, které může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.“* (Jirásek, Novák a Požár, 2015)

V oblasti kyberprostoru mluvíme o takových jevech, nebo situacích jako o **hrozbách kybernetických**.

Hrozby lze dále kategorizovat např. na **hrozby pasivní**, kdy hrozí zpřístupnění informací, aniž by došlo ke změně stavu systému zpracování dat, nebo počítačové sítě, nebo na **hrozby aktivní**, kdy se jedná o hrozby úmyslné změny stavu systému zpracování dat nebo počítačové sítě, nebo kdy je možným následkem modifikace zpráv, vkládání falešných zpráv, vydávání se za jinou osobu, nebo odmítnutí služby. V případě dlouhodobého a trvalého infiltrování a zneužívání cílového systému prostřednictvím pokročilých adaptivních technik (tedy ne jednorázového útoku), hovoříme o **pokročilé a trvalé hrozbě** (Advanced Persistent Threat – APT). (Jirásek, Novák a Požár, 2015)

Autor Jirovský rozdělil hrozby do čtyř základních kategorií a jejich vzájemný vztah vystihuje obrázek č. 2:

1. Únik informace – stav, kdy dojde k odtajnění chráněné informace neautorizovanému subjektu;
2. narušení integrity – došlo k poškození, změně, nebo vymazání dat;
3. potlačení služby – úmyslné bránění v přístupu k informacím, aplikacím či systému a
4. nelegitimní použití – využití informací neautorizovaným subjektem nebo neoprávněným způsobem. (Jirovský, 2007)



Obrázek 2 – Vztahy mezi hrozbami (zdroj: Jirovský, 2007)

Hrozby lze členit také dle zdroje hrozby:

- Hrozby způsobené člověkem.
    - Úmyslně – např. úmyslné smazání dat, konfigurace systému, fyzické poškození počítačového systému, fyzické poškození jiného prvku ICT, zcizení informací, kybernetické útoky.
    - Z nedbalosti – např. omylem smazaná data, fyzické poškození počítačového systému, poškození dat, dat, systémů či jiných prvků na základě neseznámení se s interními akty (právními nebo technickými), jiná chyba uživatele.
- Technické chyby (např. chyba softwaru nebo hardwaru).
- Vyšší moc – např. neplánovaný výpadek napájení způsobený člověkem z nedbalosti, naturogenní mimořádné události či katastrofy (povodně, zemětřesení, zásah bleskem, vichřice, požár apod.).

Členění hrozeb dle zdroje působení:

- Hrozby vnitřní – hrozby vycházející zevnitř organizace.
- Hrozby vnější – hrozby nacházející se mimo organizaci.

Členění hrozeb dle cíle hrozby:

- Útok na triádu CIA.
    - Důvěrnost (Confedentiality) – např. krádeže dat, přístupových údajů, klíčů, hardware atd.
    - Celistvost (Integrity) – chyby v nastavení oprávnění, v databázích apod.
    - Dostupnost (Availability) – útoky DoS a DDoS, fyzické útoky na servery a strukturovanou kabeláž, výpadky proudu aj.
- Útok na prvek kybernetické bezpečnosti.
    - Lidé – útoky sociálním inženýrstvím (reálně i v kyberprostoru), phishing, malware, krádeže, apod.
    - Technologie – hrozby způsobené člověkem, jak úmyslně, tak z nedbalosti, hrozby způsobené vyšší mocí (vis maior) nebo technické chyby, které mohou působit na hardware, databáze, síť a síťovou infrastrukturu, software (operační systém a jiné aplikace), nebo na informace a data uložená v počítačových systémech.
- Procesy – neoprávněné testování zabezpečení či funkčnosti procesů nastavených v organizaci aj.

Členění hrozeb dle motivace útočníka:

- Hrozby za účelem finančního prospěchu.
- Hrozby za účelem získání konkurenční převahy.
- Hrozby za účelem dokázání svých schopností.
- Hrozby za účelem odplaty.
- Hrozby z důvodu neplnění povinností. (Kolouch a Bašta, 2019)

Členění dle typu hrozeb:

- Sociální inženýrství (sociotechnika) – Smyslem sociotechniky je umělé vytvoření klamu a navození dojmu, že se jedná o reálnou situaci. Jedná se o ovlivňování, přesvědčování či manipulaci s lidmi, jejímž cílem je donutit je provést nějakou akci, nebo od nich získat informace, které by jinak neposkytli. Celý systém vychází z faktu, že nejslabším článkem řetězce je vždy uživatel, tedy člověk a hlavní myšlenkou tedy je přesvědčit uživatele - oběť, aby kýžené informace vydala sama dobrovolně a to bez spoléhání se na technické přístupy či nástroje. Klíčovým faktorem pro zisk informací je navození, nebo budování důvěry mezi útočníkem a obětí ještě před útokem, a následným využitím neopatrnosti, důvěřivosti, hlouposti a dalších lidských vlastností uživatele k realizaci útoku. Jedná se o jednoduchou metodu útoku, ale mimořádně účinnou. Útok je zpravidla veden třemi způsoby, které jsou vzájemně kombinované. Jedná se o sběr veřejně dostupných dat o oběti, fyzický útok (útočník se vydává např. za servisního pracovníka k ICT, aby zjistil co nejvíce interních informací) a psychologický útok. Metodami tohoto druhu útoků jsou:
    - Podvodné emaily,
    - Falešné webové stránky,
    - Telefonické hovory,
    - Útok „tváří v tvář“,
    - Prohledávání odpadků,
    - Prohledávání zdrojů s veřejně dostupnými informacemi o oběti (sociální sítě, weby, blogy, výroční zprávy aj.),
    - Doručení reklamních či jiných materiálů na CD, DVD či jiném paměťovém nosiči,
    - Zanechání paměťového media s malware v zájmové oblasti oběti,
    - Nabídka online služby na zkoušku (např. cloudového uložiště),
    - Dodávka či nalezení zařízení (počítačového systému),
    - Falešný servisní technik aj.

- Botnet – Výraz „bot“ je zkráceninou slova robot. Jedná se o program, který vzdáleně plní příkazy útočníka z jiného počítačového systému. Počítačový systém, který je dálkově ovládán je označován jako „zombie“, v jiných zdrojích také jako „bot“(také označováno jako zotročený počítačový systém). Jako botnet se označuje síť softwarově propojených zombie, které fungují na základě příkazu správce botnetu. Nejčastěji malwarem infikované počítače se připojí k centrálnímu řídícímu serveru (C&C – command-and-control) a kontrolu nad celým systémem má botmaster (útočník). Takto postavená síť je používána nejen k nelegální činnosti, ale i k běžné legální činnosti, jako jsou distribuované výpočty. Botnety se využívají především k přetížení vybraných aplikací, webových stránek a služeb, čímž se stávají prostředkem DDoS útoků. Dále se využívají také k šíření spamu, phishingu, malwaru, adwaru, spywaru apod. Motivací útočníka je obvykle finanční zisk.
- Malware – Malicious software, nebo-li škodlivý software je software jakéhokoliv druhu, který je využíván k narušení běžné činnosti počítačového systému zisku dat, či získání přístupů. Malware je schopen plnit několik funkcí najednou. V dnešní době označujeme pojmem malware jakýkoliv škodlivý software, které se historicky označovali různými termíny odvíjejícími se především od činnosti, kterou prováděli, např.:
    - Adware – Jedná se o software podporující reklamu (advertising supported software). Tento druh malware má nejnižší míru nebezpečnosti, za to je pro útočníka nejvíce výnosný. Adware se pak projevuje tím, že zobrazuje reklamy, reklamní sdělení, vyskakující reklamní okna na obrazovce, apod. Může obsahovat také spyware.
    - Trojské koně – Druh malware, který se tváří jako důvěryhodný soubor, který si uživatel stáhne a instaluje do svého zařízení, aniž by věděl o jeho skrytých funkcích, které jsou nebezpečné pro fungování počítačového systému. Trojské koně nemají schopnost se samostatně šířit bez pomoci uživatele.
    - Backdoors – Jedná se o druh trojských koní, které otevírají komunikační porty počítače, vlivem čehož dojde ke zjednodušení napadání zasaženého systému dalšími škodlivými programy.

- Randsomware – Jedná se o malware se schopností infikovat zranitelné cíle a požadovat výkupné, často v určitém časovém limitu. Je to častý druh útoku směřovaný proti státnímu sektoru, zdravotnickým zařízením, kritické infrastruktuře a výrobním podnikům. Nejčastěji se dostane do počítačového systému prostřednictvím malwaru. Randsomeware funguje dvěma způsoby, kdy buď omezí funkčnost celého počítačového systému, nebo jej nechá funkční, ale znepřístupní uživateli data v něm obsažená (crypto-ransomware).
- Spyware – V překladu špionážní software (spy software) je založen na tajném sběru statistických dat o uživateli, provozu jeho zařízení a využívání jeho zařízení, bez vědomí a souhlasu oběti, které jsou následně prodány kyberzločinci. Spyware je často součástí jiných neškodných programů, kde je jeho úkolem zjistit zájmy a preference uživatele, na základě kterých poté zacílí reklamu.
- Počítačové viry (Viruses) – Vyskytují se v podobě programu či závadného kódu, který je připojen k jinému souboru nebo programu, na kterém ale není závislý, sám se kopíruje a šíří bez vědomí uživatele. Viry dominovali mezi jinými druhy malware především v 80. a 90 letech minulého století.
- Červi – Červi (Worms) jsou často považovány za viry , protože nepotřebují hostitele ve formě spustitelného souboru, ale na rozdíl od virů se tyto programy šíří samostatně a analyzují slabiny v zabezpečení napadeného systému. Napadený systém následně odesílá kopie sebe sama dalším uživatelům počítačové sítě. Rychlost šíření často vede k zahlcení sítě.
- Rootkity – Programy a technologie, řazené také jako druh trojských koní, jejichž úkolem je zamaskování přítomnosti malware v počítači. Samy o sobě nejsou škodlivé, ale mění chování operačního systému, jeho částí, aplikací. Z aplikací napadají rootkity především antivirové programy, které je pak nemohou odstranit ze systému.
- Keylogger – Software, který eviduje konkrétní stisky kláves v napadeném počítači s účelem získat přístupové údaje k účtům, které uživatel na daném zařízení používá.

- Spam – Význam tohoto slova je nevyžádaná komunikace. Může se jednat o hromadné šíření nevyžádaného sdělení (zpravidla obchodní či reklamní sdělení, produkty z oblasti finanční, zdravotní, pornografické, náboženské a další oblasti), nejčastěji prostřednictvím Internetu, nebo elektronické komunikace, dále také o všechny nevyžádané zprávy nejen prostřednictvím e-mailu, SMS, MMS, ICQ, Skype, apod., ale i diskuzních fór, blogů, sociálních sítí, herních platforem, apod.
- Scam – Tímto názvem je označován podvod cílený na získání finančních prostředků oběti. Nejznámějšími typy scamu jsou:
    - Scam 19 (Nigerijské dopisy) – podvod šířící se prostřednictvím e-mailu, kdy předmětem zprávy je informace, adresát této zprávy zdědil po vzdáleném příbuzném milionový majetek a k jeho získání musí kontaktovat správce majetku (odesílatele zprávy) a zaplatit administrativní poplatky spojené s řešením dědictví.
    - Romance scam – Podvodník pod falešnou identitou získá důvěru oběti, s níž si dopisuje a předstírá k ní city. Obvykle uvádí, že pracuje v zahraničí a využívá získané důvěry oběti, která mu poskytne finance s cílem osobního setkání, nebo dokonce sňatku.
    - Hoax (žert, novinářská kachna) – Hoax jsou řetězové zprávy s obsahem zavádějících či nepravdivých informací (varování před útoky, petice, prosby o pomoc, řetězové dopisy štěstí apod.), jejichž součástí je výzva k dalšímu šíření takových zpráv.
    - Podvodné nabídky – Jedná se o zprávy šířené prostřednictvím e-mailů, sociálních sítí a dalších komunikačních kanálů jako jsou aukční portály, obsahující podvodné nabídky práce založených na systému „pyramida“ nebo „letadlo“, nabídky na nízkoúrokové půjčky, nebo naopak nabídky na vysoce výnosné investice.
- Phishing – Cílem phishingu je obvykle získat údaje oběti jako uživatelská jména, hesla, čísla platebních karet a jejich PIN. Tento druh podvodu funguje tak, že oběť na podvodné webové stránce vyplní své citlivé údaje, aniž by tušila, že stránka je falešná. Takové metody stojí na metodách sociálního inženýrství a jsou založeny na zneužití důvěry oběti.

- Phraming – Je nebezpečnější formou phishingu, útočící na DNS server (Domain Name System), který je obvykle realizován při vstupu oběti do internetového bankovnictví. Podvod funguje tak, že uživatel zadá do prohlížeče webovou adresu, ale podvodníkem je přesměrován na jiný, podvodný web věrně imitující vyhledávanou stránku. Po zadání přístupových údajů získá útočník tyto informace.
- Spear phishing - Jedná se o formu phishingového útoku, která je konkrétně směřována na vybranou osobu nebo organizaci, nebo na informace a data, kterými ona osoba nebo organizace disponuje.
- Vishing – Tato forma phishingu probíhá telefonicky za použití metod sociálního inženýrství. Cílem je získat od oběti citlivé informace v podobě přihlašovacích údajů, čísel kreditních karet, apod. Typicky se jedná o podvodné telefonáty, kdy se útočník představuje jako pracovník banky, pojišťovny apod., aby zvýšil svoji důvěryhodnost.
- Smishing – Tato forma phishingu se šíří pomocí SMS zpráv. Obvykle se jedná o zasílání pochybných odkazů, upozornění, nebo upomínek k úhradám, kdy cílem útočníka je, aby oběť otevřela zaslaný odkaz, který ji přesměruje na podvodnou stránku, nebo poslala platbu na zadaný bankovní účet.
- Hacking – Dříve byla označením „hacker“ označována technicky nadaná osoba schopna nalézat nová řešení problému. V dnešním době takto označujeme útočníky, kteří svým jednáním směřují proti IT, nebo využívají IT ke své činnosti obvykle s cílem získat přístup do cizích zařízení a systémů. Stále platí, že hacker je osoba, která má dokonalou znalost ICT, dokáže tvořit vlastní programy a využívat tuto techniku k dosažení svých cílů. Aktuálně zřejmě nejznámější hackerskou skupinou je skupina Anonymous.
- Sniffing – Jedná se o metodu monitorování sítě, kdy však dochází k nelegálnímu odposlechu dat mezi poskytovanou službou a počítačovým systémem prostřednictvím „snifferu“ jinou osobou, než správcem sítě, který provádí běžný monitoring sítě. Technicky jde o zachytávání a čtení TCP pakerů.
- DoS – Odepření služby (Denial of Service) je formou útoku na internetovou službu ve snaze vyřazení z činnosti, nebo snížení výkonu zařízení zahlcením systému.

Napadaní touto formou útoku lze identifikovat dle neobvykle pomalého načítání webových stránek, nebo jejich dočasnou neodstupností. V případě DoS útoku je zdroj útoku pouze jeden.

- DDoS (Distributed Denial of Services) - Distribuované odepření služby je další formou útoku DoS specifické tím, že dojde k zahlcení cílového počítačového systému odesíláním paketů z více počítačových systémů, což komplikuje oběti obranu.
- DRDoS (Distributed Reflected Denial of Service) – Distribuované odražené popření služby je podvrhem DoS útoku, spočívajícím v rozesílání upravených požadavků na spojení na velké množství počítačových systémů, které reagují tak, že na zaslané požadavky odpoví oběti útoku.
- Šíření závadového obsahu – V tomto případě se jedná o šíření závadového (nelegálního) obsahu, příkladem jsou zakázané druhy pornografie (dětská pornografie apod.), nebo o šíření materiálů s nenávistným a extrémistickým obsahem.
- Identity theft – Jedná se o útok, kdy je odcizena virtuální identita oběti podvodu např. prolomením přístupových údajů oběti. Pro útočníka je poté výrazně jednodušší např. oslovit některou z osob, s nimiž si oběť pravidelně dopisuje s žádostí o peněžitou pomoc, nebo sdělení citlivých údajů apod. Obvykle je krádež identity používána k rozesílání spamu, phishingových a malwarových útoků, k získání důvěrných informací, nebo k získání dalších přístupů.
- APT (Advanced Persistent Threat) – jedná se o seskupení kybernetických útočníků zaměřujících se na pokročilé a trvalé hrozby (často útočníci z řad státních organizací, nebo organizací pracujících na objednávku státu. Cílem jsou často korporace a vládní organizace. Útočníci proniknou do systémů a snaží se v nich tajně zůstat delší dobu za účelem dlouhodobé kyberšpionáže a odcizení citlivých údajů.
- Kyberterorismus – Teroristické skupiny využívají k uskutečňování útoků s cílem prosazování svým zájmů ICT a především prostředí Internetu. Cílem těchto skupin je na sebe upoutat pozornost co nejširší veřejnosti, ovlivňovat veřejné mínění buzením paniky, strachu, nenávisti, apod. Motivace teroristů je jako u běžné formy teroristu zpravidla náboženského, nebo politického charakteru.

- Kybernetické výpalné či vydírání (cyber extortion) – Formou útoku je také vyžadování výpalného, jinak útočník napadne počítačový systém, kdy dojde k poškození hardwaru, odcizení dat, apod.

(Sedlák a Konečný, 2021), (Kolouch, 2016), (Kolouch a Bašta, 2019), (ESET software spol. s r.o., © 1992-2024)

Shrnutí kapitoly

V této kapitole byly definovány základní pojmy k pochopení problematiky kyberprostoru, kybernetické bezpečnosti, kybernetických hrozeb a kybernetického bezpečnostního incidentu. Kapitola obsahuje také stručné vyjádření ke kybernetické bezpečnosti v tuzemsku a v Evropě a představení nejvýznamnějších organizací, které se kybernetickou bezpečností zabývají.

3 ANALÝZA RIZIK

Analýza rizik je základním procesem v managementu rizik, jedná se tedy o základní prvek rizikového inženýrství. V situaci, kdy nastane krize je manažer nucen k neprodlenému rozhodnutí.

Metody analýzy rizik v základu dělíme na metody kvantitativní a kvalitativní. Kvantitativní analýza rizik je založena na pravděpodobnosti výskytu jevů a pravděpodobnosti ztráty hodnoty. Oproti tomu analýza kvalitativní je využívána ke stanovení priorit mezi riziky, kdy jsou využívána data o následcích a ztrátách užitné hodnoty. Cílem je stanovení zranitelnosti nebo míry ohrožení. Výběr vhodné metody závisí na dostupnosti dat. Data lze získat nejrůznějšími způsoby od laboratorních testů, počítačových záznamů, modelování, až po indexové metody umožňují sčítat na první pohled nesouvisející údaje výsledné hodnoty mají však relativní hodnoty s čímž je potřeba nadále pracovat a nevytrhávat je z kontextu.

Každá metoda má svůj limit použití, nelze tedy předpokládat, že se jedná o univerzální nástroj. Každá metoda pro stanovení rizik je určena pro konkrétní problém, a proto jednotlivá paradigma nejsou vzájemně porovnatelné. Mezi nejpoužívanější metody analýzy rizik můžeme zařadit níže uvedené.

- Checklist (kontrolní seznam) – Jedná se o jednoduchou metodu založenou na principu předem stanoveného seznamu kontrolních otázek, podle něhož postupujeme. V checklistu můžeme pracovat i s jednotlivými váhami daných parametrů, což může z jednoduché metody analýzy vytvořit složitý formulář.
- Safety audit - Bezpečnostní kontrola má za cíl vyhledat rizikové situace a doporučit opatření pro zvýšení bezpečnosti. Metoda je založena na hledání potenciálně možné nehody problému v daném systému za pomoci seznamu předem připravených otázek a matice pro hodnocení rizik.
- What – if analýza – Analýza toho, co se, když se zabývá dopady určených situací v provozu. K aplikaci této metody je potřeba několik osob, které znají dobře organizaci a její procesy, na základě čehož si kladou otázky „co se stane když …“ o možných nehodách v provozu.

- Preliminary Hazard Analysis (PHA) –Je to předběžná analýza ohrožení, jejímž úkolem je kvantifikace, která se zabývá vyhledáváním nebezpečných stavů a nouzových situací, ale také jejich příčin a dopadů jejich zařazení do předem definovaných kategorií. Pod názvem PHA se skrývá souhrn technik vhodných k posouzení rizik.
- Process Quantitative Risk Analysis (QRA) – Systematicky a komplexně přistupuje k předpovědi četnosti a dopadů nehod analýza kvantitativních rizik. U této analýzy jsou rozlišovány verbální a číselné hodnoty. Tato analýza je pokročilá, vyžaduje náročnou databázi a počítačovou podporu.
- Hazard Operation Process (HAZOP) – Tato metoda hodnotí rizika dle pravděpodobnosti, kterou jim určíme za pomoci brainstormingu. Výstupy jsou zapisovány do tabulek. Závěrem jsou formulovány dopady, kterou jsou pro fungování systému nepřijatelné a navrhnuta doporučení ke zlepšení procesů. Jedná se o univerzální metodu, kterou lze použít v řadě oborů.
- PNH metoda (PNH) - Jedná se o jednoduchou bodovou polo-kvantitativní metodu analýzy rizik, která při výpočtu celkové míry rizika počítá s hodnotami pravděpodobnosti vzniku situace, možných následků rizika a názoru hodnotitele na míru rizika.
- Event Tree Analysis (ETA) – Metoda ETA je graficko statistickou metodou analýzy rizik, při které je názorně vyobrazen strom událostí, obvykle ve formě rozvětveného grafu s popisem, obsahující možné události, které mohou v daném systému nastat.
- Failure Mode and Effect Analysis (FME) – Analýza selhání a jejich dopadů je metodou založenou na hledání dopadů a příčin prostřednictvím strukturovaně vymezených selhání zařízení. Tato metoda se využívá pro významná rizika, kde se očekává kvantitativní přístup řešení. Je to složitější metoda, která vyžaduje rozsáhlou databázi a odpovídající počítačovou techniku.
- Fault Tree Analysis (FTA) – Tato analýza postupuje zpětně za pomoci řetězce příčin, které mohou vést k vybrané události. Tato metoda je graficko analytická,

podobná metodě ETA, kdy rozkreslený graf opět připomíná rozvětvený strom. Cílem této metody je určení pravděpodobnosti vzniku vrcholové události.

- Human Reliability Analysis (HRA) – Jedná se o metodu zabývající se lidským faktorem, jakožto původcem výskytu pohrom, nehod, havárií a útoků. Analýza lidské spolehlivosti přistupuje k hodnocení lidského faktoru z mikro ergonomického hlediska (vztah člověk – stroj) i makro ergonomického hlediska (vztah člověk – technologie). Analýza je zaměřena také na dodržování aktuálně platných pracovních předpisů a bezpečnost práce.
- Fuzzy Set and Verbal Verdict Method (FL-VV) – Metoda mlhavé logiky verbálních výroků je multikriteriální metodou rozhodovací analýzy založenou na jazykové proměnné. Využívají se zde otázky stejného typu, jako u metody WHAT IF. Metoda je velmi účinná, oblíbená a časově nenáročná, její výpovědní hodnota však stojí na pracovním týmu, který ji sestavoval. Musí se jednat o pracovníky s dostatečnou znalostí daného provozu i s touto metodou.
- Relative Ranking (RR) - Relativní klasifikace je strategií umožňující analytikům rozpoznat vlastnosti několika procesů nebo činností a určit, zda jsou takové procesy nebezpečné natolik, aby proběhlo jejich další zkoumání.
- Causes and Consequences Analysis (CCA) - Analýza příčin a dopadů kombinuje metody stromu poruch a analýzu stromu událostí. Diagram příčin a dopadů má významnou výpovědní hodnotu, protože reflektuje vztahy mezi koncovými stavy nehody a základními příčinami.
- Probabilistic Safety Assesment (PSA) - Metoda pravděpodobnostního hodnocení zobrazuje zranitelnost jednotlivých částí systému a vyjadřuje, nakolik se dané části podílejí na celkové zranitelnosti systému. Jedná se o metodu často využívanou k modelování scénářů jaderných havárií.
- Indexové metody – Tyto metody byly obvykle zavedeny konkrétním výrobním podnikem a kromě základních zohledňovaných faktorů pracují i s dalšími parametry dle dané výroby, např. s toxicitou látek. (Šefčík, 2015)

S ohledem na zaměření diplomové práce na oblast kybernetické bezpečnosti, je nutné zdůraznit, že analýza rizik hraje důležitou roli při compliance systémů.

Základním procesem před samotnou analýzou rizik je zmapování organizace, jejích chráněných aktiv a hrozeb, kterým by mohla čelit. Následně mohou být přijata ochranná opatření a zavedeny kontroly, zda jsou přijatá opatření dodržována a jak jsou efektivní.

K nastavování opatření a kontrol lze přistoupit buď plošně, tzn. opatření a kontroly nastavit tak, aby pokryly maximum aktiv a možných hrozeb), nebo přijímaná opatření přizpůsobit konkrétní situaci ve společnosti. Ve druhém případě je vhodným nástrojem k zohlednění závažnosti rizik, kterým daná organizace čelí právě analýza rizik.

Přesto, že plošný způsob je jednodušší a rychlejší variantou, nedokáže se dostatečně přizpůsobit aktuální situaci v organizaci, ani dostatečně neodráží závažnost a důsledky jednotlivých rizik. Tato varianta je tedy vhodnější a častěji používaná menšími organizacemi. Vyhláška o kybernetické bezpečnosti pak některým subjektům přímo určuje, že si musí zvolit druhou variantu. (Nonnemann, Červený a Vítek, 2022)

Shrnutí kapitoly

Poslední kapitola teoretické části této diplomové práce obsahuje definici analýzy rizik a základní popis vybraných metod analýzy rizik. Vysvětluje také důležitost analýzy rizik při výběru opatření, která budou chránit aktiva organizace před obávanými hrozbami.

II. PRAKTICKÁ ČÁST

4 OBEC S ROZŠÍŘENOU PŮSOBNOSTÍ

Veřejnou správou je chápáno řízení záležitostí státu ve věcech veřejných prostřednictvím určitých činností a osob nebo institucí. Veřejná správa se vyznačuje potřebou institucionálního a organizačního zajištění společnosti, zajištění udržitelnosti žádoucího stavu, naplnění cílů a programů stanovených na základě rozhodnutím vlády, nebo zastupitelstev. Veřejná správa je vykonávána ve veřejném zájmu, tedy s cílem, který je společnosti ku prospěchu. Samospráva a státní správa jsou dvě složky veřejné správy, díky níž jsou zajištěny služby veřejnosti.

Samosprávu vyjadřuje autonomní řízení. Lze ji dělit na územní a zájmovou. Česká republika je členěna na menší územně samosprávné celky, kterými jsou obce a na vyšší územně správní celky, kterými jsou kraje. Obce a kraje jsou tak schopny rozhodovat o svých záležitostech samy. Zájmová samospráva se týká subjektů, které spojuje společný zájem, jako je profese (např. Česká komora daňových poradců) nebo zájem (např. akademické obce).

Státní správa je jádrem veřejné správy, je uskutečňována jménem a v zájmu státu. Prostřednictvím státní správy je realizována výkonná moc státu a vyznačuje se především svým prováděcím (provádění zákonů), podzákonným (řídí se zákony) a nařizovacím charakterem (vydává závazné správní akty). V závislosti na subjektech, které státní správu vykonávají, je státní správa vykonávána buď přímo, nebo nepřímo. V případě přímé státní správy je činnost vykonávána bezprostředně státními orgány. Nepřímá státní správa, je vykonávána v tzv. přenesené působnosti veřejnoprávními korporacemi (obce, kraje), ale i fyzickými a právnickými osobami (výkon státní správy jim byl propůjčen na základě zákona, např. stanice technické kontroly, nebo lesní stráž). Působnost státní správy vyjadřuje okruh svěřených úkolů a je dělena na působnost věcnou, územní a osobní. (Kadečka a Rigel, 2009)

Objem výkonu přenesené působnosti je určen zařazením obce do jednoho ze tří stupňů. Obce I. stupně vedou evidenci obyvatel, zajišťují konání voleb v obci a zajišťují veřejný pořádek na území obce apod. Obce II. stupně zajišťují určené agendy i za obce I. stupně na základě vzájemných dohod mezi těmito obcemi, nebo na základě rozhodnutí. Jedná se především o agendy matriky, nebo stavebního úřadu (obce s pověřeným obecním úřadem). Obce III. stupně označujeme jako obce s rozšířenou působností (dále jen „ORP“).

Agenda ORP je širší oproti obcím s pověřeným obecním úřadem např. o vydávání cestovních a osobních dokladů, řidičských oprávnění, vyplácení sociálních dávek, péči o nepřizpůsobivé občany, živnostenskou agendu apod. Do této kategorie jsou zařazena také statutární města, městské části a obvody hlavního města Prahy.

Ve Zlínském kraji je zajištěn výkon státní správy prostřednictvím 13 ORP:

- Bystřice pod Hostýnem,
- Holešov,
- Kroměříž,
- Luhačovice,
- Otrokovice,
- Rožnov pod Radhoštěm,
- Uherské Hradiště,
- Uherský Brod,
- Valašské Klobouky,
- Valašské Meziříčí,
- Vizovice,
- Vsetín
- a Zlín. (Český statistický úřad, 2018)

Správní obvody ORP respektují hranice krajů, a jsou stanoveny vyhláškou Ministerstva vnitra č. 346/2020 Sb., o stanovení správních obvodů obcí s rozšířenou působností, území obvodů hlavního města Prahy a příslušnosti některých obcí do jiného okresu.

ORP Uherské Hradiště

Město Uherské Hradiště je významným historickým městem, které se nachází na jihovýchodě Moravy. V 9. a 10. století patřilo území, na kterém se dnes město rozprostírá, k jádru Velké Moravy. Založení města českým králem Přemyslem Otakarem II. je datováno do roku 1257. Hlavním záměrem k založení města byla ochrana jižní a východní hranice a velehradského kláštera před nájezdy cizích vojsk. Ve 14. století bylo město obehnáno kamennou hradbou, jejíž pozůstatky jsou dodnes součástí centra města.

Ve středověku, především na přelomu 15. a 16. století, mělo Uherské Hradiště významné postavení, disponovalo četnými privilegii. Město bylo situováno na ostrov Sv. Jiří a bylo nazýváno „Novým Velehradem“. Následující staletí bylo město mnohokrát pokoušeno nepřátelskými vpády a vojenskými střety, ale i požáry a epidemiemi. V 19. století se město začalo rozvíjet a rozšiřovat i za hranice původních hradeb, až postupně dospělo k dnešní podobě. Celý historický vývoj města se nezpochybnitelně odrazil v životech jeho obyvatel, ale i v architektonickém vzhledu města.

Město je charakteristické svými dvěma náměstími, které spojuje dnešní Prostřední ulice s budovou Staré radnice. Uherské Hradiště vzniklo v půli cesty mezi obcemi Kunovicemi a Starým Městem a bylo složeno z obyvatel těchto obcí. Tato centrální poloha v sídelní aglomeraci Kunovice-Uherské Hradiště-Staré Město činí z Uherského Hradiště vysoce atraktivní lokalitu jak z pohledu bydlení, obchodu, pracovních příležitostí, ale i kultury, sportu a společenského vyžití.

Průmysl je koncentrován především v uvedené městské aglomeraci Kunovice - Uherské Hradiště - Staré Město, dále pak do několika významnějších průmyslových středisek regionu jako jsou Buchlovice, Uherský Ostroh, nebo Hluk).

Uherské Hradiště je z pohledu regionů soudržnosti zařazeno do Zlínského kraje (NUTS 3) a spolu s Olomouckým krajem pak do regionu soudržnosti „Střední Moravy“ (NUTS 2). Uherskohradišťsko je v rámci Zlínského kraje jedním ze čtyř okresních obvodů (dalšími jsou Zlín, Vsetín a Kroměříž).

Dle dostupných informací Českého statistického úřadu k 01.01.2023 ve správním obvodu ORP Uherské Hradiště žije 89 803 obyvatel (z toho 48, 9 % mužů a 51,1 % žen). Hustota zalidnění v ORP Uherské Hradiště je na úrovni 173,4 osob na km^2. Statutem ORP město disponuje od roku 2003. Přirozený přírustek ORP činil v roce 2022 zápornou hodnotu 251 osob (tzn. že zemřelých bylo více než nově narozených). Kladný přírustek obyvatel byl zaznamenán v oblasti migrace (více přistěhovalých než vystěhovalých obyvatel) a to o celých 1400 osob.

Nezaměstnanost v této oblasti činila v roce 2022 3,34 %. Počet ekonomických subjektů v ORP Uherské Hradiště (tzn. subjekty se sídlem podnikání v ORP) přesáhl hranici 22 000 (jak z řad fyzických, tak právnických osob).

Z uvedeného množství fyzických a právnických podnikajících osob se v 24 % zaměřovalo podnikání do oblasti obchodu, ubytování, stravování a pohostinství, v 16,5 % do oblasti průmyslu, v 12,2 % do stavebnictví a necelých 5 % subjektů podnikalo v oblasti zemědělství, lesnictví a rybářství.

Z pohledu organizace veřejné správy je Město Uherské Hradiště tzv. obcí III. stupně, tedy obcí s rozšířenou pravomocí. Jedná se tedy o obec, která má nejširší rozsah působnosti v oblasti výkonu státní správy v přenesené působnosti. Toto zařazení znamená, že Uherské Hradiště vykonává státní správu v rámci přenesené působnosti i za obce I. a II. stupně spadající do jejího obvodu. Správní obvod ORP Uherské Hradiště zahrnuje 48 obcí (z toho 5 obcí se statutem města a 3 obce se statutem městyse). Z pohledu počtu obcí se tak jedná o největší správní obvod ve Zlínském kraji.

Samotné město Uherské Hradiště je složeno ze sedmi územních částí, kterými jsou Jarošov, Mařatice, Míkovice, Rybárny, Sady, Vésky a Uherské Hradiště. Město má dle dostupných údajů ČSÚ ke dni 01.01.2023 celkem 24 812 obyvatel (z toho 47,6 % mužů a 52,4 % žen).

Uherské Hradiště se geograficky rozkládá v Dolnomoravském úvalu na dolním toku řeky Moravy, přibližně 3 km nad soutokem řeky Moravy s řekou Olšavou. Charakter krajinné struktury je významně ovlivněn faktem, že město vzniklo na spletité síti říčních ramen a v údolních nivách řek Moravy a Olšavy, kromě těchto dvou toků je krajina bohatá na mrtvá a slepá říční ramena s rozmanitou krajinnou vegetací, periodicky zaplavované lužní lesy a trvalé travní porosty. Typickým prvkem krajiny v této oblasti jsou také široké lány polí. Ve východní části území města se rovina mění ve výběžek Vizovické vrchoviny, a tím i v krajinu vinohradů, mozaiku křovin a lučních porostů, uprostřed mezi urbanizovanou a intenzivně obhospodařovanou krajinou. (Město Uherské Hradiště, 2024); (ČSÚ ČR, 2023)

Město se nachází v nadmořské výšce 179 m n. m., a jeho celková rozloha činí 21 km2. Uherské Hradiště je zásobováno pitnou vodou z přilehlých zdrojů pitné vody v obcích Salaš, Ostrožská Nová Ves a Kněžpole. Zásobování města plynem je realizováno prostřednictvím vysokotlakého plynovodu ze stanice Hodonín. Elektrická energie je dodávána vedením velmi vysokého napětí z rozvodny Otrokovice. Transformovna elektrického napětí je umístěna v místní části Rybárny.

Vzhledem k tomu, že řeka Morava, která lemuje město a tvoří pomyslnou hranici mezi Uherským Hradištěm a Starým Městem, je dominantním prvkem oblasti, je město zatíženo rizikem povodní. Výše na toku řeky se do řeky Moravy vlévá řeka Bečva, která má z velkých toků nejvýznamnější vliv na výšku hladiny řeky Moravy, ze středních toků je to pak řeka Olšava, která se do Moravy vlévá až pod Uherským Hradištěm, ale ovlivňuje městské části Sady, Vésky a Míkovice. Pro městskou část Jarošov je ohrožením také potok Březnice.

Uherské Hradiště je také významným dopravním uzlem. Uherské Hradiště leží na východo-západní spojnici Brna a slovenského Trenčína, tedy na silnici E/50. Významné jsou také silnice E/55-R/55 a E/57-E/49 propojující Opavu, Vsetín a Uherské Hradiště. Státní komunikace E/497 pak zajišťuje spojení mezi Uherský Hradištěm a krajským městem Zlín. Aktuálně velmi významná pro region je stavba dálnice D55, která má spojit Olomouc a Břeclav. Probíhající výstavba úseků Napajedla-Babice, Babice-Staré Město, Staré Město – Moravský Písek po svém dokončení významně zpříjemní a urychlí cestování a značně přispěje k napojení Uherskohradišťska na celorepublikovou silniční a dálniční síť.

S ohledem na intenzitu dopravy, která je nyní vedena centrem Uherského Hradiště, je dokončení dálnice D55 a tím očekávané zmírnění přetíženosti komunikací v centru města, napjatě očekáváno. Významnou roli má Uherské Hradiště také v železniční dopravě, kdy město leží na přípojné trati Staré Město u Uherského Hradiště – Bylnice, která navazuje na 2. tranzitní železniční koridor. Uherským Hradištěm a sousedním Starým Městem projíždí významné železniční spoje propojující slováckou metropoli s největšími českými městy jako je Praha, Brno a Ostrava. Uherské Hradiště a region Slovácka je atraktivní oblastí České republiky v oblasti turismu a kultury. Tradice a folklór udržované v tomto regionu jsou oblíbené nejenom mezi místními, ale i turisty. Rovinatá krajina, ale i přilehlé Buchlovské hory přitahují nejen pěší, ale i cykloturisty. Z nejvýznamnějších kulturních akcí stojí za zmínku Slovácké slavnosti vína a otevřených památek, Letní filmová škola, nebo Slovácké beachové léto. Město je lákavé také řadou působivých historických památek. (Město Uherské Hradiště, 2024); (Rašticová, 2018); (Český statistický úřad, 2023); (Povodňové plány, 2013); (Ceskedalnice.cz, 2023)

5 VÝKON STÁTNÍ SPRÁVY V OBCI S ROZŠÍŘENOU PŮSOBNOSTÍ

K výkonu státní správy jsou na ústřední úrovni zřízena ministerstva (celkem 14 ministerstev) v souladu se zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky. Mimo ministerstva jsou na základě uvedeného zákona zřízeny také jiné orgány státní správy:

- Český báňský úřad,
- Český statistický úřad,
- Český telekomunikační úřad.
- Český úřad zeměměřičský a katastrální,
- Energetický regulační úřad,
- Národní bezpečnostní úřad,
- Správa státních hmotných rezerv,
- Státní úřad pro jadernou bezpečnost,
- Úřad pro ochranu hospodářské soutěže,
- Úřad průmyslového vlastnictví a
- Úřad vlády České republiky.

V některých případech je státní správa vykonávána bezpečnostními sbory státu, kterými jsou:

- Bezpečnostní informační služba,
- Celní správa České republiky,
- Generální inspekce bezpečnostních sborů,
- Hasičský záchranný sbor České republiky,
- Policie České republiky,
- Úřad pro zahraniční styky a informace a
- Vězeňská služba České republiky.

Výkon státní správy v ORP Uherské Hradiště

S ohledem na výše uvedené statistické údaje o oblastech, které jsou nejčastějším cílem kybernetických útoků, byl pro praktickou část této diplomové práce zvolen právě státní sektor, který zaujímá první místo nejenom v tuzemsku, ale i v rámci Evropy.

V Uherském Hradišti, jakožto v okresním městě se nachází řada organizací, kterým přísluší výkon státní správy a mohly by se tedy potenciálně stát terčem kybernetického útoku. Konkrétně lze jmenovat instituce:

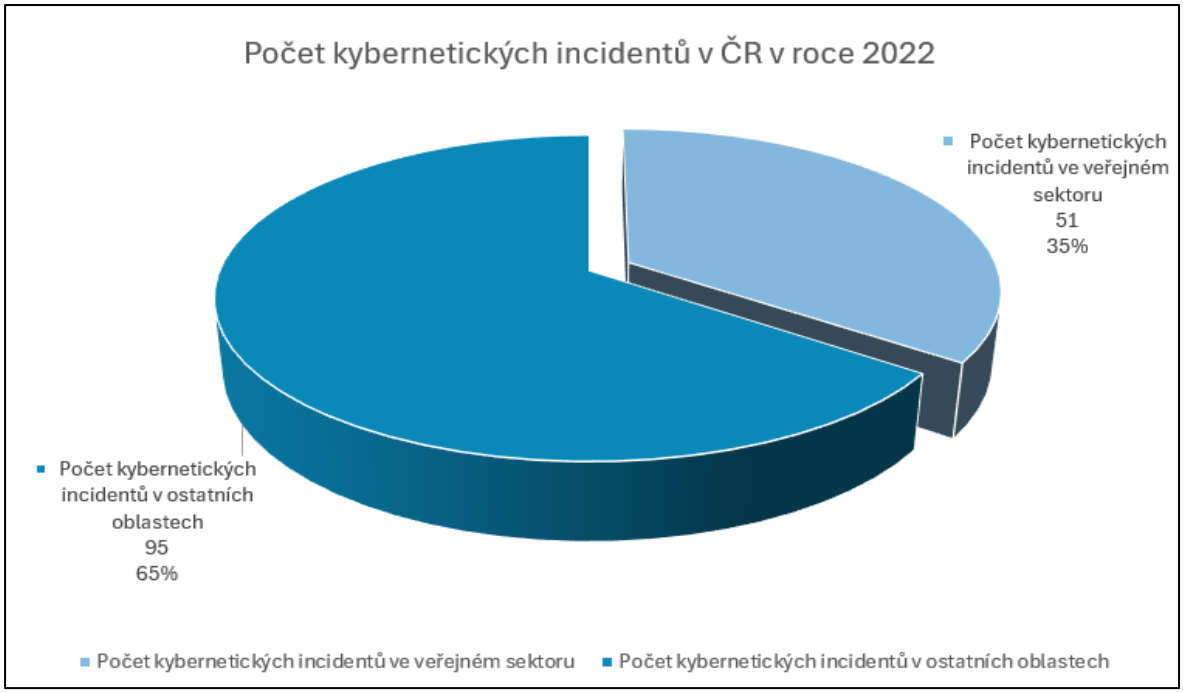
- Celní úřad pro Zlínský kraj, Územní pracoviště v Uherském Hradišti,
- Finanční úřad pro Zlínský kraj, Územní pracoviště v Uherském Hradišti,
- Hasičský záchranný sbor Zlínského kraje, Územní odbor Uherské Hradiště,
- Katastrální úřad pro Zlínský kraj, Katastrální pracoviště Uherské Hradiště,
- Krajská hygienická stanice Zlínského kraje, územní pracoviště Uherské Hradiště,
- Krajská veterinární správa pro Zlínský kraj – Oddělení veterinární hygieny Uherské Hradiště,
- Krajské ředitelství policie Zlínského kraje, Územní odbor Uherské Hradiště,
- Městský úřad Uherské Hradiště,
- Okresní soud v Uherském Hradišti,
- Okresní správa sociálního zabezpečení Uherské Hradiště,
- Okresní státní zastupitelství v Uherském Hradišti,
- Probační a mediační služba Uherské Hradiště,
- Státní pozemkový úřad, pobočka Uherské Hradiště,
- Úřad práce České republiky, Kontaktní pracoviště Uherské Hradiště,
- Úřad pro civilní letectví, oblastní kancelář Morava,
- Úřad pro zastupování státu ve věcech majetkových, odloučené pracoviště Uherské Hradiště,
- aj.

Statistika

Z údajů dostupných v poslední zveřejněné Zprávě o stavu kybernetické bezpečnosti (tedy Zprávě o stavu KB za rok 2022) jsou nejčastějšími cíli kybernetických útoků v sestupném pořadí dle množství hlášených incidentů:

- státní sektor,
- finanční sektor,
- průmysl a energetika,
- zdravotnictví,
- vzdělávání a
- digitální služby.

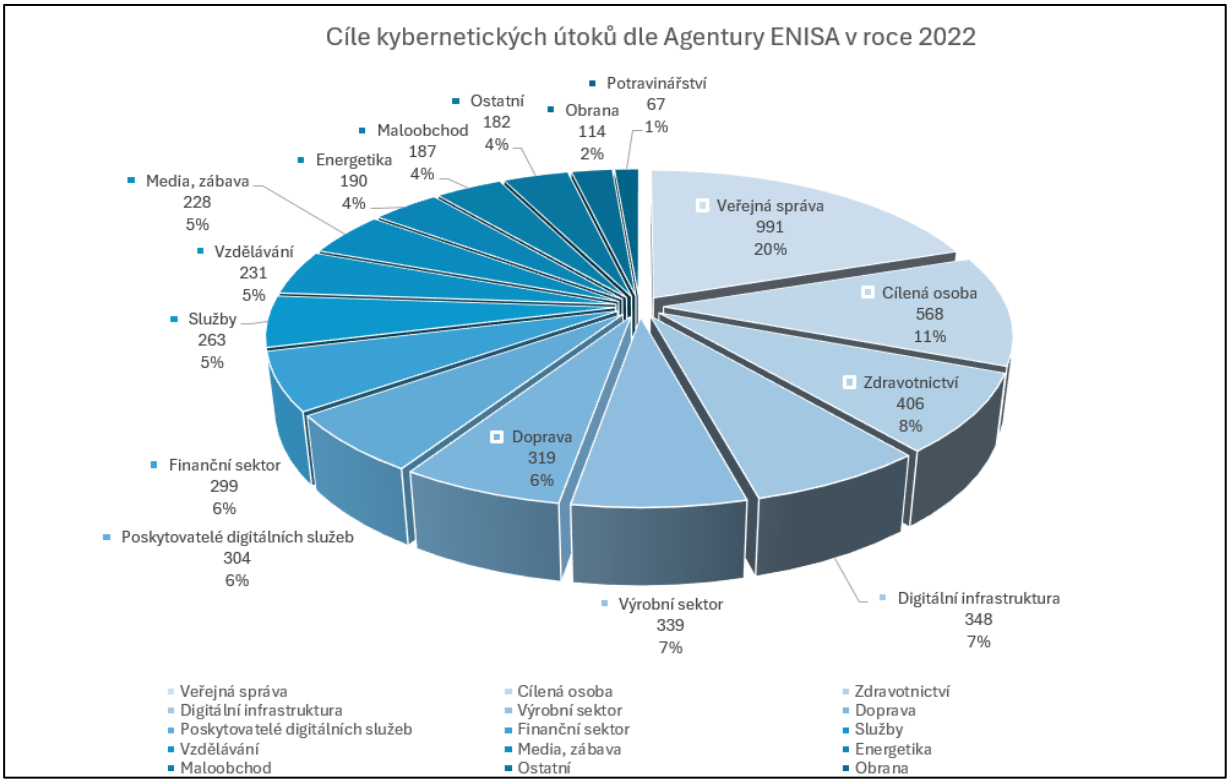
NÚKIB uvádí, že počet incidentů v oblasti státního sektoru z hlediska počtu útoků v roce 2022 klesl, proti roku předešlému. V této oblasti NÚKIB evidoval celkem 51 kybernetických incidentů namířených proti státnímu sektoru, což tvoří více než třetinu celkového počtu (146) kybernetických incidentů, které NÚKIB v daném roce řešil.



Obrázek 3 – Počet kybernetických incidentů v ČR v roce 2022 (zdorj: NÚKIB, 2023)

NÚKIB v této věci také zveřejnil výsledky dotazníkového šetření ve věci kybernetické bezpečnosti, ze kterého vyplývá, že přes pokles počtu samotných útoků naopak vzrostl počet respondentů negativně hodnotící stav kybernetické bezpečnosti v organizacích. Častým důvodem nespokojenosti s aktuálním stavem byl uváděn snížený rozpočet organizace na oblast kybernetické bezpečnosti. (NÚKIB, 2023)

Agentura ENISA informovala o cílech kybernetických útoků v Evropě. Stejně jako v tuzemsku, i v rámci Evropy počty kybernetických útoků směřovaných proti veřejné správě zaujímají první příčku v žebříčku cílů. Poměrově lze také říct, že v ČR jsou kybernetické útoky směřované proti veřejnému sektoru stejně časté, jako v Evropě.



Obrázek 4 - Cíle kybernetických útoků dle Agentury ENISA v roce 2022 (zdroj: ENISA, 2023)

6 ANALYZOVÁNÍ KYBERNETICKÝCH RIZIK VYBRANÉ ORGANIZACE

Z předcházející kapitoly bezesporu vyplývá, že nejčastějším terčem kybernetických útoků je veřejná správa. Tato kapitola se zaměřuje na jednu konkrétní organizaci z oblasti veřejné správy v ORP Uherské Hradiště a její bližší analýzu kybernetických rizik.

Z důvodu citlivosti údajů, ze kterých autor této diplomové práce vychází a jejich možnému zneužití proti analyzované organizaci, byla na základě vzájemné dohody mezi autorem práce a touto organizací domluvena anonymita organizace, která byla podmínkou pro sdílení informací. S ohledem na skutečnost, že práce je zaměřena na ORP Uherské Hradiště, analyzovaný subjekt je specifikován pouze do té míry, aby nebylo možné jej přesně identifikovat a vystavit ho tak hrozbám vyplývajícím ze zneužití zveřejněných informací.

Data byla získávána na základě strukturovaného rozhovoru se dvěma zástupci organizace (jeden pracovník na vedoucí pozici a jeden pracovník výhradně se zabývající kybernetickou bezpečností). Otázky k rozhovoru byly zpracovány na základě ***Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti***, který je podpůrným materiálem vydaným NÚKIB ve spolupráci s dalšími subjekty, k přiblížení problematiky řízení aktiv a rizik, jak organizacím bez dosavadních zkušeností, tak zkušenějším subjektům k rozšíření možností a vylepšení dosavadních postupů. Základní principy byly po konzultací s pracovníky organizace přizpůsobeny prostředí organizace. (NÚKIB et al., 2022)

6.1 Vybraná organizace z oblasti státní správy

Z kategorie státní správy byl vybrán objekt, který bude v této diplomové práci označován jako „Subjekt A“. Subjekt A je orgánem vykonávajícím jednu z oblastí státní správy.

Předmětem činnosti subjektu je výkon veřejné správy. Subjekt A je orgánem moci výkonné a také jejím vykonavatelem. Daný subjekt v hierarchii organizace spadá pod ústředí organizace, v čele s ústředním ředitelem, sídlícím v Praze, jemuž je nadřízeno věcně příslušné ministerstvo. V okresních a krajských městech jsou poté rozmístěna pracoviště na stejné úrovni, jako je pracoviště subjektu v Uherském Hradišti, v jejich čele je ředitel.

Předmětem činnosti Subjektu A je správa a vedení komplexní příslušné agendy v dotčené oblasti s ohledem na místní příslušnost, výplata dávek, kontrolní a správní činnosti související s agendou subjektu, spolupráce a předávání informací a materiálů s dotčenými orgány státní správy a dalšími zainteresovanými subjekty. Mimo uvedené agendy je klientům poskytována také poradenská a konzultační činnost, a to jak na okresních pracovištích, tak na ústřední úrovni. Poradenská a konzultační činnost probíhá prostřednictvím osobních konzultací, telefonických hovorů, nebo prostřednictvím elektronické komunikace s klienty (datová schránka, emailová schránka, klientský portál).

Organizace využívá programu pro zajištění spisové služby program elektronické spisové služby přes externího dodavatele. Program zajišťuje veškeré činnosti související s přijímáním, evidencí, přerozdělováním, zpracováváním, vyřizováním, odesíláním, ukládáním a vyřazováním dokumentů. Každý dokument, který organizace oficiálně obdrží a vyhotoví je evidován tímto programem.

Organizace spravuje klientský portál, který usnadňuje klientům komunikaci s organizací prostřednictvím vzdáleného přístupu. Přístup veřejnosti k portálu je zajištěn prostřednictvím bankovní identity, nebo identity občana.

Personální systém organizace zajišťuje výkon činnosti organizace prostřednictvím vlastních pracovníků. Úklidová služba a bezpečnostní služba je řešena prostřednictvím outsourcingu. Personální agenda obsahuje množství citlivých osobních údajů o zaměstnancích organizace, nákladech na jejich mzdy, jejich finančních poměrech (zpracování daňového přiznání, exekuce apod.).

Interní komunikace, aktuální informace a dostupnost vnitřních právních předpisů a řádů a interních dokumentů je zajištěna prostřednictvím Intranetu organizace, který je dostupný zaměstnancům pouze po přihlášení.

Organizace také využívá několik celostátních databází (např. ROS – Registr osob, ROB – Registr obyvatel apod.) a specifických aplikací vytvořených přímo pro konkrétní agendy a používaných výhradně pro správu dané agendy. Nejzásadnější pro výkon činnosti organizace jsou čtyři konkrétní aplikace.

Dále je nutno uvést, že s ohledem na skutečnost, že jde o organizaci státní správy, veškeré kroky a praktiky v oblasti řízení informací jsou dlouhodobě uskutečňovány v souladu se zákonem o KB, souvisejícími právními předpisy a mezinárodně platnými standardy ISO/IEC 27001.

Osoby podílející se na řízení aktiv a rizik

Vzhledem ke skutečnosti, že zkoumaná organizace je nižším stupněm pracoviště a je v oblasti řízení aktiv a rizik řízena svým ústředním orgánem, v jehož čele je ředitel, je výbor pro řízení kybernetické bezpečnosti organizace zřízen na centrální úrovni organizace. Vrcholové vedení orgnizace zodpovídá plně za systém řízení bezpečnosti informací (Information Security Management Systém, dále jen „ISMS“).

Výbor pro řízení kybernetické bezpečnosti organizace je ustanoven vrcholným vedením organizace a zaujímá funkci strategického a koordinačního orgánu, jehož úkolem je implementace a údržba ISMS. Mezi základní činnosti výboru patří tvorba rámce KB, definování cílů a směřování oblasti KB, definování rolí a odpovědnosti v rámci ISMS, definování požadavků na podávání zpráv a kontrolu ISMS, kontrola stavu KB a naplňování vytyčených cílů. Výbor je obsazen zástupci z vrcholového vedení organizace, z oblasti bezpečnosti, správy ICT, legislativní činnosti, ekonomické činnosti a personální činnosti organizace. Členy výboru mohou být také manažer KB a architekt KB. Dle potřeby je možné přizvat další odborníky, kteří budou mít však hlas pouze poradní.

Manažer KB je osobou, která zastává roli tzv. jednotného kontaktního místa pro oblast kybernetické bezpečnosti. Část činností souvisejících s kybernetickou bezpečností vykonává sám, jiným dohlíží. Manažer KB je zodpovědný především za řízení ISMS, komunikace a pravidelné informování vrcholového vedení organizace, komunikace s GovCERT/CSIRT, podílení se na řízení aktiv a rizik, koordinování činností při řízení kybernetických bezpečnostních incidentů, vyhodnocování vhodnosti a účinnosti bezpečnostních opatření apod.

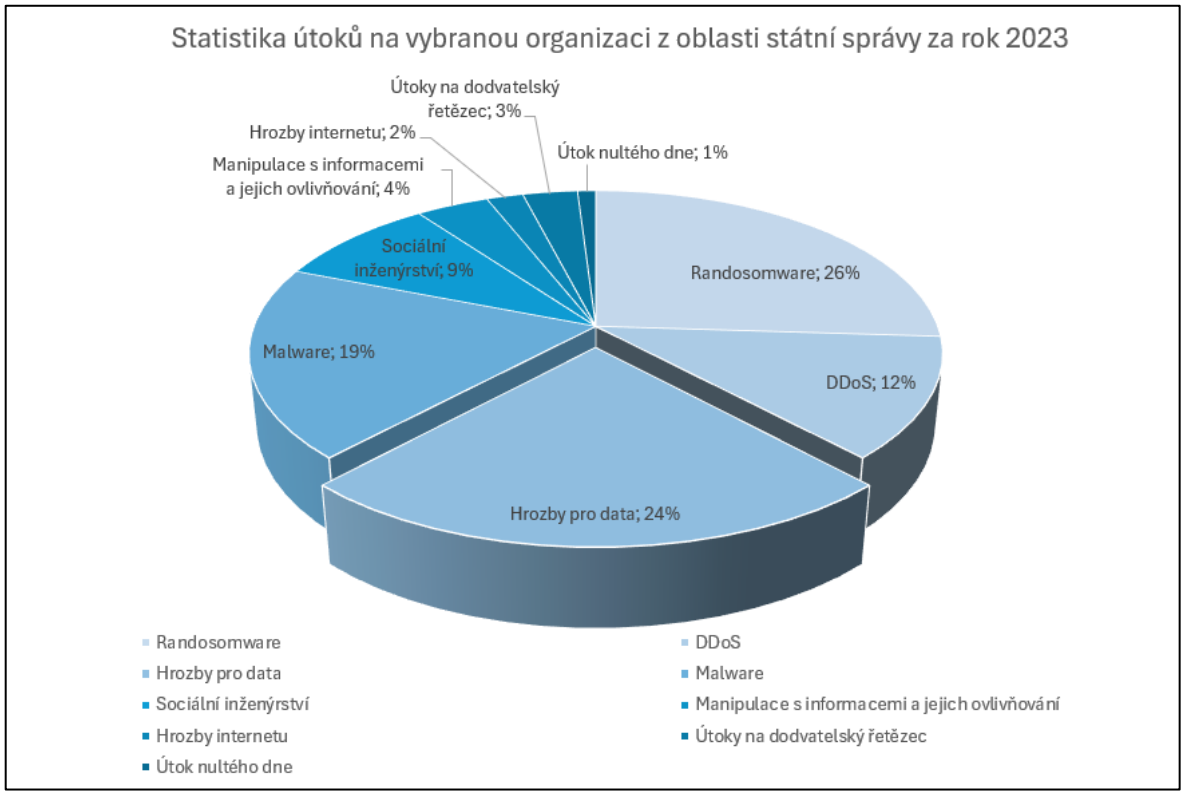
Garant aktiva je role, která vyžaduje dokonalou znalost aktiva organizace. Jeho funkce se především uplatňuje při procesu řízení a hodnocení aktiv a rizik a výběru vhodných bezpečnostních opatření. V případě zkoumané organizace je tato role zdvojená, kdy nejvýše postavený pracovník, pod kterého aktivum spadá je označován jako gestor aktiva, který určí garanta aktiva, který je mu podřízen.

Architekt KB zajišťuje bezpečnou výstavbu IS s ohledem na potřeby organizace. Odpovídá za navržená implementační opatření a zajišťuje architekturu bezpečnosti. V souladu s Vyhláškou o KB a „dobrou praxí“ nesmí být tato role zajištěna architektem IT, který je odpovědný za návrh vhodné aplikační a technologické architektury organizace, ale ani prostřednictvím vedoucího pracovníka IT.

Auditor KB je osobou odpovědnou za provedení auditu KB organizace. Tato funkce je z principu neslučitelná s rolemi manažera a architekta KB, z důvodu, že by nebyla zajištěna nestrannost auditora k hodnocení souladu SIMS s realizovanými bezpečnostními opatřeními, bezpečnostní politikou, standardy apod. V případě zkoumané organizace je role auditora KB zajištěna externě. (NÚKIB et al., 2022)

Statistika kybernetických útoků na vybranou organizaci za rok 2023

Organizace poskytla autorovi práce informace o charakteru kybernetických útoků na organizaci za rok 2023, konkrétní počty útoků nebyly sděleny. Organizace však musí čelit kybernetickým hrozbám denně. Charakter ani počet útoků se nijak výrazně neliší od dat zveřejněných NÚKIB za celou republiku, ani od dat zveřejněných agenturou ENISA pro Evropu. Zkoumaná organizace na úrovni ORP nemusela v roce 2022 řešit incident, který by musel být ohlášen NÚKIB.



Obrázek 5 – Statistika útoků na vybranou organizaci státní správy za rok 2023 (zdroj: organizace, zpracování vlastní)

6.2 Aktuální stav zabezpečení organizace

Celkové zabezpečení organizace bylo rozděleno do dvou hlavních oblastí. Fyzická ochrana objektu představuje výčet bezpečnostních řešení, které jsou vzájemně kombinovány a tím se zvyšuje jejich efektivita. Z velké části se nejedná o řešení, která prioritně zajišťují kybernetickou bezpečnost organizace, ale spíše o obecné bezpečnostní prvky, které zajišťují ochranu objektu a tím pomáhají eliminovat přístup nepověřených osob k chráněným aktivům organizace.

Druhou kategorií je pak bezpečnost sítí a služeb organizace. Tato kategorie je již přímo zacílena na bezpečnost kybernetickou, a to jak na bezpečnost zařízení (počítačů, tiskáren apod.), tak bezpečnost síťovou, uživatelskou a aplikační. Vzájemná kombinace opatření z těchto kategorií může vytvořit adekvátní bezpečnostní štít organizace v této oblasti. S ohledem na rychlý pokrok v oblasti ICT, je nutností vytrvalá bdělost a připravenost čelit novým druhům hrozeb.

6.2.1 Fyzická ochrana objektu

Základním prvkem fyzické bezpečnosti je zajištění bezpečnosti objektu tak, aby každá cizí osoba, která do objektu vstupuje měla pocit, že se o její přítomnosti ví a její pohyb je monitorován. K tomuto účelu dobře slouží vrátnice, přes kterou (případně kolem které) musí osoby z vnějšku organizace projít. Objekt organizace disponuje vrátnicí, která je umístěna při hlavním vstupu do budovy. Po celý čas, kdy je budova otevřena pro veřejnost, je zajištěna přítomnost pověřeného pracovníka.

Budova je dále u vstupních dveří opatřena kamerovým systémem. Kamerový systém čítající tři kamery (dvě otočené tak, aby byl monitorován hlavní prostor bezprostředně před budovou organizace a jednu kameru u vstupu do objektu). Zbytek objektu není kamerami monitorován. Okolí budovy je v zorném dosahu jedné z kamer městského kamerového dohlížecího systému. Záznamy z tohoto systému jsou monitorovány stálou službou městské policie s cílem sledování problematických lokalit a předcházení, ale i objasňování trestné činnosti.

Přístup do budovy bez autorizace je možný pro veřejnost pouze ve vyhrazených časech. Mimo tyto časy je budova přístupna pouze zaměstnancům na základě zaměstnaneckých čipů, díky kterým je monitorován průchod zaměstnanců a počet zaměstnanců nacházejících se v budově. Zaměstnanci nedisponují klíčem, který by jim umožnil přístup do budovy.

Čas, po který se mohou zaměstnanci zdržovat na pracovišti je také konkrétně vymezen. Mimo tuto dobu je budova uzamčena a její otvírání a zavírání je záležitostí vrátného, správce budovy, nebo externí bezpečnostní služby. Klíč od budovy má k dispozici také ředitel organizace a jeho zástupce.

Vnitřní prostor budovy již není monitorován kamerami. Převážná většina (asi 90 %) techniky se nachází v kancelářských prostorách. Přístup do kanceláří mají zaměstnanci, jejich nadřízení a provozně techničtí pracovníci. Každý zaměstnanec disponuje klíčem od své kanceláře a klíčem od kanceláře kolegů, kteří vykonávají stejnou agendu (obvykle tedy v rámci oddělení). Vedoucí zaměstnanci mají přidělený klíč, který jim umožňuje přístup do všech prostor, ve kterých se pohybují jeho podřízení. Generální klíč je výsadou ředitele organizace a jeho zástupců. Kanceláře jsou z převážné většiny umístěny v patře budovy. Okna kanceláří nejsou opatřena mřížemi ani bezpečnostními zámky. S ohledem na jejich umístění v patře budovy.

Zaměstnanci jednotlivých oddělení využívají společné zázemí, ve kterém je umístěna společná tiskárna s kopírkou a skenerem a skartovačka. Zázemí je přístupné na základě použití čipu. V případě dvou oddělení je společná tiskárna umístěna na chodbě, která je přístupná veřejnosti a její využití je opět podmíněno použitím zaměstnaneckého čipu.

Na chodbách a v místnosti se společným zázemím jsou umístěny detektory kouře. Chodby, schodiště a vstupní prostor budovy jsou opatřeny detektory pohybu, které při zaznamenání pohybu mimo pracovní dobu aktivují alarm v budově. Spuštění alarmu je vázáno na externí bezpečnostní službu. Zároveň senzor zasláním zprávy informuje ředitele organizace, jeho zástupce a správce objektu. Toto bezpečnostní opatření je aktivováno v době, mimo časový interval, kdy je budova přístupna veřejnosti a zároveň také interval, kdy je budova přístupna pro zaměstnance. Na chodbě v každém patře a v přízemí je umístěno tísňové tlačítko.

Ochrana počítačových systémů je zajištěna fyzicky tak, že každý počítač se nachází v kanceláři, která je uzamčena a přístup do počítače je chráněn přihlášením, za běžného provozu by tak neměla neoprávněná osoba mít možnost dostat se do zařízení, ani být v místnosti se zařízením sama. Tiskárny jsou umístěny ve většině případů v místnosti, která je přístupna zaměstnancům na základě použití jejich zaměstnaneckého čipu, samotná funkce přístroje je zajištěna na stejném principu. Ve dvou případech je tiskárna volně dostupná na chodbě oddělení.

Samostatnou kapitolou je serverovna, která je základem počítačové infrastruktury celé organizace. Serverovna je umístěna v patře budovy, oddělena od prostor běžně dostupných veřejnosti. Její zabezpečení spočívá nejen v možnosti přístupu jen konkrétních osob (opět regulováno pomocí čipů), ale také zajištění specifického prostředí pro uložené technologie v podobě senzorů zajišťujících detekci požárů, vlhkosti, nebo teploty. Nezbytností je také zajištění kvalitního odvětrávání a klimatizace. Serverovna je vybavena rackovými skříněmi, ve kterých jsou uchovávány servery apod.

Pro případ živelné pohromy, kterou může být v ORP Uherské Hradiště nejpravděpodobněji povodeň způsobená vylitím řeky Moravy z koryta, je serverovna umístěna v patře budovy, tedy pravděpodobnost zaplavení je minimální.

Při správě nemovitosti je důraz kladen na splnění elektrotechnických a požárních předpisů, stejně jako na dodržování BOZP v celém objektu.

Aby bylo sníženo, nebo ideálně eliminováno riziko ztráty nebo poškození dat, musí být prováděny jejich zálohy. Redundance dat je organizací zajištěna procesním způsobem. Zálohovaná data jsou prioritně ukládána v cloudu, aby byla zajištěna jejich dostupnost nezávisle na místě pořízení, část dat je ukládána na externí uložiště.

6.2.2 Bezpečnost sítí a služeb

Počítačové sítě a jejich bezpečnost musí být v základě vhodně rozděleny. Zkoumaná organizace má odděleny počítačové systémy jednotlivých oddělení pomocí sítě VLAN a demilitarizovanou zónu (dále jen „DMZ“), taktéž oddělenou od ostatních počítačových systémů, jejíž součástí jsou společné servery. Zajištění společné komunikace mezi odděleními je řešeno povolením komunikace mezi jednotlivými VLAN a DMZ. Samozřejmostí zabezpečení počítačových systému organizace je firewall, filtrující vstupní data z prostředí internetu, čímž chrání zařízení, která jsou zapojena za touto bránou.

Připojení k internetu je zajištěno prostřednictvím optického kabelu odkud přes optický převodník signál předá do Wi-Fi routerů, které řídí lokální síť (LAN). Pomocí switche (přepínače) je zajištěno propojení routeru s jednotlivými počítači, tiskárnami a síťovým datovým uložištěm. Kamerový systém a zabezpečovací systémy objektu (detektory, tísňová tlačítka, apod.) jsou zapojeny pod vlastním swittchem.

Ochrana koncových zařízení, e-mailu a cloudových aplikací je řešena prostřednictvím antivirového systému. Součástí ochrany je také šifrování disků zařízení.

Ověřování uživatelů probíhá ve větší míře pomocí hesel do používaných systémů. Uživatele musí měnit svá přístupová hesla každých 6 měsíců, přičemž požadavky na heslo jsou stanoveny tak, že minimální délka hesla je 8 znaků, přičemž heslo musí obsahovat malé a velké písmeno, číslici a speciální znak. Přístupová oprávnění uživatele ke vstupu do aplikací jsou řízena na základě pracovního zařazení pracovníka. V menší míře, je používáno ověření uživatele na základě zaměstnaneckého čipu/karty (vstup do budovy, vstup do společných prostor, využití tiskárny, přístup k vybraným aplikacím apod.).

S ohledem na efektivitu práce a omezený počet pracovníků, je využíván vzdálený přístup administrátora k počítačovým systémům uživatele v případě řešení situací, se kterými si uživatel nedokáže poradit.

Správa a dohled nad počítačovou sítí probíhá pomocí logování procesů aplikací, díky kterým může správce sítě získat přehled a informace o funkci, nebo výskytu chyb aplikací a případně řešit nastavení aplikace.

Organizace se obvykle nesetkává s nutností řešit přenosné počítačové systémy (počítačové systémy odnášené mimo organizaci, ani cizí počítačové systémy připojované do sítě organizace), charakter činnosti organizace je vázán na pracoviště a absolutní většina počítačových zařízení není přenosného charakteru. V případě potřeby přenosu dat od klienta organizace do počítače pracovníka organizace, je využíváno posílání obsahu prostřednictvím datové nebo emailové schránky.

U všech kybernetických hrozeb platí, že nejslabším článkem řetězce je lidský faktor, tedy uživatel. K předcházení chyb způsobených uživatelem, organizace pořádá pravidelná školení zaměstnanců jednou ročně. Zaměstnanci spravující IT sítě prochází důkladnějším školením 2 – 3 ročně. Školení pro zaměstnance je organizováno v online formě je obvykle zaměřeno především na pochopení rizik spojených s přístupovými údaji do počítače i používaných aplikací. V této věci vydala organizace interní předpisy, kterým reguluje chování uživatelů při využívání IT zařízení.

Organizace má vytvořený plán, jak reagovat v případě významných kybernetických incidentů, jak již bylo v této práci jednou zmíněno, u zkoumané organizace (pracoviště na úrovni ORP) nebyl detekován kybernetický incident, který by musel být hlášen NÚKIB, nebo Úřadu pro ochranu osobních údajů. Přesto jsou pracovníci ICT oddělení, vybaveni kontakty, které v případě potřeby využijí. Bezpečnostní tým je pro tyto případy sestaven na ústředí organizace a v případě potřeby je postup komunikován.

Organizace aplikuje také technické opatření před ztrátou dat vinou uživatele (DLP), které spolu s uvedenými organizačními opatřeními pokrývá hrozby ze strany uživatele.

6.3 Hodnocení aktiv organizace

Pro hodnocení rizik organizace je v první řadě nutné definovat aktiva organizace, to znamená chráněné zájmy a hodnoty organizace.

V případě že by organizace neměla definována aktiva, nemohla by být přijatá bezpečnostní opatření efektivní, protože by nebyla správně zacílena. Organizace má definována níže uvedená aktiva. Organizace všechna uvedená aktiva považuje za primární.

Aktiva nejsou rozdělena do skupiny primární a podpůrné na základě zhodnocení celkových nákladů, které organizace vynaložila na získání a udržení aktiva, význam aktiva pro činnost organizace, náklady spojenými s dobou trvání škod na aktivech, jejich odstraněním, nebo jejich ztrátou. Organizace všem svým aktivům dává stejnou hodnotu. (Smejkal a Rais, 2013)

Primární aktiva:

- služby veřejnosti,
- data a informace.
- technické vybavení:
    - počítače,
    - tiskárny,
    - telefony,
- programové vybavení (software):
    - spisová služba,
    - speciální aplikace,
    - systémový software,
    - databázový systém,
- zálohovaná data,
- lidské zdroje.

6.4 Hrozby a zranitelnosti

Pro zkoumanou společnost byly určeny uvedené hrozby, které byly rozděleny na tři skupiny. První skupinou jsou hrozby vnější, které vycházejí z vnějšku organizace. Druhou skupinou jsou hrozby zevnitř organizace. V posledním případě jde o hrozby technické.

Jako vnější hrozby pro organizaci byly určeny:

- cílený kybernetický útok pomocí technik sociálního inženýrství,
- kybernetický útok za použití špionážních technik,
- napadení elektronické komunikace (odposlech, modifikace),
- infiltrace malware do počítačového systému organizace,
- odcizení identity a její zneužití,
- útoky typu DoS – odepření služby.

Jako vnitřní hrozby pro organizaci byly určeny:

- pochybení ze strany zaměstnance,
- sabotáž,
- zneužití oprávnění administrátorů,
- zneužití oprávnění uživatelů,
- nedostatek kvalifikovaných lidských zdrojů,
- snížení rozpočtu na kybernetickou bezpečnost.

Jako technické hrozby pro organizaci byly určeny:

- dlouhodobější přerušení dodávek elektrické energie,
- selhání techniky zajišťující fyzické zabezpečení objektu (alarmy, senzory, kamery),
- narušení fyzické bezpečnosti objektu,
- selhání technického vybavení,
- selhání softwarového vybavení.

Zranitelnosti:

- nedostatečný monitoring vnitřních hrozeb,
- nedostatečné ohodnocení zaměstnanců,
- nedostatečná proškolenost zaměstnanců,
- nedostatečná údržba ICT,
- nedostatečná vnitřní kontrola,
- zastaralost software,
- neopravený software,
- slabé autorizační pověření,
- nevhodné nastavení přístupových oprávnění,
- nedostatečná ochrana vnějšího perimetru,
- nevhodný postup při detekci negativních bezpečnostních jevů,
- nejasné stanovení bezpečnostních pravidel.

6.5 Parametry hodnocení

K provedení hodnocení rizik je potřeba stanovit parametry hodnocení. Hodnotící stupnice všech parametrů rizika jsou stanoveny v rozsahu 1 – 5 dle níže uvedených tabulek.

Tabulka 1 – Parametry hodnocení pravděpodobnosti (zdroj: Šefčík, 2015)

Pravděpodobnost vzniku a existence nebezpečí	
Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5

Tabulka 2 – Parametry hodnocení možných následků ohrožení (zdroj: Šefčík, 2015; upraveno)

Možné následky ohrožení pro kyberbezpečnost organizace	
Jednoduše řešitelné	1
Mírně závažné	2
Závažné	3
Vysoce závažné	4
Ochromující	5

Tabulka 3 – Parametry hodnocení názoru hodnotitele (zdroj: Šefčík, 2015; upraveno)

Názor hodnotitele	
Zanedbatelný vliv na bezpečnost	1
Malý vliv na bezpečnost	2
Jistý vliv na bezpečnost	3
Vysoký vliv na bezpečnost	4
Trvalá	5

Hodnocení přijatelnosti míry rizika probíhá na základě stanovení stupňů přijatelnosti rizika. S ohledem na skutečnost, že všechny tři zohledňované parametry, ze kterých je velikost rizika určena mohly mít nejvyšší hodnotu 5, je maximální hodnota rizika, která mohla být zjištěna je 125. Jednotlivé intervaly hodnoty rizika přiřazené k rizikovým stupňům byly určeny na základě subjektivního uvážení hodnotitele.

Tabulka 4 – Hodnotící parametry přijatelnosti výsledného rizika (zdroj: Šefčík, 2015)

Přijatelnost míry rizika		
Rizikový stupeň	R	Míra rizika
I.	>100	Nepřijatelné riziko
II.	51 - 100	Nežádoucí riziko
III.	11 - 50	Mírné riziko
IV.	3 - 10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

6.6 Hodnocení rizik metodou PNH

Hodnocení rizik metodou PNH je rozděleno na tři části, zvláště jsou hodnoceny vnitřní hrozby v oblasti kybernetické bezpečnosti pro organizaci, vnější hrozby v oblasti kybernetické bezpečnosti pro organizaci a technické hrozby v oblasti kybernetické bezpečnosti pro organizaci.

K hodnocení rizik je možné využívat řadu metod analýzy rizik, ale také technologie, které po zadání vstupních údajů dokáží vyhotovit přehlednou analýzu. Výběr metody je zásadní pro získání správných výstupů, které od této činnosti očekáváme.

6.6.1 Hodnocení vnějších hrozeb pro organizaci

V níže uvedené tabulce nalezneme hodnocení vnějších hrozeb pro organizaci.

Tabulka 5 – Hodnocení vnějších hrozeb (zdroj: vlastní)

Zdroj hrozby	Identifikace nebezpečí	Vyhodnocení vážnosti rizika			
		P	N	H	R
Vnější hrozby pro organizaci	Cílený kybernetický útok pomocí techniky sociálního inženýrství	5	5	4	100
	Kybernetický útok za použití špionážních technik	5	5	4	100
	Napadení elektronické komunikace (odposlech, modifikace)	5	5	4	100
	Infiltrace malware do počítačového systému organizace	5	5	4	100
	Odcizení identity a její zneužití	5	5	5	125
	Útok typu DoS – odepření služby	5	5	5	125

Součinem zadaných parametrů bylo zjištěno, že vnější hrozby pro organizaci mají celkové riziko na velmi vysokých úrovních. Celková hodnota rizika neklesla pod hodnotu 100. Za nejvýznamnější nebezpečí v této oblasti tak lze označit odcizení identity a její zneužití, nebo útoky typu DoS.

6.6.2 Hodnocení vnitřních hrozeb pro organizaci

V níže uvedené tabulce nalezneme hodnocení vnitřních hrozeb pro organizaci.

Tabulka 6 – Hodnocení vnitřních hrozeb (zdroj: vlastní)

Zdroj rizika	Identifikace nebezpečí	Vyhodnocení vážnosti rizika			
		P	N	H	R
Vnitřní hrozby pro organizaci	Pochybení ze strany zaměstnance	5	3	3	**45**
	Sabotáž	3	4	4	**48**
	Zneužití oprávnění administrátorů	3	5	5	**75**
	Zneužití oprávnění uživatelů	3	4	4	**48**
	Nedostatek kvalifikovaných lidských zdrojů	3	3	3	**27**
	Snížení rozpočtu na kybernetickou bezpečnost	3	5	5	**75**

Vnitřní hrozby jsou často velmi podceňované. V tomto případě byla maximální hodnota celkového rizika stanovena na hodnotu 75 ve dvou případech – zneužití oprávnění administrátorů a snížení rozpočtu na kybernetickou bezpečnost. Oba uvedené druhy nebezpečí lze označit jako nebezpečí mírnějšího charakteru.

6.6.3 Hodnocení technických hrozeb pro organizaci

V níže uvedené tabulce nalezneme hodnocení technických hrozeb pro organizaci.

Tabulka 7 – Hodnocení technických hrozeb (zdroj: vlastní)

Zdroj rizika	Identifikace nebezpečí	Vyhodnocení vážnosti rizika			
		P	N	H	R
Technické hrozby pro organizaci	Dlouhodobější přerušení dávek elektrické energie	3	5	4	**60**
	Selhání techniky zabezpečující fyzické zabezpečení objektu	3	4	3	**36**
	Narušení fyzické bezpečnosti objektu	4	3	4	**48**
	Selhání technického vybavení	3	4	4	**48**
	Selhání softwarového vybavení	3	4	3	**48**

U technických hrozeb pro organizaci se jako nejzávažnější projevilo dlouhodobé přerušení dodávek elektrické energie. S celkovou mírou rizika 60 bylo vyhodnoceno jako nežádoucí riziko. Ostatní identifikovaná nebezpečí jsou na mírné úrovni.

Následná tabulka zobrazuje celkový výsledek hodnocení rizik metodou PNH. Výsledky jsou řazeny dle velikosti celkového rizika sestupně. Tabulka obsahuje také sloupek se slovní zhodnocením míry rizika. Už na první pohled je evidentní, že některá vyhodnocená rizika budou vyžadovat pozornost a přijetí vhodných opatření.

Tabulka 8 – Celkové hodnocení rizik metodou PNH (zdroj: vlastní)

Identifikace nebezpečí	Celkové riziko	Přijatelnost míry rizika
Odcizení identity a její zneužití	125	nepřijatelné
Útok typu DoS – odepření služby	125	nepřijatelné
Cílený kybernetický útok pomocí techniky sociálního inženýrství	100	nežádoucí
Kybernetický útok za použití špionážních technik	100	nežádoucí
Napadení elektronické komunikace (odposlech, modifikace)	100	nežádoucí
Infiltrace malware do počítačového systému organizace	100	nežádoucí
Zneužití oprávnění administrátorů	75	nežádoucí
Snížení rozpočtu na kybernetickou bezpečnost	75	nežádoucí
Dlouhodobější přerušení dávek elektrické energie	60	nežádoucí
Narušení fyzické bezpečnosti objektu	48	mírné riziko
Selhání technického vybavení	48	mírné riziko
Selhání softwarového vybavení	48	mírné riziko
Sabotáž	48	mírné riziko
Zneužití oprávnění uživatelů	48	mírné riziko
Pochybení ze strany zaměstnance	45	mírné riziko
Selhání techniky zabezpečující fyzické zabezpečení objektu	36	mírné riziko
Nedostatek kvalifikovaných lidských zdrojů	27	mírné riziko

K hodnocení rizik bylo vybráno celkem 17 nebezpečí z oblasti vnitřních, vnějších a technických hrozeb pro zkoumanou organizaci. Žádné z rizik nebylo akceptovatelné, nebo zanedbatelné.

Za nebezpečí s mírným rizikem lze považovat osm z uvedených, kdy nejvyšší hodnoty celkového rizika v pěti případech atakovaly hranici intervalu, který byl stanoven pro nežádoucí riziko.

Sedm druhů nebezpečí bylo vyhodnoceno jako nežádoucí rizika. V kategorii dominovaly čtyři hrozby, šlo o hrozbu cíleného kybernetického útoku pomocí techniky sociálního inženýrství, dále kyberútoku za využití špionážních technik, napadení elektronické komunikace a infiltrace malware do počítačového systému organizace. Všechna jmenovaná nebezpečí pocházela z kategorie vnějších hrozeb pro organizaci.

Nejvyšší příčky tabulky a tedy hrozby, které byly vyhodnoceny jako nejzávažnější, pro zkoumanou organizaci obsadily nebezpečí odcizení identity a její zneužití a útok typu DoS – odepření služby. Míra rizika těchto hrozeb je pro organizaci na nepřijatelné úrovni a řešení těchto hrozeb vyžaduje okamžitá řešení.

Z celkového zhodnocení je patrné, že významných hrozeb v oblasti kybernetické bezpečnosti není málo a jejich váha je nezanedbatelná.

7 NÁVRH OPATŘENÍ KE ZLEPŠENÍ STÁVAJÍCÍHO STAVU

Na základě hodnocení rizik pro organizaci vykonávající státní správu bylo provedeno hodnocení rizik metodou PNH. Detekovány byly tyto hrozby pro organizaci:

Odcizení identity a její zneužití

Tento typ útoků se projevuje tak, že útočník se zmocní přístupových údajů oběti a následně je využívá k poškození oběti, odcizení citlivých dat z jeho účtů nebo zařízení, nebo k páchání trestné činnosti jménem oběti. Častým důvodem, proč dochází k odcizení identity je prolomení přístupových údajů oběti. Na vinně je často nevhodně zvolené heslo. Zcizená identita je nejčastěji zneužívána k dalšímu šíření spamu, získávání informací, realizování malware a phishingových útoků.

Dobrou obranou je používání silných hesel, která se nebudou opakovat. Tzn. při tvorbě hesla využívat písmena i číslice, malá i velká písmena, i speciální znaky. Zkoumaná organizace má nastaveno, že délka hesla musí být alespoň 8 znaků za využití malých a velkých písmen a číslovek. Pro zvýšení úrovně bezpečnosti lze doporučit přidání speciálního znaku a omezení, že během posledních 12 měsíců nesmí uživatel použít stejné heslo vícekrát.

O odcizení identity lze hovořit také v případě, že útočník získá zaměstnancovu kartu/čip, který je používán ke vstupu do budovy, využívání technologií a zařízení organizace, nebo podepisování dokumentů. V ideálním případě by mělo dojít k ověření identity před zahájením prvních aktiv v informačním a komunikačním centru, řízení počtu neúspěšných pokusů o přihlášení.

Vhodným řešením k ověřování identit je zavedení biometrického ověřování. Tato technika je sice vysoce spolehlivá, ale takové řešení je nad rozpočtové možnosti organizace.

Útok typu DoS – odepření služby

Tato forma útoku se projevuje tak, že útok je směřován na některou internetovou službu a cílem je vyřazení oběti z provozu. Typické je snížení výkonu uživatelova zařízení zahlcením systému.

Zásadní roli v případě útoků DoS nebo DDoS hraje monitoring sítí. Díky správnému monitoringu sítí a síťového provozu, může být pokus o útok velmi rychle odhalen a následně řešen.

K monitorování provozu na sítích se doporučuje využívat buď pasivní formu pomocí exportu NetFlow, IPIX apod., která je vhodná k identifikaci útoků. V případě aktivní reakce na probíhající útok je cílem získání podrobností o provozu z konkrétního směru a na konkrétní adresy. (GOV/CERT, 2024)

Cílený kybernetický útok pomocí techniky sociálního inženýrství

V případě této hrozby je nejslabším článkem člověk – uživatel. Útoky jsou zpravidla realizovány ve formě podvodných emailů, phishingu, smishingu, vishingu, falešných webových stránek, fiktivních telefonických hovorů, nebo využití údajů, které jsou veřejně dostupné. V menší míře může jít o útoky tváří v tvář.

Obrana proti tomuto typu útoků by měla být založena na dostatečném proškolení zaměstnanců. Podobná školení obvykle probíhají formou online kurzu. Vhodnějším řešením by však bylo alespoň jednou ročně zařadit prezenční školení s podrobnou prezentací, jak takové útoky mohou vypadat. Základní zásady o uzamykání počítače, bezpečného hesla a pravidelné aktualizaci systémů by měly být také oživovány. Zaměstnanci by neměly využívat svých osobních ani cizích paměťových zařízení a vkládat je do pracovních počítačů. Tyto základní zásady je vhodné upravit interní směrnicí, nebo vnitřním řádem organizace.

Kybernetický útok za použití špionážních technik a napadení elektronické komunikace (odposlech, modifikace), Sabotáž

Útočník v tomto případě cílí na informace, využívá odposlechy, štěnice a podobná zařízení k zajištění informací. V sofistikovaných případech útočník modifikuje informace. Sabotáž má obvykle za následek cílené způsobení škody na aktivech organizace, nebo výpadky či destrukci procesních systémů.

K obraně proti špionáži je využíváno techniky, jako jsou detektory odposlechů, rušičky diktafonů, obaly rušicí signál, generátory bílého šumu, nebo zařízení určená k šifrované komunikaci. (ITNetwork.cz, 2024)

Infiltrace malware do počítačového systému organizace

Účelem malware je poškození nebo infiltrace počítačového systému, typickými zástupci malware jsou různé viry, trojské koně, červi apod. Jeho funkce bývá buď destruktivní, kdy maže nebo znehodnocuje data, nebo přebírá kontrolu nad počítačovým systémem. Škodlivým kódem může být infikován kterýkoliv prvek počítačového systému.

S ohledem na ochranu aktiv je Vyhláškou o KB dána povinnost zajištění nástroje pro nepřetržitou automatickou ochranu koncových stanic, mobilních zařízení, serverů, datových uložišť a výměnných datových nosičů, komunikační sítě a prvků komunikační sítě a obdobných zařízení.

Předcházení infiltraci malwaru je tedy možné zajistit pravidelnou aktualizací operačního systému, webového prohlížeče, firewallu a antivirového programu.

V prostředí zkoumané organizace může být nebezpečím škodlivého kódu vystavena tiskárna umístěna na chodbě oddělení. Její využití je sice zabezpečeno použitím zaměstnaneckého čipu, ale škodlivý software může být během pár okamžiků přenesen prostřednictvím USB flashdisku útočníka do tohoto zařízení, neboť tiskárna není dobře fyzicky zabezpečena před vnějším útočníkem. (ČESKO, 2018)

Zneužití oprávnění uživatelů a administrátorů

Problém při zneužívání oprávnění ať v roli administrátorů, tak v roli uživatelů, může činit špatné nastavení přístupových oprávnění (špatně určené skupiny nebo role).

Snížení rozpočtu na kybernetickou bezpečnost

Výdaje na kybernetickou bezpečnost by měly být jednou ze základních položek v rozpočtu každé organizace. Údržba technického vybavení organizace, síťová údržba i odborný personál pečující o kybernetickou bezpečnost organizace je základním stavebním kamenem pro udržení zdravého fungování IKT v organizaci a udržení chráněných aktiv v bezpečné zóně.

Jak již bylo v této práci uvedeno dřív, NÚKIB zveřejnil výsledky dotazníkového šetření ve věci kybernetické bezpečnosti, ze kterého vyplývá, že přes pokles počtu samotných útoků naopak vzrostl počet respondentů negativně hodnotící stav kybernetické bezpečnosti v organizacích. Častým důvodem nespokojenosti s aktuálním stavem byl uváděn snížený rozpočet organizace na oblast kybernetické bezpečnosti. (Národní úřad pro kybernetickou a informační bezpečnost, 2023)

Pochybení ze strany zaměstnance

Jak již bylo zmíněno, lidský faktor je nejslabším článkem řetězce, a tedy největší zranitelností systému. Skrze lidskou chybu, nepozornost, neopatrnost je systém lehce napadnutelný. Jak již bylo zmíněno u útoků prostřednictvím technik sociálního inženýrství, poučení a zaškolení zaměstnanců často probíhá online formou, je to rychlé a levnější řešení, ale prezenční forma školení zaměstnanců může být mnohem efektivnější.

Opatření, která by zmírnila dané hrozby byla ve větší části navrhována ve formě obecné, a je předpoklad, že alespoň částečně organizací realizována jsou, neboť je jejich zabezpečení ustanoveno Vyhláškou o KB. Zkoumaná organizace autorovi práce neposkytla bližší informace o zabezpečení organizace (fyzickém ani síťovém) v takové hloubce, aby mohlo být posouzeno konkrétněji, která opatření by bylo nejvhodnější zařadit, nebo jak podpořit stávající systém opatření. Poskytnutí bližších údajů i přes anonymizaci organizace je organizací považováno za bezpečnostní hrozbu.

8 ZMĚNY PLYNOUCÍ ZE SMĚRNICE NIS2

Jak již bylo zmíněno v teoretické části této diplomové práce směrnice NIS2 bude implementována do českého právního řádu už v říjnu tohoto roku. Od očekávané novely Vyhlášky o KB a ZoKB se očekává zajištění vysoké úrovně kybernetické bezpečnosti v celé EU. Dopad NIS2 bude široký, dotkne se stovek organizací z různých odvětví. Původní směrnice NIS se týkala provozovatelů základních a digitálních služeb, nyní se rodina organizací spadajících pod NIS2 výrazně rozroste.

Přinášené změny mají vysoký význam, proto se NÚKIB rozhodl k návrhu zcela nové regulace kybernetické bezpečnosti, jejímž základem má být právě nový ZoKB. Nový ZoKB slučuje základ z původního ZoKB s požadavky určenými směrnicí NIS2.

Všechny změny, které nastanou mají jeden hlavní cíl a tím je předcházení, zajištění a zmírňování dopadů kybernetických bezpečnostních incidentů. Z tohoto důvodu budou mít organizace povinnost stanovit rozsah řízení KB v organizaci a následně zavádět adekvátní opatření.

Novou povinností bude také zpracování analýzy rizik, včetně evidence a hodnocení aktiv, identifikaci rizik, jejich hodnocení a návrhu na implementaci bezpečnostních opatření. (NÚKIB, 2022)

8.1 Dotčené subjekty

Subjekty, které budou dotčeny změnami, které přinese směrnice NIS2, a splňují podmínky pro zařazení do kategorie „velký podnik“ dle doporučení Komise (EU) 2003/361/EC jsou graficky znázorněny v příloze I. subjekty z těchto kategorií budou zařazeny v režimu Essential, tzn. základní subjekty.

V příloze II. Jsou vyjmenovány subjekty, které dle výše uvedeného doporučení splňují podmínku „velký podnik“ a „střední podnik“, ale bude na ně kladen nižší nárok z pohledu bezpečnostních opatření, tzn. budou zařazeny v režimu Important, tzn. důležité subjekty.

Mimo tyto dva režimy jsou postaveny subjekty, které shromažďují a udržují přesnou a úplnou registraci názvu domén. Takovým subjektům plynou povinnosti z NIS2, ale nejsou zařazeny v uvedených režimech. Grafický přehled dotčených subjektů je přiložen v Příloze č. 1 k této diplomové práci.

8.2 Povinnosti pro organizace

Poskytovatel regulované služby, tedy služby, která bude navrhovanou změnou dotčena, bude povinen plnit následující povinnosti:

- registrace na portálu NÚKIB za účelem hlášení bezpečnostních incidentů,
- stanovení rozsahu řízení KB,
- zavádění bezpečnostních opatření,
- informování zákazníka o incidentech a hrozbách,
- provádění protiopatření,
- zajišťování dostupnosti strategicky významných služeb z území ČR,
- plnit povinnosti mechanismu řízení dodavatelského řetězce a
- podřídit se výkonu kontroly.

8.3 Zavádění bezpečnostních opatření

Cílem regulace je zajistit, aby důležité organizace byly vedeny k posilování své kybernetické bezpečnosti a tím preventivně předcházely, zjišťovaly a tlumily dopady možných kybernetických incidentů.

Základním krokem před zaváděním opatření je stanovení rozsahu řízení KB v organizaci, tzn. vedení potřebné dokumentace týkající se identifikace a určení relevantních organizačních částí a aktiv. Následně je možné zvažovat bezpečnostní opatření. V samostatných vyhláškách jsou stanoveny dvě samostatné sady pravidel, které mají sloužit jako návod a usnadnění.

Bezpečnostní opatření určená pro režim vyšších povinností v podstatě kopírují dosavadní podobu Vyhlášky o KB a jejich obsah se promítne do Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

Připravovaná právní úprava pro poskytovatele regulovaných služeb v nižším režimu bude obsahem Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností. (NÚKIB, 2022)

8.4 Hlášení incidentů

Model hlášení kybernetických bezpečnostních incidentů byl zachován pro subjekty s vyšší povinností z doposud zažitého procesu hlášení podle ZoKB. Model hlášení pro subjekty s nižší povinností byl subjektům zjednodušen. Vždy ovšem platí, že se hlásí pouze takové kybernetické bezpečnostní incidenty, které pochází z kyberprostoru a nelze vyloučit úmyslné zavinění.

Návrh zákona opět navazuje na již existující povinnost registrace a hlášení a upravuje pouze údaje, jaké v konkrétních situacích hlásit a lhůty pro ohlášení. Komunikace s NÚKIB bude probíhat prostřednictvím jednotné platformy Portál Úřadu. Podrobnosti jsou řešeny v Návrhu vyhlášky o Portálu Úřadu. Kromě hlášení incidentů povinnými subjekty, bude ponechána možnost dobrovolného hlášení incidentů ze strany neregulovaných subjektů.

8.5 Kontrola plnění povinností, sankce a donucovací prostředky

Kontroly plnění povinností pro subjekty s vyšší povinností budou dále provádět zaměstnanci NÚKIB jako doposud. Pro kontrolu subjektů s nižší povinností bylo původně zamýšleno delegování povinnosti kontroly na tzv. inspektory, ale nakonec od něj bylo upuštěno. V případě zjištění přestupků je NÚKIB oprávněn uložit organizaci chráněné opatření.

8.6 Změny pro zkoumanou organizaci

Za zkoumanou organizaci státní správy v ORP Uherské Hradiště bylo jejím zástupcem sděleno, že bezpečnostní pracovníci organizace na ústřední úrovni dlouhodobě sledují vývoj v oblasti nového zákona o kybernetické bezpečnosti. Režim povinností pro zkoumanou organizaci z oblasti státní správy zůstává téměř neměnný. (NÚKIB, 2022)

ZÁVĚR

Hlavním cílem této diplomové práce bylo stanoveno hodnocení rizik v oblasti kybernetické bezpečnosti vybrané obce s rozšířenou působností. Teoretická část práce byla zaměřena na vypracování literární rešerše k problematice hodnocení kybernetických rizik. Z přehledu zkoumaných elektronických i literárních zdrojů je evidentní, že téma kybernetické bezpečnosti je hojně diskutováno jak v tuzemsku, tak ve světe. S čím dál rychlejší digitalizací společnosti nabývá řešení hrozeb spojených s kyberprostorem na významu.

Druhá kapitola práce se věnovala tématům kybernetických hrozeb, kybernetických incidentů a kybernetické bezpečnosti. Prostor byl vymezen i pro popis organizací, které se touto oblastí zabývají na domácí i evropské půdě. Kapitola třetí byla zaměřena na analýzu rizik a rozličný výčet použitelných metod.

V praktické části diplomové práce se pozornost autora zaměřila na obec s rozšířenou působností Uherské Hradiště. Po prostudování statistik kybernetických útoku došlo k zjištění, že tyto útoky jsou nejčastěji mířeny proti veřejnému sektoru a státní správě. Na základě těchto indicií byly identifikovány potenciální cíle kybernetických útoků v oblasti státní správy v obci s rozšířenou působností Uherské Hradiště a byla vybrána jedna z těchto institucí, která byla z pohledu kybernetické bezpečnosti blíže zkoumána.

K hodnocení rizik zkoumané organizace byla použita metoda PNH, která zohledňuje pravděpodobnost realizace hrozby, možné dopady a názor hodnotitele. Zdroje nebezpečí byly stanoveny ze tří oblastí, z oblasti vnitřní, z oblasti vnější a technologické. Identifikováno bylo 17 hrozeb, které byly následně hodnoceny. Výsledky hodnocení ukázaly, že nejvýznamnější rizika plynou organizaci z vnější oblasti organizace. Nejobávanějšími hrozbami pro organizaci je odcizení a zneužití identity a útoky typu DoS.

V předposlední kapitole byla navržena realizovatelná opatření, která by mohla eliminovat riziko vzniku obávaných událostí. S ohledem na nedostatečnou hloubku informací týkající se fyzického a síťového zabezpečení organizace nebylo možné tyto návrhy cílit konkrétněji.

Poslední kapitola diplomové je zaměřena na velmi aktuální téma implementace Směrnice NIS2 do českého právního řádu. Cílem kapitoly bylo na základě aktuálně dostupného návrhu zákona o kybernetické bezpečnosti, definovat změny, které přinese pro zkoumanou organizaci.

SEZNAM POUŽITÉ LITERATURY

ALEXANDROU, Alex, 2022. Cybercrime *and Internet technology: theory* and *practice--the computer network infostructure and computer security, cybersecurity laws, internet of things (IoT), and mobile devices*. First edition. Boca Raton, FL: CRC Press. ISBN 978-1-032-05385-1.

ANTONUCCI, Domenic, 2017. *The cyber risk handbook: creating and measuring effective cybersecurity capabilities.* Hoboken, New Jersey: Wiley. ISBN 978-1-119-30880-5.

ARQUILLA, John, 2021. *Bitskrieg: the new challenge of cyberwarfare. First published. Cambridge*: Polity, 212 s. ISBN 978-1-5095-4362-5.

BANDLER, John a Antonia MERZON, 2022. Cybercrime *ivestigations: a comprehensive resource for everyone. First* published. Boca Raton, FL: CRC Press. ISBN 978-1-032-39998-0.

Bezpečnostní strategie České republiky 2003, *2004. Praha: Ministerstvo zahraničních věcí* ČR. ISBN 80-86345-45-9.

BUCHANAN, Ben, 2020. The *hacker and the state: cyber attacks and the new normal of geopolitics.* Cambridge, Massachusetts: Harvard University Press. ISBN 978-0-674-98755-5.

CESKEDALNICE.CZ, 2023. Dálnice D55 [online]. *In: . 2023 [cit. 2024-04-20]*. Dostupné z: https://www.ceskedalnice.cz/dalnice/d55/

ČESKO, 1998. Ústavní zákon č. 110/1998 Sb.*, o bezpečnosti České republiky, ve znění pozdějších předpisů: Zákon o bezpečnosti.* In: . 39/1998.

ČESKO, 2018. 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.* In: . 43/2018.

ČESKÝ STATISTICKÝ ÚŘAD, 2018. *Správní obvody ORP ve Zlínském kraji [online]. In: . [cit.* 2024-04-20]. Dostupné z: https://www.czso.cz/csu/czso/so-orp-zlinsky-kraj-lo44jk0dfj

ČESKÝ STATISTICKÝ ÚŘAD, 2023. Správní obvod ORP Uherské Hradiště [online]. In: . [cit. 2024-04-20]. Dostupné z: https://www.czso.cz/csu/xz/so_orp_uherske_hradiste

ČSÚ ČR, 2023. Počet obyvatel v obcích - k 1. 1. 2023 [online]. In: . [cit. 2024-03-24]. Dostupné z: https://www.czso.cz/csu/czso/pocet-obyvatel-v-obcich-k-112023

ESET SOFTWARE SPOL. S *R.O.,* © 1992-2024. Slovník IT pojmů [online]. In: ESET SOFTWARE SPOL. S R.O. [cit. 2024-01-29]. Dostupné z: https://www.eset.com/cz/slovnik/

EUROPEAN UNION AGENCY FOR CYBERSECURITY, *2023.* ENISA THREAT LANDSCAPE 2023. European Union Agency for Cybersecurity (ENISA). ISBN 978-92-9204-645-3. DOI: 10.2824/782573.

EUROPEN UNION AGENCY FOR CYBERSECURITY, 2024. ENISA [online]. 2024 [cit. 2024-01-13]. Dostupné z*: https://www.enisa*.europa.eu/about-enisa/about/cs

EVROPSKÝ PARLAMENT A RADA EU, 2016. Směrnice Evropského parlamentu Rady EU 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informačních systémů v Unii – Směrnice NIS.

GOV/CERT, 2024. DoS / DDoS útoky. In: *NCKB* [online]. [cit. 2024-04-05]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2150-doporuceni-pro-pripad-napadeni-ddos-utokem-jak-se-zachovat-a-jak-postupovat/

HÁJEK, Tomáš, 2021. Kybernetická bezpečnost vybrané obce. Uherské Hradiště. Bakalářská práce. Univerzita Tomáše Bati *ve Zlíně.*

HÁJEK, Tomáš, 2023. *Aplikovaná kybernetická bezpečnost*. Uherské Hradiště. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

*ITNETWORK.CZ, 2024. Lekce 15 - Bezpečnost pracovního prostoru - Hrozby a útoky [online]. [*cit. 2024-04-25]. Dostupné z: https://www.itnetwork.cz/bezpecnost/bezpecnost-pracovniho-prostoru-hrozby-a-utoky

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2015. Výkladový *slovník kybernetické bezpečnosti. Vyd.* 3. Praha: Policejní adademie ČR v Praze a Česká pobočka AFCEA. ISBN 978-80-7251-436-6.

JIROVSKÝ, Václav, 2007. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada. ISBN 9788024715612.

KADEČKA, Stanislav a Filip RIGEL, 2009. Výkon státní správy - kompetence, odpovědnost. Brno. Teoretická studie.

KANYBEKOVA, Baktygul et al., 2023. Pakistan Journal of Criminology: Criminological *Aspects of the Behaviour of Victims of Cyberattacks: Case Analysis of Hacking State Organizations Ensuring National Security*. Pakistan Society of Criminology, 15(4). ISSN 20742738. 20742738.

KOLOUCH, Jan, 2016. CYBERCRIME. 1. vydání. Praha: CZ.NIC. ISBN *978-80-88168-18-8.*

KOLOUCH, Jan a Pavel BAŠTA, 2019. Cybersecurity. Vyd. 1. Praha: CZ.NIC, z. s. p. o. ISBN 978-80-88168-34-8.

KONRAD, Kai A**.,** 2024. The collective security dilemma of preemptive strikes. Hybrid Gold Open Access. 313(3). ISSN 03772217.

LUKÁŠ, Luděk, 2017. Teorie bezpečnosti I. 1. vydání. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-89-7.

MĚSTO UHERSKÉ HRADIŠTĚ, 2024. Základní informace o městě [online]. In: . [cit. 2024-03-24]. Dostupné z: https://www.mesto-uh.cz/zakladni-informace-o-meste

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, *2016. Terminologický slovník* pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu. In: Ministerstvo *vnitra České republiky* [online]. [cit. 2024_01_07]. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx

MV ČR, 2023. Co je GDPR. In: MV ČR. Ministerstvo vnitra České *republiky* [online]. [cit. 2024-01-02].

MZV ČR, 2003. Bezpečnostní *strategie České republiky* 2003. Praha.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2023. *Národní strategie kybernetické bezpečnosti České republiky 2021 - 2025*.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2023. Zpráva o činnosti 2022. Praha: NÚKIB.

NONNEMANN, František, Vlastimil ČERVENÝ a Dominik VÍTEK, 2022. *Kybernetický bezpečnostní incident 3D : IT, právo a compliance*. Právní monografie. Praha: Wolters Kluwer. ISBN 978-80-7676-515-3.

NÚKIB, 2022. Nová Směrnice NIS2 a návrh zákona o kybernetické bezpečnosti. In: NÚKIB. Vzdělávací portál NÚKIB [online]. [cit. *2024-03-25]. Dostupné z:* https://osveta.nukib.gov.cz/course/view.php?id=145

NÚKIB, 2023. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022*. Dostupné také z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

NÚKIB, 2024. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2024-01-09]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/

NÚKIB ČR, 2024**.** Legislativa KB. In: NÚKIB ČR. NÚKIB ČR [online]. 2024 [cit. 2024-12-26].

NÚKIB et al., 2022. *Průvodce řízením aktiv* a rizik dle vyhlášky o kybernetické bezpečnosti [online]. Praha [cit. 2024-04-20]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

PFENNINGER, E. G. et al., 2023. Resilience against IT attacks in hospitals: Results from an exercise in a German university hospital. Hybrid Gold Open Access. 72(12). ISSN 27316858.

POVODŇOVÉ PLÁNY, 2013. Digitální povodňový plán Uherské Hradiště. In: Povodňové *plány [online]. 2023 [cit. 2024-04-20]. Dostupné* z: https://uh.povodnoveplany.cz/

RAŠTICOVÁ, Blanka, 2018. *Památky města Uherské Hradiště* [informační brožura]. Město Uherské Hradiště, odbor kultury, školství a sportu.

RICHTER, Rostislav, 2018. Slovník pojmů krizového řízení. 1. Praha: Ministerstvo vnitra, generální ředitelství Hasičského záchranného sboru ČR. ISBN 978-80-87544-91-4.

ROMANOVSKÁ, Františka a Tomáš PITNER, 2022. MULTI-LEVEL CYBERSECURITY GOVERNANCE FRAMEWORKS FOR PUBLIC ADMINISTRATION. Digitalization of Society, Business and Managenet in pandemic: 30th Interdisciplinary Information Management Talks 2022: Masaryk University, Czech Republic. ISSN 10.35011/IDIMT-2022-277.

SEDLÁK, Petr a Martin KONEČNÝ, 2021. Kybernetická *(ne)bezpečnost: Problematika bezpečnosti v* kyberprostoru. Vyd.1. Brno: CERM. ISBN 978-80-7623-068-2.

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

ŠEFČÍK, Vladimír, 2015. Analýza rizik. Skripta. *Zlín: Univerzita Tomáše Bati ve Zlíně.* ISBN 978-80-7318-696-8.

ŠULC, Vladimír, 2018. Kybernetická bezpečnost. *Vyd. 1. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk*, s.r.o. ISBN 9788073807375.

VDT TECHNOLOGY A. S., 2021. Akt o kybernetické bezpečnosti. In: VDT technology [online]. [cit. 2024-01-02]. Dostupné z: https://www.vdttechnology.com/akt-o-kyberneticke-bezpecnosti/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BOZP	Bezpečnost a ochrana zdraví při práci
C&C	command-and-control server, velící server
CCA	Causes and Consequences Analysis
CD	Compact Disk, kompaktní disk
CERT	Computer Emergency Response Team
CO_2	oxid uhličitý
CSIRT	Computer Security Incident Response Team
ČR	Česká republika
ČSÚ	Český statistický úřad
DDoS	Distributed Denial of service, útok zahlcení cílové služby
DMZ	demilitarizovaná zóna
DNS	Domain Name Systém, DNS systém
DoS	Denial of service, útok odepření služby
DVD	Digital Video Disck, DVD nosič
ETA	Event Tree Analyses, metoda stromu poruch
ENISA	Agentura Evropské unie pro kybernetickou bezpečnost (European Union Agency for Cybersecurity)
EU	Evropská unie
FL-VV	Fuzzy Set and Verbal Verdict Method, metoda mlhavé logiky verbálních toků
GDPR	Zákon na ochranu osobních údajů (General Data Protection Regulation)
HAZOP	Hazard Operation Process
HRA	Human Reliability Analysis
ICQ	I Seek You, software pro komunikaci
ICT	Informační a komunikační technologie (Information and Communication Technology)
IS	Informační systém

ISMS	Information Security Management Systém, Systém řízení bezpečnosti informací
IT	Informační technologie
IT	Informační technologie (Information Technology)
KB	Kybernetická bezpečnost
LAN	Local Area network, lokální síť
MMS	Multimediální zprávy
MV	Ministerstvo vnitra
MZV	Ministerstvo zahraničních věcí
NATO	North Atlantic Treaty Organization, Severoatlantická aliance
NCKB	Národní centrum kybernetické bezpečnosti
NCKB	Národní centrum pro kybernetickou bezpečnost
NIS	Směrnice NIS (Network and Information Security)
NIS2	Směrnice NIS2 (Network and Information Security)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
NUTS	sdružené kraje, region soudržnosti
ORP	obec s rozšířenou působností
PHA	Preliminary Hazard Analyses
PSA	Probablistic Safety Assesment
QRA	Process Quantitative Risk Analysis
ROB	Registr obyvatel
ROS	Registr osob
RR	Relative Ranking
SMS	Short message service, služba krátkých textových zpráv
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol

ÚNMZ	Úřad pro normalizaci, měření a zkušebnictví
VLAN	Virtual Local Area Network, virtuální lokální síť
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network, Bezdrátová lokální síť
ZoKB	Zákon o kybernetické bezpečnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTČENÉ SUBJEKTY NIS2

TLP: CLEAR

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential".

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

VÝZKUM

Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT

Subjekty shromažďující a udržující přesnou a úplnou registraci názvu domén.

verze 1.0, platná ke dni 16.08.2022