POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

BAKALÁŘSKÁ PRÁCE

PRAHA 2023 **KATEŘINA BÍLKOVÁ**

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE
Fakulta bezpečnostního managementu
Katedra krizového řízení

Kybernetická bezpečnost prvku kritické infrastruktury

BAKALÁŘSKÁ PRÁCE

Cyber security of the Critical Infrastructure aspect
Bacherol thesis

VEDOUCÍ PRÁCE
Ing. Karel Malinovský

AUTOR PRÁCE
Kateřina Bílková

PRAHA
2023

ANOTACE

Bakalářská práce se zabývá kybernetickou bezpečnosti u prvku kritické infrastruktury. Tímto prvkem je míněno Letiště Praha, a.s. První část shrnuje problematiku kybernetické bezpečnosti, základní terminologii a rozdělení druhů kybernetické trestné činnosti. Druhá část je zaměřena na letiště jako prvek kritické infrastruktury a jeho kybernetickou a informační bezpečnost. Součástí bakalářské práce je také rozhovor s panem inženýrem Romanem Palkovičem a panem magistrem Stanislavem Petrákem.

KLÍČOVÁ SLOVA

Letiště Praha*, *kybernetická bezpečnost*, *malware*, *kritická infrastruktura*, *centrum informační bezpečnosti*, *NÚKIB*, *kybernetická trestná činnost*, *zákon o kybernetické a informační bezpečnosti

ANNOTATION

This thesis examines cyber and information security of the Critical Infrastructure aspect. This aspect is a Prague Airport City. First section summarizes the issue of Cyber security, key terminology, and classification of different types of Cyber threats. Second section is focused on airports as aspects of Critical infrastructure and their Cyber and information security. This part also includes an interview with Mr. Roman Palkovič and Mr. Stanislav Petrák.

KEYWORDS

Prague Airport City *, *cyber security *, *malware*, *critical infrastructure*, *information security center*, *NÚKIB*, *cybercrime*, *cyber and information security law

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 5.3. 2023

Kateřina BÍLKOVÁ

Obsah

Úvod

Tématem bakalářské práce je kybernetická bezpečnost prvku kritické infrastruktury.

První kapitola se zabývá úvodem do problematiky kybernetické bezpečnosti. Ve druhé kapitole je vysvětlena základní terminologie tématu a jednotlivé pojmy v abecedním pořadí podrobně upřesněny. Třetí kapitola se věnuje kybernetické trestné činnosti, kde jsou definovány pachatelé, jejich motivy a postupy usvědčení pachatele právními orgány. Tato kapitola také obsahuje typy kybernetických hrozeb. Čtvrtá kapitola se zabývá základním kamenem v oblasti kybernetické bezpečnosti, a to legislativou, na které je možné postavit bezpečnostní opatření proti kybernetickým hrozbám. Kapitola pojednává o legislativě České republiky a Evropské unie. Pátá kapitola je věnována Národnímu úřadu pro kybernetickou a informační bezpečnost, jeho historii, cílům, důvodům vzniku, a především jeho činnosti na poli kybernetické bezpečnosti. V šesté kapitole úzce navazuje Strategie zajišťování kybernetické bezpečnosti v ČR. V sedmé je vysvětlen způsob, jakým je zajištěna kybernetická bezpečnost ve vládních institucích. Součástí kapitoly je také graf Kybernetických útoků v letech 2019-2022. Podkapitola v tomto úseku bakalářské práce, více přibližuje problematiku kybernetické a informační bezpečnosti na letištích. Osmá kapitola přibližuje metody šetření a získávání dat v oblasti kybernetické bezpečnosti na Letišti Praha, a.s. Obsahem deváté kapitoly je rozhovor s panem inženýrem Romanem Palkovičem, ředitelem informační bezpečnosti, a panem magistrem Stanislavem Petrákem, manažerem dohledu Kybernetické bezpečnosti.

V závěru bakalářské práce budou shrnuty poznatky z oblasti kybernetické bezpečnosti, které jsem získala v průběhu zpracování této práce. Problematice kybernetické bezpečnosti se věnuji již několik let a ráda bych se jí věnovala i ve svém profesním zaměření.

1. Kybernetická bezpečnost

Tato kapitola je věnována pojmu kybernetická bezpečnost, která úzce souvisí s naším každodenním životem a pohybem v online prostoru. Ať už je to zaplacení účtu kartou, nebo mobilním telefonem v supermarketu či komunikace na sociálních sítích.

Kybernetická bezpečnost je definována v odborných publikacích odlišnými způsoby. Neexistuje jednotná definice.

Pojem se skládá ze dvou slov – „kybernetická“ a „bezpečnost“. Soustřeďme se nejprve přímo na definici bezpečnost. Dle Terminologického slovníku – krizové řízení a plánování obrany státu[1], dostupném na stránkách Ministerstva vnitra, lze pojem bezpečnost definovat jako „*Stav, kdy je možné odolávat známým a předvídatelným (i nenadálým) vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí.“* Druhá část pojmu „kybernetická“ je odvozeno z anglického slova **cyber**, které anglická internetová stránka Merriam-Webster[2], definuje jako cokoli, co má spojitost s počítači a počítačovými systémy. V posledním roce byl tento pojem nejčastěji užíván právě dohromady s pojmem **security**, v překladu **bezpečnost**.

1.1. Působnost a rozdělení kybernetické trestné činnosti

Rozdělení kybernetické trestné činnosti není zcela přesné. Každý kybernetický útok se odlišuje svým průběhem i cílem a postup řešení je vždy zcela unikátní. Každý pachatel, i když jedná podle návodu zkušenějšího, dodá do

[1] Terminologický slovník – krizové řízení a plánování obrany státu – Ministerstvo vnitra České republiky*. Úvodní strana – Ministerstvo vnitra České republiky* [online]. © 2022. [cit. 20.11.2022]. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx

[2] Cyber Definition & Meaning - Merriam-Webster. *Dictionary by Merriam-Webster: America's most-trusted online dictionary* [online]. © 2022. [cit. 20.11.2022]. Dostupné z: https://www.merriam-webster.com/dictionary/cyber

kybernetického trestného činu svůj vlastní styl a zanechá podpis odlišný od jeho „mentora“.

Kybernetická trestná činnost se odlišuje od běžné trestné činnosti, jako je například krádež či vražda, následujícím znaky: úmysl krádeže citlivých dat či informací (hesla od internetového bankovnictví, osobní údaje aj.) poškozeného za použití počítače či jiného elektronického zařízení a napadení elektronického zařízení jejich vybraného cíle.[3] Kybernetickou trestnou činnost řeší organizace CERT, která je zaměřena na Národní úřad pro kybernetickou a informační bezpečnost.

Kybernetická trestná činnost tedy musí mít útočníka a subjekt, na který se zaměřuje. Pachatele této trestné činnosti označujeme obecně jako hackery, i když ne každý z podvodníků působících v kyberprostoru jím je.

Obecně můžeme tedy působnost kybernetické trestné činnosti rozdělit na dvě oblasti – kybernetické útoky na státní sektor a na soukromý sektor.[4] Obě se totiž odlišují, a to především motivem. Celkově výnosy z kybernetické trestné činnosti již téměř převýšily výnosy z běžné trestné činnosti.

V případě útoků na státní sektor jsou tyto útoky vedeny na informační systémy státu a kritickou infrastrukturu. Pachatelé mohou být jak jednotlivci, tak organizované skupiny. Všichni jsou ale ve službách cizích státu nebo odebírají od těchto zemí provizi za nabourávání do klíčových prvků v informačních systémech státní správy cílového státu. Napadený stát se tedy dostává do takzvané kybernetické války. S pomocí těchto útoků je možné oslabit infrastrukturu, klíčové prvky bezpečnosti státu, ale také například destabilizovat hospodářství. Snahou

[3] What is Cybercrime? Cybercrime Prevention & Cybercrime Security. *Kaspersky Cyber Security Solutions for Home and Business* | *Kaspersky* | *Kaspersky* [online]. ©2020. [cit. 20.11.2022]. Dostupné z: https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

[4] ŠULC, Vladimír. *Kybernetická bezpečnost*. Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., Plzeň; 2018.

je tyto důležité systémy ovládnout či je zařadit do své sítě infikovaných systémů a zařízení.

Naopak u organizovaných skupin v soukromém sektoru je hlavním motivem zisk, především finanční. Spočívá ve snaze získat peníze, ať vyrabováním bankovního konta uživatele, nebo uživatelů, například klientů určité banky. Jednotlivci v tomto případě spíše chtějí získat respekt, prosadit svůj názor a získat uznání od jiných uživatelů. Samozřejmě peníze jsou také nedílnou součástí jejich činnosti.

Schopný pachatel může získat velký obnos peněz v kyberprostoru jednoduše, protože se stačí zaměřit na uživatele neznalé kybernetických hrozeb.

2. Základní terminologie

V této kapitole je stanovena základní terminologie kybernetické bezpečnosti. Její součástí jsou klíčové pojmy sepsané v abecedním pořadí. Při zpracovávání této kapitoly jsem při výběru definic čerpala především z dvou odborných publikací: *Kybernetická bezpečnost*[5], z dokumentů Ministerstva vnitra České republiky[6] a z odborných článků a cizojazyčné webové stránky TechTarget[7], jejichž definice jsem přeložila z anglického jazyka do českého. Jedním ze zdrojů je taktéž zákon č. 181/2014, o kybernetické bezpečnosti[8].

- **Bezpečnost informací** znamená uplatnění obecných bezpečnostních opatření a postupů sloužících:
  - 1. K ochraně informací před jejich ztrátou nebo kompromitací (ztráta důvěrnosti, integrity a dalších vlastností jako například autentičnost, odpovědnost, nepopíratelnost a spolehlivost), případně k jejich zjištění a přijetí nápravných opatření.
  - 2. K zachování dostupnosti informací a schopnosti s nimi pracovat v rozsahu přidělených oprávnění. Opatření zahrnují bezpečnost počítačů, přenosů, emisí a šifrovací bezpečnost a odhalování ohrožení skutečností a systémů a jeho předcházení.
- **Bezpečnostní incident** je porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo

[5] ŠULC, Vladimír. *Kybernetická bezpečnost*. Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., Plzeň; 2018.

[6] Základní definice, vztahující se k tématu kybernetické bezpečnosti. *Ministerstvo vnitra České republiky*, [online]. © 2009. [cit. 19.11.2022]. Dostupné z: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx

[7] Data Management/Data Warehousing information, news and tips - *SearchDataManagement. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget* [online]. © [cit. 20.11.2022] Dostupné z: https://www.techtarget.com/searchdatamanagement/

[8] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: Sbírka zákonů, 29.8. 2014. ISSN

standardních bezpečnostních pravidel provozu Informační a komunikační technologie.

- **Bezpečnostní opatření** definujeme jako souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech, dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.
- **Data** ve sféře informačních technologií jsou informace, které byly přeloženy do formy, která umožňuje přenos nebo zprocesování.
- **Hacker** je obecný název pro pachatele kybernetické trestné činnosti.
- **Hardware** je obecný pojem, který se vztahuje na veškeré fyzické části počítače (například počítačová myš, reproduktor, klávesnice)
- **Hrozba** je potencionální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.
- **Informační systém:**
  - 1. Funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky.
  - 2. Komplex prvků nacházejících se ve vzájemné interakci.
- **Internet** je globální systém propojených počítačových sítí, které používají standartní internetový protokol (TCP/IP).
- **Kritická informační infrastruktura** znamená zákonem jasně vymezený komplex informačních systémů, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.
- **Kybernetická trestná činnost** je jakákoli trestná činnost, která zahrnuje počítač, připojené zařízení nebo počítačovou síť.
- **Kybernetický prostor** definuje digitální prostředí, umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací.

- **Kybernetický útok** znamená útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.
- **Malware** (ze dvou slov *malicious* [podlý] a *software*) jedná se o obecný název pro škodlivé programy. Mezi škodlivý software se řadí počítačové viry, trojské koně, červy, špionážní software.
- **Počítačová síť** je soubor počítačů spolu s komunikační infrastrukturou (komunikační linky, technické vybavení, programové vybavení a konfigurační údaje), jejímž prostřednictvím si (počítače) mohou vzájemně posílat a sdílet data.
- **Ransomware** je název pro škodlivý program, který zašifruje data a nabízí jejich rozšifrování po zaplacení výkupného (například virus, trojský kůň)
- **Software** (programové vybavení) je sada programů používaných v počítači, které vykonávají zpracování dat, či konkrétních úloh.
- **Správce systému** je osoba zodpovědná za řízení a údržbu počítačového systému.
- **Uživatelem** definuje každou fyzickou nebo právnickou osobu, která využívá službu informační společnosti, zejména za účelem vyhledání či zpřístupnění informací.
- **Virus** je typem malwaru, který se šíří z počítače na počítač tím, že se připojí k jiným aplikacím. Následně může působit nežádoucí a nebezpečnou činnost. Má v sobě obvykle zabudován mechanismus dalšího šíření či mutací.

3. Kybernetická trestná činnost

V České republice se s kybernetickými hrozbami uživatelé elektronických zařízení setkávají nejčastěji na internetu. Dopadení pachatele kybernetické trestné činnosti není jednoduché, oproti trestné činnosti, která probíhá v „reálném světě“ a je možné pachatele chytit přímo fyzicky. Dobří hackeři dokáží velmi dobře zamaskovat svoji polohu, například s pomocí šifrování či VPN. VPN je funkce, která zamaskuje útočníkovu IP adresu, a i když pachatel působí z území České republiky, veřejnosti se pak jeví, že vysílá například ze Spojených států amerických. Musíme si ale také uvědomit, že ohrožení a ztráta dat není pouze s pomocí hackování a počítače. K citlivým datům a informacím se může dostat i někdo, kdo fyzicky ukradne počítačový hardware, na kterém jsou daná data. V kyberprostoru také hackeři nepoužívají svá skutečná jména, aby omezili možnosti svého dopadení. Používání přezdívek je něco zcela normálního v kyberprostoru a dělá to každý, kdo se trochu vyzná v hlubinách internetu. Jejich vynalézavost při vyvíjení nových hrozeb a nových kombinací malwarů způsobuje, že jsou vždy o krok napřed. Proto se spíše než dopadení pachatele, snaží vyšetřovatelé nejprve zastavit jejich působení a dopad jejich činů. Tímto způsobem mohou najít i stopy v kyberprostoru. Každý hacker má stejně jako zloděj či vrah svůj modus operandi, který se opakuje.

U kyberkriminality se zjišťuje, zda se jedná o jeden či více trestných činů, které se opakují[9]. Aby bylo možné pachatele usvědčit, je nutné získat nejprve informace o samotném útoku. Jaká byla jeho struktura, délka a následné vyčíslení škody. Pokud možné zjistit informace o pachateli – jakou přezdívkou se představil při použití ransomwaru a následnému vydírání, zda dělal pravopisné chyby či používal některá neobvyklá slova. Ale nejsou to pouze škodlivé softwary, které představují riziko při pohybu na internetové síti. Riziko velmi často představuje

[9] KOLOUCH, Jan. BAŠTA, Pavel. a kol. *CyberSecurity.* 1. vydání. CZ.NIC, z. s. p. o., Praha 2019.

také nedostatečná opatrnost při sdílení osobních dat a informací na sociálních sítích či oslabená hesla na soukromých účtech.

Vše, co se sdílí na Facebooku, Instagramu či Twitteru, nelze vrátit zpět. Proto je potřeba si uvědomit, že cokoli dáme online, dáváme k dispozici všem uživatelům internetu. Konkrétní případ škodlivých informací byl součástí aféry s režisérem filmu od společnosti Disney, Jamesem Gunnem, v roce 2018. Jeho téměř deset let staré příspěvky na Twitteru s nevhodným obsahem způsobily vyhození režiséra ze studia a přerušení natáčení jeho filmů. Internetové sítě mohou také podněcovat paniku. Například při současné situaci se po internetu objevuje mnoho tzv. Fake News. Tyto falešné poplašné zprávy obsahují sice nepravé informace, ale mohou ovlivnit veřejné mínění. Proto se doporučuje na vyhledávání informací používat oficiální webové stránky ověřených zpravodajských služeb.

3.1. Pachatelé kybernetické trestné činnosti

Osobu, která páchá častější a velmi vážnou kybernetickou trestnou činnost s cílem krádeže dat či citlivých informací, nazýváme „hacker“. Tento pojem pochází z anglického jazyka a při jeho používání jej nepřekládáme.

Definice pojmu dle cizojazyčné internetové stránky TechTarget, zabývající se pojmy kybernetické bezpečnosti[10], cituji: *„Hacker je osoba, která používá počítač, networking či jiné schopnosti k získání nepovoleného přístupu do systému nebo internetových stránek s cílem páchat trestnou činnost.“* Hacker může například ukrást soukromé informace, které následně využije k vydírání své oběti, či je hacker schopen zcela vyřadit z provozu internetovou stránku za pomocí některého z počítačových virů. Ve velkém procentu případ, poté, co hacker získá

[10] What is a hacker*?. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget* [online]. Copyright © [cit. 20.11.2022] Dostupné z: https://www.techtarget.com/searchsecurity/definition/hacker

data, tak je zašifruje a požaduje finance za jejich opětovné odblokování a poskytnutí.

V 1960 byl pojem „hacker“ použit poprvé. V té době neznamenal negativní působení. Zpočátku bylo toto slovo spíše používáno jako jakýsi obdivný název pro osobu, která byla schopná rychle a kreativně přijít na způsob vyřešení technického problému. V dnešní době je tento pojem bohužel hojně využíván pro osoby, které používají své schopnosti a možnosti k ilegální činnosti.

V komunitách zabývajících se kybernetikou byly dříve definovány dva základní typy hackerů – black hat hackers (černí) a white hat hackers (bílí). Jak se postupně informační technologie rozvíjely a více osob se snažilo stát se hackery, vznikaly nové skupiny a jejich názvy. Každou z těchto skupin definují jejich základní cíle. Toto rozdělení není definitivní, slouží pouze jako orientační. Ne každého hackera je možné zařadit do konkrétní skupiny.

- **Black hat hackers** neboli **neetičtí hackeři** se vědomě snaží získat neautorizovaný přístup k internetovým stránkám, aplikacím a elektronickým zařízením a jejich následnému poškození či se zaměřují na specifické subjekty, aby páchali ilegální trestní činnost. Tyto útoky zahrnují vydírání s pomocí malwaru ransomware, krádež citlivých dat a informací, poškození či totální zničení elektronických zařízení a internetových stránek. Jsou to pachatelé trestné činnosti z důvodu jejich neetického jednání, které je proti zákonu. Dále mohou působit v ilegálních aktivitách, jako je špionáž, krádeže identit a DDoS útoky.
- **White hat hackers** neboli **etičtí či autorizování hackeři** se snaží používat své schopnosti ve prospěch společnosti, cílené ji nepoškozují. Mnoho z nich se podílí na tzv. pen testing (test proniknutí do systému), kdy si je najaly firmy, aby ostestovaly bezpečnost svých vnitřních systémů. Hackeři se o to následně pokusí a následně podají hlášení spolu s doporučením, co je možné zlepšit a jakým způsobem může nepovolaná osoba proniknout k jejich soukromým datům. Bezpečnostní

firmy, pro které tito hackeři pracují, následně mohou opatření zabudovat do systémů dříve, než se přes tyto slabiny někdo může dostat dovnitř.

- **Gray hat hackers** se řadí na pomezí mezi bílé a černé skupiny. Jejich motivy mohou být podobné jako u výše zmíněných, ale primárně nejsou zaměřené na ilegální či prospěšnou činnost. Pokud se pokusí a proniknou do systému, je to ilegální cestou, ale nepokouší se o hrubé narušení. Nejsou motivováni jenom penězi – mohou například nabídnout opravu chyb, které v systému našli.
- **Red hat hackers** neboli **ostrozrací hackeři** jsou podobní etickým hackerům, ale jejich pravý cíl hackingu leží v jiné rovině. Cíleně vyhledávají neetické hackery a snaží se jejich útoky zastavit většinou ilegální cestou. Příkladem může být nainstalování škodlivého programu do elektronického zařízení jednoho z jejich „nepřátel“.
- **Blue hat hackers** neboli **pomstychtiví hackeři** využívají své schopnosti jako zbraň proti konkrétní osobě, organizaci či bývalému zaměstnavateli. Používají ilegálně získaná data od svých obětí, aby jim následně zničili jejich život. Například zveřejní citlivá data své cílené oběti online. Pro firmu může být toto kritické, pokud budou zveřejněna data, která mohou způsobit ztrátu důvěryhodnosti klientů.
- **Script kiddies** jsou amatéři, kteří nemají příliš zkušeností ani schopností háčkovat, ale testují, co dokáží. Ve většině případů nezpůsobí příliš škod.
- **Hacktivists** nejsou samostatní hackeři, ale skupiny, které s pomocí kybernetických útoků dosahují politických změn. Jejich způsob se zaměřuje na širokou veřejnost a cílem je přivést pozornost na určité problémy, které jsou dle hacktivistů porušením etických zásad nebo základních lidských práv.

3.2. Typy kybernetických hrozeb[11]

Pachatelé kybernetické trestné činnosti, jak bylo zmíněno výše, mají mnoho způsobů, jak mohou získat data a informace od kohokoli z nás. Kybernetické hrozby je možné rozdělit do několika skupin.

Držet krok s novými technologiemi, trendy bezpečnosti a obecně proces ohrožující data je náročné. Obzvláště v tomto odvětví kybernetiky, kdy se vše velmi rychle vyvíjí. Stejně tak i nové kybernetické hrozby. Některé z osvědčených postupů při páchání ilegální činnosti však zůstávají stejné již řadu let z důvodu vysoké úspěšnosti.

Tyto již osvědčené hrozby patří mezi problémy, se kterými může přijít do styku každý uživatel internetu podceňující nebezpečí, jež číhá v kyberprostoru. Právě tito uživatelé jsou nejvíce ohrožení a stanou se obětmi, protože nevěří, že by online prostředí mohlo být pro ně reálnou hrozbou. Co není fyzické, není reálné. Tato rozšířená myšlenka je často příležitostí pro pachatele. Přitom nikdo z těchto uživatelů by jistě dobrovolně v reálném světě nikomu neposkytl své jméno, adresu či klíče od bytu.

Přitom kybernetické útoky a viry jsou reálné. Například phishing, který je rozšířený po celém světě, patří k velmi rychlým způsobům, jak chytrý a nepříliš schopný hacker může přijít lehko k penězům s minimem úsilí.

Vytvořit si falešnou e-mailovou adresu, webovou stránku a odeslat podvodný e-mail se nezdá příliš náročné, ale každý z těchto útoků je do detailů naplánovaný. Pokud je úspěšný, může hacker dělat se získanými údaji cokoli. A okradený uživatel si uvědomí, že se stal obětí, až když je jeho účet zablokován nebo mu zmizí peníze z banky, protože se hacker dostal k jeho přihlašovacím údajům do internetového bankovnictví.

[11] What is Cybersecurity? Everything You Need to Know | TechTarget. *Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget* [online]. © [cit. 20.11.2022] Dostupné z: https://www.techtarget.com/searchsecurity/definition/cybersecurity

Typy kybernetických hrozeb jsou seřazeny abecedně, některé jsou přeloženy do českého jazyka. V oblasti informačních technologií se používá přednostně anglický jazyk, který pomáhá v mezinárodní spolupráci mezi subjekty kybernetické bezpečnosti.

- **APTs – Advanced persistent threats (dlouhé, stálé útoky)** jsou útoky, kdy hacker se pohybuje nezpozorován ve stejné síti s cílem krást opakovaně data.
- **DDoS – Distributed-denial-of-service (odstřihnutí od sítě)** je typ útoku, kdy mnoho různých systémů naruší běh serveru nebo internetové stránky. Hacker zablokuje cíl s pomocí velkého počtu zpráv, žádostí či objednávek. Tento postup může ohrožovaný systém zpomalit nebo přinutit ke spadnutí.
- **Insider threaths (hrozba od někoho zevnitř)** je narušení bezpečnosti či způsobení ztrát společnosti osobou uvnitř. Ať už je to klient, zaměstnanec nebo spolupracující společnost. Osoba mohla způsobit chybu nechtěně, nebo měla jasný motiv společnost poškodit.
- **Malware** je typ škodlivého softwaru, kdy může být použit jakýkoli soubor, aplikace nebo program k poškození uživatele počítače, např. červy, virusy, trojské koně a spyware.
- **MitM – Man-in-the-middle (osoba uprostřed) .** U této hrozby se jedná o „odposlouchávající“ útoky. Pachatel zprovozní konverzaci či vyměňování informací mezi dvěma subjekty, které věří, že komunikují spolu bezpečně.
- **Phishing** je forma sociálního inženýrství, kdy zaslaný e-mail nebo textová zpráva připomíná oficiální společnost, působí věrohodně a vypadá podobně jako zaslané bankovní společností. Velmi často se jedná o náhodné útoky, kdy cílem pachatele je ukrást citlivá data jako jsou přihlašovací údaje do bankovnictví či číslo kreditní karty.
- **Ransomware (vyděračský software)** je jeden z typů malwaru. Útočník se dostane do souborů v elektronickém zařízení své oběti a tato data

zašifruje. Nejčastěji toho dosáhne pomocí e-mailu obsahujícího falešný infikovaný soubor. Za odšifrování dat následně žádá výkupné.

- **Sociální inženýrství** je útok závisející na lidských interakcích s pachatelem, kterými může získat citlivá data uživatele a následně je zneužít k vlastnímu užitku.
- **Spear phishing** je typ phishingu, který má konkrétně stanoveného uživatele, a proto to jsou podvodné e-maily a textové zprávy od organizací či společností, které pachatelova oběť zná.
- **Spyware** se řadí do skupiny malwarů. Cílem je nepozorovaně špehovat uživatele napadeného elektronického zařízení a následně veškeré získané informace poskytnout bez souhlasu a vědomí napadeného třetí straně, která na tom může mít také podíl.
- **Trojský kůň** je typ malwaru, který je uživatelem nainstalován do jejich zařízení jako neškodný dodatek nějakého softwaru či samostatný program. Sám tento vir neškodí, ale přenáší škodlivý software jako je například ransomware.

4. Legislativa v oblasti kybernetické bezpečnosti

V této kapitole se zaměřím na veškerou legislativu, která je v oblasti kybernetické bezpečnosti stěžejní. Každý z těchto zákonů na sebe navzájem působí a jsou postupně novelizovány v závislosti na nových kybernetických útocích. Dále jsou zde uvedeny i vyhlášky a nařízení vlády, které souvisí s kybernetickou bezpečností na poli zabezpečení státní infrastruktury a systémů.

4.1. Legislativa České republiky[12]

1. **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.**
    - Zákon č. 181/2014 Sb. vešel v platnost 29. srpna 2014 s účinností od 1. ledna 2015. Tento zákon pojednává o kybernetické bezpečnosti a upravuje práva a povinnosti osob jakož i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Hlavním cílem tohoto zákona je stanovit základní úroveň bezpečnostních opatření, zlepšit odhalování, opatření a hlášení bezpečnostních incidentů. Zároveň upravuje i činnost dohledových pracovišť. V roce 2017 proběhlo několik novelizací. Dvě nejvýznamnější jsou prostřednictvím zákona č. 104/2017 Sb. s účinností od 1. července 2017 a zákon č. 205/2017 Sb. s účinností od 1. srpna 2017. Do dnešního data proběhly další novelizace – zákonem č. 183/2017 Sb., zákonem č. 35/2018 Sb., zákonem č. 111/2019 Sb., zákonem č. 12/2020 Sb., zákonem č. 261/2021 a zákonem č. 226/2022. Poslední uvedená novelizace zákona je účinná od 6. srpna 2022.
2. **Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti**

[12] Národní úřad pro kybernetickou a informační bezpečnost – Legislativa. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. © [cit. 28.11.2022] Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

3. **Vyhláška č. 82/2018, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.**
    - Obě vyhlášky zpracovávají směrnici NIS. Každá z nich upravuje obsah a strukturu bezpečnostní dokumentace, obsah a rozsah bezpečnostních opatřeních, typy, 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 a jejich kopií.
4. **Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.**

Vstoupila v platnost dne 19. prosince 2014. Vyhláška stanovila kritéria pro určení významných informačních systémů. V roce 2020 byla novelizována. Tato novela vyhlášky č. 317/2014 Sb., má za cíl zpřesnit kritéria pro určení významnosti daného systému. Nabytí účinnosti bylo rozloženo do tří období. Kompletní znění nabude účinnosti 1. ledna 2023.

5. **Nařízení vlády č. 432/2010 Sb., o kritériích určení prvku kritické infrastruktury.**

Toto nařízení vešlo v platnost 30. prosince 2010. Definuje průřezová a odvětvová kritéria pro určení prvku kritické infrastruktury. V příloze tohoto nařízení je definováno 9 odvětví (energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a infomační systémy, finanční trh a měna, nouzové služby, veřejná správa) a kritéria pro určení prvku kritické infrastruktury. Pro potřeby mé bakalářské práce se zaměřím na **V. odvětví DOPRAVA,** konkrétně písmeno C, letecká doprava.

6. **Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.**
7. **Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.**
8. **Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.**
9. **Směrnice Evropského parlamentu a Rady EU 2016/1148 o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS).**
    - Tato směrnice vešla v platnost z důvodů zásadní role informačních systémů a informací ve společnosti. Jak je zmíněno v dané směrnici v úvodu: (3) *Sítě a informační systémy, především internet, plní zásadní roli při usnadňování přeshraničního pohybu zboží, služeb a osob. Vzhledem k tomuto nadnárodnímu rozměru se může významné narušení uvedených systémů, ať již úmyslné či neúmyslné, dotknout jednotlivých členských států i Unie jako celku, a to bez ohledu na místo, kde k takovému narušení došlo. Bezpečnost sítí a informačních systémů je proto základním předpokladem pro hladké fungování vnitřního trhu.*[13]
10. **Nařízení Evropského parlamentu a Rady EU 2019/881 ze dne 17. dubna 2018 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologiích.**[14]

[13] Směrnice Evropského parlamentu a Rady EU 2016/1148 o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informačních systémů v Unii. In: ,2016. ISSN

[14] Nařízení Evropského parlamentu a Rady EU 2019/881 ze dne 17. dubna 2018 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologiích.

5. Národní úřad pro kybernetickou a informační bezpečnost[15]

Národní úřad pro kybernetickou a informační bezpečnost je správním úřadem pro kybernetickou bezpečnost, kryptografickou ochranu, ochranu utajovaných informací pro oblast informačních a komunikačních systémů a problematiku veřejné regulované služby systému Galileo (viz. 5.1.). Úřad vznikl na základě zákona č. 205/2017 Sb. Tento zákon změnil původní zákon č. 181/2014 Sb., o kybernetické bezpečnosti. NÚKIB započal svoji činnost 1. srpna 2017. Ředitelem Národního úřadu pro kybernetickou bezpečnost je v současnosti Ing. Lukáš Kintr. Součástí tohoto úřadu je také NCKB neboli Národní centrum kybernetické bezpečnosti. Tato výkonná sekce zajišťuje mimo jiné vládní CERT. Ředitel NÚKIB má také Rozkladovou komisi v čele s předsedou Mgr. Pavlem Králem. Pod poslední odbor patří také pozice: Bezpečnostní ředitel, Manažer kybernetické bezpečnosti, Architekt kybernetické bezpečnosti, Auditor kybernetické bezpečnosti, Interní Auditor a Pověřenec pro ochranu osobních údajů.

5.1. Činnost NÚKIB[16]

Činnosti úřadu spadají pod tři základní sekce – Sekce provozně právní, Sekce národního centra kybernetické bezpečnosti a Sekce informační bezpečnosti. Každá z těchto sekcí má své vlastní odbory a jednotlivá oddělení. Všechny sekce navzájem spolupracují a doplňují se.

[15] Národní úřad pro kybernetickou a informační bezpečnost - O úřadu. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. © [cit. 11.1.2023] Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu/

[16] Národní úřad pro kybernetickou a informační bezpečnost - Organizační struktura úřadu. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. © [cit. 11.1.2023]. Dostupné z: https://www.nukib.cz/cs/o-nukib/organizacni-struktura-uradu/

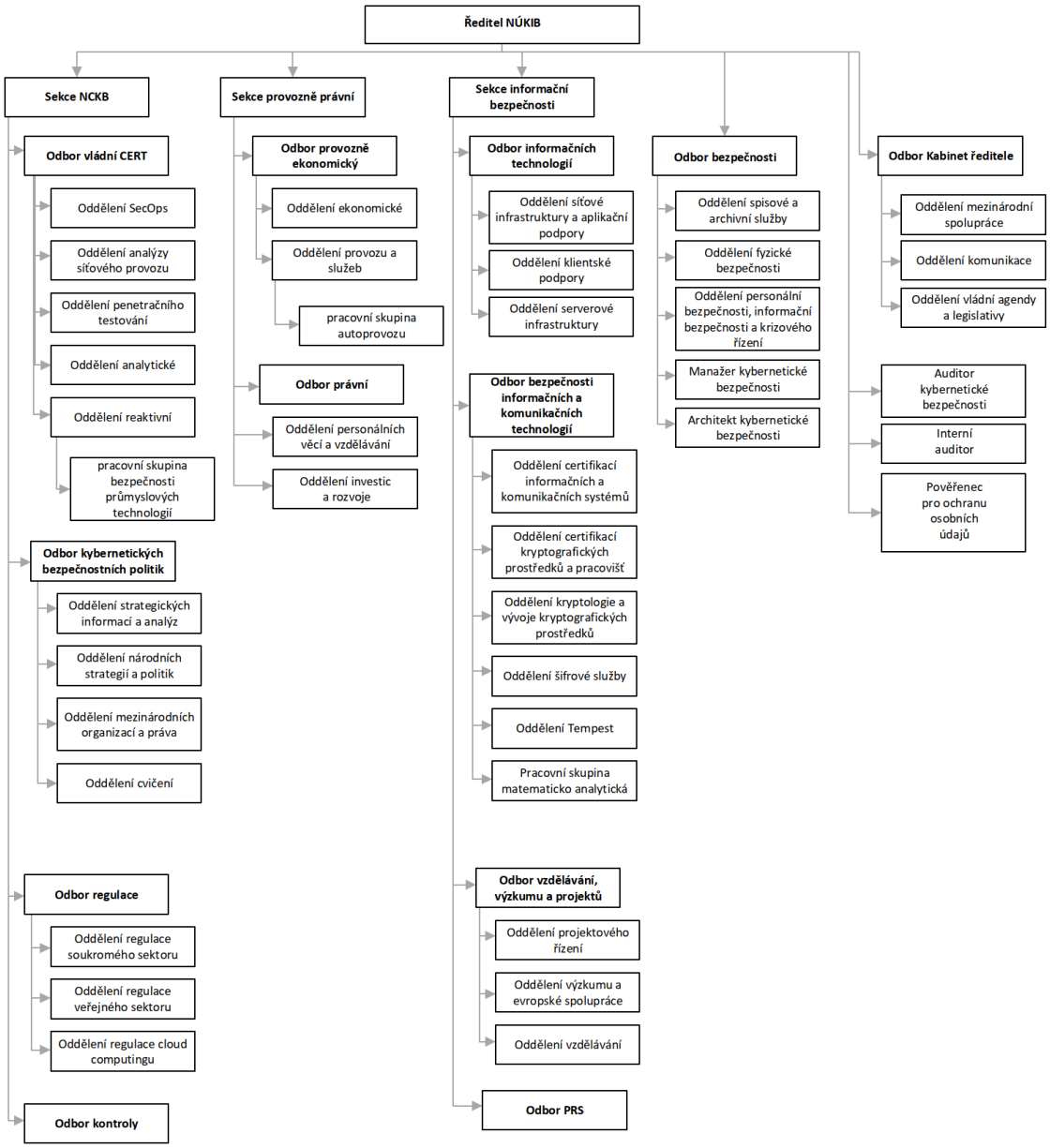
5.1.1. EGNSS Gallileo[17]

Evropský globální navigační družicový systém určuje mimo jiné přesnou polohu a čas kdekoli na zemi. Jeho vývoj řídí Evropská komise, vyvíjí ho Evropská kosmická agentura a jeho provoz zajišťuje Agentura pro EGNSS sídlící v Praze. Program financuje Evropská unie. Výhodou tohoto systému je, že ho může používat neomezený počet uživatelů. Implementaci systému Gallileo v České republice má na starosti Národní centrum PRS, zkráceně NCPRS, a je pověřeno příslušným orgánem PRS. Jeho oblast působnosti je velmi rozsáhlá, řadí se sem veškerá činnost spojená se systémem Gallileo. NCPRS tedy kromě implementace služby v ČR také spravuje provoz PRS, vypracování a aktualizace provozních předpisů, reprezentace v pracovních skupinách programu Gallileo v Evropské unii, řešící problematiku PRS a bezpečnosti EGNSS, a v neposlední řadě i přípravu a realizaci auditů[18].

[17] Národní úřad pro kybernetickou a informační bezpečnost – Program Galileo. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. © [cit. 11.1.2023]. Dostupné Dostupné z: https://nukib.cz/cs/galileo-prs/program-galileo/

[18] Národní úřad pro kybernetickou a informační bezpečnost – Galileo PRS. *Národní úřad pro kybernetickou a informační bezpečnost – Úvodní stránka* [online]. © [cit. 11.1.2023]. Dostupné Dostupné z: https://www.nukib.cz/cs/galileo-prs/

5.1.2. Schéma sekcí, odborů a oddělení Národního úřadu pro kybernetickou a informační bezpečnost.



Obr.1. Schéma NÚKIB[19]

[19] Národní úřad pro kybernetickou a informační bezpečnost – Organizační struktura úřadu. *Národní úřad pro kybernetickou a informační bezpečnost – Úvodní stránka* [online]. © [cit. 11.1.2023]. Dostupné Dostupné z: https://nukib.cz/cs/o-nukib/organizacni-struktura-uradu/

5.1.3. Sekce personalistiky, práva a provozu[20]

- **Odbor právní.** Poskytuje komplexní právní služby pro provoz činnosti instituce a zajišťuje plnění rozličných povinností vyplývajících z postavení úřadu jako ústředního správního orgánu. Právní odbor je rovněž odpovědný za výběrová a zadávací řízení veřejných zakázek, které mimo jiné zahrnují přípravu a evidence smluvní dokumentace. V neposlední řadě tento odbor je odpovědný za porušení pravomocí udělených v rozsahu povinnosti NÚKIB. Pokrývá také další správní řízení vedená úřadem. Pod právním odborem jsou dvě oddělení – oddělení právní a oddělení veřejných zakázek.
- **Odbor provozně ekonomický.** Pod tento odbor řadíme čtyři oddělení.
  - **Oddělení ekonomické.** Zajišťuje složité účetní agendy a zúčtovává účetní agendy v platebním a zúčtovacím styku úřadu s peněžními ústavy. Dále zajišťuje metodiku a postupy zúčtování. Kromě toho i zodpovídá za přípravu celé agendy, připravuje návrhy rozpočtů ve všech oblastech činnosti úřadu a provádí ekonomické rozbory. Na konci zúčtovacího období provádí vyúčtování výdajů FKSP. V neposlední řadě účtuje prostředky v cizích měnách pro zaměstnance na zahraniční cesty.
  - **Oddělení investic.** Plánuje a řídí tvorbu investičních projektů a zajišťuje jejich realizaci. Podává návrhy na stavební činnost a opravy investičního charakteru. Vše navrhuje do rozpočtu příslušného roku. Zpracovává a zajišťuje projektovou dokumentaci včetně projednání jednotlivých činnosti v rámci předprojektové, projektové a realizační činnosti. Zajišťuje veškeré náležitosti spojené s uváděním staveb do provozu.
  - **Oddělení provozu a služeb.** Koordinuje a zajišťuje materiálně technické zabezpečení instituce s výjimkou informačních a

[20] Národní úřad pro kybernetickou a informační bezpečnost - Organizační struktura úřadu. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní* stránka [online]. © [cit. 11.1.2023]. Dostupné Dostupné z: https://www.nukib.cz/cs/o-nukib/organizacni-struktura-uradu/

komunikačních technologií, vede evidence movitého a nemovitého majetku NÚKIBu a provádí jeho inventuru. Dohlíží na údržbu celkového majetku. Dále zajišťuje I provoz a údržbu služebních vozidel.

- **Oddělení personálních věcí a vzdělávání** – Provozuje personální, vzdělávací, mzdovou a sociální politiku v souladu s předpisy pracovního práva tzn. Zákoník práce a prováděcími předpisy. V závislosti na těchto dokumentech kontroluje dodržování pracovněprávních předpisů a zajišťuje evidence zaměstnanců. Provádí přijímací řízení s uchazeči o zaměstnání, zařizuje praxe pro studenty vysokých škol. Podílí se také na tvorbě pracovněprávní legislativy a vnitřních aktů řízení.

- **Odbor bezpečnosti.** Velmi důležitý odbor má pod sebou čtyři oddělení.
  - **Oddělení spisové a archívní služby**. Odpovídá za provoz archívů a činnosti podatelny a spisovny, registru utajovaných informací, specializovaného a bezpečnostního archivu. Kromě toho systematicky řídí spisovou službu, podílí se na vytváření interních aktů řízení a dalších dokumentů v oblasti ochrany utajovaných informací, také dohlíží na dodržování zásad ochrany utajovaných informací.
  - **Oddělení fyzické bezpečnosti.** Jeho činnost je prováděna v souladu se z. č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění pozdějších předpisů a vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti. Podílí se na tvorbě projektů fyzické ostrahy a projektové dokumentaci při rekonstrukčních a stavebních objektů. Řídí a zabezpečuje provoz při mimořádných událostech, spravuje technické zabezpečení, přístupy a klíčové systémy. Na ochraně objektů úřadu spolupracuje s Ochrannou službou Policie ČR.
  - **Oddělení informační bezpečnosti.** Provádí bezpečnostní řízení informačních a komunikačních systémů NÚKIBu nakládajících

s utajovanými informacemi, stará se o jejich dokumentaci a účetnictví v souladu s příslušnou legislativou. Zajišťuje plánování a rozvoj výše zmíněných systémů a kontroluje jejich provozní podmínky a plnění povinností souvisejících s jejich certifikací. Spolupracuje s *Cyber Security Manager a Architect* na zajišťování spolupráce v oblasti kybernetické bezpečnosti.

- **Oddělení personální bezpečnosti a krizového řízení.** Realizuje a zajišťuje přípravu úřadu k řešení krizových situací ve spolupráci s dalšími organizačními složkami v rámci NÚKIB. Reaguje na aktuální krizové incidenty a podílí se na tvorbě legislativy v oblasti krizového řízení a jejich zavádění do praxe. Zajišťuje a provádí činnosti osobní bezpečnosti v rozsahu stanoveném zákonem a vnitřním řádem úřadu.

5.1.4. Sekce národního centra kybernetické bezpečnosti[21]

- **Odbor vládní CERT (*GovCERT*).** Tento odbor má velmi rozsáhlou strukturu čítající šest různých oddělení.
  - **Oddělení reaktivní.** Primární náplní práce tohoto oddělení je prvotní koordinace, zpracování a následné řešení kybernetických bezpečnostních incidentů a vedení komunikačních kanálů s ostatními subjekty zasaženými krizovou situací.
  - **Oddělení analýzy síťového provozu.** Provozuje síťové sondy, IDS/IPS systémy a honeypoty. Také se věnuje analýze dat z odlišných serverů, síťových zařízení aj.
  - **Oddělení analytické.** Soustředí se na zkoumání dat. Provádí forenzní výzkum počítačů a jiných elektronických zařízení, analyzuje i malware a reverzní inženýrství.

[21] Národní úřad pro kybernetickou a informační bezpečnost – Organizační struktura úřadu. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. © [cit. 11.1.2023]. Dostupné z: https://www.nukib.cz/cs/o-nukib/organizacni-struktura-uradu/

- **Oddělení penetračního testování.** Zde se provádí praktické prověřování konkrétního zabezpečení s pomocí penetračního testování. V dnešní době je nabízeno mnoho služeb v tomto duchu – externí a interní penetrační testy, testy mobilních aplikací, wifi sítí nebo nestandartní testy konkrétního zařízení. Konzultuje také nasazení nových technologií.
- **Oddělení bezpečnosti operačních technologií.** Oddělení zaměřené na problematiku kybernetické bezpečnosti průmyslově orientovaných technologií či řídících systémů. Tyto systémy mohou být součástí Kritické infrastruktury ČR nebo jiných subjektů. Má podíl i na procesu regulace a kontroly subjektů provozujících operační technologie. Nabízejí i technické konzultace po domluvě.
- **Oddělení SecOps (Security Operations).** Hlavní činností oddělení je vývoj aplikací, jejich nasazení a zabezpečení s důrazem na využití nejnovějších technologií. Tato činnost je realizována jak pro vnitřní potřebu vládního CERT, tak při spolupráci s externími subjekty. Mezi aktuální projekty je zařazen například ***Cyber Czech*** (Největší kybernetické cvičení v České republice). Oddělení má také dvě pracovní skupiny – Pracovní skupina Neveřejného webu a Pracovní skupina Cloudových technologií.

- **Odbor regulace.** Zabývá se z. č. 181/2014 Sb., o kybernetické bezpečnosti. Každodenně komunikuje s regulovanými subjekty, ať už jde o regulační nebo metodickou podporu. Podílí se v přípravě legislativy v oblasti kybernetické bezpečnosti a hraje klíčovou roli při definování a ochraně informační infrastruktury významných systémů základních služeb ČR. Má pod sebou tři oddělení.
  - **Oddělení regulace soukromého sektoru.** Zajišťuje určení provozovatelů základních služeb – tato aplikace je prováděna na základě vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

- **Oddělení regulace veřejného sektoru.** Zajišťuje identifikaci významných IS – aplikováno na základě vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Zajišťuje i určení kritické infrastruktury ve veřejném sektoru. Má na starosti i komunikaci s příslušnými regulátory.
- **Oddělení regulace cloud computingu.** Zajišťování posuzování nabídek cloud computingu dle zákona o informačních systémech pro veřejnou správu. Pomáhá a poskytuje konzultace na posouzení dopadů narušení systémů pro účely procesů cloud computingu u orgánů veřejné moci. Komunikuje s příslušnými regulátory. Patří sem i Pracovní skupina Evropských certifikací.

- **Odbor kontroly.** Provádí kontroly dodržování povinností dle zákona o kybernetické bezpečnosti u regulovaných subjektů. Podílí se s odborem regulace na přípravě legislativy v oblasti kybernetické bezpečnosti a poskytuje metodickou podporu regulovaným subjektům. Spolupracuje i s dalšími kontrolními orgány. Dělí se na tři kontrolní oddělení: **Oddělení kontroly 1, Oddělení kontroly 2, Oddělení kontroly 3**.

5.1.5. Sekce informačních systémů[22]

- **Odbor bezpečnosti informačních a komunikačních technologií.** Obsahuje šest odlišných oddělení.
  - **Oddělení vývoje kryptografických prostředků.** Náplní funkce je základní aplikovaný výzkum a také vývoj v oblasti kryptografie. Vyvíjí, schvaluje národní šifrové algoritmy a vytváří národní politiku v této oblasti. Zabezpečuje také vývoj kryptografických schémat pro použití v kryptografických prostředcích ochrany utajovaných informací.

[22] Národní úřad pro kybernetickou a informační bezpečnost – Organizační struktura úřadu. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. © [cit. 11.1.2023]. Dostupné z: https://www.nukib.cz/cs/o-nukib/organizacni-struktura-uradu/

- **Oddělení certifikací informačních a komunikačních systémů.** Plní úkoly Národního střediska pro bezpečnost informačních systémů a provádí jejich následnou certifikaci. Zajišťuje povinnost úřadu jako orgánu pro bezpečnostní akreditaci IS nakládajících s utajovanými informacemi pro NATO, EU a jiné mezinárodní organizace. Také provádí styk s těmito organizacemi a průběžnou kontrolní činnost v akreditovaných systémech dle požadavků NATO či EU.
- **Oddělení certifikací kryptografických prostředků a pracovišť.** Téměř stejná náplň práce jako oddělení certifikací informačních a komunikačních systémů. Navíc stanovuje bezpečnostní standardy, které musí kryptografické pracoviště splňovat.
- **Oddělení Tempest.** Soustředí se na měření kompromitujícího elektromagnetického vyřazování, provádí analýzu a následné vyhodnocení elektrických a elektronických zařízení z hlediska úniku utajovaných informací. **Pracovní skupina kryptografických analýz**
- **Oddělení odborné podpory**
- **Oddělení Národní distribuční středisko.** Zajišťuje plnění úkolů a povinností zadaných NDA (Národní distribuční středisko) a provádí ověření odborné způsobilosti zaměstnanců v oddělení kryptografické ochrany.
- **Pracovní skupina CDA**

- **Odbor informačních technologií**
  - **Oddělení síťové infrastruktury a dohledu.** Zabývá se systémovou podporou aplikace ERP, personalistikou, mzdami a spisovou službou. Má na starosti instalaci systémů, uživatelskou podporu a správu, a především údržbu databází pro výše uvedené systémy. Také se zabývá strategickými a rozvojovými záměry v oblasti informačních systémů. **Pracovní skupina provozního dohledu**

- **Oddělení serverové infrastruktury.** Především udržuje veškeré komunikační cesty úřadu. Dále se zaměřuje na instalaci, přípravu i správu a optimalizaci serverové infrastruktury. Dále udržuje v provozu interně vyvinuté nástroje pro zabezpečenou komunikaci.
- **Oddělení podpory aplikací a rozvoje**
- **Oddělení klientské podpory.** Zabývá se podporou uživatelů v oblasti IT – veškeré problémy s hardwarem a softwarem koncových stanic a příslušenství uživatelů.
- **Oddělení bezpečnosti satelitních služeb.** Je odpovědné za implementaci a rozvor regulované služby systému Gallileo v ČR a koordinuje veškeré aktivity spojené s PRS. To vše v souladu s platnou legislativou Evropské Unie – 1104/2011/EU Sb.

5.1.6. Sekce strategických agend a spolupráce[23]

- **Odbor mezinárodní spolupráce a Evropské unie, Odbor cvičení a vzdělávání, Odbor centrální analytiky, Odbor kabinet ředitele**

[23] Národní úřad pro kybernetickou a informační bezpečnost – Organizační struktura úřadu. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. © [cit. 11.1.2023]. Dostupné z: https://www.nukib.cz/cs/o-nukib/organizacni-struktura-uradu/

6. Strategie zajišťování kybernetické bezpečnosti v ČR

V České republice probíhá zajišťování kybernetické bezpečnosti na základě propojení mezi jednotlivými institucemi. Tato strategie je prezentována ve schématu, který jsem vložila níže. Strategie je platná od roku 2020 na následujících pět let. Nová strategie kybernetické bezpečnosti v České republice bude zpracována a publikována v roce 2025, což znamená za dva roky. Jednotlivé instituce a úřady obsažené ve schématu mají přímo na svých webových stránkách definována práva a povinnosti, které vyplývají z této strategie.

Národní úřad pro kybernetickou bezpečnost je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.[24] **Ministerstvo zahraničních věcí ČR** se podílí na formulaci, provádění a koordinaci zahraniční politiky ČR v oblasti kybernetické bezpečnosti. Zajišťuje plnění hlavních cílů Národní strategie kybernetické bezpečnosti v mezinárodněpolitické oblasti.[25] **Ministerstvo vnitra ČR** má samostatné oddělení zaměřené na kybernetickou bezpečnost. **Bezpečnostní informační služba** se zabývá˘, např. šetřením nejrůznějších druhů elektronických útoků s dopadem na chráněné zájmy ČR, a dále shromažďováním a analýzou informací o reálných či potenciálních hrozbách a rizicích souvisejících s provozováním strategických informačních a komunikačních systémů, jejichž zničení či narušení by mohlo mít vážný dopad na bezpečnost či ekonomické zájmy ČR.[26] **Ministerstvo obrany ČR** působí v rámci Strategie kybernetické bezpečnosti v České republice dvěma

[24] Národní úřad pro kybernetickou a informační bezpečnost – O NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. © [cit. 11.1.2023]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

[25] Odbor kybernetické bezpečnosti | *Ministerstvo zahraničních věcí České republiky* [online]. © [cit. 11.1.2023]. Dostupné z: https://www.mzv.cz/jnp/cz/o_ministerstvu/organizacni_struktura/utvary_mzv/odbor_kyberneticke_bezpecnosti.html

[26] Kybernetická bezpečnost | BIS. *Bezpečnostní informační služba České republiky* | *BIS* [online]. Copyright © 2023 Bezpečnostní informační služba [cit. 19.01.2023]. Dostupné z: https://www.bis.cz/kyberneticka-bezpecnost/

institucemi – Národní centrum kybernetických operací a Generální štáb Armády České republiky.

Generální štáb Armády České republiky interaguje s pomocí Velitelství informačních a kybernetických sil. **Velitelství informačních a kybernetických sil** je strategickým nástrojem přispívajícím k bezpečnosti a obraně České republiky. Ve struktuře velení a řízení Armády České republiky spadá do taktické úrovně společně s pozemními silami, vzdušnými silami a velitelstvím teritoria.[27] Národní centrum kybernetických operací je vojenské zpravodajství, které se právě buduje za účelem kybernetické obrany.[28]

Národní centrála proti organizovanému zločinu je výkonným pracovištěm služby kriminální policie a vyšetřování s působností na celém území České republiky. V rámci své působnosti se specializuje na odhalování organizovaného zločinu, finanční kriminality, závažné hospodářské trestné činnosti a korupce.[29]

[27] *Armáda České republiky* [online]. © [cit. 19.1.2023]. Dostupné z: https://acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/

[28] Vojenské zpravodajství | Kybernetická obrana. *Vojenské zpravodajství* [online]. © [cit. 11.1.2023]. Dostupné z: https://www.vzcr.cz/kyberneticka-obrana-46

[29] Národní centrála proti organizovanému zločinu SKPV - Policie České republiky. *Úvodní strana - Policie České republiky* [online]. Copyright © 2023 Policie ČR, všechna práva vyhrazena [cit. 19.01.2023]. Dostupné z: https://www.policie.cz/clanek/narodni-centrala-proti-organizovanemu-zlocinu-skpv.aspx

Obr. 2. Strategie zajišťování kybernetické bezpečnosti v ČR[30]

Kybernetickou bezpečností se v České republice zabývá i mnoho jiných organizací, které nejsou uvedeny v oficiální Strategii zajišťování kybernetické bezpečnosti v České republice. Jejich práce je, ale také velmi důležitá pro odhalování nových hrozeb či školení zaměstnanců firem v této oblasti. Informace o těchto organizacích jsem získala přímo z jejich internetových stránek. Většina z těchto organizací je podpůrná pro jiné organizace na poli vzdělávání a vývoje do budoucna a vylepšování bezpečnosti i rozvoje informačních a komunikačních technologií. Mezi tyto organizace patří také národní CERT v jednotlivých státech, například v Rakousku, Polsku, ve Slovenské republice nebo ve Spojených státech amerických.[31]

[30] Vláda schválila strategii kybernetické bezpečnosti na následujících pět let | *IT SECURITY NETWORK NEWS. IT SECURITY NETWORK NEWS* [online]. Copyright © 2022 [cit. 19.01.2023]. Dostupné z: https://www.itsec-nn.com/vlada-schvalila-strategii-kybernetickebezpecnosti-na-nasledujicich-pet-let/

[31] CyberSecurity.CZ. *CyberSecurity.CZ* [online]. © [cit. 19.1.2023]. Dostupné z: https://www.cybersecurity.cz/links.html

AFCEA má svoji pobočku v České republice od 5. května 1993. Dlouhodobě se zaměřuje na oblast podpory rozvoje informačních a komunikačních technologií ozbrojených sil. Ozbrojené síly České republiky představují jeden z významných nástrojů obrany všeobecně uznávaných morálních hodnot. Českou pobočku řídí třináctičlenná rada v čele s prezidentem pobočky, kterým je v současné době Ing. Tomáš Müller. Tato pobočka má osm čestných viceprezidentů. Mezi nimi je také současný prezident České republiky armádní generál v.z. Ing. Petr Pavel, M.A.[32]

CESNET je zájmové sdružení právnických osob se sídlem v Praze. Předmětem jejich činnosti je provádění nezávislých aktivit výzkumu a vývoje v oblasti informačních a komunikačních technologií a zároveň poskytování služeb v této oblasti. Dále podporují vzdělávání a uvádění výsledků vlastních výzkumů z teorie do praxe aj. Vše je realizováno v rozsahu získaných dotací.[33] Zároveň se podílí na rozšiřování e-infrastruktury. E-infrastruktura je komplexní sada informatických nástrojů použitelných pro řešení problémů z celé řady oborů.[34] K tomuto sdružení patří také CESNET CERTS, který zodpovídá za řešení bezpečnostních incidentů v síti, kterou CESNET využívá. Princip je stejný jako u vládního CERTu.

CZ.NIC-CSIRT je bezpečnostní tým pro dohled nad sdružením CZ.NIC.

ČIMIB (Český institut manažerů informační bezpečnosti) je profesní sdružení, založeno v roce 2007. Jeho cílem je sdružovat odborníky z oblasti informační bezpečnosti. Členy jsou odborníci, především ze státní správy, finanční instituce, komerční i neziskové subjekty a technologičtí dodavatelé. Velmi

[32] Česká pobočka AFCEA | AFCEA. *AFCEA* [online]. © [cit. 19.1.2023]. Dostupné z: https://www.afcea.cz/ceska-pobocka-afcea1/

[33] CESNET | Základní informace o sdružení CESNET. CESNET | *CESNET, zájmové sdružení právnických osob* [online]. Copyright © 1996 [cit. 11.02.2023]. Dostupné z: https://www.cesnet.cz/sdruzeni/zakladni-informace-o-sdruzeni-cesnet/

[34] CESNET | E-infrastruktura. CESNET | *CESNET, zájmové sdružení právnických osob* [online]. Copyright © 1996 [cit. 11.02.2023]. Dostupné z: https://www.cesnet.cz/e-infrastruktura/

důležitou součástí tohoto sdružení je legislativní část. ČIMIB nenavrhuje změny v zákonech a nové zákony o kybernetické bezpečnosti, ale pomáhá jejich uvedení do praxe.[35]

[35] o ČIMIBu | cimib.cz. *Český institut manažerů informační bezpečnosti* | cimib.cz [online]. © [cit. 19.1.2023]. Dostupné z: https://www.cimib.cz/o-cimibu/

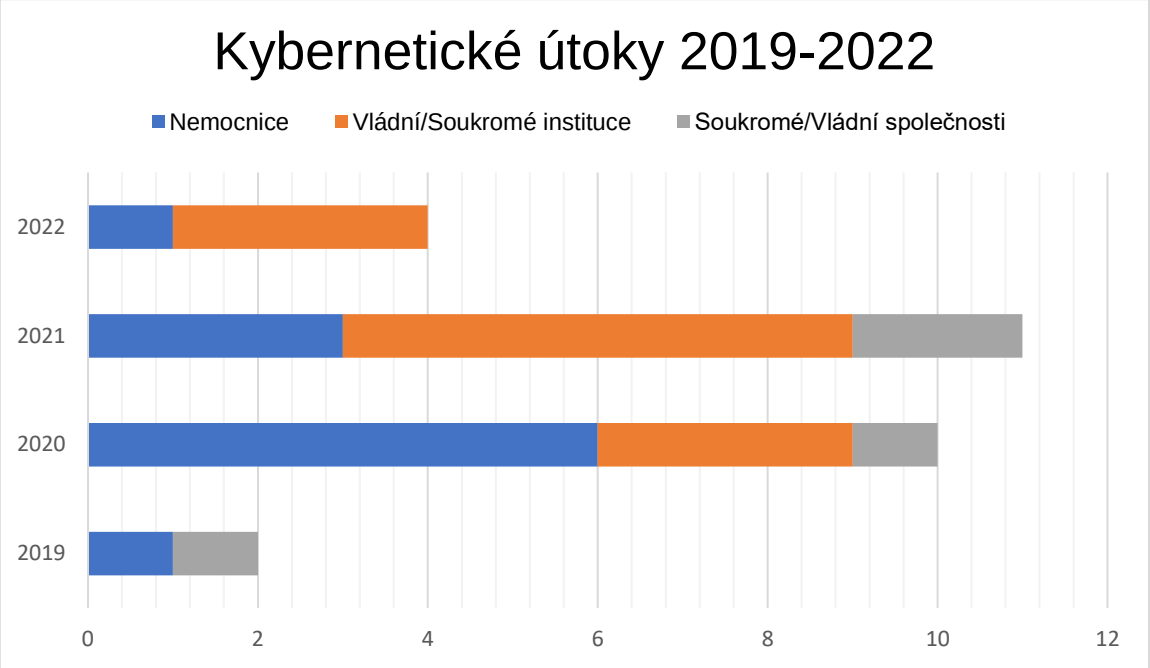
7. Kybernetická bezpečnost ve vládním sektoru

Ochraně letišť proti kybernetickým hrozbám se v posledních letech věnuje více pozornosti. Po celém světě si zaměstnanci různých firem začínají uvědomovat, jak výrazně se technologie posunuly kupředu. Obětí hackerů se může stát jakákoli společnost, která je připojena k internetové síti a pohybuje množstvím dat v kyberprostoru. Vlády jednotlivých států, Českou republiku nevyjímaje, začaly v poslední deseti letech více investovat do kybernetické bezpečnosti a obrany proti hrozbám nejen z reálného světa, ale i z toho kybernetického. V nejnovější Bezpečnostní strategii České republiky, která byla schválena v únoru 2015, jsou kybernetické útoky zmíněné na 11. straně. V citaci z tohoto bezpečnostního dokumentu je určena i jedna definic kyberprostoru jako celku: *„Kybernetické útoky. Kybernetický prostor je velmi specifický neexistencí geografických hranic a relativizací vzdálenosti mezi zdroji hrozeb a potenciálním cílem. Díky své asymetričnosti pak umožňuje státním i nestátním aktérům poškodit strategické a významné zájmy ČR bez využití konvenčních prostředků. Neustále se zvyšuje počet a sofistikovanost kybernetických útoků proti veřejné a soukromé sféře. Tyto útoky mohou způsobit selhání zejména komunikačních, energetických a dopravních sítí či dopravních procesů, průmyslových nebo finančních systémů, mající za následek významné hmotné škody. Závislost ozbrojených sil státu na informačních a komunikačních systémech může mít vliv na obranyschopnost státu. S kybernetickými útoky zároveň úzce souvisí problematika politické a ekonomické špionáže.“*[36] Kybernetická trestná činnost tedy patří k hrozbám, které začínají být patrné každým uplynulým rokem. Hackeři a jiní pachatelé se neustále zlepšují a vymýšlejí nové a nové hrozby, kterými by mohli vážně narušit infrastrukturu.

Na vytvořeném grafu jsem porovnala počty napadených institucí od roku 2019 do 2022. Tuto dobu jsem zvolila z důvodu velké aktivity hackerů na vládní instituce, prvky kritické infrastruktury i mediálních společností. Důvodem je také

[36] S. 11. - *Bezpečnostní strategie České republiky* [online]. Praha: Ministerstvo zahraničních věcí České republiky, únor 2015.

počátek celosvětové pandemie koronaviru v roce 2020, která uspíšila převod dat a informací do elektronické podoby. Do grafu jsem zanesla kybernetické útoky velkého rozsahu, které ovlivnily postupný vývoj zvýšeného zájmu o kybernetickou bezpečnost v České republice.



Graf. č. 1. Kybernetické útoky 2019–2022

Ze získaných výsledků jsem vyvodila následující závěry. Rok **2019** znamenal počátek hackerských útoků v České republice. V následujících letech 11. prosince byla napadena Benešovská nemocnice a 23. prosince byla ochromena počítačová síť společnosti OKD. V roce **2020** bylo zaznamenáno více útoků na nemocnice a polikliniky. V každém z případů byly ochromeny systémy nemocnice a způsobilo se tak ochromení celého systému. Následky byly především finančního charakteru. Hackerům šlo tento rok především o přístupové údaje nebo citlivá data. Mezi zasaženými bylo také Letiště Praha, bezpečnostnímu týmu se ale povedlo jednotlivé útoky zastavit. Mezi napadenými se objevily i interní systémy Ministerstva vnitra ČR – zde však nešlo o konkrétní cíl. Hacker se snažil zjistit zranitelná místa. V roce **2021** byl napaden systém veřejné správy dne 4.

března. Tento útok měl za následek poškození některých dat Magistrátu Hl. města Prahy. Vláda zareagovala vyhrazením financí na zajištění kybernetické bezpečnosti veřejné správy. Hackeři také napadli kolem 500 serverů skrze poštovní servery Microsoft Exchange. O tomto nebezpečí informoval NÚKIB. Pod útokem se ocitly i tři polikliniky v Praze. 22. března byl napaden server Českých drah, bezpečnost na trati ale hackeři neovlivnili. Napaden byl také Institut plánování a rozvoje hlavního města Prahy i Národní knihovna ČR. V uplynulém roce **2022** se více hackerů začalo zaměřovat na státní instituce a společnosti. Pod útokem se ocitla aplikace Ministerstva financí ČR, portál Českých drah a Portál veřejné správy. K těmto třem útokům se po jejich provedením doznala protiruská skupina Killnet.[37]

7.1. Kybernetická bezpečnost na letištích[38]

Letiště Praha, a.s. patří mezi prvky kritické infrastruktury dle Nařízení vlády 432/2010, o kritériích určení prvku kritické infrastruktury, konkrétně písmeno C. Letecká doprava, v níž je letiště obecně definováno následovně: **C. 1 Letiště**, Veřejné mezinárodní letiště způsobilé přijetí letu podle přístrojů, u kterého není možné leteckou obchodní dopravu zajistit alternativním letištěm nebo alternativní zajištění je příliš nákladné, nehospodárné nebo velmi těžko proveditelné. **Alternativním letištěm** se rozumí veřejné mezinárodní letiště, které **a)** je schopno zajistit nejméně 80 % letecké obchodní dopravy letiště, pro které je určeno jako alternativní, **b)** je v čase 2 hodin dosažitelné jiným druhem dopravy, **c)** má dostatečnou kapacitu pohybových ploch a kapacitu terminálu, **d)** má stejnou nebo podobnou kategorii jako letiště, pro které je určeno jako alternativní, a **e)** je způsobilé přijmout let vykonaný podle přístrojů. **C. 2 Řízení letového provozu**

[37] Hackerským útokům čelily v Česku nemocnice, *Národní knihovna či volební web - Novinky.* [online]. Copyright © 2003 [cit. 13.02.2023]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-hackerskym-utokum-celily-v-cesku-nemocnice-narodni-knihovna-ci-volebni-web-40394428

[38] Bezpečnost létání začíná čím dál více mimo letiště a letadla. Například v kyberprostoru | Letecké právo | Zprávy | *Flying Revue. Flying Revue - Vše pro příznivce létání* [online]. © [cit. 19.1.2023]. Dostupné z: https://www.flying-revue.cz/kam-se-zacina-rozsirovat-ochrana-letectvi

a) přibližovací služba řízení a letištní služba řízení letiště určeného jako kritická infrastruktura, nebo **b)** oblastní služba řízení poskytující letové provozní služby včetně řízení letového provozu ve vzdušném prostoru České republiky. **D. Vnitrozemská vodní doprava** Vnitrozemská vodní cesta, jejíž užití nelze nahradit užitím náhradní vnitrozemské vodní cesty ani dopravou jiného druhu. [39]

V dnešní době, především v posledních deseti letech, se mezinárodní letiště častěji zaměřují na kybernetické hrozby a posilují ochranu svého kyberprostoru. S postupem modernizace a elektronizace letištních služeb vznikla totiž kritická místa výrazně závislá na kyberprostoru, např. nové technologie zavedené do systému řízení letadel, online propojení jednotlivých dopravců, ale také řízení leteckého provozu. Díky modernizaci, například možnost objednávání a zrušení letu z pohodlí domova, zaznamenala letiště a letecké společnosti větší zájem o leteckou dopravu, ale objevily se také nevýhody využívání kyberprostoru. Pachatelé kybernetické trestné činnosti mohou způsobit nemalé škody nejen na majetku, ale i ve vážnějších případech na životech. Řízení letecké dopravy mají na starosti zaměstnanci, kteří se starají o bezpečný průlet skrze jejich zóny. Pokud by se ale hacker dostal do systémů této instituce a přerušil provoz, mohlo by dojít k vážným ztrátám na životech, např. by se dvě letadla mohla srazit ve vzdušném prostoru. To, co začalo jako obyčejné vydírání nebo krádež informací či dat, by mohlo skončit katastrofou. Z tohoto důvodu začala jednotlivá letiště investovat do kybernetické bezpečnosti, například vytvořením dohledových center. Dohledové centrum je instituce založená za účelem dohledu nad bezpečnostními incidenty a událostmi pro potřebu udržovat tým správců, analytiků a bezpečnostních expertů na vysoké úrovni.[40] Finanční investice jsou v řádech milionů. Bezpečnostní technici si totiž uvědomují, že pro zabezpečení pracoviště a zajištění bezpečného přesunu zákazníků, je důležité zajistit co nejlepší ochranu. Kyberprostor je sice

[39] Nařízení vlády č. 432/2010 Sb., o kritériích určení prvku kritické infrastruktury. In: Sbírka zákonů, 30.12. 2010.

[40] Bezpečnostní dohled jako služba | *AUTOCONT. AUTOCONT a.s.* | *AUTOCONT* [online]. © [cit. 19.1.2023]. Dostupné z: https://www.autocont.cz/produktlisty/security-supervision-as-a-service

mohutný a ubránit se proti všem hrozbám není možné, ale letiště musí patřit mezi špičku v zajišťování bezpečnosti svých klientů a zaměstnanců.

Dohledové centrum kybernetické bezpečnosti se na Letišti Praha, a.s., je oficiálně označované jako CSIRT LKPR. Členové tohoto týmu jsou zaměstnanci útvaru Informační bezpečnosti. Pro komunikaci s dalšími centry se užívá i název CSOC (Cyber Safety Operation Center, v překladu operační centrum kybernetické bezpečnosti). Tým má v současnosti 15 členů.

Cíle dohledového centra:

- Poskytování služeb v oblasti informační bezpečnosti a bezpečnosti průmyslových řídících systémů používaných Letištěm Praha
- Osvětová a školící činnost v rámci své konstituce
- Proaktivní a reaktivní služby v oblasti informační bezpečnosti
- Zajištění jednoduchého a důvěryhodného kontaktu pro celou síť Letiště Praha
- Koordinace řešení a prevence bezpečnostních incidentů v sítích Letiště Praha
- Pomoc institucím připojeným k sítím v rámci působnosti CSIRT LKPR a vytvoření jejich bezpečnostní strategie.[41]

[41] CSIRT LKPR | Letiště Václava Havla Praha, Ruzyně. Letiště Václava Havla Praha | *Letiště Václava Havla Praha, Ruzyně* [online]. Copyright © [cit. 13.02.2023]. Dostupné z: https://www.prg.aero/csirt

8. Metody šetření[42]

8.1. Dotazník

Dotazník jako metoda šetření se řadí mezi kvantitativní metody sběru dat. Na rozdíl od kvalitativních metod, které obsahují menší počet respondentů, obecné doporučení je pět až deset osob, kvantitativní metody jsou zaměřeny především na sbírání dat od respondentů ve značném množství kupříkladu padesát osob z jedné organizace. Získaná data mohou být užita i v dalším statistickém šetření. Kvalitativní metody, jako je například rozhovor je obtížné vyhodnotit obecně a formálně, protože dochází k užšímu lidskému kontaktu.

Dotazník je ideální metodou nejen pro odborné práce, jejichž autoři velmi často potřebují velké množství dat, aby mohli potvrdit svoji hypotézu, ale také zaměstnanci firem, které si potřebují ověřit například bezpečnostní problém nebo zjistit, jak dobře jsou ostatní zaměstnanci proškoleni.

Postup při tvorbě dotazníku není pevně stanoven, ale aby byl dotazník ve výsledku efektivní, je vždy potřebné udělat následující kroky: **1.** Formulovat problém, který chceme řešit. **2.** Stanovení hypotéz. Vytvoření předpokladu k problému nebo cíli, ke kterému data potřebujeme. **3.** Sběr dat pomocí dotazníku, který má jasně formulované otázky. U případů, kdy následně potřebujeme i grafy, se doporučují jednoduché otázky typu ANO/NE. **4.** Analýza sesbíraných dat a jejich následně zpracování. **5.** Implementace závěrů. Může následovat také využití získaných dat k dalšímu rozvoji skupiny/organizace apod., kde jsme šetření prováděli. Pokud je dotazník vytvořen správně, je možné získat během krátkého období velké množství odpovědí a následně je vyhodnotit. Můj dotazník, který jsem vytvořila s pomocí služby Survio je zaměřen na téma mé bakalářské práce „Kybernetická bezpečnost prvku kritické infrastruktury“. Dotazník má pět částí, z nichž každá se zabývá jinou oblastí kybernetické bezpečnosti. Obsahuje 24

[42] Kvantitativní výzkum vs. kvalitativní výzkum - *Survio. Redirecting to /en/* [online]. Copyright © Copyright 2012 [cit. 06.02.2023]. Dostupné z: https://www.survio.com/cs/blog/jak-vytvorit-dotaznik/kvantitativni-vyzkum-kvalitativni-vyzkum

otázek, které jsou otevřené i uzavřené. Cílem dotazníkového šetření je ověřit, zda zaměstnanci Letiště Praha, a.s., kteří jsou pravidelně proškolováni oddělením bezpečnosti v oblasti kybernetické bezpečnosti, přesunuli tyto znalosti také do svého soukromého života. Pokud ano, jak to učinili? Tyto otázky mě velmi zajímaly a z velké části přispívaly k vybrání tématu bakalářské práce. Z vlastní zkušenosti vím, že můj otec, pan Ing. Evžen Bílek, který je zaměstnancem letiště v oddělení interní komunikace, se velmi zajímá o současné kybernetické hrozby a zároveň doma zavádí některé doporučené postupy. Předpokládám, že letiště jako velmi zabezpečené pracoviště, dbající na proškolení každého zaměstnance z hlediska kybernetické bezpečnosti, může ovlivnit i zaměstnancův život v jeho/její domácnosti.

Pro potřeby bakalářské práce bylo záměrem pod záštitou Operačního centra pro kybernetickou bezpečnost Letiště Praha, a.s., rozeslat dotazníkové šetření hromadně s pomocí e-mailu. V prvním kroku jsem nejprve napsala panu řediteli tohoto pracoviště, Ing. Romanu Palkovičovi, a poslala mu zpracovaný dotazník. Pan Palkovič vzápětí zareagoval a po následné diskuzi o možném zneužití získaných dat, se ukázalo, že by mohlo být nebezpečné tyto informace zveřejnit, protože soukromé informace mohou obsahovat také citlivé firemní informace. Přístup pana ředitele Palkoviče byl v souladu se zásadami kybernetické a informační bezpečnosti na Letišti PrahaS. Dotazník by bylo možné rozeslat pouze s otázkami obecného charakteru o kybernetické bezpečnosti a menšímu počtu zaměstnanců. Na základě výše uvedeného zjištění jsem dotazníkové šetření nahradila rozhovorem s inženýrem Palkovičem a magistrem Petrákem o obecném fungování procesů týkajících se kybernetické bezpečnosti v rámci Letiště Praha,a.s. Využila jsem rozhovor jako kvalitativní metodu sběru dat.

8.2. Rozhovor[43]

Rozhovor se řadí mezi kvalitativní metody šetření. Kvalitativní postup je orientován na popis a zjišťování jevů. Jsou zde využívána více slova než obecná data a tyto metody bývají podrobnější. Zpravidla se výzkum provádí na menším počtům respondentů. Výhodou výzkumu s pomocí rozhovoru je jeho flexibilita při sběru odpovědí – je možné zareagovat či rozvést otázku více podrobněji na poli, které autora zajímá. Rozhovor se snaží o porozumění celku a je možné jeho otázky přizpůsobit novým informacím. U kvalitativního rozhovoru je velmi důležité, jakým způsobem jsou kladeny otázky, jejich počet i provázanost. Otázky by měly být otevřené, neutrální a jasné. Každá otázka by měla dát možnost respondentovi odpovědět vlastními slovy. Je důležité, aby dotazovaný vyjádřil svůj názor. Zároveň je možné touto metodou dosáhnout propojení mezi otázkami, které tazatel pokládá. Obvykle je užitečné, pokud se tazatel zaměří i na pocity respondenta. Je vhodné ptát se na otázky typu „Jaký je Váš názor…“ nebo „Co si myslíte, že představuje…“[44] V tomto duchu tvorbu a pracování s metodou rozhovoru zmiňuje ve své knize Pavel Hendl: *„Vedení kvalitativního rozhovoru je umění i vědou zároveň. Vyžaduje dovednost, citlivost, koncentraci, impersonální porozumění a disciplínu.“*[45] Na provedení rozhoru neexistují žádná pravidla, ale doporučení, která byla sepsána kvalifikovanými odborníky. V rozhovoru, který je přepsán v 9. kapitole, se zaměstnanci Letiště Praha, jsem využila tento teoretický základ vedení rozhovoru. Rozhovor byl veden na základě připravených otázek, které jsem v jeho průběhu doplňovala jinými otázkami, které vedli k následné diskuzi a více přiblížily problematiku, které se v bakalářské práci věnuji.

---

[43] Metodika ke zpracování závěrečné práce pro vybrané nelékařské zdravotnické obory | *Lékařská fakulta Masarykovy univerzity. Informační systém* [online]. Copyright © 2019 Masarykova univerzita [cit. 13.02.2023]. Dostupné z: https://is.muni.cz/do/rect/el/estud/lf/js19/metodika_zp/web/pages/06-kvalitativni.html

[44] Kvalitativní rozhovory – polostrukturované a nestrukturované – *WikiKnihovna.* [online]. © [cit. 19.1.2023]. Dostupné z: https://wiki.knihovna.cz/index.php?title=Kvalitativn%C3%AD_rozhovory_%E2%80%93_polostrukturovan%C3%A9_a_nestrukturovan%C3%A9

[45] HENDL, Jan. *Kvalitativní výzkum: základní metody a aplikace.* Praha: Portál, 2005, s. 168–172

Pro potřeby rozhovoru s panem inženýrem Palkovičem a panem magistrem Petrákem jsem stanovila tři hypotézy, které jsou vzájemně provázány. Hypotézy zároveň vycházejí z mého vlastního výzkumu kybernetických hrozeb v České republice v uplynulých letech.

1. **„Jakou funkci plní dohledové centrum CSOC při boji s kybernetickými hrozbami, které ohrožují Letiště Praha?“**
2. **„Je lidský faktor jednou z největších hrozeb v oblasti kybernetické bezpečnosti?“**
3. **„Jaký je názor respondentů na nově schválený zákon o kybernetické bezpečnosti, případně ovlivní to ve vyšší míře tuto sekci Letiště Praha?“**

9. Rozhovor s Ing. Romanem Palkovičem a Mgr. Stanislavem Petrákem

Rozhovor s panem Ing. Romanem Palkovičem, a Mgr. Stanislavem Petrákem, proběhl v budově APC na Letišti Praha, a.s. Při vstupu do budovy jsem se musela legitimovat a na vrátnici proběhla kontrola občanského průkazu. Následně jsem byla uvedena do centra CSOC panem inženýrem Palkovičem, kde již čekal také pan magistr Petrák. Rozhovor trval 25 minut. K některým otázkám se vyjádřili oba, k některým jen jeden z nich. Pro větší přehlednost jsem odpovědí vložila iniciály jmen Ing. Romana Palkoviče (dále RP) a Mgr. Stanislava Petráka (dále SP).

Dobrý den, děkuji Vám za Vaši ochotu. Nejprve bych Vás poprosila, abyste se mi představili a popsali, jakou náplň práce zastáváte na Letišti Praha a.s.

RP: Jmenuji se Roman Palkovič a má pozice je ředitel informační bezpečnosti a z pohledu zákona o kybernetické bezpečnosti zastávám roli manažera kybernetické bezpečnosti. Moje role má dvě odlišné funkce. První manažerská obsahuje řízení lidí, strategie, aktivit a zároveň kontrolu, aby vše fungovalo a sedělo v rámci organizační jednotky informační bezpečnosti (OJ IBE). Druhá funkce nemanažerská zodpovídá za fungování systému informační bezpečnosti jako celku. CSOC řeší tu technickou část včetně reakce na události a incidenty a pak jsou tady metodici, kteří řeší legislativu v oblasti kybernetické bezpečnosti. V rámci letiště jsou to zejména různé směrnice, metodiky a pracovní postupy. Dále jsou to například úpravy stávajících systémů nebo zavádění úplně nových. S tím souvisí také Analýza rizik. Metodici zde prochází a vyhodnotí, jestli je tam něco potřeba upravit, co se týká informačních systémů a požadavků na bezpečnost.

SP: Jmenuji se Stanislav Petrák a jsem manažer dohledu kybernetické bezpečnosti. Z pohledu zákona o Kybernetické bezpečnosti jsem architektem kybernetické bezpečnosti, na rozdíl od Romana (Ing. Roman Palkovič), který je

primárně manažerem. Já a můj tým neustále sbíráme nové informace, reagujeme na incidenty a snažíme se nasazovat nové investice.

Je tedy pozice krizového manažera a pozice manažera kybernetické bezpečnosti totožná?

RP: Není. Je to rozdílné a oddělené zaměření. Manažer kybernetické bezpečnosti skutečně zajišťuje, aby společnost byla v souladu se zákonem. A třeba i to, že bude existovat nějaký plán pro řešení kybernetických incidentů. Následně je role krizového manažera, který řeší přímo danou situaci a její průběh.

Mou další otázkou je role a funkce dohledového centra na Letišti Praha, a.s. v oblasti informační a kybernetické bezpečnosti.

RP: Kybernetická bezpečnost je podkapitolou informační bezpečnosti. Kybernetickou bezpečnost řeší přímo Standa (Mgr. Stanislav Petrák) a tým CSOC, jehož primární náplní je odhalovat a reagovat na bezpečnostní události a incidenty. Informační bezpečnost je širší pojem, který vlastně řeší ochranu informací nehledě na to, zda jsou v digitální nebo vytištěné podobě.

Jak vůbec IBE vzniklo? Vedlo to ke zlepšení zajištění kybernetické bezpečnosti? Popřípadě jakým způsobem toto ovlivnil v posledních letech Covid-19?

SP: Kyberbezpečnost se na letišti zaváděla s prvním zákonem o kybernetické bezpečnosti, ale v té době se ještě nevědělo, na jakém místě bude stát v zákoně, který vešel v platnost v 2015. Od té doby se rozvíjela informační bezpečnost a postupně se začalo zjišťovat, jak je to v zákoně strukturované. Před covidem v roce 2018 se začalo vše více rozvíjet. Tehdy se jel systém 5x8 hodin, s příchodem covidu 2019/2020 sice bylo postavení současných prostor trochu zabrzděno a zavedl se dohled 24/7. Důležitost kybernetické bezpečnosti se tak postupně zvyšovala. Kvůli probíhající digitalizaci se také vymýšlely nové bezpečnostní postupy. Například po rozšíření služby Microsoft Teams během pandemie. Druhým milníkem byl následně počátek války na Ukrajině. Zvedla počty

DDoS i Phishingových útoků. Především se šíří phishing. Zkrátka je velký narůst různých útoků.

V návaznosti na tento pohled, jaké jsou dle vás z odborného hlediska nejrozšířenější kybernetická hrozba na Letišti Praha, a.s.?

SP: Největší nebezpečí je nevzdělaný uživatel. Tito uživatelé jsou nejvíce ohrožení. Přímo konkrétní hrozbou je dle mého názoru nejvíce DDoS a phishing.

Lidský faktor byl údajně i příčinou úspěšného útoku ransomwaru na Benešovskou nemocnici v roce 2019. Případ byl hojně medializovaný. Co bylo tehdy dle Vás tím největším problémem? Mohl za to skutečně pouze nezkušený uživatel?

SP: Slyšel jsem o tom. Myslím, že tam bylo problémů více. Nezkušení uživatelé, zastaralé systémy a zabezpečení infrastruktury bylo špatně navrženo.

RP: Celá oblast zabezpečení má vždy tři pilíře – lidi, procesy a technologie.

Nedávno byl schválen nový zákon v oblasti kybernetické bezpečnosti, který by měl vytvořit nejméně 6000 nových pracovních míst.

RP: Zákon jako takový je v pořádku a je dobře, že jej máme, pokud to vezmu jak z pohledu firem, tak bezpečí ČR jako takové. Když to vztáhnu na Letiště Praha, a.s., bude to mít zejména dopad z pohledu personální stránky. Bude to soupeření s trhem, abychom si naše lidi udrželi.

Jaké firmy si myslíte, že budou mít největší problém s tímto zákonem? Už v posledním roce se kybernetická bezpečnost více řeší ve firmách a probíhají školení.

RP: Rozhodně ty, co disponují vyšším kapitálem, to budou mít jednodušší v tom, že do určité míry si budou moct soulad se zákonem nakoupit třeba jako službu. Určitě bude poptávka po lidech, kteří ve firmě, když nic jiného, bezpečnost alespoň zaštítí a budou komunikovat s externí firmou. Co má od ideálního řešení

skutečně daleko. Vždy bude platit i pravidlo proporcionality – malá zubní ordinace asi nebude řešit stejným způsobem bezpečnost, jako například banka, ale požadavek na zvýšení bezpečnosti vznikne vždy.

SP: Dnes je pod zákonem o kybernetické bezpečnosti 300 až 350 firem. S novým zákonem se přidají další. Ale ne všechny stávající firmy mají dostatečně vysokou bezpečnost, aby splnily podmínky dané zákonem. Hlavně lidé jsou klíčoví.

IT jde neustále kupředu a stejně tak i kybernetické hrozby. Modernizace je tedy důležitým prvkem. Jaké kroky jsou podnikány v tomto směru?

SP: Bezpečnost lze začít budovat za použití stávajících systémů. 80 % bezpečnosti se zvládlo za 20 % investic. Dnes investujeme 80 % a 20 % se vrací do zabezpečení. Na to množství systémů, které jdou dopředu, je potřeba vymyslet nové zabezpečení a systémy.

RP: Technologie, které máme rozvíjíme a vedle toho jsou nové technologie, které plánujeme implementovat.

Moje poslední otázka je zaměřena na Českou republiku jako celek. Co považujete za největší hrozbu ve Vašem oboru?

SP: Kybernetická bezpečnost není na takové úrovni, kterou bychom chtěli. A díky tomu vázne i komunikace mezi firmami.

RP: Záleží na tom, jak bude ČR postupovat v zahraniční politice. Existuje řada skupin ve státech, jako jsou Čína a Rusko. Je to jen otázka času, na koho vlastně zamíří, na koho se zaměří a kdy se projeví jejich útok. Navyšováním bezpečnosti jim to vše ztěžujeme, ale pokud se na nás zaměří, tak v závěru jen prodlužujeme dobu od zahájení přípravy po úspěšný útok.

SP: Je to jako doping. Ten, kdo dopuje, je vždy napřed. Pokud se útočí na firmy, jde především o zisk. Ale hackerské skupiny států, u nich to není o zisku, ale o nějaké té politice, a o to, co je nad tím.

SP: Řekněme si to narovinu. Pokud někdo bude chtít, tak nás hackne. Nesmíme si dělat iluze.

Děkuji Vám za předané podněty a provedený rozhovor. Jsem velmi vděčná, že jste mi pomohli navázat spolupráci. Přeji Vám hezký den.

10. Vyhodnocení hypotéz

V této kapitole se zabývám získanými informacemi v návaznosti na hypotézy, které jsem stanovila. **1. „Jakou funkci plní dohledové centrum CSOC při boji s kybernetickými hrozbami, které ohrožují Letiště Praha, a.s.?“** Z provedeného rozhovoru vyplývá, že dohledové centrum CSOC řeší technické části v oblasti kybernetické bezpečnosti. Řadí se sem také reakce na události a bezpečnostní incidenty. Součástí centra jsou také metodici, kteří řeší legislativu (směrnice, metodiky, pracovní postupy), úpravy stávajících systémů a též provádějí Analýzu rizik. **2. „Představuje lidský faktor jednu z největších hrozeb v oblasti kybernetické bezpečnosti?“** V mé výzkumné činnosti se již delší dobu zabývám touto myšlenkou. Dlouhodobým porovnáváním příčin kybernetických incidentů ve státním a veřejném sektoru jsem došla k závěru, že nevzdělaný pracovník představuje nebezpečí, které nezachrání ani špičkový antivirus. Pan magistr Petrák také tuto hypotézu potvrdil. Vzdělání v oblasti kybernetické bezpečnosti dle mého názoru představuje nejvíce zranitelnou stránku a může být nebezpečnější než hackerský útok, který jsou technici schopni odrazit. Na Letišti Praha, a.s. jsou zaměstnanci pravidelně proškolováni, především z důvodu předejít těmto problémům. V jiných firmách si také začínají uvědomovat nebezpečí nevzdělaného uživatele a nový zákon tuto oblast podpoří. Jistě bude mít tento zákon příznivý účinek ve více oblastech než jen ve vzdělávací. **3. „Jaký je názor respondentů na nově schválený zákon o kybernetické bezpečnosti, případně ovlivní to ve vyšší míře tuto sekci Letiště Praha, a.s.?“** Tuto hypotézu jsem zařadila z důvodu potencionálních změn, které bude nutno na poli kybernetické a informační bezpečnosti zavést. Pan inženýr Palkovič osvětlil situaci, která nastane na Letišti, a.s. Spíše než zavedení nových pravidel a systémů na Letišti Praha, a.s. v oblasti kybernetické bezpečnosti, bude větší zátěž představovat trh práce a případný odliv zaměstnanců. Pracovní místa se budou tvořit i v jiných firmách a Letiště Praha, a.s. jako jeden z mnoha zaměstnavatelů bude muset reagovat, např. zvýšením platů.

Závěr

Letiště Praha, a.s. jako prvek kritické infrastruktury přistupuje ke kybernetické a informační bezpečnosti jako k oblasti, na kterou je potřeba brát zřetel. Pravidelné školení zaměstnanců, investice do nových systémů ochrany citlivých dat, úprava stávajících systémů a jejich zdokonalování, toto je jen zlomek z celkového obrazu. Letiště aktivně vyhledává informace o nových hrozbách a s pomocí metod jako je Analýza rizika či Krizový management prověřují stávající situaci na pracovišti. Jako firma si Letiště Praha, a.s. uvědomuje, jakým způsobem jsou kybernetická a informační bezpečnost důležité a nenahraditelné.

Poslední desetiletí zaznamenal svět obrovský krok kupředu v oblasti informačních technologií. Světová pandemie přispěla k uspíšení nevyhnutelného – převod dat do elektronické podoby. Koncept práce z domova se v posledních pěti letech změnil, a nejen soukromé firmy byly nuceny reagovat. Útočníci i oběti se přesunuli do kyberprostoru a každý den po celém světě probíhají boje, kdy se hackeři snaží dostat do institucí a aktivně tak ničit, špehovat, narušovat a krást data. Jiné prvky kritické infrastruktury a další instituce v České republice začínají na své obraně a bezpečnosti pracovat. Každý proškolený zaměstnanec jakékoli firmy, společnosti, instituce, úřadu představuje krok ke zvýšení bezpečnosti proti kybernetickým hrozbám v oblasti kritické infrastruktury. Tito zaměstnanci následně mohou své vědomosti předat dále rodině, přátelům, blízkým. Já osobně jako člověk, který se o kybernetickou bezpečnost zajímá už několik let a chce se v této oblasti dále profesně rozvíjet, se také aktivně snažím pomáhat ve svém okolí lidem, kteří si nejsou jistí v online prostředí a stávají se tak velmi snadným cílem pro kybernetické útoky. Na tuto nejnutnější obranu existuje několik pravidel. Ale je potřebné si uvědomit, že i když je obrana sebe lepší, hackeři budou vždy napřed. Obrana proti hrozbě je nejvíce efektivní, pokud známe její dopady. Jak zmínil pan inženýr Palkovič v rozhovoru v deváté kapitole: *„Je to jako doping. Ten, kdo dopuje, je vždy napřed.“*, následně doplněn panem magistrem Petrákem: *„Řekněme si to narovinu. Pokud někdo bude chtít, tak nás hackne. Nesmíme si dělat iluze.*“

Seznam použité literatury

1. HENDL, Jan. *Kvalitativní výzkum: základní metody a aplikace.* Praha: Portál, 2005, s. 168 - 172. ISBN 80-7367-040-2
2. KOLEKTIV autorů. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech*. Vydavatel a tisk: Policejní Akademie České republiky v Praze. Praha 2020. ISBN: 9788072515059
3. KOLOUCH, Jan. BAŠTA, Pavel. a kol. *CyberSecurity.* 1. vydání. CZ.NIC, z. s. p. o., Praha 2019. ISBN: 9788088168317
4. MAURER, Tim. Cyber Mercenaries – THE STATE, HACKERS, AND POWER. Cambridge University Press., United Kingdom 2018. ISBN: 9781107566866
5. SEDLÁK, Petr. KONEČNÝ, Martin. a kolektiv. Kybernetická (ne)bezpečnost. CERM, Brno 2021. ISBN: 9788076230682
6. ŠULC, Vladimír. *Kybernetická bezpečnost*. Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., Plzeň; 2018. ISBN: 9788073807375.
7. *Bezpečnostní strategie České republiky* [online]. Praha: Ministerstvo zahraničních věcí České republiky, únor 2015. S. 24. Dostupné online. ISBN 978-80-7441-005-5.
8. Terminologický slovník – krizové řízení a plánování obrany státu - Ministerstvo vnitra České republiky. Úvodní strana – Ministerstvo vnitra České republiky [online]. Copyright © 2022 Ministerstvo vnitra České republiky, všechna práva vyhrazena Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx
9. Základní definice, vztahující se k tématu kybernetické bezpečnosti. *Ministerstvo vnitra České republiky*, 2009. Dostupné z: http://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx
10. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: Sbírka zákonů, 29.8. 2014.

11. Nařízení vlády č. 432/2010 Sb., o kritériích určení prvku kritické infrastruktury. In: Sbírka zákonů, 30.12. 2010.
12. Směrnice Evropského parlamentu a Rady EU 2016/1148 o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informačních systémů v Unii.
13. Nařízení Evropského parlamentu a Rady EU 2019/881,2018 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologiích.

Internetové zdroje

14. https://www.flying-revue.cz/kam-se-zacina-rozsirovat-ochrana-letectvi
15. https://www.autocont.cz/produktlisty/security-supervision-as-a-service
16. https://www.cesnet.cz/sdruzeni/zakladni-informace-o-sdruzeni-cesnet/
17. https://www.cesnet.cz/e-infrastruktura/
18. https://www.prg.aero/csirt
19. https://www.merriam-webster.com/dictionary/cyber
20. https://www.cybersecurity.cz/links.html
21. https://www.afcea.cz/ceska-pobocka-afcea1/
22. https://www.techtarget.com/searchdatamanagement/
23. https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-hackerskym-utokum-celily-v-cesku-nemocnice-narodni-knihovna-ci-volebni-web-40394428
24. https://www.survio.com/cs/blog/jak-vytvorit-dotaznik/kvantitativni-vyzkum-kvalitativni-vyzkum
25. https://www.bis.cz/kyberneticka-bezpecnost/
26. https://www.policie.cz/clanek/narodni-centrala-proti-organizovanemu-zlocinu-skpv.aspx
27. https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/
28. https://www.nukib.cz/cs/o-nukib/o-uradu/
29. https://www.nukib.cz/cs/o-nukib/organizacni-struktura-uradu/

30. https://nukib.cz/cs/galileo-prs/program-galileo/
31. https://www.nukib.cz/cs/galileo-prs/
32. https://www.nukib.cz/images/PRS/galileo2.jpg
33. https://www.epravo.cz/top/aktualne/nova-evropska-legislativa-v-kyberneticke-bezpecnosti-115320.html
34. https://www.cimib.cz/o-cimibu/
35. https://www.mzv.cz/jnp/cz/o_ministerstvu/organizacni_struktura/utvary_mzv/odbor_kyberneticke_bezpecnosti.html
36. https://acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/
37. https://www.itsec-nn.com/vlada-schvalila-strategii-kyberneticke-bezpecnosti-na-nasledujicich-pet-let/
38. https://www.vzcr.cz/kyberneticka-obrana-46
39. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime
40. https://www.techtarget.com/searchsecurity/definition/hacker