Kybernetické hrozby a jejich dopady na společnost v době světových krizí

Bc. Nikola Rebhanová

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. Nikola Rebhanová**
Osobní číslo:	**L22640**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Kybernetické hrozby a jejich dopady na společnost v době světových krizí**

Zásady pro vypracování

1. Zpracujte teoretický vstup vztahující se k dané problematice.
2. Proveďte posouzení vybraných globálních hrozeb v kontextu kybernetické bezpečnosti.
3. Identifikujte dopady vybraných kybernetických hrozeb na globální společnost.
4. Proveďte vyhodnocení dosažených výsledků a navrhněte vlastní řešení.

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

Seznam doporučené literatury:

1. COLLINS, Alan. *Contemporary security studies.* 3rd edition. United Kingdom: Oxford University Press, 2013. ISBN 978--0-19-969477-8.
2. DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha: Profesional Publishing s.r.o., 2019. ISBN 978-80-88260-39-4.
3. NONNEMANN, František, Vlastimil Červený a Dominik VÍTEK. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance.* Praha: Wolters Kluwer, 2022. ISBN 978-80-7676-515-3.

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 na 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: 26.4.2024

Jméno a příjmení studenta: Bc. Nikola Rebhanová

.....
podpis studenta

ABSTRAKT

Diplomová práce je zaměřená na kybernetické hrozby, které převládaly v době pandemie covid-19, Rusko-ukrajinského konfliktu a surovinové a energetické krize. Cílem práce je demonstrovat na příkladech vybraných kybernetických hrozeb dopady na společnost během světových krizí 21. století, které měly vliv na Českou republiku. Pro zjištění dopadů byla využita metoda What-if a poté metoda Analýza stromu událostí – ETA.

Klíčová slova: kybernetická bezpečnost, kybernetické hrozby, světové krize, ransomware, phishing, What-if, ETA

ABSTRACT

The Master's thesis focuses on the cyber threats spread during the COVID-19 pandemic, the Russian-Ukrainian conflict and the resource and energy crisis.

The goal of the thesis is to use selected examples of cyber threats to demonstrate the impact on society during the global crises of the 21st century that affected the Czech Republic. The impacts were identified by using the What-if analysis and then the Event Tree Analysis – ETA.

Keywords: cybersecurity, cyber threats, global crises, ransomware, phishing, What-if, ETA

Tímto bych ráda poděkovala vedoucímu mé diplomové práce panu Ing. Lukáši Pavlíkovi, Ph.D., za jeho ochotu, vstřícnost, za odborné připomínky a čas, který mi věnoval během psaní práce.

Chtěla bych poděkovat i mé rodině a přátelům, kteří mě po celou dobu mého studia podporovali.

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

OBSAH

ÚVOD

Kybernetická bezpečnost je v dnešní moderní době jedním z nejdiskutovanějším tématem vůbec. S nabývajícím pokrokem technologií a větší závislostí na digitálním světě se otvírá nový svět možností, ale zároveň i svět hrozeb. Kybernetické hrozby se čím dál častěji stávají realitou, která může mít mimořádně závažné dopady na společnost. O to víc je společnost zranitelnější, pokud se vede nějaký konflikt nebo nastane nějaká krizová situace. Hrozby jsou různorodé a útočníci se neustále vyvíjejí a zdokonalují své techniky. Tyto hrozby poškozují nejen jednotlivce, ale i firmy a národní instituce.

Tato diplomová práce se zaměřuje na kybernetické hrozby spojené se světovými krizemi. Hlavním cílem práce je vyhledat dopady spojené s kybernetickými hrozbami.

V úvodní části je základní seznámení s pojmy a výrazy využívanými v oblasti kybernetické bezpečnosti. Následně se v práci nachází právní rámec, který v této oblasti napomáhá zabraňovat, odolávat a zmírňovat následky útoků.

Důležitou součástí práce je i uvedení do kybernetických hrozeb jako takových. Jsou zde popsány jednotlivé typy útoků. Od kategorie útoků řadících se pod malware, přes sociální inženýrství až po DDoS útoky.

Jelikož práce pojednává o potenciálních útocích v době krizí, jsou zde vytyčeny nejzásadnější krize, které probíhaly ve 21. století až doposud. Tyto krize zásadně ovlivnily kyberprostor ve světě včetně kybernetické bezpečnosti v České republice. Mezi hlavní krize, o kterých bude pojednáváno jsou covid-19, Rusko-ukrajinský konflikt a surovinová a energetická krize.

V praktické části jsou tyto krize lépe popsány a dochází zde k propojení dané krize s kybernetickou bezpečností. Na jednotlivé oblasti navazuje analýza what–if, ve které jsou tvořeny scénáře příčin, ze kterých dále vyplývají důsledky a navazující metoda ETA, pomocí níž se hledají další možné dopady.

CÍLE PRÁCE A POUŽITÉ METODY

Cíl diplomové práce:

- Zjistit, jaké kybernetické hrozby ovlivňovaly Českou republiku během krizí 21. století.
- Demonstrovat na příkladech vybraných kybernetických hrozeb dopady na společnost během světových krizí 21. století, které měly vliv na Českou republiku.

Použité metody:

- Sběr dat a informací – metoda byla použita při zpracování teoretické části, dále při tvorbě podkladů praktické části práce.
- Brainstorming – jedná se o kreativní metodu, pomocí níž lidé vymýšlí nápady. Probíhá formou spontánní diskuse na dané téma. Metoda využita v teoretické i praktické části práce (Kadeřábková, 2020).
- What-if – metoda je založena na brainstormingu, při kterém pracovní tým prověřuje formou dotazů a odpovědí neočekávané události, které se mohou v procesu vyskytnout. Dotazy začínají charakteristickým „What – if“ - Co se stane, když? (Metoda „What – If“ (Co se stane, když..), 2022). Metoda byla použita pro vytvoření jednotlivých scénářů na zjištění dopadů kybernetických hrozeb.
- ETA – Jedná se o analytickou techniku, která se používá k vyhodnocení průběhu procesu a událostí vedoucích k možné nehodě (ETA (Event tree analysis) - analýza stromu událostí, @2024).

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ TERMINOLOGIE

První kapitola si klade za cíl vymezit základní pojmy v oblasti informační a komunikační technologii. Základní definice v kybernetické bezpečnosti. A mimo jiné i samotný právní rámec, o který se opírá oblast kybernetické bezpečnosti v České republice.

1.1 Informační a komunikační technologie

Úvodem této kapitoly je potřeba definovat samotný informační systém a jeho části.

Informační systém je možné definovat jako funkční celek, který má cíl zabezpečit cílevědomé a systematické shromažďování, zpracovávání, uschovávání a zpřístupňování informací a dat. Definice zahrnuje i datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie, postupy a související právní normy (Jirásek et al., 2022).

„Lze jej chápat i jako systém vzájemně propojených informací a procesů, které s těmito informacemi pracují“ (Sedlák, Konečný, 2023, s. 13).

Informační systém se skládá z:

- **Hardware** (dále jen „HW“) – jedná se o komponenty počítače, kterými jsou například monitor, klávesnice, mikrofon, procesor, operační paměť, různé druhy karet (grafická), apod. (Smejkal, 2018).
- **Software** (dále jen „SW“) – nebo také programové nástroje zahrnující systémové programy, které řídí fungování počítače, efektivní práci s daty a řídí komunikaci mezi počítačem a vnějším světem (Klimeš, @2024).
- **Dataware** (dále jen „DW“) – datové zdroje, které ke své práci využívají programové prostředky (Klimeš, @2024).
- **Peopleware** (dále jen „PW“) – lidská složka – řeší otázky fungování člověka v počítačovém prostředí, do kterého je zasazen (Klimeš, @2024).
- **Orgware** (dále jen „OW“) – organizační složka – soubor nařízení a pravidel, které definují provoz a využití informačních systémů a technologií (Klimeš, @2024).

Informační a komunikační technologie je veškerá technika, která zpracovává a přenáší informace, jedná se zejména o výpočetní a komunikační techniku a její programové vybavení (Doucek et al., 2019).

1.2 Kybernetická bezpečnost

Druhá podkapitola se bude věnovat pojmům, které se vyskytují v oblasti kybernetické bezpečnosti.

1.2.1 Definice a základní pojmy kybernetické bezpečnosti

Na začátek je důležité si objasnit pojem bezpečnost.

Bezpečnost podle terminologického slovníku ministerstva vnitra („dále jen MV“) je definována jako „*stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost. Je to tedy míra stability systému a jeho primární a sekundární adaptace“* (Terminologický slovník pojmů z oblasti krizového řízení…, 2016, s.5).

Bezpečnost informací je definována jako zachování důvěrnosti, integrity a dostupnosti informací. Důvěrnost je vlastnost, která zajišťuje, že informace nejsou dostupné nebo zpřístupněny neoprávněným jednotlivcům, entitám nebo procesům. Integrita znamená zajistit přesnost a úplnost informací a dostupnost vyjadřuje schopnost poskytovat přístup a použitelnost informací na žádost oprávněné entity. Bezpečnost informací má za cíl podporovat konkrétní úkoly nebo plány organizace, které se mohou lišit v závislosti na typu organizace (Nonnemann et al., 2022).

Kybernetická bezpečnost může být definována mnoha způsoby.

Jedno z prvních použití termínu kybernetická bezpečnost lze nalézt v Computer Science and Telecommunications Board´s Report. Text pochází z roku 1991 a bezpečnost je zde definována jako „*ochrana proti nechtěnému zpřístupnění, modifikaci nebo zničení dat v systému, a také zabezpečení systémů samotných*“ (Pačka, 2019, s. 11).

Ve výkladovém slovníku kybernetické bezpečnosti je tato bezpečnost definována jako *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru a zajištění důvěrnosti, integrity a dostupnosti informací v kybernetickém prostoru“* (Jirásek et al., 2022, s. 97).

Dle terminologického slovníku MV „*kybernetická bezpečnost zahrnuje ochranu důvěrnosti, integrity a dostupnosti informací při jejich zpracování, úschově, distribuci a prezentaci"* (Terminologický slovník pojmů z oblasti krizového řízení…,2016). Přičemž důvěrností se rozumí vlastnost informace, která o ní vypovídá, že není dostupná nebo není odhalena neoprávněným osobám, entitám či procesům. Integrita je vlastnost přesnosti, úplnosti a jistoty, že data nebyla neoprávněně změněna a jsou stále důvěryhodná a dostupnost představuje vlastnost použitelnosti a přístupnosti oprávněným entitám (Terminologický slovník pojmů z oblasti krizového řízení…,2016).

Kybernetická bezpečnostní událost je dle zákona o kybernetické bezpečnosti „*událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací"* (Česko, 2014). *Synonymem této zákonné definice se proto může stát i pojem kybernetická hrozba* (Ramešová, 2023).

Kybernetická hrozba je hrozba vyskytující se v kybernetickém prostoru (Doucek et al., 2019). Kolouch a kolektiv uvádí, že kybernetická hrozba je možnost poškození nebo narušení počítačové sítě nebo počítačového systému. Jedná se o akt umožňující změnu informace, aplikace či samotného systému (Kolouch et al., 2019). Odborná literatura vymezuje čtyři základní skupiny hrozeb, a to:

- **Únik informací** – při kterém dojde k vyzrazení chráněných informací.
- **Narušení integrity** – jedná se o změnu, poškození nebo vymazání dat.
- **Potlačení služby** – tím se rozumí úmyslné zabránění k přístupu k informacím, aplikacím nebo systému.
- **Nelegitimní použití** – znamená užívání informací neautorizovaným subjektem či neoprávněným způsobem (Kolouch et al., 2019).

Existuje celá řada klasifikací kybernetických hrozeb, ale nejčastěji jsou hrozby členěny dle:

- **Zdroje hrozby:**
  - Hrozby způsobené člověkem – **úmyslně** (úmyslné smazání dat, fyzické poškození počítačového systému, zcizení dat a informací, kybernetické útoky). **Z nedbalosti** (smazání dat omylem, fyzické poškození prvku ICT – překopnutí kabeláže, jiná chyba uživatele) (Kolouch et al., 2019).

- Technické chyby – *„chyba softwaru a hardwaru“* (Kolouch et al., 2019, s.77).
- Vyšší moc – *„neplánovaný výpadek napájení, přírodní události, katastrofy“* (Kolouch et al., 2019, s.77).

- **Zdroje působení***:*
  - *„vnitřní a vnější hrozby“* (Kolouch et al., 2019, s.77).
- **Cíle hrozby:**
  - Útok na triádu CIA – Confidentiality (důvěrnost), Integrity (celistvost), Availability (dostupnost) (Kolouch et al., 2019).

Obrázek 1 – Triáda CIA (Čermák, 2008)

  - Útok na některý z prvků kybernetické bezpečnosti – lidé (útoky sociálního inženýrství), technologie (hrozby působící na HW, SW, databáze, síť, informace a data uložená v počítačových systémech) a procesy (nekompetentní testování zabezpečení či funkčnosti procesů) (Kolouch et al., 2019).

- **Motivace:**
  - finanční zisk;

- zisk konkurenční převahy;
- dokázaní svých schopností;
- odplata;
- neplnění povinností (Kolouch et al., 2019).

- **Typy hrozeb:**
  - *„sociální inženýrství,*
  - *botnet,*
  - *malware,*
  - *ransomware,*
  - *spam/scam,*
  - *podvodné nabídky,*
  - *phishing,*
  - *pharming,*
  - *spear phishing,*
  - *vishing,*
  - *smishing,*
  - *hacking,*
  - *sniffing,*
  - *DoS, DDoS, DRDoS útoky,*
  - *šíření závadového obsahu,*
  - *kyberterorismus,*
  - *kybernetické výpalné či vydírání"* (Kolouch et al., 2019, s. 79).

Kybernetické riziko *je „riziko způsobené kybernetickou hrozbou"* (Doucek et al., 2019, s. 17).

Kybernetický incident je kybernetická událost, při níž dojde ke ztrátě informační bezpečnosti, narušení kybernetické bezpečnosti a která může mít dopad na aktivitu

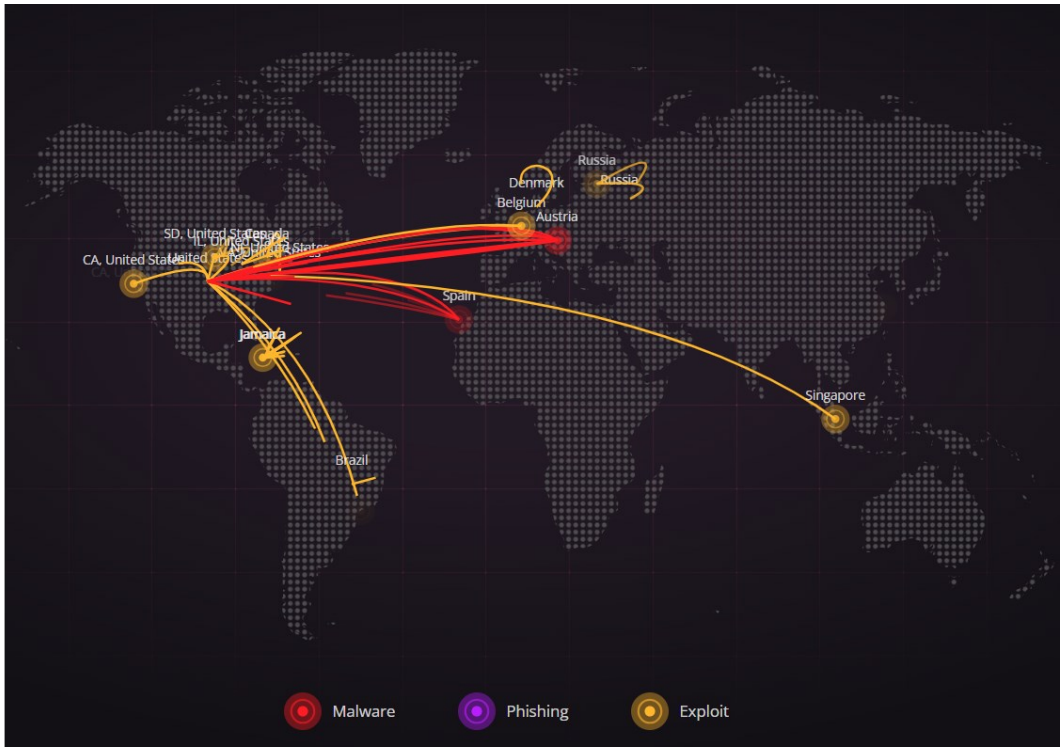
organizace. Rozlišuje se hned několik typů kybernetických bezpečnostních incidentů, jedná se zejména o:

- **Závady v systému nebo jeho špatná funkcionalita** – situace vznikne, pokud napadený systém nebo počítačová síť způsobí škodu systému třetí strany
  nebo poškodí systém dodavatele služeb, což má dopad i na ostatní činnosti v kyberprostoru (Doucek et al., 2019).
- **Prolomení ochrany důvěrnosti dat** – situace vznikne, pokud uložená data v systému jsou odcizena. Může k tomu dojít i v případě, kdy je systém spravován třetí stranou (Doucek et al., 2019).
- **Byla ztracena dostupnost dat nebo byla porušena jejich integrita** – k tomu dochází, pokud uložená data v systému byla poškozena nebo smazána, obdobně jako tomu je v předchozím bodě, i tato situace může vzniknout v případě, kdy je systém spravován třetí osobou (Doucek et al., 2019).
- **Poškozující aktivita** – jedná se o zneužití technologií za účelem způsobit poškození (kyberšikana na sociálních sítích, snaha o získání přístupu k datům s úmyslem je smazat) (Doucek et al., 2019).
- **Lidská chyba** – jedná se o situaci, kdy člověk neúmyslně poškodí systém, počítačovou síť (Doucek et al., 2019).

Kybernetický prostor je prostor, který je složený z internetu a dalších počítačových sítí, dále je složen z digitálních zařízení a systémů, služeb a procesů, které na nich probíhají. Umožňuje tím propojení globální infrastruktury mezi široké spektrum jak osobních, tak i podnikatelských a správních aktivit. Tento prostor lze chápat i jako veřejný, to znamená, že prostor nikdo nevlastní (žádný úřad, ani osoba, případně stát). Proto by měla být jeho bezpečnost koordinována a řízena různými subjekty na různých úrovních. Subjekty by měly mezi sebou spolupracovat na předávání si informací o rizicích a společně se připravovat na opatření proti bezpečnostním incidentům, které by je mohly ohrozit či poškodit (Collins, 2013, Doucek et al., 2019).

Kybernetický prostor má několik základních charakteristik:

- **Anonymita –** identita uživatele pohybující se v kyberprostoru není jasně prokazatelná.
- **Asymetričnost** – činnosti v kybernetickém prostoru bez ohledu na význam a důvěryhodnost uživatele, mohou mít významný dopad na ostatní uživatele sítě.
- **Neexistence hranic** – v kyberprostoru nejsou aktivity uživatelů omezovány žádným právním systémem, kulturou či jinou suverenitou.
- **Okamžitost –** každá akce provedená v kyberprostoru může mít okamžitý negativní dopad na celý svět.
- **Volný vstup i ukončení pobytu v něm** – každý může do prostoru kdykoli vstoupit i jej kdykoli opustit a ukončit tak svou aktivitu.
- **Interakce** – činnosti vytvářené uživateli mohou pomáhat získávat znalosti, ale i významně ovlivnit ostatní uživatele (Doucek et al., 2019).



Obrázek 2 – Mapa kybernetických útoků v reálném čase (Live Cyber Threat Map, @2024)

Na Obrázek 2 – Mapa kybernetických útoků v reálném čase (Live Cyber Threat Map, @2024) lze vidět kybernetické útoky v kyberprostoru v reálném čase, tedy ze dne 15. 3.2024.

Kybernetický útok zákon o kybernetické bezpečnosti nedefinuje. Nicméně se termín používá ve spojení s útoky, které jsou vedeny na hodnoty ve virtuálním prostředí *„za účelem narušení, znepřístupnění, zničení či ovládnutí počítačového prostředí či infrastruktury nebo zničení integrity dat či odcizení kontrolovaných informací“* i ve spojení s útoky, které využívají informační či komunikační technologie (Ramešová, 2023, s. 110).

1.3 Právní rámec v oblasti kybernetické bezpečnosti

Kybernetickou bezpečnost řeší celá řada právních zákonů, vyhlášek a směrnic.

1.3.1 Zákony a vyhlášky

Mezi základní normy řešící tuto oblast se řadí:

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

Tento zákon, o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZKB“), upravuje práva a povinnosti osob, působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zpracovává příslušný předpis Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. Zákon dále definuje systém zajištění kybernetické bezpečnosti, kde jsou charakterizována bezpečnostní opatření, kybernetická bezpečnostní událost a incident a hlášení takového incidentu. Hlavní cíle zákona jsou: stanovení základní úrovně bezpečnostních opatření, zlepšení detekce kybernetických bezpečnostních incidentů, zavedení hlášení kybernetických incidentů, zavedení systému opatření k reakci na kybernetické bezpečnostní incidenty a upravení činnosti dohledových pracovišť. Mezi důvody přijetí tohoto zákona se řadí jednak nárůst projevů terorismu, a to i kyberterorismu, a rostoucí závislost subjektů na fungování informačních technologií (Česko, 2014a; Legislativa KB, @2023; Smejkal, 2018).

- Na tento zákon navazuje **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).** *„Vyhláška zapracovává příslušný předpis Evropské unie (dále jen „EU“) – Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Vyhláška upravuje: obsah a strukturu*

bezpečnostní dokumentace; obsah a rozsah bezpečnostních opatření; 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; způsob likvidace dat, provozních údajů, informací a jejich kopií" (Česko, 2018).

- Další vyhláška navazující na tento zákon je **vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.** *„Touto vyhláškou se stanoví významné informační systémy a jejich určující kritéria. Informační systém je systém, jehož správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný při výkonu působnosti orgánu veřejné moci k zajištění: elektronické pošty; kontrolní nebo inspekční činnosti anebo státního dozoru; výkonu veřejné moci při přípravě na krizové situace a jejich řešení; výkonu spisové služby; mezinárodní spolupráce nebo zadávání veřejných zakázek. Určujícím kritériem je skutečnost, že narušení bezpečnosti informací v informačním systému by mohlo způsobit: omezení či narušení poskytování služeb nebo informací orgánem veřejné moci veřejnosti; omezení či narušení hospodaření orgánu veřejné moci; jiné omezení či narušení fungování orgánu veřejné moci; Zásah do osobního života nebo do práv fyzických nebo právnických osob postihující nejméně 50 000 osob; ohrožení či narušení veřejného zájmu a toto omezení nebude možné odvrátit bez vynaložených nepřiměřených nákladů*" (Česko, 2014b).

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

  Zákon obsahuje zásady pro stanovení utajovaných informací a přístup k nim, další požadavky na jejich ochranu, zásady a podmínky pro stanovení citlivých činností

  a s tím spojený výkon státní správy. První část zákona definuje základní pojmy jako jsou například utajovaná informace; zájmy České republiky (dále jen „ČR") (např.: zachování její svrchovanosti, územní celistvosti, zajištění vnitřního pořádku a bezpečnosti apod.); odpovědná osoba (např.: u ministerstva ministr,

u Bezpečnostní informační služby ředitel, u České národní banky guvernér apod.); cizí moc; neoprávněná osoba. Druhá část se zabývá ochranou utajovaných zpráv, kde je definována újma zájmu ČR či nevýhodnost pro zájmy ČR; stupně utajení – přísně tajné, tajné, důvěrné a vyhrazené; druhy zajištění ochrany utajovaných informací (např.: personální, průmyslovou, administrativní, fyzickou bezpečností a kryptografickou ochranou). Třetí část se zabývá bezpečnostní způsobilostí, kdy zákon definuje citlivost; bezúhonnost; osobnostní způsobilost; spolehlivost; povinnosti fyzické osoby, právnické osoby, podnikající fyzické osoby a orgánu státu. Čtvrtá část se zabývá obecnými zásadami bezpečnostního řízení; účastníky a průběhem řízení. Pátá část vymezuje výkon státní správy; práva a povinnosti úřadu, národního úřadu pro kybernetickou a informační bezpečnost, zpravodajských služeb, ministerstva vnitra a policie. Šestá a sedmá část se zabývá kontrolou činností, osmá část se zabývá přestupky a v poslední části jsou uvedena přechodná a závěrečná ustanovení (Česko, 2005).

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

Tento zákon zapracovává příslušný předpis EU – Směrnice Evropského parlamentu a Rady (EU) 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a přímo navazuje na předpis EU – Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Zákon obsahuje: zpracování osobních údajů; ochranu osobních údajů při jejich zpracování za účelem předcházení, vyhledávání či odhalování trestné činnosti a při zajišťování bezpečnosti ČR, veřejného pořádku a vnitřní bezpečnosti. Dále pojednává o ochraně osobních údajů při zajišťování obranných a bezpečnostních zájmů ČR; úřadu; přestupcích; poslední část obsahuje přechodná, zrušovací a závěrečná ustanovení (Česko, 2019).

1.3.2 Normy

Česká agentura pro standardizaci je státní příspěvková organizace zřízena Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví (dále jen „ÚNMZ“) dle zákona

č. 265/2017 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

Od 1.1.2018 Česká agentura pro standardizaci převzala veškerou činnost související s tvorbou, vydáváním a distribucí technických norem od ÚNMZ (Agentura, © 2024).

Internationa Organization for Standardization zkráceně ISO, je mezinárodní organizace pro normalizaci se sídlem v Ženevě. Jedná se o nezávislou a celosvětově působící nevládní organizaci založenou v roce 1947, kdy jejím cílem je vytvářet a zveřejňovat mezinárodní normy. Normy ISO jsou mezinárodně uznávané standardy, které slouží pro zvyšování kvality a bezpečnosti výrobků a služeb a mimo jiné usnadňují jejich výměnu mezi zeměmi a společnostmi. Mimo to si normalizace klade za cíl podporovat spolupráci mezi institucemi a společnostmi v oblasti obchodu, techniky a vědy (Droege, 2022).

Za normalizaci bezpečnosti informací je odpovědnost svěřena podkomisi JTC1/SC27 – bezpečnostní techniky IT. V roce 2005 ISO oznámila zavedení nové řady norem ISO 27000, která se zaměřuje na problematiku řízení bezpečnosti informací. Tato norma vychází z principu PDCA (plánuj, dělej, kontroluj, jednej) (Doucek et al., 2019).

Základní normy ISO/IEC 27000:

- **ČSN ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník**

  „Tato norma poskytuje přehled systému řízení bezpečnosti informací, které tvoří předmět rodiny norem ISMS a definuje související termíny. Termíny a definice uvedené v této normě se týkají termínů a definic obecně použitých v rodině norem ISMS, nikoliv všech termínů a definic“ (Sedlák a Konečný, 2023, s.56).

- **ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky**

  Tato norma je více zaměřená na praktické řízení rizik, informační bezpečnosti, kybernetické bezpečnosti a ochrany osobních údajů oproti normě předchozí. Tato norma definuje požadavky na systém řízení. V hlavní části jsou specifikovány požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování zdokumentovaného systému managementu informační bezpečnosti (Sedlák a Konečný, 2023).

- **ČSN ISO/IEC 27002 Bezpečnost informací – kybernetická bezpečnost – ochrana soukromí – opatření bezpečnosti informací**

Nová norma, která změnila název definuje bezpečnostní opatření, proti kterým se ověřuje funkčnost zavedené normy ISO/IEC 27001. V této normě došlo ke změně struktury, opatření jsou prezentována pomocí jednoduché taxonomie a souvisejících atributů. Některá opatření byla sloučena, jiná odstraněna a bylo zavedeno několik nových opatření (Sedlák a Konečný, 2023).

- **ČSN ISO/IEC 27003 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny**

Norma představuje pokyny k požadavkům na systém řízení bezpečnosti informací (ISMS), jak je specifikován v normě ČSN ISO/IEC 27001. Dále poskytuje doporučení („měl by“), možnosti („může“) a oprávnění („smí“) ve vztahu k nim. Cílem této normy není poskytnout obecné pokyny týkající se všech aspektů bezpečnosti informací, ale představuje obecný dokument, který má být použitelný pro všechny organizace bez ohledu na typ, velikost nebo povahu. Každá organizace si sama určí, které části této normy se na ní v souladu s jejím specifickým organizačním kontextem vztahují (Sedlák a Konečný, 2023).

- **ČSN ISO/IEC 27004 Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení**

Norma stanovuje monitorování a měření výkonnosti informační bezpečnosti, monitorování a měření efektivnosti systému řízení informační bezpečnosti zahrnující jeho procesy, opatření, analýzu a hodnocení výsledků monitorování a měření (Sedlák a Konečný, 2023).

- **ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací**

Norma nabízí doporučení pro řízení rizik bezpečnosti informací v rámci organizace, podporuje obecné koncepty upřesněné v ČSN ISO/IEC 27001 a v ČSN ISO/IEC 27002 a je strukturovaná tak, aby dostatečně podporovala implementaci informační bezpečnosti založené na přístupu řízení rizik. Tento typ dokumentu mohou použít všechny typy organizací (například komerční organizace, vládní úřady, neziskové

organizace), které chtějí řídit rizika, které mohou kompromitovat bezpečnost informací organizace (Sedlák a Konečný, 2023).

- **ČSN ISO/IEC 27006 Informační technologie – Bezpečnostní techniky – požadavky na orgány provádějící audit a certifikaci systému řízení bezpečnosti informací**

Hlavním úkolem této normy je umožnit akreditačním orgánům její použití a harmonizace s ostatními normami, dle kterých se provádějí hodnocení certifikačních orgánů usilujících o akreditaci a nastavuje kritéria pro organizace, které se zabývají auditem a certifikací systému řízení (Sedlák a Konečný, 2023).

- **ČSN ISO/IEC 27007 Informační technologie – kybernetická bezpečnost a ochrana soukromí – směrnice pro audit systému řízení bezpečnosti informací**

Audit lze provádět na základě řady kritérií, samostatně nebo v kombinaci. Tato norma nabízí pokyny pro všechny velikosti a typy organizací a audity ISMS různých předmětů a rozsahů, včetně těch, které provádějí velké auditorské týmy, většinou větších organizací. Takové pokyny by měly být přizpůsobeny dle předmětu, složitosti a rozsahu programu auditu ISMS (Sedlák a Konečný, 2023).

- **ČSN ISO/IEC 27009 Informační technologie – Kybernetická bezpečnost a ochrana soukromí – Použití ISO/IEC 27001 v jednotlivých odvětvích – Požadavky**

Norma, která specifikuje požadavky na vytvoření norem specifických pro jednotlivá odvětví, které rozšiřují ISO/IEC 27001 a doplňují nebo pozměňují ISO/IEC 27002 tak, aby podporovaly konkrétní odvětví (obor, oblast použití či trh) (Sedlák a Konečný, 2023).

- **ČSN ISO/IEC 27032 Informační technologie – Bezpečnostní techniky – Směrnice pro kybernetickou bezpečnost**

Norma zahrnuje doporučení ve vztahu k bezpečnosti v kyberprostoru. Zahrnuje základní bezpečnostní postupy pro oblasti jako jsou bezpečnost informací, sítí, internetu či ochrana kritické informační infrastruktury. Dále poskytuje doporučení pro efektivní sdílení informací a koordinaci řízení incidentů mezi organizacemi, uživateli, vládami nebo poskytovateli služeb. Norma se zabývá klíčovými hrozbami

nacházející se v kyberprostoru jako je sociální inženýrství, malware, odcizení identity apod. (Sedlák a Konečný, 2023).

1.3.3 Směrnice NIS II

Směrnice NIS II představuje základ kybernetické bezpečnosti v Evropě. K publikaci oficiálního znění směrnice došlo dne 27. prosince 2022 v Úředním věstníku Evropské unie. Dvacátým dnem od vyvěšení se stává směrnice platnou – toto datum tedy připadá na 16. ledna 2023. Směrnice určuje nová pravidla při řešení kybernetické bezpečnosti uvnitř organizací. Platnost však neznamená, že subjekty spadající do její působnosti musí ihned začít plnit všechny povinnosti, které přináší. Udává povinnost členskému státu převést text směrnice do národního práva. Lhůta, ve které musí členské státy platnou směrnici promítnout do národního práva, je stanovena na 21 měsíců. Tedy ČR musí implementovat tuto směrnici formou novelizace zákona o kybernetické bezpečnosti, do 18. října 2024. Nová směrnice rozšiřuje okruh povinných osob v oblasti kybernetické bezpečnosti a dotkne se více než 6000 firem a organizací v Česku, na Slovensku pak 3000 a bude mít zásadní vliv na jejich fungování. Zavádí totiž řadu pravidel pro zajištění bezpečnosti jejich kyberprostoru proti hackerským útokům (Donát et al., 2022; Obecné informace o směrnici NIS II a budoucí národní úpravě, @2024; Vše o NIS 2, @2024).

Kybernetické útoky jsou dnes již běžnou realitou a mohou vážně narušit nejen soukromé subjekty, ale i kritickou infrastrukturu kteréhokoli státu. Staly se součástí válečných konfliktů, slouží jako nástroj teroristů a jsou používány k manipulaci. Proto se EU rozhodla posílit regulaci, aby zvýšila celkovou úroveň odolnosti vůči kybernetickým hrozbám v Evropě. EU zavádí řadu pravidel pro zajištění bezpečnosti a odolnosti kyberprostoru proti hackerským útokům. Pravidla mají zaručit lepší schopnost reagovat na případné incidenty. Nejde o nic nového, NIS II rozšíří působnost již existující a platné směrnice NIS, která se ale díky stále rychlejší digitální transformaci ukázala být nedostačující (Donát et al., 2022; Vše o NIS 2, @2024).

Nově bude mít právní úprava dopad na poskytovatele IT služeb, výrobní podniky, poštovní a kurýrní služby nebo organizace působící v oblasti výzkumu. V odvětvích, na která už stávající právní úprava dopadá, pak dojde k rozšíření okruhu povinných osob – například v energetice budou nově regulováni obchodníci s plynem a elektřinou (Donát et al., 2022). Původní směrnice NIS se týkala jen provozovatelů takzvaných základních a digitálních služeb, ve směrnici NIS II se ale subjekty nově dělí na **základní** a **důležité**. Do "základní"

skupiny byli při tom přeřazeni nejen původní provozovatelé základních služeb, ale i nové subjekty, mimo jiné státní správa. NIS II navíc přidává oproti původní směrnici ještě jedno kritérium – velikost firmy. Povinnými osobami dle směrnice budou až na výjimky pouze organizace dosahující alespoň velikosti středního podniku tedy s minimálně 50 zaměstnanci a 10 miliony eur obratu, což je zhruba 250 miliónů Kč. Mezi subjekty základního významu (s přísnějšími povinnostmi) spadají subjekty v odvětví dopravy, zdravotnictví, digitální infrastruktury, veřejné správy či v odvětvích energetiky a IT služeb. Mezi důležité subjekty (s mírnějšími povinnostmi) řadíme subjekty poštovní a kurýrní služby, nakládání s odpady, chemického, potravinářského a vybraných oblastí zpracovatelského průmyslu. Působnost směrnice se nebude vztahovat na orgány veřejné správy v oblasti národní a veřejné bezpečnosti, obrany, vymáhání práva (zejm. vyšetřování trestných činů), soudní moc, parlamenty a národní banky, avšak tyto subjekty mohou být zahrnuty v působnosti národní právní úpravy (Donát et al., 2022; Vše o NIS 2, @2024).

1.4 Kybernetická bezpečnost v České republice

Pro oblast kybernetické bezpečnosti v České republice je od roku 2015 účinný zákon 181/2014 Sb. o kybernetické bezpečnosti. V roce 2018 nabývá účinnosti Obecné nařízení na ochranu osobních údajů – GDPR (General Data Protection Regulation), který nahrazuje zákon č. 101/2000 Sb. o ochraně osobních údajů.

V roce 2017 byl zřízen Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“), kterým je správním úřadem pro kybernetickou bezpečnost, ochranu utajovaných informací pro oblast informačních a komunikačních systémů, kryptografickou ochranu a problematiku veřejně regulované služby navigačního systému Galileo. Pro kybernetickou bezpečnost v ČR jsou důležité volně dostupné materiály na stránkách NÚKIB. Jedná se zejména o aktuální Národní strategii kybernetické bezpečnosti ČR a Akčního plánu k této strategii (Sedlák, Konečný a kol., 2022)

1.4.1 Národní strategie kybernetické bezpečnosti České republiky na období let 2021 až 2025

Česká republika zavedla efektivní model spolupráce na národní i mezinárodní úrovni v oblasti kybernetické bezpečnosti, v němž jsou jasně stanovené povinnosti a pravomoci každého subjektu. Na základě toho se kybernetická bezpečnost stala v posledních letech důležitým předmětem zahraniční politiky. Hlavními cílovými skupinami jsou bezpečnostní

orgány a subjekty veřejné správy, přičemž strategie se snaží informovat i širší společnost o opatřeních v boji proti kybernetickým hrozbám. Úkolem je poskytnout spolehlivé a bezpečné využívání kyberprostoru a moderních technologií pro celou společnost. Strategie respektuje logický rámec přípravy veřejných strategií a je strukturována do tří hlavních vizí (Národní strategie kybernetické bezpečnosti České republiky, 2020):

- ***Sebevědomě v kyberprostoru*** *– „společný přístup ke kybernetické bezpečnosti; bezpečná infrastruktura; účinná strategická komunikace; sebevědomá reakce; budoucí výzvy“* (Sedlák, Konečný a kol., 2022, s. 44).
- ***Silná a spolehlivá spojenectví*** *– „efektivní mezinárodní spolupráce; prohlubování a tvorba aktivních spojenectví; mezinárodní právní rámec; schopnost a expertíza“* (Sedlák, Konečný a kol., 2022, s. 44).
- ***Odolná společnost 4.0.*** *– „zabezpečení digitální společnosti a veřejné správy; vzdělávání a osvěta; rozšiřování expertní základy“* (Sedlák, Konečný a kol., 2022, s. 44).

V první vizi je důležitým prvkem zajišťování kybernetické bezpečnosti v ČR. Druhá vize je založena směřování k mezinárodní spolupráci, na základě čehož dochází k posílení společné bezpečnosti a obranyschopnosti. V poslední vizi se objevují nové pojmy:

- **Odolná společnost 4.0** – jedná se o společnost naplno využívající výhody moderních technologií s minimalizací kybernetických rizik.
- **Digitální hygiena** – sada pravidel, postupů a návyků, které umožňují uživatelům bezpečné operace ve virtuálním prostředí.
- **Odolný systém zajištění kybernetické bezpečnosti –** experti na kybernetickou bezpečnost; pracovníci v oblasti národní bezpečnosti; pracovníci veřejného sektoru a společnost (Sedlák, Konečný a kol., 2022).

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

K naplnění a dosažení hlavních cílů Národní strategie kybernetické bezpečnosti je zapotřebí realizovat a úspěšně naplňovat úkoly uvedené v tomto plánu. Pro splnění stanovených úkolů je nezbytná aktivní spolupráce orgánů a osob povinných podle zákona č. 181/2014 Sb.,

o kybernetické bezpečnosti a souvisejících předpisů, a dalších subjektů veřejné správy ČR v koordinaci a dle potřeb uvedeného odpovědného subjektu. Pro naplnění vytyčených cílů, vyplývající z Národní strategii kybernetické bezpečnosti, jsou v tomto plánu vytyčeny jednotlivé úkoly. Ke každému úkolu je přiřazen kód, odpovědný subjekt (např: NÚKIB, MV, MO, MZV, AČR apod.) a časový rámec, do kdy má být zadaný úkol splněn (Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025, 2021).

2 VYBRANÉ KYBERNETICKÉ HROZBY

Kybernetické hrozby představují pro jednotlivce, organizace či firmy různá rizika vyplývající ze zneužití informačních a komunikačních technologií. Motivů útočníka je hned několik, mezi ně patří zejména zisk finančních prostředků či jiných cenných informací jako jsou například osobní údaje nebo soukromá data. Útočníci často používají vydírání jako nástroj ke získání finančního prospěchu při návratu dat. Dalšími motivy mohou být poškození pověsti, vyřizování účtů, aktivismus nebo politické cíle (Králová, 2023).

2.1 Malware

Známý jako „škodlivý software“, který poškozuje či deaktivuje počítač, jeho systémy, poškozuje tablety nebo mobilní zařízení za pomoci převzetí částečné kontroly nad operacemi zařízení. Malware nepoškozuje fyzicky hardware, ale může ukrást nebo smazat data, dále špehovat uživatele zařízení bez jeho vědomí a svolení.

Pro nezkušené „oko“ je velmi složité odhalit škodlivé soubory. Nicméně je lze odhalit různými způsoby. Například může docházet ke zpomalení zařízení, kdy jedním z vedlejších účinků malwaru je snížení rychlosti operačního systému. Dalším možným identifikátorem může být stav, kdy je obrazovka zaplavena otravnými reklamami, neočekávané vyskakovací reklamy. Jedná se zejména o adware. Může mít podobu textové zprávy například „Blahopřejeme, vyhráli jste poukázku do Disneyland!“ Dalším rozeznávacím faktorem může být stav, kdy antivirový produkt přestane fungovat nebo jej nelze znovu zapnout. Existuje zde i možnost, že uživatel ztratí přístup ke svým souborům nebo celému zařízení, tento stav je důsledkem infekce ransomware.

Dva způsoby, kterými se malware dostává do systému, tedy počítače, jsou internet a e-mail. Tedy kdykoli, kdy je uživatel připojen do online světa, je zranitelný (Malware, @2024; What is malware? @2024).

Mezi základní typy malwaru řadíme spyware, adware, červy, trojské koně, ransomware apod.

2.1.1 Spyware

Spyware je obtížně odhalitelný, protože se instaluje na pozadí a v systému se chová nenápadně. Maskuje svou činnost za důvěryhodně vypadající procesy. Uživatel může zjistit jeho přítomnost až v okamžiku, kdy se spyware aktivuje a začne provádět podezřelou

činnost. Uživatel může zaznamenat zpomalení internetového připojení, pozorovat neobvyklý provoz v síti nebo identifikovat podezřelý software v seznamu běžících procesů.

Útočníci k útoku využívají koordinovanou síť kompromitovaných zařízení (tzv. botnet síť, která je tvořena ze „zombie“ počítačů). S pomocí řídících serverů (C&C = Command and Control) odesílají přes botnet nevyžádané požadavky v řádu až terabitů za sekundu. Jejich cílem je zaměřit se na síťové prvky systému internetového připojení, které jsou nezbytné k navázání internetového připojení (např. routery), webové stránky, servery či databáze. Snaží se o přetížení těchto systémů (Spyware, @2024).

Existuje několik typů spywaru, jedná se například o:

- **Infostealer** – jedná se o škodlivý špionážní software, jehož hlavním cílem je krádež osobních a citlivých informací ze zařízení oběti. Tyto informace mohou zahrnovat bankovní údaje nebo přihlašovací informace k online účtům. Infostealer, který je zaměřený na hesla, označujeme jako password stealer. Infostealery jsou navrženy tak, aby byly co nejméně nápadné a často se šíří prostřednictvím e-mailů nebo webových stránek, které vypadají důvěryhodně. Zároveň má v uživateli vyvolat pocit naléhavosti a přimět ho otevřít infikovanou přílohu nebo odkaz. Což následně spustí instalaci škodlivého kódu. Jakmile se infostealer dostane do systému, začne sbírat informace a odesílat je zpět útočníkům. Získané informace mohou být použity pro různé škodlivé účely jako jsou krádež identity, podvody s kreditními kartami nebo dokonce vydírání. Infostealery představují jednu z nejnebezpečnějších forem malwaru, protože dokáží odcizit obrovské množství citlivých informací bez povšimnutí uživatele (Infostealer, @2024).
- **Keylogger –** je druh škodlivého softwaru z kategorie infostealerů. který je schopen bez vědomí uživatele zaznamenávat stisky kláves, a tak odcizit jeho citlivé údaje. Kromě softwarových keyloggerů existují také hardwarové. V těchto případech se jedná o fyzická zařízení, která se připojují mezi počítač a klávesnici (Keylogger, @2024).
- **Browser hijacker** – „*dokáže změnit výchozí nastavení prohlížeče, a sledovat historii prohlížení“* (Spyware, @2024).
- **Banking trojan** – je typ malwaru, který krade přihlašovací údaje do online bankovnictví, například pomocí keyloggingu (zaznamenávání stisknutých kláves)

nebo pomocí překrytí obrazovky skutečné bankovní aplikace vrstvou podvodné aplikace (Spyware, @2024).

- **Fake spyware removal tool** – je software tvářící se jako nástroj na odstranění spywaru, ale ve skutečnosti sám instaluje spyware (Spyware, @2024).

2.1.2 Ransomware

Ransomware je forma malwaru, kterým kyberzločinci infikují počítače nebo sítě. Ransomware zablokuje přístup k systému nebo zašifruje jeho data. Útočníci poté požadují od svých obětí výkupné pro obnovení přístupu k datům. Odtud pochází název ransomware – výkupné. Ti mají tři možnosti, a to zaplatit výkupné (nejčastěji v kryptoměně), pokusit se malware odstranit nebo restartovat své zařízení.

Asi nejznámější ransomware útok, který se stal v ČR je útok na Benešovskou nemocnici v roce 2019. Výsledkem tohoto útoku bylo zašifrování důležitých dat v počítačích nemocnice. Mimo výkupného utrpěla nemocnice další ztráty včetně omezení provozu lékařských výkonů, ztráty finančních prostředků od zdravotních pojišťoven na vyšetření a operace a také ztráty transfuzní stanice v důsledku omezení výroby a prodeje krevních derivátů. Nemocnice byla nucena investovat značné finanční prostředky do nového bezpečnostního systému, reinstalace softwaru a obnovy systémů včetně zaškolení personálu. Celková škoda byla vyčíslena na více než 59 milionů korun. Kriminalistům Středočeského kraje se nepodařilo pachatele vypátrat (Dubovecká, 2024).

Často k útokům dochází prostřednictvím phishingu či spearphishingu. V obou případech přijde oběti podvodný e-mail, který obsahuje zavirovanou přílohu (např. spustitelný soubor s koncovkou .exe) nebo odkaz na zavirovanou stránku. V současné době jsou častým cílem útoků velké firmy nebo veřejné instituce. Důvodem může být tlak ze strany veřejnosti na co nejrychlejší obnovení služeb. Tím dávají útočníkům vyšší šanci na zaplacení výkupného (Vyděračské útoky ransomwarem jsou čím dál cílenější, 2020).

2.1.3 Adware

Jedná se o další typ malwaru, který může infikovat počítač nebo mobilní telefon. Tento typ malwaru může zobrazovat „otravné“ reklamy nebo sledovat internetovou aktivitu uživatele. To umožňuje adware lépe cílit obsah vyskakovacích oken. Adware vzniklo zkrácením slov „**ad**vertising-supported soft**ware**“ (software podporující reklamu). Sám o sobě bývá adware většinou neškodný, nicméně může odkazovat na phishingové

stránky nebo stránky šířící malware. Často stahuje další reklamní obsah do zařízení, což může způsobit uživateli zahlcení reklamou a tím mu výrazně snížit pohodlí při práci či surfování online. Adware představuje nebezpečí, pokud sleduje uživatele obdobně jako spyware, nebo odkazuje na další škodlivý kód (Adware, @2024).

Adware i spyware jsou oba typy škodlivého softwaru, nicméně adware se obvykle instaluje s vědomím a souhlasem uživatele, oproti spyware, který je instalován bez vědomí a souhlasu uživatele. Adware se zaměřuje převážně na zobrazování reklam a může také sledovat internetovou aktivitu uživatele za účelem cílení reklam. Spyware sbírá tajné informace o uživateli, jako jsou hesla, osobní údaje a odesílá je útočníkům. Celkově lze říci, že spyware je většinou nebezpečnější a škodlivější než adware, neboť krade citlivé údaje od uživatelů (Adware, @2024).

2.1.4 Počítačový vir

Počítačový virus je druh malwaru, který se připojuje k jiným programům, například k dokumentům, a může se kopírovat a šířit poté, co jej uživatel poprvé spustí v systému. Například uživatel může obdržet e-mail se škodlivou přílohou, kterou otevře a virus se poté spustí na jeho počítači. Viry mohou být skryty v přílohách, které se tváří jako vtipné obrázky, pohlednice, zvukové nebo video soubory. Šíření počítačových virů může také nastat při stahování souborů z internetu. Mohou poškodit data, zpomalit systém či zaznamenávat stisknuté klávesy. Viry pro své šíření potřebují akci ze strany uživatele, nikdy se nebudou šířit bez akce. Počítačový virus vyžaduje hostitelský program, dále vyžaduje pro přenos z jednoho systému do druhého akci uživatele a připojuje kousky svého škodlivého kódu k jiným souborům nebo soubory přímo nahrazuje svými kopiemi (Prevence a odstranění virů a jiného malwaru, @2024; What is computer virus?, @2024,).

2.1.5 Počítačový červ

Počítačový červ představuje program obsahující škodlivý kód, který útočí na hostitelské počítače a šíří se dál skrze sítě. Tím se liší od virů, protože červ se dokáže šířit sám a není závislý na hostitelském souboru. Červ ke svému šíření využívá hlavně elektronickou poštu. Červ se šíří automaticky díky chybám v zabezpečení e-mailových pošt, sítě nebo operačního systému. A často zaplavují systém dříve, než se objeví skutečná příčina. Červ bývá daleko nebezpečnější než jiné formy škodlivého kódu díky rychlému šíření přes internet. Při podezření na nákazu červem se doporučuje infikovaný soubor okamžitě odstranit,

aby nedocházelo k dalším škodám (Červ, @2024; Prevence a odstranění virů a jiného malwaru, @2024).

2.1.6 Trojský kůň

Zkráceně „trojan“, je typ škodlivého kódu, který se maskuje uvnitř jiných programů. Tváří se jako užitečná aplikace nebo aktualizace. Na rozdíl od viru se nedokáže sám šířit ani infikovat další soubory. Do zařízení obětí se často dostává za pomoci technik sociálního inženýrství, například s užitečně vypadajícím programem nebo prostřednictvím e-mailových příloh. Útočníci různými způsoby maskují a zakrývají škodlivý kód a tím se snaží zamaskovat jeho skutečnou funkci. Pachatelé často kód vkládají do jiných souborů nebo programů, které na první pohled vypadají legitimně. Uživatelé pak škodlivý kód spouští v dobré víře. Jakmile je zařízení infikováno, dochází ke škodám dle naprogramování kódu. Trojské koně se využívají k převzetí kontroly nad napadeným zařízením, k získání uživatelských dat a jejich odeslání útočníkovi, stažení a spuštění jiného škodlivého softwaru v napadeném systému a provádění mnoha dalších nekalých činností (Šulc, 2018; Trojský kůň, @2024; What is a Trojan horse?, @2024).

Trojský kůň se může do počítače dostat několika způsoby. Například stažením cracknutých aplikací; z neznámých bezplatných programů (jako je bezplatná hra); otevírání příloh, které mohou být infikované nebo návštěva stinných stránek (What is a Trojan horse?, @2024).

2.1.7 Exploit

Exploit představuje formu škodlivého kódu, který využívá chyb nebo zranitelností v systému k dosažení neočekávaného nebo nežádoucího chování počítače. Útoky představují hrozbu převzetí kontroly nad celým počítačovým systémem, eskalaci oprávnění nebo vyřazení služeb (například útoky typu DDoS). Útočníci nejčastěji využívají exploit k vložení různých typů malwaru do systému (Exploit, @2024).

Zero-day exploit představuje nejnebezpečnější typ exploitu, který využívá zranitelnosti, jež nejsou známy vývojářům softwaru ani široké veřejnosti, pouze hackerovi. Termín „exploit“ je odvozen z anglického slovesa „to exploit“, což znamená „využít něco ve svůj prospěch“ (Exploit, @2024).

2.2 Sociální inženýrství

Útočníci využívají sociálního inženýrství k tomu, aby se vydávali za autoritu nebo zástupce známé instituce. V obětech se snaží vyvolat emoce jako je radost, strach případně stud pomocí lživých informací. A snaží se vyvíjet tlak na rychlou reakci. Tím z oběti vylákat citlivé informace, data nebo peníze. Většina technik často nevyžaduje žádné technické znalosti a může jej použít jak drobný zloděj, tak profesionální hacker. Osoba ovládající techniku sociálního inženýrství se nazývá sociotechnikem. Útoky sociálního inženýrství často zahrnují psychologickou manipulaci, která vede uživatele k předání důvěrných informací nebo citlivých dat pod vlivem vyvolaných emocí jako je strach nebo naléhavost. Útoky jsou často vedeny pomocí e-mailové zprávy, telefonátem, případně SMS zprávou, ojediněle útočník oběť osobně navštíví (Social Engineering: Definition & 6 Attack Types, 2023; Sociální inženýrství, @2024; Šulc, 2018).

2.2.1 Phishing

Slovo phishing pochází z anglického slova fishing neboli lov ryb. Lov ryb má představovat útočníka (lovec), který nadhodí háček s návnadou, v podobě výhodné nabídky, a čeká, zda se oběť (ryba) chytí. Ve slově fishing bylo zaměněno písmeno „f“ za „ph“, které vychází ze slova „phreaks“. Název „phreaks“ nesla hackerská skupina z USA, která ilegálně experimentovala s telekomunikačními systémy v devadesátých letech (Phishing, © 2024).

Phishing je typ kybernetického útoku techniky sociálního inženýrství, který využívá nejslabšího článku kybernetické bezpečnosti, tedy lidský zdroj. Útočník se snaží od obětí získat citlivá data nebo spouští škodlivý kód na zařízeních oběti. Nejčastěji phishingový útok probíhá za pomocí e-mailové zprávy, kdy útočník žádá oběť o informace k platební kartě nebo o přihlašovací údaje do internetovému bankovnictví (6 Common Phishing Attacks and How to Protect Against Them, 2023; Phishing, @2024).

Dříve byly phishingové útoky lehce odhalitelné z důvodu špatného používaní českého jazyka a odlišné domény v e-mailech. V posledních letech bývají e-maily sofistikovanější (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021).

Typy phishingových útoků:

- **Deceptive phishing –** je podvodný phishing, který se řadí mezi nejběžnější typy takového útoku. Útok spočívá v tom, že se podvodník vydává za legitimní společnost či odesílatele s cílem vylákat z oběti osobní data případně přihlašovací údaje.

E-maily mají vzbuzovat pocit naléhavosti, aby vyděsily uživatele a ti následně udělali to, co útočníci chtějí. Často jsou e-maily detekovány včas pro jejich gramatické a pravopisné chyby (6 Common Phishing Attacks and How to Protect Against Them, 2023).

- **Spear phishing –** při tomto útoku útočník předem získává veškeré dostupné informace o své cílové skupině nebo jednotlivci a následně vytvoří phishingovou zprávu přesně na míru. Podvodníci upravují své e-maily tak, aby příjemce přiměli k domněnce, že odesílatele znají, a proto mu mohou důvěřovat. Cílem je oběť přimět, aby klikla na škodlivou URL adresu nebo přílohu e-mailu, kde předá své osobní údaje. Mezi nejběžnější techniky používané při tomto typu útoků je ukládání škodlivých dokumentů v cloudových službách, jako jsou Dropbox, Disk Google. Phishingovým útokům pomáhá i umělá inteligence, která usnadňuje podvodníků získávat osobní údaje ze sociálních sítí uživatele. Ti pak mohou pomocí uniklých dat vytvářet cílené návnady (6 Common Phishing Attacks and How to Protect Against Them, 2023; Phishing, @2024).
- **Whaling –** je typ spear phisingu zaměřený na tzv. velké ryby, tedy na majitele firem, vrcholové manažery, vedoucí pracovníky. K útokům dochází zejména z důvodu neúčasti vysoce postavených osob ve společnosti na školeních v oblasti kybernetické bezpečnosti (6 Common Phishing Attacks and How to Protect Against Them, 2023; Phishing, @2024).
- **Vishing –** v tomto případě se již nejedná o podvodný e-mail, nýbrž o útok pomocí telefonního hovoru. Jedná se o tzv. voice phishing, kdy útočník může využívat předem namluvené a automaticky přehrávané zprávy, někdy vytvořené za pomocí generátorů, které převádí text na mluvené slovo. Telefonní čísla útočníků vypadají jako čísla skutečných institucí, za které se útočníci vydávají, tzv. "spoofing" (Phishing, @2024).
- **Smishing –** nebo také SMS phishing, je útok, kdy útočník zasílá podvodnou zprávu na mobilní telefon. Zpráva většinou obsahuje podvodné odkazy, které vyzývají ke kliknutí, nebo obsahuje telefonní číslo, popřípadě e-mail, přes který je oběť naváděna ke kontaktování instituce, za kterou se podvodníci vydávají (Phishing, @2024).

- **Page hijacking –** jedná se o formu phishingu, při níž jsou uživatelé nevědomky přesměrováni na podvodné webové stránky. Útočníci vytvářejí kopie existujících webových stránek a začnou tento web upřednostňovat před původním webem. Případně útočníci poškodí legitimní webové stránky, aby uživatele přesměrovali na ty škodlivé (Phishing, @2024).
- **Catfishing –** v tomto případě se jedná o podvodnou činnost, při které si útočník na internetu, zpravidla na sociálních sítích, vytváří falešnou identitu s cílem manipulovat s obětí, navazovat vztahy, provádět kyberšikanu nebo dosáhnout finančního zisku (Phishing, @2024).

2.2.2 Pharming

Jedná se o typ kybernetického útoku sociálního inženýrství, kdy útočník manipuluje s provozem webových stránek s cílem zmocnit se soukromých informací uživatelů nebo infikovat jejich počítače malwarem. Za tímto účelem útočníci vytvoří falešný web, který napodobuje cílovou webovou stránku, a pomocí několika metod přesměrují uživatele na falešný web. Kybernetičtí zločinci často vytvářejí podvodné repliky bankovních stránek za účelem shromažďovat citlivé údaje, jako jsou uživatelská jména, hesla, čísla sociálního zabezpečení a informace o platebních kartách. „*Pharming využívá výhod základů procházení internetu – konkrétně řady písmen, která tvoří internetovou adresu (xyz.example.com), aby připojení pokračovalo, musí být převedeno na IP adresu serverem DNS (systém názvů domén)“* (Co je Pharming?, 2021).

A jak se Pharming liší od phishingu? Přestože existují podobné požadované výsledky mezi pharmingem a phishingem, metody používané u obou se liší. Pharming se zaměřuje na útoky na systém DNS, zatímco phishing cílí hlavně na manipulaci samotných uživatelů. Nicméně phishing může hrát důležitou roli i při provádění pharmingu. Phishing je druh kybernetického podvodu, kdy útočníci používají e-maily, které předstírají, že pocházejí od důvěryhodných organizací, jako jsou banky nebo vydavatelé kreditních karet. Tyto e-maily obsahují škodlivé odkazy, pokud na ně oběť klikne, přesměruje ji to na falešné webové stránky. Na falešných stránkách jsou oběti podvedeny k zadání přihlašovacích údajů, údajů o kartě a dalších citlivých informací. Zatímco pharming lze vnímat jako formu phishingu bez nutnosti nalákat oběť. To znamená, že není třeba, aby oběť klikla na škodlivý odkaz. Místo toho je oběť okamžitě přesměrována na falešný web prostřednictvím falešného

záznamu DNS nebo záznamem hostitele. Pharming tak lze chápat jako "phishing bez návnady" (Co je Pharming?, 2021).

2.3 DoS a DDoS útoky

Kybernetický útok typu DoS: je útok, pomocí kterého lze omezit či vyřadit služby počítačových systémů. Jedná se buď o generování velkého množství podvržených požadavků s cílem přehltit systém nebo přenosovou cestu, nebo jde o sofistikovaný útok na slabá místa v cílovém systému nebo přenosové cestě (DoS / DDoS útoky, 2013).

Zkratka DDoS označuje „Distributed Denial of Service“ - „Distribuované odmítnutí služby“ a vystihuje cíl útočníků i způsob provedení útoku.

DDoS útok je druh kybernetického útoku, během kterého se útočníci snaží narušit či poškodit webovou stránku, síť nebo jinou online službu tím, že ji zahltí velkým množstvím falešných nebo nevyžádaných požadavků. Toto přetížení zapříčiní pokles výkonu, omezení nebo dokonce výpadek služby. Útok je prováděn prostřednictvím sítě infikovaných počítačů (tzv. „zombie“) z různých částí světa, tzv. distribuovanou botnet síť. Kvůli tomu není možné útok zastavit blokováním jednoho konkrétního zařízení (DDoS útok, @2024).

Botnet síť je rozsáhlá síť infikovaných zařízení, známých také jako "zombies", které jsou ovládány kybernetickými útočníky, tzv. "bot herder". Botnety se využívají k přetížení vybraných aplikací, webových stránek nebo služeb, a tak slouží jako prostředek pro provádění DDoS útoků. Mimo toho se mohou využít k distribuci spamu, adwaru, spywaru a dalšího škodlivého softwaru (Botnet, @2024).

Motivy pro DDoS útoky se mohou lišit. Kyberzločinci jsou často motivováni finančním ziskem, kdy prodávají útoky jako službu. Dalším důvodem může být vydírání, kdy útočníci požadují výkupné výměnou za ukončení útoku a odblokování online služby případně webové stránky. V některých případech stojí za útoky hacktivismus, kdy aktivisté brání občanské či politické ideály a snaží se upozornit na nespravedlnost pomocí hackingu. Některé útoky jsou prováděny jako odplata za určité rozhodnutí nebo chování společnosti. Například během ruské invaze na Ukrajinu hackeři provedli DDoS útok na ruský propagandistický kanál Russia Today, což vedlo k dočasnému vypadnutí kanálu. Dalším možným motivem může být nekalá konkurence, která usiluje o poškození firmy ze stejného oboru tím, že přetíží její server a tím ji oslabí. Například vypadnutí e-shopu během Vánoc může způsobit firmě značné ztráty. Výpadek v tržbách pak může představovat

během pár hodin miliónové ztráty. Některé DDoS útoky jsou použity jako kamufláž pro jiné, závažnější aktivity jako je kybernetická špionáž či sabotáž (Co je to DDoS útok a co o něm potřebujete vědět?, 2022; DDoS útok, @2024; Šulc, 2018).

Rozdíl mezi DoS a DDoS útokem spočívá v počtu útočících zařízení. DoS útok je realizován jedním zařízením, které používá skript nebo nástroj k útoku na jediný cíl, obvykle jeden konkrétní server nebo koncové zařízení. Naopak u DDoS útoků se využívá rozsáhlá síť kompromitovaných zařízení, tzv. botnet, ovládaných útočníkem. Síť útočí souběžně a jejím cílem je přetížení větších zařízení, aplikací, webových stránek a služeb nebo dokonce celé firemní sítě (DDoS útok, @2024).

Existují různé typy útoků. Nejčastěji se rozdělují do tři kategorií, a to:

- **Útoky na úrovni aplikací** – jsou nejjednodušší formou DDoS útoku. Útoky napodobují běžné požadavky na server. Jinak řečeno, počítače nebo zařízení v botnetu se spojí, aby přistupovaly na server nebo webovou stránku stejně, jako běžní uživatelé. Avšak jak se DDoS útok stupňuje, objem těchto zdánlivě legitimních požadavků je pro server příliš velký na to, aby ho zvládl, a proto se server zhroutí (Porter, 2024).
- **Protokolové útoky** – útok využívá způsob, jakým servery zpracovávají data, s cílem zahlcení a přetížení daného cíle. Některé varianty protokolových útoky spočívají v tom, že botnet odesílá datové pakety, které server sestavuje. Server pak čeká na potvrzení od zdrojové IP adresy, které však nikdy nedostane. I přes to, že server nedostává potvrzení, stále přijímá další údaje k rozbalení, což vede k přetížení (Porter, 2024).
- **Volumetrické útoky** – *„jsou podobné aplikačním útokům, s malým rozdílem. V této formě DDoS je celá dostupná šířka pásma serveru vyčerpána požadavky botnetu, které byly určitým způsobem zesíleny. Například botnety mohou někdy přimět servery, aby si samy posílaly obrovské množství dat. To znamená, že server musí zpracovat příjem, sestavení, odeslání a opětovné přijetí těchto údajů“* (Porter, 2024).

Kybernetické útoky, jako jsou DoS a DDoS útoky, či sabotáže, jsou stále častější a tvoří podstatnou část kybernetických bezpečnostních incidentů. Avšak zpravidla nemají významnější dopady. Jejich podíl v meziročním porovnání neustále roste. Například v červenci 2021 představovaly 22 % všech kybernetických incidentů, zatímco v červnu

2022 už to bylo 75 %. V lednu 2023 došlo k více než dvojnásobnému nárůstu celkového počtu incidentů kvůli DDoS útokům, které zasáhly webové stránky soukromých i státních subjektů. Za útoky stála ruskojazyčná skupina NoName057(16), která se zaměřuje na země NATO a na české cíle začala útočit 11. ledna 2023. Většina z útoků však měla dočasné trvání bez významných dopadů (Ramešová, 2023).

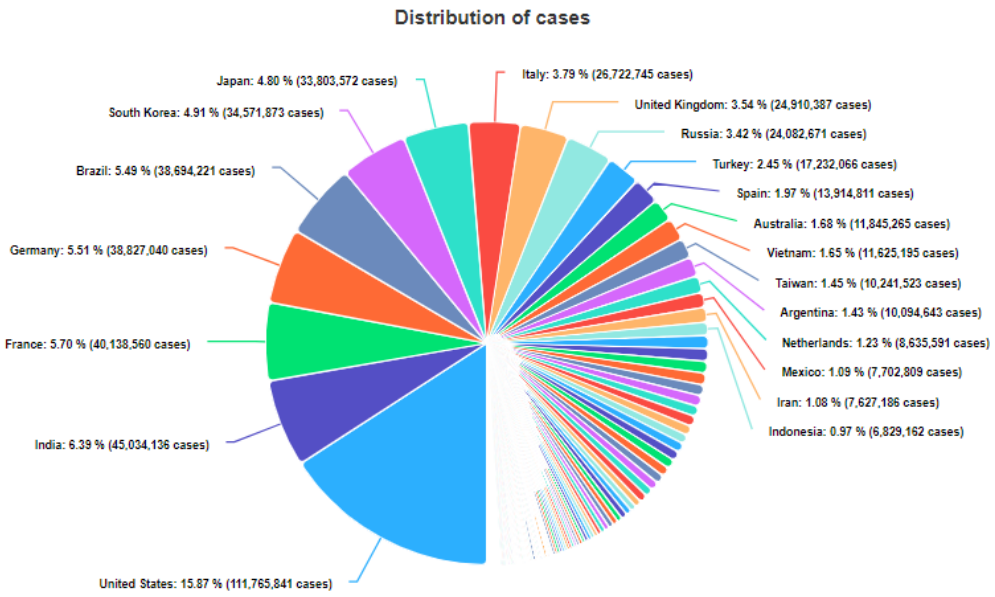
3 VYBRANÉ SVĚTOVÉ KRIZE VE 21. STOLETÍ

Tato kapitola bude pojednávat o charakteristice světových krizí, se kterými bude autorka této práce, pracovat později v praktické části diplomové práce. Autorka vybírala krize, kterým svět čelí v posledních letech.

3.1 Pandemie covid-19

Covid-19 je název používaný pro infekci způsobenou koronavirem SARS-CoV-2, který se poprvé objevil na konci roku 2019 ve městě Wu–chan v Číně. Během krátké doby se nové onemocnění, později označené jako covid-19, rychle rozšířilo po celém světě. Dne 11. března 2020 Světová zdravotnická organizace (dále jen „WHO“) označila šíření tohoto koronaviru za pandemii (hromadný výskyt infekčního onemocnění velkého rozsahu). Na konci roku 2019 se v Číně objevila série zápalů plic nejasného původu s prvními oficiálně hlášenými případy dne 31. prosince 2019 ve městě Wu-chanu. Pneumonie se objevila u lidí, kteří pracovali na trhu, kde se prodávaly živé ryby, mořské plody, ptáci a další zvířecí produkty. Přesný původce onemocnění a způsob přenosu byly neznámé. Počáteční ohnisko ve Wu-chanu se rychle rozšířilo po celé Číně. Další případy se brzy objevily i v dalších částech světa, zprvu v Asii a Austrálii, později v Evropě, Africe a Americe. První případ onemocnění v České republice byl zaznamenán dne 1. března 2020. Virus se může šířit ústy nebo nosem infikované osoby ve formě malých kapalných částic při kašlání, kýchání, mluvení či zpívání. I proto se během největší krize nosily roušky a respirátory. Částice mohou být různé velikosti, od větších respiračních kapiček až po menší aerosoly (Coronavirus disease (COVID-19), @2024; COVID-19: úvod, inkubační doba…, 2024; Slepecký a kol., 2022).

K datumu 1.4.2024 bylo celosvětově potvrzeno 704 539 977 případů covid-19. Na následky tohoto onemocnění zemřelo 7 008 958 lidí po celém světě.



Obrázek 3 – Výskyt případů covid-19 ve světě (Coronavirus Worldwide Graphs, 2024)

Na Obrázek 3 – Výskyt případů covid-19 ve světě (Coronavirus Worldwide Graphs, 2024) lze vidět, že nejvíce výskytů onemocnění covid-19 je v USA, jedná se o více než 111 milionů případů. Další zemí s vysokým počtem výskytu je Indie s více jak 45 milionů, Francie s 40 milionů a Německo, kde onemocnělo více než 38 milionů lidí. Česká republika je v pomyslném žebříčku v počtu potvrzených případů na 34. místě s 4 759 041 případy onemocnění. A na následky zemřelo 43 517 osob (Coronavirus Worldwide Graphs, 2024).

3.2 Válka na Ukrajině

Válka na Ukrajině představuje největší mezinárodní ozbrojený konflikt na evropském kontinentu od konce druhé světové války. Od anexe Krymu v roce 2014 lze tuto situaci považovat za vrchol Rusko-ukrajinského napětí (Spišák, 2022). Konflikt započal 24. 2. 2022, kdy Ruská federace zaútočila na Ukrajinu. Před ozbrojeným útokem na Ukrajinu došlo ze strany Ruské federace k uznání tzv. Lidových republik Doněcké a Luhanské (dále jen „DLR a LLR“). K uznání těchto lidových republik došlo 21. 2. 2022 dekrety prezidenta Putina, které krok objasňují údajným projevem vůle lidu DLR a LLR a odmítnutím Ukrajiny řešit konflikt mírovou cestou v souladu s Minskými dohodami. Dekret předpokládá zahájení "diplomatických vztahů" s Doněckou a Luhanskou lidovou republikou, uzavření dohody o přátelství, spolupráci a vzájemné pomoci mezi Ruskem a oběma entitami a nasazení ruských ozbrojených sil na jejich území s cílem zajištění míru. Žádný jiný stát se nepřipojil k uznání tzv. Lidových republik. Některé země podpořily ruský

postoj nebo vyjádřilo pochopení, například Bělorusko, Sýrie či Venezuela, zatímco některé země jako Čína, Indie a Brazílie zaujaly ne zcela jasný postoj. Všechny ostatní státy kritizovaly uznání DLR a LLR. Na území Ukrajiny se mimo Ruské federace vojensky angažuje ještě jeden stát, Bělorusko. Tento stát poskytuje jednak své území jako základnu pro vedení bojových operací ze strany ozbrojených sil Ruské federace, ale podle dostupných informací také sám vyslal na Ukrajinu některé jednotky. Na konci února roku 2022 se Ruská federace dopustila alespoň dvou jednání, která nejsou slučitelná s mezinárodním právem. Prvním jednáním je předčasné uznání tzv. Lidových republik, kdy Rusko zasáhlo do územní celistvosti a suverenity Ukrajiny. Druhým, ještě závažnějším porušením mezinárodního práva, je útok na Ukrajinu. Rusko se hájí kolektivní sebeobranou na podporu DLR a LLR a preventivní sebeobranou, nicméně s tím Rusko neobstojí. Kolektivní sebeobranu sice mezinárodní právo zná, situace na Ukrajině ale nesplňuje podmínky, na něž je její legalita vázána, chybí napadený „stát“, chybí ozbrojený útok (Konflikt na Ukrajině z pohledu mezinárodního práva…, 2022).

Úřad Vysokého komisaře Organizace spojených národů (dále jen „OSN“) pro lidská práva oznámil, že si konflikt vyžádal životy nejméně 10 582 civilistů a počet zraněných je nejméně 19 000. Přičemž skutečná čísla jsou pravděpodobně výrazně vyšší. Údaje OSN ukazují, že téměř 6,5 milionu Ukrajinců hledalo útočiště po celém světě, přičemž asi 3,7 milionu dalších bylo vysídleno uvnitř země.

Klíčové momenty konfliktu:

- *„Ruský prezident Vladimir Putin oznámil zahájení „zvláštní vojenské operace“ na Ukrajině 24. února 2022, tři dny poté, co prohlásil, že Moskva uzná ukrajinské Doněcké a Luhanské oblasti jako nezávislé státy“* (Teslova, Eruygur, 2024).
- *„V počáteční fázi ruské síly učinily významný pokrok směrem ke Kyjevu. V Irpinu a Buchě došlo k prudkým střetům, přičemž posledně jmenovaný získal celosvětovou pozornost, když prezident Volodymyr Zelenskyj obvinil Rusko ze spáchání válečných zločinů, což Moskva popřela“* (Teslova, Eruygur, 2024).
- *„Ukrajina 2. dubna uvedla, že znovu převzala kontrolu nad celým regionem Kyjeva“* (Teslova, Eruygur, 2024).
- V březnu 2022 došlo k převzetí kontroly Záporožské jaderné elektrárny, největší evropskou jadernou elektrárnou a jednou z největších na světě, ruskými silami (Teslova, Eruygur, 2024).

- V červenci došlo k dohodě o obnovení vývozu obilí ze tří ukrajinských černomořských přístavů, které byly pozastaveny kvůli válce. Dohody dosáhly Turecko, OSN, Rusko a Ukrajina v Istanbulu. Rusko po roce od dohody odstoupilo (Teslova, Eruygur, 2024).
- Putin poprvé od druhé světové války sáhl na částečnou mobilizaci v zemi, povoláno bylo 300 000 Rusů ve věku od 18 do 50 let (Teslova, Eruygur, 2024).
- V říjnu 2022 došlo k výbuch krymského mostu, klíčový úsek mezi spojující Rusko a Krym. Putin z útoku obvinil ukrajinskou rozvědku. A útok označil za teroristický (Teslova, Eruygur, 2024).
- V listopadu 2022 došlo ke stažení ruských jednotek z Chersonu, přístavního města na jihu Ukrajiny (Teslova, Eruygur, 2024).
- 21. května 2023 Rusko vyhlásilo plnou kontrolu nad městem Bachmut, důležitým dopravním a logistickým uzlem v Doněcké oblasti, které se nachází v převážně rusky mluvící industrializované oblasti Donbas (Teslova, Eruygur, 2024).
- Rusko s Běloruskem 25. května 2023 podepsaly dohodu o rozmístění ruských jaderných zbraní v Bělorusku (Teslova, Eruygur, 2024).
- Od doby, co začal konflikt mezi Izraelem a Palestinou, tak došlo k přesměrování západní finanční a vojenské pomoci určené Ukrajině na Izrael. Ustoupil také ukrajinský konflikt do pozadí, zejména pokud jde o pokrytí globálních médií a politickou pozornost (Teslova, Eruygur, 2024).

3.3 Surovinová a energetická krize

V důsledku Rusko–ukrajinské války se prohlubuje celosvětová potravinová krize. Ceny plodin a potravin od poloviny roku 2020 rostou. Ruská invaze způsobila další navýšení cen.

V důsledku války došlo na Ukrajině, která je jedním z největších vývozců obilovin, k dramatickému poklesu exportu svých produktů. To vyvolává značné obavy o potravinovém zabezpečení milionů lidí po celém světě. Pokles ukrajinské produkce obilovin v letech 2022-2023 činila až 29 %. Před vypuknutím války bylo přibližně 90 % ukrajinských zemědělských produktů exportováno po moři. Ruská armáda však v průběhu konfliktu zablokovala černomořské přístavy na Ukrajině, a tím prakticky zastavila veškerý vývoz. EU byla nucena přijmout opatření a zřídit alternativní dopravní

cesty („trasy solidarity“) a opatření zaměřená na odblokování přístavů („Černomořská obilná iniciativa“). Díky opatřením se vývoz zvýšil a ceny potravin stabilně klesaly. Nicméně Rusko v červenci roku 2023 upustilo od Černomořské obilné iniciativy. Do tohoto okamžiku bylo 40 % ukrajinského obilí dopravováno přes černomořské přístavy a zbylých 60 % bylo vyváženo pozemní cestou pomocí tras solidarity. Po Ruském odstoupení se vývoz z Ukrajiny opět snížil a ceny stouply. Další prognózy jsou pozitivní, nicméně celosvětové zásobování potravinami zůstává nejisté, neboť válka a izolace černomořských přístavů ze strany Ruska omezují schopnost Ukrajiny vyvážet obilí a potraviny na světový trh (Infografika – Jak ruská invaze na Ukrajinu prohlubuje celosvětovou potravinovou krizi, 2023).

Ceny potravin jsou kolísavé, stejně proměnlivé jsou také ceny energií. Agrese Ruska vůči Ukrajině vedla ke zvýšení cen paliv v EU a vzrostly obavy ohledně bezpečnosti dodávek energií. Situaci ještě zhoršilo rozhodnutí Ruska pozastavit dodávky plynu do několika členských států EU (Dopad invaze Ruska na Ukrajinu na trhy: reakce EU, 2024). Ruská snaha využít energii jako politickou zbraň měla ničivý dopad na trhy s energií. Energetická krize dosáhla vrcholu v srpnu 2022, kdy ceny energií dosáhly rekordních hodnot. Mimořádně vysoké účty za energii tvrdě zasáhly občany a podniky v celé EU. Členské státy EU usoudily, že se musí co nejdříve vymanit ze závislosti na ruských fosilních palivech, a to diverzifikací dodávek a dodavatelů a snížením využívání fosilních paliv a urychlením přechodu na čistší energii. Díky relativně rychlé reakci se podařilo snížit závislost na Rusku, kde celkový podíl ruského plynu (zkapalněného zemního plynu a zemního plynu z potrubí) na dovozu do EU klesl ze 45–50 % v předkrizových letech na 15 %. Dále byla zajištěna bezpečnost dodávek energie. Před zimou 2022–2023 byly naplněny zásobníky plynu na téměř 95 % a v říjnu roku 2023 byly zásobníky plné na 99% kapacity. Mimo jiné se podařilo podpořit využívání obnovitelných zdrojů energie, kdy rok 2022 byl rekordním rokem pro solární energii. V květnu 2022 bylo v EU poprvé vyrobeno více elektřiny z větrné a solární energie než z fosilních paliv. Země EU přijaly tržní mechanismus s cílem omezit mimořádné výkyvy cen plynu v EU a tím zmírnit dopad prudkého nárůstu cen na občany a ekonomiku. Mechanismus funguje tak, že pokud ceny plynu dosáhnou mimořádně vysoké úrovně, použije se cenový strop pro transakce se zemním plynem (Ceny energií a bezpečnost dodávek, 2024).

3.4 Izraelsko-palestinský konflikt

Izraelsko-palestinský konflikt má své kořeny na konci devatenáctého století. V roce 1947 byla přijata rezoluce 181, známá jako Plán na rozdělení, který měl rozdělit britské mandátní území Palestiny na arabské a židovské státy. Rezoluce byla přijata OSN. Dne 14. května 1948 byl vyhlášen Stát Izrael, což vedlo k vypuknutí první arabsko-izraelské války. Tato válka skončila v roce 1949 vítězstvím Izraele, avšak zároveň došlo k přesunu 750 000 Palestinců a území bylo rozděleno na tři části: Stát Izrael, Západní břeh řeky Jordán a Pás Gazy.

Aktuální konflikt započal 7. října roku 2023 mezi Izraelem a hnutím Hamás, militantní islamistickou skupinou. Hnutí Hamás kontroluje pásmo Gazy od roku 2006 a jedná se o nejvýznamnější eskalaci izraelsko-palestinského konfliktu za několik desetiletí. Bojovníci z hnutí Hamás odpálili rakety na Izrael a zaútočili na města na jihu Izraele a poblíž hranic Pásma Gazy. Během útoků bylo zabito více než 1300 Izraelců, zraněno 3300 osob a stovky lidí byly vzaty jako rukojmí. Izrael byl zaskočen, nicméně den po útoku izraelský kabinet formálně vyhlásil válku Hamásu. Následoval pokyn ministra obrany izraelským obranným silám, aby provedly „úplné obležení“ Gazy. Izrael nadále udržuje plné obklíčení Pásma Gazy, přerušuje dodávky elektřiny, vody a zásoby potravin a léčiv jsou stále nedostatkové. Před konfliktem v Pásmu Gazy žilo přes 2 miliony Palestinců, kteří byli nuceni před válkou utéct, zejména do Egypta (Bouri, Roy, 2024; Israeli-Palestinian Conflict, 2024).

4 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Teoretická část byla rozdělena do dvou kapitol, které byly následně rozvinuty do podkapitol. První kapitola byla věnována základní terminologii. Byly zde analyzovány základní definice v oblasti kybernetické bezpečnosti. Velmi důležitou částí je i samotný právní rámec, který je uplatňován v oblasti kybernetické bezpečnosti. Mezi stěžejní zákony patřící do této problematiky je zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Na tento zákon navazující 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). A velmi důležitá je i směrnice NIS 2 z roku 2022. Poslední část první kapitoly byla věnována klíčovým dokumentům, jmenovitě Národní strategii kybernetické bezpečnosti České republiky a Akčnímu plánu k Národní strategii kybernetické bezpečnosti České republiky. V druhé kapitole byly rozebrány jednotlivé vybrané kybernetické hrozby, mezi nimiž byly malware a jeho dělení, sociální inženýrství a jeho typy, DDoS útoky. Závěrečná část byla věnována nastínění světových krizí ve 21. století. Konkrétně se jedná o pandemii covid-19, Rusko-ukrajinský konflikt, surovinovou a energetickou krizi a Izraelsko-palestinský konflikt. Tyto krize budou rozpracovány v praktické části diplomové práce.

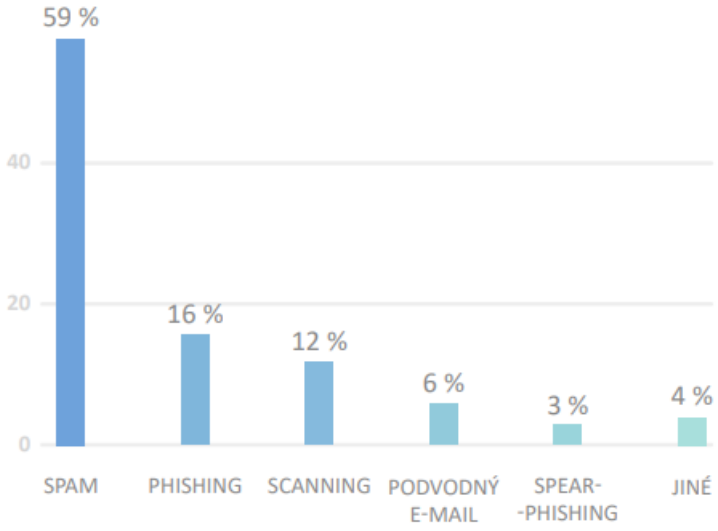
II. PRAKTICKÁ ČÁST

5 VYBRANÉ SVĚTOVÉ KRIZE 21. STOLETÍ V KONTEXTU KYBERNETICKÝCH HROZEB

Tato kapitola si klade za cíl uchopit světové krize, zmiňované v předchozí kapitole v teoretické části, v kontextu kybernetických hrozeb. Dle statistik zjistit, jaké kybernetické útoky se v dané krizi vyskytovaly, které byly nejzávažnější a dále s nimi pracovat. Krize, které autorka diplomové práce vybrala jsou z posledních let, a konkrétně se jedná o pandemii covid-19, Rusko-ukrajinský konflikt, surovinovou a energetickou krizi a Izraelsko-palestinský konflikt.

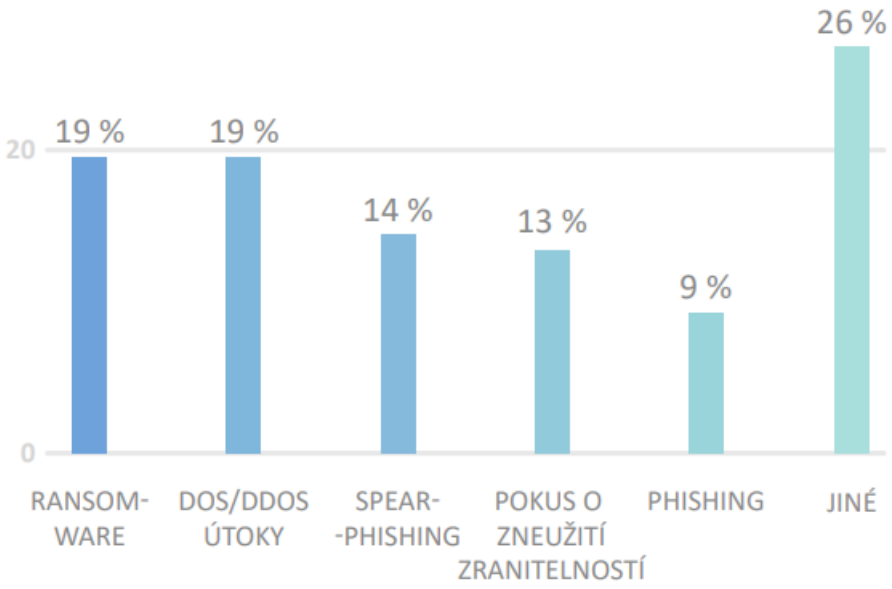
5.1 Kybernetické hrozby během pandemie covid-19 za rok 2020

Zpráva o stavu kybernetické bezpečnosti za rok 2020 udává, že tento rok se vyznačoval zvýšením kybernetických útoků na české instituce, organizace, firmy ve všech sektorech. V roce 2020 bylo nahlášeno 468 incidentů, což je více než dvojnásobek případů oproti roku 2019, kdy bylo nahlášeno 217 incidentů. Rovněž se zvýšila závažnost incidentů, jak potvrzují útoky na Fakultní nemocnici Brno a Psychiatrickou nemocnici Kosmonosy. Mezi nejčastějšími typy útoků v roce 2020 byly spam, phishing a scanning. Mezi nejvážnější hrozbu pro kybernetickou bezpečnost v tomto roce bezesporu patřil ransomware, s nímž útočníci cílili hlavně na zdravotnický sektor. Zvýšený nárůst útoků proti nemocnicím lze do velké míry přisoudit probíhající pandemii a zaměření kyberkriminálních skupin na konkrétní instituce s vyšší pravděpodobností zaplacení výkupného. Problémem mohl být i fakt, že velké množství organizací se potýkalo s nedostatkem odborníků v oblasti kybernetické bezpečnosti (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021).



Obrázek 4 – Nejčastější typy kybernetických útoků v roce 2020 (Zpráva o stavu kybernetických útoků České republiky za rok 2020, 2021)

Na obrázku 4 lze vidět grafické znázornění nejčastějších kybernetických hrozeb v roce 2020. Graf vychází z dotazníku, který rozeslal NÚKIB subjektům regulovaným zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, tak i dalším klíčovým institucím a organizacím, které ZKB regulovány nejsou. Dotazník vyplnilo celkem 222 subjektů, z toho 63 institucí z veřejného sektoru, 24 finančních institucí, 77 zdravotnických zařízení, 14 organizací poskytujících digitální služby, 12 subjektů z energetického sektoru, 12 subjektů z průmyslu a 20 vzdělávacích institucí. Jako nejzávažnější útoky označili respondenti ransomware, DoS/DDoS útoky, spear-phishingové e-maily vizte obrázek č. 5. Přestože více než polovina respondentů uvedla, že detekovala alespoň jeden pokus o kybernetický útok, téměř u tří čtvrtin těchto útoků nedošlo ke kybernetickému incidentu, tedy k narušení důvěrnosti, integrity, dostupnosti informací nebo služeb. Největší počet incidentů detekovaly instituce veřejné správy a zdravotnická zařízení (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021).



Obrázek 5 – Nejzávažnější typy útoků v roce 2020 (Zpráva o stavu kybernetických útoků České republiky za rok 2020, 2021)

NÚKIB v tomto roce řešil hned 99 z 468 incidentů. Nejvíce kybernetických incidentů bylo řešeno v oblasti státní správy. Druhou nejčastější řešenou oblastí byl sektor zdravotnictví.

Nejvýznamnějším a nejzávažnějším incidentem, který řešil NÚKIB, bylo zašifrování systémů Fakultní nemocnice Brno ransomwarem, ke kterému došlo v březnu 2020. Incident vedl k významnému omezení provozu nemocnice na třech lokalitách a způsobil škody v řádu stovek milionů korun. Ve stejném měsíci se stala obětí ransomwaru i Psychiatrická nemocnice Kosmonosy. V tomto případě byla ochromena zejména její administrativní infrastruktura. Nicméně schopnost poskytovat péči pacientům nebyla ohrožena, nedošlo k zasažení systémů, které jsou určeny k záchraně lidských životů. Třetím významným incidentem roku 2020 se stala kompromitace několika desítek e-mailových účtů ve strategické státní správě, což bylo způsobeno úspěšnou spear-phishingovou kampaní. Kromě narušení důvěrnosti obsahu schránek, došlo i k nedostupnosti e-mailových služeb na jeden až dva dny (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021).

Rok 2020 se vyznačoval významným nárustem vyděračských útoků, tedy ransomwaru. Jak již bylo zmíněno, v březnu došlo k útokům na nemocnici v Brně a Psychiatrickou nemocnici Kosmonosy. Následující měsíc došlo k útokům na Povodí Vltavy a na radnici městské části Prahy 3. Tyto útoky neměly souvislost, ačkoliv se odehrály ve stejný den. Během útoku na státní podnik Povodí Vltavy, který patří Ministerstvu zemědělství, nedošlo

k přerušení prvků kritické informační infrastruktury a nebyl tak narušen provoz přehrad ani dodávky pitné vody. Při útoku na radnici v městské části Prahy 3 došlo dočasně k vyřazení provozu služeb systému CzechPoint na jejím území a způsobil nefunkčnost webu a několika dalších systémů (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021).

V porovnání se světem je v ČR výskyt ransomwaru nižší, protože se útočníci tohoto typu útoků více orientují na západní Evropu, Blízký východ a USA. Svůj podíl na tom může nést i fakt, že v zahraničí mohou organizace využít finančních náhrad z pojištění proti vyděračským útokům. V ČR pojišťovny z pojistných podmínek vylučují náhrady škod po ransomwarových útocích a platbu výkupného odmítá i z etických důvodů (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021).

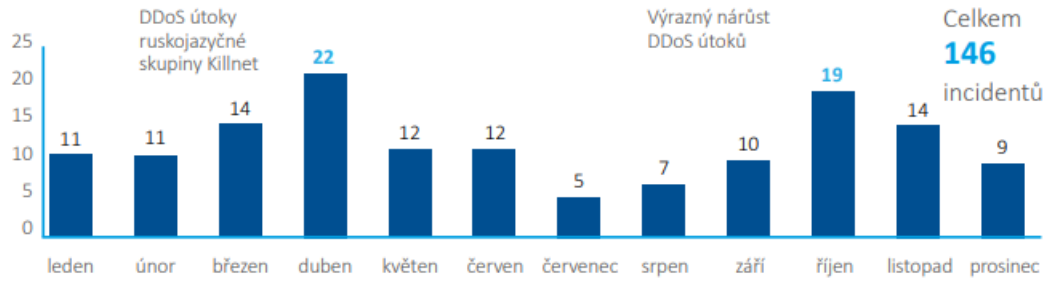
Jak již bylo zmíněno výše, rok 2020 byl rokem, kdy probíhala po celém světě pandemie covid-19. České nemocnice a zdravotnická zařízení se stala atraktivním terčem ransomware útoků, kdy je to z velké části přisuzováno právě pandemii, při které byl na zdravotnická zařízení vyvíjen tlak na poskytování lékařské péče, a proto existovala vyšší šance, že útočníkům zaplatí požadované výkupné (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021).

5.2 DDoS útoky během Rusko-ukrajinského konfliktu

Zásadní událostí roku 2022 je bezesporu ruská invaze na Ukrajinu, která začala 24. února a zásadním způsobem změnila bezpečnostní situaci na našem kontinentu. Konflikt má bezpochyby vliv i na dění v kyberprostoru.

V roce 2022 došlo ke snížení kybernetických incidentů řešených NÚKIB z předešlého roku ze 157 na 146. Ale policie České republiky (dále jen „PČR“) zaznamenala skoro dvojnásobný nárůst kyberkriminálních aktivit.

Zaznamenané incidenty byly do jisté míry spojené s ruskou invazí na Ukrajinu. Nejvíce incidentů proběhlo v měsíci dubnu a říjnu. V těchto měsících docházelo k vysokému nárustu počtu DDoS útoků. Za nárustem stály ruskojazyčné hacktivistické skupiny. K dubnové DDoS kampani se přihlásila skupina Killnet, k části říjnových útoků se přihlásila skupina Anonymous Russia. Za útoky jednoznačně stála podpora Ukrajiny ze strany České republiky (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022, 2023).



Obrázek 6 – Počet řešených incidentů za rok 2022 (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022, 2023)

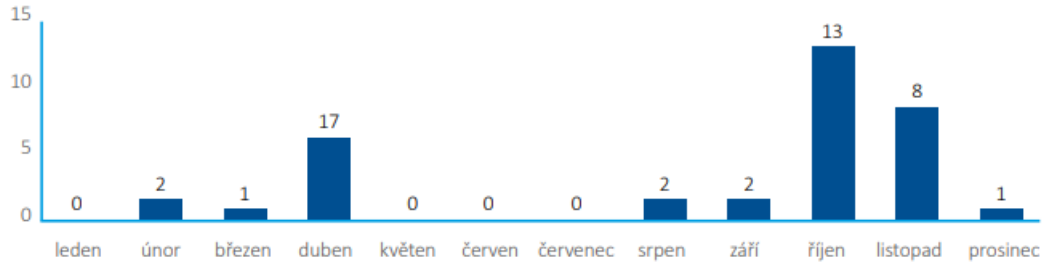
Obrázek č. 6 zobrazuje incidenty řešených NÚKIB v roce 2022. Z grafu lze vyčíst, že v měsíci dubnu a říjnu bylo řešeno nejvíce incidentů.

Ruská invaze na Ukrajinu měla za následek zvýšené riziko kybernetických útoků vůči státům podporujícím Ukrajinu. Cílem hacktivistů byly primárně subjekty veřejného sektoru, ale i řada soukromých organizací.

Dubnová DDoS kampaň skupiny Killnet – v dubnu roku 2022 provedla ruskojazyčná hackerská skupina Killnet dvě série DDoS útoků proti webovým stránkám českých subjektů. První etapa probíhala od 19.4–21.4. a byla mířena na třináct subjektů nevyjímaje NÚKIB a několika ministerstev ČR. Druhá etapa proběhla dne 27.4., kdy bylo napadnuto dalších devět subjektů. „*Počátek útoků se překrýval s oznámením oprav ukrajinské těžké vojenské techniky na území ČR, přičemž útočníci své útoky oznámili na svém telegramovém účtu*“ (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022, 2023).

Říjnová DDoS kampaň skupiny Anonymous Russia – další DDoS kampaň proběhla dne 2. října 2022, kdy hackerská skupina Anonymous Russia oznámila na svém telegramovém profilu útoky na české subjekty. Mezi dotčenými subjekty byly vládní instituce, média, banky, dokonce i letiště. Útoky nakonec nepřinesly negativní dopad na subjekty. Zasažen byl jen zlomek deklarovaných cílů.

Kromě těchto dvou zmiňovaných kampaní docházelo během roku k dalších DDoS útokům, přičemž měsíční počet incidentů způsobených DDoS útoky, které byly zároveň řešeny NÚKIB, lze vidět níže, viz obrázek č. 7. (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022, 2023).



Obrázek 7 – Měsíční vývoj DDoS útoků řešených NÚKIB (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022, 2023)

Proruské hacktivistické skupiny používaly DDoS útoky jako nástroj své propagandy. Ačkoliv reálné škody byly minimální, tak medializace útoků v tuzemsku pomohla skupinám Killnet či Anonymous Russia k propagaci domácímu publiku, prostřednictvím Telegramu se snahou zveličit reálné dopady útoků. Přílišná medializace útoků v napadených zemích tak paradoxně podporovala cíle útočníků (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022, 2023).

Vedle těchto dvou kampaní došlo v ČR také ke kyberšpionážní kampani vůči jedné ze strategických institucí státu. Za kampaní pravděpodobně stojí ruským státem podporovaný aktér APT29 (označován taky jako Cozy Bear, The Dukes či NOBELIUM). Ten je často připisován ruské Službě vnější rozvědky. V této kampani došlo k napadnutí e-mailové schránky jednoho ze zaměstnanců instituce. Pomocí schránky útočník rozeslal spear-phishingové e-maily na více než tisícovku adres partnerských organizací. Dalším cílem útočníka byla snaha kompromitovat další zaměstnance napadené instituce, přičemž maximálně využíval informace obsažené v původní kompromitované schránce (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022, 2023).

5.3 Kybernetické útoky během surovinové a energetické krize

Válka na Ukrajině v roce 2022 sebou přinesla i energetickou a surovinovou krizi. V tomto roce bylo zaznamenáno 146 kybernetických incidentů, nejvíce se vyskytovaly DDoS útoky (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022, 2023). Nicméně nelze s jistotou zjistit, zdali útoky měly souvislost se samotným konfliktem nebo se surovinovou a energetickou krizí.

V roce 2022 výrazně přibyl nárůst kybernetických útoků na energetický průmysl. To lze přisoudit vyvíjející se technologii, která stále více spoléhá na digitální systémy. I když to přináší řadu výhod, má to za následek zranitelnost sektoru vůči kybernetickým hrozbám. Energetický sektor je pro útočníky atraktivním cílem z několik důvodů.

Energetické systémy jsou v zásadě páteří hospodářské činnosti země. Energetický sektor je silně závislý na distribuované komplexní infrastruktuře. To znamená, že existuje větší útočná plocha, na kterou se mohou zaměřovat aktéři kybernetických hrozeb. Dalším důvodem je neodbornost a nevyspělost v oblasti kybernetické bezpečnosti (James, 2023).

Příklady kybernetických útoků ve světě v roce 2022:

- V první polovině roku 2022 došlo na celém světě k sedmi kybernetickým útokům zaměřeným na sektor energetiky. Jeden z útoků byl na evropský sektor ropných produktů. Sektor byl zasažen začátkem tohoto roku kybernetickým útokem, který se zaměřil na nakládací zařízení v Německu a rozšířil se na klíčové terminály v síti Amsterdam-Rotterdam-Antverpy. Postiženo bylo celkem 17 terminálů (11 v Německu a šest v síti Amsterdam-Rotterdam-Antverpy) (Gupte, Critchlow, 2022).
- Útok na Ukrajinskou státní jadernou energetickou společnost – v srpnu roku 2022 ruská hacktivistická skupina s názvem „Lidová kybernetická armáda“ zapojila několik milionů robotů do útoku botů s cílem zničit web této společnosti. Přerušení online služeb trvalo několik hodin, ale žádný trvalý negativní dopad nezůstal. Útok byl součástí kampaně s cílem vytvořit strach z jaderné katastrofy a terorizovat Evropany (Recent Cyber Attacks, @2024).
- Útok na řeckého distributora zemního plynu – řecký národní distributor plynu DESFA ohlásil výskyt kybernetického útoku v srpnu 2022. Útok zasáhl část IT infrastruktury společnosti, který způsobil únik dat. Jednalo se o ransomware, kdy útočníci požadovali výkupné za navrácení a neprozrazení dat. Společnost odmítla výkupné zaplatit (Recent Cyber Attacks, @2024).
- Útok na vodní společnost South Staffordshire – jako předešlé útoky, i tento se stal v srpnu roku 2022. Útok způsobil narušení sítě v její interní podnikové síti a ztrátu dat. Útočníci hrozili manipulací s vodou dodávanou společností (Recent Cyber Attacks, @2024).
- Útok na litevskou energetickou společnost – DDoS útok v červenci roku 2022 zablokoval přístup na web litevské energetické společnosti Ignitis Group. Společnosti se povedlo útok zastavit a omezit jeho poškození pomocí DDoS Protection. K žádnému úniku dat nedošlo, ale útoky byly trvalé a pokračující.

K odpovědnosti se přihlásila proruská skupina Killnet. Útok byl iniciován kvůli litevské podpoře Ukrajiny ve válce s Ruskem (Recent Cyber Attacks, @2024).

5.4 Kybernetické útoky během Izraelsko-palestinského konfliktu

Tento konflikt započal 7. října roku 2023, kdy bojovníci z hnutí Hamás odpálili rakety na Izrael a zaútočili na města na jihu Izraele a poblíž hranic pásma Gazy.

Po útoku na Izrael došlo v tomto státě k navýšení kybernetických útoků. Do útoků byly zapojené zcela nové skupiny, ale i nově přeorientované skupiny, které doteď byly zaměřené na Ukrajinu. Jde o skupiny napojené na režim v Moskvě nebo Teheránu. Mezi obětmi jsou ale i země podporující Izrael, na vrcholu v počtu obdržených útoků stojí Itálie, Francie a Indie. Petr Cícha ze společnosti Check Point Software Technologies v tiskové zprávě uvedl, že během prvních dní došlo k osmnáctiprocentnímu nárůstu kybernetických útoků na cíle v Izraeli. „*Ve vládním a vojenském sektoru došlo dokonce k nárůstu kyberútoků o 52 % oproti průměru v týdnu před 7. říjnem.“* Přitom v celosvětovém trendu došlo k poklesu o 4 %. Daniel Šafář, který je ze stejné společnosti jako p. Cícha uvedl, „*že od začátku války byly zaznamenány stovky zpráv o různých DDoS útocích od desítek hacktivistických skupin. Mezi nejaktivnější patří proislámské skupiny jako Ghost of Palestine nebo Team_insane_Pakistan. DDoS útokům údajně čelily také vládní subjekty a velké společnosti, jako je například Bank of Israel, mobilní společnost Cellcom, izraelský parlament Kneset a další“.* Dopad naprosté většiny útoků byl ale mizivý, neboť útoky byly vedeny buď proti velmi malým webovým stránkám v Izraeli, nebo trvaly pouhé sekundy až minuty. Část skupin, které jsou napojeny na ruský režim obrací svou pozornost od Ukrajiny k Izraeli. Mezi takové skupiny patří skupina Anonymous Sudan. Skupina tvrdí, že hodinu po napadení Izraele způsobila výpadky izraelské civilní aplikace, která je určená pro varování obyvatelstva před raketovými útoky. Mimo to tato skupina spolu s Killnet otevřely sdílený kanál zaměřující se na aktivity proti Izraeli. Útoky se nedotýkaly pouze samotné Izraele, ale i zemí, které ho podporují. Například muslimská hacktivistická skupina Mysterious Team Bangladesh tvrdila, že způsobila výpadek internetových stránek německé letecké společnosti Lufthansa a německého přístavu Kie (Jurek, 2023). Člen týmu kybernetické bezpečnosti společnosti Equinix pro internetovou infrastrukturu uvedl, že nejméně 60 webů se dostalo pod DDoS útoky. Útoky byly z poloviny mířeny na stránky izraelské vlády. Některé z těchto napadených stránek byly znehodnoceny tak, aby zobrazovaly zprávy týkající se „Svobodné Palestiny“ (Hay Newman, Burgess, 2023).

Společnost zabývající se kybernetickou bezpečností S2 Grupo uvedla, že dopad v kybernetické oblasti rozvíjejí především hacktivistické skupiny. Konflikt mezi Izraelem a Palestinou zvýšil počet kybernetických útoků mezi oběma zeměmi. Tým odborníků ze společnosti S2 Grupo provedl analýzu, ze které lze vyčíst hlavní důsledky konfliktu. Mezi hlavní dopady řadí nárůst kybernetického rizika vůči veřejným a soukromým subjektům v západních zemích, které mají blízko k Izraeli. Útočníci budou konflikt využívat k ovlivňování kampaní. Cíle kybernetických útoků se zaměří na kritické infrastruktury a strategické sektory nepřátelských zemí (Ten cyber impacts of the Israeli-Palestinian conflict worldwide, 2023).

NÚKIB v roce 2023 zaznamenal vyšší počet kybernetických incidentů, celkem se jednalo o 262 incidentů. V porovnání s rokem 2022 došlo k téměř dvojnásobnému nárůstu. Příčinou byly hlavně opakované vlny DDoS útoků vedené zejména proruskými hacktivistickými skupinami. Úřad zaznamenal také několik „novinek“ na poli kybernetických incidentů. Jednou z novinek bylo požití velkého počtu účtů vytvořených pomocí botů, tím se jim povedlo podkopat důvěryhodnost oficiálních účtů postižených subjektů. Způsobilo to jejich nefunkčnost, zejména v souvislosti s doručováním e-mailů. Do kyberprostoru se v loňském roce promítl také rychlý pokrok v oblasti generativní umělé inteligence (dále jen „AI“) a chatbotů. Tyto nástroje se dnes zneužívají ke generování phishingu či psaní škodlivého kódu. Ředitel NÚKIB upozornil, že útoky s rozvojem AI a využíváním chatbotů budou stále sofistikovanější (NÚKIB v roce 2023 zaznamenal rekordní počet kybernetických incidentů, 2024). Co se týče kybernetických útoků na ČR v souvislosti s tímto konfliktem, tak podrobnější analýza stavu kybernetické bezpečnosti České republiky za rok 2023 nebyla v průběhu psaní diplomové práce zpracována. Z dostupných zdrojů lze prozatím vyloučit navýšení rizika kybernetických hrozeb pro ČR v souvislosti s tímto konfliktem. Z tohoto důvodu tento konflikt nebude dále rozebírán v práci.

6 METODA WHAT-IF

Tato část práce bude zahrnovat scénáře vybraných kybernetických hrozeb během světových krizí. Hrozby, které byly vybrány jsou takové, které se vyskytují nejčastěji vizte Obrázek 4 – Nejčastější typy kybernetických útoků v roce 2020 (Zpráva o stavu kybernetických útoků České republiky za rok 2020, 2021) a Obrázek 5 – Nejzávažnější typy útoků v roce 2020 (Zpráva o stavu kybernetických útoků České republiky za rok 2020, 2021). Jedná se o ransomware, DDoS útok, phishing, sociální inženýrství v podobě dezinformace a spam. Jednotlivé scénáře by měly ukázat, jaké mohou nastat dopady v jednotlivých typech kybernetických hrozeb.

6.1 Pandemie covid-19

V této kapitole, na základě metody What-if, budou pomocí scénářů předvedeny potenciální dopady kybernetických hrozeb v době pandemie covid-19.

Tabulka 1 – Metoda What-if – pandemie covid-19 (vlastní zpracování, 2024)

Pandemie covid-19			
P.č.	Typ kybernetické hrozby	Příčina	Důsledek
1.	Ransomware	I. Útočníci zablokovali registr na PCR testy a požadují výkupné. II. Farmaceutická společnost dokončovala vakcínu na zvládnutí pandemie, když byla náhle napadena kyberútočníky. III. V nemocnici došlo k odříznutí přístupu k elektronickým	I. Občané se nemohli objednat na PCR test a bez něj nesměli do práce, do obchodu, na úřady. Nemocnice musela zaplatit výkupné za obnovu. II. Zaměstnanci se nedostanou do svých počítačů a je ohrožena práce na vakcíně.

		záznamům pacientů. Sestry nemohly zadávat objednávky na léky a operační sály	III. Ohrožení pacientů z důvodů neuskutečnění operace. Ochromení chodu celé nemocnice. Finanční ztráty nemocnice za obnovu provozu. Řešení žalob ze strany pacientů.
2.	Phishing	I. Občan obdržel e-mail pro potvrzení objednávky na PCR test s požadavkem doplnění informací. II. Občan obdržel e-mailovou zprávu o nezaplacení PCR a požadavku o urychlenou nápravu. III. Rodiče žáků základní školy obdrželi zprávu, že se ve škole vyskytl případ nakažení, a aby okamžitě své dítě poslali k lékaři.	I. Občanovi po vyplnění potřebných informací, včetně údajů k bankovnímu účtu, zmizely peníze. II. Občan po vyplnění náležitostí obdržených e-mailem přišel o peníze z bankovního účtu. III. Panika. Rodiče mohou nevědomky poskytnout pachateli osobní údaje. Útočníci se mohou dostat k údajům o žácích, zaměstnanců. Narušení soukromí, bezpečnosti.
3.	Dezinformace	I. „*Nucené škodlivé očkování. Společnost byla informována o nuceném hromadném očkování, kdy do jejich*	I. Panika obyvatel, kteří se domnívali, že se do jejich těl dostanou nanočipy, sledující jejich životy. II. Vznik zmatku, skupování všech výrobků. Zavírání

		těl budou vpravovány jedy.“ II. Po internetu se šířila videa s umírajícími lidmi na ulici. III. *„Pandemii si vymyslely vlády po celém světě, aby mohly v lidech vyvolat strach, zakrýt jiné problémy.“*	se doma před „apokalypsou“. III. Zlehčování situace. Neuposlechnutí nařízení, ochranných opatření vlády.
4.	DDoS útok	I. Hygienická stanice se dostala pod DDoS útoky, kdy jim na několik hodin vypadly webové stránky. II. Hackeři provedli masivní útok na telefonní linky hygienické stanice. III. Útok byl veden proti nemocnici, kde došlo k vyřazení online systému.	I. V důsledku nefungujících webových stránek se občané nedostali k důležitým informacím o pandemii, včetně statistik a bezpečnostních doporučení. II. V důsledku přetížení telefonní linky se občané nemohli dovolat na hygienickou stanici a nemohli tak zjistit stav jejich onemocnění. III. Lékaři se nemohli dostat k zdravotnickým záznamům o pacientovi, k plánům léčby a dalším informacím. Docházelo

			k ohrožení pacientů a zdržení léčby.
5.	Spam	I. Útočníci rozeslali e-mailové zprávy s falešnou informací o neúčinnosti vakcíny a s nabídkou jiných alternativ. II. Útočníci žádali na sociálních sítích o peněžní dary pro rodiny obětí pandemie. III. Útočníci vydávající se za kabinet vlády, rozeslali e-mailové zprávy s přílohou o nových vládních nařízeních. Příloha obsahovala spyware.	I. Lidé utratili své peníze za neúčinné a nebezpečné výrobky. II. Lidé s dobrou vůlí poslali své peníze podvodníkům, které už nikdy neuvidí. III. Uživatelům po otevření přílohy se do zařízení nainstaloval infostealer. Pomocí něj zjistili útočnici přihlašovací údaje k bankovnímu účtu oběti.

6.2 Rusko-ukrajinský konflikt

V této kapitole, na základě metody What-if, budou pomocí scénářů předvedeny potenciální dopady kybernetických hrozeb v době Rusko-ukrajinského konfliktu.

Tabulka 2 – Metoda What-if – Rusko-ukrajinský konflikt (vlastní zpracování, 2024)

Rusko-ukrajinský konflikt			
P.č	Typ kybernetické hrozby	Příčina	Důsledek
1.	Ransomware	I. Útočníci se rozhodli ztížit ukrajinským uprchlíkům žádat o azyl na MÚ. Po úspěšném průniku do systému dochází k jeho zablokování. Útočníci požadují výkupné ve výši 20 tisíc eur. II. Skupina útočníků provedla úspěšný průnik do systémů MV ČR pomocí phishingu	I. Zastavení procesu přijímání žadatelů o azyl. Omezení poskytování pomoci uprchlíkům. II. Došlo k zašifrování důležitých dokumentů, dalších citlivých informací a narušení činnosti ministerstva.
2.	Phishing	I. Útočníci rozeslali e-mailové zprávy s žádostí o finanční pomoc při humanitární pomoci obětem konfliktu. II. Útočník se vydával za válečného novináře, který poskytoval exkluzivní záběry o válce. Jím poslaný e-mail	I. Finanční ztráty obelhaných občanů. Poškození jména humanitární organizace. Oběti bez pomoci. II. Uživatel se po odkliknutí odkazu nevědomky nainstaloval malware do zařízení, prostřednictvím něhož ho útočník sleduje.

		obsahoval škodlivý odkaz. III. Zločinecká skupina vytvořila falešné webové stránky humanitární organizace. Pomocí e-mailových zpráv rozeslala odkaz na tyto stránky. Na stránkách žádali o finanční dary pro humanitární pomoc. Ve skutečnosti byly dary použity ve prospěch zločinců.	III. Poškození jména organizace. Nárůst nedůvěry lidí vůči humanitárním organizacím, nadacím. Méně příspěvků na pomoc.
3.	Dezinformace	I. Pachatelé prostřednictvím sociálních sítí začali šířit falešné informace o uprchlících z Ukrajiny. Jednalo se zejména o šíření nemocí. II. Falešné zprávy o vojenských operacích. Zprávy zahrnovaly falešné údaje o útocích na civilisty, nemocnice včetně fotek a videí z oblasti bojů. III. Prezident Pavel vyhlásil mobilizaci! Má ambice	I. Vyvolání v obyvatelích ČR strach, ale i nenávist vůči uprchlíkům. Nárůst rasismu a xenofobie. Poškození pověsti ČR ve světě. II. Vyvolání emocí jako jsou strach, hněv ve společnosti. III. Panika občanů, nedůvěra v prezidenta a jeho krocích.

		posílat naše děti do války!	
4.	DDoS útok	I. Útočníci si za svůj cíl vybrali stránky České televize, která vytvářela reportáže o dění na bojišti. II. Webové stránky ministerstva vnitra byly napadeny hackery. Stránky kvůli přetížení byly na 5 hodin nedostupné.	I. Občané se nemohli dostat k novým informacím o boji. II. Omezení přístupu k veřejným službám, k důležitým informacím. Zvýšená nejistota.
5.	Spam	I. Na tisíce e-mailových adres přišla zpráva s odkazem, aby lidé pomohli Ukrajincům. II. Na sociálních sítích se šířila zpráva: Česko v šoku! První ruská vozidla na našem území! Po otevření odkazu si uživatelé nevědomky nainstalovali malware do zařízení.	I. Ztráta peněz, agresivita vůči Ukrajincům. II. Panika. Finanční ztráty v důsledku odstranění malwaru.

6.3 Surovinová a energetická krize

V této kapitole, na základě metody What-if, budou pomocí scénářů předvedeny potenciální dopady kybernetických hrozeb v době surovinové a energetické krize.

Tabulka 3 – Metoda What-if – surovinová a energetická krize (vlastní zpracování, 2024)

Surovinová a energetická krize			
P.č	Typ kybernetické hrozby	Příčina	Důsledek
1.	Ransomware	I. Útočníci zahájili ransomware útok na informační systém společnosti ČEZ prostřednictvím phishingové zprávy, kterou otevřel jeden ze zaměstnanců v e-mailu. II. Útok byl veden na jadernou elektrárnu Dukovany. Po přístupu od systému došlo k zašifrování dat a zablokování systémů.	I. Došlo k zašifrování dat. Byl narušen provoz. Došlo k přerušení dodávek energie do domácností, podniků. II. Blokace provozu elektrárny, zastavení nebo omezení výroby elektřiny. Únik radiace a ohrožení obyvatel a ŽP.
2.	Phishing	I. E-mail od ČSOB: Pozor, Vaše peníze jsou v nebezpečí, schovejte si je u nás! II. Útočník zaslal falešný e-mail s nabídkou exkluzivní ceny za koupě solárního panelu. E-mail obsahoval odkaz na stránku, kde dotyčný	I. Ztráta peněz, osobních údajů, identity. II. Ztráta identity, peněz, nainstalovaný malware v zařízení, který dál škodí. III. Okradení občané. Nedůvěra v humanitární organizace, v humanitární

		vyplnil formulář včetně platebních údajů. III. Pachatel prostřednictvím sociální sítě žádal humanitární pomoc pro rodinu, která jen stěží může zaplatit zálohy za energie.	pomoc. Psychologické dopady.
3.	Dezinformace	I. Na sociálních sítích se šířila zpráva o nedostatku plynu na nadcházející zimu. II. Falešné zprávy o tom, že větrné turbíny vám mohou zničit rodinný dům.	I. Strach občanů z nedostatku tepla. Panika na trhu a propad cen. II. Vržení špatného světla na využití alternativních zdrojů energie.
4.	DDoS útok	I. Útok na burze pro online obchodování s energiemi. II. Útok vedený na webové stránky a online systémy správy státních hmotných rezerv.	I. Narušení obchodování a manipulace s cenami, to by vedlo k nestabilitě trhu. II. Zahlcení síťového připojení, nedostupnost webových stránek a online služeb pro zaměstnance. Narušení řízení a monitorování zásob surovin.
5.	Spam	I. Nejlevnější energie seženete jen u nás!	I. Horší podmínky při odstoupení. Riziko

		II. Falešné zprávy na sociálních sítích o prohlubující se energetické krizi.	bankrotu dodavatele energií. II. Panika a nejistota ve společnosti. Šíření dezinformací.

6.4 Dílčí závěr

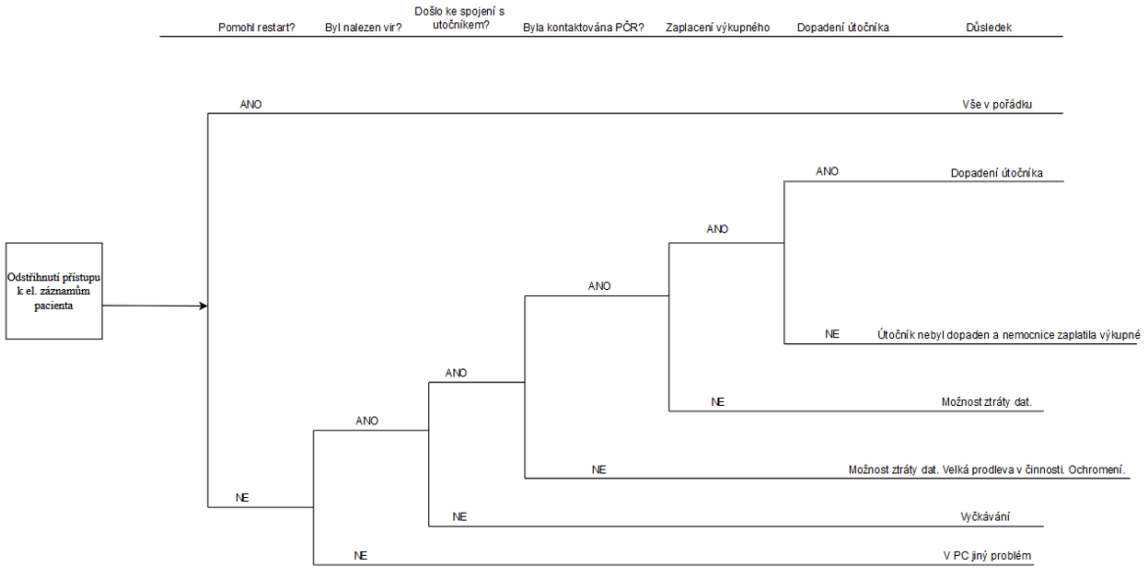
Kapitolou 5 chtěla autorka názorně ukázat, jaké konkrétní dopady na společnost mohou mít kybernetické hrozby. Některé hrozby mohou být navzájem propojené, proto jsou dopady totožné. Během pandemie covid-19 docházelo k ohrožení pacientů, finančním ztrátám, panice a zmatku občanů. Jako nejvážnější kybernetickou hrozbu během pandemie lze označit ransomware, který mohl mít za následek ohrožení pacientů a provoz nemocnic. Dopady Rusko-ukrajinského konfliktu byly opět finanční ztráty, kdy občané v dobré víře přispívali na humanitární pomoc, kam se ale peníze nikdy nedostali. Dalším dopadem bylo vyvolání negativních emocí, agrese a hněv na uprchlíky, ale i na činnost vlády a vládních institucí. Jako nejzávažnější hrozbu v období tohoto konfliktu lze označit DDoS útoky, které měly za následek vyřazení provozu webových stránek ministerstev, PČR a dalších institucí. Dopady během surovinové a energetické krize byly jako v předchozích případech ztráta peněz, panika a nejistota ve společnosti. Jako nejvážnější hrozbu lze označit phishing, kdy útočníci cílili na nejslabší článek, a to na člověka. Nejistý člověk se snadno nechal nalákat na levnější energie.

7 ANALÝZA STROMU UDÁLOSTÍ

Na základě metody ETA chce autorka přiblížit možné další dopady na vybraných příkladech krizových situací. Iniciační událost byla vybrána z předchozí metody What-if a vždy pouze jedna kybernetická hrozba v dané krizi.

7.1 Ransomware během pandemie covid-19

V případě této krize byla autorkou vybrána kybernetická hrozba ransomware. Pomocí rozebrání scénáře se ukázaly další možné dopady.



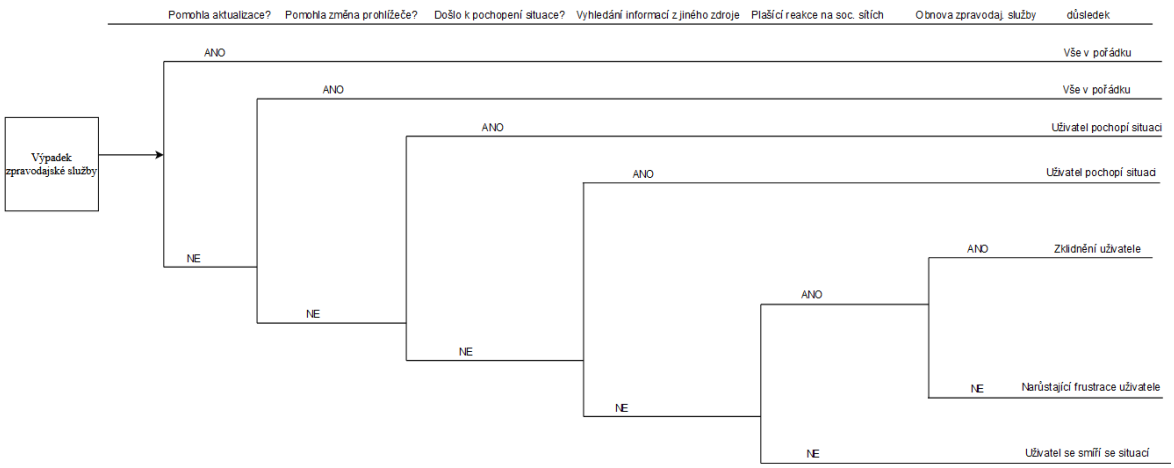
Obrázek 8 – ETA – scénář ransomwaru během pandemie covid-19 (zpracování: vlastní)

Scénář vychází z toho, že v nemocnici došlo k odstřihnutí přístupu k elektronickému záznamu pacienta. Lékař se nemůže dostat do systému. Scénář obsahuje otázky, na které se odpovídá ANO a NE. Pokud na první otázku, zda pomohl restart zařízení, lékař odpověděl ANO, tak se nic zásadního neděje a lékař může dál pokračovat ve své práci. Pokud odpověděl NE, za pomoci antivirového programu zjišťuje, jestli se v zařízení nenachází vir. V případě, že se vir v zařízení nenachází, je nutné problém hledat jinde. V případě nalezení viru může dojít ke spojení s útočníkem. Velmi často se v případě ransomwaru zobrazí na obrazce zpráva, že byl dotyčný napaden hackery a následují další informace. V tento moment by mělo dojít ke kontaktování IT specialistů, ale i PČR. Pokud by k tomu nedošlo, je zde velké riziko, že se stav nezmění a chod nemocnice bude pozastaven na dobu neurčitou. Pacientům se nebudou moci vydávat léky, nebudou moci probíhat lékařská šetření, operace.

Mohla by na základě neuskutečnění operace či nevydání potřených léků vznikat frustrace pacientů, která by v nehorším případě mohla skončit násilným činem. Takový násilný čin by pak vedl k velké nejistotě a panice občanů. K nedůvěře ve zdravotnictví. V další fázi útoku je velmi důležité rozhodnout, zda útočníkům bude vyplaceno výkupné či nikoliv. Není nikdy jisté, zda útočníci po zaplacení vydají dešifrovací kódy. V případě, kdy by útočník nebyl dopaden, je tu veliké riziko, že stejný nebo podobný útok udělá znovu. Opět by to vneslo do společnosti pocit nejistoty, strachu. Mohlo by docházet k žalobám vůči nemocnici a s tím spojené další finanční výdaje. Mohlo by to vést až k uzavření nemocnice. Pokud by to byla nemocnice v malém městě, občané by museli začít dojíždět do vzdálenějších nemocnic. Pro občany důchodového věku by taková situace mohla znamenat, že radši nebudou žádat o pomoc a mohli by umírat v nedůstojných podmínkách.

7.2 DDoS útok během Rusko-ukrajinského konfliktu

V této krizi byla autorkou vybrána kybernetická hrozba DDoS útok. Pomocí rozebrání scénáře se naskytly další možné dopady.



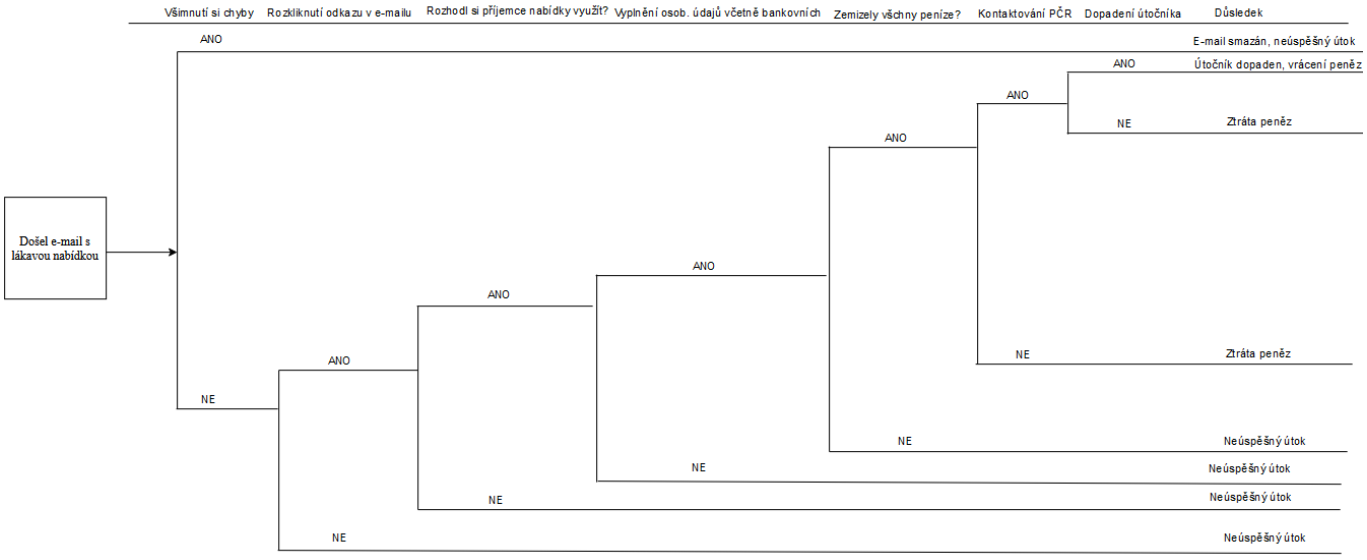
Obrázek 9 – ETA – scénář DDoS útoku během Rusko-ukrajinského konfliktu (zpracování: vlastní)

V tomto scénáři došlo k výpadku zpravodajské služby České televize. Nastiňuje situaci, kdy na území Polska dopadla raketa a zabila člověka a nebylo ještě zřejmé, které straně konfliktu patřila. V tomto období docházelo k hledání informací, jak k tomu mohlo dojít. Občan se snažil rozkliknout stránku, na které by se dozvěděl nové informace o události z Polska, ale stránka mu nešla načíst. Pomohla aktualizace stránky? Pokud ano, občan

si mohl přečíst článek. Pokud ne, mohl se pokusit změnit prohlížeč. V případě, že změna pomohla, opět si mohl v klidu přečíst článek. Pokud změna nepomohla, občan se zamyslel a došel k uvědomění, že momentálně jsou stránky nefunkční a počká, až to opraví. Spoustu lidí nicméně nepochopí, že se nyní nepodívají na stránky, a tak zkouší zjistit informace z jiného zdroje. Pokud se nedostanou ke kýžené informaci může u nich pomalu vznikat panika, úzkost, že někdo nechce, aby se k informacím dostali. Mohou vymýšlet dezinformace. Domáhat se práva na informaci na sociálních sítí, tím strhnout davy. Může docházet k shromažďování a demonstrování. Tím vzniká tlak nejen na občany, ale i na vládu a zainteresované subjekty.

7.3 Phishing během surovinové a energetické krize

V této krizi byla autorkou vybrána kybernetická hrozba phishing. Pomocí rozebrání scénáře se naskytly další možné dopady.



Obrázek 10 – ETA – scénář phishingu během surovinové a energetické krize (zpracování: vlastní)

V průběhu této krize docházelo velmi často k různým lákavým nabídkám na levnější bydlení, levnější energie. Autorka chtěla na základě této skutečnosti poukázat na dopady spojené s phishingovým útokem vedeným prostřednictvím e-mailové zprávy.

Jako iniciační událost byl zvolen e-mail s lákavou nabídkou na levné solární panely. Pokud přijde taková zpráva je hned v prvotní fázi důležité zjistit, zda neobsahuje gramatické chyby. Občas se chyby vyskytují, a to je velký ukazatel toho, že se jedná o podvrh a útok může být

zastaven hned v počátku. Po rozkliknutí odkazu může dojít k vyhodnocení, že lákavá nabídka nebude přijata, a tudíž je útok opět zmařen. V případě přijetí dochází k vyplnění osobních údajů, včetně těch bankovních. V tuto chvíli jsou dvě možnosti. Z účtu odejdou pouze peníze, za které je koupen solární panel nebo dojde ke ztrátě všech peněz. Dochází k frustraci oběti. Následky mohou být až fatální, kdy si sáhne na život nebo vezme život druhým. Pokud by nedošlo ke kontaktování PČR a k dopadení útočníka, tak mohou být ohroženi další občané nebo i firmy. Může vzrůstat nedůvěra a agrese vůči bankám a jejím zaměstnancům. Pokud by byl dopaden pachatel nemusí to znamenat návrat peněz.

8 ZHODNOCENÍ

V diplomové práci byly definovány kybernetické hrozby, které se vyskytovaly během vybraných krizí. V průběhu pandemie covid-19 byli občané ČR nejvíce postihnuti phishingem, nicméně za nejzávažnější kybernetickou hrozbou byl považován ransomware. Ransomware nejčastěji cílil zejména na zdravotnická zařízení. Byla zde pro útočníky větší šance, že dosáhnou výkupného. Během této krize došlo i k několika útokům na Povodí Vltavy a na radnici části města Prahy. Nicméně v porovnání se světem byl výskyt ransomwaru nižší. Hlavně z důvodu, že v ČR pojišťovny vylučují náhrady škod po ransomwarových útocích. Během této krize byly vyhledány dopady jako ohrožení pacientů, ochromení činnosti v nemocnicích, finanční ztráty pro nemocnice, které byly nuceny zaplatit výkupné za dešifrovací klíče.

V případě phishingu lidé přicházeli o své peníze (např.: sbírky pro oběti covidu-19), o narušení soukromí, mnohdy i přicházeli o svou identitu. Společností se šířila panika, ať už z vládních nařízeních (např.: nucené očkování pro vybraná povolání, nošení roušek, dodržování zákazu vycházení), tak později z důvodů dezinformací ohledně očkování. Zvyšoval se počet vládních demonstrací. Na začátku pandemie docházelo také k masivnímu šíření dezinformací. Občané ve velkém skupovali například potraviny či sanitární zboží a tvořili si doma zásoby. Tímto docházelo k zásadnímu nedostatku hygienických a zdravotnických potřeb v nemocnicích.

V průběhu Rusko-ukrajinského konfliktu se ČR stala obětí několika DDoS útoků. Je to přisuzováno podpoře Ukrajiny ze strany ČR. Útoky zasáhly webové stránky několika subjektů, včetně NÚKIB a ministerstva, média, banky, dokonce i letiště. Hacktivistické skupiny používaly DDoS útoky jako nástroj své propagandy. Mezi dopady lze zařadit bezesporu finanční ztráty, kdy lidé v dobré víře posílali peníze na sbírky pro uprchlíky, ale i rodinám obětí války. Peníze však končily u útočníků. To neslo další negativní dopad, a to neochotu pomáhat nebo i ztrátu dobrého jména organizací zaštiťující humanitární pomoc. Dalším dopadem je agrese vůči lidem z Ukrajiny z důvodu dezinformací. V této době je jim přisuzován nárust výskytu černého kašle. S tím souvisí strach a nenávist vůči tomuto národu. Dalším důsledkem dezinformací byla bezesporu panika, kdy se šířila informace, že Petr Pavel, pokud se stane prezidentem, tak vyšle Čechy do války na Ukrajinu. Touto dezinformací také vzrostla nedůvěra vůči prezidentu republiky, ale také i vůči vládě samotné.

Surovinová a energetická krize probíhala souběžně s Rusko-ukrajinským konfliktem, proto bylo velmi obtížné zjistit, jaké dopady sebou krize nesla. Nicméně velkým úskalím byly phishingové útoky. Kdy docházelo k lákavým nabídkám, hlavně ohledně levného bydlení, případně levnějších energií. Občané málokdy rozpoznali chyby nacházející se v došlé poště a slepě naletěli podvodníkům. Útočníci se stávají sofistikovanějšími, takže je těžší rozpoznat podvrhy.

9 NÁVRHY NA ZLEPŠENÍ

S pokrokem doby musí přijít i zlepšení, co se zabezpečení kybernetické bezpečnosti týče. Je velmi důležité předcházet vzniku možného útoku, a proto by měl každý člověk začít u sebe. Proto je velice důležité, aby si lidé zálohovali svá data a pravidelně aktualizovali SW a systémy. Neaktualizovaný systém znamená velkou zranitelnost vůči bezpečnostním chybám. Tyto chyby se snaží softwaroví inženýři každou aktualizací minimalizovat. Aktualizace často obsahují opravy, které mohou snížit riziko útoku. Zálohovat by se mělo hlavně na externí disky. Každý si musí dát velký pozor na co kliká, hlavně co se e-mailových příloh týče, zejména pokud se jedná o neznámé odesílatele. Spoustu útoků probíhá právě v rámci těchto příloh nebo odkazů. Často odkazy mívají podobu naléhavé až fascinující zprávy. A nutí příjemce na ně kliknout. Většina takových zpráv pořád obsahuje gramatické chyby, ale útočníci jsou čím dál tím zdatnější, takže je někdy na první pohled složité takovou inkriminovanou zprávu odhalit. Dost tomu napomáhá AI, která už je na úrovni, kdy chyby dělá minimálně. S tímto úzce souvisí obezřetnost při klikání na odkazy webových stránek, které jsou podezřelé, případně neznámé. Ať už odkazy nacházející se v e-mailových zprávách, tak i odkazy objevující se na sociálních sítích, zejména Facebooku, kde se pod každým příspěvkem objevuje pofidérní odkaz. Stačí se podívat na jméno, případně profil, který takový odkaz posílá a člověk by si měl hned uvědomit, že v tom může být nějaká nekalost. Pokud si nejsem jistý, radši ze stránky odejdu. Pořádně si prohlídnout dané stránky, pokud se na ní vyskytují chyby, případně tam je rozmazané logo, může to poukazovat na podvrh. Velmi důležité jsou informace, které o sobě uživatel poskytuje na internetu, ať už v běžných konverzacích na sociálních sítích a jiných mediích, tak i v soukromých zprávách. Nestahovat si filmy, seriály nebo písničky z neověřených stránek, z důvodu možnosti omylem nainstalovat společně s médiem malware. Používat silná hesla a nejlépe s dvoufázovým ověřením, včetně používání pouze jednoho hesla pro jeden účet. Využívat biometrická ověření (otisk prstu, sken obličeje atd.), v hesle mít obsažena velká, malá písmena a číslice. Nepoužívat v hesle jméno a příjmení, adresu bydliště, jména mazlíčků, oblíbených kapel a podobné informace vztahující se k danému uživateli. Heslo měnit alespoň jednou za tři měsíce a neukládat si je v prohlížečích či v peněžence.

Určitě je velmi důležité nevěřit všem zprávám, které se dostanou do veřejného povědomí. Zprávy si ověřovat z několika zdrojů a prohlubovat kritické myšlení. Většina zpráv

má za cíl šokovat, vyvolat určité emoce. Je důležité se na získané informace dívat kriticky a případně pak tyto poplašné zprávy dále nesdílet a nešířit.

Za zmínku stojí i pořízení antivirového programu, který by měl nalézat kompromitované soubory a programy a odstranit je nebo aspoň upozornit na jejich přítomnost. Existuje jich celá řada, ale je důležité, aby se používal vždy jen jeden takový program. Pokud by se používaly dva a více, mohlo by docházet k jejich vzájemnému rušení a neúčinnosti. Velkým problémem je i nízká proškolenost zaměstnanců a všech, co používají internet. Taková informace vychází i ze zprávy o stavu kybernetické bezpečnosti. V ČR je dlouhodobý nedostatek specialistů na kybernetickou bezpečnost, a to nahrává útočníkům do karet. Je důležité neustále edukovat obyvatelstvo o možných rizicích při pohybu na internetu. Nejen osoby důchodového věku, ale i děti, které nemají takové povědomí o možných rizicích na internetu. Chybí tu besedy, prostřednictvím nichž by se šířily informace o nebezpečí. Ve školách neprobíhají sezení na toto téma. Je to dáno právě nedostatkem odborníků, ale i školní osnovou, která se nepřizpůsobuje dostatečně rychle dnešnímu světu. Přitom taková osvěta by pomohla zvýšit povědomí o kybernetických hrozbách a zásadách kybernetické bezpečnosti a tím snížit potenciální rizika útoků. Dalším opatřením může být pravidelná kontrola bankovního účtu, zdali z něho neodchází více transakcí, než by ve skutečnosti mělo. Dále nepřipojovat se na veřejné Wi-Fi sítě, které mohou být potencionálně využívány útočníky, a ti by mohli sledovat aktivity uživatele. Nepřipojovat do svých zařízení cizí flashdisky, které v sobě mohou ukrývat malware, a pak dotyčnému způsobit potíže.

Pokud bude uživatel napaden malwarem je důležité co nejrychleji odpojit zařízení od sítě, aby se zabránilo šíření na další zařízení. V případě, že jde o napadení zaměstnance ve firmě, a mohlo by dojít k rozšíření prostřednictvím společného serveru, musí ho nahlásit IT specialistovi. Po nalezení hrozby je nutné ji co nejdříve odstranit a pro jistotu změnit hesla. Zjistit, zda mám data zálohovaná a zda jsou v pořádku.

Při napadení ransomwarem je možné postupovat stejně. Nicméně při tomto typu útoku útočníci požadují výkupné, tak je třeba si dobře rozmyslet, zda výkupné zaplatit či nikoliv. Není žádná záruka, že vám útočník po platbě data nebo zařízení dešifruje.

U podezřelých e-mailů, SMS zpráv či odkazů na sociálních sítích je podstatné, abychom na ně nijak reagovali, nejlépe je rovnou smazali. Nikdy neposkytovat citlivé informace jako jsou hesla, osobní či bankovní údaje. Pokud už uživatel klikne na takový odkaz, měl by z něho ihned odejít a zkontrolovat antivirovým programem, jestli se v zařízení

nenachází škodlivý kód nebo aplikace. Zároveň by o této skutečnosti měl informovat své kontakty, aby se tomu vyvarovali.

Stát by měl vynaložit úsilí na aktualizaci zákona o kybernetické bezpečnosti. Přeci jenom je tento zákon z roku 2014, a svět se od té doby dost změnil. Dále se zaměřit na výzkumu a vývoj nových technologií pro detekci a reakci na kybernetické útoky. Investovat do školení a osvěty veřejnosti, firem o bezpečnostních hrozbách. Spolupracovat na mezinárodní úrovni s ostatními státy v rámci organizací (EU, NATO). Vyměňovat si informace o kybernetických hrozbách, zranitelnostech a osvědčených postupech. Neustálé zlepšování bezpečnosti kritické infrastruktury (nemocnice, elektrárny, banky). Vytvářet podmínky pro nové odborníky v kybernetické bezpečnosti.

Pokud už by se člověk stal obětí jakéhokoliv kybernetického útoku, tak je velmi důležité zachovat klidnou hlavu. Kontaktovat PČR. Pokud se stane obětí bankovního útoku, ihned kontaktovat svoji banku a začít to řešit. V dnešní době se často stává, že máte telefonní hovor se svým bankéřem, který vám oznamuje, že máte nějaké podezřelé transakce na účtu a abyste si radši své peníze přemístili na záložní účet. Žádná banka neřeší únik dat či zneužití účtů klientů telefonickou formou. Nikdy nenaléhá na své klienty, aby si vybrali hotovost a následně je vložili na jiný účet. V první řadě je důležité si toto uvědomit a ihned hovor ukončit. Realita ale bohužel bývá taková, že jste takovou zprávou zaskočeni a uděláte vše tak, jak vám do telefonu řekne útočník.

Pokud by nastala další krizová situace nebo mimořádná událost, je důležité být obezřetný. V tu chvíli se objeví spoustu zlých lidí, kteří budou chtít ze situace těžit a z lidí vylákat peníze.

ZÁVĚR

Diplomová práce byla zaměřena na dopady kybernetických hrozeb v průběhů světových krizích.

První kapitola se zabývala uvedením do problematiky. Základní pojmy v oblasti kybernetické bezpečnosti, dále právní rámec, kde byl definován zákon o kybernetické bezpečnosti, na tento zákon navazující vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat a vyhláška o významných informačních systémech a jejich určujících kritériích. V další části byla definována ISO norma řady 27 000, která se zaměřuje na problematiku řízení bezpečnosti. V teoretické části byla zmíněna i směrnice NIS II, která představuje základ kybernetické bezpečnosti v Evropě a určuje nová pravidla při řešení kybernetické bezpečnosti uvnitř organizací. V poslední části byly popsány dva klíčové strategické dokumenty, a to Národní strategie kybernetické bezpečnosti ČR a Akční plán k národní strategii kybernetické bezpečnosti ČR.

Druhá kapitola práce nese název Vybrané kybernetické hrozby. V této kapitole došlo k seznámení čtenáře s vybranými kybernetickými hrozbami. Hrozby, které autorka vybrala byly malware, který dále rozšířila o jednotlivé typy malwaru jako je spyware, adware, červy, trojské koně, ransomware. Dále se jednalo o sociální inženýrství, do kterého řadíme phishing a pharming, v poslední části došlo k seznámení s DDoS útoky.

Poslední kapitola teoretické části patřila významným světovým krizím 21. století, mezi které autorka zařadila pandemii covid-19, Rusko-ukrajinský konflikt, surovinovou a energetickou krizi a Izraelsko-palestinský konflikt.

Začátek praktické části patřil kapitole, která si kladla za cíl zasadit vybrané krize 21. století do kontextu kybernetické bezpečnosti. Zjistit, jaké kybernetické hrozby se během dané krize vyskytovaly nejvíce. Další část spočívala v již nalezení samotných dopadů těchto hrozeb. Autorka proto využila metody What-if na základě, které vymýšlela možné scénáře s potencionálními dopady. Scénáře byly jak fiktivní, tak ale i skutečné. Z této části byl vyřazen Izraelsko-palestinský konflikt z důvodu neprokázanosti kybernetických hrozeb vůči ČR. Po této metodě následovala metoda Analýza stromu událostí. Na základě této metody chtěla autorka přiblížit další možné dopady vybraných kybernetických hrozeb, které byly zásadní pro jednotlivé krize.

SEZNAM POUŽITÉ LITERATURY

6 Common Phishing Attacks and How to Protect Against Them, 2023. Online. Fortra. Dostupné z: https://www.tripwire.com/state-of-security/6-common-phishing-attacks-and-how-to-protect-against-them. [cit. 2024-02-01].

Adware, @2024. Online. Eset Progress. Protected. Dostupné z: https://www.eset.com/cz/adware/. [cit. 2024-02-06].

Agentura, © 2024. Online. Česká agentura pro standardizaci. Dostupné z: https://www.agentura-cas.cz/o-nas/agentura/. [cit. 2024-01-31].

Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025, 2021. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf. [cit. 2024-02-13].

Botnet, @2024. Online. Eset Progress. Protected. Dostupné z: https://www.eset.com/cz/botnet/. [cit. 2024-02-05].

BOURI, Christina a ROY, Diana, 2024. *The Israel-Hamas War: The Humanitarian Crisis in Gaza*. Online. Global conflict tracker. Dostupné z: https://www.cfr.org/in-brief/israel-hamas-war-humanitarian-crisis-gaza. [cit. 2024-03-08].

Co je Pharming?, 2021. Online. SSL.com. Dostupné z: https://www.ssl.com/cs/blogy/co-je-pharming/. [cit. 2024-02-06].

Co je to DDoS útok a co o něm potřebujete vědět?, 2022. Online. Dvojklik. Dostupné z: https://www.dvojklik.cz/co-je-to-ddos-utok-a-co-o-nem-potrebujete-vedet/#_ga=2.34455585.1848894915.1709638733-2111758644.1699440518&_gac=1.6426502.1707226178.EAIaIQobChMIj-qZi-mWhAMVapJoCR2s9giCEAAYASAAEgKZifD_BwE. [cit. 2024-02-05].

COLLINS, Alan, 2013. *Contemporary security studies*. 3rd edition. United Kingdom: Oxford University Press. ISBN 978-0-19-969477-8.

Coronavirus disease (COVID-19), @2024. Online. World Health Organization. Dostupné z: https://www.who.int/health-topics/coronavirus#tab=tab_1. [cit. 2024-03-13].

Coronavirus Worldwide Graphs, 2024. Online. In: Worldometers. Dostupné z: https://www.worldometers.info/coronavirus/worldwide-graphs/. [cit. 2024-04-01].

COVID-19: úvod, inkubační doba, původce a sezónnost onemocnění, 2024. Online. Národní zdravotnický informační portál. Dostupné z: https://www.nzip.cz/clanek/447-covid-19-zakladni-informace. [cit. 2024-03-13].

Ceny energií a bezpečnost dodávek, 2024. Online. Evropská rada / Rada Evropské unie. Dostupné z: https://www.consilium.europa.eu/cs/policies/energy-prices-and-security-of-supply/. [cit. 2024-03-12].

ČERMÁK, Miroslav, 2008. *CIA: Důvěrnost-Integrita-Dostupnost*. Online. In: Clever an dsmart. 2010. Dostupné z: https://www.cleverandsmart.cz/duvernost-integrita-dostupnost/. [cit. 2024-03-15].

Červ, @2024. Online. Eset Progress. Protected. Dostupné z: https://help.eset.com/glossary/cs-CZ/worms.html. [cit. 2024-02-06].

ČESKO, 2005. Zákon č. 412/2005 Sb., o *ochraně utajovaných informací a o bezpečnostní způsobilosti*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

ČESKO, 2014a. Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181?text=kybernetick%C3%BD+z%C3%A1kon

ČESKO, 2014b. Vyhláška č. 317/2014 Sb., *o významných informačních systémech a jejich určujících kritériích.* In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-317

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: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82/zneni-20180528#p36-1

ČESKO, 2019. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

DDoS útok, @2024. Online. Eset Progress. Protected. Dostupné z: https://www.eset.com/cz/ddos-utok/. [cit. 2024-02-05].

DONÁT, Josef; TOMÍŠEK, Jan a JENÍČEK, Michal, 2022. *NIS2: Nová regulace kybernetické bezpečnosti v EU*. Online. Epravo.cz. Dostupné z: https://www.epravo.cz/top/clanky/nis2-nova-regulace-kyberneticke-bezpecnosti-veu-115691.html. [cit. 2024-02-07].

Dopad invaze Ruska na Ukrajinu na trhy: reakce EU, 2024. Online. Evropská rada / Rada Evropské unie. Dostupné z: https://www.consilium.europa.eu/cs/policies/eu-response-ukraine-invasion/impact-of-russia-s-invasion-of-ukraine-on-the-markets-eu-response/. [cit. 2024-03-12].

DoS / DDoS útoky, 2013. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/download/publikace/doporuceni/Doporuceni_DDoS.pdf. [cit. 2024-02-15].

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

DROEGE, Ute, 2022. *Co znamená ISO a norma ISO?* Online. Simply leveraging Quality. Dostupné z: https://www.dqsglobal.com/cs-cz/vzdelavani/blog/co-znamena-iso-a-norma-iso. [cit. 2024-02-07].

DUBOVECKÁ, Klára, 2024. *Ransomware jako kybernetická hrozba – útoky a typy*. Online. Kybez. Dostupné z: https://kybez.cz/ransomware-jako-kyberneticka-hrozba-utoky-a-typy/. [cit. 2024-02-06].

ETA (Event tree analysis) - analýza stromu událostí, @2024. Online. Managementmania. Dostupné z: https://managementmania.com/cs/eta-event-tree-analysis-analyza-stromu-udalosti. [cit. 2024-04-20].

Exploit, @2024. Online. Eset Progress. Protected. Dostupné z: https://www.eset.com/cz/exploit/. [cit. 2024-03-08].

GUPTE, Eklavya a CRITCHLOW, Andrew, 2022. *Ukraine war triggers spike in energy attacks, supply disruptions in H1 2022*. Online. S&P Global Commodity Insights. Dostupné z:

https://www.spglobal.com/commodityinsights/en/marketinsights/latestnews/agriculture/071322-ukraine-war-triggers-spike-in-energy-attacks-supply-disruptions-in-h1-2022. [cit. 2024-03-27].

HAY NEWMAN, Lili a BURGESS, Matt, 2023. *Activist Hackers Are Racing Into the Israel-Hamas War—for Both Sides*. Online. Wired. Dostupné z: https://www.wired.com/story/israel-hamas-war-hacktivism/. [cit. 2024-03-25].

Infografika – Jak ruská invaze na Ukrajinu prohlubuje celosvětovou potravinovou krizi, 2023. Online. Evropská rada / Rada Evropské unie. Dostupné z: https://www.consilium.europa.eu/cs/infographics/how-the-russian-invasion-of-ukraine-has-further-aggravated-the-global-food-crisis/. [cit. 2024-02-25].

Infostealer, @2024. Online. Eset Progress. Protected. Dostupné z: https://www.eset.com/cz/infostealer/. [cit. 2024-02-06].

Israeli-Palestinian Conflict, 2024. Online. Global conflict tracker. Dostupné z: https://www.cfr.org/global-conflict-tracker/conflict/israeli-palestinian-conflict. [cit. 2024-03-08].

JAMES, Luka, 2023. *Energy sector: More cyber attacks in 2022 than ever before*. Online. Power and beyond. Dostupné z: https://www.power-and-beyond.com/energy-sector-more-cyber-attacks-in-2022-than-ever-before-a-a53dfeb9e1a85d8a0710a010c7a7e7d3/. [cit. 2024-03-27].

JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef, 2022. *Výkladový slovník kybernetické bezpečnosti*. Online. In: CyberSecurity.cz Kybernetická bezpečnost a obrana. Dostupné z: https://www.cybersecurity.cz/data/Slovnik_523el.pdf. [cit. 2023-11-08].

JUREK, Jakub, 2023. *Proti Izraeli a jeho spojencům vypukla mohutná kybernetická válka, zasažena je i Evropská unie*. Online. EuroZprávy. Dostupné z: https://eurozpravy.cz/zahranicni/proti-izraeli-a-jeho-spojencum-vypukla-mohutna-kyberneticka-valka-zasazena-i-evropska-unie.myalh3q2. [cit. 2024-03-25].

KADEŘÁBKOVÁ, Markéta, 2020. *Brainstorming aneb kreativní metoda, která šetří čas*!. Online. Orangeacademy. Dostupné z: https://orangeacademy.cz/clanky/brainstorming/. [cit. 2024-04-20].

Keylogger, @2024. Online. Eset Progress. Protected. Dostupné z: https://www.eset.com/cz/keylogger/. [cit. 2024-02-06].

KLIMEŠ, Cyril, @2024. *Informační systémy 1*. Online. In:. Dostupné z: https://web.osu.cz/~Zacek/infs1/skripta-old.pdf. [cit. 2024-03-15].

KOLOUCH, Jan; BAŠTA, Pavel a KUNC, Martin, 2019. *CyberSecurity*. Online. Praha: CZ.NIC, z. s. p. o. ISBN 978-80-88168-34-8. Dostupné z: https://www.eknizky.sk/wp-content/uploads/2019/01/cybersecurity.pdf. [cit. 2023-11-24].

Konflikt na Ukrajině z pohledu mezinárodního práva, část I. uznání tzv. lidových republik a legalita použití síly, 2022. Online. Ústav mezinárodních vztahů Praha. Dostupné z: https://www.iir.cz/konflikt-na-ukrajine-z-pohledu-mezinarodniho-prava-cast-i-uznani-tzv-lidovych-republik-a-legalita-pouziti-sily. [cit. 2024-03-13].

KRÁLOVÁ, Michaela, 2023. *Kybernetické hrozby a jak se před nimi chránit*. Online. Cdc data. Dostupné z: https://www.cdc.cz/cs/kyberneticke-hrozby-a-jak-se-pred-nimi-chranit/. [cit. 2024-03-08].

Legislativa KB, @2023. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/. [cit. 2023-11-15].

Live Cyber Threat Map, @2024. Online. In: CheckPoint. Dostupné z: https://threatmap.checkpoint.com/. [cit. 2024-03-15].

Malware, @2024. Online. Eset Progress. Protected. Dostupné z: https://www.eset.com/cz/malware/. [cit. 2024-02-06].

Metoda „What – If" (Co se stane, když..), 2022. Online. Guard7 safety solution. Dostupné z: https://www.guard7.cz/metoda-what-if-co-se-stane-kdyz/. [cit. 2024-04-20].

Národní strategie kybernetické bezpečnosti České republiky, 2020. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf. [cit. 2024-02-13].

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

NÚKIB v roce 2023 zaznamenal rekordní počet kybernetických incidentů, 2024. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z:

https://nukib.gov.cz/cs/infoservis/aktuality/2073-nukib-v-roce-2023-zaznamenal-rekordni-pocet-kybernetickych-incidentu/. [cit. 2024-03-25].

Obecné informace o směrnici NIS2 a budoucí národní úpravě, @2024. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=3456. [cit. 2024-02-07].

PAČKA, Roman, 2019. *CSIRT: V přední linii boje proti kybernetickým hrozbám*. Brno: Centrum pro studium demokracie a kultury, o.p.s.: Masarykova univerzita. ISBN 978-80-7325-473-5.

Phishing, @2024. Online. Eset Progress. Protected. Dostupné z: https://www.eset.com/cz/phishing/. [cit. 2024-02-01].

PORTER, Evan, 2024. *Co je DDoS útok a jak mu zabránit v roce 2024*. Online. SafetyDetectives. Dostupné z: https://cs.safetydetectives.com/blog/co-je-ddos-utok-a-jak-mu-zabranit/#what. [cit. 2024-02-25].

Prevence a odstranění virů a jiného malwaru, @2024. Online. Microsoft. Dostupné z: https://support.microsoft.com/cs-cz/topic/prevence-a-odstran%C4%9Bn%C3%AD-vir%C5%AF-a-jin%C3%A9ho-malwaru-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5. [cit. 2024-02-06].

RAMEŠOVÁ, Kristina, 2023. *Právní regulace kybernetické bezpečnosti a její meze*. Praha: C.H. Beck. ISBN 978-80-7400-931-0.

Recent Cyber Attacks, @2024. Online. Fortinet. Dostupné z: https://www.fortinet.com/resources/cyberglossary/recent-cyber-attacks. [cit. 2024-03-27].

SEDLÁK, Petr a KONEČNÝ, Martin, 2019. *Přeměna ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM. ISBN 978-80-7623-110-8.

SEDLÁK, Petr a KONEČNÝ, Martin a kol., 2022. *Kybernetická (ne)bezpečnost. Problematika bezpečnosti v kyberprostoru*. Brno: Akademické nakladatelství CERM. ISBN 978-80-7623-068-2.

SLEPECKÝ, Jaroslav a kol., 2022. *Aktuální otázky bezpečnostního managementu v kontextu probíhající pandemie covid-19*. České Budějovice: Vysoká škola evropských a regionálních studií. ISBN 978-80-7556-106-0.

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

Social Engineering: Definition & 6 Attack Types, 2023. Online. Fortra. Dostupné z: https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for. [cit. 2024-02-01].

Sociální inženýrství, @2024. Online. Eset Progress. Protected. Dostupné z: https://www.eset.com/cz/socialni-inzenyrtsvi-a-bezpecnost-firmy/. [cit. 2024-02-01].

SPIŠÁK, Ján, 2022. *Vojenské aspekty války na Ukrajině*. Online. Roč. 2022, č. 4. Dostupné z: https://doi.org/10.3849/2336-2995.31.2022.04.103-118. [cit. 2024-03-13].

Spyware, @2024. Online. Eset Progress. Protected. Dostupné z: https://www.eset.com/cz/spyware/. [cit. 2024-02-06].

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk. ISBN 978-80-7380-737-5.

Ten cyber impacts of the Israeli-Palestinian conflict worldwide, 2023. Online. S2Grupo. Dostupné z: https://s2grupo.es/en/ten-cyber-impacts-of-the-israeli-palestinian-conflict-worldwide/. [cit. 2024-03-25].

Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu, 2016. Online. In: Ministerstvo vnitra České republiky. Dostupné z: https://www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx. [cit. 2023-11-08].

TESLOVA, Elena a ERUYGUR, Burc, 2024. *Two years of war: How the Russia-Ukraine conflict has unfolded*. Online. In: Aa. Dostupné z: https://www.aa.com.tr/en/europe/two-years-of-war-how-the-russia-ukraine-conflict-has-unfolded/3145895. [cit. 2024-04-01].

Trojský kůň, @2024. Online. Eset Progress. Protected. Dostupné z: https://www.eset.com/cz/trojsky-kun/. [cit. 2024-02-06].

Vše o NIS 2, @2024. Online. NIS2. Dostupné z: https://nis2.tech/smernice-nis-2/. [cit. 2024-02-07].

Vyděračské útoky ransomwarem jsou čím dál cílenější, 2020. Online. HTTPS://NUKIB.GOV.CZ/CS/. Národní úřad pro kybernetickou a informační bezpečnost.

Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1644-vyderacske-utoky-ransomwarem-jsou-cim-dal-cilenejsi/. [cit. 2024-03-20].

What is computer virus?, @2024. Online. Malwarebytes. Dostupné z: https://www.malwarebytes.com/computer-virus. [cit. 2024-02-06].

What is malware?, @2024. Online. Malwarebytes. Dostupné z: https://www.malwarebytes.com/malware. [cit. 2024-02-06].

What is a Trojan horse?, @2024. Online. Malwarebytes. Dostupné z: https://www.malwarebytes.com/trojan. [cit. 2024-02-06].

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021. Online. Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf. [cit. 2024-03-16].

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022, 2023. Online. Národní úřad pro kybernetickou a informační bezpečnost. 2023. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf. [cit. 2024-03-20].

SEZNAM POUŽITÝCH ZKRATEK

AČR – Armáda České republiky

AI – Umělá inteligence

ČSN – Česká technická norma

ČR – Česká republika

DDoS – Distributed Denial of Service – Distribuované odmítnutí služby

DLR – Doněcká lidová republika

DW – Dataware

EU – Evropská unie

GDPR – General Data Protection Regulation

HW – Hardware

ISMS – Systém řízení bezpečnosti informací

ISO – Mezinárodní organizace pro normalizaci

IP – Internetový protokol

IT – Informační technologie

LLR – Luhanská lidová republika

MO – Ministerstvo obrany

MV – Ministerstvo vnitra

MZV – Ministerstvo zahraničních věcí

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OSN – Organizace spojených národů

OW – Orgware – organizační složka

PČR – Policie České republiky

PW – Peopleware – lidská složka

SMS – služba krátkých textových zpráv

SW – Software

USA – Spojené státy americké

ÚNMZ – Úřad pro technickou normalizaci, metrologii a státní zkušebnictví

ZKB – Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů

ŽP – Životní prostředí

SEZNAM OBRÁZKŮ

SEZNAM TABULEK