Odolnost příslušníků silových složek státu proti sociálnímu inženýrství

Bc. Štěpán Rožek

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Štěpán Rožek**
Osobní číslo:	**A20581**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní technologie**
Forma studia:	**Kombinovaná**
Téma práce:	**Odolnost příslušníků silových složek státu proti sociálnímu inženýrství**
Téma práce anglicky:	**Resistance of State Forces Members to Social Engineering**

Zásady pro vypracování

1. Proveďte literární rešerši tématu práce.
2. Nalezněte a analyzujte možné postupy řešení.
3. Zvolte metodiku a navrhněte vhodné řešení.
4. Realizujte vlastní návrh pro zvolené prostředí.
5. Vyhodnoťte přínosy své práce a její reálnou použitelnost v praxi.

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

Seznam doporučené literatury:

1. JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 9788074543128. Dostupné také z: http://hdl.handle.net/10563/25821.
2. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 9788072514366.
3. KOLOUCH, Jan. *CYBERCRIME*. Praha: CZ.NIC, z.s.p.o., 2016. Edice CZ.NIC. ISBN 978-80-88168-18-8. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf
4. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. prosince 2021**
Termín odevzdání diplomové práce: **23. května 2022**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že 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 totožné.

Ve Zlíně, dne 10. 5. 2022

Štěpán Rožek v. r.
podpis studenta

ABSTRAKT

Cílem diplomové práce je poukázat na úroveň odolnosti uživatelů v rámci resortu Ministerstva obrany a Armády České republiky proti technikám sociálního inženýrství, především proti phishingovým útokům. Teoretická část je především zaměřena na literární rešerši problematiky kybernetické kriminality se zaměřením na sociální inženýrství, jak v civilním sektoru, tak v armádním prostředí. Praktická část se zabývá statistikou kybernetických bezpečnostních událostí a incidentů získané ze systémů MO/AČR centrem CIRC za určité časové období. Zároveň interpretuje reálné snímky podvodných technik sociálního inženýrství a následná doporučení, díky kterým lze předpokládat zvýšení odolnosti příslušníků vůči těmto hrozbám.

Klíčová slova: sociální inženýrství, kybernetická kriminalita, kyberprostor, Armáda České republiky, phishing

ABSTRACT

The aim of the diploma thesis is to point out the level of resistance of users within the Ministry of Defense and the Army of the Czech Republic against social engineering techniques, especially against phishing attacks. The theoretical part is mainly focused on literary research on cybercrime with a focus on social engineering, both in the civilian sector and in the military environment. The practical part deals with the statistics of cyber security events and incidents obtained from the MO / ACR systems by the CIRC center for a certain period of time. At the same time, it interprets real images of fraudulent techniques social engineering and subsequent recommendations to increase resilience to these threats.

Keywords: social engineering, cybercrime, cyberspace, Army of the Czech Republic, phishing

Mé poděkování patří především prof. Mgr. Roman Jaškovi, Ph.D., DBA za věcné rady a připomínky, které mi během psaní této diplomové práce poskytoval. Dále bych chtěl poděkovat svým služebním nadřízeným a kolegům, kteří mě ve studiu podporovali. V neposlední řadě patří velký dík za podporu také mé manželce Monice a rodině.

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

OBSAH

ÚVOD

Diplomová práce se zabývá problematikou kybernetické bezpečnosti a kriminality a s ní souvisejícím sociálním inženýrstvím, která se dotýká téměř každého uživatele, který je součástí celosvětové sítě Internet či jakékoliv firemní interní sítě. Jelikož se využívání komunikačních prostředků a chytrých (smart) zařízení týká i příslušníků ozbrojených složek, je třeba tyto hrozby a z nich vyplývající rizika brát vážně a zavádět smysluplná opatření, vedoucí ke zvyšování povědomí o této problematice, s cílem zvýšení odolnosti uživatelů vůči těmto hrozbám. Přínosem této práce je především reálná interpretace podob kybernetických útoků sociálního inženýrství, cílených na příslušníky AČR a uživatele Ministerstva obrany. Poskytnutím reálných snímků útoků, které v tomto sektoru a jeho systémech proběhly, se předpokládá zvýšení odolnosti uživatelů, kteří se s touto diplomovou prací seznámí.

Cílem této diplomové práce bylo v rámci možností a citlivosti zkoumaného prostředí, které dává omezený prostor ve zveřejňování informací, zjistit úroveň odolnosti uživatelů proti technikám sociálního inženýrství v resortu Ministerstva obrany – Armády České republiky. Na základě spolupráce s centrem CIRC a poskytnutých datech o kybernetických bezpečnostních událostech a incidentech, pak poukázat na nutnost zvyšování trvalé odolnosti uživatelů proti sociální manipulaci. Důležitá je především i znalost ovlivnění uživatelů v civilním sektoru, která nám dává předpoklad, v čem „trénovat“ odolnost uživatelů v rámci resortu Ministerstva obrany a AČR.

I. TEORETICKÁ ČÁST

1 CHARAKTERISTIKA PROSTŘEDÍ A ZÁKLADNÍ POJMY

Dle Zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a 93. Normativního výnosu Ministerstva obrany – reakce na kybernetické bezpečnostní incidenty v resortu Ministerstva obrany z Věstníku Ministerstva obrany ze dne 23. září 2014, jsou definovány základní pojmy v oblasti kybernetické bezpečnosti následovně:

- Kybernetická bezpečnostní událost – *„Událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.“* [1]
- Kybernetický bezpečnostní incident – *„Narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“* [1]
- Kybernetická hrozba – „*Potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, jejímž výsledkem může být narušení bezpečnosti informací v systému nebo narušení bezpečnosti systému.“* [2]
- Kybernetický útok – *„Jednání entity, které způsobí kybernetický bezpečnostní incident a vede k narušení bezpečnosti informací v systému nebo narušení bezpečnosti systému.“* [2]
- Kybernetická obrana – *„Aplikace bezpečnostních opatření k ochraně systému proti kybernetickému útoku a zmírňování jeho následků.“* [2]
- Kybernetická bezpečnost – „*Představuje soubor opatření, která jsou přijata, aby byl ochráněn počítačový systém před neoprávněným přístupem či útokem.“* [3]

1.1 Internet a kyberprostor

Internetem se rozumí celosvětová decentralizovaná síť, do které jsou připojeny zařízení umožňující vzájemnou komunikaci a výměnu dat. [4]

Definic kyberprostoru existuje mnoho, avšak jako nejvíce relevantní a pochopitelná se jeví definice: „*fiktivní prostředí, ve kterém dochází ke komunikaci skrze počítačové sítě*“. Jedná se tedy o decentralizovaný, globální, dynamický prostor, který je vytvářen a měněn uživateli prostřednictvím komunikačních a informační technologií. Z armádního hlediska se díky velkému rozvoji v oblasti informačních a komunikačních technologií jedná o prakticky o nové válečné prostředí. [3]

1.2 Informační a komunikační technologie (ICT)

Za ICT jsou považována všechna zařízení, která jsou schopna komunikovat a přenášet data v kyberprostoru prostřednictvím sítě internet. Pojem ICT (Information and Communication Technologies) tak zahrnuje mobilní telefony, smartphony, tablety, počítače, bezdrátové sítě a další prostředky, které uživatelům umožňují získávat, měnit, přenášet či uchovávat informace v digitální formě. [5]

Obr. 1. Informační a komunikační technologie [6]

Dle nejaktuálnějšího reportu zveřejněného ITU (International Telecommunication Union), v překladu Mezinárodní komunikační unie, v roce 2021 využívalo síť internet 4,9 miliardy uživatelů, což prakticky znamená, že 63 % obyvatel světové populace je tzv. online. Oproti roku 2019 se počet uživatelů zvýšil o skoro 800 milionů, což značí nárůst o 17 %. [7]

1.3 Sociální inženýrství

Sociálním inženýrstvím jsou nazývány manipulativní či přesvědčovací techniky, které slouží k „donucení“ uživatele, resp. oběti, provést určitou akci nebo k získání informací, které by za normálních okolností neposkytl. Zjednodušeně řečeno: *„Smyslem je v oběti navodit dojem, že situace, v níž se nachází, je jiná, než ve skutečnosti je.“* [8]

Při kybernetických útocích, kdy je využíváno sociální inženýrství, tedy dochází ke zneužití nevědomosti a důvěry oběti. Ne nadarmo je tak člověk označován za nejslabší článek jakéhokoliv bezpečnostního systému. [8] Významný sociotechnik Kevin Mitnick popisuje sociální inženýrství následovně: *„Ten, kdo mámí z lidí peníze je obyčejný podvodník, zatímco ten, kdo využívá manipulace a přesvědčování vůči firmám – obvykle se záměrem získání informací – je sociotechnik.“* [9]

1.4 Ozbrojené síly České republiky

Ozbrojené síly České republiky jsou složky sloužící k zajištění bezpečnosti státu, tvořeny vojáky v činné službě, určených k plnění smluvních mezinárodních závazků o společné obraně proti napadení a dalších úkolů dle Zákona o ozbrojených silách České republiky č. 219/1999 Sb. Dělí se na Armádu České republiky, Vojenskou kancelář prezidenta republiky a Hradní stráž. Vrchním velitelem ozbrojených sil je prezident. [10]

1.4.1 Armáda České republiky a resort Ministerstva obrany

Armáda České republiky (AČR) je hlavní složkou ozbrojených sil České republiky v působnosti Ministerstva obrany (MO), čítající 26928 vojáků z povolání. Dále pak v resortu MO působí 7090 občanských zaměstnanců a 1109 státních zaměstnanců. Celkový počet osob v působnosti MO činí 35127 (k 1.1.2021). [11]

Obr. 2. Znak AČR [12]

Ministerstvo obrany je ústředním orgánem státní správy pro zabezpečování obrany České republiky včetně řízení AČR a správu vojenských újezdů dle §16 Zákona 2/1969 Sb. o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky. [13]

Armáda ČR se dále dělí na:

- Pozemní síly
- Vzdušné síly
- Speciální síly
- Teritoriální síly
- Kybernetické síly

1.4.1.1 Pozemní síly

Pozemní síly jsou základním prvkem ve struktuře AČR tvořeny přibližně 13000 vojáků z povolání, vyznačující se vysokou mobilitou a palebnou silou, jejichž úkolem je příprava sil a prostředků k plnění úkolů v rámci obrany České republiky a plnění mezinárodních závazků, včetně možnosti nasazení jako podpory pro Integrovaný záchranný systém (IZS) při živelných katastrofách, pandemiích apod. [14]

1.4.1.2 Vzdušné síly

Vzdušné síly AČR jsou určeny k obraně vzdušeného prostoru státu v rámci integrovaného systému protivzdušné a protiraketové obrany NATO. V době míru zajišťují službu pátrání a záchrany (SAR), leteckou záchrannou službu či přepravu ústavních či vládních činitelů. V neposlední řadě jsou také součástí Integrovaného záchranného systému (IZS). [15]

1.4.1.3 Speciální síly

Speciální síly jsou samostatný druh sil, který poskytuje České republice vysoce flexibilní a efektivní strategický nástroj v oblasti zajištění obrany a bezpečnosti. [16] Jednotky speciálních sil jsou určeny k provádění speciálních operací v jakýchkoliv geografických či klimatických podmínkách. [16]

1.4.1.4 Teritoriální síly

Teritoriální síly tvoří velitelství teritoria v přímé podřízenosti náčelníka Generálního štábu AČR spolu s krajskými vojenskými velitelstvími (KVV). Úkolem teritoriálních sil je zajištění teritoriální obrany a ochrany důležitých objektů pro obranu státu. V neposlední řadě

se teritoriální síly podílí na podpoře spojeneckých vojsk vyskytujících se na území České republiky a přípravu občanů k obraně státu. [17]

1.4.1.5 Kybernetické síly

Kybernetické síly jsou poměrně novým prvkem AČR pod vedením Velitelství kybernetických sil a informačních operaci (VeKySIO), které vzniklo v roce 2019.

Úkolem tohoto druhu vojsk je, jak už z názvu vyplývá, ochrana a obrana kybernetického prostoru a schopnost vést v tomto prostoru vojenské operace i civilně-vojenskou spolupráci. [18]

1.4.2 Vojenská kancelář prezidenta republiky

Vojenská kancelář prezidenta republiky je vojenským útvarem ozbrojených sil České republiky plnící úkoly dle §26 zákona č. 219/1999 Sb. o ozbrojených silách České republiky. Zajišťuje úkoly a realizace výkonů související s ústavními pravomocemi prezidenta republiky včetně administrace či analytické a informační podpory. [19]

1.4.3 Hradní stráž

Hradní stráž je vojenským útvarem podřízeným náčelníkovi Vojenské kanceláře prezidenta republiky plnící úkoly v oblasti vnější ostrahy a obrany Pražského hradu a organizaci vojenských poct. V případě krizových stavů vyvolaných nevojenskými či vojenskými situacemi vyhlášenými v teritoriu Hradní stráže zajišťuje Hradní stáž plnění specifických úkolů dle Krizového plánu Kanceláře prezidenta republiky a Plánu bojové a mobilizační pohotovosti Hradní stráže. [20]

1.5 Kybernetická bezpečnost a obrana

Pojmem kybernetická bezpečnost je myšlen souhrn opatření či prostředků, které směřují k zajištění ochrany kybernetického prostoru. Jedná se tak o prostředky technické, právní, organizační či vzdělávací s cílem zajistit integritu a dostupnost dat a informací v kybernetickém prostoru. [21] Je však nutné si uvědomit, že „*absolutní bezpečnost neexistuje a absolutní bezpečnost neexistuje a tedy vždy nutně existuje míra akceptovatelného rizika.*“ [22]

Kybernetická obrana je pojem, který označuje konkrétní činnosti a postupy vedoucí k obraně proti útokům vedeným v kyberprostoru a ofenzivní činnosti. [21]

1.5.1 Vojenské zpravodajství a Národní centrum kybernetických operací (NCKO)

Vojenské zpravodajství se v rámci svých běžných aktivit týkající se zpravodajské činnosti, zahrnující získávání, shromažďování a vyhodnocování informací důležitých pro obranu České republiky podílí na zajišťování kybernetické obrany. Pro tyto účely je budováno Národní centrum kybernetických operací, jehož úkolem je vytvořit účinný systém obrany České republiky v kybernetickém prostoru. [23]

Národní centrum kybernetických operací, jako odpovědný objekt pro zajišťování kybernetické obrany zpracovalo tzv. Strategii kybernetické obrany ČR na období 2018-2022, kde ve veřejné části popisuje obecně problematiku kybernetické obrany a v neveřejné části souhrn konkrétních opatření a jejich implementaci. [21]

1.5.2 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

„Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.“ [24]

Mezi důležité činnosti NÚKIB patří projednávání přestupků dle Zákona o kybernetické bezpečnosti č. 181/2014 Sb. a Zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, kdy projednává přestupky týkající se bezpečnosti utajovaných informací v rámci komunikačních a informačních systémů a v kryptografické ochraně.

Národní úřad pro kybernetickou a informační bezpečnost dále vydává ochranné opatření formou opatření obecné povahy a různých doporučení či varování, kdy je cílem upozornit na případné hrozby v kyberprostoru a snížit vyplývající bezpečnostní rizika.

Ve spolupráci s Velitelstvím informačních a kybernetických sil za vojenskou část je NÚKIB koordinátorem civilní části různých cvičení simulující krizové situace a různé scénáře od kompromitací systémů po podvržené aplikace, kterých se obě složky účastní. [25]

1.5.3 Velitelství informačních a kybernetický sil (VeKySIO)

Velitelství informačních a kybernetických sil (VeKySIO) působí na taktické úrovní po boku s Pozemními silami, Vzdušnými silami a Velitelstvím teritoria pod velením Velitelství pro operace. V součinnosti s ostatními druhy sil a vojenským zpravodajstvím je schopné vést a provádět operace v kyberprostoru včetně monitoringu, plánování a řízení operací. [26]

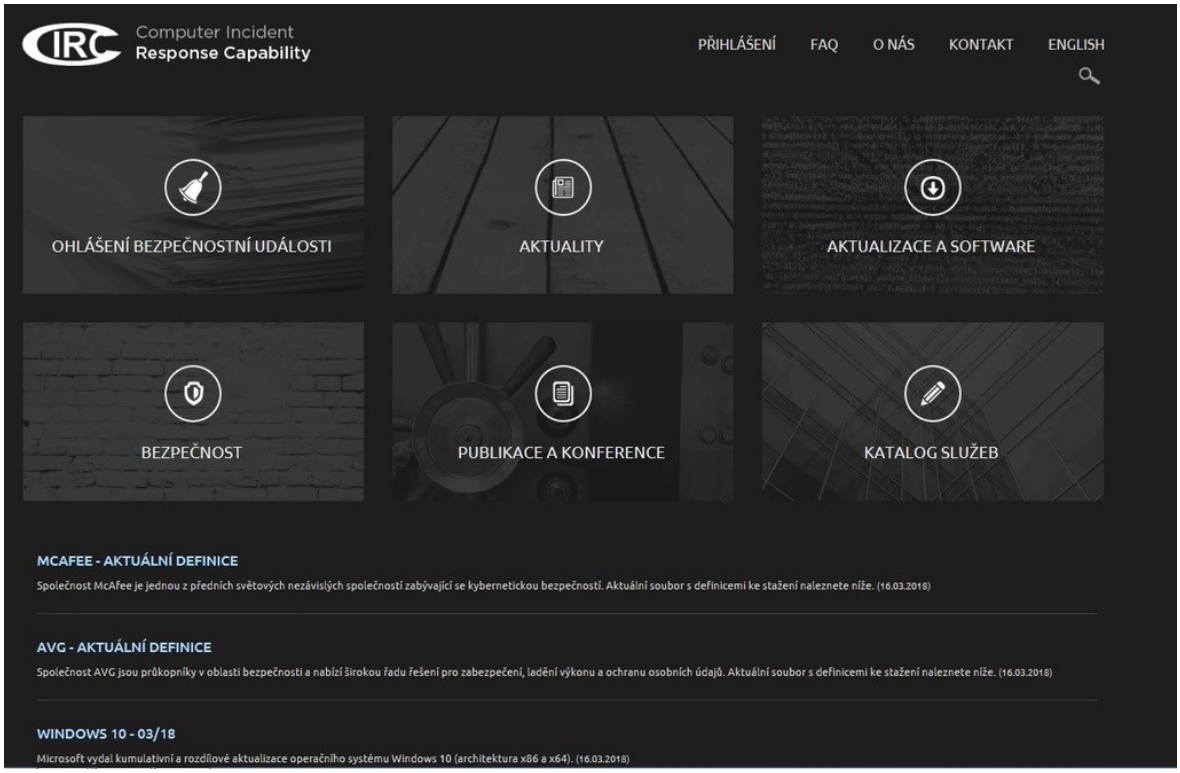
Obr. 3. Velitelství kybernetických sil a informačních operací [18]

VeKySIO taktéž v rámci své obvyklé činnosti podílí na vojenských cvičeních, kterých se AČR účastní s cílem provádět testovací kybernetické útoky na různé systémy. Jeden z těchto testovacích útoků byl proveden v rámci cvičení Resolute Effort 22, kdy byl proveden kybernetický útok na obrněná vozidla KVBP Pandur II, který vyřadil systém několika těmto vozidlům. V rámci tohoto útoku proběhlo ověření znalostí a zdokonalení Týmu rychlé reakce, který provedl diagnostiku problému a techniku zprovoznil. [27]

Obr. 4. Kybernetický útok na vozidla Pandur [28]

1.5.4 CIRC

Centrum CIRC (Computer Incident Response Capability), které je prvkem Velitelství kybernetických sil a informačních operací (VeKySIO), slouží k nepřetržitému monitoringu, detekci, analýze a vyhodnocování kybernetických bezpečnostních událostí a incidentů pro zajištění kybernetické obrany systémů používaných v rámci resortu Ministerstva obrany. Úkolem centra CIRC je taktéž šířit bezpečnostní povědomí o problematice kybernetických hrozeb mezi uživateli i správci informačních a komunikačních systémů. Pomocí interního informačního portálu poskytuje centrum CIRC uživatelům možnost otestování softwaru (SW) a vydává opravné SW balíčky ke zvýšení kybernetické bezpečnosti v rámci systémů používaných v resortu MO. [29]



Obr. 5. Úvodní stránky Centra CIRC [30]

Tento portál lze následně využít k bezpečnému stahování softwaru, který byl pracovníky tohoto centra prověřen a byla otestována jeho bezpečnost pro použití v systémech MO. Zároveň lze pomocí tohoto portálu ohlásit kybernetické bezpečnostní události, kterými se následně zabývá analytická skupina a dochází k jejich prošetření.

1.6 Systémy v rámci Ministerstva obrany a AČR

V současné době je v rámci Ministerstva obrany a v Armádě České republiky využíváno více jak 10 informačních systémů, z nichž každý plní jinou funkci, avšak jejich obsahem je velké množství citlivých dat, které mohou být při jejich kompromitaci zneužity.

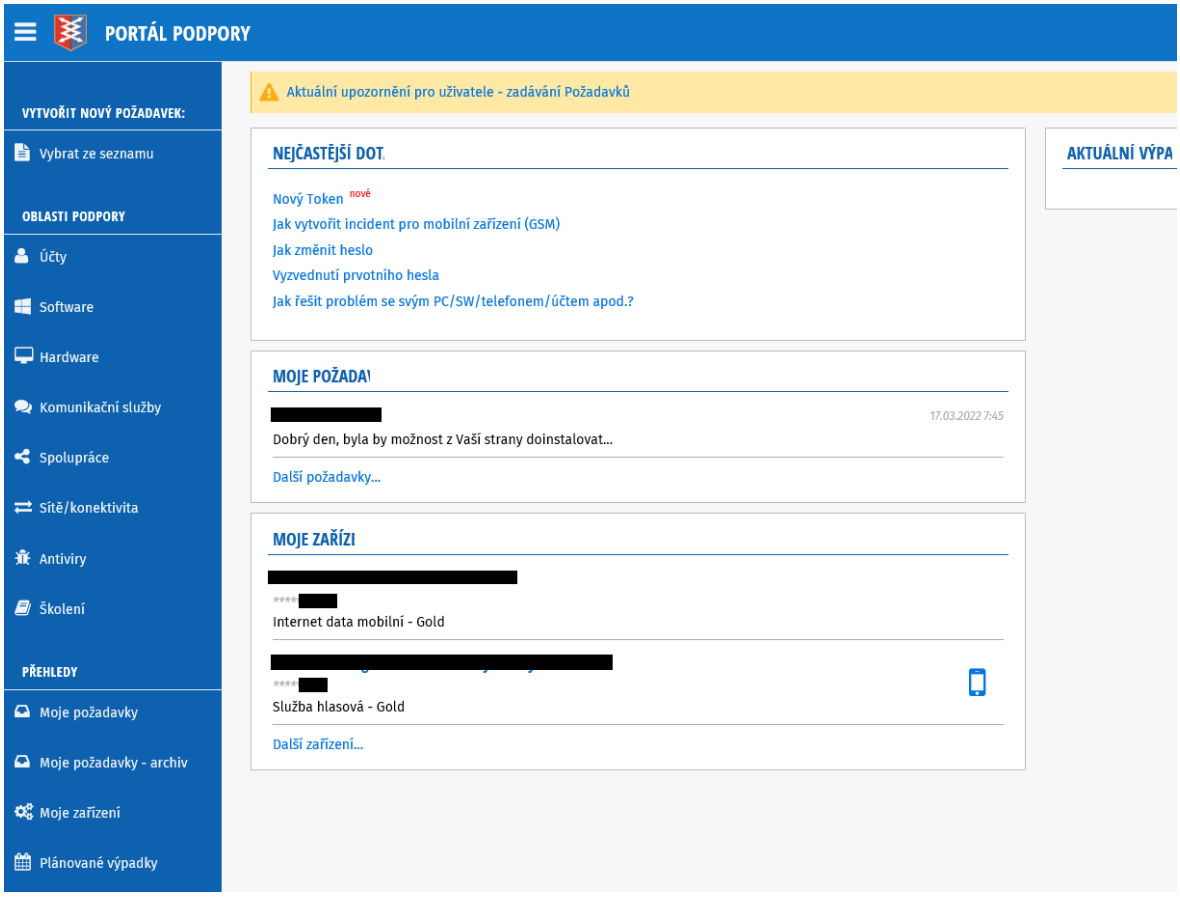
Příkladem jsou systémy:

- ŠIS – Štábní informační systém;
- ISL – Informační systém logistiky;
- IMO – Internet Ministerstva obrany;
- FIS – Finanční informační systém;
- ISSP – Informační systém služby a personálu;
- ZdravIS – Zdravotnický informační systém;
- OTS VŘ PozS – Operačně taktický systém velení a řízení pozemních sil.

1.6.1 ŠIS – Štábní informační systém

Štábní informační systém (ŠIS) patří mezi nejvyužívanější informační systém v AČR vůbec. Jedná se o informační systém určený k podpoře každodenních činností velitelů a štábů. Účelem tohoto systému je podpora procesů velení, plánování a řízení. V rámci celého resortu Ministerstva obrany je ŠIS integrujícím prvkem systémů elektronické pošty. Kybernetická bezpečnost ŠIS je zajištěna výhradně příslušníky MO. [31]

V rámci Štábního informačního systému je k dispozici tzv. Portál podpory uživatele, včetně vzdálené podpory HELPDESK, kde uživatel nalezne informace týkající se řešení běžných problémů v rámci ŠIS. V případě, že se jedná o problém, který není schopen uživatel vyřešit samostatně, lze vytvořit požadavek, který si převezme provozní správa ŠIS, která je schopna problém vzdáleným přístupem vyřešit.



Obr. 6. Portál podpory systému v systému ŠIS [archiv autora]

1.6.2 IMO – Internet Ministerstva obrany

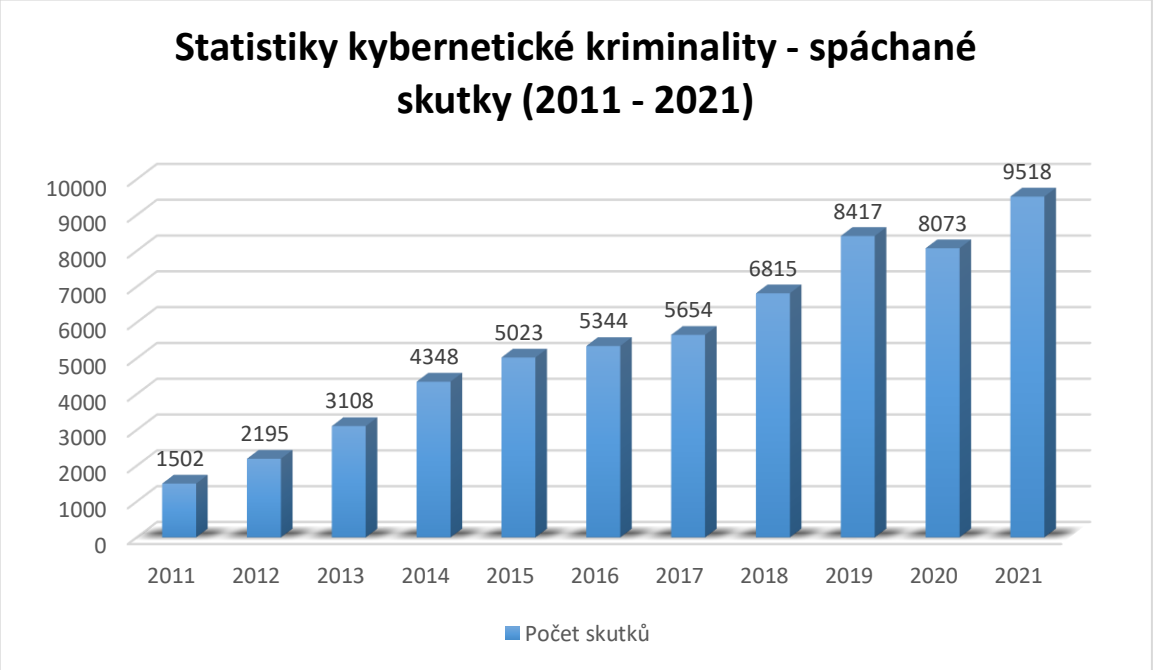
Internet Ministerstva obrany je služba, která příslušníkům MO zajišťuje přístup do celosvětové sítě Internet. IMO je určen k podpoře činností pracovníků, kteří v rámci své pracovní náplně potřebují získávat informace z veřejných zdrojů. [31]

Přístup do této sítě je možný pouze s využitím proxy serveru, který funguje jako filtr a blokuje přístup k určitým webovým stránkám.

2 KYBERNETICKÁ KRIMINALITA

Kybernetická kriminalita, alias kyberkriminalita či počítačová kriminalita se projevuje prostřednictvím tzv. kybernetických útoků. Jedná se tedy o protiprávní jednání v kyberprostoru, které je možno dle Zákona č. 40/2009 Sb. Trestního zákoníku postihovat. [8]

Dle statistik Policie ČR bylo v roce 2021 registrováno 9 518 skutků z kategorie kybernetické kriminality, což je meziroční nárůst o 17,9 %. Jednalo se především o jednání klasifikované jako podvod, poškozování a zneužití záznamu na nosiči informací, neoprávněného držení platebního prostředku a porušování autorského práva a práv k autorské známce. V rámci nejčastějšího projevu kybernetické kriminality, podvodných jednání, docházelo ke zneužití citlivých údajů obětí a finančním podvodům prostřednictvím podvodných emailových zpráv či komunikací skrze sociální sítě a další komunikační kanály. [32]

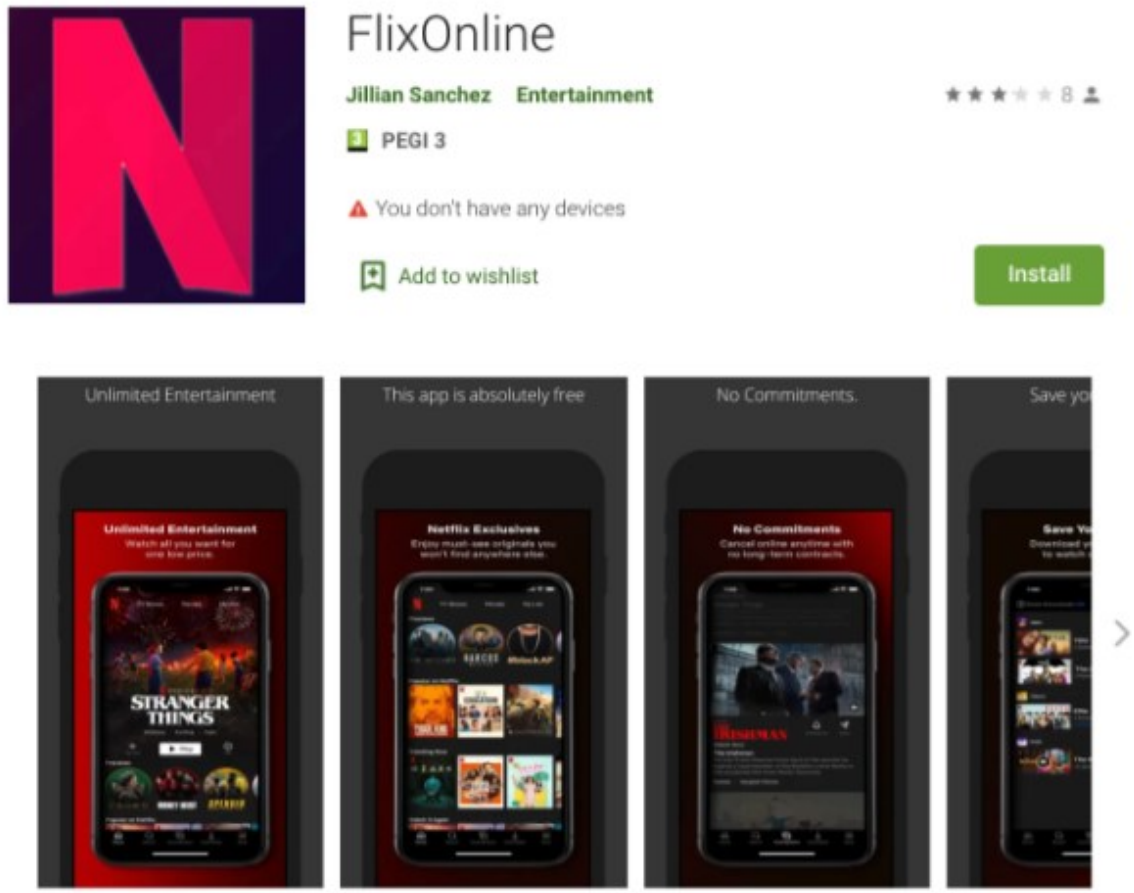


Obr. 7. Statistika skutků kybernetické kriminality v období 2011–2021 [32]

2.1 Malware

Za malware (malicious software) je označován jakýkoliv škodlivý kód, který je schopný při průniku do systému narušit jeho integritu a získávat, ničit či jinak kompromitovat informace. [8] Dle společnosti ESET se v roce 2021 zvýšil počet malware o 20 %. Nejčastějším cílem bylo získání uživatelských hesel a přihlašovacích údajů do

elektronického bankovnictví. Zvýšený výskyt malware byl jak u operačního systému Windows, tak u platformy Android, který je hojně zastoupený v chytrých zařízeních – především v chytrých mobilních telefonech (smartphonech). Uživatele Windows nejčastěji ohrožoval v roce 2021 spyware pod názvem Agent Tesla, který byl šířen cíleným emailovým spamem v českém jazyce. Uživatele systému Android v tomto roce ohrožoval bankovní malware s názvem Cerberus. Výrazný nárůst byl zaznamenán taktéž u tzv. dropperů, což je výraz pro malware, který se šíří pomocí aplikace, kterou uživatel do zařízení nainstaluje v dobré víře, že se jedná o užitečný nástroj či službu. [33]



Obr. 8. Podvodná aplikace v aplikaci Google Play [34]

Aplikace FlixOnline, která byla objevena společností Check Point Research (CPR), v sobě ukrývala malware, který po instalaci do zařízení vyžadoval povolení ke čtení oznámení, kontaktů a obsah příchozích zpráv. Tato aplikace slibovala po instalaci bezplatný přístup ke službě Netflix, která patří mezi nejznámější poskytovatele audiovizuálního obsahu.

Povolení těchto oprávnění reálně znamenalo, že aplikace mohla odesílat falešné zprávy pod jménem oběti v chatovacích aplikacích Messenger, Whatsapp a dalších. Šíření této aplikace probíhalo právě pomocí těchto zpráv, které vyzývaly kontakty ke stažení této aplikace. [35]

2.2 Ransomware

Za ransomware je považován malware, který data v zařízení zašifruje a pro jejich dešifrování vyzývá k zaplacení výkupného především prostřednictvím kryptoměn (Bitcoin, Ethereum, Litecoin aj.). Ransomware lze rozlišit na dva typy dle jeho chování v zasaženém zařízení. [36]

První typ tohoto malwaru je ransomware, který v zařízení data zašifruje a systém v zařízení se stane zcela nefunkčním. Příkladem tohoto typu ransomware byl i tzv. Policejní ransomware, který v zařízení zablokoval přístup k účtu uživatele OS Windows s upozorněním o nalezeném závadném materiálu v zařízení, které je v rozporu s právním systémem dané země. Zároveň vyzýval uživatele jménem policie k zaplacení určité finanční částky, po jejíž úhradě dojde k odblokování systému zařízení. [8]

Obr. 9. Policejní ransomware [37]

Druhým typem, který je častěji využíván je ransomware, který uživateli ponechá systém v zařízení funkční, avšak zašifruje data v něm uložená, což zapříčiní jejich nepřístupnost. V praxi to znamená zašifrování pevného disku počítače či úložiště v mobilním zařízení s požadavkem na zaplacení určité částky na účet útočníka. Kvůli zachování anonymity

využívají útočníci platby pomocí kryptoměn či různých předplacených služeb. Pro zvýšení nátlaku na psychiku oběti útočníci zpravidla stanoví ve výzvě i časovou lhůtu, po jejíž vypršení dojde ke smazání klíče k dešifrování dat. [8]

2.3 Adware

Adware neboli zkrácená verze „advertising malware“ je typ škodlivého kódu, který není pro uživatele zasaženého zařízení tak nebezpečný jako jiné typy malware, avšak je dosti obtěžující. Adware se projevuje v infikovaném zařízení zobrazováním vyskakovacích (pop-up) oken zobrazujících reklamní sdělení či zobrazuje explicitní obsah (porno stránky aj.).

Ačkoli se adware na první pohled nejeví jako nebezpečná forma malware, není vyloučeno, že jeho součástí není například spyware, který je schopen sledovat činnosti uživatele napadeného zařízení s cílem odcizení citlivých informací. [8]

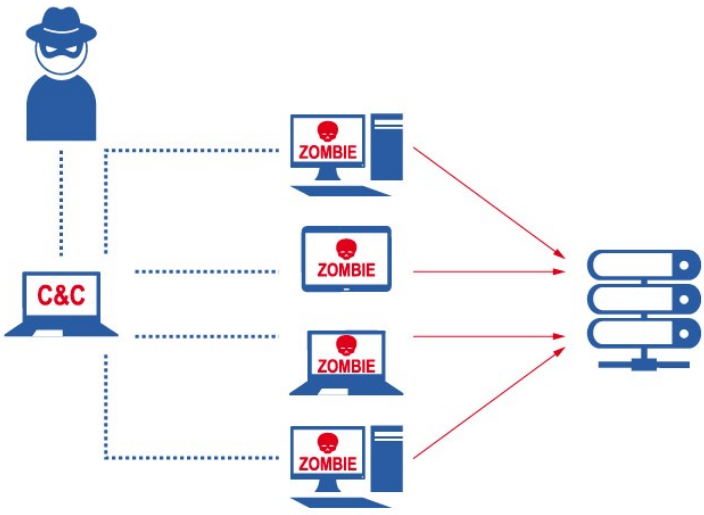
Obr. 10. Adware [8]

2.4 Spyware

Spyware je druh malwaru, který je schopen „špehovat " aktivity uživatele. Jednoduše řečeno, sleduje činnost, kterou uživatel na svém zařízení běžně provádí. Cílem tohoto malwaru je zisk různých dat, která jsou pak dále využívána například k lepšímu cílení reklam. Existuje však i typ spyware, který je schopný získat přístup k mikrofonu či kameře v zařízení. Takový spyware lze považovat za významné bezpečnostní riziko, jelikož může vést až k průmyslové špionáži či krádeži identity. [38] Spyware bývá často implementován do instalačních souborů různých aplikací či software. Uživatelé si spyware do zařízení nainstalují často nevědomky, jelikož zpravidla bez čtení odsouhlasí vše, k čemu je instalační průvodce vyzve. [8]

2.5 Botnet

Za Botnet je označována síť veškerých zařízení napadených malwarem, který umožňuje jejich vzdálené ovládání útočníkem z centrálního místa. Jedná se tak o počítače, chytré telefony, routery, pračky, robotické vysavače, IP kamery a další zařízení, která jsou schopna komunikovat v rámci celosvětové sítě internet. Pomocí technik sociálního inženýrství útočníci infikují zařízení malwarem, o kterém uživatel (oběť) nemá tušení a běží tzv. na pozadí. Malware následně v infikovaném zařízení (zombie) naváže spojení s tzv. C&C serverem a útočník tak pomocí vzdálené správy získává nad zařízením plnou kontrolu. Síť tzv. zombie zařízení pak útočníci pronajímají k páchání kybernetických útoků – zpravidla DDoS či šíření spamu. [39]



Obr. 11. Botnet útoky [40]

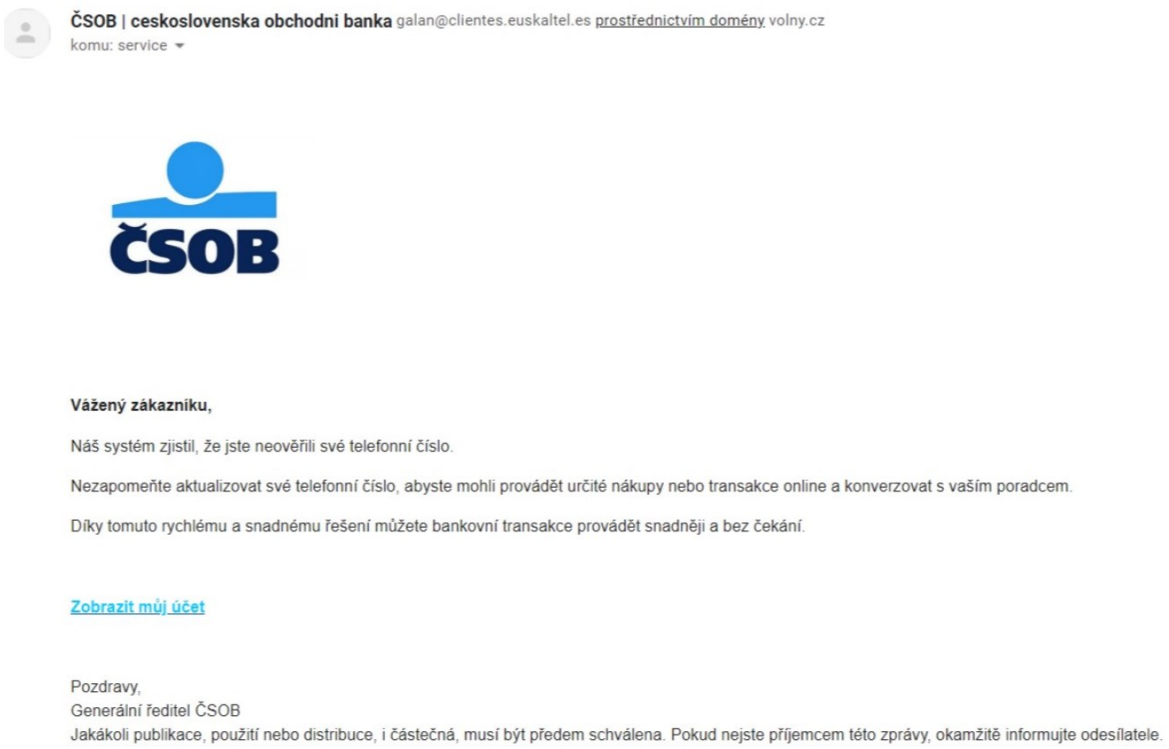
3 FORMY SOCIÁLNÍHO INŽENÝRSTVÍ

Způsobů, jakými útočníci dosáhnou svého cíle – a to především zmocnění se citlivých údajů či přimění k určité akci, kterou oběť v nevědomosti a dobré víře provede existuje několik. Každý z nich je specifický a lze jej zařadit mezi následující formy sociálního inženýrství.

3.1 Phishing

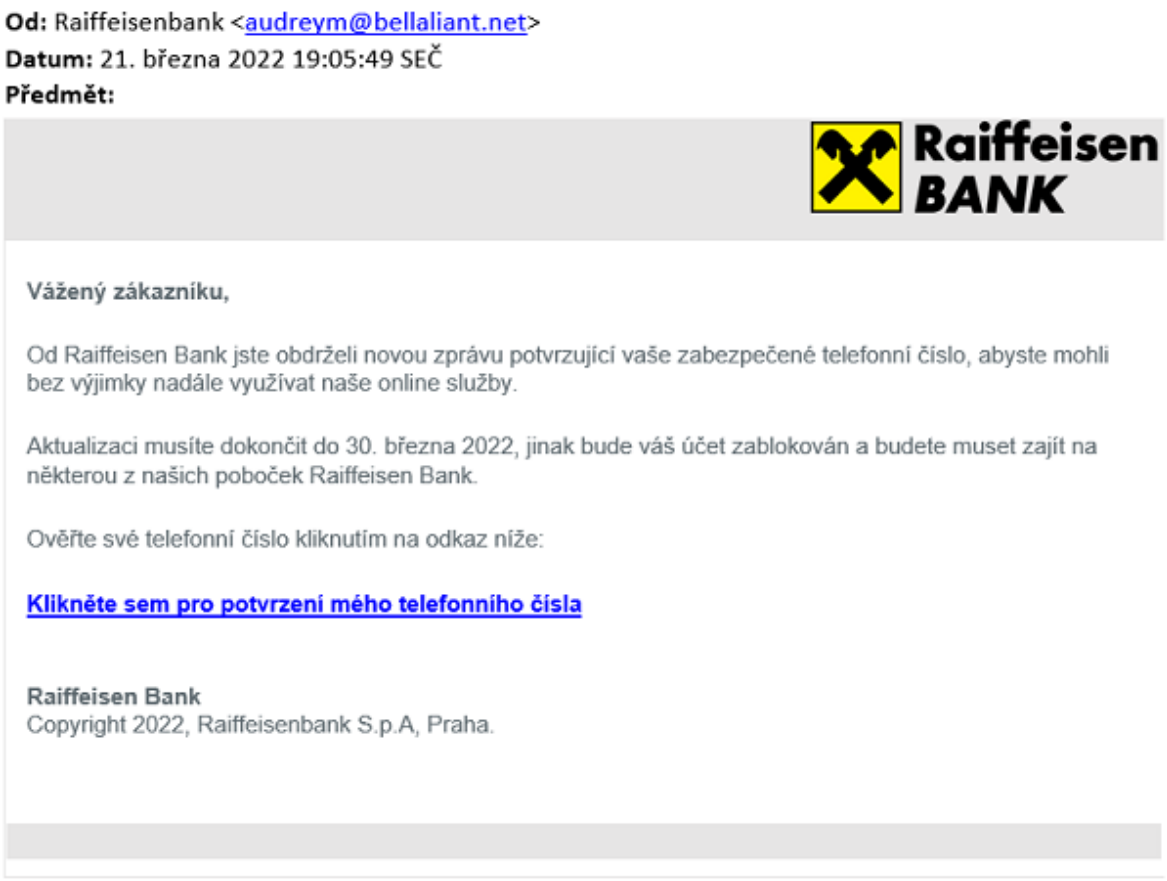
Jednou z nejpoužívanějších technik sociálního inženýrství je tzv. Phishing. Tento výraz se používá pro „*podvodné či klamavé jednání, jehož cílem je získat informace o uživateli, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN aj.“* [8]

Ve světě informačních technologií je tato technika útočníky ve velké míře využívána, jelikož útočníkům v kyberprostoru umožňuje šířit podvodné zprávy velkému množství potenciálních obětí a s minimálním vynaloženým úsilím oproti světu reálnému. Nejčastěji se s phishingem uživatelé setkávají v emailových zprávách. Email, který útočníci odešlou se tváří například jako důležitá zpráva z banky, pojišťovny či jiné důvěryhodné společnosti a vyzývá ke kliknutí na odkaz, který je součástí této zprávy. Zpravidla je uživatel vyzýván ke změně hesla kvůli možnému napadení jeho účtu apod. Jakmile uživatel tento odkaz navštíví, dostává se na podvrženou webovou stránku, která bývá takřka identická s originální webovou stránkou dané společnosti. Jakmile uživatel na této podvržené webové stránce vyplní své uživatelské údaje, stává se obětí úspěšného phishingového útoku. Tyto uživatelské údaje jsou následně odeslány útočníkům, kteří pak získávají přístup k účtu oběti a dochází k odcizení finančních prostředků. [8]



Obr. 12. Phishingový email vydávající se za ČSOB [41]

Na výše uvedeném snímku z emailové schránky lze pozorovat, že útočníci používají ke zvýšení důvěryhodnosti logo Československé obchodní banky. Email vyzývá uživatele ke kliknutí na odkaz a k ověření telefonního čísla, díky čemuž může provádět nákupy a transakce online. Po důkladnějším prozkoumání tohoto podvodného emailu si lze všimnout množství gramatických chyb, které by měly potenciální oběť odradit ke kliknutí a podlehnutí této hrozby. Taktéž si lze všimnout podezřelého odesílatele tohoto emailu, který s ČSOB jistě nemá nic společného.



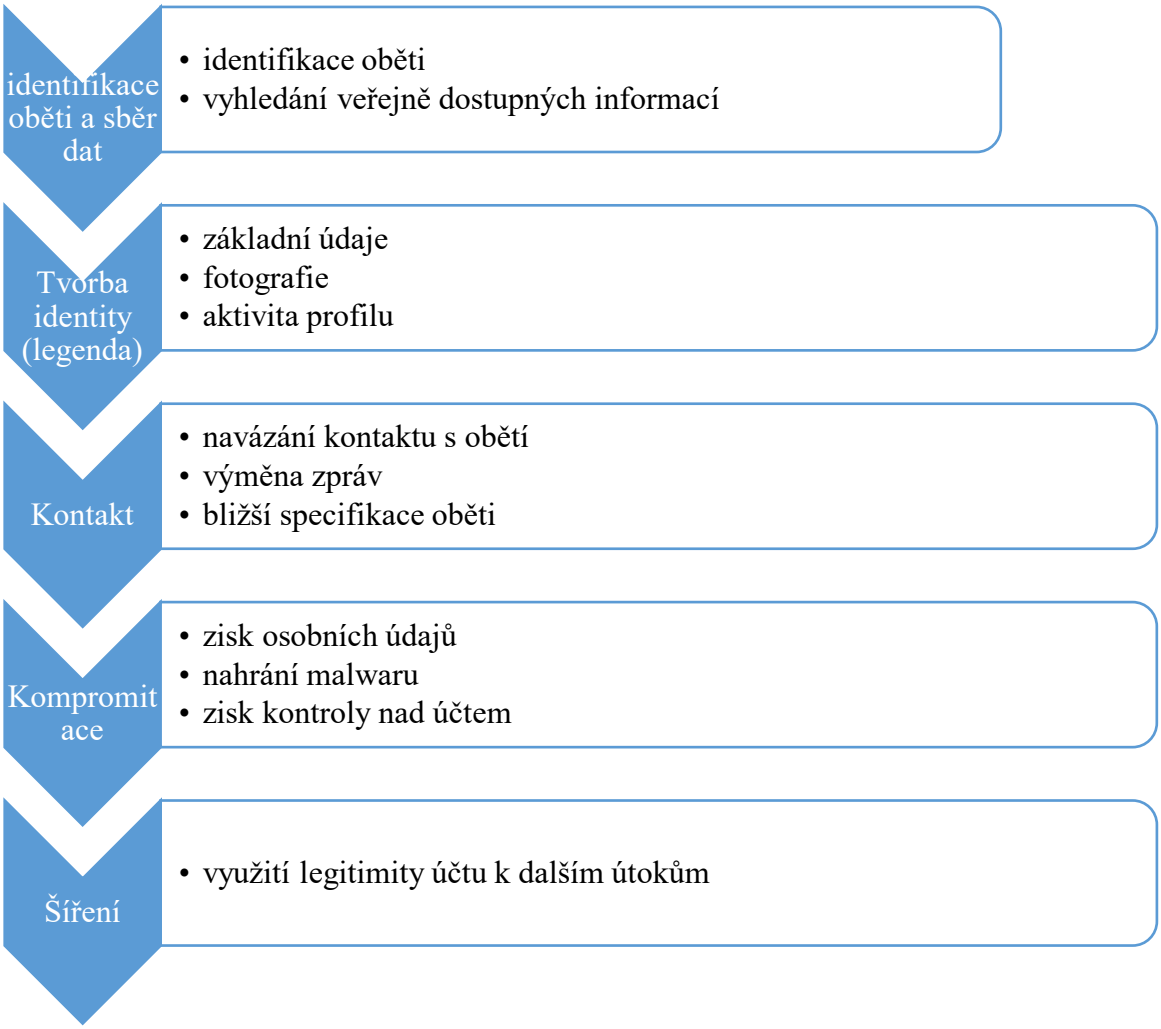
Obr. 13. Phishingový e-mail z 21. 3. 2022 (Raiffeisenbank) [42]

Phishingový email z 21. 3. 2022, který obdržel klient Raiffeisenbank vyzývá ke kliknutí na odkaz z důvodu potvrzení telefonního čísla. Tentokrát je potenciální oběť vystavena i výhrůžce zablokování účtu, pokud danou akci neprovede do určitého data. Toto může v uživateli vyvolat pocit strachu, kdy pod nátlakem neuváženě na daný odkaz klikne a na podvržené webové stránce vyplní požadované údaje, které se následně přepošlou útočníkovi.

3.2 Spear phishing

Spear phishing se oproti klasickému phishingu vyznačuje tím, že je tento útok cílený na konkrétní organizaci či konkrétního uživatele. Škody způsobené tímto typem útoku se ročně pohybují řádově v desítkách až stovkách miliard korun. Útoky bývají velice sofistikované a mnohdy je i pro zkušeného uživatele problém odhalit, že se jedná o falešnou emailovou zprávu či zprávu v chatovacích aplikacích. Motivací útočníků je ve většině případů finanční zisk.

3.2.1 Fáze spear phishingu



Obr. 14. Fáze spear phishingu [43]

Identifikace oběti a sběr dat

Dříve, než dojde k samotnému spear phishingovému útoku, je ze strany útočníka potřeba identifikovat konkrétní osobu nebo skupinu v cílové organizaci, na kterou bude útok směřován. K tomto kroku lze využít sociální sítě, kde lidé často ve svých profilech uvádí svého zaměstnavatele a další citlivé informace. Právě díky těmto a dalším veřejným informacím, např. z webových stránek zaměstnavatele, lze identifikovat jednotlivé zaměstnance či skupinu a zahájit spear phishingovou kampaň. Snahou útočníků je zjistit co nejvíce informací o dané osobě či skupině. Jedná se především o emailové adresy, telefonní čísla, zájmy, přátele či rodinné příslušníky. Čím více informací o konkrétním zaměstnanci či skupině útočníci před útokem zjistí, tím větší je pravděpodobnost úspěchu tohoto typu útoku, jelikož mohou vytvořit útok tzv. na míru.

Legenda

Jakmile útočníci sesbírají dostatek informací a podkladů pro útok, je třeba sestavit příběh „na míru“ například formou emailu či zprávy na sociálních sítích, na základě informací sesbíraných v předchozí fázi.

Při spear-phishingových útocích útočníci zakládají falešné emailové schránky či důvěryhodně vypadající profily na sociálních sítích, které pak používají ke komunikaci s obětí. Cílovým stavem je nevzbudit zprávou či emailem u oběti podezření a přimět k otevření přílohy, která je součástí tohoto na míru vytvořeného příběhu.

Kontakt

Jakmile útočníci získají dostatečný počet podkladů, na základě kterých sestaví důvěryhodnou legendu, dochází k navázání kontaktu s obětí. Jak již bylo zmíněno v předchozím kroku, jedná se zpravidla o email s přílohou obsahující malware. V případě sociálních sítí pak žádost o přátelství či zpráva v chatovací aplikaci.

„Neodhalitelná spear-phishingová“ zpráva by měla splňovat náležitosti, které jsou běžné v rámci dané organizace, jako je tykání, vykání, podpis a správný formát emailové adresy.

Kompromitace

Tato fáze je v podstatě vyvrcholení celé akce. Jestliže po fázi kontaktu útočníka dojde k otevření infikované přílohy a antivirová ochrana na zařízení oběti tuto hrozbu nezaregistruje, dojde ke kompromitaci daného systému. Hojně využívaným malwarem je tzv. Remote Access Trojan, který útočníkům umožní vzdálený přístup do zařízení a tím pádem i plnou kontrolu infikovaného zařízení. Ze strany útočníků pak jednoduše probíhají krádeže dat a instalace dalšího škodlivého kódu, např. oblíbeného ransomware.

Šíření

Pro útočníky je důležité, aby se škodlivý kód v zařízení začal šířit po síti dané organizace a infikoval tak další zařízení, ze kterých je možno získávat další data, instalovat malware, či je používat k autentické spear-phishingové komunikaci s dalšími zaměstnanci. [43]

3.3 Pharming

Pharming útoky představují jednu z nejnebezpečnějších forem phishingu, jelikož při nich dochází k napadení DNS serveru, který slouží k překládání doménového jména na IP adresu. Uživatel, který zadá ve svém internetovém prohlížeči určitou webovou adresu je pak přesměrován na adresu webového serveru, kde se nachází podvržená webová stránka, která je k věrnou imitací originální stránky. Jakmile na této webové adrese uživatel zadá přihlašovací údaje, dostávají se do rukou útočníka, který je dále využije ke své další trestné činnosti. Pharming útok se dá realizovat i napadením koncového zařízení uživatele pomocí malware, kdy dochází ke změnám v souboru hostitelů. [8]

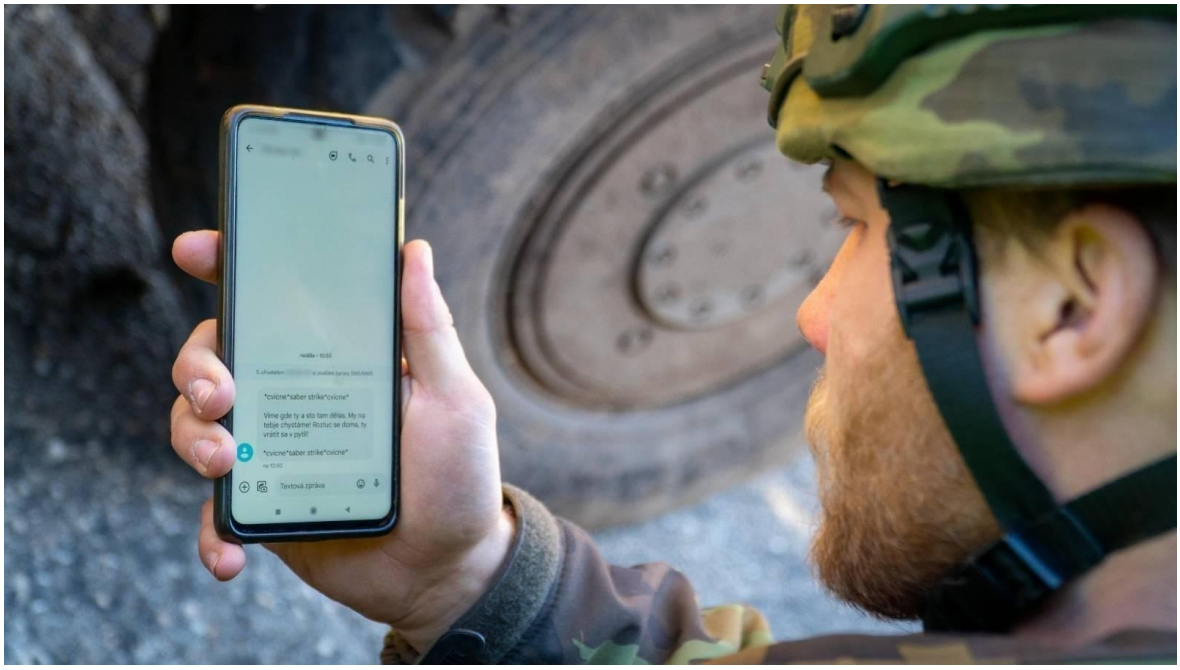
3.4 Vishing

Za tzv. Vishing je považována forma phishingu, kdy je k získání citlivých údajů či provedení určité akce využíváno telefonního hovoru. Útočníci se při tomto hovoru, pro zvýšení důvěryhodnosti představují jako pracovníci bankovních společností či jiných institucí. [8]

3.5 SMiShing

Smishing je forma phishingu, při které se k distribuci podvodných zpráv využívají SMS zprávy. Především se jedná o zprávy, které uživatele vyzývají k zavolání na placené linky či kliknutí na podvodné URL adresy, popřípadě provedení jiné akce. [8]

V rámci armádního cvičení Saber Strike 2022 byly právě SMS zprávy využity k otestování odolnosti příslušníků AČR proti sociálnímu inženýrství. SMS zprávy s různými výzvami či výhružkami týkajících se vyzrazení pozice, opuštění prostoru aj., byly rozesílány prostřednictvím Velitelství informačních a kybernetických sil především příslušníkům ve velitelských funkcích. [27]



Obr. 15. Sociální inženýrství v praxi – AČR [44]

Na obrázku výše se jednalo o výhružnou SMS s textem: „*Víme gde ty a sto tam dělas, My na tebje chystáme! Rozluc se doma, ty vrátit se v pytli!*“

Cílem tedy bylo touto formou sledovat reakce a chování jednotlivých příslušníků AČR, kteří tyto SMS obdrželi. Dle sdělení VeKySIO se vojáky tzv. zlomit nepodařilo a sociotechnickým útokům sociálního inženýrství odolali. [27]

3.6 Dezinformace a deepfakes

Dezinformace či fake news, jsou výrazy pro záměrně nepravdivé zprávy, které se šíří především v médiích s cílem manipulovat s veřejným míněním a uváděním diváka či čtenáře v omyl.

Příkladem dezinformací mohou být v dnešní době podvržená videa či fotografie z války na Ukrajině s cílem ovlivnění vojenského konfliktu. Dezinformace mohou mít za následek demoralizaci a destabilizaci společnosti, čímž se dá dosáhnout různých politických či ekonomických rozvratů bez pomoci vojenských prostředků. Dezinformační vlny audiovizuálního obsahu týkající se války na Ukrajině měly za cíl [45]

Obr. 16. Screenshot z dezinformačního videa – údajný přelet vojenských letounů nad Ukrajinou [46]

Masivně šířené video na sociálních sítích s komentářem o náletech ruských stíhacích letounů na Ukrajinu a začínající 3. světové válce. Stejné video však bylo nahráno na portál YouTube již v květnu v roce 2020. Jednalo se o video z příprav na vojenskou přehlídku v Moskvě. [45]

Tzv. Deepfake je výraz pro relativně novou formu kyberkriminality a sociálního inženýrství. Jedná se o falešná videa vytvořená počítačem za pomoci umělé inteligence a strojového učení. V prvopočátku, kdy tato technologie nebyla tolik vyvinutá, nebylo složité takto podvržené video odhalit ani pro naprostého laika. V dnešní době jsou však Deepfake videa

poměrně kvalitně zpracována a běžný divák si tak nemusí všimnout detailů, kterých si všimne odborník. Deepfake byl využit například na videu s Barrackem Obamou, kdy vulgárně mluvil o prezidentu Spojených států amerických Donaldu Trumpovi nebo video s Markem Zuckerbergerem, kde se vyjadřuje ohledně ovládání miliard lidí pomocí ukradených dat. [47] Aktuálně jsou deepfake videa využívána jako součást informační války vzhledem k vojenskému konfliktu na Ukrajině.

Obr. 17. Deepfake video ukrajinského prezidenta Volodymyra Zelenského (vlevo) a záběr z reálného videa (vpravo) [48]

Z výše uvedeného snímku lze poměrně snadno rozpoznat, že se jedná o podvržené deepfake video, avšak pro určitou skupinu diváků, kteří mají problémy se zrakem či starší generace, které o těchto technologiích nemají ponětí, se může jevit jako nepodvržené a mohou tak snadno manipulaci podlehnout.

4 EXPERIMENT SOCIÁLNÍHO INŽENÝRSTVÍ V RÁMCI CVIČENÍ NATO

Během nejmenovaného armádního cvičení Severoatlantické aliance (NATO) v uplynulých letech byl skupinou vědců, za souhlasu velení, proveden experiment zaměřený na sociální inženýrství a získávání dat z otevřených zdrojů (open-source) o cvičících jednotkách a jejich jednotlivých členů armády.

Cílem tohoto 3-4 týdny trvajícího experimentu bylo zjistit, zda je možné za pomoci sociálního inženýrství a získaných dat přimět jednotky či jednotlivé vojáky například opustit své pozice, neplnit rozkazy či získat informace, které by neměly být vyzrazeny.

V rámci tohoto experimentu bylo týmem vědců využito metodiky sociálního inženýrství, falešných profilů a skupin na sociálních sítích, získávání dat z veřejných profilů jednotlivých příslušníků cvičení.

Sběr dat probíhal převážně pomocí monitoringu profilů příslušníků cvičení na sociálních sítích Facebook, Instagram a Twitter. Informací o jednotlivých cvičících a probíhajícím cvičení bylo zjištěno nečekaně velké množství. Pomocí falešných profilů a podvržených skupin na Facebooku bylo možno zjistit takřka celou cvičící jednotku včetně vlastních pozic a informací o aktivních fázích cvičení.

Jako největší zdroj aktuálních informací o jednotkách a jednotlivých příslušníků byla sociální síť Instagram, kde vojáci sdíleli fotografie, stories a bylo tak v několika případech snadné identifikovat jejich polohu.

Vojáci, na které byly použity techniky sociálního inženýrství, o sobě sdělili daleko větší množství informací, než které byl tým vědců schopný získat ze sociálních sítí a profilů těchto příslušníků. Pomocí technik sociálního inženýrství se podařilo získat jejich polohu s přesností na jeden kilometr, a to včetně jejich nadřízených prvků. K dalším informacím, které se vědcům podařilo v rámci tohoto experimentu získat, byly telefonní čísla, emailové adresy či fotky vybavení jednotek. [49]

Z tohoto experimentu je zřejmé, že problematika odolnosti příslušníků silových složek proti sociálnímu inženýrství je poměrně klíčová záležitost, na kterou je třeba adekvátně reagovat a neustále rozšiřovat povědomí o těchto kybernetických hrozbách.

II. PRAKTICKÁ ČÁST

5 KYBERNETICKÉ BEZPEČNOSTNÍ UDÁLOSTI A INCIDENTY V RESORTU MO

Ve spolupráci s centrem CIRC, bude na základě dat o kybernetických bezpečnostních událostech a incidentech sesbíraných za určité časové období provedena praktická část této diplomové práce. Jelikož se uživatelů v rámci Ministerstva obrany a AČR týká používání chytrých služebních telefonů, tabletů a počítačů s přístupem do sítě internet, dotýká se těchto uživatelů problematika kybernetických hrozeb, zejména sociálního inženýrství. Výstup ze získaných dat je z 4. kvartálu předešlého roku 2021, resp. říjen–prosinec. Data, která budou v této diplomové práci použita, budou reprezentována obecně, bez bližší specifikace kybernetických incidentů (jména uživatelů či účtů).

5.1 Kybernetické bezpečnostní událostí a incidenty za říjen 2021

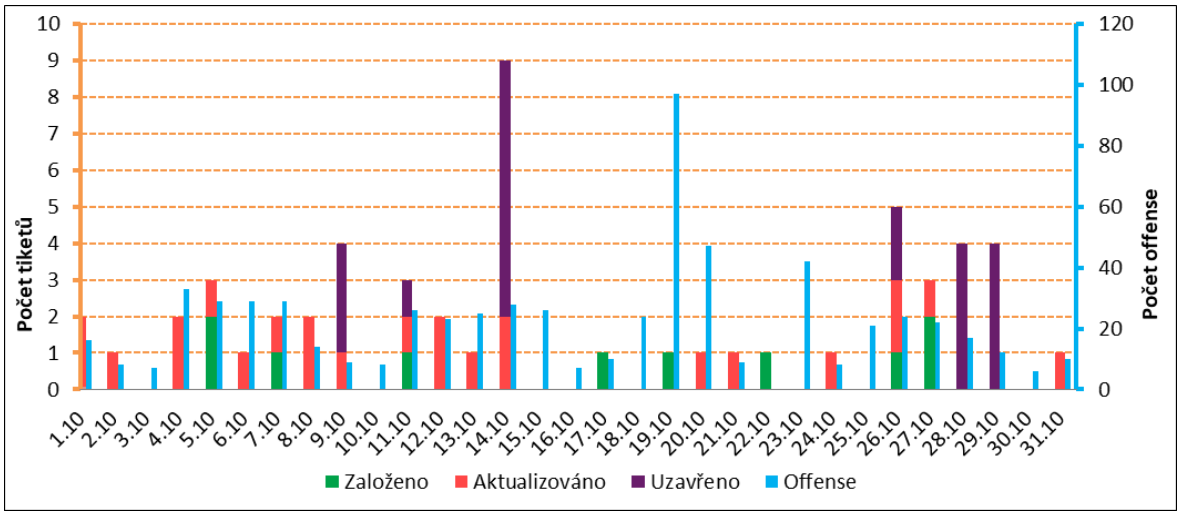
V následující tabulce jsou zobrazeny počty založených, aktualizovaných a uzavřených tiketů v měsíci říjnu 2021 včetně počtu řešených kybernetických bezpečnostních událostí (KBU) a kybernetických bezpečnostních incidentů (KBI).

„V případě, že bezpečnostní událost způsobí narušení bezpečnosti informací v informačním systému nebo narušení dostupnosti a spolehlivosti služeb poskytovaných informačním systémem, je povyšována na kybernetickou bezpečnostní událost nebo kybernetický bezpečnostní incident.“ [zdroj: CIRC]

Tab. 1. Počty řešených bezpečnostních událostí v říjnu 2021 [zdroj: CIRC]

Počet řešených bezpečnostních událostí	Založeno tiketů	10
	Aktualizováno tiketů	24
	Uzavřeno tiketů	21
Počet řešených podezřelých událostí	666	
Počet řešených KBU	0	
Počet řešených KBI	1	

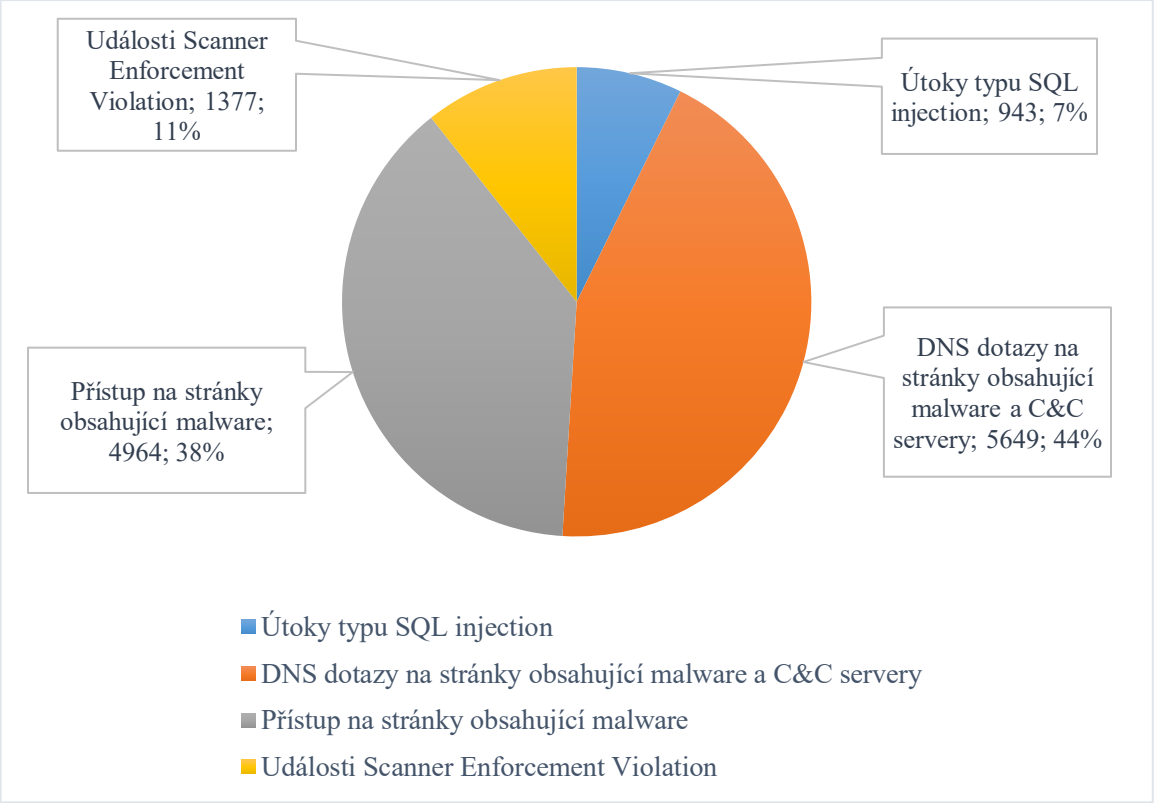
Jak je z tabulky výše patrné, opravdu ke kybernetickým útokům na uživatele v rámci MO dochází. Proto je třeba prvek, jako je CIRC podporovat a udržovat v činnosti.



Obr. 18. Graf počtů řešených bezpečnostních událostí (říjen) [zdroj: CIRC]

V měsíci říjnu bylo operátory centra CIRC řešeno 666 podezřelých událostí, což je v průměru 21 kybernetických událostí během jednoho dne v rámci resortu MO. Tikety, které byly uživateli založené a aktualizované se týkaly především phishingových e-mailů v rámci sítě PD IMO, či přístupu uživatelů na webové odkazy s malwarem, těžby kryptoměn apod.

5.1.1 Neúspěšné kybernetické útoky na infrastrukturu AČR (říjen 2021)



Obr. 19. Neúspěšné kybernetické útoky na infrastrukturu AČR z veřejného internetu (říjen) [zdroj: CIRC]

V daném měsíci došlo ke zvýšení počtu událostí spojených s útoky typu SQL Injection. Hodnoty kopírují trend jednotlivých měsíců roku 2021. Většina pokusů o využití různých zranitelností byla blokována bezpečnostními technologiemi využívaných v rámci MO.

5.1.2 Vyhodnocení (říjen 2021)

V měsíci říjnu došlo k jednomu kybernetickému bezpečnostnímu incidentu (KBI), který se týkal kompromitace e-mailové schránky uživatele na doméně @army.cz. Uživatel se stal obětí sociálního inženýrství – phishingového e-mailu. Po rozkliknutí odkazu v daném e-mailu došlo k přesměrování na podvrženou webovou stránku, kde uživatel vyplnil své přihlašovací údaje. Tímto došlo ke kompromitaci emailové schránky uživatele a útočníci využili tuto napadenou emailovou schránku k rozesílání spamových zpráv.

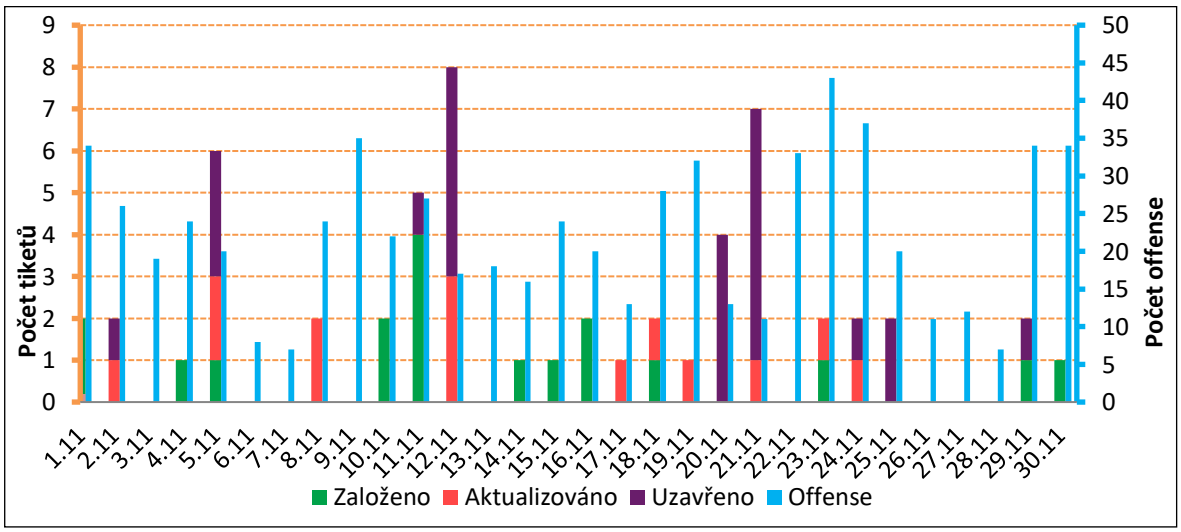
5.2 Kybernetické bezpečnostní události a incidenty za listopad 2021

V následující tabulce jsou zobrazeny počty založených, aktualizovaných a uzavřených tiketů v měsíci listopadu 2021, včetně počtu řešených kybernetických bezpečnostních událostí (KBU) a kybernetických bezpečnostních incidentů (KBI).

Tab. 2. Počty řešených bezpečnostních událostí v listopadu 2021 [zdroj: CIRC]

Počet řešených bezpečnostních událostí	Založeno tiketů	18
	Aktualizováno tiketů	14
	Uzavřeno tiketů	24
Počet řešených podezřelých událostí	669	
Počet řešených KBU	1	
Počet řešených KBI	1	

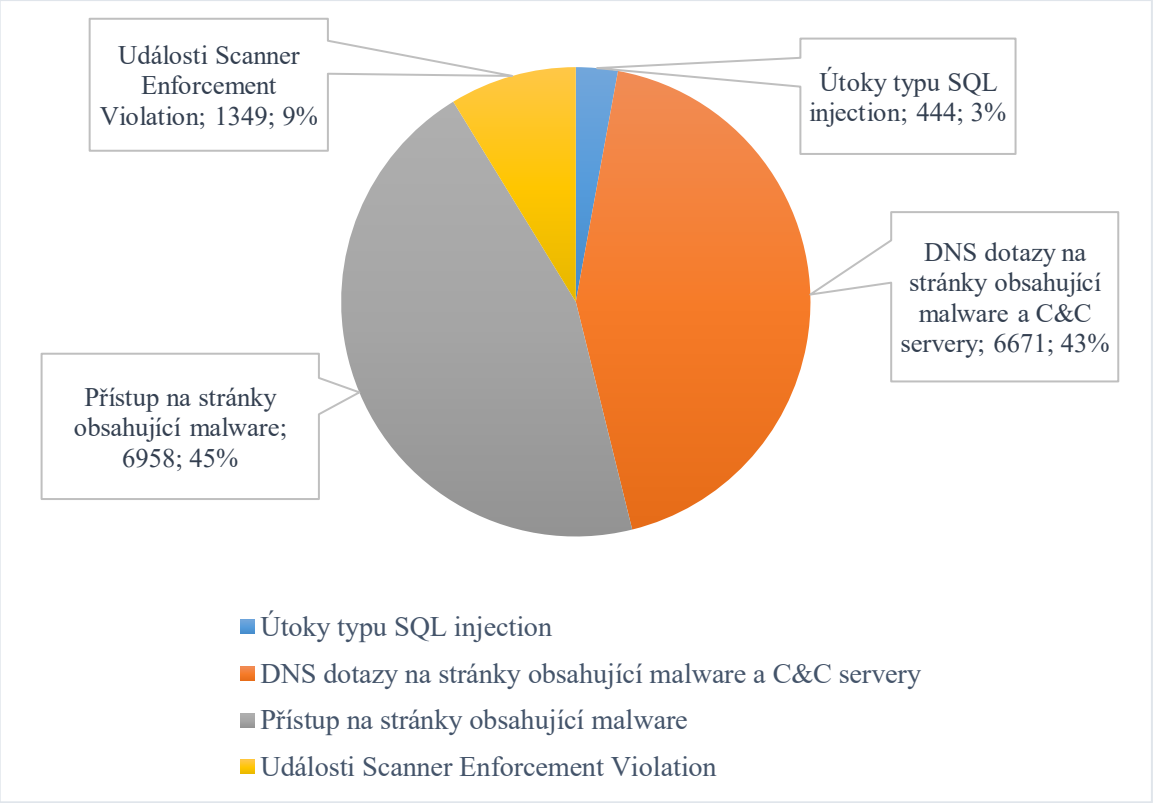
Oproti předešlému měsíci došlo k velmi mírnému nárustu počtu řešených podezřelých událostí. Celkem bylo operační směnou CIRC řešeno 669 podezřelých událostí. Z počtu 669 podezřelých událostí došlo klasifikaci jednoho KBU a jednoho KBI.



Obr. 20. Graf počtu řešených bezpečnostních událostí (listopad) [zdroj: CIRC]

Založené a aktualizované tikety se opět týkaly především phishingových e-mailů a prověřování tzv. indikátorů kompromitace (IP adresy, URL a domény, hashe).

5.2.1 Neúspěšné kybernetické útoky na infrastrukturu AČR (listopad 2021)



Obr. 21. Neúspěšné kybernetické útoky na infrastrukturu AČR z veřejného internetu (listopad) [zdroj: CIRC]

Z grafu výše je patrné, že došlo ke snížení počtu útoků typu SQL Injection. Zároveň došlo ke zvýšení počtu navštívených webových stránek, které obsahovaly malware a růst byl taktéž zaznamenán DNS dotazech na C&C servery (botnet).

5.2.2 Vyhodnocení (listopad 2021)

V tomto měsíci došlo k řešení jedné kybernetické bezpečnostní události (KBU) týkající se zneužití přístupu ke služebnímu PC uživatele „XY“. KBU se týkala možné kompromitace armádního systému ŠIS, což však bylo po analýze vyvráceno. Při této KBU došlo ke zneužití služebního PC ke krádeži prostředků z bankovního účtu uživatele. Uživatel byl útočníkem za pomocí technik sociálního inženýrství přesvědčen ke zpřístupnění údajů o své platební kartě a umožnil útočníkům vzdálený přístup k zařízení. Při tomto útoku došlo ke krádeži finančních prostředků, ale nedošlo ke kompromitaci služebních dat či sítě.

Vzhledem k předchozímu měsíci, kdy došlo ke kybernetickému bezpečnostnímu incidentu (KBI) týkajícího se kompromitace schránek na doméně @army.cz, bylo zasláno aktualizační hlášení a ukončení analýzy útoku ze strany CIRC.

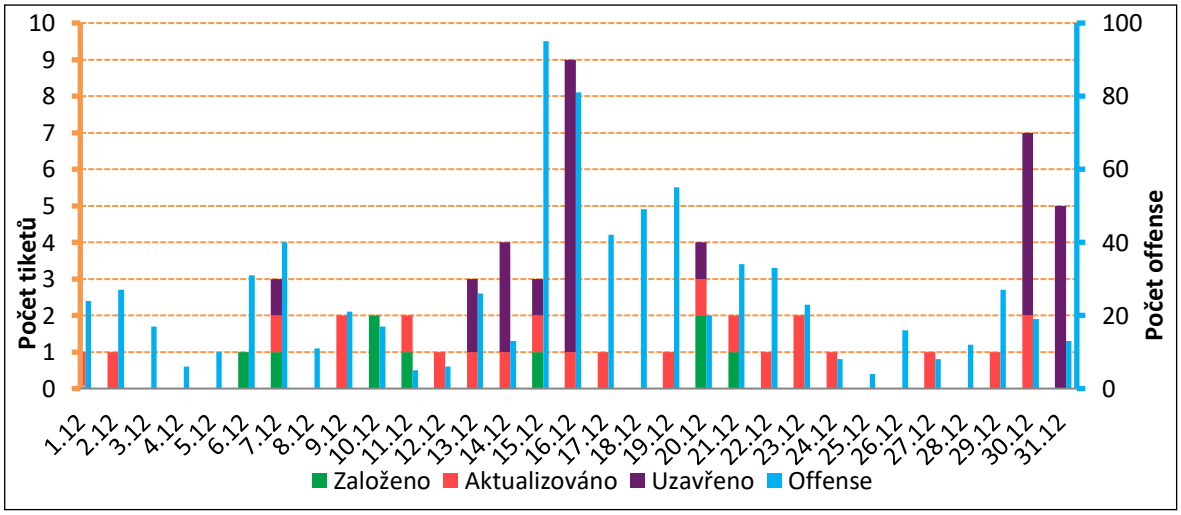
5.3 Kybernetické bezpečnostní událostí a incidenty za prosinec 2021

V následující tabulce jsou zobrazeny počty založených, aktualizovaných a uzavřených tiketů v měsíci prosinci 2021, včetně počtu řešených kybernetických bezpečnostních událostí (KBU) a kybernetických bezpečnostních incidentů (KBI).

Tab. 3. Počty řešených bezpečnostních událostí v prosinci 2021 [zdroj: CIRC]

Počet řešených bezpečnostních událostí	Založeno tiketů	9
	Aktualizováno tiketů	23
	Uzavřeno tiketů	26
Počet řešených podezřelých událostí	793	
Počet řešených KBU	0	
Počet řešených KBI	0	

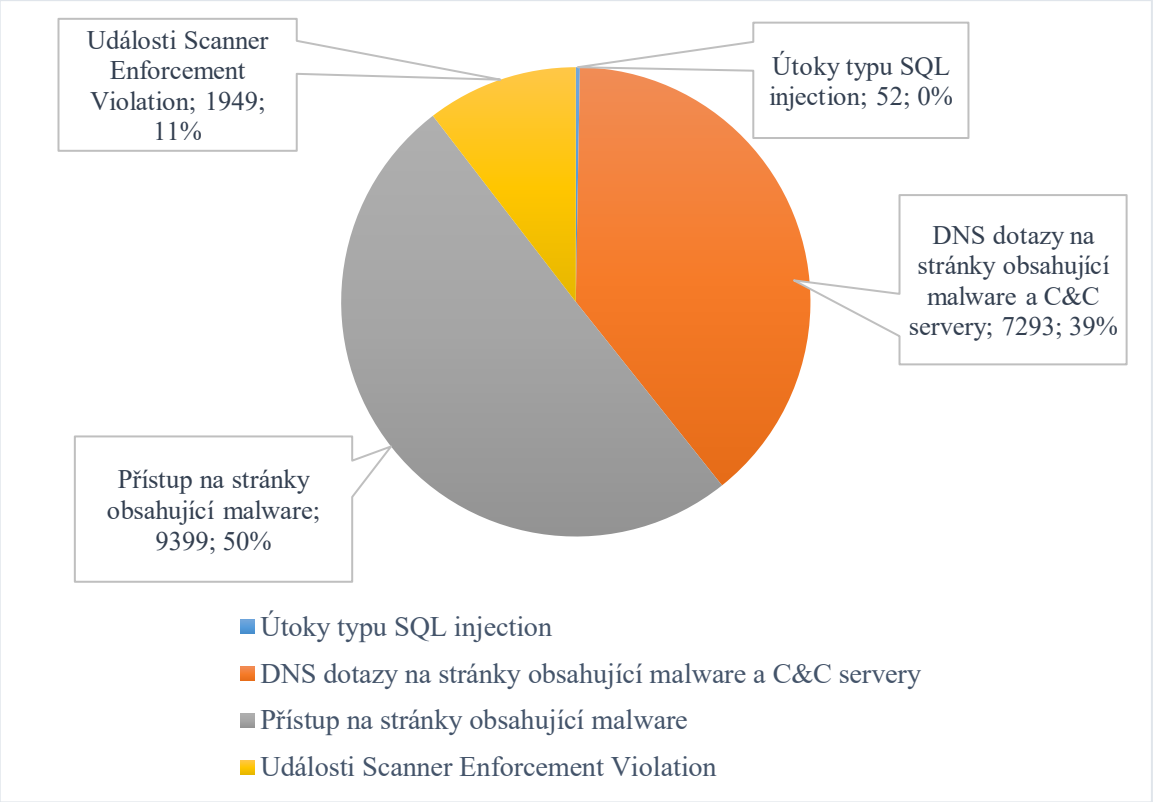
Z hlediska počtu řešených bezpečnostních událostí za 4. kvartál 2021 se jedná o nejvyšší počet, avšak paradoxně v tomto měsíci nedošlo ke zjištění žádné KBU ani KBI.



Obr. 22. Graf počtů řešených bezpečnostních událostí (listopad) [zdroj: CIRC]

Celkem bylo operační směnou CIRC řešeno 793 bezpečnostních událostí. Založené a aktualizované tikety se týkaly především phishingových e-mailů, nestandartní síťové komunikace na uživatelských stanicích (přístup na URL obsahující malware či cryptomining apod.). V neposlední řadě pak zjištěných zranitelností a prověřování indikátorů kompromitace.

5.3.1 Neúspěšné kybernetické útoky na infrastrukturu AČR (prosinec 2021)



Obr. 23. Neúspěšné kybernetické útoky na infrastrukturu AČR z veřejného internetu (prosinec) [zdroj: CIRC]

Z grafu je patrné, že došlo oproti předcházejícím měsícům o výrazný pokles v počtech událostí spojenými s útoky typu SQL Injection. Hodnoty jsou značně ovlivněny aktuálními zranitelnostmi v systémech a jejich opatřeními.

5.3.2 Vyhodnocení (prosinec 2021)

Z hlediska kybernetických bezpečnostních událostí (KBU) a kybernetických bezpečnostních incidentů (KBI) byl prosinec měsícem, kdy centrum CIRC neřešilo žádnou KBU ani KBI i přes nejvyšší počet řešených podezřelých událostí viz.

Tab. 3. Počty řešených bezpečnostních událostí v prosinci 2021.

5.4 Vyhodnocení kybernetické bezpečnosti za 4. kvartál 2021

V tabulce níže je shrnutí počtu řešených tiketů a bezpečnostních událostí za období třetího kvartálu 2021 (říjen–prosinec), včetně počtu řešených kybernetických bezpečnostních událostí (KBU) a kybernetických bezpečnostních incidentů (KBI).

Tab. 4. Počty řešených bezpečnostních událostí v 4. kvartálu 2021 [zdroj: CIRC]

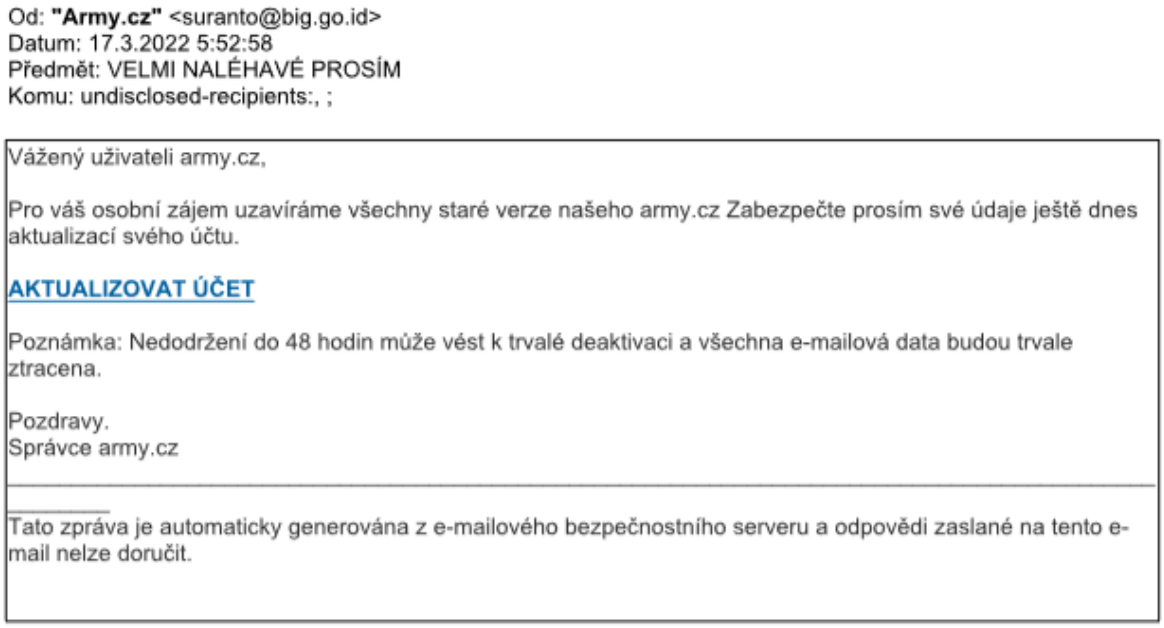
Počet řešených bezpečnostních událostí	Založeno tiketů	37
	Aktualizováno tiketů	61
	Uzavřeno tiketů	71
Počet řešených podezřelých událostí	2128	
Počet řešených KBU	1	
Počet řešených KBI	1	

Celkem bylo operační směnou CIRC v tomto tříměsíčním období řešeno 2128 podezřelých událostí, z čehož byl 1x KBU a 1x KBI.

Jak již bylo v předchozích vyhodnoceních zmíněno, jedna řešená KBU se týkala zneužití přístupu ke služebnímu PC uživatele, kdy však nedošlo, po analýze, ke kompromitaci služebních dat ani sítě, tudíž se nejednalo o KBI. Došlo však ke krádeži blíže nespecifikovaných finančních prostředků z bankovního účtu daného uživatele. Z hlediska KBI se v tomto období týkalo kompromitace služebních emailových schránek na doméně @army.cz, kdy byly tyto zneužité schránky použity k šíření spamu.

5.4.1 Příklad phishingového emailu a webové stránky 1.

Na obrázcích níže jsou zobrazeny příklady phishingových emailů a webových stránek cílených na příslušníky AČR.



Od: **"Army.cz"** <suranto@big.go.id>
Datum: 17.3.2022 5:52:58
Předmět: VELMI NALÉHAVÉ PROSÍM
Komu: undisclosed-recipients:, ;

Vážený uživateli army.cz,

Pro váš osobní zájem uzavíráme všechny staré verze našeho army.cz Zabezpečte prosím své údaje ještě dnes aktualizací svého účtu.

AKTUALIZOVAT ÚČET

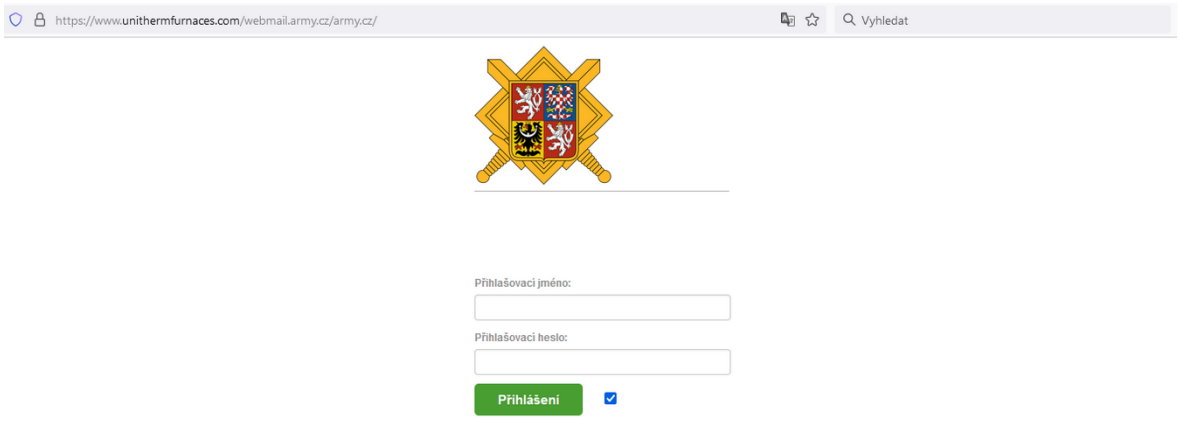
Poznámka: Nedodržení do 48 hodin může vést k trvalé deaktivaci a všechna e-mailová data budou trvale ztracena.

Pozdravy.
Správce army.cz

Tato zpráva je automaticky generována z e-mailového bezpečnostního serveru a odpovědi zaslané na tento e-mail nelze doručit.

Obr. 24. Phishingový email cílený na příslušníky AČR [zdroj: CIRC]

Email ze dne 17. 3. 2022 obdrželo několik příslušníků AČR využívající emailové schránky na doméně @army.cz. Podvržená emailová zpráva vybízela uživatele k co nejrychlejší aktualizaci údajů pomocí odkazu, který směřoval na podvrženou webovou stránku s formulářem pro změnu hesla viz. obrázek níže.



Obr. 25. Phishingová webová stránka pro změnu hesla [zdroj: CIRC]

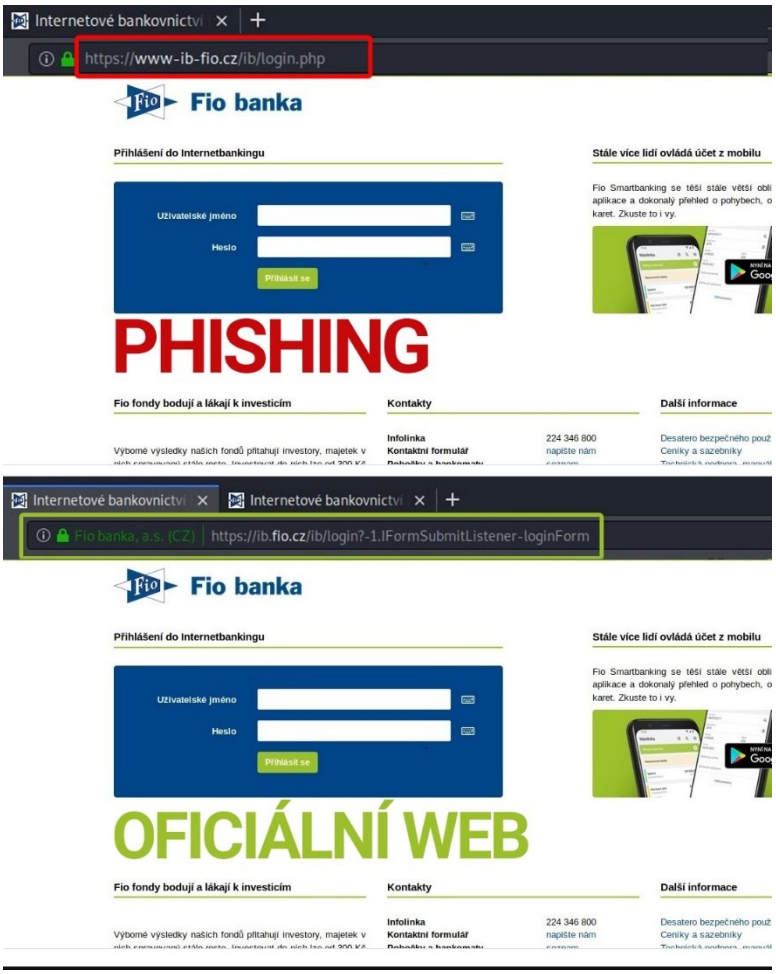
V případě kliknutí na odkaz uvedený v podvodném emailu byl uživatel přesměrován na adresu www.unitherfurnaces.com/webmail.army.cz/army.cz, která očividně nemá s oficiální doménou army.cz nic společného. Útočníci se však snažili uživatele přesvědčit k provedení změny údajů reálným logem AČR, které umístili nad formulář pro přihlášení.

5.4.2 Příklad phishingového emailu a webové stránky 2.

Dalším příkladem phishingu byl email cílený na příslušníky MO s emailovou schránkou opět na doméně @army.cz. Znění e-mailu: *„Na váš účet Fio bylo dočasně zablokováno, dokud nepotvrdíte svou identitu kliknutím sem.“*

Po rozkliknutí emailu byl uživatel přesměrován na stránky, které vypadaly identicky s oficiální, nepodvrženou přihlašovací stránkou Fio banky s rozdílem pomlček v doméně.

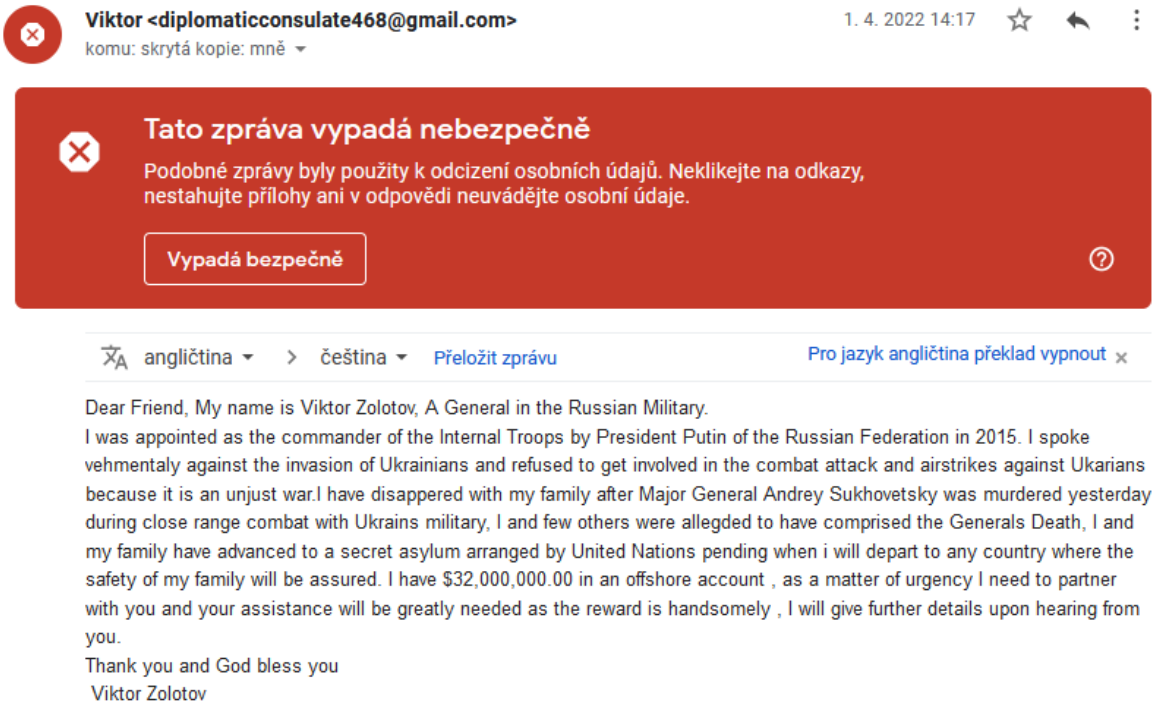
Oficiální doména Fio banky a přihlašovací webová stránka je ve znění – www.ib.fio.cz, avšak podvržená webová stránka používala webovou stránku na doménovém názvu www-ib-fio.cz.



Obr. 26. Phishing vs. oficiální webová stránka [zdroj: CIRC, upraveno Rožek 2022]

5.4.3 Příklad phishingového emailu 3.

Vzhledem k aktuální situaci s válečným konfliktem na Ukrajině dochází k šíření podvodných emailů využívající této situace. Email, který mi byl do emailové schránky doručen, má být od jistého generála ruské armády Viktora Zolotova prostřednictvím záměrně vytvořené emailové schránky diplomaticconsulate468@gmail.com, vydávající se za „diplomatický konzulát“. V emailu jsem tímto generálem, který musel kvůli nesouhlasu s válečným konfliktem a neuposlechnutí rozkazů utéct z Ruska, vyzýván ke spolupráci a zajištění bezpečí jeho rodiny v naší zemi, výměnou za finanční odměnu.



Obr. 27. Podvodný email doručený do osobní emailové schránky [archiv autora]

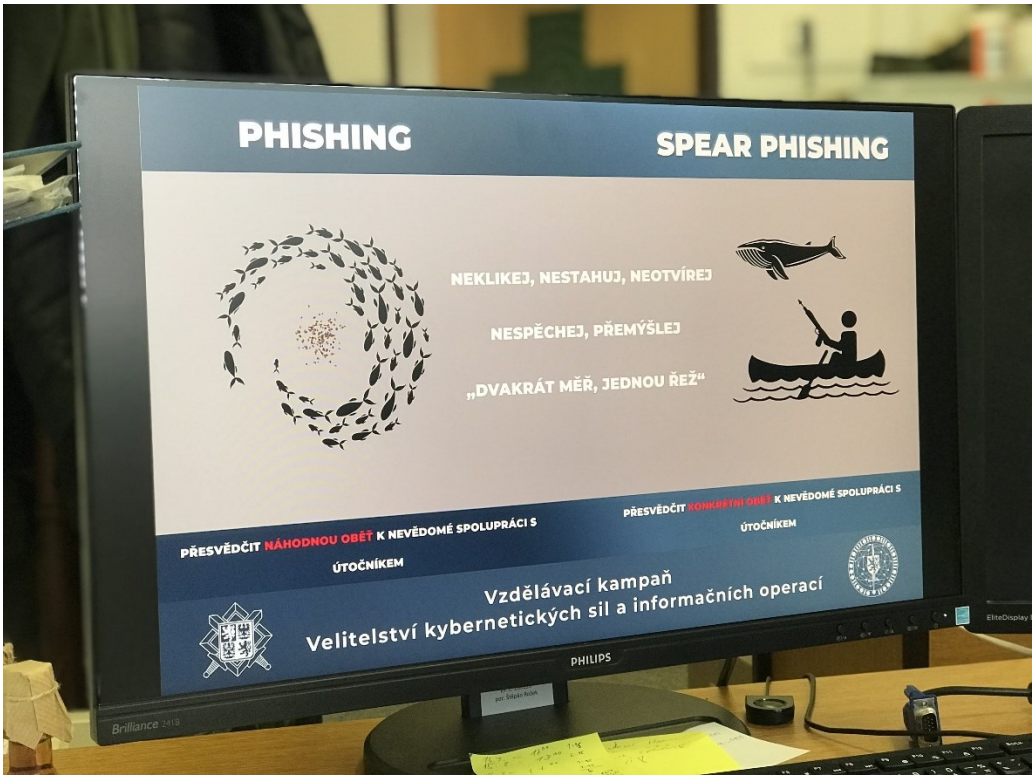
Při kladné reakci na tuto zprávu by se dal očekávat navazující email k uhrazení letenek, či jiných nezbytných nákladů. V případě, že by k úhradě požadujících finančních prostředků došlo, byla by pravděpodobně komunikace ze strany „útočníka“ ukončena anebo naopak stupňována tak, aby docházelo k další nezbytné finanční pomoci.

Na obrázku lze pozorovat, že bezpečnostní algoritmy emailového klienta upozornili na možné bezpečnostní riziko tohoto emailu.

6 ZVYŠOVÁNÍ ODOLNOSTI PŘÍSLUŠNÍKŮ AČR PROTI SOCIÁLNÍMU INŽENÝRSTVÍ

Vzhledem ke vzrůstajícímu počtu případů kybernetické kriminality se v rámci AČR za podpory Velitelství kybernetických sil a informačních operací vytvořila vzdělávací kampaň, která cílí na uživatele Štábního informačního systému (ŠIS). Jelikož jsou uživatelské stanice v tomto systému pod centralizovanou správou, bylo možné rozdistribuovat na každou koncovou stanici této sítě spořič obrazovky, který se aktivuje po 15 minutách nečinnosti.

Na spořiči obrazovky jsou jednoduše, za pomocí ilustrací, vysvětleny projevy kybernetické kriminality a sociálního inženýrství, zejména phishingu. Zároveň jsou uživatelé vyzýváni k pravidelnému sledování aktuálních hrozeb a doporučení na interním portálu CIRC.

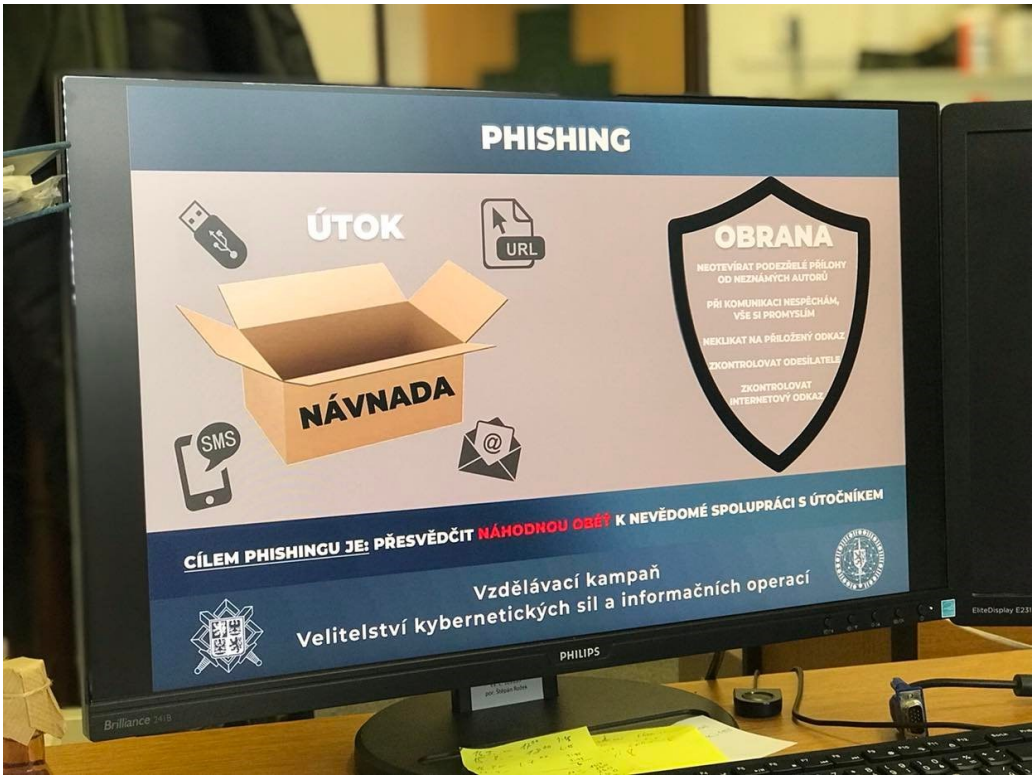


Obr. 28. Vzdělávací kampaň VeKySIO – phishing a spear phishing [archiv autora]

Na spořiči obrazovky, v rámci systému ŠIS, je jednoduše a stručně vysvětlený rozdíl mezi phishingem a spear phishingem pomocí ilustrované grafiky a věcných textů.

Obr. 29. Vzdělávací kampaň VeKySIO [archiv autora]

Další obrazovka, která upozorňuje na podvodné techniky, kdy se útočníci vydávají za pracovníky banky a požadují čísla platebních karet či kopie osobních dokladů.



Obr. 30. Vzdělávací kampaň VeKySIO [archiv autora]

Obr. 31. Vzdělávací kampaň VeKySIO [archiv autora]

6.1 Manuál pro uživatele – podezřelý email a webové stránky

Jelikož se na uživatelské schránky na doméně @army.cz začaly ve velké míře šířit podvodné emaily, je vhodné uživatelům poskytnout manuál, který by pomohl minimalizovat riziko podlehnutí sociálnímu inženýrství a následné zneužití emailové schránky včetně krádeží citlivých údajů. Cílem tohoto manuálu je tedy pomocí několika pravidel a doporučení „naučit“ uživatele v rámci Ministerstva obrany – AČR rozpoznat phishingový email či webové stránky a následně na tuto hrozbu reagovat.

6.1.1 Kontrola adresy odesílatele a domény

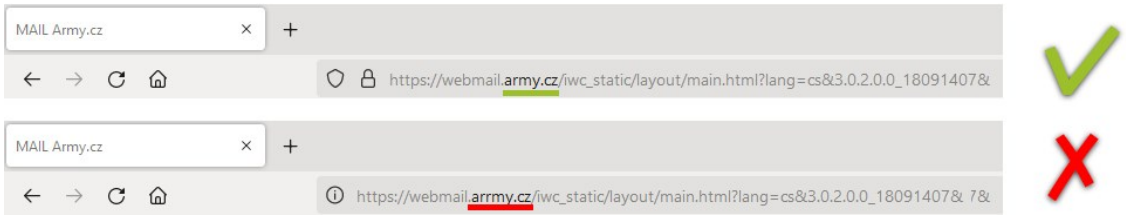
Jako první proveďte kontrolu odesílatele emailu. Mějte se však na pozoru, jelikož phishing může obsahovat i email ze známé emailové schránky, pokud k ní má útočník přístup.

Obsahem většiny phishingových emailů je URL odkaz, na který vás útočník „nutí“ kliknout. Po najetí myší na text tohoto odkazu se v dolní, zpravidla levé části webového prohlížeče zobrazí adresa, na kterou tento odkaz směřuje. Zkontrolujte tedy, zda doménový název neobsahuje jiné znaky, překlepy, pomlčky nebo zcela odlišný název.

Obr. 32. Kontrola správnosti URL adresy [archiv autora]

Z tohoto screenshotu lze jasně rozpoznat, že se jedná o phishingový email vydávající se za Českou poštu. Po přejetí myší přes odkaz se v levém dolním rohu zobrazí URL adresa, na kterou následně bude přesměrováno. Je zřejmé, že se společností Česká pošta nemá nic společného.

Na dalším případu lze pozorovat, jakým způsobem útočníci využívají nepozornosti oběti pomocí zdvojeného písmene „m“ v doménovém názvu. Namísto oficiálního army.cz je uživatel přesměrován na armmy.cz, čehož si nemusí všimnout. Vždy proto kontrolujte správnost domény v adresním řádku prohlížeče.



Obr. 33. Oficiální vs. phishingový doménový název [archiv autora]

6.1.2 Gramatické chyby a oslovení

Jelikož phishingové emaily ze zkušeností přicházejí ze zahraničí, často je jednoduché rozpoznat phishing pouze pomocí gramatických chyb a špatného slovosledu. Útočníci využívají k překladům podvodných emailů či webových stránek různé online překladače, které však určitá slova či věty překládají doslovně, což by mělo být pro rodilého mluvčího varování před možným phishingovým útokem. Stejně tak obecné oslovení v emailu může být známka phishingové zprávy.

Obr. 34. Gramatické chyby v phishingovém emailu [archiv autora]

6.1.3 Urgence a důležitost zprávy

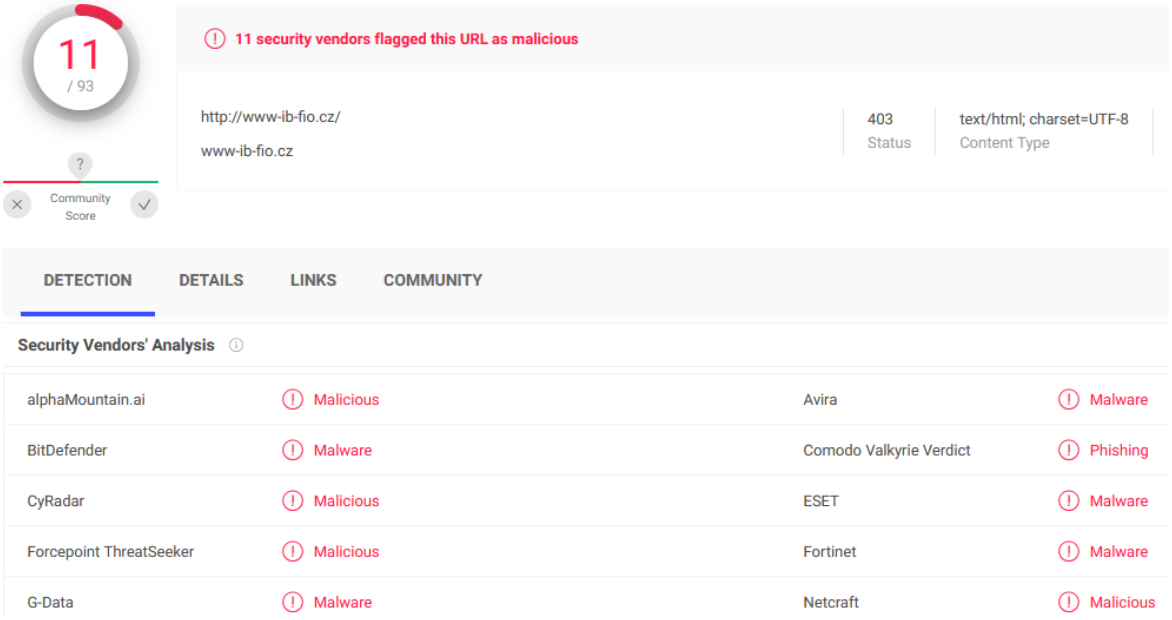
V rámci technik sociálního inženýrství útočníci využívají metody přesvědčování pomocí urgence a důležitosti zprávy. Může se tak jednat o naléhavé výzvy ke změně hesla či PINu platební karty z důvodu napadení účtu, zaplacení faktury po splatnosti apod.

Obr. 35. Urgence a důležitost v phishingové zprávě [50]

6.1.4 Malware přílohy

Velmi častým phishingovým útokem jsou emailové zprávy, které obsahují přílohy infikované malwarem. Proto obecná rada zní – nikdy neotevírejte přílohy od neznámých odesílatelů. Na pozoru se však mějte i před přílohami od známých kontaktů a každou přílohu před jejím otevřením prověřte pomocí antivirového softwaru na daném zařízení.

Pro zjištění malware lze využít i bezplatný online nástroj na adrese VirusTotal.com určený ke kontrole přítomnosti škodlivých kódů jak v přílohách, tak na webových stránkách. Nástroj taktéž nabízí možnost prověření IP adres či hashe souborů.



Obr. 36. Výsledek kontroly podezřelé URL adresy z emailu [archiv autora]

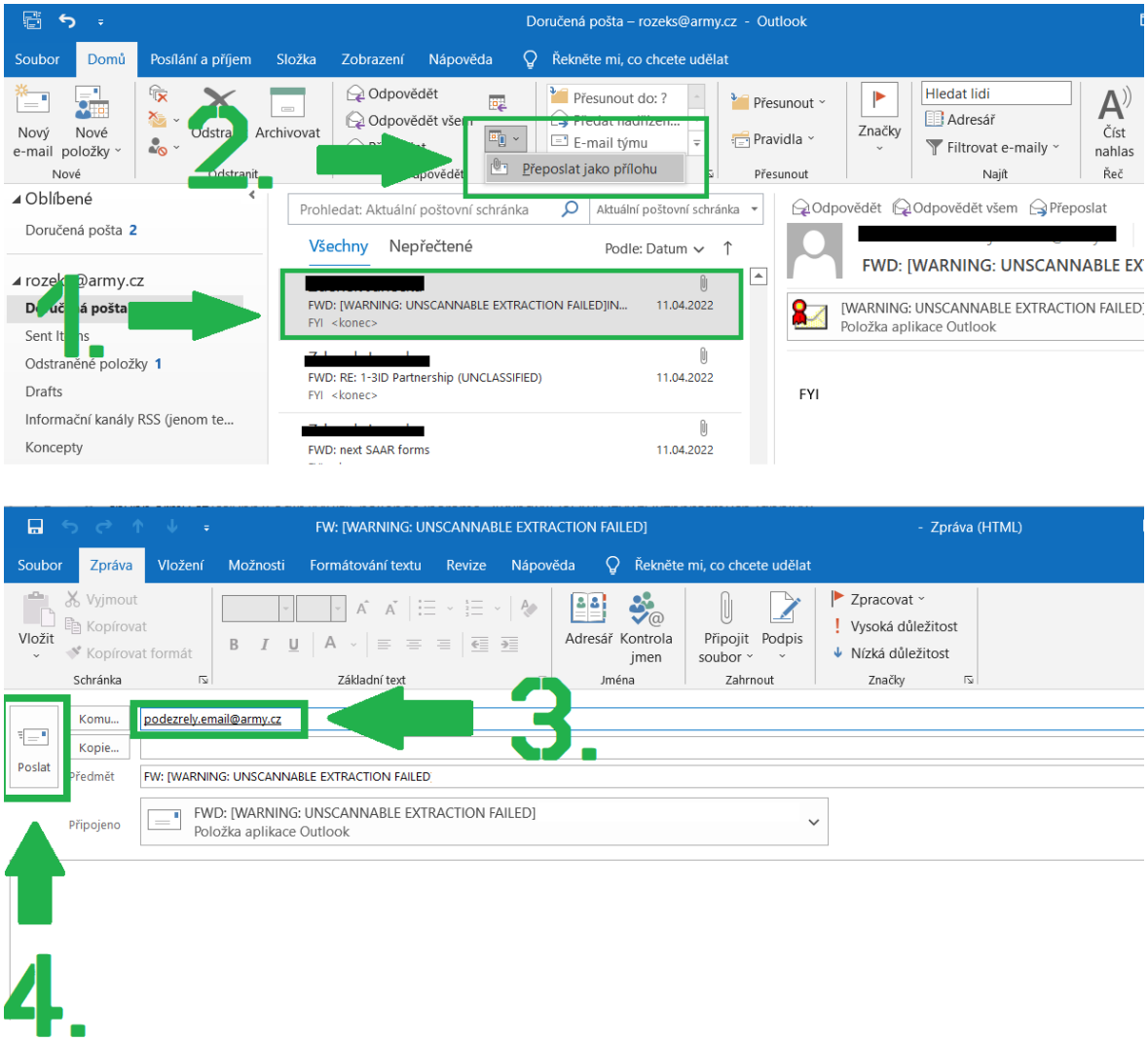
Po zadání podezřelé URL adresy či podezřelého souboru z emailu tento online nástroj, poskytující prověření v databázích antivirových společností, je schopný během několika málo sekund poskytnout výsledek, zda se jedná o přílohu infikovanou malwarem či phishingovou stránku apod. Pro otestování funkčnosti tohoto nástroje byla použita doména www-ib-fio.cz, zmíněna v kapitole 5.4.2, kdy se útočníci snažili cílit phishingový email na příslušníky MO/AČR používající Fio banku.

6.2 Nahlášení podvodného emailu centru CIRC z prostředí Outlook

Z důvodu množících se phishingových útoků na uživatele v rámci MO/AČR je třeba, aby tyto útoky, zejména phishingové emaily v prostředí @army.cz, byly oznamovány a analyzovány specialisty z centra CIRC. Díky tomuto lze upozornit na případné nové typy phishingových útoků a varovat tak ostatní uživatele.

V případě obdržení podezřelého emailu s přílohou je třeba zvolit následující postup:

1. Vyberte podezřelý email
2. V horním menu vybrat ikonu „další“ a „přeposlat jako přílohu“
3. jako adresu příjemce zvolte **podezrely.email@army.cz**, který je vyčleněn pro tyto hlášení
4. Odešlete email a smažte jej ze své poštovní schránky



Obr. 37. Nahlášení podezřelého emailu [archiv autora]

Jakmile dojde k odeslání emailu na uvedenou adresu **podezrely.email@army.cz**, centrum CIRC, tuto zprávu převezme a specialisté provedou detailní analýzu. Na základě výsledků analýz jsou aplikovány bezpečnostní opatření a dochází tak ke zvýšení úrovně kybernetické ochrany rezortu MO.

ZÁVĚR

Teoretická část diplomové práce se zabývala literární rešerší dané problematiky sociálního inženýrství a s ním spojené kybernetické kriminality, jak v civilním sektoru, tak v prostředí Ministerstva obrany a Armády české republiky. Zároveň stručně charakterizuje zkoumané prostředí a systémy používané v rámci této složky.

Praktická část diplomové práce byla provedena ve spolupráci s Centrem CIRC, které se zabývá kybernetickými hrozbami a incidenty v rámci používaných systémů v resortu MO/AČR. Na základě dat o kybernetických bezpečnostních událostech a incidentech sesbíraných v období od 1. října do 31. prosince roku 2021, bylo provedeno vyhodnocení, které potvrzuje potřebnost získávání odolnosti příslušníků silových složek státu proti sociálnímu inženýrství, jelikož během těchto sledovaných měsíců došlo ke kybernetickému bezpečnostnímu incidentu, týkajícího se kompromitace služební emailové schránky na doméně @army.cz. Zároveň byla v měsíci listopadu 2021 řešena kybernetická bezpečnostní událost, kdy sice nedošlo ke kompromitaci služebních dat či emailových schránek, ale došlo k odcizení soukromých finančních prostředků uživatele, který podlehl manipulačním technikám.
Vzhledem k poměru počtu řešených bezpečnostních událostí a počtu bezpečnostních incidentů však lze konstatovat, že míra odolnosti příslušníků MO/AČR je na poměrně vysoké úrovni.

Další část praktické části práce byla věnována aktuálním opatřením, které jsou distribuovány v rámci AČR mezi uživatele, s cílem zvyšování odolnosti proti kybernetickým hrozbám a vyobrazení reálných příkladů phishingových útoků, které byly cíleny na uživatele v rámci systémů MO a AČR. Poslední část se zabývá manuálem pro uživatele, který za pomoci reálných ukázek a postupů slouží jako pomůcka pro rozpoznání podvodných emailů či webových stránek a následný postup k nahlášení těchto aktivit, díky čemuž dochází k celkovému zvyšování kybernetické ochrany v resortu MO.

Přínosem této diplomové práce je především reálné vyobrazení phishingových útoků pro uživatele v rámci MO/AČR, kteří se s touto problematikou zatím nesetkali a manuál k detekci podezřelých emailových zpráv včetně postupu jejich nahlášení centru CIRC. Úkolem bylo také v rámci možností, které dávají omezený prostor ve zveřejňování informací z tohoto citlivého prostředí, poukázat na nutnost zvyšování trvalé odolnosti proti sociální manipulaci.

SEZNAM POUŽITÉ LITERATURY

[1] Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. [cit. 2020-02-16]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[2] *VĚSTNÍK MO ročník 2014 - 93. NORMATIVNÍ VÝNOS MINISTERSTVA OBRANY: Reakce na kybernetické bezpečnostní incidenty v rezortu Ministerstva obrany*. In: . Ministerstvo obrany, 2014, částka 19.

[3] KOLOUCH, Jan, Pavel BAŠTA, Andrea KROPÁČOVÁ a Martin KUNC. *CyberSecurity* [online]. Praha, 2019 [cit. 2020-02-14]. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

[4] ZELINKOVÁ, Věra. Kyberprostor – WikiKnihovna. In: *WikiKnihovna* [online]. [cit. 2020-02-09]. Dostupné z: http://wiki.knihovna.cz/index.php/Kyberprostor

[5] Information and Communication Technologies (ICT) | AIMS. In: *Homepage | AIMS* [online]. [cit. 2022-02-13]. Dostupné z: http://aims.fao.org/information-and-communication-technologies-ict

[6] ICT ŘEŠENÍ. In: *Úvod | HTICLUSTER.EU* [online]. [cit. 2022-02-13]. Dostupné z: http://www.hticluster.eu/upload/images/press_15Sep14.jpg

[7] *Measuring digital development Facts and figures 2021* [online]. International Telecommunication Union, 2021 [cit. 2022-02-13]. ISBN 978-92-61-35401-5. Dostupné z: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

[8] KOLOUCH, Jan. *CyberCrime* [online]. 1. Praha: CZ.NIC, z.s.p.o., 2016 [cit. 2019-12-12]. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

[9] MITNICK, Kevin D. a William L. SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-736-1210-6.

[10] Zákon č. 219/1999 Sb.: Zákon o ozbrojených silách České republiky. In: *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. [cit. 2022-01-23]. Dostupné z: https://www.zakonyprolidi.cz/cs/1999-219

[11] *Vývoj skutečných počtů osob v resortu MO ČR v letech 1992 - 2021* [online]. 2022 [cit. 2022-01-23]. Dostupné z: https://mocr.army.cz/assets/dokumenty-a-legislativa/cisla/vyvoj-sp-rezortu-mo-v-letech--1992---2021.xls

[12] Znak AČR. In: *Wikipedie, otevřená encyklopedie* [online]. [cit. 2022-02-07]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/thumb/1/15/Logo_of_the_Czech_Armed_Forces.svg/1024px-Logo_of_the_Czech_Armed_Forces.svg.png

[13] Působnost a činnosti | Ministerstvo obrany. In: *Ministerstvo obrany* [online]. [cit. 2022-01-25]. Dostupné z: https://mocr.army.cz/ministr-a-ministerstvo/pusobnost/pusobnost-a-cinnosti-5131/

[14] Velitelství Pozemních sil AČR | Armáda ČR. In: *Armáda ČR* [online]. [cit. 2022-01-25]. Dostupné z: https://acr.army.cz/struktura/generalni/poz/velitelstvi-pozemnich-sil-acr-221600/

[15] Velitelství Vzdušných sil AČR | Armáda ČR. In: *Armáda ČR* [online]. [cit. 2022-01-25]. Dostupné z: https://acr.army.cz/struktura/generalni-stab/velitelstvi-vzdusnych-sil-86864/

[16] Ředitelství speciálních sil | Armáda ČR. In: *Armáda ČR* [online]. [cit. 2022-01-25]. Dostupné z: https://acr.army.cz/struktura/generalni/specialni-sily/reditelstvi-specialnich-sil-104392/

[17] Velitelství teritoria | Armáda ČR. In: *Armáda ČR* [online]. [cit. 2022-02-07]. Dostupné z: https://acr.army.cz/struktura/generalni/ter/velitelstvi-teritoria-214170/

[18] Armáda ČR - Velitelství kybernetických sil a informačních operací. In: *Twitter* [online]. [cit. 2022-02-07]. Dostupné z: https://pbs.twimg.com/media/D-c6NcJXkAAigke?format=jpg&name=large

[19] Působnost - Pražský hrad. In: *Pražský hrad - Prezident České republiky* [online]. [cit. 2022-01-25]. Dostupné z: https://www.hrad.cz/cs/prezident-cr/vojenska-kancelar-

prezidenta-republiky-a-hradni-straz/vojenska-kancelar-prezidenta-republiky/pusobnost

[20] Působnost | hrad.army.cz. In: *Vítejte na stránkách Hradní stráže* [online]. [cit. 2022-01-25]. Dostupné z: https://hrad.army.cz/pusobnost

[21] *Strategie kybernetické obrany ČR: Národní centrum kybernetických operací* [online]. 2018 [cit. 2022-03-05]. Dostupné z: https://www.vzcr.cz/uploads/46-Strategie-kyberneticke-obrany-CR.pdf

[22] JAŠEK, PH.D., DBA, Prof. Mgr. Roman a Ing. David MALANÍK, PH.D. *Bezpečnost informačních systémů* [online]. Zlín, 2013 [cit. 2022-04-23]. Dostupné z: http://hdl.handle.net/10563/25821

[23] Vojenské zpravodajství | Kdo jsme. In: *Vojenské zpravodajství* [online]. [cit. 2022-03-05]. Dostupné z: https://www.vzcr.cz/kdo-jsme-35

[24] Národní úřad pro kybernetickou a informační bezpečnost - O NÚKIB. In: *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2022-03-12]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

[25] *ZPRÁVA O ČINNOSTI 2020: NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST* [online]. In: . [cit. 2022-03-31]. Dostupné z: https://nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_cinnosti_NUKIB%20-%202020.pdf

[26] Velitelství informačních a kybernetických sil | Armáda ČR. In: *Armáda ČR* [online]. [cit. 2022-02-07]. Dostupné z: https://acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/

[27] Velitelství Informačních a Kybernetických sil. In: *Facebook* [online]. [cit. 2022-04-05]. Dostupné z: https://www.facebook.com/VeKySIO

[28] Kybernetický útok na vozidla Pandur. In: *Facebook* [online]. [cit. 2022-04-05]. Dostupné z: https://scontent.fprg1-1.fna.fbcdn.net/v/t39.30808-6/275549939_1108205393332378_434696487177963059_n.jpg?_nc_cat=105&ccb=1-5&_nc_sid=730e14&_nc_ohc=kxkdH2AZjasAX_VGYHj&_nc_ht=scontent.fprg1-

1.fna&oh=00_AT88bGoXM4Qq2Ee64A1NdwImE5jjdwPL8k7qv8Dj7NBnhA&oe=62504326

[29] O nás | circ.army.cz. In: *Circ.army.cz* [online]. [cit. 2022-02-17]. Dostupné z: https://circ.army.cz/o-nas

[30] Úvodní stránky Centra CIRC jsou zdrojem informací z oblasti kybernetické bezpečnosti. In: *Armáda ČR* [online]. [cit. 2022-03-20]. Dostupné z: https://acr.army.cz/assets/informacni-servis/zpravodajstvi/8_1507.jpg

[31] *Katalog 2007* [online]. In: . Ministerstvo obrany ČR – AVIS, 2007 [cit. 2022-03-19]. Dostupné z: https://www.army.cz/assets/files/9369/KATALOG_2007_part_4.pdf

[32] Vývoj registrované kriminality v roce 2021. In: *Policie České republiky* [online]. [cit. 2022-03-04]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx

[33] Jaký byl rok 2021 z pohledu kybernetických hrozeb? Hlavním cílem byla hesla, objem detekcí malwaru vzrostl o čtvrtinu. In: *Malware Protection & Internet Security; ESET* [online]. [cit. 2022-03-20]. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/jaky-byl-rok-2021-z-pohledu-kybernetickych-hrozeb-hlavnim-cilem-byla-hesla-objem-detekci-malwaru-v/

[34] Podvodná aplikace FlixOnline. In: *Svět Huawei; Magazín o společnostech Huawei a Honor. Nabízíme Vám novinky, recenze a zajímavé články.* [online]. [cit. 2022-03-20]. Dostupné z: https://svethuawei.eu/wp-content/uploads/2021/04/Screenshot_2021-04-08-whatsapp-1-webp-WEBP-obrazek-614-%C3%97-497-bodu.png

[35] Nový malware ovlivňuje uživatele Androidu tím, že je láká na bezplatné předplatné Netflixu. In: *Svět Huawei; Magazín o společnostech Huawei a Honor. Nabízíme Vám novinky, recenze a zajímavé články.* [online]. [cit. 2022-03-20]. Dostupné z: https://svethuawei.eu/novy-malware-ovlivnuje-uzivatele-androidu-tim-ze-je-laka-na-bezplatne-predplatne-netflixu/

[36] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013 [cit. 2019-12-19]. ISBN 978-80-7251-397-0. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

[37] Takto vypadá falešné upozornění u tzv. policejního viru. In: *SSL/TLS od největšího prodejce ve střední Evropě s nejlepší podporou.* [online]. [cit. 2022-03-21]. Dostupné z: https://www.sslmarket.cz/images/blog/policejni-virus.jpg

[38] ROŽEK, Štěpán. *Bezpečnostní rizika při využívání smart technologií*. Zlín, 2020. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně - Fakulta aplikované informatiky. Vedoucí práce PhDr. Mgr. Stanislav Zelinka.

[39] Botnet - INTERNETEM BEZPEČNĚ. In: *INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem* [online]. [cit. 2022-03-27]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/botnet/

[40] BotNet - INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem. In: *INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem* [online]. [cit. 2022-03-27]. Dostupné z: https://www.internetembezpecne.cz/wp-content/uploads/2017/07/BOTNET.jpg

[41] Phishingový email vydávající se za ČSOB. In: *Twitter* [online]. [cit. 2022-03-30]. Dostupné z: https://pbs.twimg.com/media/EfOQJpHX0AEgbvz?format=jpg&name=large

[42] Phishingový e-mail z 21.3.2022 (Raiffeisenbank). In: *Banka inspirovaná klienty | Raiffeisenbank* [online]. [cit. 2022-03-30]. Dostupné z: https://www.rb.cz/pictures/phishing/utok-email-21032022.png

[43] *PODVODNÉ E-MAILY NEBO ZPRÁVY NA SOCIÁLNÍCH SÍTÍCH NA MÍRU: SPEAR-PHISHING A JAK SE PŘED NÍM CHRÁNIT* [online]. In: . s. 12 [cit. 2022-04-05]. Dostupné z: https://nukib.cz/download/publikace/analyzy/Spear-phishing_a_jak_se_pred_nim_chranit.pdf

[44] Výhružné SMS v rámci cvičení Saber Strike 2022. In: *Facebook* [online]. [cit. 2022-04-08]. Dostupné z: https://scontent-frt3-1.xx.fbcdn.net/v/t39.30808-6/275495980_1108204566665794_7144607821144358907_n.jpg?_nc_cat=107&ccb=1-5&_nc_sid=730e14&_nc_ohc=p_o3QX1VQCIAX-FY30p&_nc_ht=scontent-frt3-1.xx&oh=00_AT_nX57YrUCtlqQA4BhUA-4HZcRSBDs11tugJF-WMaWVAg&oe=625538BC

[45] Dezinformace spojené s válkou na Ukrajině. In: *Projekt E-bezpečí - E-Bezpečí* [online]. [cit. 2022-04-07]. Dostupné z: https://www.e-bezpeci.cz/index.php/70-projekt-fake-news/2518-dezinformace-spojene-s-valkou-na-ukrajine

[46] Flyby Moscow (May 04, 2020). In: *Youtube* [online]. [cit. 2022-04-23]. Dostupné z: https://www.youtube.com/watch?v=JQkO5XsQMag

[47] Europol varuje před deepfake technologií. Může vyvolat politickou nestabilitu a polarizaci. In: *EURACTIV.cz; Evropská unie v českých souvislostech* [online]. [cit. 2022-04-07]. Dostupné z: https://euractiv.cz/section/digitalni-agenda/news/europol-varuje-pred-deepfake-technologii-muze-vyvolat-politickou-nestabilitu-a-polarizaci/

[48] Deepfake video ukrajinského prezidenta Volodymyra Zelenského (vlevo) a záběr z reálného videa (vpravo). In: *Blesk.cz - zprávy, celebrity, sport, zábava* [online]. [cit. 2022-04-07]. Dostupné z: https://1884403144.rsc.cdn77.org/foto/ukrajina-volodymyr-zelenskyj-deepfake/Zml0LWluLzk3OHg5OTk5L2ZpbHRlcnM6cXVhbGl0eSg4NSk6bm9fdXBzY2FsZSgpL2ltZw/7600886.jpg?v=0&st=i4zjgCZEWdLcrn_U4nmbBm0EDatVf2tOlUkq92nEoQ4&ts=1600812000&e=0

[49] BERTOLIN, Giorgio, John D. GALLACHER, Kateryna KONONOVA, Tetiana MARCHENKO, Nora BITENIECE a Edward H. CHRISTIE. *RESPONDING TO COGNITIVE SECURITY CHALLENGES* [online]. NATO STRATCOM COE, 2019 [cit. 2022-04-21]. ISBN 978-9934-564-39-0. Dostupné z: https://stratcomcoe.org/pdfjs/?file=/publications/download/web_Responing-to-Cognitive.pdf?zoom=page-fit

[50] Phishingový útok na klienty Fio banky. In: *ESET, Norton, Bitdefender, AVG, Avast antivirus včetně verzí ke stažení zdarma | Antivirové Centrum* [online]. [cit. 2022-04-17]. Dostupné z: https://www.antivirovecentrum.cz/design/ac/images/vlastni/aktuality/FioPhishing.jpg

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ICT	Informační a komunikační technologie
ITU	Mezinárodní telekomunikační unie
MO	Ministerstvo obrany
CIRC	Computer Incident Response Capability
AČR	Armáda České republiky
NATO	Severoatlantická aliance
KVV	Krajské vojenské velitelství
VeKySIO	Velitelství kybernetických sil a informačních operací
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
NCKO	Národní centrum kybernetických operací
PD IMO	Přístupová doména internetu Ministerstva obrany
ŠIS	Štábní informační systém
SW	Software
OS	Operační systém
C&C	Command and Control server (řídící server pro malware – botnet)
DDoS	(Distributed) Denial of Service – (distribuované) odepření služby
DNS	Domain Name System
IP	Logická adresa zařízení v síti
KBU	Kybernetická bezpečnostní událost
KBI	Kybernetický bezpečnostní incident

SEZNAM OBRÁZKŮ

SEZNAM TABULEK