Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Modelování kybernetických bezpečnostních hrozeb

Diplomová práce

Autor: Bc. Jan Štěpán
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Almer Lubomír, Ph.D.

Hradec Králové duben 2023

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 23.4.2023 Bc. Jan Štěpán

Poděkování:

Děkuji vedoucímu diplomové práce Ing. Lubomíru Almerovi, Ph.D. za metodické vedení práce a veškerou poskytnutou pomoc. Zároveň bych chtěl poděkovat rodině i přítelkyni za podporu a univerzitě za poskytnutí laboratoře.

Anotace

Cílem práce bylo představit a nasimulovat vybrané taktiky a techniky útoků, které jsou typické pro prostředí zdravotnických zařízení. Společně s tím dále vyhodnotit možnosti ochrany proti těmto hrozbám. Dále byla analyzována topologie, která se v tomto sektoru využívá a následně se pomocí série testů ve virtuálním prostředí vyzkoušely vybrané útoky, které byly rozděleny do tří scénářů. V teoretické části jsou popsána východiska, ze kterých autor vycházel během psaní práce. Byla provedena analýza a rozbor vybraných metod útoků a protiopatření. Výsledkem práce je vyhodnocení úspěšnosti scénářů, detekování potenciálně slabých míst v zabezpečení laboratoře zdravotnického zařízení a souhrn opatření, která lze použít k vylepšení zabezpečení.

Annotation

Title: Cyber threat modeling

The goal of this thesis was to evaluate and simulate selected cyber attack tactics and techniques that are common for the healthcare sector. Along with that, the goal was to further evaluate the possibilities of protection against these threats. Furthermore, the topology itself that is used in the healthcare facility was described and selected attacks were analysed using a series of tests in a virtual environment. Cyber threats were in this thesis divided into three scenarios. The theoretical part describes the basic information regarding security from which the author proceeded while writing the thesis. An analysis and evaluation of selected attack methods and countermeasures was carried out at the end. Result of this thesis is the evaluation of the success of the scenarios, the detection of potential weaknesses in the security of the healthcare laboratory facility and a summary of the measures that can be used to improve the security.

Obsah

Seznam obrázků

1 Úvod

Modernizace a digitalizace je trendem posledních několika let a dnes se dotýká téměř každého sektoru. Jedním z těchto sektorů je zdravotnictví, kde modernizace mohla přispět nejen v oblasti poskytovaných služeb, ale zároveň v možnosti efektivního využívání moderních specializovaných přístrojů. I zde se však najdou stinné stránky, mezi které patří například riziko odcizení citlivých dat pacientů. Ta se nachází ve velkém množství uvnitř zdravotnických zařízení, a proto je třeba tyto organizace chránit a zajistit jejich dostupnost, důvěrnost a integritu.

Samotné útoky a jejich možné vektory jsou detailně analyzovány v následujících kapitolách. Přestože jsou komplexní útoky složeny z několika taktik a technik, lze problematiku přístupu do systému kategorizovat do dvou základních skupin. Napadení technických prostředků samotného systému nebo využití lidského faktoru, jenž má k systému přístup.

Právě lidský faktor podle dostupných dat za poslední tři roky představuje největší zranitelnost většiny systémů. Na tuto skutečnost poukazuje údaj, kdy až v 98 % útoků na komerční sféru, státní podniky a infrastrukturu bylo využito nějaké z metod sociálního inženýrství.[1] Dále statistika uvádí, že častým cílem útoků bylo odcizení dat a napadení malwarem typu ransomware, kdy komerční sektor byl cílem ve 40 % případů a nejvíce zasaženou částí infrastruktury bylo zdravotnictví, na které mířilo 13 % zaznamenaných hrozeb.[2] Tato statistika se liší napříč státy a kontinenty.

Druhou kategorií je poté překonání technických prostředků zabezpečení. Při správném nastavení zabezpečovacích prvků se může jednat o úkol velice náročný a zdlouhavý. V pozdějších kapitolách jsou představeny taktiky a techniky útoků, společně s jejich možnými mitigacemi.

Zabezpečení a kybernetická bezpečnost je komplexní proces skládající se z několika částí. U zdravotnického zařízení musí být též dodržena potřebná legislativa v kombinaci s organizačními a technickými opatřeními, která jsou popsána v teoretické části práce. Důležité je též zmínit, že bezpečnost tvoří do značné míry prevence a předcházení samotným útokům. Toho by mělo být dosaženo za pomocí navržených mitigací a protiopatření.

Oproti ostatním sektorům nese modernizované zdravotnictví určitou zodpovědnost vůči lidskému zdraví ve společnosti. Cílem této práce je zaměřit se na problematiku modelování hrozeb a hodnocení rizik v rámci zdravotnického zařízení. Aby měla práce relevantní výsledek, který bude v reálném světě aplikovatelný, byl vytvořen dotazník, který byl vyplněn odborníkem z praxe v jednom blíže nespecifikovaném zdravotnického zařízení. Dotazník je obsažen v příloze práce a obsahuje otázky týkající se nejen organizace, ale také základní charakteristiky topologie. Na základě odpovědí z nich je v praktické části sestaven model laboratoře se zjištěnými poznatky, na kterých byly testovány útoky a navrženy možnosti obrany. Z bezpečnostních důvodů nebude zmiňováno místo a druh zdravotnického zařízení. Stejným způsobem zůstane i zaměstnanec, který se na dotazníku podílel, v anonymitě.

2 Cíl práce

Diplomová práce je zaměřena na oblast zabezpečení zdravotnického zařízení. Cílem práce je analýza oblasti kybernetické bezpečnosti zmíněných zařízení a následné vytvoření testovacího prostředí laboratoře, ve kterém budou simulovány vybrané kybernetické útoky.

Teoretická část diplomové práce je věnována analýze. V rámci analýzy tohoto tématu je nejdříve proveden průzkum legislativy, jednotlivých kategorií útoků, útočníků a v neposlední řadě možností samotné obrany. Tato analytická část tak poskytuje základní rámcové vymezení zkoumané problematiky.

Praktická část je zaměřena na vytvoření zmíněné laboratoře, jejíž topologie modeluje reálnou strukturu ve zdravotnickém zařízení. Toho bude dosaženo ve školní laboratoři na reálných síťových prvcích. Následně se na modelu vyzkouší vybrané útoky, které byly zvoleny na základě rozhovoru s odborníkem z praxe. Podle výsledků a na základě teoretických poznatků útoků bude cílem praktické části vytvořit výstup, reprezentující soubor opatření a technických prostředků, které přispějí ke zvýšení kybernetického zabezpečení na úroveň, kdy budou citlivá data lépe chráněna.

3 Metodika zpracování

Diplomová práce „Modelování kybernetických bezpečnostních hrozeb“ byla vytvořena postupy, které odpovídají metodám zpracování vědecké práce. Tyto metody nebyly většinou aplikovány izolovaně, ale ve vzájemné souvislosti.

V první části práce byla použita zejména rešerše dostupných materiálů, dokumentů v elektronické podobě, norem, zákonů a článků z internetu. Literární rešerše pomohla poskytnou aktuální pohled na zkoumanou problematiku. Z obecných metod byla dále použita analýza, syntéza, indukce a dedukce. Analýza byla využita v souvislosti s objektivizací a objasněním jednotlivých zkoumaných aspektů, zejména pak vybraných scénářů, které byly zvoleny na základě konzultace se zaměstnancem zdravotnického zařízení a kybernetické bezpečnosti. Syntéza byla použita pro sumarizaci získaných poznatků. Indukce a dedukce byly využity pro stanovení vztahů mezi jednotlivými zkoumanými a simulovanými scénáři.

Pro zpracování praktické části diplomové práce bylo v první části použito dotazníkové šetření, následně byla použita metoda testování, v rámci které bylo vytvořeno testovací prostředí a jako poslední bylo provedeno testování samotného modelu v laboratoři pomocí penetračních testů.

V práci jsou testovány dvě hypotézy:

- Dokáže soubor navržených opatření úplně předejít některému z běžných typů útoků?
- Sníží soubor navržených opatření počet útoků na celý systém?

4 Kybernetická bezpečnost

Mezi jeden z největších lidských objevů lze bez pochyby zařadit internet. Počítačová síť propojující dnes již celý svět, kde se přenos informací napříč celou strukturou pohybuje v řádu milisekund. Téměř instantně je tak možné posílat zprávy, dokumenty, obrázky, videa a další různý obsah. Jedná se o revoluci v komunikaci, která má velký podíl na tváři dnešního světa.[5] Mnoho služeb bylo digitalizováno, a tak se bohužel ani tato technologie neobešla bez určitého zneužití ve formě kybernetické kriminality.[1][2][6] Nejdříve je však vhodné definovat určité základní pojmy, které budou využívány.

První důležitý pojem se nazývá **kyberprostor**. Většina běžných lidí označuje kyberprostor nevědomky jako „internet“, avšak toto označení není přesné. Podle zákona o kybernetické bezpečnosti 181/2014 sb. je přesnou definicí kyberprostoru takové digitální prostředí, které umožňuje vznik, zpracování a výměnu informací. Zároveň ho tvoří informační systémy, služby a sítě elektrotechnických komunikací.[3] Naproti tomu pojem internet je označení pro celosvětovou síť, která agreguje menší osobní, univerzitní a komerční sítě. Znamená tak více vymezení se k infrastruktuře než k virtuálnímu prostoru, jak je tomu u kyberprostoru.[5]

Kyberkriminalita označuje jakoukoli trestnou činnost páchanou v kyberprostoru. Na území České republiky spadá vyšetřování této trestné činnosti pod Policii České republiky. V úvodu byla zmínka o statistice zvyšujícího se počtu kybernetických útoků ve světě. Česká republika v tomto není výjimka a podle dat Policie České republiky se počet případů kyberkriminality zvýšil z roku 2011 s 1502 případů na 8417 případů v roce 2019.[6] Dále podle dat společnosti CZ.NIC, která je vrchním českým poskytovatelem internetu, byl počet případů 9518 v roce 2021.[7]

S kybernetickou kriminalitou se velmi prolíná třetí pojem **kyberterorismus**. Jedná se o terorismus, který je prováděn v kyberprostoru.[8] Detailní rozdělení, popis kyberútoků a kategorizace hrozeb se nachází v samostatné kapitole.

4.1 Kyberbezpečnost

Kyberbezpečnost je možné definovat jako soubor technik, metod a přístupů, které potenciální útok buď kompletně mitigují nebo alespoň maximálně zamezují škodám.[5][8] Legislativně ji lze také popsat jako způsob zajištění integrity, důvěrnosti a dostupnosti dat a zajistit ochranu aktiv.[3] Pojem je jinak velice těžko přesněji definovatelný. Konkrétní zabezpečení je totiž výsledkem implementace jednotlivých opatření, které zajišťuje v organizaci osoba s adekvátní bezpečnostní rolí k tomu pověřená.[4]

Bezpečnost lze definovat seskupením pravidel a dobrých zvyků, které jsou z části dány zákonem jako povinné a doporučeními, jenž je dobré dodržovat, za účelem ochrany.[5][8] Přeneseno do kyberprostoru, jedná se o data a aktiva ve formě prvků informačních systémů.[3][4]

4.2 Legislativa

Kyberbezpečnost obsahuje podstatnou část legislativního charakteru. Je důležité zmínit, že právně se nastavuje pouze zabezpečovací politika, ne však jeho přesná implementace. Ta už závisí na konkrétním subjektu, který bude kybernetickou bezpečnost řešit. V rámci Evropské unie je legislativa tvořena směrnicemi NIS a NIS2.[9] Konkrétní další opatření a specifikace však závisí na každém státu. V České republice je kyberbezpečnost obsažena v zákonu o kybernetické bezpečnosti (181/2014 Sb.)[9] a ve vyhlášce o kybernetické bezpečnosti (82/2018 Sb.).[9] Tyto dva zmíněné dokumenty obsahují soupis pravidel, doporučení a definice pojmů i subjektů, na které se daná bezpečnost musí aplikovat. Kontrolou subjektů je pověřen Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který dohlíží na dodržování těchto pravidel.[3][10] Existují též rozšiřující rámce, normy a standardy v oblasti kybernetické bezpečnosti. Mezi důležité standardy patří především ISO 27k.[58]

Práce je zaměřena na testování bezpečnosti na modelu laboratoře zdravotnického zařízení. Jestliže je kybernetická bezpečnost dána z podstatné části legislativně, je zapotřebí identifikovat a analyzovat body týkají se zdravotnického sektoru, přesněji konkrétního zařízení.

4.3 Zranitelnosti a hrozby

V rámci analýzy je provedena identifikace zranitelností a potenciálních hrozeb. Dle Výkladového slovníku kybernetické bezpečnosti je zranitelnost definována jako slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami.[8] Národní legislativa definuje několik základních druhů zranitelností. Podle přílohy č. 3 vyhlášky o kybernetické bezpečnosti 82/2018 Sb. se jedná o následující zranitelnosti:[4]

1. *Nedostatečná údržba informačního a komunikačního systému*
2. *Zastaralost informačního a komunikačního systému*
3. *Nedostatečná ochrana vnějšího perimetru*
4. *Nedostatečné bezpečnostní povědomí uživatelů a administrátorů*
5. *Nevhodné nastavení přístupových oprávnění*
6. *Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů*
7. *Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závažné způsoby chování*
8. *Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů, bezpečnostních rolí*
9. *Nedostatečná ochrana aktiv*
10. *Nevhodná bezpečnostní architektura*
11. *Nedostatečná míra nezávislé kontroly*
12. *Neschopnost včasného odhalení ze strany zaměstnanců*

Uvedené zranitelnosti představují obecný výčet, který musí být přizpůsoben potřebám a požadavkům jednotlivých organizací. Za tímto účelem jsou realizovány detailní analýzy, jako je například analýza dopadů, analýza současného stavu aj.

Právě tyto zranitelnosti poskytují prostor, který může být využit k napadení. Samotné kybernetické útoky na systém (též hrozby) jsou také definovány ve vyhlášce o kybernetické bezpečnosti následujícím výčtem:[4]

1. *Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů*
2. *Poškození nebo selhání technického anebo programového vybavení*
3. *Zneužití identity*
4. *Užívaní programového vybavení v rozporu s licenčními podmínkami*
5. *Škodlivý kód*
6. *Narušení fyzické bezpečnosti*
7. *Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie*
8. *Zneužití nebo neoprávněná modifikace údajů*
9. *Ztráta, odcizení nebo poškození aktiva*
10. *Nedodržení smluvního závazku ze strany dodavatele*
11. *Pochybení ze strany zaměstnanců*
12. *Zneužití vnitřních prostředků, sabotáž*
13. *Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb*
14. *Nedostatek zaměstnanců s potřebnou odbornou úrovní*
15. *Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik*
16. *Zneužití vyměnitelných technických nosičů dat*
17. *Napadení elektronické komunikace (odposlech, modifikace)*

Stejně jako v případě zranitelností, i zde platí pravidlo, že o detailní analýzu potenciálních hrozeb a vektorů útoků se stará sama organizace. Za pomocí těchto informací je nyní možné identifikovat přesnější metody a vektory potenciálních útoků, možnosti obrany i opatření, která by minimalizovala zranitelnosti, a tím co nejvíce předcházela hrozbám.

4.4 Opatření

Napadení systému v legislativní terminologii je tak možné definovat jako hrozbu využívající některé ze zranitelností. Je žádoucí takové situaci zabránit, a proto existují opatření. Podle zákona o kybernetické bezpečnosti pojem opatření znamená *souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru*. V podstatě se tak jedná o výčet doporučení a nařízení, jež mají minimalizovat riziko a dopad hrozeb. V paragrafu 5 jsou dále bezpečností opatření rozdělena na dvě hlavní kategorie a následně vyjmenována.[3] Jejich přesnou a detailní definici lze najít ve vyhlášce o kybernetické bezpečnosti.[4]

4.4.1 Organizační opatření

Do první skupiny patří organizační opatření. Jedná se o interní pravidla přístupu k bezpečnosti z hlediska organizace, převážně tedy zaměstnanců a dodavatelů. Opět i v tomto případě zákon definuje pouze rámec opatření. Konkrétní provedení závisí na samotné organizaci a osobě v ní k tomu pověřené, která tak jedná na základě provedené analýzy. Z pohledu legislativy spadá pod organizační opatření následující:[3]

- *systém řízení bezpečnosti informací,*
- *řízení rizik,*
- *bezpečnostní politika,*
- *organizační bezpečnost,*
- *stanovení bezpečnostních požadavků pro dodavatele,*
- *řízení aktiv,*
- *bezpečnost lidských zdrojů,*
- *řízení provozu a komunikací,*
- *řízení přístupu osob,*
- *akvizice, vývoj a údržba,*
- *zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,*
- *řízení kontinuity činností,*

- *kontrola a audit.*

Zmíněná opatření jsou dále reflektována v praktické části v rámci návrhů a doporučení. Některé už z principu lze jen těžko konkrétně nasimulovat, avšak jiné jsou naopak zcela stěžejní. Jelikož se jedná předlohou o zdravotnické zařízení založené na reálných údajích, jsou již potřebná opatření promítnuta v samotném návrhu modelu.

Prvním organizačním opatřením je **systém řízení bezpečnosti informací**. Vyhláška toto organizační opatření definuje vymezením povinností pověřené osobě stanovit cíle, rozsah a požadavky na řízení bezpečnosti informací. Pod tento bod spadá i základní řízení rizik z předchozího výčtu hrozeb a provádění auditů i kontrol plnění příslušných bezpečnostních politik.[4] V praktickém modelu jsou některé definice tohoto opatření nerealizovatelné, jelikož se nejedná o celý reálný subjekt. Důvod, proč je tento bod stěžejní je však prostý, jelikož klade základní otázky bezpečnosti, a to konkrétně **co** je třeba chránit, **jakým způsobem** toho bude dosaženo a **před čím** je nutné systém chránit.

Druhým opatřením je **řízení rizik**, které dále a hlouběji pracuje s možnými hrozbami v dané organizaci. Povinná osoba v tomto případě musí stanovit metodiku hodnocení rizik a jednotlivá kritéria jejich akceptovatelnosti. Dále identifikuje významné hrozby, vypracovává jednotlivé zprávy ohledně hodnocení rizik a zpracovává prohlášení o aplikovatelnosti. Významné je též zavedení plánu zvládání rizik touto osobou, kdy je třeba předem jasně definovat cíle a přínosy bezpečnostních opatření pro jednotlivá rizika.[4] V rámci modelu toto opatření bude reprezentováno autorem práce ve formě provedení detailní analýzy jednotlivých vektorů útoků. V návaznosti na minulý bod se tak jedná o analýzu a rozšíření otázky „**před čím** je nutné systém chránit“.

Bezpečnostní politikou se rozumí jasná definice a sepsání veškerých platných pravidel, nařízení, směrnic a pokynů platící pro jednotlivé zaměstnance, skupiny zaměstnanců či pro organizaci jako celek.[4]

Mezi následující opatření patří **organizační bezpečnost**. V rámci tohoto bodu zajistí pověřená osoba, že bude optimálně stanovena bezpečnostní politika organizace. Společně s tím je třeba, aby byla zajištěna dostupnost jednotlivých

zdrojů potřebných pro řízení bezpečnosti. Zároveň toto opatření definuje nutnost motivace dalších zaměstnanců k rozvíjení efektivity bezpečnosti řízení a integrace systémů řízení bezpečnosti do procesů povinné osoby. Proces zabezpečení systému není jednorázový a je neustále nutné ho v čase vyvíjet. Pověřená osoba má za úkol také prosazovat neustálé vylepšování systému řízení bezpečnosti. Za důležitý úkon lze rovněž považovat stanovení pravidel pro administrátory v rámci řízení bezpečnosti, společně se zárukou zachováním jejich mlčenlivosti před nepověřenými osobami.[4] V praktické části bude toto opatření simulováno v rámci samotného návrhu celého modelu, zejména vyřazením některých potenciálních útoků.

Dalším bodem v seznamu opatření je **stanovení bezpečnostních požadavků pro dodavatele**. K porušení bezpečnosti totiž nemusí dojít pouze z vnitřku organizace. Zejména je řeč o přístupu externistů a dodavatelů do systému. Na vině též může být produkt od dodavatele, to ovšem záleží na jejich povaze a na povaze organizace samotné. Podle vyhlášky odpovědná osoba v rámci tohoto opatření zodpovídá za určení pravidel pro jednotlivé dodavatele, které musí zohledňovat požadavky systému organizace v oblasti řízení bezpečnosti informací. Společně s tím je povinna tato osoba vést evidenci všech dodavatelů. V případě změny je její povinností informovat dodavatele o nových opatřeních v organizaci. Zodpovídá za seznamování dodavatelů s pravidly a v případě nedorozumění jejich následnému řádnému vyložení. Dále řídí rizika spojená s dodavateli a zajišťuje kontrolu plnění pravidel z externí strany.[4] V rámci modelu má tento bod váhu zejména ve využití některých dalších možných vektorů útoků.

Mezi jedno ze základních opatření patří bezpochyby **řízení aktiv**. Podle legislativy má pověřená osoba stanovit metodiku pro identifikaci, hodnocení a evidenci aktiv. Aktiva jsou dále rozdělena do skupin, kdy pro každou kategorii se definují patřičná opatření zabezpečení. V rámci tohoto bodu je také činnost vyhodnocení vzájemných vazeb mezi aktivy.[4] Jelikož je model založen na reálné implementaci, bude už vycházet z reálného uplatnění tohoto pravidla. Nicméně i tak je tento bod stěžejní ve fázi přípravy jakéhokoli zabezpečení, jelikož se bude zaobírat tím, co je třeba chránit. Jedná se tak o první logický krok, který by měl být učiněn u takového plánování. V první řadě je třeba vždy identifikovat, které věci,

zařízení, data, též souhrnně označené jako aktiva, je nutné ochránit. Až následně je možné řešit způsoby, metody a konkrétní implementace týkající se samotné bezpečnosti. V modelu se konkrétně jedná o zaručení správné funkčnosti zařízení v síti a nenarušení důvěrnosti, dostupnosti a integrity dat. Při reálné aplikaci ve zdravotnickém zařízení tato ochrana znamená i bezpečí pro zdraví pacientů ze strany technického vybavení, kdy se mohou spolehnout na správnost informací v systému.

V návaznosti na statistiku v úvodu, během níž bylo zmíněno, že za podstatnou částí útoků stojí především sociální inženýrství, je další opatření **bezpečnost lidských zdrojů**. Právě toto organizační opatření dává povinnost osobě zhodnotit stav a potřeby systému a sestavit plán rozvoje bezpečnostního povědomí mezi uživateli systému a zaměstnanci organizace. Především musí být dodržována vhodná pravidelná školení zaměstnanců a seznamování se s pravidly bezpečnostní politiky. Administrátoři a uživatelé s určitou bezpečnostní rolí musí být poučeni o jejich povinnostech. Osoba je rovněž odpovědná za dohlížení na dodržování těchto pravidel zaměstnanci.[4] V rámci modelu, který není reálnou organizací, nemá smysl simulovat školení zaměstnanců jako takové. Stěžejní je ovšem pro práci zejména z důvodu možných skupin útoků pomocí metod sociálního inženýrství. Ty mohou z části obcházet jinak funkční bezpečnostní prvky.

Následující opatření, označené zákonem o kybernetické bezpečnosti jako **řízení provozu a komunikací**, pokládá pověřené osobě úlohu stanovení práv a povinností uživatelů, administrátorů a osob zastávající bezpečnostní role. Vedle toho se musí osoba dále starat o řízení provozu a komunikací, určení souboru postupů a pravidel pro spuštění, ukončení a restart systému nebo obnovení jeho chodu po selhání. Dále osoba řeší ochranu proti škodlivému kódu, řízení technických zranitelností, řízení a schvalování provozních změn. V neposlední řadě do tohoto opatření patří sledování, plánování a řízení kapacit technických a lidských zdrojů. Součástí je také zajištění ochrany informací a dat v průběhu celého jejich životního cyklu. Zároveň s tímto bodem souvisí pravidla vytváření periodických záloh, jejich kontrola použitelnosti a také oddělení testovacího a provozního nasazení systému.[4] Ve vazbě na praktickou část práce se jedná spíš o integrovanou část modelu jako takového. Zejména ohledně záloh a obnovení systému. Tato opatření nemají velký

účinek na možné metody útoků, které budou simulovány na modelu. Slouží zejména při napadení ransomwarem, či v případě pádu systému a jeho následné obnovy.

Řízení přístupu osob je opatření, které lze shrnout jako povinnost pověřené osoby rozdělit přístupová práva a role tak, aby nedocházelo k vytváření bezpečnostních zranitelností. Mezi metody řízení patří vytváření rolí s konkrétními právy pro konkrétní pracovní pozice, využívání pouze prostředků nutných k vykonání činnosti, omezení a kontrola softwarových prostředků, jenž mohou překonat systémové nebo aplikační kontroly či využití nástroje pro správu a ověření identity. Součástí celého procesu je také dokumentace přidělování a odebírání přístupových oprávnění.[4] V praxi se jedná o důležitou součást řízení bezpečnosti pomocí rozdělení minimálních práv běžným zaměstnancům. V modelu práce, který je pouze reprezentací topologie, se toto opatření promítne do některých scénářů útoků.

Opatření **akvizice, vývoj a údržba** cílí především na stanovení bezpečnostních požadavků u projektování, vývoje, testování a údržby systému. Zde je třeba zmínit povinnost pověřené osoby provádět bezpečnostní testování nové verze systému a nových funkcí před nasazením do provozu.[4] V modelu je toto opatření prakticky neaplikovatelné.

Velice důležitým bodem organizačních opatření je **zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.** Jak název napovídá, kritickou funkcí je zde zavedení procesu detekce událostí spolu s vyhodnocováním bezpečnostních incidentů. K tomu je zapotřebí mít definované postupy pro identifikaci, získání a uchování podkladů potřebných pro následnou analýzu incidentu. Při vyhodnocení, že se jedná o riziko, nastává nutnost informovat zaměstnance a osoby bezpečnostních rolí o vzniklé situaci, aplikovat opatření pro kompletní odvrácení incidentu či jeho maximálnímu zmírnění. Zároveň je třeba kybernetické incidenty nahlašovat a uchovávat o nich záznamy a jak byly zvládnuty. Úspěšnost nasazených opatření je měřena a v případě nutnosti dále upravena, aby pokud možno stejný problém znovu nevznikl.[4] Praktická část práce je analýza provedených hrozeb, jejich zvládnutí a vyhodnocení opatření za použití virtuálního modelu místo reálného systému. Tedy se jedná v podstatě o aplikace tohoto pravidla pro modelovou situaci.

Opatření **řízení kontinuity činností** pojednává o hodnocení rizik a analýzy dopadů na systém, respektive na jeho přerušení. Pověřená osoba musí určit dobu obnovení systému po incidentu, dále samotný bod obnovení dat a minimální úroveň poskytovaných služeb. Toto řízení kontinuity jasně definuje pomocí pravidel a havarijních plánů, které pravidelně testuje.[4]

Posledním organizačním opatřením je **kontrola a audit.** Jako u většiny činností i u kybernetické bezpečnosti je zapotřebí provádět audit a dokumentovat jeho výsledky. Kontroluje se zejména dodržování bezpečnostní politiky, kdy na základě těchto výsledků může být sestaven plán rozvoje bezpečnostního povědomí a zlepšení zvládání rizik. Naskytuje se zároveň možnost posoudit nastavená opatření se známými užitečnými metodami z praxe, též známé pod anglickým pojmem *best practice*. Audit by měl být prováděn pravidelně a osobou, která je nezávislá.[4]

Organizační opatření existují jako jeden ze dvou důležitých pilířů kybernetické bezpečnosti. V rámci praktické části této práce je zřejmé, že některé z těchto opatření nelze aplikovat přímo, jako by tomu bylo u reálného subjektu, avšak nepřímo pomocí samotné struktury modelu, která tato opatření implicitně obsahuje.

4.4.2 Technická opatření

Technická opatření jsou více zaměřena na bezpečnost ve významu, ve kterém si ho většina lidí představuje. Jedná se tak o jednotlivé zabezpečovací prvky, a to nejen ty fyzické, kterými může být například biometrické zařízení pro autentizace při přístupu k důležitým komponentám systému, ale i softwarové řešení zabezpečení ve formě antiviru, firewallu či kryptografického protokolu.[5]

Stejně jako organizační opatření jsou vyjmenována v zákonu o kybernetické bezpečnosti 181/2014 Sb. a definovány ve vyhlášce o kybernetické bezpečnosti 82/2018 Sb. Obdobně jako v předchozí kapitole budou opatření nejdříve vyjmenována a následně detailněji analyzovaná. Důležitá je v tomto případě vazba na model v praktické části práce. Mezi jednotlivá technická opatření patří:[3]

- *fyzická bezpečnost,*

- *nástroj pro ochranu integrity komunikačních sítí,*
- *nástroj pro ověřování identity uživatelů,*
- *nástroj pro řízení přístupových oprávnění,*
- *nástroj pro ochranu před škodlivým kódem,*
- *nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,*
- *nástroj pro detekci kybernetických bezpečnostních událostí,*
- *nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,*
- *aplikační bezpečnost,*
- *kryptografické prostředky,*
- *nástroj pro zajišťování úrovně dostupnosti informací a*
- *bezpečnost průmyslových a řídících systémů.*

Stejně jako v případě organizačních opatření, i zde budou některá opatření v modelu z principu ignorována a jiná naopak zahrnuta již v jeho struktuře. Například řešení fyzické bezpečnosti jako takové, mezi které patří zajištění perimetru nebude ve virtuálním modelu možné. Podle vyhlášky lze definovat jednotlivá technická opatření následovně.[4]

Prvním krokem **fyzické bezpečnosti** je, aby odpovědná osoba zaručila předcházení zneužívání aktiv a jejich krádežím či poškozování. K tomuto účelu slouží vymezení perimetru jako efektivní prevence. Stanoví se oblast, kde jsou uchovávány či zpracovávány informace a znepřístupní se osobám nevyžadujících přítomnost aktiv ke své práci. To stejné platí pro místo, kde jsou umístěny technické prostředky informačního a komunikačního systému. Je tak zapotřebí tato místa fyzicky oddělit nebo přesunout samotná aktiva tak, aby bylo možné zamezit vstupu neoprávněných osob.[4] Mezi prostředky fyzické bezpečnosti patří oddělené místnosti, zámky, dveře opatřené zámkem na čipové karty či s biometrickým senzorem, kamerový systém, alarm a další.[5] Model práce s fyzickou bezpečností jako takovou explicitně nepracuje, i když je promítnuta už v samotné topologii laboratoře a systému.

K tomu, aby bylo dosaženo fyzické bezpečnosti, je zapotřebí řešit opatření pojednávající o **nástroji pro ochranu integrity komunikačních sítí**. V tomto

případě se jedná zejména o síť počítačovou. Detailní rozbor počítačových sítí není obsahem práce, avšak je zapotřebí zmínit fakt, že pouze propojit jednotlivé komponenty není dostačující. Pro dosažení základní úrovně zabezpečení je třeba zajistit segmentaci sítě.[4][5] V rámci sítě zároveň aktivně detekovat a následně blokovat jakoukoli nežádoucí komunikaci. Dále pomocí kryptografických protokolů je třeba zajistit důvěrnost a integritu dat při vzdáleném přenosu dat, vzdálené správě systému nebo při přístupu do sítě pomocí bezdrátové technologie.[4] V modelu je opatření reprezentováno samotnou topologií laboratoře a počítačové sítě.

Dalším opatřením je **nástroj pro ověřování identity uživatelů.** Z předchozích pravidel je zřejmé, že kritické segmenty mají být fyzicky i topologicky odděleny. K systému musí ale někdo přistupovat, ať už externě či v případě samotných zaměstnanců. Přístup nemůže být otevřený libovolným osobám. Vyhláška definuje tento bod jako nástroj, který je použit pro ověření totožnosti uživatele, administrátora nebo aplikace. Figuruje zde pověřená osoba, která má využívat nástroj pro správu uživatelských, administrátorských a aplikačních identit. Kromě jiného osobě zákon ukládá povinnost řídit možný počet neúspěšných přihlášení do systému, uchovávat autentizační údaje odolně proti off-line útokům, vyhodnocovat odolnost posílaných autentizačních údajů proti zneužití, ověřit identitu uživatele po určené době neaktivity a dodržovat důvěrnost údajů při zpětném přihlášení. Je možné zde zařadit též využití více faktorového ověření totožnosti.[4] Kromě znalostního faktoru, běžně kombinace jméno a heslo, jsou i další faktory zabezpečení, které se dají podstatně hůř zneužít či odcizit. Mezi běžně používané další faktory patří faktor vlastnický. Běžně se využívá mobilní telefon, kdy navíc k zadanému jménu a heslu přijde zpráva s jednorázovým kódem. Více faktorové ověřování lze potkat i u běžného výběru z bankomatu. Zde se prokazuje majitel karty faktorem vlastnickým, jelikož má fyzickou platební kartu, a zároveň znalostním faktorem ve formě PIN kódu. Mezi zástupce faktoru vlastnictví patří i hardwarové klíčenky, čipové karty i obyčejné klíče. Existuje dále biometrický faktor využívající zejména otisk prstu, profil tváře či sítnici oka.[5] Zmíněno zde bylo heslo, a právě pravidla pro jejich vytváření musí osoba definovat. Především jde o minimální délku, využití symbolů, velkých a malých písmen, čísel nebo odmítnutí

hesla v případě, kdy bylo nalezeno mezi posledními použitými. Podle vyhlášky je minimální délka hesla 12 znaků u uživatelů a 17 znaků pro administrátory a aplikace. Nemělo by být povoleno využít nejznámější hesla, posledních alespoň 12 vlastních hesel a mělo by obsahovat kombinaci znaků, symbolů a čísel. Jelikož je heslo zranitelnější čím déle je nastaveno, definuje vyhláška limit 18 měsíců jako nejdelší možný časový interval pro povinnou změnu hesla.[4] Nelze jednoznačně stanovit bezpečný interval pro změnu hesla, protože každé heslo je jinak silné. Je nutné změnit heslo v případě jeho odcizení nebo prolomení, po kybernetickém incidentu či jen při podezření, že ho někdo jiný mohl získat. V případě prolomení hesla se může útočník dostat do systému jako běžný uživatel z čehož plynou určité směry útoku, které budou v modelu zhodnoceny.

Mezi další body technické bezpečnosti je zařazen **nástroj pro řízení přístupových oprávnění.** Zde má pověřená osoba využívat centralizovaný nástroj přístupových oprávnění, aby zabezpečila řízení práv pro přístup k jednotlivým aktivům systému, nebo pro zápis a čtení dat a změnu oprávnění.[4]

Následující **nástroj pro ochranu před škodlivým kódem** představuje důležitý prvek v kybernetické bezpečnosti. Legislativně je definován jako povinnost pověřené osoby s ohledem na důležitost aktiv zajistit automatickou ochranu koncových stanic, mobilních zařízení, serverů, datových úložišť a vyměnitelných datových nosičů. Ochráněny by měly být i prvky komunikační sítě a veškerá další zařízení v síti, u kterých je to možné. K tomuto bodu spadá i monitorování a řízení používání výměnných zařízení a datových nosičů, správa jejich automatického spuštění obsahu a řízení oprávnění ke spuštění kódu. Základem ochrany proti škodlivému kódu se rozumí rovněž pravidelná aktualizace využívaných nástrojů i samotného softwaru jednotlivých zařízení.[4] V modelu lze zohlednit využitelnými vektory útoku.

Nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů lze také označit pojmem vytváření logů. V organizaci je pověřená osoba zodpovědná za uchovávání důležitých událostí spojených s nejrůznějšími aktivitami uživatelů systému. Přesné detaily ohledně logů jsou popsány ve vyhlášce, nicméně souhrnně je možné říct, že zejména se zaznamenává čas, typ činnosti, identifikace aktiva, identifikace uživatele a výsledek

operace, zda byla provedena či nikoliv. Zaznamenávány mohou též být přístupy do systému, tedy přihlašování a odhlašování jednotlivých uživatelů. Tyto záznamy je nutné bezpečně ukládat a spravovat.[4] Pro testovací scénáře v praktické části nedůležité, avšak v reálné organizaci užitečné a nutné, zejména pro analýzu a následné vyhodnocení logů.

V reakci na organizační opatření ohledně detekce kybernetických incidentů a událostí existuje technické opatření, které ho řeší. Jedná se o **nástroj pro detekci kybernetických bezpečnostních událostí**, který je důležitou součástí celého procesu zabezpečení. Odpovědná osoba využívá v organizaci nástroj, sloužící k ověření a kontrole přenášených dat v rámci komunikační sítě, na perimetru sítě a blokuje nežádoucí komunikaci. Charakterizace detailních prvků, zejména firewall, IDS a IPS, obsažena v kapitole o zabezpečovacích metodách. V rámci legislativy jsou důležité předchozí zmíněné body, aby byla zabezpečena bezpečnost koncových zařízení, serverů, datových úložišť a dalších aktiv.[4] Modelovou situaci toto opatření ovlivní zejména množstvím použitelných způsobů útoků.

Následujícím prvkem technické bezpečnosti je **nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí.** Navazuje na organizační opatření a také na předchozí 2 body. Jestliže je detekována událost, je nutné provést sběr relevantních informací a celou situaci vyhodnotit. K tomuto účelu má pověřená osoba nástroje, kdy v případě kvalitní analýzy je možné odhalit potenciální hrozbu. Zde je žádoucí mít optimálně nastavená bezpečnostní pravidla, aby co možná nejméně docházelo k falešným poplachům.[4]

Aplikační bezpečností se rozumí požadavek na pověřenou osobu vykonávat testování informačního a komunikačního systému se zaměřením na významná aktiva za pomocí penetračních testů. Zejména je kritické provádět tyto testy před uvedením systému do provozu, nebo při jeho významné změně. Pod aplikační bezpečnost spadá zajištění trvalé ochrany aplikací, informací a transakcí před neoprávněnou činností a popřením již provedených činností.[4]

Mezi jedny z posledních technických opatření legislativy patří **kryptografické prostředky**, které zajišťují používání aktuálně odolných kryptografických nástrojů, přesněji kryptografických algoritmů a klíčů. Postupně v čase jsou šifry překonány, a proto je třeba tyto nástroje neustále držet aktuální. Do tohoto opatření spadají

kromě kryptografických klíčů i certifikáty. K povinnostem pověřené osoby patří generovat, spravovat, ukládat, distribuovat a měnit klíče a certifikáty. Dále má osoba v rámci správy povinnost též provádět zneplatnění certifikátů, společně s likvidací starých klíčů. V rámci tohoto opatření je na osobu kladena povinnost pravidelně provádět audit a kontrolu. Při vybírání kryptografických algoritmů může být přihlédnuto k doporučení národního úřadu pro kybernetickou a informační bezpečnost, avšak není to podmínkou.[4]

Nástroj pro zajišťování úrovně dostupnosti informací navazuje na organizační opatření ohledně kontinuity a dostupnosti. Zde odpovědná osoba zavádí různá opatření zajišťující určenou úroveň dostupnosti systému, zejména v případě kybernetického bezpečnostního incidentu. Důležitým prvkem opatření je zajištění zabezpečení kritických aktiv či jejich redundance. Jedná se především o aktiva, která jsou nezbytné pro dostupnost systému.[4]

Posledním technickým opatřením je zajištění **bezpečnosti průmyslových a řídících systémů.** V tématu této práce se jedná o jeden z nejdůležitějších opatření, jelikož právě zdravotnické zařízení obsahuje několik specifických zařízení, které svou architekturou je možné začadit do této kategorie. Legislativa v tomto bodu definuje povinnost pověřené osoby zajistit bezpečnost v rámci průmyslových, řídících a obdobných specifických systémů. K tomu může využít nejrůznějších nástrojů a opatření, které zajistí použití technických a programových prostředků, jenž jsou určeny do specifického prostředí. Dále lze omezit fyzický přístup zaměstnanců a dalších osob k těmto systémům. Kromě jiného lze vyčleněním komunikační sítě od ostatní infrastruktury a omezením vzdáleného přístupu zvýšit bezpečnost systému. Součástí je též ochrana před využitím známých zranitelností. V případě kybernetického incidentu, pak je možné hovořit i o obnovení do normálního chodu.[4] Zde je patrné, že právě tento bod je důležitý pro téma práce. Ve zdravotnické laboratoři se nachází mnoho specifických přístrojů patřící do této kategorie. Jako jedna z největších možných hrozeb bude zkoumána možnost napadnout právě tato zařízení.

Z pohledu legislativy byla provedena analýza organizačních a technických opatření. Ta se v modelu promítnou už přímo v jeho návrhu a topologii. Z části vychází model již z existující implementace v reálném světě, kde jsou tato opatření

již aplikována. Některá chybějící nebo autorovi neznámá relevantní opatření budou na model aplikována a utvoří tak finální formu virtuální laboratoře. Zde následně na základě detekovaných zranitelností budou provedeny možné vybrané hrozby.

4.5 Kategorizace hrozeb pomocí MITRE ATT&CK

V návaznosti na předchozí kapitolu, která definuje kybernetickou bezpečnost z hlediska legislativy, je žádoucí provést analýzu a kategorizaci jednotlivých hrozeb a zranitelností, a to za využití konkrétních taktik a technik. Pro tento účel bude primárně využit veřejně dostupný framework MITRE ATT&CK společně s dokumentem „Threat Landscape 2022“ od Evropské agentury pro bezpečnost sítí a informací, která se zabývá kybernetickou bezpečností v Evropě od roku 2004.[12]

4.5.1 MITRE ATT&CK framework

Prvním z důležitých zdrojů této části práce je framework ATT&CK od společnosti Mitre. Jedná se o online knihovnu taktik a technik útoků, společně s možnostmi obrany proti nim. Uživatel tak může snadno vyhledávat určité kategorie, k nim příslušné bezpečnostní prvky nebo zranitelnosti. Významné je dělení, podle kterého je framework členěn na tři hlavní skupiny: enterprise, mobile a ICS. Existuje podstatný rozdíl mezi těmito kategoriemi, zejména v taktikách samotných útoků, jak popisuje jedna z následujících kapitol.[13][28][29]

4.5.2 Enterprise a ICS

Do skupiny enterprise je možné zařadit všechny běžné systémy informačních technologií (**IT**), které tvoří technické prostředí celé organizace či subjektu. Přesněji se jedná o servery, počítače, síťové prvky a další podobné vybavení.[14] Druhým pojmem ICS, z anglického industrial control system, se rozumí průmyslový řídící systém[8], který patří do skupiny operačních technologií (**OT**).[14] Jedná se o systém řízení technologických celků. Mezi známé příklady těchto systémů patří **SCADA** či PLC řadiče.[8]

4.5.3 Rozdíly IT a OT

Informační technologie (IT) se zaměřují především na data a fungování komunikace napříč organizací. V běžné firmě jde tak často o e-mailovou, webovou a cloudovou službu, společně se zajištěním komunikace mezi stanicemi, servery a prvky sítě. Cílem je **dostupnost**, **důvěrnost** a **integrita** dat, popřípadě i **dostupnost** provozovaných služeb.[14]

Pojem OT, neboli operační technologie, poté nahlíží na organizaci z pohledu propojování, monitorování, správu a zabezpečení průmyslových operací a procesů. Klasickým příkladem spadajícím do kategorie OT je SCADA, neboli supervisory control and data acquisition, který je definován jako systém pro dispečerské řízení a sběr údajů. Může se jednat o průmyslové řídící systémy, nebo počítačové systémy pro kontrolu, správu a řízení procesů. Procesy mohou být několika typů.[8][14]

- **Průmyslové** – výroba elektrické energie
- **Infrastrukturní** – úprava a distribuce pitné vody, odvádění odpadní vody nebo komunikační systémy
- **Zařízení** – letiště či železniční stanice.[8]

Tyto systémy lze pomocí SCADA vzdáleně monitorovat a ovládat. Modelovou situaci této práce, která se zaobírá zdravotnickou laboratoří, lze z části považovat za takový systém, jelikož zdravotnické zařízení vlastní určitou formu centrálního řízení sdružující všechny laboratoře dohromady. SCADA není vymezena pouze na průmyslový sektor a co se týče její struktury, skládá se ze tří hlavních komponent:[15]

- **Centrální řídící centrum** obsahující všechny servery s běžícím SCADA softwarem
- Několik vzdálených **lokálních kontrolních systémů**, jenž mají přístup k fyzickým zařízením
- **Komunikační systém** propojující první dvě komponenty.[15]

Informační a operační technologie řeší trochu jiné zájmy při zabezpečení a soustředí se na vlastní cíle. Oba směry jsou však zneužitelné při potenciálním útoku, a proto je nutné se zaměřit na taktiky a techniky proti oběma z nich. Ať už by

se jednalo o útok na data samotná v IT systémech, či na řízení samotných zařízení pomocí ICS. Z tohoto důvodu byly z MITRE ATT&CK vybrány kategorie Enterprise i ICS pro zastoupení obou skupin.[28][29][14]

4.5.4 Taktika a technika

S kybernetickým útokem, jeho analýzou a následnou kategorizací se pojí dva stěžejní pojmy. Jedná se o taktiku a techniku, které tvoří společně s typem cíle, procedurami a druhem útočníka základní charakteristiku hrozby. Právě taktika zde představuje motivaci útočníka k provedení aktu. Méně formálně se uvádí, že taktika představuje otázky: „proč“, „za jakým cílem“ či „co chtěl útočník získat“. Kupříkladu útočník může požadovat spuštění kódu na cílovém zařízení.[5][30] Taktiku lze též popsat jako vysoko úrovňový popis chování útočníka.[16]

Naproti tomu technika představuje odpověď na otázky: „jak“ a „jakým způsobem“ chce útočník dosáhnout svého cíle. Už tak není vymezena pouze myšlenka útočníka, ale konkrétní metoda, například odcizením a následným podvržením bezpečnostního tokenu.[31] Technika je detailní popis chování útočníka v konkrétní taktice.[16]

K taktice a technice patří i procedury, ty jsou detailním nízko úrovňovým popisem techniky. Dohromady se označují zkratkou TTP a vyjadřují tendence využití konkrétního mechanismu, slabiny nebo malwaru útočníkem.[16]

4.5.4.1 Taktiky Enterprise

Prvním ze dvou pohledů na zdravotnickou laboratoř obsahuje enterprise taktiky, tedy motivace útočníků při napadání běžného IT vybavení oběti. Snahou je tak provést analýzu a následně lokalizovat nejpravděpodobnější důvod útočníků, popřípadě nalezení nejsnadnějšího přístupu za pomocí autorovi známým informacím, které získal z reálné organizace.

Framework MITRE ATT&CK kategorizuje taktiky na enterprise systémy následujícím způsobem:[30]

- **Reconnaissance** (průzkum) – Jedná se zpravidla o jeden z prvních kroků útočníka, kdy se snaží získat informace o svém cíli. Ty následně je možné

využít v identifikaci dalšího jeho postupu, zda budou využity přímo v útoku nebo se stanou základem pro složitější a pokročilejší metody sběru informací. Do této taktiky lze zařadit jak aktivní, tak i pasivní sběr dat.[32]

- **Resource Development** (zajištění zdrojů) – V případě zajištění zdrojů se útočník snaží o získání určitého zdroje, který následně využije při útoku. Pojem zdroj je zde velice obecný a zahrnuje vše od počítačového a programové vybavení, až po například přístupový účet. Tyto zdroje může útočník získat legální nebo nelegální cestou. Konkrétním příkladem zdroje je vlastní DNS nebo e-mailový server, již zmíněný přístupový účet do napadaného systému, vytvořený či koupený malware a botnet.[33]
- **Initial Access** (prvotní přístup) – Tato taktika obsahuje techniky vztažené k pokusu útočníka proniknout do cílového systému či sítě. Obecně je využito veřejného rozhraní webového serveru, které je otevřené do internetu nebo pomocí technik sociálního inženýrství.[34]
- **Execution** (pokus o spuštění škodlivého kódu) - Útočník se snaží spustit na vzdáleném zařízení skript, pomocí kterého může například provést sken vnitřní sítě nebo odcizit data.[35]
- **Persistence** (setrvání) – Vyjadřuje taktiku útočníka setrvat v systému i po restartu, změně přístupových údajů a odříznutí jeho původního připojení k systému. Záměrem je tak vytvořit trvalý přístup k cíli.[36]
- **Privilege Escalation** (zvýšení práv) – Taktika zvýšení přístupových práv je využita útočníkem za cílem dostat ve svém vzdáleném přístupu co největší možná práva, aby se mohl dostat dále do systému. Využít může slabin samotného systému, špatné konfigurace prvků nebo známých slabin. Mezi zvýšené přístupy patří SYSTEM/root, lokální administrátor, uživatelský účet s právy podobným administrátorovi nebo uživatelský účet s právem pro práci se specifickou operací či funkcí, kterou útočník může využít.[37]
- **Defense Evasion** (vyhýbání se zabezpečení) – Snahou útočníka v tomto případě je vyhnout se odhalení během svého útoku. Techniky této taktiky obsahují vypnutí, odinstalování či obcházení bezpečnostních programů

a maskování dat a skriptů. Zneužity mohou být důvěrné procesy, mezi které útočník zamaskuje i svůj malware.[38]

- **Credential Access** (přístup k účtům) – Taktika přístupu k účtům zahrnuje techniky pro získávání přístupových údajů a hesel do systému, často pomocí sledování stisků klávesnice či výpisů z paměti zařízení. S oficiálním účtem může útočník snadněji a více nepozorovaně procházet systém.[39]
- **Discovery** (objevování) – Pokročilejší taktika sledování cíle. Útočník se snaží zjistit co nejvíce informacích o prostředí, vnitřní síti, topologii a jaké možnosti má s momentálním přístupem do systému.[40]
- **Lateral Movement** (postranní pohyb) – Útočník se snaží v prostředí rozšiřovat svůj vliv do dalších systémů. Často ke splnění svého cíle potřebuje útočník přistupovat z více částí systému či potřebuje mít přístup k více účtům.[41]
- **Collection** (sběr dat) – Sběr dat útočník může považovat za svůj primární nebo sekundární cíl. Často jsou data sbírána za účelem následného odcizení, viz Exfiltration. Mezi nejrůznější druhy sbíraných dat patří e-mailová komunikace, audio a video záznam i například data z disků a vyměnitelných médií zapojených do systému.[42]
- **Command and Control** (příkazy a řízení) – Tato taktika znamená pro útočníka snahu o komunikaci s ovládaným napadeným systémem. Pro minimalizaci odhalení je komunikace maskována jako běžný provoz. Existuje mnoho způsobů, kdy výsledná možnost odhalení komunikace záleží také na úrovni zabezpečení cílové infrastruktury.[43]
- **Exfiltration** (opuštění) – Vyjadřuje útočníkovu motivaci pokusit se odcizit data. Jakmile jsou data získána, jsou obvykle zabalena a odeslána v komprimované a zašifrované formě, aby se předešlo odhalení.[44]
- **Impact** (úder/dopad) – Poslední taktikou podle frameworku MITRE ATT&CK na IT systémy je útočníkova snaha o manipulaci, přerušení nebo úplné zničení systému či dat. Jedná se o útok na integritu nebo dostupnost dat, popřípadě celého systému. Pokud je útočníkovým cílem pouze manipulace s daty v jeho prospěch, nemusí být dlouhou dobu odhalen. Může

se však jednat o útočníkův poslední cíl, kdy už dosáhl všech předchozích úkonů.[45]

4.5.4.2 Taktiky ICS

Jelikož lze laboratoř a celé zdravotnické zařízení pokládat za ICS, je zde provedeno představení ICS taktik.[17] Ty jsou některé podobné s jejich enterprise obdobou. Existují zde však rozdílné taktiky a techniky, které poskytují nové vektory útoků.[29] Stejně jako ve zbytku kapitoly, i zde bylo při zpracování postupováno podle MITRE ATT&CK frameworku.

- **Initial Access** (prvotní přístup) – Vyjadřuje snahu útočníka dostat se k ICS systému. Techniky patřící pod získání přístupu kompromitují operační technologická aktiva, IT zdroje a OT komunikační síť. Přístup je zároveň možné získat například z třetích stran, kterými mohou být dodavatelé či vzdálené servisní účty s administrátorským oprávněním.[46]
- **Execution** (spuštění) – Útočník může chtít spustit vzdáleně vlastní kód nebo manipulovat se systémovými funkcemi, parametry a daty bez patřičných oprávnění. Techniky se zabývají převážně možnostmi spustit kód na vzdáleném či lokálním systému, popřípadě na některém z operačních aktiv.[47]
- **Persistence** (setrvání) – Taktika, během které se útočník snaží zachovat si svůj přístup trvale. Přesněji řečeno po změnách přístupových údajů, přerušení jeho pokusu o přístup a restartech systémů či samotných zařízení.[48]
- **Privilege Escalation** (získání práv) – Útočník se snaží různými technikami získat vyšší přístupová práva pro další postup ICS systémem. Obdoba enterprise verze stejné taktiky.[49]
- **Evasion** (vyhýbání se zabezpečení) – V tomto případě se útočník snaží vyhnout zabezpečovacím prvkům systému a zařízení. Může se jednat o techniky odstraňování záznamů o přítomnosti útočníka, odposlouchávání a narušení komunikace nebo například využívání slabin. Útočník se může také rozhodnout využít přístupu do důvěrného zařízení, které bude

vykonávat jeho pokyny, což může být špatně odhalitelné jako vnější působení.[50]

- **Discovery** (objevování) – Taktika objevování spočívá v útočníkově snaze o získání informací ohledně dalších prvcích a struktuře systému, včetně interakcí mezi jeho částmi. Útočník disponující těmito informacemi je schopen identifikovat další zařízení, které později může napadnout a využít v dalším jeho cíli.[51]
- **Lateral Movement** (postranní pohyb) – Postranní pohyb útočníka Mitre definuje jako snahu o pohyb skrz ICS systém. Útočník v tuto chvíli už disponuje určitou znalostí systému a snaží se dostat do dalších prvků a získat přístupy na více místech. V ICS systémech je oproti enterprise verzi této taktiky také možné šíření nejen pomocí IT infrastruktury, ale také pomocí OT sítě. Snahou je získat pozici, ze které bude moci splnit svůj další cíl.[52]
- **Collection** (sběr dat) – Tato taktika je úzce spjata s taktikou objevování. Útočník zde vyjadřuje snahu o získání konkrétních informací, například v podobě odezvy či odpovědi z ICS systému. Mezi hlavní techniky patří sledování síťového provozu, sledování stavů a režimů ICS systému, identifikace speciálních rolí se specifickými oprávněními v rámci systému nebo hledání konfigurací a manuálů k specifickým přístrojům, které nejsou jinak veřejně publikované na internetu. Ty mohou být využity jako zdroj informací o typu přístrojů a slabinách.[53]
- **Command and Control** (příkazy a řízení) – Vyjadřuje pokus útočníka komunikovat a ovládat vzdálené napadené systémy s přístupem do ICS prostředí. Podobně jako u stejnojmenné enterprise taktiky, i zde je snaha o maskování komunikace, aby vypadala jako běžný provoz.[54]
- **Inhibit Response Function** (omezení možností zásahu) – Taktika specifická pro ICS, která popisuje situaci, kdy se útočník aktivně snaží potlačit, omezit nebo úplně přerušit možnost zásahu ze strany operátorů zařízení a ostatních bezpečnostních a ochranných prvků. Běžně, při navození stavu nouze či poruchy, systém zareaguje formou alarmu nebo zásahem operátora, který zmíněný problém rozpozná. Útočník se v rámci této taktiky snaží o mitigaci této odezvy ve formě manipulace údajů, které systém poskytuje jako odezvu,

vypnutím varovných a bezpečnostních prvků nebo odříznutím operátora od řízení. Toto samotné může být cílem útočníka, i když podle Mitre je častěji použita taktika v kombinaci s technikou úderu (Impact), jelikož dokáže způsobit chaos, který na sebe strhne pozornost.[55]

- **Impair Process Control** (narušení procesu) – Předposlední taktikou ICS definuje Mitre motivaci útočníka o manipulaci, přerušení nebo poškození fyzických procesů. Toho dosáhne za pomocí modifikace samotných fyzických přístrojů. V případě této práce by se jednalo o specializovaný přístroj v laboratoři, například pro rozbor krve. Jednou z možností je změna parametrů, a tím špatné vyhodnocování výsledků (popřípadě fyzická práce specializovaného stroje) nebo zablokování přístroje, a tím znemožnění jeho použití do doby vyřešení problému. V případě fyzických zařízení používaných v průmyslu by mohlo dojít ke zničení přístroje a způsobení škody, což už ale patří do následující taktiky. Propojení s předchozí a následující taktikou je patrné. Často totiž může následovat po předchozí taktice, kdy útočník zablokoval možnost systému informovat o chybách či zamezil operátorům zavést účinná protiopatření.[56]
- **Impact** (úder/dopad) – MITRE ATT&CK framework definuje ICS Impact jako taktiku útočníka snažícího se o manipulaci, přerušení nebo zničení ICS, jeho dat a prostředí. Jedná se o stejný motiv jako v případě enterprise. Jak již bylo řečeno v minulé taktice, patří sem fyzické zničení zařízení, poškození jeho okolí, přerušení procesu v organizaci a všechny další případy, kdy je způsobeno finanční, majetkové, reputační či jiné poškození.[57]

4.5.5 Druhy útočníků

Pro detailní modelování hrozeb a plné pochopení možných útoků je zapotřebí znát několik různých informací. Mezi důležité a již vysvětlené patří principy TTP (taktika, technika, procedura), které definují hlavní cíl a způsob provedení útoku. Podstatným faktorem však zůstává i samotný útočník. Pomocí kategorizace lze získat jeho profil a lépe vyhodnotit nejpravděpodobnější vektory útoku. Pod pojmem útočník je možné označit jednotlivce či určitou skupinu snažící se o aktivaci

kybernetické hrozby. Rozdělení do skupin tak lze udělat z několika pohledů, mezi které patří motivace, znalosti, počet a možnosti.[18]

Základním přehledem je rozdělení útočníků na 4 hlavní kategorie, které lze najít v mnoha veřejných zdrojích. Zdrojem zde bude dokument Threat Landscape od společnosti Enisa, jelikož dále definuje trendy těchto skupin. Ty budou relevantní v další kapitole. Zmíněné kategorie zní následovně:[11]

I. **State-sponsored actors** (státem podporovaní aktéři) – Nejvíce profesionální a sofistikovaní ze zmíněných typů útočníků s přístupem k prakticky neomezenému zdroji znalostí a peněz, jelikož jsou sponzorováni konkrétní zemí či skupinami více států. Nejčastější motivací této skupiny je špionáž, získávání citlivých informací z průmyslu a národních společností ostatních států. Státem podporovaní aktéři mají své místo například i v kybernetické válce.[5][18][19]
II. **Cybercrime actors** (kybernetičtí zločinci) – Za druhou významnou kategorii lze považovat kybernetické zločince. Jedná se o jedince či skupiny spojené s konáním trestných činů v kyberprostoru. Často jsou součástí organizovaného zločinu a jejich primárním cílem je finanční prospěch. Mezi hlavní taktiky této skupiny patří přístup k datům a jejich následná exfiltrace za účelem prodeje nebo jejich zničení na objednání. Zaměřují se zejména na instituce pracující s mnoha citlivými i relevantními daty.[5][18][19]
III. **Hacker-for-hire actors** (hackeři najmutí na zakázku) – Hacker je osoba disponující technickými znalostmi v oblasti kybernetické bezpečnosti. Obecně existují 3 hlavní kategorie hackerů, lišící se podle především morálních a legislativních zásad. Jelikož záleží na schopnostech daného jednotlivce nebo skupiny, nelze blíže specifikovat znalosti a prostředky, kterými budou disponovat. To záleží na jejich objednavateli. Většinou sledují vlastní cíle jako je reputace nebo bohatství.[18]
    - **White hat hacker** – Etická skupina neporušující zákon a pracující čistě legálně. Na zakázku pouze testují bezpečnost systémů

a poskytují zpětnou vazbu o slabinách a možnostech neoprávněného přístupu.[18]

- **Gray hat hacker** – Naproti etické skupině se liší v tom, že do systému nevstupuje na zakázku z cílové organizace. Po proniknutí do systému následně informuje jeho majitele o odhalených slabinách.[18]
- **Black hat hacker** – Skupina hackerů sledující pouze své zájmy. Nemají problém s překročením zákona a nabourávání systémů na zakázku.[18]

IV. **Hacktivists** (hacktivisté) – Dalším názvem lze tuto skupinu nazvat jako kybernetičtí aktivisté. Využívají především útoků ve formě odcizení a následné zveřejnění dat ku prospěchu jejich agendě. Nejčastěji je jejich motivací vlastní přesvědčení nebo pomsta. Peněžní zisky nejsou pro ně natolik důležité. Jejich schopnosti a finanční možnosti závisí na samotných členech skupiny či jejich sponzorovi. Některé zdroje je definují jako samozvané bojovníky za svobodu slova, protože odhalují pravdu nebo tajné informace „zlých korporací".[18][19]

Tato rozdělení definují základní kategorie útočníků hlavně podle finančních a znalostních možností, kterými disponují. Dále je možné útočníky kategorizovat následujícím způsobem.[18][19]

- **Cyber Terrorists** (kybernetičtí teroristé) – Definuje typ útočníka, který se snaží způsobit největší možný chaos a ničení. Mezi cíle této skupiny lze zařadit mazání dat, zastavení poskytovaných služeb a následné ničení veškerých možných cílů. Stejně jako u běžného terorismu, motivací je upozornit na svou ideu.[19]
- **Script Kiddies** (skript děťátka) – Amatéři s omezenými znalostmi a finančními prostředky. Disponují pouze nástroji a metodami dostupnými volně na internetu. Hlavní motivací je především vlastní potěšení ze samotného nabourávání do systému. Často využívají dávno známé a starší slabiny. Nepředstavují velkou hrozbu.[18][19]

- **Recreational Cyber Attackers** (rekreační hackeři) – Jejich hlavním motivem je sláva a získávání reputace. Podobné předchozí kategorii s tím rozdílem, že znají slabinu svého cíle. Vyznačují se omezenými možnostmi, znalostmi a malou paletou dostupných nástrojů.[18]
- **Insiders** (osoba uvnitř organizace) – Pod tímto pojmem lze najít osoby, které mohou a zároveň nemusí být samotnými hackery. Celý pojem je dosti obecný a lze dále dělit. Hlavní myšlenka je však stejná. Člověk, který má přístup do organizace, má také možnost obejít vnější bezpečnostní opatření systému a poskytnout výchozí bod k útoku zevnitř. Rozdělit tuto kategorii je možné podle motivace a účelu. Touto osobou může být zaměstnanec, bývalý zaměstnanec, stážista nebo ve specifických případech i zákazník, který získal částečný vhled a přístup do firmy.[18][19]
    - **Malicious Insider Threats** – Do prvního typu hrozeb osob uvnitř organizace je možné zařadit všechny úmyslné činy s cílem uškodit. Nejčastěji jde o odcizení dat nebo jejich smazání. Typickým příkladem může být zaměstnanec, který dostal výpověď a chce se mstít. Dále se může jednat o špatně finančně ohodnoceného nebo nespokojeného pracovníka, který dostane peněžní ohodnocení za doručení interních dat. Motivací je tak pomsta nebo finanční odměna.[18][19]
    - **Accidental Insider Threats** – Další kategorií se rozumí náhodná chyba zaměstnance. K útoku může dojít omylem bez záměru dotyčné osoby, a tedy zde motivace k útoku úplně chybí. Typickým příkladem může být nechtěné smazání důležitých dat, které nejsou zálohovány a nemají nikde svou kopii.[18] Jiný zdroj tuto kategorii označuje jako **internal user error**.[19]
    - **Negligent Insider Threats** – Posledním druhem vnitřních útoků zaměstnaných osob je nedbalost. Neopatrností či nedodržováním pravidel může dojít k narušení bezpečnosti. Společnou vlastností s předchozí kapitolou je fakt, že v obou případech osoba nemá motivaci k provedení útoku a došlo

k němu zcela náhodou. Na rozdíl však od nešťastné události, zde za to může pracovník a jeho nedodržování stanovených pravidel.[18]

Jak je patrné, útočníků je několik typů, kteří se liší jejich motivací, znalostmi, možnostmi a úmyslem. Pro zajištění největší bezpečnosti při modelaci hrozeb je vhodné odhadnout profil možných útočníků a zaměřit se na jejich možnosti a pravděpodobné přístupy do systému. Kvůli tomu je důležité znát samotné útočníky. Obecně je možné je rozdělit podle motivace, zda vůbec chtějí či nechtějí kompromitovat systém. V prvním případě se jedná o nehodu či nedbalost. V druhém případě může být účelem k provedení útoku politický, finanční či osobní.[18]

4.5.6 Trendy hrozeb

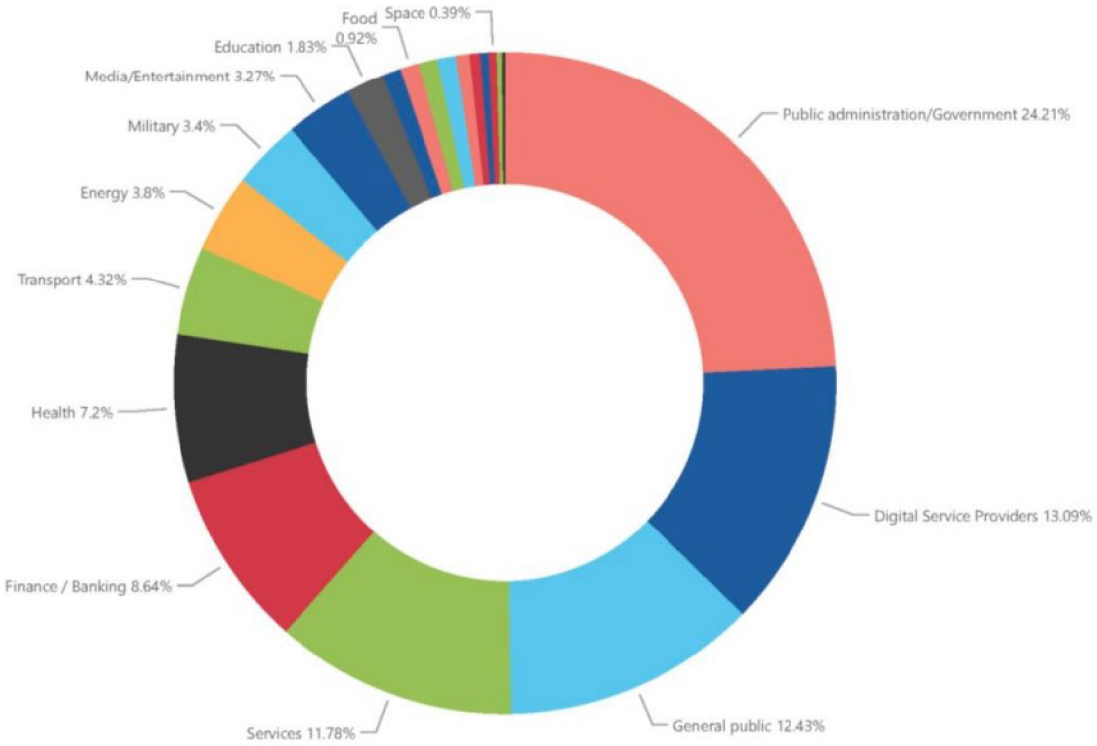
V rámci zajištění bezpečnosti je kromě znalosti útočníka a samotných útoků také vhodné sledovat trendy a inovace v oblasti hrozeb. Bez monitorování aktualit může snadno dojít k zestárnutí systému, jehož zabezpečení neodolá novým typům hrozeb. Analýzu trendů lze hodnotit z několika pohledů. Ať už podle čtyř hlavních výše zmíněných skupin útočníků, tak i například podle taktik a technik definovaných Mitre.[11]

Trendy podle útočníků je možné shrnout následovně. U **státem sponzorovaných aktérů** byl za rok 2022 zaznamenán zvýšený nárůst ve využívání kritických slabin a útoků nultého dne (0-day exploit), přesněji chyb, které nebyly výrobcem softwaru opraveny. Právě využívání těchto slabin bylo zjištěno jako nejčastější vektor útoku. To je možné vysvětlit zejména kvůli rekordnímu počtu nově identifikovaných zranitelností.[20] Dalším důvodem je pravděpodobně podle společnosti Enisa samotná digitalizace, kterou vzniká větší množství systémů. Státem podporovaní aktéři zároveň mají zdroje na hledání a případné vytváření slabin, jenž jim umožní přístup do cílového systému.[11] Zdroj Mandiant uvádí invazi na Ukrajině za další zdroj státem podporovaného úsilí o získání přístupu a informací k systémům, kdy je primárně cíle dosaženo využitím slabin.[21] Enisa ve svém vyjádření u této kategorie útočníků zdůraznila na zvýšenou úroveň ohrožení OT sítí a ICS. Z 18 nových skupin byly tři zaměřeny právě na tyto technologie.[11]

Kategorie **kyberzločinců** a obecně kybernetického organizovaného zločinu, zaznamenaly nárůst ve využívání napadení dodavatelského řetězce. Vzrostl počet útoků na průmyslový sektor, kde je především využito útoků proti OT sítím, dále poté zdravotnický a energetický sektor. Společnost Enisa dále doporučuje zahrnout útok na dodavatele do modelování hrozeb prováděné v organizaci. Oblíbeným nástrojem kyberzločinců se stal ransomware a v případě OT sítí specificky zaměřený malware na specifické zařízení či systém. Vzhledem k rozšíření povědomí o ransomwaru za poslední roky se několik organizací rozhodlo místo zaplacení výkupného obnovit systém ze zálohy. Za rok 2022 bylo pozorováno několik případů využití ransomwaru na zašifrování samotných záloh, aby byly oběti donuceny k zaplacení požadované částky.[11]

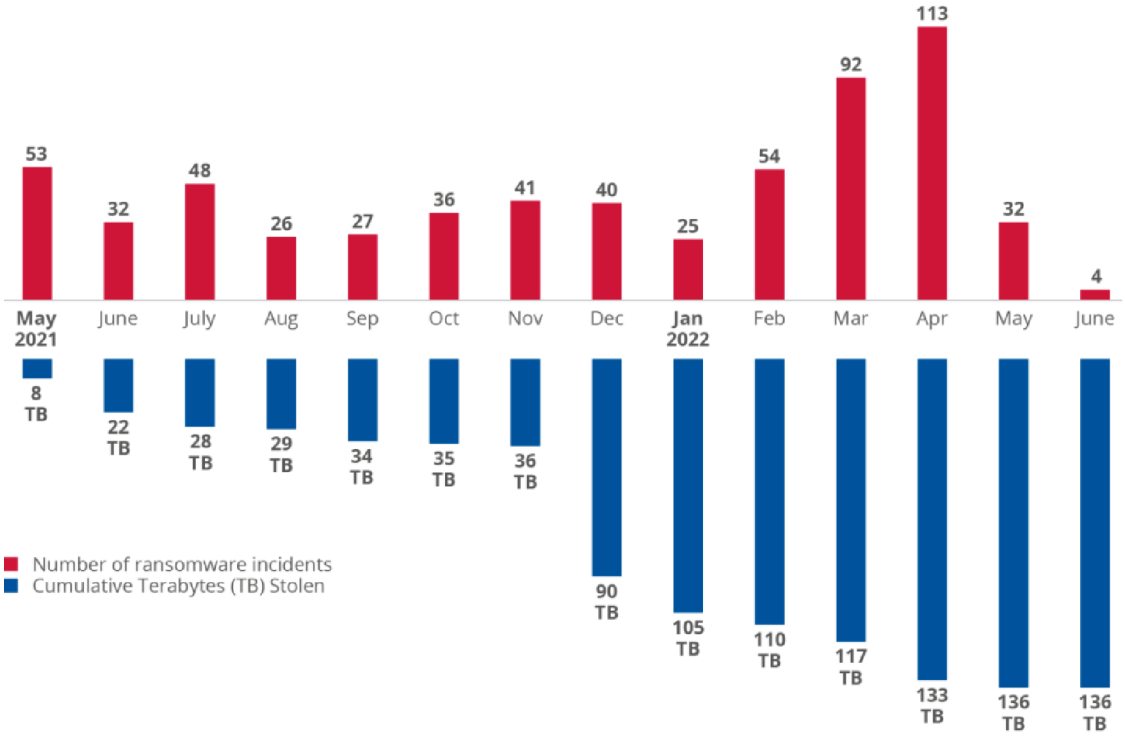
Hackeři na zakázku se stali populárnějšími a více využívanými. Za nárůstem stojí pravděpodobně větší pozornost médií u kybernetických hrozeb[11] a agrese na Ukrajině ze strany Ruska.[21] Mediální pozornost přilákal za poslední dobu například Projekt Pegasus, který se šířil přes mobilní platformu a sbíral data od přibližně 30.000 novinářů, právníků a světových politiků.[22] Zároveň dochází k použití kybernetických nástrojů soukromých společností a subjektů, využívání slabin a spolupráce se skupinou vládou podporovaných aktérů.[11]

Trend u poslední skupiny **hacktivistů** je možné označit za vznik nové vlny kybernetického aktivismu. Primárně za touto vlnou stojí konflikt na Ukrajině a subjektivní druh motivace skupin se zapojit v rámci jejich přesvědčení.[11][21] Zaznamenána byla aktivita přibližně v 70 známých skupinách, které se po začátku konfliktu přidali k jedné ze stran. Nejčastějším cílem se pro tyto skupiny staly nejen běžné organizace nepřátelské strany, ale také subjekty patřící do kritické infrastruktury. Dalším často napadeným druhem organizací se stala samotná média a vládní organizace. Mezi útoky, které skupiny využily patří omezení či úplné přerušení dostupnosti DDoS, znehodnocování dat i aktiv a v neposlední řadě úniky dat.[11][23] Během konfliktu se objevil i případ využití ransomwaru na systém správy železniční sítě Běloruska za účelem zpomalit zásobování ruských jednotek.[11]



Obrázek 1 – Zasažené sektory v rozmezí 06/2021-07/2022
Zdroj: Enisa Threat Landscape 2022[11]

V rámci trendů samotných technik hrozeb lze pozorovat několik zajímavých poznatků. V první řadě se jedná o vysoký počet případů užití ransomwaru a enormní počet odcizených dat. Mezi hlavní představitele v roce 2022 patří ransomware LockBit, Conti a ALPHV/BlackCat. Cílem byly různé systémy, primárně s operačními systémy Linux a Windows 7 a vyšší. Dále k trendům patří zvýšený počet přístupů do systému pomocí sociálního inženýrství, který se stal nejčastějším počátečním vektorem útoku. S nástupem pandemie COVID-19 se rozmohla celosvětově práce z domu, což s sebou v mnoha případech přinášelo vzdálené připojování do sítě organizace. Útočníci tak v mnoha případech využívají prolamování slabých přihlašovacích údajů pomocí útoku hrubou silou v kombinaci se sociálním inženýrstvím k zajištění prvotního bodu v systému. Obě metody jsou levné a nenáročné.[11]



Obrázek 2 – Poměr mezi počtem útoků ransomware (červená) a počtem odcizených dat v TB (modrá)
Zdroj: Enisa Threat Landscape 2022[11]

Se vzrůstajícím počtem nasbíraných dat vzrostl také počet nechtěných i úmyslných úniků dat. Přičemž přibližně 80 % dat bylo odcizeno zvenku za pomoci útoku na data, zatímco zbylých 20 % tvoří nechtěné úniky dat zevnitř organizace. Motivaci experti vyhodnotili v 90 % za účelem finančního zisku a v necelých zbylých 10 % tvořila převážnou část špionáž. Mezi nejvíce napadené sektory v tomto ohledu patří finanční, pojišťovnický a zdravotnický sektor. V posledním ze zmiňovaných sektorů byla data napadena ve třech čtvrtinách případů pomocí zneužití webové aplikace, nejrůznějších slabin v konfiguraci a přístupem do samotného systému. Dále bylo zaznamenáno u 39 % případů využití osoby uvnitř organizace.[11]

V samotných vektorech útoků se rok 2022 moc nelišil od předchozího roku. Mezi nejčastější vektory patří odcizené přihlašovací údaje ve 40 %, ransomware ve 25 % a phishing v přibližně 20 % útoků. Další nárůst byl detekován ve využívání cizích, či syntetických identit.[11]

4.6 Dílčí závěr

Legislativně určené zranitelnosti a hrozby jsou promítnuty dále v práci na vybraných taktikách a technikách útoků. Na základě informací z rozhovoru s odborníkem ze zdravotnického zařízení a z odpovědí v dotazníku existuje několik vektorů útoků na základě vyjmenovaných zranitelností. Jedná se především o možnou zastaralost informačního a komunikačního systému a nevhodnou bezpečností architekturu.

Na základě těchto zranitelností a za pomocí dotazníku a rozhovoru lze specifikovat, že mezi nejpravděpodobnější hrozby ze seznamu definovaným vyhláškou o kybernetické bezpečnosti patří zneužití identity, a to zejména při vzdáleném přístupu. Škodlivý kód při nahrání malwaru nebo při pochybení ze strany zaměstnanců. Dalším bodem je zneužití nebo neoprávněná modifikace údajů. Zneužití vnitřních prostředků a sabotáž jsou pak typické pro útočníky uvnitř organizace. Poslední potenciální hrozbou může být zneužití vyměnitelných technických nosičů dat.

Taktiky a techniky podle MITRE ATT&CK jsou v práci promítnuty v samotných scénářích. Zvoleny byly na základě relevance ve vazbě na trendy kybernetických hrozeb, kategorie útočníků a výstupy dotazníkového šetření.

5 Scénáře kybernetických hrozeb

Cílem práce je provést modelování hrozeb v laboratorním prostředí, které reprezentuje podobu reálného prostředí. Modelování hrozeb definuje NIST (Národní institut pro standardy a technologii) jako proces vyhodnocení možných hrozeb a obranných opatření vybrané logické entity. Pod pojmem entita může být samotný systém, data, aplikace, prostředí nebo uživatel. Pro správné a kvalitní provedení analýzy je třeba disponovat znalostmi o potenciálních útocích, slabinách řešeného systému a útočnících.[24]

Na základě dotazníkového šetření a získaných znalostí z předchozích kapitol je možné definovat modelovací scénáře zaměřené na potenciální problémy systému. Navrženy jsou tři scénáře, které odráží potenciální slabiny na základě možných hrozeb, jejich trendů za poslední roky a kategorií útočníků. Scénáře jsou logicky členěny podle prvotního průzkumu, dále pohybu v systému a infiltraci až po dosažení bodu, kdy je útočník teoreticky schopen ovlivnit systém samotný. Všechny tři scénáře dohromady tak popisují jeden souvislý komplexní útok od začátku do konce.

Součástí každého scénáře je i soupis relevantních taktik a jejich technik. Dále se mnoho z nich dělí na další sub-techniky. Ke dni zpracování diplomové práce framework obsahuje v enterprise oblasti 193 skupin a 401 jednotlivých technik.[31] Z důvodu rozsáhlosti zkoumané problematiky byly uvedené skupiny a techniky podrobeny selekci, v rámci které bylo vybráno omezené množství technik relevantních ke zkoumané problematice.

5.1 První scénář – Analýza

První scénář obsahuje prvotní fázi útoku na subjekt. Definovat lze primárně pomocí **Reconnaissance** taktiky. Jedná se o první nutný krok v každém kybernetickém útoku. Taktika průzkumu cíle je obsáhlá a nelze jednoznačně definovat, jaké všechny informace útočník bude potřebovat, či které informace mu budou užitečné. Čím více je schopen získat, tím pravděpodobněji bude útok úspěšnější. S větším počtem informací o oběti je zároveň možné volit další možné vektory útoků.

Za sekundární lze považovat taktiku **Resource Development**. Tu však nelze v práci na modelu reálně otestovat. Pozornost však bude zaměřena jejím technikám získávání uživatelských účtů ve spolupráci s metodami sociálního inženýrství.

Součástí zjišťování útočníka může být získání přehledu o topologii cílové sítě. Tyto informace již autor získal pomocí konzultace a dotazníku. Základem prvního scénáře je tak zanalyzovat a otestovat, jaké informace je útočník schopen získat pomocí metod aktivního skenování, ale i za použití metod sociálního inženýrství. V rámci sběru dat je zaměřena pozornost i na získání informací o zaměstnancích, které by bylo následně možné využít k tomuto účelu. To je realizováno analýzou internetových stránek zdravotnické organizace a pokusem o získání informací pomocí internetových databází a nástrojů. Cílem je zjistit, zda je možné identifikovat opatření, která by přispěla k bezpečnosti organizace a zamezila prvotnímu sběru dat, které dále umožňují útočníkovi v dalším počínání. Z bezpečnostních důvodů nebude v práci zmiňován žádný odkaz, či jakákoli konkrétní jména a obsah bude anonymizován. Výstupy jsou uvedeny v kapitole 6.

5.1.1 Relevantní taktiky a techniky

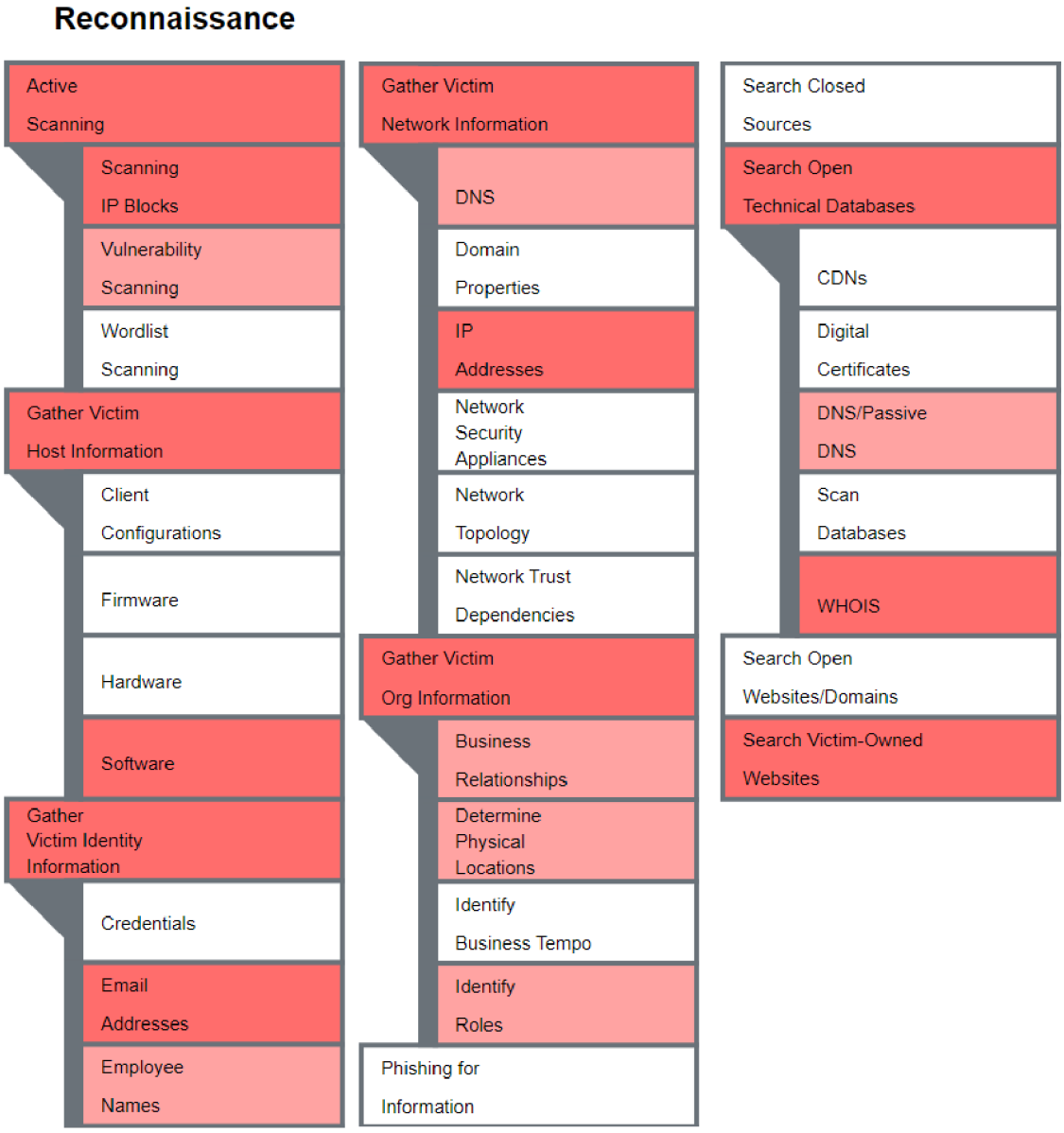
Relevantní enterprise taktikou pro první scénář je **Reconnaissance**, která definuje samotný prvotní průzkum. Pro následné podpůrné operace, které během testování ve virtuálním prostředí nelze nasimulovat, se využívá technik **Resource Development**.

Mezi základní využité techniky MITRE ATT&CK frameworku patří především sběr informací o oběti pomocí aktivního skenování, získání informací o softwaru na cílovém zařízení, zjištění organizačních struktur, a to včetně jmen, e-mailových adres a rolí některých zaměstnanců, prohledání otevřených technických databází a průzkum provedený na obětí vlastněnou internetovou stránkou. Společně s cílovou zdravotnickou organizací byly také prohledány webové stránky dalších zdravotnických zařízení v regionu spadajících pod správu společného subjektu.

Přesné techniky Mitre jsou pro **Reconnaissance** vypsány v následujícím seznamu:[32]

- **Active Scanning** – Scanning IP Blocks, Vulnerability Scanning
- **Gather Victim Host Information** – Software
- **Gather Victim Identity Information** – Email Addresses, Employee Names
- **Gather victim network information** – DNS, IP addresses
- **Search victim-owned websites**
- **Search open technical databases** – DNS, WHOIS

Výše zmíněné techniky jsou zobrazeny v rámci frameworku ATT&CK na Obrázku 3. Výraznější barvou jsou označeny techniky, kterým byla věnována větší pozornost.



Obrázek 3 – Zvolené techniky taktiky Reconnaissance
Zdroj: Vlastní

5.2 Druhý scénář – Možnosti uvnitř systému

Druhý scénář volně navazuje na první fázi kybernetického útoku enterprise subjektu a rovněž je úzce svázán s následujícím scénářem. Zde se pracuje s předpokladem, že již útočník má přehled o oběti, disponuje potřebnými znalostmi, prvotním přístupem a jeho cílem se nyní stává zjistit, jak může dále pokračovat v útoku. Zároveň je modelována snaha útočníka o rozšíření své působnosti na další aktiva v síti.

Scénář obsahuje primárně Mitre taktiky **Initial Access**, **Execution**, **Privilege Escalation**, **Defense Evasion**, **Credential Access**, **Discovery**, **Lateral Movement** a **Collection**. Na začátku se vychází z předpokladu útočníkova přístupu. Z dostupných informací byl vyhodnocen nejpravděpodobnější přístup pomocí sociálního inženýrství, přesněji přes odcizený účet, spuštěný malware nebo získání hesla z jiných služeb využívaných zaměstnancem. Dále pak prolomení hesla pomocí slovníkového útoku, či získání přístupu přes vyměnitelné externí paměťové médium.

Než však dojde k naplnění scénáře, je zapotřebí sestavit fyzický model topologie. Pro samotné testování se využívá nástrojů specializovaných k penetračním testům a frameworku společnosti Mitre. Ten obsahuje pro každou relevantní taktiku tohoto scénáře několik technik a jejich implementace, které lze zkusit na připravené topologii. Z tohoto důvodu je tento scénář mnohem obsáhlejší oproti prvnímu a třetímu scénáři, kvůli čemuž poté některé společné kroky v posledním scénáři nebudou znovu simulovány.

Cílem scénáře je zkoumat možnosti útočníka za pomocí zmíněných nástrojů a navrhnout doporučení, která by minimalizovala jeho možnosti po přístupu do systému.

5.2.1 Relevantní taktiky a techniky

Vzhledem k počtu testovaných taktik a technik je scénář obsáhlý. Jak je ovšem patrné z popisu scénáře, jedná se především o získání prvotního přístupu v systému, kde je následně testován pokus o získání vyššího oprávnění. Na základě statistiky byl vyhodnocen jako nejpravděpodobnější bod přístupu metodou sociálního inženýrství, pomocí infikovaného přenosového média, nebo přes

odcizený účet. Předpokládá se následně útočníkova motivace spustit svůj vlastní kód či skript, nejpravděpodobněji z běžné příkazové řádky. V neposlední řadě je zaměřena pozornost na detekci a vyhnutí se zabezpečovacím prvkům, získání dalších přihlašovacích údajů, sběr dat a prozkoumání vnitřní sítě.

Mezi relevantní enterprise taktiky a techniky MITRE ATT&CK patří:

Initial Access[34]

- Phishing
- Replication Through Removable Media
- Valid Accounts

Execution[35]

- Command and Scripting Interpreter – PowerShell, Windows Command Shell, Unix Shell, JavaScript

Privilige Escalation[37]

- Abuse Elevation Control Mechanism
- Valid Accounts

Defense Evasion[38]

- Abuse Elevation Control Mechanism
- Impair Defenses
- Indicator Removal
- Valid Accounts

Credential Access[39]

- Credentials From Password Stores
- OS Credential Dumping
- Steal Web Session Cookie
- Unsecured Credentials

Discovery[40]

- Account Discovery
- Browser Bookmark Discovery
- Password Policy Discovery
- Process Discovery
- Software Discovery
- System Information Discovery

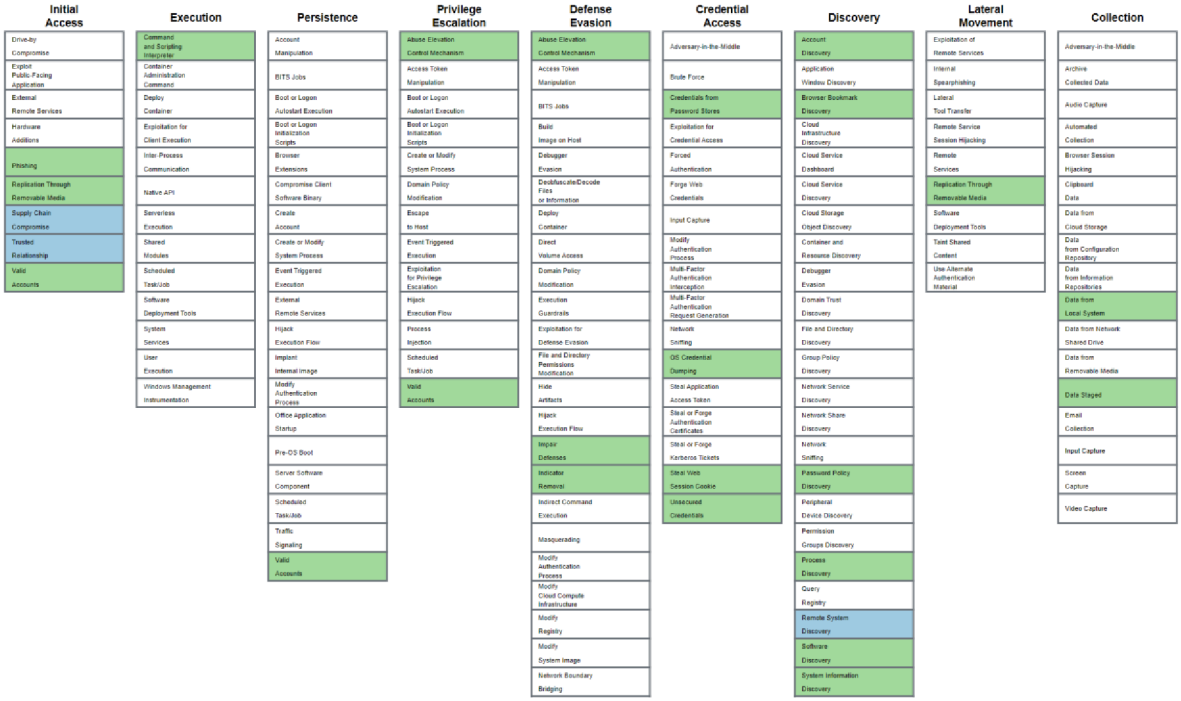
Lateral movement[41]

- Replication Through Removeable Media

Collection[42]

- Data From Local System
- Data Staged

Obrázek 4 reprezentuje výše zmíněné techniky mapované na část frameworku MITRE ATT&CK. Techniky pro druhý scénář jsou vyznačeny zelenou barvou.



Obrázek 4 – Vyznačené výše uvedené techniky
Zdroj: Vlastní

5.3 Třetí scénář – Ovlivnění systému

Třetí a poslední scénář navazuje na kroky kybernetického útoku otestované v předchozí modelové situaci. Velké množství kroků se překrývá s předchozím scénářem, a proto zde jsou relevantní pouze techniky, které jsou odlišné. Jednat se tak bude zejména o odcizení dat a možnosti útoku na samotný systém, což lze kategorizovat Mitre taktikami **Exfiltration** a **Impact**.

První dva scénáře obsahovaly různé taktiky a techniky útoků v rámci enterprise kategorie cíle. Jak bylo však zmíněno dříve, ve zdravotnických zařízeních se také běžně vyskytují určité formy ICS systémů. Z tohoto důvodu se třetí scénář věnuje z části i oblasti ICS, kdy v rámci modelu není úplně možno otestovat reálný ICS systém, avšak je provedena analýza rizik ICS scénářů na základě útoku na zařízení s enterprise platformou. Pracuje se s předpokladem spuštěného ICS klienta na koncové stanici, kde jsou testovány vybrané techniky.

Přístup do systému byl identifikován nejpravděpodobněji na základě trendů přes dodavatele, či za pomocí sociálního inženýrství. Vzhledem ke statistikám, mezi nejpravděpodobnější motivace útočníka může patřit využití ransomwaru či odcizení dat.

Cílem scénáře je zjistit a analyzovat možné metody napadení dostupnosti, integrity či důvěrnosti dat nebo cílového zařízení. Součástí je i část zaměřená na ICS systémy, zejména na klientské verze spuštěné na běžném operačním systému Windows.

5.3.1 Relevantní taktiky a techniky

Poslední scénář je nadstavba na jeho předchůdce s cílem reprezentovat útočníkovu snahu o získání dat, ovlivnění systému či k získání přístupu k platformě podporující ICS systém. Obsaženy jsou proto nejen doplňující taktiky a techniky Mitre v rámci enterprise, ale i ICS, které jsou vysvětleny a je provedena pouze analýza na základě informací z frameworku ATT&CK.

Initial Access[34]

- Trusted Relationship

Discovery[40]

- Remote System Discovery

Exfiltration[44]

- Exfiltration Over Physical Medium

Impact[45]

- Data Destruction
- Data Encrypted for Impact
- Service Stop
- System Shutdown/Reboot

ICS Initial Access[46]

- Supply Chain Compromise

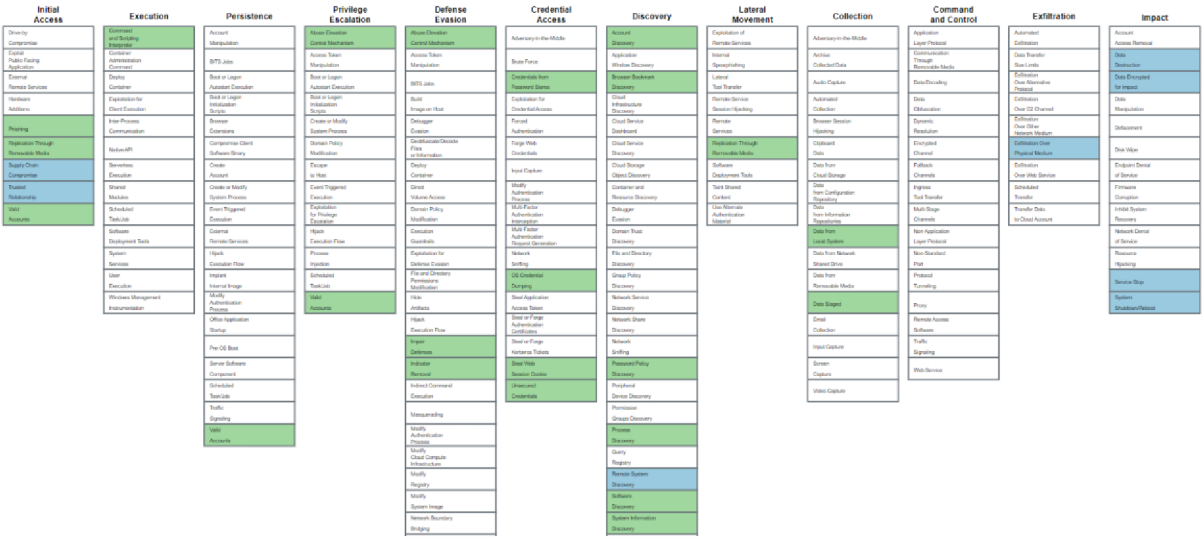
ICS Inhibit Response Function[55]

- Alarm Suppression

ICS Impair Process Control[56]

- Modify Parameter

Zvolené taktiky pro třetí scénář jsou vyznačeny v rámci části frameworku MITRE ATT&CK na Obrázku 5 modrou barvou.



Obrázek 5 - Vyznačené výše uvedené techniky
Zdroj: Vlastní

6 Testování scénářů ve virtuálním prostředí

V teoretické části bylo modelování hrozeb definováno jako zhodnocení rizik na základě znalosti útočníka, hrozeb, systému a možností obrany. Primární náplní testování scénářů ve virtuálním prostředí je provést tyto testy na modelovaném subjektu zdravotnického zařízení. Na základě testování a výstupů z jednotlivých scénářů jsou identifikovány možné slabiny, zpracována jejich hodnocení a doporučení. U možných slabin je dále kladen důraz na zjištění účinného opatření, které by zamezovalo napadení.

6.1 První scénář

V rámci prvního scénáře je analyzováno, jaké informace je možné zjistit o zdravotnickém subjektu. Sociální inženýrství je reprezentováno v práci pouze souhrnem informací, se kterými může útočník pracovat. Autor práce nezasílal žádné podvodné e-maily do reálné organizace.

6.1.1 Využívané nástroje

Využito je především technických internetových databází v kombinaci se stránkou vlastněnou obětí. Z veřejných databázových nástrojů bylo využito WHOIS (https://who.is/) a CenSys (https://search.censys.io/). Z aktivních nástrojů pak nástroj pro skenování adres a portů Nmap.

Při testování scénáře bylo zjištěno, že zdravotnické zařízení využívá s dalším zařízením společnou šablonu internetového portálu. Obě organizace totiž spadají pod jeden nadřazený subjekt. Prohledán tak je i internetový portál druhé organizace ve snaze získat dodatečné informace.

6.1.2 Identifikované skutečnosti

Přesné hodnoty jsou v práci vzhledem k povaze dat anonymizovány. V technických databázích byly o doméně organizace zjištěny následující údaje:

- Zkrácená jména administrátorů domény
- Datum registrace domény
- Kontakt na administrátory systému – jméno, adresa, název organizace

- Název organizace, pod kterou je doména zaregistrována

Otevřená databáze WHOIS a další podobné jsou schopné poskytnout veřejné informace, které samy o sobě nedávají útočníkovi možnost provést ihned specifický útok. K čemu ovšem mohou být využité je další analýza a studování dotyčných osob. Zde záleží na typu útočníka. Autor práce zkusil využít pro zjištění informací vyhledávač Google a sociální sítě LinkedIn a Facebook. U hned prvního administrátora byla do 2 hodin zjištěna osobní i pracovní e-mailová adresa, místo bydliště, pracovní i osobní telefonní číslo, a dokonce byla nalezena podepsaná anonymizovaná smlouva touto osobou.

U smlouvy je patrný nedostačující způsob, kterým je anonymizovaná. Jedná se o výpis z registru smluv, spadající pod oficiální správu České republiky s doménou https://smlouvy.gov.cz/. Při jednoduchém označení začerněného textu představující e-mailovou adresu se uživateli v dolní části obrazovky zobrazí odkaz s jejím přesným zněním. I další údaje, které nemají takto automatizovaný odkaz je možné jednoduše ze smlouvy získat. Stačí označit kýžený kus textu a vykopírovat obsah například do editoru či prohlížeče.

V závislosti na typu útočníka je možné takto dále postupovat a zjišťovat stále větší množství informací. Mezi užitečné druhy patří například využívané služby obětí. Tyto informace následně míří na téma sociálního inženýrství, jehož testování není předmětem této práce. Nicméně je třeba poukázat na fakt, že lze získat mnoho informací k tomuto účelu snadno využitelným.

Následuje využití internetového nástroje CenSys. Ten po zadání doménového jména či IP adresy serveru načte informace o službách a jejich portech. Jedná se o metodu skenování, která není tak detailní jako například nástroj Nmap, nicméně je dostupná online ze všech zařízení. V případě prvního scénáře jsou výstupem ze služby dva nalezené záznamy o organizaci, jež odpovídají webovému a e-mailovému serveru. Analýza obou serverů odhalila následující informace.

Webový server

- IP adresa
- Provozovaný operační systém – Linux Ubuntu

- Veřejné porty a služby – 80/HTTP, 443/HTTPS, 500/IKE a 10443/http

E-mailový server

- Reverzní DNS záznam – mail.názevOrganizace.cz
- Provozovaný operační systém – Fortinet FortiOS
- Veřejné porty a služby – 10443/HTTP

Na webovém serveru je spuštěna samotná internetová stránka, přesněji se jedná o porty 80 a 443 protokolu HTTP/S. Dále je možné si všimnout protokolu na výměnu bezpečnostních klíčů IKE na portu 500 a spuštěná webová služba na portu 10443. Při zadání adresy s portem do prohlížeče je uživatel přesměrován na přihlášení do systému od společnosti Sophos, která se zabývá vytvářením bezpečnostního softwaru a hardwaru. Další specifikace nasazeného systému nebyly zkoumány.

V rámci analýzy webových portálů byly nalezeny výroční zprávy zdravotnických organizací, které obsahují vnitřní strukturu, a to včetně seznamu některých výše postavených zaměstnanců. Zde je uvedeno v několika případech nejen jejich jméno, ale také e-mailová adresa.

U e-mailového serveru byl nalezen na portu 10443 přes HTTP protokol přihlašovací formulář do služby společnosti Fortinet. Uživatel má možnost zadat přihlašovací jméno a heslo, popřípadě spustit aplikaci FortiClient. Systémové specifikace již dále nebyly analyzovány.

Posledním využitým nástrojem je specializovaný software Nmap. Ten je k dispozici pro platformy Windows, Linux a MacOS. Je možné získat z oficiální stránky zdrojový kód pro využití na dalších systémech. Jedná se o nástroj umožňující aktivní skenování v síti. Uživatel musí zadat potřebné vlastnosti prováděného skenu a definovat svůj cíl. Jako cíl je možné zvolit doménu, adresu či skupinu adres. Zároveň je možné definovat skenování portů, kdy se program pokusí získat informace o aktivních portech, protokolech, spuštěných službách a jejich verzích. Následně bylo nastaveno, aby program po ukončení své funkce vyexportoval výsledek do textového souboru. Volitelných možností, které definují druh využitého skenu je velké množství a lze je nalézt v oficiální dokumentaci na adrese https://nmap.org/book/man-briefoptions.html.

Výsledek programu Nmap ukázal nové i již známé otevřené porty z nástroje Censys doplněné o další užitečné informace. S příkazem, který byl zadán se Nmap pokusil zjistit verze běžících služeb na daných portech. Přesná syntax příkazu vypadá následovně: „nmap -v -A -p -sV -version-all -O -oN result.txt <adresa IP>“. Zajímavou informací je verze webového serveru, na které je spuštěn internetový portál. Jedná se o dnes již starší verzi serveru Apache 2.4.29 vydané v druhé polovině roku 2017.[25] Na tuto verzi je možné na internetu nalézt několik chyb a zranitelností. Dále byl nalezen port 5060 s protokolem SIP a port 8443 se službou OpenVPN.

6.1.3 Vyhodnocení

V rámci prvotního průzkumu zdravotnického subjektu bylo vyhodnoceno jako největší riziko pro organizaci využívání více než pět let staré verze webového serveru, který má několik známých zranitelností, jež mohou být využity útočníkem. V rámci prvotní analýzy nebyly zhodnoceny aplikace bezpečnostních firem na portech 10443. Znalost verze útočník využije především k hledání slabin a možností, jak získat prvotní přístup do systému. Některé kritické slabiny dokonce mohou způsobit pád systému, či jeho dočasné přerušení.

Dalším potenciálním rizikem bylo vyhodnoceno zveřejňování jmen, e-mailových adres a případně i pracovních pozic několika zaměstnanců ve výročních zprávách. Toto se týká také druhého subjektu, jelikož jeho zpráva obsahovala rozsáhlý diagram zobrazující strukturu uvnitř společnosti. Taková data mohou sloužit útočníkům k získání ponětí o struktuře a vedou k lepšímu využití metod sociálního inženýrství.

Jelikož se jedná o organizaci patřící do veřejného sektoru, jsou ve státním registru smluv nedostatečně skryty informace o některých zaměstnancích zdravotnického zařízení, které lze jednoduše získat a dále využít nejpravděpodobněji pro sociální inženýrství.

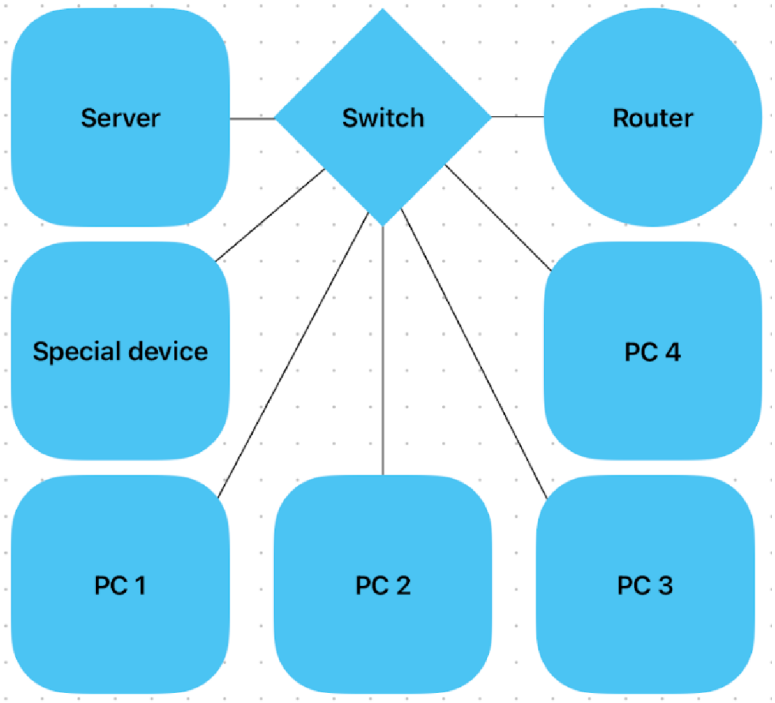
6.2 Druhý scénář

Ve druhém scénáři jsou analyzovány možnosti útočníka v samotném systému. Popsány jsou postupy při vytváření modelu, využité nástroje, získané poznatky a na

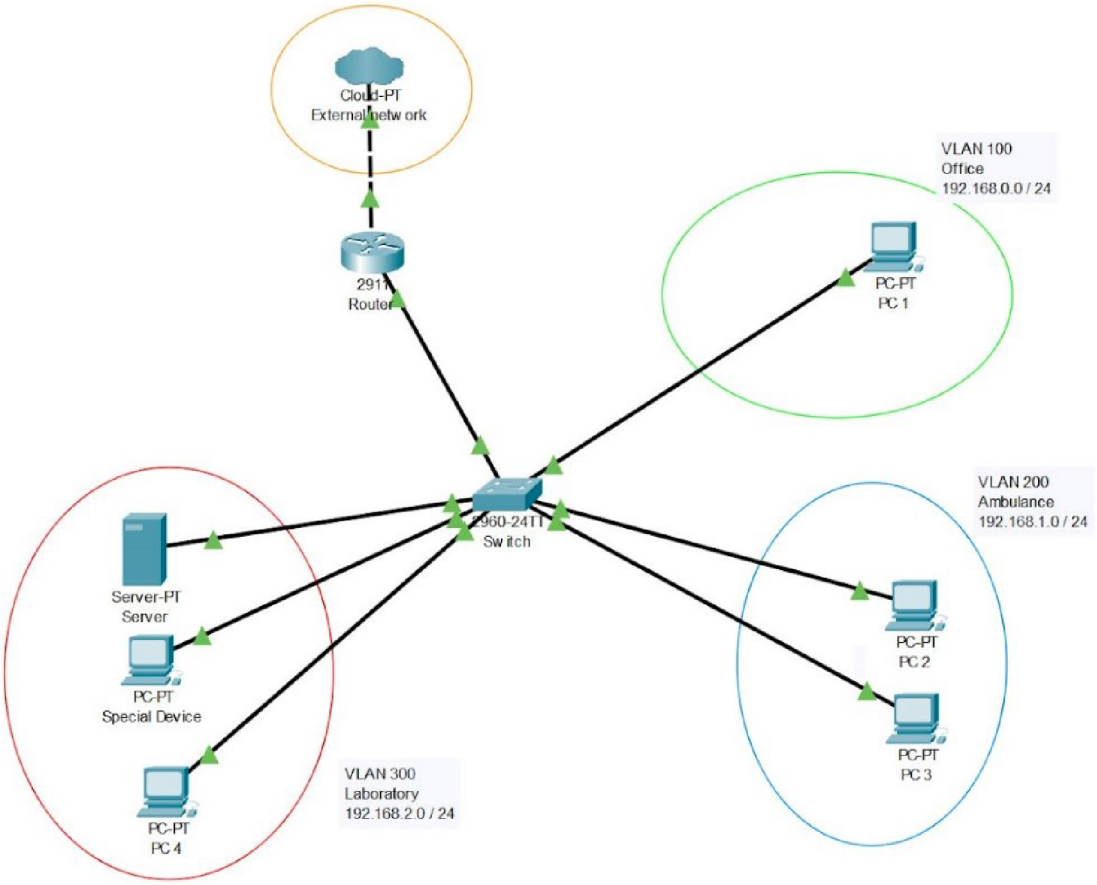
závěr i zhodnocení výsledků. Využito bylo předem definovaných procedur a technik v MITRE CALDERA, jež byly vybrány na základě statistiky v oblasti trendů kybernetických hrozeb jako nejpravděpodobnější. Tyto trendy byly zmíněny v teoretické části práce. Funkčnost některých technik vyžadovala stažení či vytvoření dodatečného malwaru či jiného programu. Jelikož je cílem práce analyzovat slabá místa systému a vyhodnotit možnosti útoku, není cílem testovat samotné funkce vybraného malwaru. Rozhodující pro práci je, zda je možné provést útok takového typu a případně, jakým způsobem zlepšit zabezpečení, aby se dalo dotyčné hrozbě zcela vyhnout.

6.2.1 Testovací prostředí laboratoře

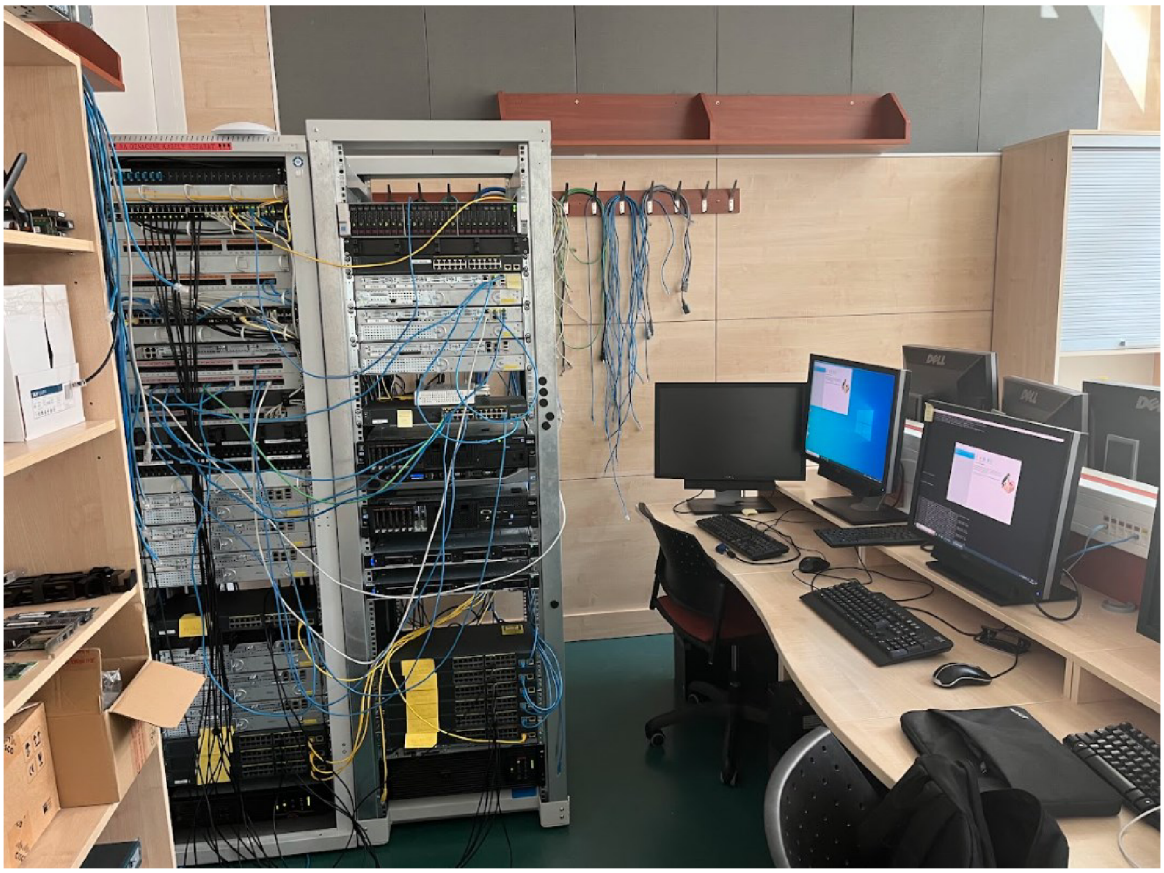
Celý model byl nejprve na základě dotazníku a rozhovoru s odborníkem z praxe sestaven jako diagram určující základní topologii. Ta je reprezentována Obrázkem 6. Následně byla topologie vymodelována v programu Cisco Packet Tracer, kterou vizualizuje Obrázek 7. Zde jsou již přesně definovány IP adresy koncových stanic, rozsahy jednotlivých sítí a zařazení do Virtuálních LAN skupin. Ty jsou na laboratoř tři a oddělují síť na kancelář či místnost pro zaměstnance, ambulanci a laboratoř, ve které je jedním z klientů specializované analytické zařízení. Všechny stanice jsou zapojeny do fyzického prvku switch, který je propojen s routerem. Oddělení je pouze virtuální a aby mohly stanice komunikovat je využito architektury Router-On-A-Stick. Router směruje provoz mezi jednotlivými virtuálními sítěmi a obsahuje jedno připojení mimo vnitřní síť. To reprezentuje připojení do zbytku sítě organizace či jako prostředek vzdálené správy pomocí VPN. V rámci programu Packet Tracer byla na prvcích provedena potřebná konfigurace. Při otestování funkčnosti se přešlo na nasazení fyzického modelu. Jeho infrastrukturu tvoří síťové prvky společnosti Cisco. Jmenovitě se jedná o router **Cisco 2911** a switch **Catalyst 2960**, které jsou v síťové laboratoři J-5 Univerzity Hradec Králové. Právě ve zmíněné učebně bylo následně na síť připojeno šest počítačů reprezentujících jednotlivé koncové stanice, jak je reprezentováno na Obrázku 8.



Obrázek 6 – Prvotní diagram topologie
Zdroj: Vlastní



Obrázek 7 – Topologie v Cisco Packet Tracer
Zdroj: Vlastní



Obrázek 8 – Modelované prostředí v laboratoři J-5
Zdroj: Vlastní

6.2.2 Využívané nástroje

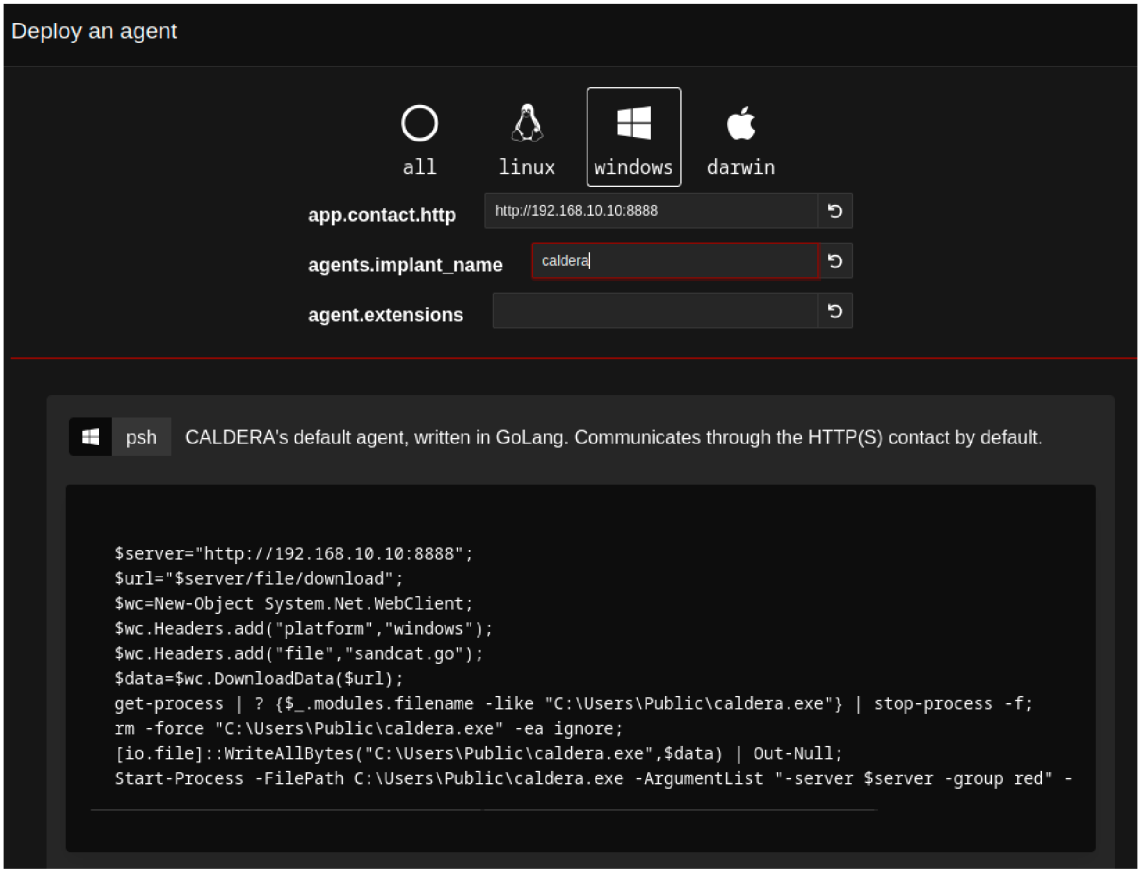
V rámci modelování topologie byl využit software Cisco Packet Tracer. Ten sloužil k sestavení topologie a odzkoušení její konfigurace. Ovšem na samotné testování technik a útoků byla využita linuxová distribuce Kali Purple. Kali linux je operační systém zaměřený čistě na testování kybernetické bezpečnosti, jehož specializovaných nástrojů autor využil. Využita byla vydaná verze nazvaná Purple.[26] Vzhledem k počtu testovaných technik a faktu, že se jedná o model, nikoliv testování konkrétní slabiny systému, byl dále vybrán framework MITRE CALDERA.

MITRE CALDERA slouží k automatickému testování technik definovaných frameworkem MITRE ATT&CK. Jedná se o prostředí, které umožňuje zvolit požadované techniky, nastavit jejich parametry, vybrat typ agenta a spustit automatizovaný test. Následně se CALDERA pokusí o splnění vybraných technik

pomocí předem definovaných procedur.[27] Vzniklo tak automatické testování bezpečnosti, a to na základě předem daných parametrů.

6.2.3 Průběh testování

Nejdříve byl v CALDERA zvolen agent, který provádí vybrané útoky. Následně byla vytvořena operace, která obsahovala relevantní techniky. Pro ně agent po spuštění začal automaticky testovat definované procedury. Vytvoření agenta je znázorněno Obrázkem 9.



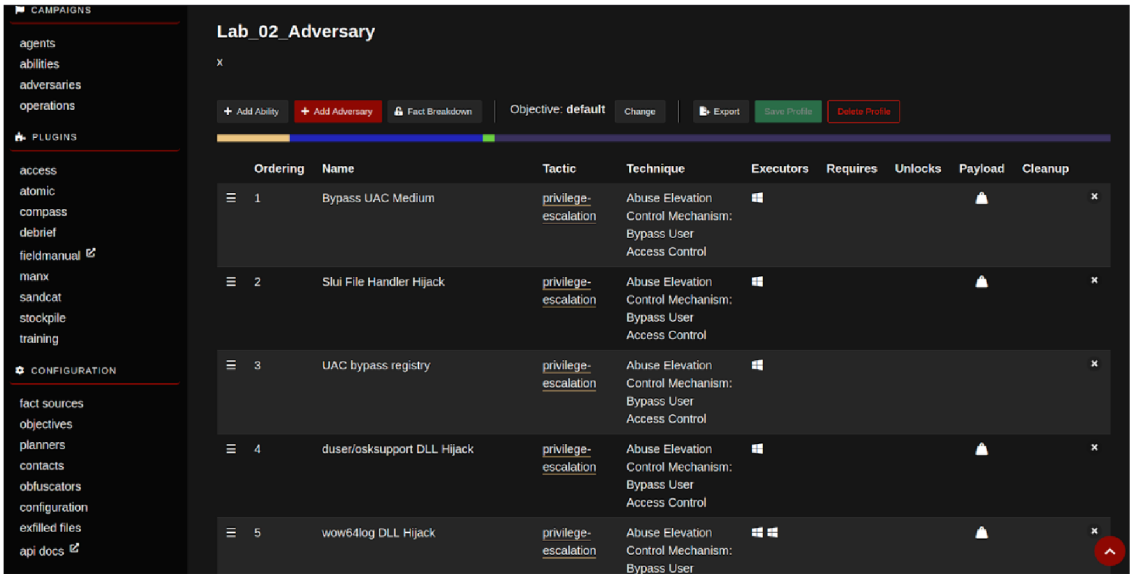
Obrázek 9 – Vytváření agenta v MITRE CALDERA
Zdroj: Vlastní

Přístup do systému byl předpokládán za pomocí účtu získaného sociálním inženýrstvím, zjištěním a využitím slabiny za pomocí informací v předchozím scénáři, kupříkladu na webovém serveru, či byl zanesen do systému na přenosném paměťovém médiu.

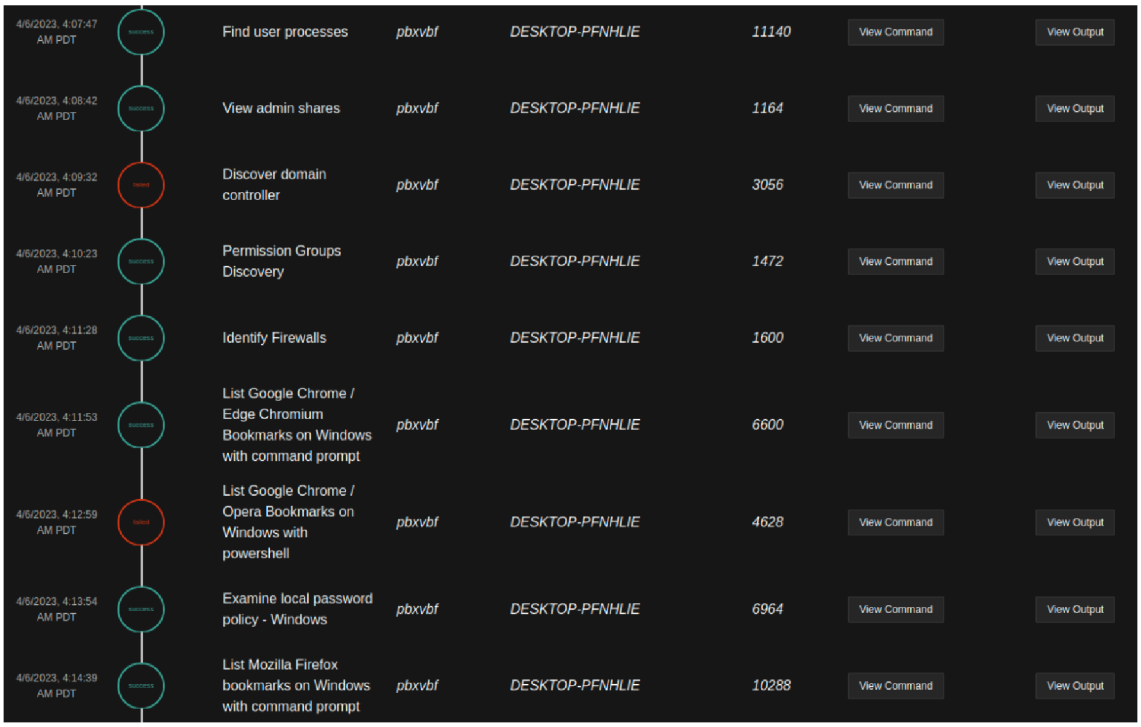
Po ukončení operace bylo využito možnosti frameworku CALDERA vygenerovat závěrečnou zprávu. Jejím obsahem je seznam agentů a diskrétní grafy

zobrazující cestu útoku, jednotlivé kroky, taktiky, techniky a získané informace. Dále je součástí výpisu tabulka mapování na framework MITRE ATT&CK. Zde jsou zmíněny taktiky, techniky a procedury, které byly použity. Poté následuje sekce informací, které byly zjištěny během operace. Jednotlivé prováděné akce jsou vypsány v tabulce s údajem, zda je k nim dostupná získaná informace. V poslední tabulce na konci dokumentu jsou vypsány právě výše uvedené informace, tedy zjištěné údaje o systému. Příkladem takové informace může být získané uživatelské jméno přihlášeného uživatele či název počítače. Během testování scénářů tímto způsobem bylo získáno mnoho užitečných údajů, které dále byly využity v navrhovaných protiopatřeních.

Zmíněný výpis je výsledkem definované operace. Ta seskupuje vybrané techniky, které CALDERA provádí po spuštění testu. Vytvořená operace obsahující techniky scénáře je viditelná na Obrázku 10. Spuštěnou operace s průběžnými výsledky reprezentuje Obrázek 11.



Obrázek 10 – Vytvořená operace pro druhý scénář
Zdroj: Vlastní



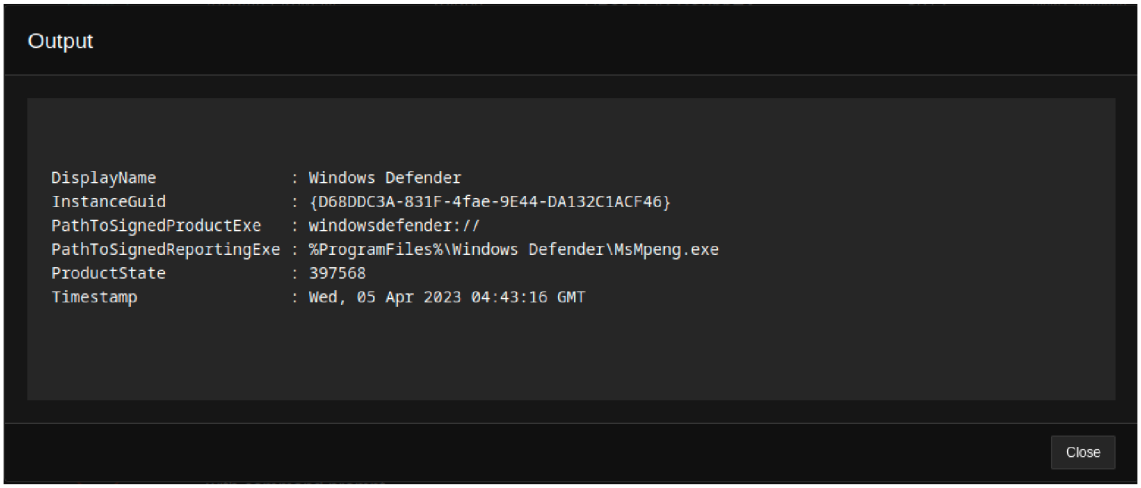
Obrázek 11 – Probíhající operace s průběžnými výsledky
Zdroj: Vlastní

6.2.4 Výsledek operace

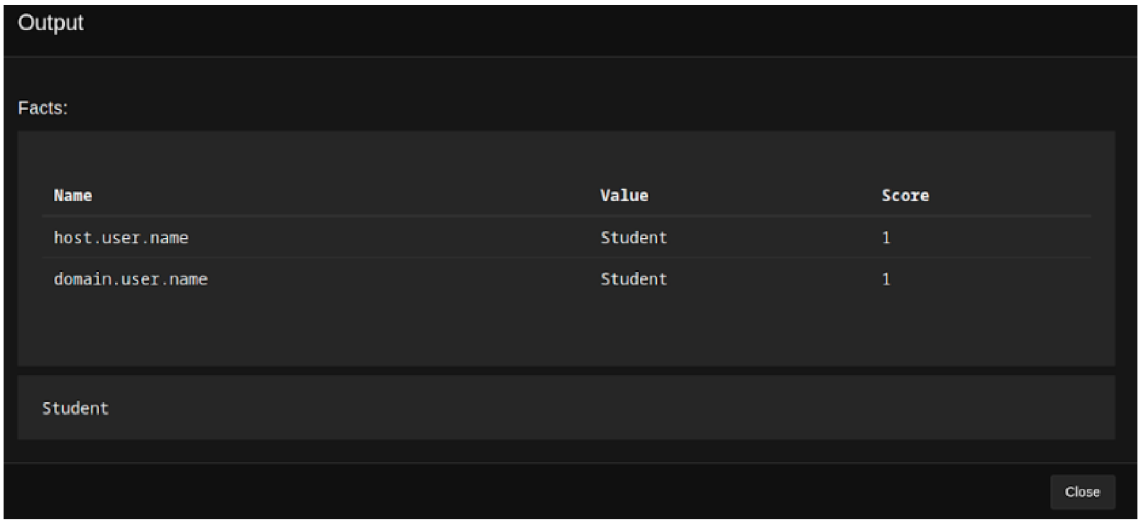
V rámci vlastního scénáře byl simulován vstup přes externí účet či zabezpečení. V prvním kroku se tedy rozhodl zjistit informace o systému, na kterém se nachází. Dalším jeho krokem bylo pokusit se detekovat a zneškodnit jakékoli obranné prostředky, které by mu bránily v jeho pokusu o získání vyšších práv, dalších přihlašovacích údajů nebo v pokusu o proniknutí do dalšího zařízení v síti.

Ze zkoumaných technik byla nejúspěšnější taktika **Discovery**. Ta dokázala zjistit název počítače, přihlášeného uživatele, objevit další zařízení v síti (server, specializované zařízení a router), spuštěné funkce a programy na počítači, uživatelské účty, a dokonce i organizační pravidla pro tvorbu hesla. Útočník tak získá základní údaje, se kterými může dále pracovat při hledání známých slabin a chyb. Odhalena byla i některá více osobní data jako například záložky z internetového prohlížeče a soubory cookies obsahující stále validní přihlášené relace. Zde existuje riziko odhalení informací, které ohrožují další bezpečnost systému. Se znalostí odhalitelných informací lze ovšem navrhnout opatření a doporučení, která dokážou omezit nebo zkomplikovat další kroky útočníka.

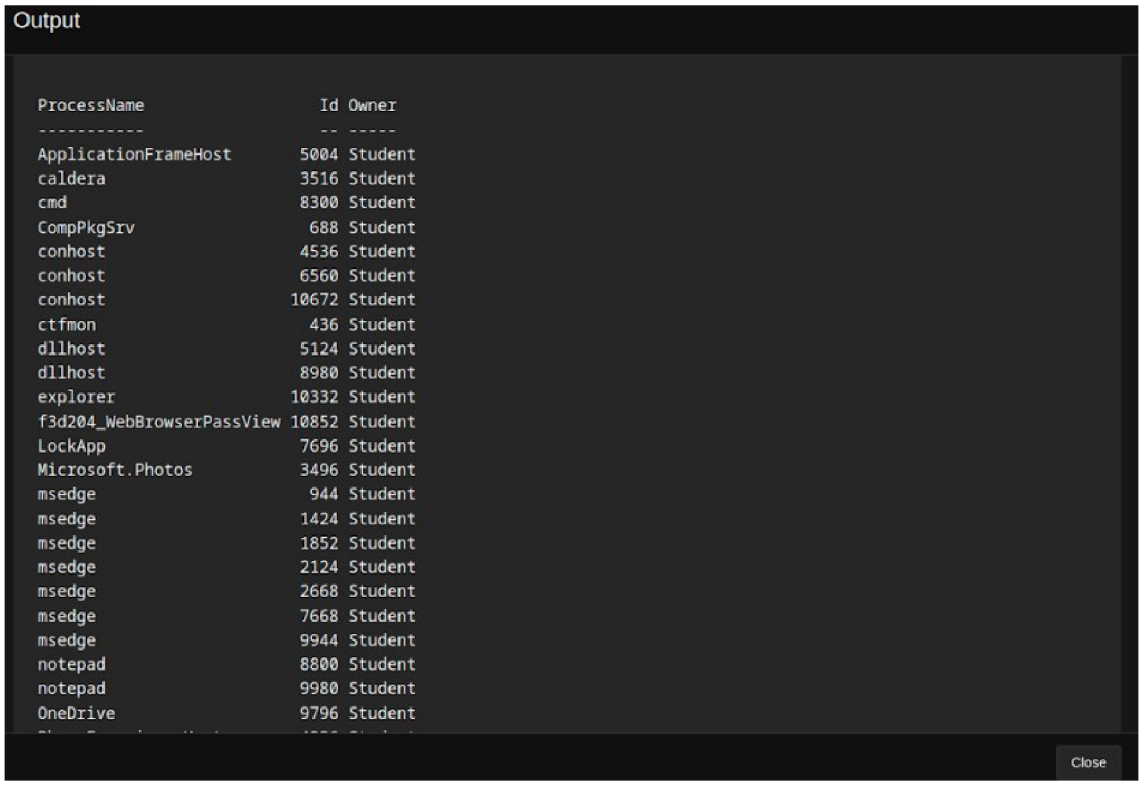
Na Obrázku 12, 13 a 14 jsou znázorněny dílčí výstupy, které se podařilo v rámci simulace identifikovat.



Obrázek 12 – Detekovaný antivirový program
Zdroj: Vlastní



Obrázek 13 – Zjištění přihlášeného uživatele
Zdroj: Vlastní



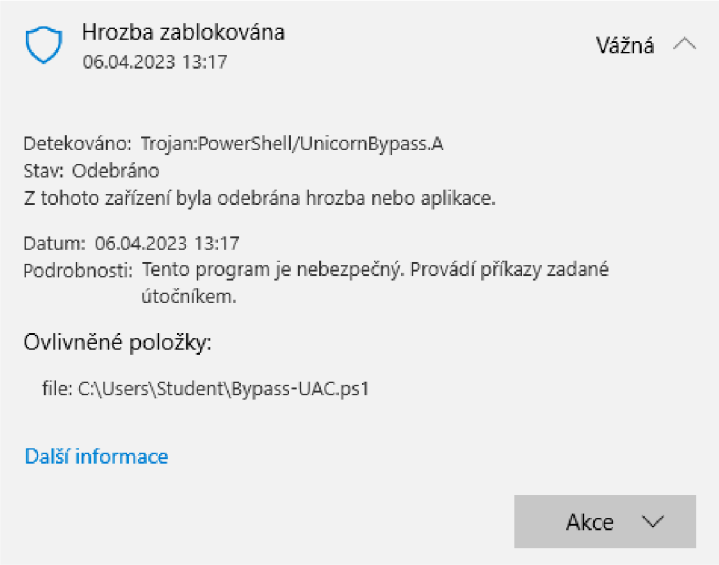
Obrázek 14 – Nalezené běžící procesy
Zdroj: Vlastní

Další testovanou technikou se stalo provádění příkazů **Execution**. Bylo zjištěno, že příkazy a skripty v příkazové řádce představují další možné riziko. Odhalit lze pomocí základních příkazů systémové informace nebo je umožněno útočníkovi provádět vlastní kód. Na některé pokročilejší techniky by však bylo potřeba administrátorské oprávnění, na jehož získání se soustředí techniky **Privilege Escalation**.

Jedná se už o složitější techniky získávání vyšších oprávnění. CALDERA v tomto případě neuspěla při snaze o získání administrátorské oprávnění, zejména z důvodu zablokování antivirovým programem a chybějícím souborem využívajícím zranitelnost. Na základě dat z dotazníku lze vypozorovat zpětnou vazbu ohledně této taktiky. Jedná se především o aktualizované operační systémy v organizaci na koncových stanicích a evidence zásahů pomocí administrátorských účtů, které jinak nejsou volně přístupné běžným uživatelům. Pokud jsou tato pravidla opravdu dodržena, pak existuje malé riziko zneužití těchto slabin a možností získání vyššího

oprávnění přes vybrané scénáře. To ovšem nevylučuje nově objevené slabiny a zranitelnosti nultého dne, které byly zmíněny v rámci teoretické části práce.

Techniky **Defense Evasion** pak závisí na využívaném antivirovém programu. Na testovacích zařízeních byl nasazen aktualizovaný základní Windows Defender, který zároveň identifikovala CALDERA v prvním kroku scénáře. V případě, kdy je program aktualizován, je schopen známé malwary odhalit a zablokovat jejich činnost, jak ukazuje Obrázek 15. Problém nastává, pokud by nebyla dodržena politika zmíněná v dotazníku. Starší verze obsahují slabiny, pomocí kterých je útočník schopen program úplně vypnout nebo omezit jeho hlášení uživateli o detekovaných hrozbách. V takovém případě pak útočník může setrvávat na zařízení a soustředit se na svůj cíl, kdy získá volnost v rámci testování různých druhů malwaru.



Obrázek 15 – Antivirový program při detekci techniky
Zdroj: Vlastní

Testovány dále byly předpřipravené Windows červy. Zde byl nalezen problém frameworku, jelikož je celá struktura útoku postavena na šíření přes internet a využívala jako jednu z technik data z DNS serveru. Jelikož byl model založen na datech z dotazníku, přístup do vnějšího internetu z laboratoře samotné je vyloučen, pouze pro vzdálenou správu. Červ se tak nepřipojil do internetu, kde nenalezl z IP adresy DNS serveru požadovaná data. Jinak využíval techniky podobné

z vlastní definované operace. Zjištění tedy byla stejná v rámci získání vyššího oprávnění, vyhýbání se zabezpečení a v dalších taktikách a technikách.

Poslední zkoumanou oblastí byla taktika **Credential Access**. Zde byla identifikována a vyzkoušena technika získání přístupových údajů z prohlížeče. Jelikož zaměstnanci zde mají přístup pouze do intranetu, je třeba upozornit na možnost získání hesla z prohlížeče, který si je ukládá na zařízení. Zaměstnanci mohou využívat stejná hesla na pracovní služby jako například k přístupu do samotného systému. Zde tedy existuje riziko v uložených heslech.

6.2.5 Vyhodnocení

Při analýze výsledků scénáře bylo zjištěno, že pro vybrané techniky v rámci taktik získávání vyšších práv a vyhýbání se bezpečnostním prvkům je základem aktualizovaný operační systém a aktuální program poskytující antivirovou kontrolu. Jak již bylo zmíněno, provozování nejnovější verze není zcela dostatečné a neznamená imunitu proti veškerým útokům. Stále zde hrozí využití dosud neobjevených zranitelností, avšak udržováním aktuální verze si lze zajistit ochranu proti starším a již známým slabinám.

Útočník je schopen odhalit v takové topologii další klienty a může se tak šířit po vnitřní síti. Zde se projevilo opatření ve formě Virtuálních LAN, které zabránilo útočníkovi v odhalení ostatních zařízení mimo tuto virtuální síť. Jelikož má útočník přístup k informaci o IP adrese stroje, na kterém se nachází, podle masky lze jednoduše zjistit i další adresy stejné sítě, jež může zkusit skenovat. Částečným řešením tak může být nerozdělovat IP adresy postupně v rámci organizace, kdy útočník může zkusit sken hned dalšího bloku adres. Zde avšak záleží na politice organizace, návrhu topologie a požadavkách na použité adresy.

Framework CALDERA se v tomto případě osvědčil jako efektivní automatizovaný způsob testování bezpečnosti. V organizaci, kde na bezpečnost nejsou vydány dostatečné prostředky, by mohl sloužit ke zlepšení bezpečnosti, zejména v ušetření lidských a tím i finančních zdrojů. Výstup frameworku CALDERA je znázorněn Obrázkem 16 a 17.

STEPS GRAPH

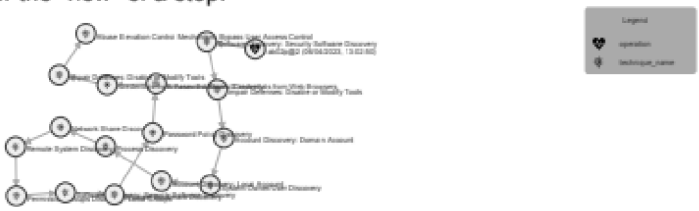
This is a graphical display of the agents connected to the command and control (C2), the operations run, and the steps of each operation as they relate to the agents.

TACTIC GRAPH

This graph displays the order of tactics executed by the operation. A tactic explains the general purpose or the "why" of a step.

TECHNIQUE GRAPH

This graph displays the order of techniques executed by the operation. A technique explains the technical method or the "how" of a step.



Obrázek 16 – Ukázka výstupu CALDERA Debrief
Zdroj: Vlastní

OPERATIONS DEBRIEF

TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities
Credential-access	T1555.003: Credentials from Password Stores: Credentials from Web Browsers	lab02p@2 (06/04/2023, 13:02:50) WebBrowserPassView - Credentials from Browser
Defense-evasion	T1562.001: Impair Defenses: Disable or Modify Tools	lab02p@2 (06/04/2023, 13:02:50) Kill antimalware protected processes using Backstab Disable Arbitrary Security Windows Service Stop and Remove Arbitrary Security Windows Service
Discovery	T1518.001: Software Discovery: Security Software Discovery T1087.002: Account Discovery: Domain Account T1033: System Owner/User Discovery T1087.001: Account Discovery: Local Account T1057: Process Discovery T1135: Network Share Discovery T1018: Remote System Discovery T1069.001: Permission Groups Discovery: Local Groups T1217: Browser Bookmark Discovery T1201: Password Policy Discovery	lab02p@2 (06/04/2023, 13:02:50) Discover antivirus programs Account Discovery (all) Identify active user Identify local users Find user processes View admin shares Discover domain controller Permission Groups Discovery Identify Firewalls List Google Chrome / Edge Chromium Bookmarks on Windows with command prompt List Google Chrome / Opera Bookmarks on Windows with powershell Examine local password policy - Windows List Mozilla Firefox bookmarks on Windows with command prompt
Privilege-escalation	T1548.002: Abuse Elevation Control Mechanism: Bypass User Access Control	lab02p@2 (06/04/2023, 13:02:50) Bypass UAC Medium Slui File Handler Hijack UAC bypass registry duser/osksupport DLL Hijack wow64log DLL Hijack

Obrázek 17 – Mapování CALDERA výstupu na MITRE ATT&CK
Zdroj: Vlastní

Dále bylo identifikováno riziko bezpečnostní politiky hesla. Jak je u veřejného subjektu dáno legislativou, existují minimální požadavky na tvorbu hesla. Tyto standardy musí organizace dodržet, avšak tyto požadavky nemusí být zárukou bezpečných hesel. Zejména v případě, kdy útočník zná potřebná pravidla, může slovníkový útok či útok hrubou silou přizpůsobit těmto požadavkům. Zde se jako řešení nabízí zpřísnění politiky hesel, případně by bylo možné využít jiného typu

nastavování hesel, kde by se jejich správa řešila externě, a tedy by je útočník nebyl schopen získat z koncového zařízení. Zároveň se jako bezpečnostní riziko jeví využívání stejných hesel zaměstnanci na více místech systému a jejich následné ukládání do klíčenek. Opatřením v tomto případě by se mohlo stát interní nařízení organizace.

Též je zde důležitý prvotní přístup, který byl zvolen na základě statistiky a dat z posledních několika let. Velký důraz je třeba klást na poučení zaměstnanců ohledně podvodných e-mailů, odkazů a souborů.

6.3 Třetí scénář

Třetí scénář rozšiřuje předchozí techniky o pokus získání dat, ovlivnění systému či způsobení škody. Vychází z bodu, kde útočník skončil během předchozího scénáře. Analyzována je možnost útočníka provádět akce, které mají reálný dopad na systém nebo jeho uživatele.

6.3.1 Využívané nástroje

Jelikož se jedná o návazný scénář, je pokračováno ve využívání existující infrastruktury. Použit je navíc třetí a poslední výchozí červ Windows z frameworku CALDERA společně s již zmíněnými technikami taktiky **Impact** a **Exfiltration**.

6.3.2 Výsledky technik

Výsledek třetího scénáře přinesl zjištění, kdy útočník je schopen v takovém případě udělat kopii nalezených dat a přenést je na přenosné médium či poslat kamkoli po síti.

Dále byl zkoumán přístup k práci se soubory. Soubory totiž v cílovém specializovaném zařízení mohou představovat například výsledky testů či zdravotnické snímky. Na základě dat z organizace jsou některé výsledky přenášeny po síti, zatímco jiné se přenáší pomocí paměťových médií. Zde útočník může data získat a následně si jejich kopii uložit pro účely odcizení. Vytváření souborů je také využitelné v rámci sociálního inženýrství v případě snahy o provedení podvodu na zaměstnance, jak bylo zmíněno ke konci předchozího scénáře.

V rámci spouštění kódu a manipulace se soubory hrozí možnost využití ransomwaru. Ten má ve zdravotnickém sektoru statisticky vysokou pravděpodobnost. Jen s využitím přístupu v rámci scénáře je možné zašifrovat minimálně koncová zařízení včetně platformy Windows, na které u specializovaného zařízení bude spuštěna nadstavba určitého industriálního systému.

6.3.3 Vyhodnocení

Existuje riziko u vstupu do systému pomocí přenosného média. Zejména u následného využití stejné metody pro odcizení dat. Podle definice by se jednalo o útočníka s využitím osoby typu **insider**, což je v organizaci možné vzhledem k získanému dotazníku, jelikož ne všechny porty jsou fyzicky nedostupné.

Zajímavější je ovšem možnost vytváření a manipulace se soubory, která byla odhalena v rámci scénáře. To může útočník využít v podstrčení oběti vlastní škodlivý program. Zároveň je útočník schopen mazat a měnit tímto způsobem data uložená na zařízení, a tím způsobit ohrožení jejich integrity.

V rámci taktiky **Impact** se pak jedná především o vypnutí a restartování systému, které může útočník na počítači uložit ve formě skriptu nebo automatického spuštění po startu. Je tak schopen například na jedné či více cílových stanicí dočasně zamezit používání systému. Zároveň existuje možnost využití ransomwaru, kde je riziko zastavení procesů do doby obnovení stabilního stavu jednotlivých zařízení. V případě útočníkova přístupu k serveru by pak mohlo být využito daleko rozsáhlejšího dosahu ransomwaru, zejména na data v databázi.

Zkoumána byla i možnost využití taktik ICS. Vzhledem k absenci reálného systému je modelování hrozeb v této oblasti založeno pouze na teoretických poznatcích. Mezi největší hrozby, o které by se mohl útočník pokusit byly vyhodnoceny techniky ovlivňující parametry přístroje určující jeho provoz a ovlivnění hlášení výjimečných stavů a chyb přístrojem. Hlášení stavů, chyb a problémů je důležitou součástí bezpečnosti. Zajišťuje tak zpětnou vazbu operátorům, kteří v případě nouze mohou zařízení na dálku odstavit. Pokud zařízení nevykazuje známky poruchy je těžké zjistit, že je s ním vzdáleně nepovoleně

manipulováno. Druhou taktikou a jejími technikami může být samotná změna parametrů. Ta může být nastavena tak, že přístroj bude ve svém výstupu ukazovat nesprávné informace, nebo se změní parametry ovlivňující provoz samotného zařízení, kdy může dojít k případnému poškození přístroje či jeho vzorků. V případě například analyzační centrifugy pro rozbor krve se může jednat o zvýšení otáček do takové míry, že dojde k mechanickému poškození. Zkoumání takových technik však bez fyzického přístroje a reálného využívaného softwaru nebylo možné. Ovšem i přes tuto skutečnost existují způsoby napadení operačního systému specializovanou vrstvou. V případě přístrojů kompatibilních se systémy Windows by tak bylo možné provést útok na tuto vrstvu, nikoliv na specializovaný systém.

7 Možnosti obrany a protiopatření

V průběhu scénářů bylo simulováno několik technik útoků na modelový systém. Všechny doposud dosažené výsledky a závěry pochází od autora s využitím praktického testu a na základě statistických dat. V rámci frameworku MITRE ATT&CK jsou ovšem definovány u technik i jejich možné mitigace, které jsou v této části představeny a zhodnoceny. Provedeno je následné porovnání se závěry autora, která získal během praktické části.

7.1 První scénář

V relaci na první scénář nabízí MITRE ATT&CK jako hlavní řešení **Pre-compromise**. Jedná se o protiopatření, které používají organizace ještě před samotným útokem. Je definováno u většiny technik taktik **Reconnaissance** a **Resource Development**. Mitigace však pouze doporučuje organizaci minimalizovat množství dat, které poskytuje třetím stranám či zveřejňuje do internetu. Jinými technickými způsoby nelze zvýšit bezpečnost v rámci těchto technik. Přestože nelze sběru dat účinně zabránit, v případě aktivního skenování lze některé techniky odhalit. Jmenovitě se jedná o analýzu a monitorování síťového provozu pomocí softwaru a následného vyhodnocování. Phishing v organizaci lze detekovat pomocí analýzy zasílaných e-mailů a jejich obsahu. Poslední možností detekce, zejména metod sociálního inženýrství, je sledování, zda neexistuje osoba

vydávající se za zaměstnance organizace. Objevení takového profilu může znamenat odhalení útoku v jeho rané fázi, kdy je možné zaměřit se na zvýšení bezpečnosti.[59]

Toto opatření je tedy totožné s názorem, ke kterému dospěl autor během praktické zkoušky scénáře. Minimalizovat množství publikovaných dat. Přidána může být snaha samotných zaměstnanců, například nesdílet jakékoli informace spojené s prací na internetu, zejména pak na sociálních sítích. Důrazněji by měla také organizace dohlížet na dodržené bezpečnostních politik třetích stran, což je možné demonstrovat například na špatně anonymizované veřejné smlouvě.

7.2 Druhý scénář

Druhý scénář obsahuje oproti předchozímu scénáři výrazně více technik z několika odlišných taktik. Zde Mitre definuje hned několik technických mitigací. První kategorie opatření se týká taktiky **Initial Access**. Proti prvotnímu přístupu pomocí sociálního inženýrství jsou podle Mitre definovány mitigace Antivirus/Antimalware, Network Intrusion Prevention, Restrict Web-Based Content, Software Configuration a User Training. Pokud se útočník pokusí poslat malware pomocí e-mailu, měl by se na koncové stanici nacházet aktualizovaný antivirový software, o čemž pojednává první zmíněná mitigace. Druhé protiopatření sleduje podvodné e-maily a snaží se je rovnou odstraňovat, či alespoň označovat jako potenciálně škodlivé. Třetí mitigace zmiňuje možnost blokování určitého obsahu, pokud to neovlivní chod organizace. Příkladem takové blokace může být zakázání posílání vybraných typů souborů, či omezení domén, které mohou být navštíveny z vnitřku sítě. Čtvrté opatření se zaměřuje na důvěryhodnost odesílatelů a možnost filtrování zpráv podle validity jeho domény nebo obsahu zprávy. Poslední možností je správné, důkladné a pravidelné vzdělávání a trénování zaměstnanců v oblasti sociálního inženýrství. Proškolení pracovníci mají mimo jiné i větší tendenci rozeznat podvodné e-maily.[60]

Další velice pravděpodobnou technikou přístupu bylo využití vyměnitelného paměťového zařízení. Zde Mitre definuje jako možnost Behavior Prevention on Endpoint, tedy možnost systému Windows 10 zapnout Attack Surface Reduction (ASR), což zamezuje spouštění vybraných typů souborů z vyměnitelných zařízení.

Další možnost Mitre navrhuje vypnutí úplného automatické připojování vyměnitelných zařízení, či jejich zakázání nebo omezení na organizační úrovni. V případě potřeby lze i kompletně limitovat využívání vyměnitelných zařízení.[61]

Poslední vyhodnocenou metodou přístupu jsou validní účty. Zde existují některé technická opatření, například bezpečnost samotných aplikací, která požaduje, aby hesla byla uložena v bezpečném stavu, tedy zašifrovaná. Neukládat hesla za žádných okolností v čitelné formě bez jakéhokoliv zabezpečení. Dále nenechávat v systému výchozí účty, měnit hesla a pokud se v systému nachází SSH klíče, mít je bezpečně uložené a pravidelně měnit. Též by se mělo neustále sledovat, kde je zapotřebí administrátorských účtů a udržovat jinak minimální možná práva. S tím související pravidelný audit, mazání účtů již neaktivních uživatelů a dostatečné školení zaměstnanců o důležitosti bezpečnosti. Možným řešením je též zavedení více faktorového ověřování. Možnosti sledování jsou v zaznamenávání logů aktivit každého uživatele a jejich vyhodnocování.[62]

Druhou taktikou testovanou v rámci scénáře byl **Execution**, přesněji Command and Scripting Interpreter. Mitigace Mitre identifikuje jako využití antivirového softwaru, dále již dříve zmíněného Attack Surface Reduction, ve kterém lze nastavit omezení na provádění Visual Basic a JavaScript skriptů. Pokud je to v organizaci možné, pak lze nastavit používání PowerShell příkazové řádky pro pouze administrátory a zakázat spouštění neověřených aplikací a skriptů. Jednou z metod detekce provádění skriptů je sledování modulů a knihoven, které se načítají pro potřeby skriptů. Dále sledování argumentů prováděných příkazů, pokus o spuštění skriptu mimo doby údržby nebo zásahu administrátora a analýza provozu na síti. V případě sociálního inženýrství a skriptů spouštěných uživateli jsou definována stejná opatření v kombinaci se školením zaměstnanců.[63]

Taktika **Privilege Escalation** byla ve scénáři zastoupena převážně technikou Abuse Elevation Control Mechanism. Pro tuto techniku navrhuje Mitre mitigace pomocí pravidelného auditu, kdy se sledují nové zranitelnosti UAC (User Account Control) na platformě Windows a zda se neobjevila taková zranitelnost, která by byla schopná způsobit narušení bezpečnosti organizace. Kromě pravidelného auditu je možné také zakázat systému spouštět jakékoli aplikace a skripty, jež nebyly staženy z povoleného ověřeného zdroje. Dalšími opatřeními v této kategorii jsou

odstranění uživatelů z lokální administrátorské skupiny a povinnosti zadání hesla k manipulaci nebo spuštění souborů pracujících s uživatelskými právy na platformě Linux. Přestože existují metody, jak obejít systém UAC, je doporučeno využít nejpřísnější pravidla, která lze implementovat v rámci nenarušení provozu organizace. Detekce techniky zahrnuje kontrolu spouštěných příkazů, zejména jejich argumentů, kontrolou souborů, které mají nastavené bity setuid nebo setgid, sledováním příkazů na API, zda nevykazují známky techniky Process Injection. Některé techniky prolomení UAC vyžadují uživatelsky dostupnou modifikaci registrů Windows. Z tohoto důvodu se doporučuje sledovat jakékoli změny registrů a provádět vyhodnocení těchto změn. V rámci techniky Valid Accounts jsou navrženy stejné mitigace jako u jejího předchozího využití v taktice Initial Access.[64][62]

První technikou taktiky **Defense Evasion** je předešlá technika v rámci **Privilege Escalation** s názvem Abuse Elevation Control Mechanism. Proto i zde platí všechna opatření z minulého odstavce, která jsou dále obohacená o mitigace technik **Impair Defenses** a **Indicator Removal**. První ze zmíněných technik je možné mitigovat za pomocí zakázání spouštění jiných aplikací než těch povolených organizací, zajištění, že veškeré operace a soubory spojené s registry, bezpečností a logováním jsou dostupné pouze pro administrátory systému a existuje zde systém řízení práv, který zakazuje běžným uživatelům jakoukoli manipulaci s bezpečnostním či logovacím softwarem. Detekce probíhá za pomocí sledování argumentů spouštěných skriptů, sledování stavu funkce Firewall a modifikaci pravidel tohoto bezpečnostního prvku a sledování běžících i silou ukončených procesů. K dalším metodám odhalení techniky patří vyhodnocování logů, analýza metadat procesů a změny v registrech.[65]

Pro techniku **Indicator Removal**, Mitre identifikovalo jako možné mitigace šifrování důležitých uložených dat, a to i během jejich přenosu, automatické odesílání logů na místo k tomu určené a nenechávat je pouze na daném lokálním úložišti zařízení, kde by jejich modifikace a čtení měla být zajištěna administrátorským přístupem. Mezi metody odhalení této techniky patří výše uvedené v předchozím odstavci obohacené o sledování provozu na síti a sledování

smazaných souborů, zda se mezi nimi nenachází logy či jiné soubory zachycující události v systému.[66]

Během scénáře se pokusila CALDERA v několika technikách o **Credential Access**. Možnosti mitigací získání hesel z klíčenek (Credentials From Password Stores) je za pomocí zadání silného hesla na samotnou klíčenku. Zde autor práce dospěl k závěru, že v rámci zvýšení bezpečnosti lze přestat využívat uložená hesla úplně. Detekovat přístup k uloženým heslům lze pomocí sledování přístupů k souboru s hesly. Dále poté sledovat prováděné příkazy, zda se nesnaží o čtení ze souborů obsahující hesla.[67]

Testovanou technikou získání hesel bylo i OS Credentials Dumping. Tuto techniku lze omezit pomocí správy přístupů pro Replicating Directory Changes, na Windows 10 definováním pravidel pro ASR na zabezpečení LSASS pro zabránění odcizení přihlašovacích údajů a zapnutí funkce Credential Guard, která chrání LSA. Další metodou zabezpečení je zašifrování a bezpečné uložení záloh Domain Controlleru. Na zvážení organizace je také vypnutí na systému NTLM a autentizaci WDigest. Zároveň je vhodné, aby měli všichni administrátoři rozdílná a složitá hesla napříč systémem. Samotná politika hesel se též týká zaměstnanců. Z tohoto důvodu je třeba poučit zaměstnance o nutnosti odlišných a složitých hesel, což je v souhlasu s názorem, ke kterému dospěl autor během praktické části. Detekce techniky spočívá ve sledování skriptů, registrů a běžících procesů, v kombinaci s analýzou provozu na síti. Hledána je jakákoli manipulace či pokusy o ní v rámci SAM (Security Account Manager).[68]

Druhý scénář se též zaměřil na pokus o získání souborů cookies z prohlížeče a z nezabezpečených zdrojů, kterým může být například historie příkazové řádky, kde administrátor prováděl v minulosti operace s vyššími právy. Pro tyto případy navrhuje Mitre mitigace ve formě více faktorového ověřování, automatickým pravidelným mazáním souborů cookies a poučením uživatelů. Metodou detekce pak může být kontrola přístupu uživatelů do složek s těmito soubory či monitorování procesů, které se snaží přistoupit k souborům cookies. Riziko nezabezpečených přihlašovacích údajů lze zmírnit správnou konfigurací práv skupin, pravidelným auditem, jehož cílem je hledat soubory či příkazy obsahující hesla, kde existuje riziko jejich odhalení a následné odcizení, šifrování citlivých dat na discích, vypnutím

historie v příkazové řádce, zakázáním ukládání hesel do souborů v rámci organizace na všech zařízeních a zamezit přístupu do registrů uživatelům bez administrátorského oprávnění. Techniku je možné detekovat pomocí sledování přístupu do souboru s historií příkazů, sledování pokusů o provedení příkazů se špatným heslem, které je jinde v systému platné a pomocí monitorování registrů.[69][70]

Technikami taktiky **Discovery** bylo možné zjistit během praktické části důležité informace. Mezi protiopatření techniky Account Discovery patří samotná konfigurace operačního systému, kde je možné vypnout vyjmenování administrátorských účtů. Její zjištění je možné za pomocí sledování přístupu do uživatelských souborů (/Users).[71] Techniku získání záložek z prohlížeče nelze účinně mitigovat, pouze detekovat pomocí přístupu k uloženým souborům.[72] U odhalení politik jednotlivých hesel existuje doporučená mitigace Mitre ve formě zajištění využití validních filtrů hesel pomocí DLL filtrů.[73] Process Discovery, System Information Discovery a Software Discovery jsou metody, které též nelze efektivně omezit.[74][75][76] U poslední techniky však lze z části využít omezení pomocí VLAN, které byly využity jak v modelu, tak jsou implementovány v rámci organizace.

V rámci **Lateral Movement** byla zastoupena technika Replication Through Removable Media. Limitovat útočníkovo číření pomocí vyměnitelných médií lze zapnutím pravidel ASR na blokaci spustitelných typů souborů, vypnutím automatického načítání vyměnitelných disků a organizačním opatřením omezujícím využívání těchto paměťových zařízení. Detekovat techniku je poté možno za pomocí monitorování nově vytvořených disků, kontroly vytváření souborů a přístupu k nim.[78]

Poslední taktika **Collection** zahrnovala ve scénáři techniky Data from Local System a Data Staged. Proti první zmíněné technice lze jako možnou obranu označit obecnou politiku přístupu k citlivým datům, jmenovitě v omezení přístupu a šifrováním dat.[79] Zde se Mitre shoduje s autorovým závěrem, a to šifrovat důležitá data a nechávat je uložená na místě s vysokým stupněm zabezpečení. Detekovat takový případ je následně možné pomocí monitorování prováděných skriptů, souborů, procesů a podezřelých programů. Pro Data Staged pak neexistuje aktivní

obranné opatření, pouze detekce, zda si útočník nikde nepřipravuje data, která by následně chtěl odeslat mimo systém. Užitečné tak může být hledat archivy ve formátech **.zip** a **.rar**.[80]

7.3 Třetí scénář

Poslední scénář navazuje na techniky možností útočníka doplněné o nějakou formu splnění běžného cíle útočníka. Ten může v oblasti zdravotnictví být nejčastěji odcizit citlivá data, způsobit výpadek, žádat výkupné za navrácení dat nebo získat přístup k ICS systému.

Částečně byla ve scénáři zmíněna taktika **Discovery**. Ta již byla hlavně využita v předchozím scénáři, avšak jedna technika byla součástí připravené operace v MITRE CALDERA. Jedná se o techniku Remote System Discovery, u které Mitre nedefinuje žádné možné mitigace.[77]

Možnostmi odcizení dat ze systému se věnuje taktika **Exfiltration**, která již byla v práci představena dříve. Ve scénáři byla vyzkoušena metoda Exfiltration over Physical Medium, kde byl předpokládána i dřívější technika za využití přenosného média. Stejně jako u předchozích technik využívajících vyměnitelná paměťová média, i zde je doporučení na omezení jejich využívání v organizaci nebo vypnutí automatického spuštění média. Zároveň Mitre zmiňuje možnost Data loss prevention, přesněji možnosti automatické detekce kopírování citlivých dat na fyzické médium. Detekce se opět zaměřuje na sledování připojených zařízení, procesů a přístupu k souborům. Kdyby se útočník snažil o přenos přes internet, například pomocí protokolů FTP, pak Mitre definuje zásady dodržení monitorování provozu na síti, segmentaci sítě a využití Network intrusion detection and prevention system, které odhalují provoz k útočníkovi a následně ho mohou blokovat.[81]

Poslední taktikou v rámci třetího scénáře je **Impact**. Zde na základě statistiky bylo vyhodnoceno jako nejpravděpodobnější využití ransomwaru. Dále bylo v laboratoři zjištěno, že útočník může vypnout a zablokovat dočasně napadená zařízení. Jednalo by se tedy o techniky Data Destruction, Data Encrypted for Impact, Service Stop a System Shutdown/Reboot. V prvním případě je mitigací vytvoření

záloh. Pravidelné zálohování je první rychlou možností, jak obnovit smazaná data. V tomto případě je ovšem nutno dbát z velké části na zabezpečení samotných záloh, ke kterým útočník nesmí získat přístup. Detekcí mazání dat může být využívání dotyčných příkazů, detekování mazání souborů a vytváření procesů s účelem mazání dat.[82]

Další metodou obrany, tentokrát proti druhé technice, je opět vytváření záloh v kombinaci s Windows 10 ASR pravidlem, které dokáže blokovat některé vykonávané operace připomínající ransomware.[83] Zde je opět třeba klást důraz na zabezpečení záloh, jelikož i samotné zálohy se mohou stát cílem ransomwaru.

Třetí techniku Service Stop lze mírnit pomocí segmentace sítě, správné rozdělení oprávnění k souborům a procesům v rámci kritické funkčnosti a zabránění možnostem vypnutí služby. Detekovat techniku je možné pomocí monitorování příkazů určených k vypnutí služby, změn souborů souvisejících se službou, vytváření procesů k tomu určeným nebo pomocí sledování hodnot registrů schopných službu ovlivnit.[84]

Poslední zmíněnou technikou je vypnutí systému či způsobení jeho restartování. To může vést k nedostupnosti zařízení, a tím způsobení ztrát organizace. Zde Mitre nedefinuje žádné účinné opatření specifické pro tuto metodu. Detekovat techniku je možné pomocí sledování příkazů pro vypnutí, vytvořeného procesu, který by se o vypnutí staral či monitorování logů a metrik samotných zařízení, zda nevykazují toto chování.[85]

7.3.1 ICS

V rámci scénáře bylo zmíněno napojení na ICS systémy. Zde byly vybrány dvě techniky dvou ICS specifických taktik, které by mohl útočník využít u specializovaných přístrojů spadajících do této kategorie.

První technikou je Alarm Suppression patřící do taktiky **Inhibit Response Function**. Jedná se o omezení funkcí varování, které zařízení hlásí, když kondice zařízení není ideální. Dojde tak k odstranění zpětné vazby k operátorovi. Mitigací se pak stává definování počtu povolených připojení k zařízení na počet potřebný organizací a nenechávat otevřené nepotřebné sloty. Dále izolací specializovaných

zařízení od IT infrastruktury pomocí segmentace sítě. K omezení dopadu techniky lze využít například i statické komunikace v síti, kde je jasně definovaný host a port. Detekovat manipulaci s varovným systémem je poté možné pomocí sledování provozu na síti, kdy se hledá aktivita útočníka a operační databáze, která zaznamenává oznámení ze zařízení. Z absence těchto signálů lze poznat manipulaci.[86]

Druhou technikou ICS je Modify Parameter. Ta spadá pod **Impair Process Control** taktiku a jedná se o změnu řídících parametrů v rámci ICS systému. Metodami mitigace jsou poté audit integrity parametrů a načítaných programů. Příkladem mohou být kontrolní součty. Zároveň by u specializovaných zařízení mělo být definováno, kým mohou být parametry modifikovány a nastavovány. Detekovat tyto změny je možné pomocí aplikačních logů, analýzy ICS sítě a případného upozornění samotného zařízení, jestliže jeho varovný systém nebyl napaden v rámci předchozí techniky.[87]

V útocích za poslední dobu se objevilo množství útoků pomocí dodavatelů. Jmenovitě Supply Chain Compromise u ICS systémů. Jedná se o techniku **Initial Access** a lze ji omezit pomocí provádění auditu ohledně potenciálních zranitelností v přístupu přes dodavatele organizace, nezabezpečeného softwaru a přístupových práv dodavatelů. Dalšími možnostmi jsou podepisování softwaru od samotného dodavatele, pravidelný update programového vybavení, provedení vlastní analýzy slabin a pomocí správy dodavatelů, kde je s dodavateli komunikováno, jsou vyhodnocovány jejich rizika a vypracován systém ohodnocení míry zabezpečení. Detekovat přístup pomocí dodavatele je možné z metadat využívaného softwaru dodavatele, kde jsou nalezeny známky manipulace útočníka.[88]

8 Shrnutí výsledků

V průběhu řešení práce bylo zjištěno několik poznatků ohledně bezpečnosti vybraného zdravotnického zařízení, ze kterého lze vytvořit následující shrnutí.

Na základě odpovědí z dotazníku organizace splňuje implementaci legislativních standardů určených zákonem a vyhláškou o kybernetické bezpečnosti. Přesná míra dodržování nemohla být zjištěna, avšak jestliže jsou body zmíněné v dotazníku plněny řádně, je zde dodržena mitigace útoků pomocí pravidelného zálohování a vyhodnocování logů. Autorovi nebyl sdělen rozsah vytváření logů. Zde je doporučení podle vypsaných protiopatření logovat veškerou aktivitu uživatelů a procesů, která následně může být vyhodnocena. Zálohy je též doporučeno ukládat na oddělené zařízení k tomu určené, což minimalizuje riziko jejich napadnutí a zneužití v případě kybernetické hrozby. Logy je též vhodné ukládat na externím místě, jelikož ze zařízení mohou být při napadení snadněji odstraněny.

V dotazníku je dále uvedeno, že systém je aktualizovaný a udržovaný. Navzdory tomu byl během prvního scénáře nalezen spuštěný webový server, jehož verze je dnes několik let stará a obsahuje známé odhalené slabiny. Zde lze formulovat doporučení ve zvýšeném důrazu na aktualizace napříč organizací, využívání antivirové ochrany a tréninku uživatelů, což jsou ochranná opatření mnoha technik druhého scénáře.

Důležitým aspektem zabezpečení jsou pak samotná hesla. Zde by měl být kladen důraz především na přísná organizační pravidla a poučení zaměstnanců. Ti by neměli využívat stejná hesla napříč systémem a nevyužívat tato hesla v jiných službách mimo organizaci. Za zmínku stojí též útočníkova možnost získat politiku pro tvorbu hesel, pomocí které je možné zefektivnit slovníkové útoky. Poučení zaměstnanců a využití zmíněného opatření může přispět ke zlepšení zabezpečení v rámci této kategorie.

Samotnou kategorií zabezpečení je i viditelnost organizace z vnějšku. První scénář se zabýval touto otázkou a bylo zjištěno, že lze na internetu dohledat špatně anonymizovanou smlouvu odhalující citlivé informace, výroční zprávy odhalující strukturu organizace a jména, e-maily, bydliště a čísla zaměstnanců. Zde by mělo být

v zájmu organizace kontrolovat uveřejňované dokumenty, zda jsou správně anonymizovány, že zveřejňované zprávy neodhalují strukturu či infrastrukturu organizace a nesdílejí sami zaměstnanci citlivé údaje. Toho lze dosáhnout interním nařízením a ověřit fyzickou kontrolou určenou osobou.

Vzhledem k nárůstu napadání dodavatelů je dobré se ujistit, že je vztah mezi organizací a dodavatelem vhodně monitorován a že je využito některého z navržených opatření.

Lidský faktor se za poslední roky stal velkou součástí kybernetických útoků. Z tohoto důvodu je doporučeno vést pravidelná školení zaměstnanců zejména v oblasti sociálního inženýrství. Poučení by mělo být i v případě využívání vyměnitelných médií, kdy by měl být zdůrazněn zákaz zapojování osobních médií do jakéhokoli zařízení systému a následné dodržování stanové politiky organizace.

Přispět k zabezpečení může i testování své bezpečnosti samotnou organizací. Z finančního hlediska nemá zdravotnické zařízení možnost vlastnit specializovaný tým. Nabízí se řešení ve formě využívání automatizovaných nástrojů a frameworků, jakým je například v práci využitý MITRE CALDERA. Při předpokladu stejné, či alespoň podobné, infrastruktury i v dalších zdravotnických zařízení, je možné navrhnout jeden profil, který by se spustil ve více organizacích zároveň. Proběhlo by tak vyhodnocení u více subjektů s jedním scénářem, jestliže sdílejí podobné předpoklady topologie. Předpoklad společné topologie však neplatí pouze u společného testování, nýbrž také u opatření samotných. Ta mohou být v takovém případě také aplikovaná na více zdravotnických zařízení zároveň.

Doporučená opatření lze tedy shrnout v závěru na maximální možnou eliminaci lidského faktoru za pomoci kvalitního a pravidelného školení, nastavení a dodržování vhodných organizačních opatření, které zároveň neomezí fungování společnosti, kontrolu a vyhodnocování logů, spuštěných programů a skriptů, provozu na síti, přístupu do systému a přístupu k důležitým souborům. Důležitým aspektem je též dodržení hierarchie práv a jejich správné rozdělení jednotlivým uživatelským účtům, kdy je zároveň prováděna jejich pravidelná správa.

9 Závěry a doporučení

V rámci zpracování práce bylo dosaženo všech hlavních i dílčích cílů. Byla zanalyzována legislativa kybernetické bezpečnosti, různé taktiky a techniky za pomocí MITRE ATT&CK a následně i možnosti opatření pro tyto útoky. Během praktického testování na modelu byla sestavena podobná topologie, na níž byly vyzkoušeny tři scénáře. Jejich vyhodnocení a výsledky jsou následně porovnány s oficiálně navrženými opatřeními.

Metodika práce též zmiňuje dvě hypotézy. Jelikož se jedná o model a nebylo řešení testováno na opravdové infrastruktuře fungující organizace, nebylo možné hypotézy ověřit. Na základě teoretických a praktických poznatků lze pouze odhadnout jejich výsledek. První hypotéza se týká předcházení běžnému útoku pomocí navržených opatření. Zde závisí především na kategorii útočníka, pokud má potřebné znalosti a finanční prostředky. Dalším faktorem je též lidský faktor, jelikož jak je ze statistik patrné, sociální inženýrství zde hraje důležitou roli. Je však možné dojít k závěru, že vyšší úroveň zabezpečení má vyšší pravděpodobnost odrazit útok, zejména méně sofistikované kategorie útočníků. Tuto otázku řeší z části i druhá hypotéza, která zkoumala otázku, zda navržená opatření dokážou snížit počet útoků na systém. Zde jsou stejné předpoklady jako u první hypotézy. Záleží na druhu útočníka, přesněji na jeho schopnostech odhalit slabiny. Jestliže přijde amatérský útočník před zabezpečený systém a nemůže najít žádnou slabinu, pak je možné předpokládat, že vyšší zabezpečení bude vést k vyšší pravděpodobnosti odrazení amatérského útočníka. Profesionální útočník, který si dokáže sám slabiny vytvářet, pak pravděpodobně nebude od útoku odrazen, zejména kvůli značnému množství znalostí a financí. Ani tato hypotéza však nemohla být reálně otestována a její výsledek je založen na výsledcích praktické a teoretické části práce.

Zvolené téma má mnoho směrů, kterými by šlo zkoumat v rámci dalších prací. Vzhledem k velkému počtu vybraných technik a taktik by určitě bylo možné vybrat pouze některé z nich, které by následně bylo možné analyzovat více do hloubky. Nabízí se také testování přímo v samotné organizaci, zaměření se pouze na jeden typ útoku, který s povolením organizace zkusit v běžném provozu. Je také možné změnit typ organizace mimo zdravotnický sektor, kde jsou rozdílné potřeby na

zabezpečení a kde primárně působí rozdílná kategorie útočníků. Celé téma by se též dalo udělat ze samotné analýzy a implementace zmíněných opatření.

Úroveň zabezpečení zkoumané zdravotnické organizace dosahuje legislativních požadavků a již plní mnoho z navržených opatření. Objeveno ovšem bylo několik potenciálně zranitelných oblastí, ve kterých by organizace mohla zlepšit své snažení za účelem zvýšení kybernetické bezpečnosti.

10 Seznam použité literatury

[1] E. Sayegh, "2022 In Review: An Eventful Cybersecurity Year," Forbes. https://www.forbes.com/sites/emilsayegh/2022/12/13/2022-in-review-an-eventful-cybersecurity-year/ (accessed Jan. 12, 2023).

[2] "2022 Cyber Security Statistics Trends & Data," PurpleSec. https://purplesec.us/resources/cyber-security-statistics/ (accessed Jan. 12, 2023).

[3] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Zákony pro lidi.cz [online], AION CS 2010-2023 [cit. 3. 1. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[4] ČESKO. 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: Zákony pro lidi.cz [online], AION CS 2010-2023 [cit. 3. 1. 2023]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

[5] ŠTĚPÁN, Jan. Zabezpečení počítačové sítě [online]. Hradec Králové, 2021 [cit. 2023-01-03]. Dostupné z: https://theses.cz/id/o8jyk7/. Bakalářská práce. Univerzita Hradec Králové, Fakulta informatiky a managementu. Vedoucí práce Ing. Tomáš Svoboda, Ph.D.

[6] Kyberkriminalita. Policie České republiky [online]. Praha: PČR, 2023 [cit. 2023-01-19]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[7] NOVÁK, Jaromír. Kybernetická kriminalita v roce 2021 očima státního zastupitelství. Blog CZ.NIC [online]. Praha: CZ.NIC, 2022 [cit. 2023-01-19]. Dostupné z: https://blog.nic.cz/2022/07/28/kyberneticka-kriminalita-v-roce-2021-ocima-statniho-zastupitelstvi/

[8] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti [online]. 3rd ed. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA, 2015 [cit. 2023-02-15]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/slovnik/

[9] Legislativa KB. NÚKIB [online]. Brno: NÚKIB, 2023 [cit. 2023-02-15]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[10] Regulace a kontrola. NÚKIB [online]. Brno: NÚKIB, 2023 [cit. 2023-02-15]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/

[11] Enisa Threat Landscape 2022 [online]. Attika: Enisa, 2022 [cit. 2023-03-01]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[12] Enisa about [online]. Attika: Enisa, 2022 [cit. 2023-03-01]. Dostupné z: https://www.enisa.europa.eu/about-enisa/

[13] MITRE ATT&CK v12 [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-03-01]. Dostupné z: https://attack.mitre.org/

[14] How Do OT and IT Differ?. Cisco [online]. San José, California: Cisco, 2023 [cit. 2023-03-08]. Dostupné z: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html

[15] What's the Difference Between OT, ICS, SCADA and DCS?. Securicon [online]. Alexandria, Virginia: Securicon, 2019 [cit. 2023-03-08]. Dostupné z: https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/

[16] JOHNSON, Chris, Lee BADGER, David WALTERMIRE, Julie SNYDER a Clem SKORUPKA. Guide to Cyber Threat Information Sharing. NIST Computer security resource center [online]. Gaithersburg, Maryland: NIST, 2016 [cit. 2023-03-09]. Dostupné z: https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures

[17] PEKAROVA, Sarka. Industrial Control Systems in Healthcare Environments. Dreamlabs technologies [online]. Bern: Dreamlab, 2021 [cit. 2023-03-16]. Dostupné z: https://dreamlab.net/en/blog/scada-ics/post/industrial-control-systems-in-healthcare-environments/

[18] Most Common Types of Cyber Attackers. DataFlair Training [online]. CA, USA: DataFlair, 2023 [cit. 2023-03-21]. Dostupné z: https://data-flair.training/blogs/most-common-types-of-cyber-attackers/

[19] 7 TYPES OF CYBER THREAT ACTORS AND THEIR DAMAGE. Redlegg [online]. Chicago: Redlegg Blog, 2020 [cit. 2023-03-21]. Dostupné z: https://www.redlegg.com/blog/cyber-threat-actor-types

[20] KUTSCHER, JURGEN. M-Trends 2022: Cyber Security Metrics, Insights and Guidance From the Frontlines. Mandiant [online]. Virginia, USA: Mandiant, 2022 [cit. 2023-03-26]. Dostupné z: https://www.mandiant.com/resources/blog/m-trends-2022

[21] SADOWSKI, JAMES a RYAN HALL. Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation. Mandiant [online]. Virginia, USA: Mandiant, 2022 [cit. 2023-03-26]. Dostupné z: https://www.mandiant.com/resources/blog/russia-invasion-ukraine-retaliation

[22] Pegasus Project: Macron among world leaders selected as potential targets of NSO spyware. Amnesty [online]. Londýn: Amnesty international, 2021 [cit. 2023-03-27]. Dostupné z: https://www.amnesty.org/en/latest/press-release/2021/07/world-leaders-potential-targets-of-nso-group-pegasus-spyware/

[23] The Changing Landscape of Hacktivism. SecAlliance [online]. Londýn: SecAlliance, 2022 [cit. 2023-03-27]. Dostupné z: https://www.secalliance.com/blog/the-changing-landscape-of-hacktivism

[24] Security and Privacy Controls for Information Systems and Organizations. NIST [online]. Gaithersburg, USA: NIST, 2020 [cit. 2023-03-30]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[25] [ANNOUNCE] Apache HTTP Server 2.4.29 Released. The Mail Archive [online]. USA: The Mail Archive, 2017 [cit. 2023-04-11]. Dostupné z: https://www.mail-archive.com/announce@httpd.apache.org/msg00119.html

[26] Kali Linux 2023.1 Release (Kali Purple & Python Changes). Kali [online]. Kali, 2023 [cit. 2023-04-11]. Dostupné z: https://www.kali.org/blog/kali-linux-2023-1-release/

[27] MITRE CALDERA. MITRE CALDERA [online]. Virginie: Mitre, 2023 [cit. 2023-04-11]. Dostupné z: https://caldera.mitre.org/

[28] Enterprise Matrix. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/matrices/enterprise/

[29] ICS Matrix. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/matrices/ics/

[30] Enterprise Tactics. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/enterprise/

[31] Enterprise Techniques. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/enterprise/

[32] Reconnaissance. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0043/

[33] Resource Development. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0042/

[34] Initial Access. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0001/

[35] Execution. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0002/

[36] Persistence. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0003/

[37] Privilege Escalation. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0004/

[38] Defense Evasion. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0005/

[39] Credential Access. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0006/

[40] Discovery. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0007/

[41] Lateral Movement. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0008/

[42] Collection. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0009/

[43] Command and Control. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0011/

[44] Exfiltration. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0010/

[45] Impact. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0040/

[46] Initial Access. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0108/

[47] Execution. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0104/

[48] Persistence. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0110/

[49] Privilege Escalation. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0111/

[50] Evasion. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0103/

[51] Discovery. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0102/

[52] Lateral Movement. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0109/

[53] Collection. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0100/

[54] Command and Control. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0101/

[55] Inhibit Response Function. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0107/

[56] Impair Process Control. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0106/

[57] Impact. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/tactics/TA0105/

[58] About ISO27k standards. ISO27k Information Security [online]. Nový Zéland: IsecT, 2023 [cit. 2023-04-20]. Dostupné z: https://www.iso27001security.com/html/iso27000.html

[59] Pre-compromise. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/mitigations/M1056/

[60] Phishing. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1566/

[61] Replication Through Removable Media. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1091/

[62] Valid Accounts. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1078/

[63] Command and Scripting Interpreter. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1059/

[64] Abuse Elevation Control Mechanism. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1548/

[65] Impair Defenses. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1562/

[66] Indicator Removal. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1070/

[67] Credentials from Password Stores. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1555/

[68] OS Credential Dumping. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1003/

[69] Steal Web Session Cookie. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1539/

[70] Unsecured Credentials. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1552/

[71] Account Discovery. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1087/

[72] Browser Bookmark Discovery. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1217/

[73] Password Policy Discovery. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1201/

[74] Process Discovery. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1057/

[75] Software Discovery. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1518/

[76] System Information Discovery. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1082/

[77] Remote System Discovery. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1018/

[78] Replication Through Removable Media. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1091/

[79] Data from Local System. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1005/

[80] Data Staged. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1074/

[81] Exfiltration Over Physical Medium. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1052/

[82] Data Destruction. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1485/

[83] Data Encrypted for Impact. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1486/

[84] Service Stop. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1489/

[85] System Shutdown/Reboot. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T1529/

[86] Alarm Suppression. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T0878/

[87] Modify Parameter. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T0836/

[88] Supply Chain Compromise. MITRE ATT&CK [online]. McLean, Virginia, USA: Mitre, 2022 [cit. 2023-04-20]. Dostupné z: https://attack.mitre.org/techniques/T0862/

11 Přílohy

1) Scénáře namapovány na framework MITRE ATT&CK
2) Dotazník provedený ve zdravotnickém zařízení

about

DP Lab

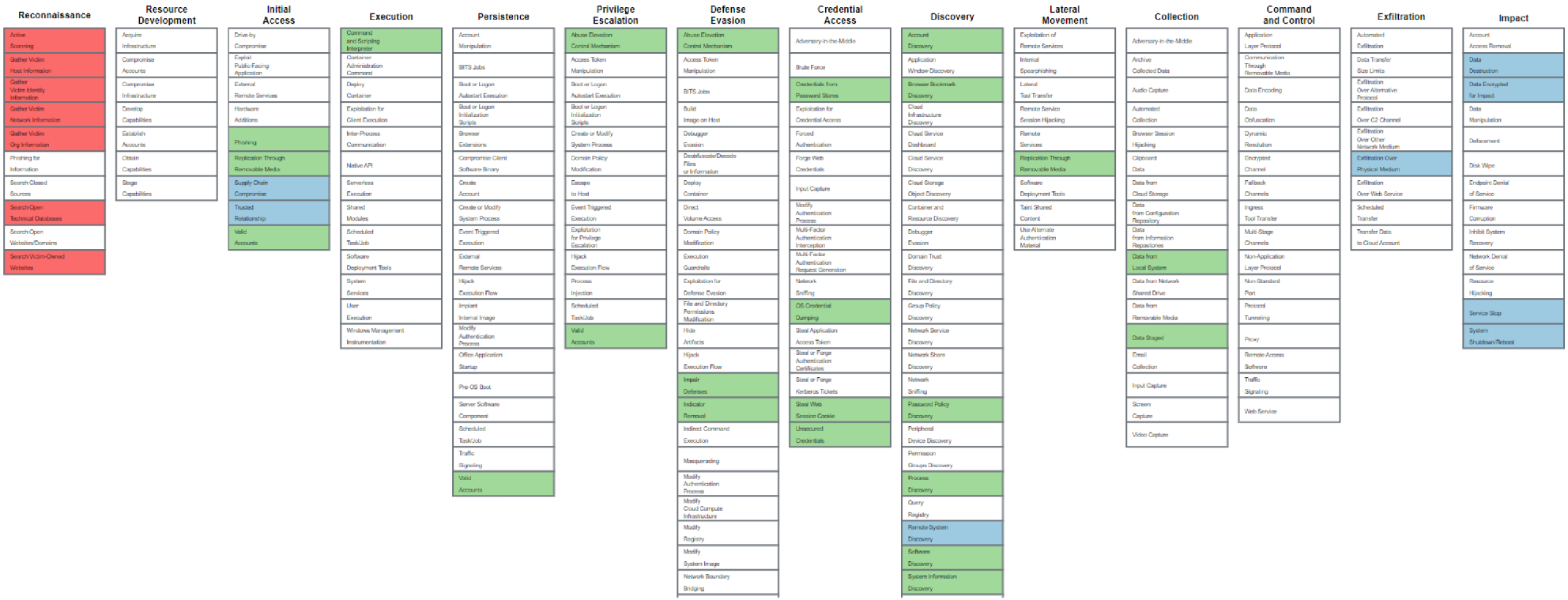
Scénář 1 - červená; Scénář 2 - zelená; Scénář 3 - modrá

domain

Enterprise ATT&CK v12

platforms

Linux, macOS, Windows, Network, PRE, Containers, Office 365, SaaS, Google Workspace, IaaS, Azure AD



Příloha č. 1

FAKULTA INFORMATIKY A MANAGEMENTU
UNIVERZITA HRADEC KRÁLOVÉ

DOTAZNÍK KYBERNETICKÉ BEZPEČNOSTI ZDRAVOTNICKÉHO ZAŘÍZENÍ

(doplněk k diplomové práci)

Obor:	Aplikovaná informatika
Ročník:	5. ročník
Datum zpracování:	15. listopadu 2022
Autor:	Jan Štěpán

Upozornění

Tento dotazník slouží k zjištění parametrů a následnému zpřesnění topologie, na základě které, bude vytvořen model laboratoře. V práci nebude specifikováno, o které zdravotnické zařízení se jedná. Informace získané z těchto otázek poslouží pouze pro lepší specifikaci modelu, díky čemuž se opatření, která vzejdou v praktické části práce, budou dát lépe a přesněji aplikovat.

Otázky

Na otázky, které jsou označeny * není třeba, jestliže je předešlá odpověď NE.

Architektura

1)	Je využíván některý nemocniční systém NIS?	ANO
2)	Je využíván některý laboratorní systém LIS?	ANO
3)	Je využíván některý obrazový systém PACS?	ANO
4)	Uplatňuje se princip klient – server?	ANO

Server

1)	Využívá server platformy Windows?	ANO
2)	Využívá server platformy Linux?	ANO
3)	Je operační systém aktualizovaný?	ANO
4)	Nachází se zde databázový server?	ANO
5)	Je databáze na odděleném serveru? * je na oddělené části serveru	ANO

Síť

1)	Je síť rozdělena na segmenty pomocí VLAN?	ANO
2)	Jedná se o topologii závislou na centrálním prvku?	NE
3)	Je síť sdílená s jinou infrastrukturou (mimo laboratoř)?	NE

Vzdálený přístup

1)	Je k zařízením v síti umožněn vzdálený přístup?	ANO
2)	Je vzdálený přístup realizován za použití VPN? *	ANO
3)	Mají některá zařízení v síti nastavený automatický update?	NE
4)	Je zdrojem aktualizací oficiální dodavatel? *	ANO

Práva

1)	Nachází se zde administrátorské účty pro správu databáze?	ANO
2)	Nachází se zde administrátorské účty pro správu OS?	NE
3)	Nachází se zde administrátorské účty na běžných počítačích?	NE

Zálohy a logy

1) Je zde realizováno ukládání logů? ANO
2) Je zde realizováno vyhodnocování logů? * ANO
3) Probíhá proces zálohování dat? ANO
4) Probíhá proces zálohování konfigurací a nastavení? ANO
5) Je zálohování realizováno na pravidelné bázi? * automatizovaně ANO

Bezpečnost

1) Existuje možnost připojení vlastního přenosného média ze strany zaměstnanců? (např. vlastní flash médium přes USB, …) ANO, ovšem tento postup je interním příkazem zakázán. Zejména na ambulancích je ovšem nutnost číst pacientem přinesená média, kde mají výsledky vyšetření od lékařů, které pacient nechce posílat prostřednictvím systémů. Jsou pracoviště, kde je přístup technicky zakázán.
2) Existuje možnost použití zařízení v síti pro osobní využití? (např. prohlížení vlastního obsahu, přístup k internetu, …) Přístup do internetu ano, ale například přihlášení se do osobního emailu na jiné doméně než je www.[redacted].cz je pro všechny uživatele zakázáno.
   ANO
3) Je potřeba předem schválit zásah uživatele s administrátorskými právy? Ano

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání diplomové práce

Autor:	**Bc. Jan Štěpán**
Studium:	I2100083
Studijní program:	N1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název diplomové práce:	**Modelování kybernetických bezpečnostních hrozeb**
Název diplomové práce AJ:	Cyber threat modeling

Cíl, metody, literatura, předpoklady:

Cílem práce je nasimulovat vybrané kybernetické útoky ve virtuálním prostředí. Dále v tomto virtuálním prostředí otestovat a navrhnout možnosti obrany proti těmto kybernetickým útokům.

Teoretická část bude věnována základnímu pojmovému aparátu ve vztahu k řešené problematice, identifikaci hrozeb, MITRE technikám a taktikám, virtuálnímu prostředí na platformách Linux a Windows a jeho využitelnosti při modelování hrozeb.

Praktická část bude věnována modelování hrozeb ve virtualizovaném labovém prostředí a návrhu obrany proti těmto hrozbám. Navrženy budou organizační a technická opatření. Součástí praktické části bude popis labového prostředí, jeho výstavby, ověření funkčnosti a projev kybernetických bezpečnostních hrozeb.

Předpokládaná osnova diplomové práce:

- Úvod
- Kyberbezpečnost
- Kategorie útoků
- Vybrané scénáře
- Jejich otestování ve viruálním prostředí
- Možnosti obrany (Návrhy a doporučení)
- Závěr

1. Normy z rodiny ISO/IEC 27k
2. Zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti
3. https://attack.mitre.org/
4. https://www.root.cz/knihy/linux-dokumentacni-projekt-4-vydani/

Zadávající pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	Ing. Lubomír Almer, Ph.D.
Datum zadání závěrečné práce:	15.10.2021