Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Využití MITRE ATT&CK pro efektivní řízení kybernetické bezpečnosti

Diplomová práce

Autor: Bc. Ondřej Daniš

Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové duben 2022

Prohlášení:

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

V Hradci Králové, dne 29. 4. 2022 Bc. Ondřej Daniš

Poděkování:

Děkuji vedoucímu diplomové práce panu Mgr. Josefovi Horálkovi, Ph.D. za odbornou pomoc, metodické vedení práce a za cenné rady, kterými přispěl k vypracování této diplomové práce.

Anotace

Diplomová práce se zabývá využitím znalostní báze MITRE ATT&CK pro efektivní řízení kybernetické bezpečnosti se zaměření na platformy Windows a Linux. Úvodní část práce pojednává o základních termínech kybernetické bezpečnosti a správních orgánu na území České republiky. Další oblast je zaměřena na představení struktury, nástrojů a metod používání projektu MITRE ATT&CK. Po uvedení do kontextu znalostní báze jsou na základě zpráv od organizací zabývající se kybernetickou bezpečností, vybrány útočné techniky pro obě platformy. V druhé části práce jsou nejprve vybrané techniky propojeny s dostupnými formami zmírnění dopadu útoku a vytvořeny oblasti zkoumání. Na základě obecných informací ze znalostní báze je následně v každé oblasti navrženo řešení v podobě postupů a konfiguračních parametrů.

Klíčová slova: MITRE ATT&CK, kybernetická bezpečnost, mitigace, Windows, Linux

Annotation

Title: Use of MITRE ATT&CK for effective cyber security management

The diploma thesis is dedicated to use of the MITRE ATT&CK knowledge base for effective cyber security management focused on Windows and Linux platforms. The opening part of the thesis is mapping the basic terms of cyber security and administrative authorities in the Czech Republic. The next section is describing the structure, tools and methods of the MITRE ATT&CK project usage. Once introduced in the respective context of the knowledge base, appropriate attack techniques for both platforms are selected, based cyber security organisation´s reports. In the second part of the diploma thesis, selected techniques are linked with available forms of mitigating the attack impact, which generates the respective research areas. Based on general information from the knowledge base, a solutions are then figured for each area suggesting suitable procedures and configuration parameters.

Keywords: MITRE ATT&CK, cyber security, mitigation, Windows, Linux

Obsah

1 Úvod

S rostoucím začleněním a používáním informačních technologií v běžném životě se současně navýšil i počet kybernetických útoků směřující na všechny možné typy infrastruktury. Výrazně tomu napomáhají i nynější světové okolnosti v podobě pandemie, díky které se musela řada společností z větší části přesunout do online světa, aby zachovala svoji funkčnost. Každý člověk, firma, státní orgán disponuje svými cennými informacemi („know-how“) nebo kritickou infrastrukturou. Jejich případná ztráta, byť jen částečná, může způsobit fatální následky, které v mnoha případech hraničí s jejich existencí. Na základě potenciálně stoupajícího rizika, vzrostl tlak na kvalitní zabezpečení virtuálního prostoru. Z tohoto důvodu postupně vznikají celosvětové organizace, státní úřady či soukromé subjekty zabývající se kybernetickou bezpečností. Zajištění kyberprostoru ovšem není lehký úkol, neboť útoky jsou stále sofistikovanější a komplexnější. Pole působnosti útočníků nedoznává hranic a napadení lze očekávat i v méně významných sektorech.

Obrana proti kybernetickým hrozbám se z výše zmíněných důvodů stala velmi diskutovaným a kritickým tématem, které vyžaduje velmi intenzivní mezinárodní propojení a spolupráci. Vzhledem k neustálé inovaci taktik, technik a procedur útočníků je právě sdílení informací jedním z důležitých zdrojů pomáhající k prevenci nebo zmírnění aplikovaných útoků. Před poskytnutím informací je ovšem důležité dostupná data o útoku důkladně zanalyzovat a detekovat použité techniky útočníka, neboť tím lze značně zvýšit efektivitu a účinnost řízení bezpečnosti. Právě těmito oblastmi se zabývají poskytovatelé zpravodajství označované jako Cyber Threat Intelligence, ze kterých následně čerpají analytici operačních center pro bezpečnost nebo další týmy zabývající se touto problematikou.

Samotná interpretace zpráv o kybernetických hrozbách není oficiálně řízená žádným standardem a její struktura tak bývá odlišná. Pro spotřebitele může tento fakt představovat v některých případech složitější postupy při identifikaci a pochopení útoku. I když není zatím stanovena jednotná oficiální cesta pro vytváření těchto zpráv, která by zaručila společnou taxonomii, vznikla již hojně používaná řešení napříč kybernetickou komunitou. Jedno z nich představila i světoznámá organizace MITRE, která vytvořila

strukturovaný jazyk STIX pro popis CTI informací a znalostní bázi ATT&CK vedoucí k pochopení útoků.

Diplomová práce se zaměřuje na představení a použití projektu MITRE ATT&CK, který lze označit jako jeden z hlavních zdrojů informací o kybernetických hrozbách. Zároveň poskytuje detailní sadu charakteristik, umožňující komplexní pochopení chování útočníka. Tyto informace posléze pomáhají obráncům k vhodnému zvolení obranných mechanismů a efektivnímu řízení kybernetické bezpečnosti.

2 Cíl práce

Cílem diplomové práce je v první řadě seznámit její čtenáře se základními pojmy a termíny týkající se kybernetické bezpečnosti a dále s organizacemi, jež se danou problematikou zabývají na území České republiky. V další části autor kompletně představí znalostní bázi MITRE ATT&CK. V jednotlivých bodech bude upřesněna struktura projektu, nástroje a metody používání. Na základě nabytých informací a bližšího průzkumu problematiky autor definuje relevantní taktiky a techniky cílící na základní funkcionalitu platforem Windows a Linux. V praktické části se autor zaměří na zvolený výběr útočných technik a navrhne možné formy zmírnění dopadu pro obě platformy.

3 Rešerše

Zatímco rámec MITER ATT&CK účinně pomáhá organizacím s obranou proti kybernetickým hrozbám, dostupnost literatury pro využívání této technologie je vcelku omezená. V této kapitole bude shrnuta literatura a odborné články, které se zabývají reálnou integrací MITRE ATT&CK v rámci kybernetické bezpečnosti.

Výzkumníci Oosthoek a Doerr [1] demonstrují ve své odborné práci, jak lze rámec MITER ATT&CK použít při mapování malwarových útoků. Malware figuruje mezi jednou z nejvíce útočníky využívaných technik. Autoři vycházejí ze zprávy společnosti Verizon Data Breach Investigations, která uvádí, že útoky malwaru tvoří až 30 % narušení dat. Kvůli závažnosti malwarových útoků je pro kybernetické odborníky důležité získat přehled o tom, jak útočníci tuto techniku zneužívají. K provedení tohoto výzkumu autoři shromáždili data související s analýzou malwaru z renomované databáze Malpedia, která nabízí zdroj pro rychlou identifikaci malwaru. V rámci zkoumání použili MITER ATT&CK k mapování 951 jedinečných skupin malwaru na platformě Windows. Díky této znalostní bázi mohli výzkumníci popsat techniky malwaru, které mohou útočníci použít k útoku na systém. Prostřednictvím aplikace rámce MITRE ATT&CK shromáždili dostatečný obnos informací o chování protivníků, což pomohlo zavést nejvhodnější preventivní mechanismy. Autoři konstatují, že díky společné taxonomii, byli schopni pochopit, jak útočníci provádějí malwarové útoky od plánování až po provedení.

V práci *Learning the Associations of MITRE ATT&CK Adversarial Techniques* [2] se autoři pomocí statistické analýzy při aplikaci strojového učení na různé datové sady hlášených útoků, pokoušejí predikovat techniky útočníka definované v rámci MITRE ATT&CK. Datová sada obsahovala celkem 270 případů útoků, které se skládaly z 209 technik. Autoři pro analýzu využívají kvalitativních a kvantitativních statistických metod, zejména shlukování a korelaci. Výsledky hodnocení výzkumu ukazují, že autory navržený algoritmus ve velké míře případů asociuje vzájemné informace s technikami z rámce MITER ATT&CK. Díky tomu mohou předvídat útočníkem používané techniky.

Odborný článek *A-DEMO: ATT&CK Documentation, Emulation and Mitigation Operations* [3] je zaměřený na implementaci frameworku A-DEMO, který má poskytovat strukturovanou metodologii pro správnou analýzu, dokumentaci, emulaci a mitigaci kybernetických útoků z reálného světa. Autoři článku rozdělují používání

navrhovaného frameworku do šesti fází, ve kterých jsou provedeny specifické úkony, které zajistí replikaci chování útočníka. První tři fáze jsou vyhrazené pro vizualizaci prostředí, kdy se postupně přes kroky jako například definice síťové topologie, určení hardwaru a softwaru nebo diagnostiku zranitelností, emuluje reálně využívané prostředí. Zbylé tři fáze jsou postaveny na využití rámce MITRE ATT&CK, který obsahuje všechny podrobné informace pro vytvoření dokumentace, sestavení scénáře útoku a následné možnosti v podobě opatření. Autoři demonstrují celý návrh a všechny výše zmíněné kroky v rámci emulace využití malwaru rootkit na modelové infrastruktuře zdravotnického prostředí.

Práce *Forensic Analysis of Advanced Persistent Threat Attacks in Cloud Environments* [4] se zabývá studií zaměřenou na použití rámce MITRE ATT&CK ve spojení s prováděním forenzních analýz kybernetických útoků na cloudových platformách. Autorka používá matici ATT&CK jako základní znalostní zdroj pro identifikaci důkazů o útoku na cloud platformu z dostupných informací. Výsledky jsou následně agregovány a korelovány, což umožňuje zkonstruování jednotlivých kroků útoku. Práce je demonstrována na modelovém virtuálním prostředí s aplikací techniky SQL Injection. V provedené analýze dochází k identifikaci forenzních dat a převodu na situace před a po útoku. Informace jsou poté zpracovány nástrojem, který automaticky sestaví kroky útoku.

V poslední představené studii *Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation* [5] se autoři zaměřují na hybridní model pro odhalování taktik, technik a postupů útočníka pomocí útočného zabezpečení. V praxi se jedná o proaktivní vyhledávání hrozeb prostřednictvím emulace protivníka. V úvodu článku jsou shrnuty obdobné přístupy, například v podobě red teamingu a zároveň definovány jejich nevýhody. V další části se již zaměřují na představení navrženého indukovaného modelu emulace a jeho užití v rámci definovaného modelového prostředí. Pro navržení emulačního plánu a detekci technik, autoři využívají matici ATT&CK. Konkrétně se při modelaci zaměřují na techniky skupin APT28 a APT3.

4 Úvod do kybernetické bezpečnosti

S narůstající tendencí kybernetických útoků se celosvětově řešeným tématem stává ochrana a bezpečnost v rámci virtuálního prostoru, též označovaného jako kyberprostor. Obor řešící tuto problematiku se nazývá kybernetická bezpečnost. Jednotnou a přesně vystihující definici tohoto pojmu, prozatím odborníci nestanovili. Ovšem v celkovém shrnutí ho lze definovat jako praxi zabývající se souhrnem technických, právních a organizačních pravidel zajišťující ochranu počítačových systémů, ICT prvků a citlivých informací uživatelů. Na základě definovaných pravidel jsou dále postaveny nástroje, pokyny, postupy nebo školení za jejichž pomoci je možné udržet bezpečnost v rámci organizací a majetku jednotlivých uživatelů proti bezpečnostním rizikům v kybernetickém prostředí. Nelze ovšem opomenout úzké propojení virtuálního a reálného světa, proto můžeme uvažovat o využití kybernetické bezpečnosti i mimo virtuální prostor. [6][7]

4.1 Princip CIA

V základní reprezentaci bezpečnostních cílů nalezneme tři pilíře v podobě důvěrnosti (confidentiality), celistvosti (integrity) a dostupnosti (availability). Právě tyto faktory slouží v celkovém měřítku pro vyhodnocení bezpečnostní infrastruktury každé organizace. Zároveň je ale vhodné, nahlížet na každý z bodů individuálně, protože tím můžeme zvolit vhodnější způsoby provedení zabezpečení nebo řešení případných problémů. Ideální scénář představuje definici a implementaci všech tří norem, díky nimž je bezpečnost silnější a lépe čelí incidentům a hrozbám. V opačném případě lze přepokládat, že bude zajisté jedna z těchto zásad porušena. [8][9]

4.1.1 Důvěrnost

Hlavní cíl důvěrnosti spočívá v zajištění dostupnosti dat a informací pouze pro oprávněné subjekty, entity nebo jednotlivce. V praxi se jedná o kontrolu přístupu k datům na základě úspěšné autentizace. Pokud nedojde ke správnému ověření přístupových údajů nelze k datům nebo zařízením přístup poskytnout. Důvěrnost může být narušena mnoha způsoby. Z pohledu kybernetického prostředí se však nejčastěji jedná o přímé kybernetické útoky s cílem získat přístupy k systémům nebo proniknout do aplikací či databází. Mezi hojně používanými technikami útočníků, nalezneme

například skenování a odposlouchávání sítě. Další faktor, který může mít za následek porušení důvěrnosti je neúmyslná lidská chyba, případně zanedbání bezpečnostních kontrol. V těchto případech lze uvažovat o nedostatečném šifrování komunikace, zcizení přístupových údajů nebo dokonce celého hardwaru. Z tohoto důvodu je užitečné provést různé ochranné mechanismy proti jejímu prolomení. Mezi ně patří například šifrování dat, zejména při přenosu v procesech, řízení a kontroly přístupů nebo vícefaktorové autentizace. Dále je vhodné aplikovat na data klasifikační schémata dle bezpečnostních standardů s jejichž pomocí ohodnotíme jejich kritičnost. Nelze také opomenout řádné proškolení přistupujících uživatelů. [8][10]

4.1.2 Integrita

Integrita neboli celistvost vyznačuje vlastnost přesnosti a úplnosti aktiva. Zaručuje se tím, že nebyl proveden neoprávněný zásah do dat, systémů nebo nastavení. V informačních technologiích jsou s tímto termínem spojovány terminologie integrita dat nebo integrita systému. Pokud dojde k narušení integrity byla provedena nežádoucí modifikace, jejíž následky se mohou dostavit až po uplynutí delší doby. Obdobně jako u důvěrnosti, lze předpokládat záměrné poškození útočníkem nebo chybu lidského faktoru. Protiopatření chránící integritu zahrnuje například hašování, šifrování, digitální certifikáty nebo digitální podpisy. [9]

4.1.3 Dostupnost

Poslední ze základních vlastností je dostupnost, neboť i když budou dodrženy oba předchozí pilíře, bez dostupnosti dat nebo počítačových systémů, se nedostává jejich využití. Z tohoto hlediska lze definovat dostupnost jako vlastnost garantující přístup k datům, informacím či systémům na žádost oprávněné entity. Dostupnost může být ohrožena řadou faktorů. Kromě napadení systému útočníkem z předchozích případů zde přibývají i živelné pohromy nebo prostý výpadek dodávky elektřiny. Pro dobré zajištění se doporučuje využívat redundantních řešení hardwarových prvků, aktualizace softwarových systémů a v neposlední řadě pravidelné zálohování dat. [6][8]

4.2 Prvky a procesy bezpečnosti

Aplikace kybernetické bezpečnosti do prostředí vyžaduje vzájemnou interakci prvků vyskytujících se v kyberprostoru. Mezi tyto prvky lze zařadit definované procesy, technologie nebo lidskou složku. Zajisté by bylo ideální, aby tato vzájemná spolupráce dodržovala všechna nastolená pravidla. Nicméně takzvané „stoprocentní kybernetické bezpečí“ není a nebude ho možné nejspíše vytvořit. Úkolem všech vyjmenovaných elementů je minimalizovat chybná jednání, alespoň do dostatečně bezpečné míry.

Základ bezpečného prostředí představují nastavená pravidla a procesy, díky kterým lze efektivně řešit bezpečnost nebo případné komplikace. Výběr a nastavení těchto procesů je velmi rozsáhlý a často individuální. Pro představu lze uvést například:

- řízení a vyhodnocování rizik,
- instalace ICT prvků a aplikací,
- údržba a aktualizace systémů,
- penetrační testování, detekce kybernetických útoků,
- bezpečnostní auditování,
- edukativní činnost, školení.

Při vhodném navržení a nastavení by mělo dojít k účelnému zabezpečení prostředí. Nelze opomenout, že díky proměnlivému chování kybernetických hrozeb je důležité provádět vhodné modifikace, tak aby byla udržena kvalita zabezpečení. [6]

4.3 Životní cyklus kybernetické bezpečnosti

Zavedení kybernetické bezpečnosti představuje sled činností zaměřených na prevenci, detekci a reakci na případné hrozby. Aplikací těchto definovaných úkonů, lze dosáhnout dostatečné míry zabezpečení prostředí, nikoliv však absolutní ochrany. Vzhledem k širokému spektru kybernetických hrozeb, které se neustále vyvíjí nebo mění je důležité zvolený soubor operací procházet v nekonečné smyčce. Odborníci na kybernetickou bezpečnost označují tento soubor jako životní cyklus kybernetické bezpečnosti a znázorňují ho často pomocí diagramu, který zobrazuje obrázek č.1.

Obrázek 1 - Diagram životního cyklu kybernetické bezpečnosti
Zdroj: [11]

Z představeného schématu je možné pozorovat jednotlivé kroky implementace kybernetické bezpečnosti. V prvním kroku se na základě analýzy prostředí stanovují základní rizika a úrovně zabezpečení. Druhým krokem je definice a navržení systému za pomoci vhodných bezpečnostních opatření, které se vyhodnotí na základě rizik. Třetí krok zahrnuje zavedení navrhnutých opatření a postupů jejichž cílem je zajistit minimální dopad hrozeb na provoz. V předposledním kroku celého cyklu probíhá monitorování a kontrola implementovaných opatření. Poslední krokem je audit neboli odhalení rizik a hrozeb při sledování operací v prostředí. Na základě identifikace hrozby je realizováno opatření, které zabraňuje další interakci v systému. Po tomto kroku se opět přechází na první bod a cyklus se provede znovu. [12]

4.4 Základní terminologie

Problematika kybernetické bezpečnosti je velmi rozsáhlé a rychle rozvíjející se téma. Z tohoto důvodu je pro snadnější uvedení do daného oboru vhodné zmínit zlomek zásadních termínů, které se často používají v odborných publikacích a článcích nebo v přímé komunikaci.

4.4.1 Informace

Jedná se o jakýkoliv znakový výstup neboli data, která mají význam pro vlastníka a komunikující protistranu. [13]

4.4.2 Aktivum

Aktivum definuje cokoliv, co má určitou hodnotu pro jednotlivce, organizaci nebo jiný objekt veřejné správy. Nemusí se však jednat pouze o nějaký objekt nebo věc. Z pohledu kybernetické bezpečnosti je aktivem označována například i vlastnost (dostupnost dat) nebo skupina lidí (administrátoři). Obecně se aktiva rozdělují na čtyři zájmové typy:

- **personál –** zaměstnanci organizace a jejich znalosti a schopnosti,
- **zařízení** – místa, nástroje, HW a SW vybavení umožňující uskutečnit personálu pracovat,
- **procesy –** postupy a pravidla, kterými se organizace řídí a používá pro dosažení cílů,
- **informace –** data držená jednotlivcem, skupinou nebo organizací. [14]

4.4.3 Riziko

Pravděpodobnost reálné hrozby, která by měla negativní dopad na aktivum. V praxi se jedná o možnou událost, při které jsou například poškozena nebo odcizena data. V rámci životního cyklu kybernetické bezpečnosti jsou právě tyto pravděpodobnosti vyjadřovány pomocí analýzy rizika. Pro stanovení rizika se obecně používají tři základní otázky:

- Co špatného se může stát? Co může selhat?
- S jakou pravděpodobností nastane nežádoucí stav?
- Jaké zranitelnosti lze zneužít?

Pro bližší specifikaci rizika jsou následně použity další doplňující otázky, které ovlivňují jeho charakteristiku. Analyzovat míru rizika vyžaduje dobrou znalost aktiv a možných hrozeb, které se v jejich prostoru vyskytují. Po vyhodnocení těchto rizik se stanovují opatření, při nichž dochází k jejich minimalizování nebo odstranění. [6][14]

4.4.4 Zranitelnost

Zranitelnosti představují neošetřená místa a způsoby jakými mohou být aktiva kompromitována útočníkem. Z praktického hlediska se jedná o porušení jednoho nebo více pilířů principu CIA představeného v kapitole 4.1. Zranitelnosti lze rozdělit na známé a neznámé. V případě známých zranitelností jsou následně vydány opravy v podobě

bezpečnostních záplat. Důležitou roli u neznámých zranitelností hraje její objevitel, protože pokud se jedná o útočníka, může dojít k poškození aktiva dříve, než dojde k opravě. [14]

4.4.5 Kybernetická hrozba

Kybernetická hrozba představuje událost nebo stav, který může potenciálně způsobit ztrátu aktiv nebo na ně mít nežádoucí vliv. Ať už se jedná o poškození systému, modifikaci dat nebo nedostupnost služeb, jejím hlavním cílem je způsobit některou formu škody. Konkrétní příčiny ztráty aktiv mohou vyplývat z různých podmínek a událostí. Pro představu lze například uvést živelné pohromy, fyzické poškození, HW a SW chyby, neodbornost jednotlivce, ale také úmyslné napadení útočníkem. [15]

4.4.6 Kybernetická událost a incident

Dalo by se předpokládat, že pojem událost a incident ztotožňují jeden pojem ovšem výklady o kybernetické bezpečnosti je definují odlišně. Bezpečnostní událost představuje jakýkoliv nežádoucí pozorovatelný výskyt v systému nebo síti, který může narušit bezpečnost nebo integritu aktiva. Zpravidla by se jednalo o událost, při které by mohlo dojít k selhání nastavených politik bezpečnosti. Bezpečnostní incident bezprostředně navazuje na událost, ovšem při incidentu již dojde k prolomení bezpečnostních zásad. Pro názornou ukázku lze uvést jednoduchý příklad, kdy dojde zaměstnanci email se škodlivým malwarem (událost). Pro jeho nainstalování je však nutná součinnost zaměstnance. V případě že dojde k instalaci, běžící program infikoval počítač a navázal spojení s útočníkem. V tomto případě se bezpečnost prolomila a je již evidována jako bezpečnostní incident. [16]

4.4.7 Kybernetický útok a kriminalita

Za kybernetický útok je považována nezákonná, nepovolená akce útočící na prvky umístěné v kyberprostoru. Její záměr může mít různý charakter, ať už se jedná o krádež dat, poškození subjektu nebo získání citlivých informací, vždy je směřován proti zájmům jiné osoby. Útok má velmi podobné rysy jako incident, ovšem je zde jeden podstatný rozdíl. K incidentu může dojít neúmyslně, jak již bylo zmíněno u hrozby. V případě kybernetického útoku se však jedná o úmyslné (občas „náhodné“) napadení objektu, za účelem ho poškodit. Typy útoku lze rozdělit do následujících kategorií:

- **přerušení** – forma útoku specializující se na dostupnost aktiva (vyřazení služby, poškození softwaru, porucha OS),
- **odposlech** – forma útoku specializující se na důvěrnost, neověřený subjekt si neoprávněně zpřístupní aktivum (zkopírování softwaru nebo dat),
- **změna** – forma útoku specializující se na integritu, neověřený subjekt ovlivní aktivum (úprava uložených/přenášených dat, přidání funkcionality do softwaru),
- **přidaná hodnota** – forma útoku specializující se na autenticitu (falešná data, podvržení transakcí).

Kybernetickou kriminalitu lze považovat jako odvětví klasické kriminality, kdy dochází také k protiprávnímu jednání (krádeže, podvody, zcizení identity). Tento druh nezákonného jednání, ale operuje v kyberprostoru a jeho nástrojem nejsou fyzické činy, nýbrž zmiňované kybernetické útoky. Vzhledem k dnešní digitální době se čísla incidentů, ve kterých je použita kybernetická kriminalita postupně zvedají. V mnoha případech není pachatel dohledán. Za častý cíl kybernetických útoků lze považovat státní nebo kritické subjekty jako nemocnice, úřady, firmy ale i celé státy. Typy a formy útoků jsou velmi rozmanité, mezi nejpoužívanější metody se řadí tyto:

- **DoS** – cíle tohoto útoku je znepřístupnit službu. Útočník vysílá velké množství požadavků na službu, až dojde k jejímu přehlcení a není schopná odpovídat na relevantní dotazy,
- **DDoS** – forma DoS útoku, který je prováděn z velkého počtu počítačů v jednom časovém úseku,
- **MITM** – útočník se snaží odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem,
- **Phishing** – získávání citlivých údajů za účelem jejich následného zneužití,
- **Ransomware** – škodlivý software šifrující data nebo soubory systému za které následně útočník vyžaduje výkupné pro jejich odšifrování,
- **Spoofing** – útok založený na falšování identity zdroje. [17][18]

4.5 Kybernetická bezpečnost v ČR

Problematiku kybernetické bezpečnosti můžeme považovat stále za vcelku nový obor, ovšem i tak se za velmi krátké období stal jedním z klíčových témat při obraně státních subjektů. Není tomu jinak ani v případě České republiky. Prvotní správu kybernetické a informační bezpečnosti mělo ve své kompetenci Ministerstvo informatiky, které bylo ale v roce 2007 zrušeno a kompetence se převedla na Ministerstvo vnitra. V březnu roku 2010 byl přes schvalovací proces několika usnesení o „Národní strategii informační bezpečnosti České republiky“ zvolen gestorem a národní autoritou kybernetické bezpečnosti Národní bezpečnostní úřad. Mezi hlavní cíle tohoto státního úřadu patřilo kromě koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetických útoků, navrhování a přijímání různých opatření i příprava nového zákona o kybernetické bezpečnosti.

Nový zákon byl předložen a následně podepsán prezidentem České republiky dne 29. srpna 2014 s nabytím účinnosti od začátku roku 2015. Ve sbírce zákonu byl označen číslem 181/2014 Sb.. Cíl tohoto zákona spočívá v implementaci funkčního systému, který zajišťuje kybernetickou bezpečnost, zahrnuje bezpečnostní opatření, detekuje bezpečnostní události nebo zavádí činnost dohledových pracovišť. Zákon vychází z evropské směrnice NIS, norem ISO 27000 a COBIT.

Zákon doznal od svého zavedení různých právních úprav a přidání dalších stanovisek, a proto byl dne 1.srpna 2017 novelizován zákonem č. 205/2017 Sb.. [19][20]

4.6 NÚKIB

Právě na základě novely vznikl nový úřad Národní úřad pro kybernetickou a informační bezpečnost sídlící v Brně, který je ústředním správním orgánem v oblasti kybernetické bezpečnosti v České republice. Úlohou tohoto správního úřadu je kybernetická bezpečnost státu, ochrana utajovaných informací pro oblast informačních a komunikačních technologii či kryptografická ochrana. Na půdě tohoto úřadu se navrhují a vznikají bezpečnostní standardy, strategie nebo zákony, které nastavují bezpečnostní politiku České republiky v oblasti kybernetiky. Další z důležitých funkcí NÚKIB je národní a mezinárodní spolupráce s bezpečnostními týmy, která napomáhá k efektivnější ochraně státu. Kromě kybernetické bezpečnosti se úřad dále zabývá i problematikou ohledně veřejné služby navigačního systému Galileo. [21]

4.6.1 Vládní CERT

Představuje bezpečnostní tým označovaný jako GovCERT.CZ, který je součástí NÚKIB. Z pohledu bezpečnosti státu zastává klíčovou roli, neboť se zabývá ochranou kritických informačních infrastruktur a informačních systémů, specifikovaných dle zákona o kybernetické bezpečnosti. Úlohou týmu je efektivně řešit bezpečnostní výzvy, přijímat a evidovat kybernetické incidenty a účelně předcházet možným hrozbám. Zároveň by tento tým měl působit jako kvalifikovaný zdroj informací ohledně bezpečnosti pro státní orgány, instituce i občany. Obdobné státní týmy nalezneme v každé zemi, která potřebuje chránit své kritické systémy. Pokud je kritická infrastruktura provozována soukromým subjektem, jež má svůj bezpečnostní tým, je dle zákona o kybernetické bezpečnosti povinen plnit nadefinované úkony vůči vládnímu CERT týmu. aby v případě bezpečnostního incidentu došlo k vyřešení a obnovení provozu. [22]

4.6.2 Národní CERT

Jedná se o bezpečnostní tým, který je obdobou vládního CERT týmu. Hlavní rozdíl mezi těmito sdruženími je přesně definován v zákoně o kybernetické bezpečnosti. Z pohledu rozdělení kompetenci a správy lze národní CERT definovat jako koordinátora a řešitele ostatních bezpečnostní incidentů v systémech a sítích provozovaných v České republice kromě kritických, které spravuje vládní CERT. V České republice tuto roli zastává již od roku 2015 provozovatel sítí a informačních systémů CZ.NIC. [23]

4.7 Mezinárodní normy

Pro řízení a vhodnou implementaci kybernetické bezpečnosti byly vytvořeny mezinárodní normy. Norma představuje směrnici či pravidlo, stanovující požadované vlastnosti, procesy nebo určité práce. Mezi nejznámější celosvětové organizace zabývající se normami patří ISO, IEC nebo ITU. Každý stát má svůj úřad, který se stará o správu norem na daném území. V České republice tuto roli zastává Úřad pro technickou normalizaci, metrologii a státní zkušebnictví**.** Tento úřad vydává již upravenou mezinárodní normu pod označením **ČSN,** v níž jsou zahrnuty všechny platné normy.

Pro kybernetickou bezpečnost se jeví jako nedůležitější skupina norem **ČSN ISO/IEC 27xxx**, která má za úkol pomoci se zavedením a provozem systému managementu bezpečnosti informací ISMS. Celkem se v této skupině nachází 114 norem, mezi základními nalezneme:

- **ČSN ISO/IEC 27000 -** Systémy řízení bezpečnosti informací – Přehled a slovník,
- **ČSN ISO/IEC 27001 -** Systémy managementu bezpečnosti informací – Požadavky,
- **ČSN ISO/IEC 27002** – Soubor postupů pro opatření bezpečnosti informací,
- **ČSN ISO/IEC 27003** – Systémy řízení bezpečnosti informací – Pokyny,
- **ČSN ISO/IEC 27004** – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení,
- **ČSN ISO/IEC 27005** – Řízení rizik bezpečnosti informací. [20][24]

5 MITRE ATT&CK

MITRE ATT&CK představuje globálně dostupnou znalostní bázi a modelaci chování kybernetického útočníka, založeného na pozorování v rámci reálného světa. Hlavním zaměřením tohoto projektu je definovat a kategorizovat taktiky, techniky a postupy protivníků v rámci kybernetické bezpečnosti. Vzhledem k evidenci útoků, tak báze ATT&CK zároveň vytváří i formy obrany, které jsou užitečným základem pro vývoj bezpečnostních modelů a metodologií.

Za vznikem rámce ATT&CK stojí společnost MITRE, která v rámci jednoho ze svých výzkumů potřebovala systematicky kategorizovat chování útočníků. Projekt nesl název Fort Meade Experiment a jeho náplní bylo v monitorovaném modelovém prostředí analyzovat a testovat pokročilé techniky hackerských útoků. Na základě shromážděných dat z pokusů byla postupně vytvořena podstatná část rámce. První oficiální model znalostní báze vznikl v září 2013 a primárně se orientoval na použití Windows platformy v podnikové prostředí. V následujících letech rámec zaznamenal jistá vylepšení na základě interních výzkumů společnosti MITRE, ale i příspěvku z komunity zabývající se kybernetickou bezpečností. V roce 2017 byl rozšířen o platformy Linux a Mac nebo doplňkový model PREATT&CK. V tomtéž roce byl vydán i první rámec, který se soustředil výhradně na mobilní zařízení. ATT&CK je velice pružný a každým rokem dochází k jeho obměnám. V nynější podobě zahrnuje například i chování útočníků v dnes velmi využívaných cloudových službách nebo průmyslových řídících systémech. [25]

5.1 Rozdělení dle technologických domén

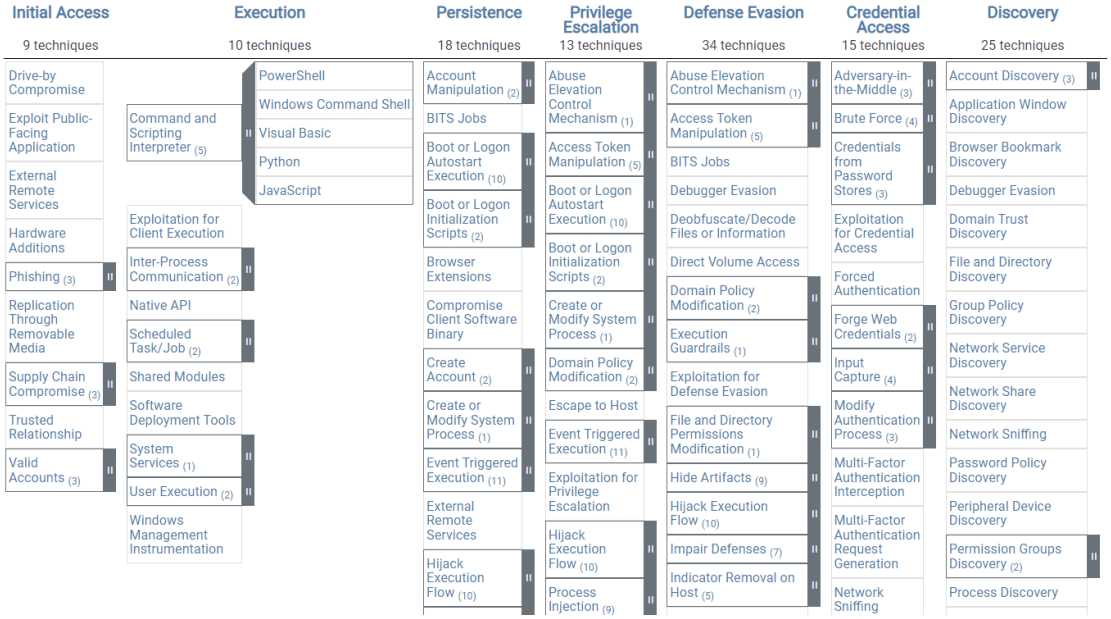
Rámec ATT&CK zpracovává více technologických odvětví, proto je rozdělen do tří zastupujících domén. Každá z těchto kategorií představuje technologie, ve nichž útočník operuje a která omezení musí pro dosažení svých cílů prolomit. Rámec je organizován do následujících oblastí:

- **Enterprise** – síťové a cloudové technologie,
- **Mobile** – mobilní komunikační zařízení,
- **ICS** – průmyslové řídící systémy.

Kategorie jsou dále rozděleny na několik platforem – systémů nebo aplikací, které více specifikují útočníkův záměr. V případě Enterprise domény jsou představeny platformy Windows, Linux, macOS, cloudové aplikace a služby (Office 365, Azure AD, SaaS, IaaS), síťové prvky a kontejnerové technologie. Mobilní doména obsahuje dva nejpoužívanější operační systémy Android a iOS. Rozsah rámce dále rozšiřuje nový modul PREATT&CK, jež je nezávislý na technologii. Modul upozorňuje na chování útočníků vykonávající průzkumy a shromažďování informací před získáním přístupu k sítím nebo systémům. [25][26]

5.2 Struktura rámce ATT&CK

Základním stavebním kamenem rámce ATT&CK je soubor technik a sub-technik, definující operace útočníků při provádění útoku. Stanovené cíle napadení jsou prezentovány a kategorizovány jako taktiky. Vzájemné vztahy mezi taktikami, technikami a dílčími technikami rámec vizualizuje maticí ATT&CK pro každou ze zmíněných domén. Tím je umožněn rychlý a přehledný přístup k informacím. V kontextu diplomové práce bude stěžejní matice pro doménu Enterprise, která ke své poslední dostupné aktualizaci z listopadu roku 2021 nabízí 14 kategorií taktik, 188 technik a 379 dílčích technik. Náhled na část této matice je zobrazen na obrázku č.2. [26]



Obrázek 2 - Náhled na matici ATT&CK
Zdroj: [26]

5.2.1 Taktiky

Taktiky reprezentují cíle útočníka, kterých lze dosáhnout během útoku. Zároveň každá z taktik definuje kategorie pro techniky a dílčí techniky, protože ty útočník používá právě pro dosažení cíle. Pro přesné určení taktiky slouží unikátní identifikátor v podobě kombinace textového řetězce s číslem po vzoru TA00XX, kde XX tvoří koncové číslo taktiky. Taktiky jsou dále doplněny o vlastní popis, aby bylo možné přesně zařadit využité techniky. Dostupné taktiky pro doménu Enterprise jsou představeny v následujících odstavcích. [27][28]

TA0001 – Initial Access

Počáteční přístup obsahuje techniky, při kterých se útočník orientuje na zisk přístupu k síti nebo systémům. Úkolem technik v této kategorii je využití slabin na veřejně přístupných bodech, kdy v případě úspěchu vzniká opěrný bod pro nepřetržitý nebo částečný přístup. [29]

TA0002 – Execution

Taktiky provedení obsahují techniky zaměřené na spouštění škodlivého kódu na přístupných systémech. Často je tato taktika použita s technikami z dalších kategorií a dochází k rozsáhlejšímu napadení. [29]

TA0003 – Persistence

Persistence neboli vytrvalost označuje cíl, při kterém útočníci využívají techniky pro trvalé zachování přístupu k systémům i v případě restartování, změně údajů nebo dalších forem přerušení. Zejména dochází ke změně konfigurace v oblasti práv, přidání kódu při startu systémů nebo úpravě programů. [29]

TA0004 – Privilege Escalation

Technikami napříč taktice s eskalací práv chtějí protivníci získat oprávnění s vyšší úrovní přístupu v rámci sítí nebo systémů. Na základě získaných práv mohou pokračovat v dalších taktikách, při nichž jsou nabytá oprávnění potřebná. [29]

TA0005 – Defense Evasion

Cílem této taktiky je použít operace zakrývající odhalení kompromitujícího chování z pohledu útočníků. Techniky se zaměřují na deaktivaci nebo odinstalování bezpečnostních programů, podvržení dat nebo zneužití důvěryhodných procesů. [29]

TA0006 – Credential Access

Primárním úkolem protivníků je ukrást přístupové údaje, nejčastěji v podobě přihlašovacího jména a hesla pro legitimní přístup. Použitím těchto údajů snižuje útočníkovo včasné odhalení a poskytuje mu prostor pro další manipulaci v systému. [29]

TA0007 – Discovery

Kategorie objevu a průzkumu disponuje technikami pro získání znalosti o napadeném prostředí. Útočník se pozorováním a zkoumáním systémů lépe zorientuje a může následně stanovit vhodnou strategii pro ovládání prostředí. [29]

TA0008 – Lateral Movement

Taktika se skládá z technik, které umožňují vzdálený přístup a ovládání systémů v síti. Často je tato taktika používaná v návaznosti na předchozí taktiku orientovanou na sledování a průzkum prostředí. Terčem útoku mohou být například služby jako SSH, VNC nebo přístup na vzdálenou plochu. [29]

TA0009 – Collection

Shromažďování dat a informací představuje jeden z dalších cílů případné kompromitace. Cílem je seskupit relevantní a citlivá data majitele, která následně mohou být ukradena, odstraněna nebo šifrována. Mezi běžné cílové zdroje patří emaily, multimediální soubory, data z prohlížeče nebo údaje o zadávání z klávesnice. [29]

TA0010 – Exfiltration

Exfiltrace vyznačuje techniky při kterých se útočník pokouší data ukrást a plně navazuje na shromažďování dat. Jakmile jsou data seskupena, následuje často jejich komprese s šifrováním a přenos z cílové sítě přes některou formu média. [29]

TA0011 – Command and Control

V této kategorii nalezneme formy technik a atributů při používání komunikace s napadenými systémy v rámci jejich sítě. Útočníci běžně využívají standardních komunikačních protokolů, aby napodobili běžný provoz a maskovali své operace. [29]

TA0040 – Impact

Skládá se z technik nesoucích přímý dopad na kompromitované systémy a data. Používané techniky vedou k narušení dostupnosti nebo integrity systémů. Dále mohou dopady provedených útoků zničit nebo poškodit data. Tyto techniky jsou často používány k dosažení záměrů nebo jako forma krytí pro porušení důvěrnosti. [29]

TA0043 – Reconnaissance

Taktika označená jako průzkum zahrnuje techniky útočníků zaměřující se na získávání a shromažďování informací ohledně vybraného cíle. Informace mohou obsahovat podrobnosti o infrastruktuře, systémech nebo zaměstnancích organizace. Tato taktika se využívá zejména k stanovení priorit v rámci dalšího záměru. [29]

TA0042 – Resource Development

Rozvoj zdrojů se skládá z technik, kde útočníci vytvářejí, nakupují nebo kompromitují zdroje podporující jejich následné formy útoků. Mezi takovými zdroji figurují například prvky infrastruktury, domény, účty nebo schopnosti lidí. [29]

5.2.2 Techniky a dílčí techniky

Techniky popisují metody útočníků, které používají pro dosaženích svých cílů. Zároveň lze z použité techniky definovat, jaký prostředek bude získán. Existuje mnoho forem útoku, jak dosáhnout jednotlivých taktických cílů. Proto každá z definovaných taktik disponuje více technikami. Z pohledu útoku je možné dosáhnout několika cílů obdobnými technikami útoku, a proto jsou některé techniky sdílené napříč maticí. Každý z prvků rámce ATT&CK má svůj jednoznačný identifikátor, není tomu jinak ani u technik. Formát jejich označení spočívá opět v kombinaci textového symbolu T se čtyřmi číslicemi jako například T1584. Jednotlivé techniky jsou doplněny o další důležité informace v podobě následujících bodů:

- charakteristika,
- zasažené platformy,
- potřebná oprávnění,
- dílčí techniky,
- procedury – skupiny a softwary,
- formy mitigace,
- detekce dle zdrojů dat.

Dílčí techniky byly založeny na základě větší přehlednosti a různých úrovní granularity, aby se více specifikoval daný soubor činností. Sub-techniky představují podrobnější popis implementace konkrétní techniky. V praxi to znamená, že konkrétní techniku lze provést několika různými dílčími technikami. I z pohledu označení, dochází pouze k rozšíření původního identifikátor techniky o tečku s číslicí, například T1584.001. Dílčí technika má stejně jako její předek své doplňující informace, formát zůstává obdobný jako výše zmíněný. [25][30]

5.2.3 Mitigace

Hlavní obsah rámce v podobě kategorií taktik, technik a dílčích technik je doplněn o další podpůrné třídy, které pomáhají s detekcí a řešením dané metody útoku. Mitigace neboli zmírnění patří mezi jeden z doplňujících objektů a představuje bezpečnostní návrhy a technologie, které mohou zabránit úspěšnému vykonání techniky. Tyto formy jsou nezávislé na platformách, protože nepopisují konkrétní vyřešení problému, nýbrž obecný popis vhodný pro danou oblast. Z pohledu rámce nese jejich identifikační znak kromě číslic písmeno M, například M1047 vyjadřující audit. V aktuální verzi rámce ATT&CK je pro doménu Enterprise dostupných 41 forem mitigace, pro představu lze uvést například segmentaci sítě, prevenci proti spouštění skriptů nebo zálohování dat. [25]

5.2.4 Skupiny

Veřejné i soukromé organizace zabývající se kybernetickou bezpečností sledují podezřelé a nežádoucí aktivity útočníků. Na základě analýzy v podobě různých metodologií a použitých technik jsou útočníci identifikováni a označeni pod veřejně známým názvem. V rámci ATT&CK jsou vedeny pod objektem skupiny, které definují

sady narušení, kolekci hrozeb, skupinu lidí představující obvykle cílenou a trvalou hrozbu. Některé skupiny této znalostní báze mají přiřazené další názvy, které jsou označované jako přidružené skupiny. Tato označení vznikají na základě hlášení napříč organizacemi a jsou párována v rámci překryvu podobných aktivit. Vzhledem k faktu, že jsou při přiřazování ostatních názvů využita pouze veřejná hlášení. Analytici doporučují provést podrobnější zkoumání technik, neboť se skupiny nemusí shodovat v konkrétním řešení. Skupiny mohou využívat napřímo definované techniky nebo některý ze softwarů, který je aplikuje. V ATT&CK je každá skupina kromě možných přidružených jmen doplněna o popis a reference na její využití v praxi. Její identifikátor začíná na písmeno G. [31]

5.2.5 Software

Kategorie Software zastupuje různé typy softwarů využitých útočníkem během útoku. V obecné rovině lze specifikovat software jako vlastní nebo komerční kód případně přímé nástroje operačních systémů, které konkretizují použitou techniku nebo dílčí techniku útočníka. Software je dle rámce rozdělen na dvě kategorie:

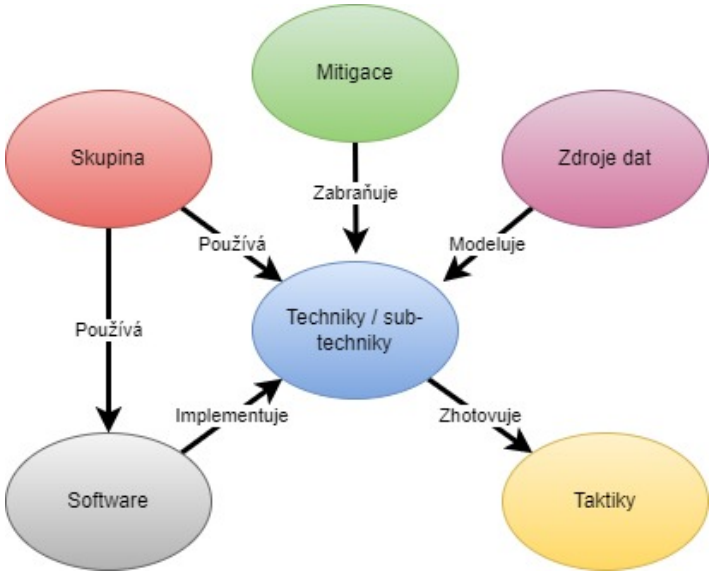
- Nástroj – open source nebo komerční software, který může používat obránce, tester, člen red teamu nebo útočník. Do této skupiny spadají například PsExec, netstat a další,
- Malware – software vytvořený na zakázku nebo s volně dostupným kódem využívající se pro škodlivé operace útočníků.

Obdobně jako u skupin jsou softwary integrovány na základě veřejných hlášení organizací. Z tohoto důvodu jsou i zde kromě specifikovaného názvu doplněny přidružené aliasy v rámci překrývání funkcionalit. V detailnějších pohledech na jednotlivé příklady softwarů lze nalézt informace o spárovaných technikách a skupinách, kategorii softwaru nebo platformě, na které se používá. I tato skupina má své identifikační označení začínající písmenem S. [25][32]

5.2.6 Zdroje dat

Zdroje dat reprezentují informace shromážděné senzory nebo logovací systémy sbírající relevantní data, na jejichž základě lze detekovat provedené techniky mapované v rámci ATT&CK. Zdroje dat bývají často přehlíženým faktorem při určení nepřátelských akcí. Jedná se však o jeden ze způsobů, jak vytvořit vztah mezi použitými technikami a útočníkem. Právě informace ze zdrojových dat poskytují pro každou techniku cenný kontext a vytvářejí možnost zlepšit detekční strategii a tím i pozici v rámci zabezpečení. [33]

Všechny představené kategorie modelu ATT&CK jsou navzájem propojené určitými souvislostmi. Vzájemné vztahy uvedené u každého typu objektu zobrazuje diagram na obrázek č.3.



Obrázek 3 - Model rámce ATT&CK
Zdroj: Převzato a upraveno z [33]

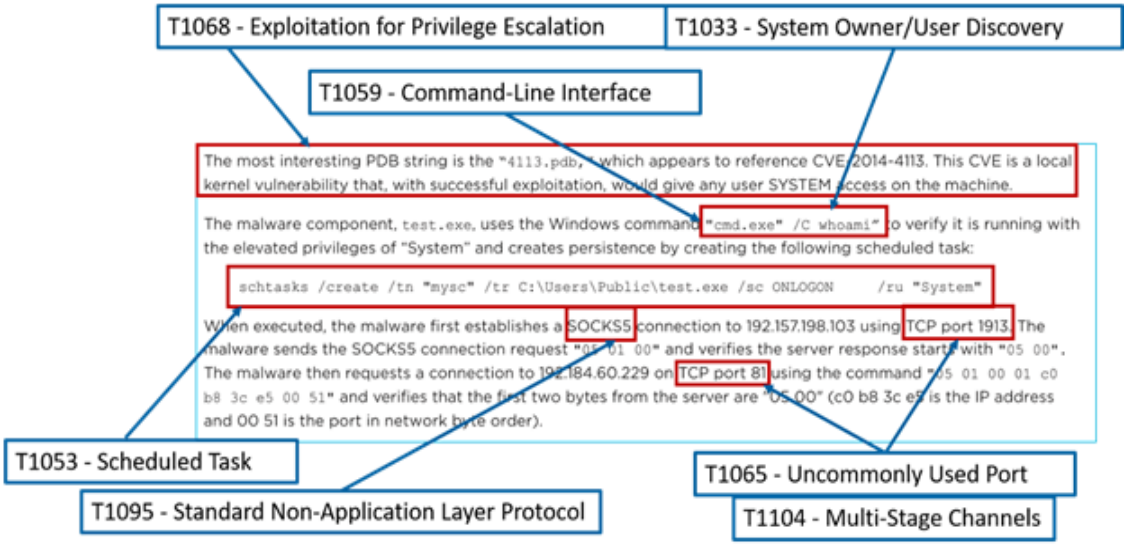
5.3 Mapování

Aby bylo možné rámec ATT&CK správně používat je důležité vědět, jak mapovat získaná data do matice. Úspěšným mapováním lze vytvořit profil útočníka, provádět analýzy aktivit a následně je začlenit do hlášení pro účely detekce, reakce a mitigace. Mapování informací můžeme provádět z pohledu zdroje dvěma různými způsoby.

První typ zdroje informací přináší interní nebo externí reporty z již uskutečněných incidentů. V hotových zprávách o útoku se často vyskytuje mnoho vodítek, které mohou

při analýze mapování zefektivnit. Vzhledem k rozsáhlosti matice je vhodné postupovat podle následujících kroků:

1. **Pochopení matice ATT&CK a útoku** – první krok zahrnuje seznámení se strukturou rámce a podrobné prostudování zprávy o incidentu. V počátečním průzkumu je důležité se zaměřit na hledání relevantních informací o provedených činností,
2. **Nalezení chování a vykonané činnosti** – k získání požadovaného kontextu o provedené akci je vhodné na daný problém nahlížet v širším smyslu. Pro pochopení útočníkova chování by nejdříve měly být identifikovány všechny jeho možné náznaky. Kromě prvotních indicií jako je IP adresa lze uvažovat například i nad použitým softwarem. K nalezení většiny použitých činnosti bývá využito populárních přístupů v podobě hledání a vyznačení klíčových sloves,
3. **Průzkum chování –** pokud nalezené chování neznáme nebo kontext útoku není komplexní, musí se provést detailnější průzkum. Využitím dalších dostupných zdrojů od subjektů zabývajících se kybernetickou bezpečností můžeme získat nové technické detaily. Díky tomu lze nalézt další návaznosti, které pomohou pochopit celkové chování protivníka a související cíle,
4. **Určení taktiky –** chceme-li identifikovat taktiku musíme zvážit a určit protivníkovi cíle. Na základě předchozích kroků by mělo identifikované chování odpovídat jedné z představených taktik v kapitole **5.2.1**,
5. **Určení technik a dílčích technik –** určení techniky může být trochu složitější operace. Po vybrání taktiky následuje prozkoumání všech dostupných technik a propojení s definovaným chováním z reportu,
6. **Porovnání výsledků s ostatními analýzami –** pokud lze tak učinit je vhodné porovnat dosažené mapování s analýzami od dalších analytiků. Spolupráce s dalšími analytiky může poskytnout jiný úhel pohledu na daný problém. Vzájemné porovnání může vést k přesnějšímu zmapování taktik a technik. [34] [35]



Obrázek 4 - Mapování technik z reportu
Zdroj: [34]

Druhým ze zdrojů pro mapování jsou nezpracovaná surová data. Tato data zahrnují kombinaci více zdrojů informací, které mohou obsahovat znaky škodlivého chování. Původcem této formy dat mohou být například zachycené síťové pakety, události systému, příkazy shell nebo výstupy z forenzní analýzy disku. Postup mapování používá obdobný sled operací, které jsou představeny u prvního typu zdroje. Vyžaduje ovšem větší odbornost a znalost systémů pro provádějící osobu. Značné ulehčení při tomto typu průzkumu představuje využití dalších nástrojů, které shromažďují a analyzují nezpracovaná data. Tyto nástroje jsou označovány zkratkou SIEM a většinou již mají nadefinovaná různá pravidla detekce, postavena například i přímo na matici ATT&CK. [35]

5.4 Nástroje

Projekt ATT&CK se postupně od doby svého uvedení stal jedním z nejpoužívanější podkladů pro řízení a udržování kybernetické bezpečnosti. V počátcích neexistovalo mnoho nástrojů, jak efektivně analyzovat a navrhovat používané techniky. Jedním z prvotně využívaných programů byl a stále zůstává tabulkový editor Excel. Na základě rostoucího zájmu v rámci celosvětové komunity začaly vznikat další open-source i komerční nástroje, které umožňují tuto znalostní bázi efektivněji využívat. Kromě maticové podoby je ATT&CK dostupný i ve strojově čitelném formátu STIX, který se využívá pro výměnu informací o kybernetických hrozbách. Tento strukturovaný jazyk

právě využívají zmíněné podpůrné nástroje pro svou implementaci. Pro lepší orientaci je vhodné představit základní nástroje. Některé z nich budou využity i při dalším zpracování diplomové práce. [36]

5.4.1 MITRE ATT&CK Navigator

Navigator je webový i desktopový nástroj poskytující základní navigaci a anotaci rámce ATT&CK. Oproti tabulkovému editoru poskytuje komfortní rozhraní pro vizualizaci vlastního návrhu obraného pokrytí, testovací plány nebo detekci využívaných technik. Hlavní výhodou pro uživatele je možnost definovaní vlastních pohledů v rámci jednotlivých platforem, zvýrazňovaní a obodování útočníkových technik. Navigator dále umožňuje export vytvořených matic do několika formátů pro další využití nebo zpětném nahrání do aplikace.[36][37]

5.4.2 MITRE Caldera

Analýza bezpečnostních aspektů prostřednictvím penetračního testování nebo emulace protivníka v zastoupení červených týmů je často nákladná na finance i lidské zdroje. Z tohoto důvodu se zakladatelé rámce ATT&CK zaměřili i na jeho efektivní využití a vytvořili platformu Caldera. Tento systém nabízí inteligentní, automatizovaný proces pro rutinní testování zabezpečení koncových zařízení formou replikace chování útočníka. Caldera je založena na matici ATT&CK, ze které implementuje dostupné techniky. Analýzou dosažených výsledků se definují bezpečnostní hrozby, což umožňuje včasnou reakci na jejich odstranění a možnost vyladění detekčních systémů.

Caldera je složena ze dvou komponent server a pluginy. Server obsahuje webové rozhraní pro snadné ovládání a komunikační rozhraní pro agenty umístěné na koncových bodech. Pluginy představují samostatnou jednotku, která rozšiřuje funkčnosti základního pilíře v podobě serveru. Mezi nimi figurují právě i agenti, kteří slouží pro provádění zvolených technik na koncových zařízeních. Implementaci a používání softwaru Caldera vystihuje dosti podrobná dokumentace a její kód je veřejně dostupný. [38][39]

5.4.3 Atomic Red Team

Dalším z často využívaných open source nástrojů je Atomic Red Team poskytující jednoduchou formu na simulaci napadení. Velké procento těchto aplikací je založeno na programovacím jazyce Python nebo jiném skriptovacím jazyce. Atomic Red Team

poskytuje knihovnu testů založených na technikách rámce ATT&CK, které využívají pro své spuštění nástroje dostupné v rámci základní instalace systému. Platforma tak nabízí snadnou metodu, jak emulovat chování útočníka a detekovat bezpečností problémy.

Techniky mohou být implementovány jednotlivě nebo formou zřetězení testů dohromady a emulovat některou ze skupin definovaných ve znalostní bázi ATT&CK. Jednou z nevýhod využití tohoto nástroje může být neposkytnutí zpětné vazby. Takže detekci a reakci koncového bodu musí provést člověk nebo některý z integrovaných analytických nástrojů. [38]

Kromě dalších volně dostupných softwarů jsou k dispozici i komerční nástroje, které implementují matici ATT&CK a rozšiřují tím portfolio dostupných služeb. V mnoha případech se jedná o SIEM systémy sbírající a analyzující bezpečnostní události ze všech možných vrstev infrastruktury. Mezi těmito produkty figurují například IBM QRadar, Azure Sentinel nebo Splunk. Porovnáním s open source nástroji poskytují zejména robustnější bezpečnostní řešení, které napomáhá organizacím k udržení bezpečnosti.

5.5 Využití matice ATT&CK

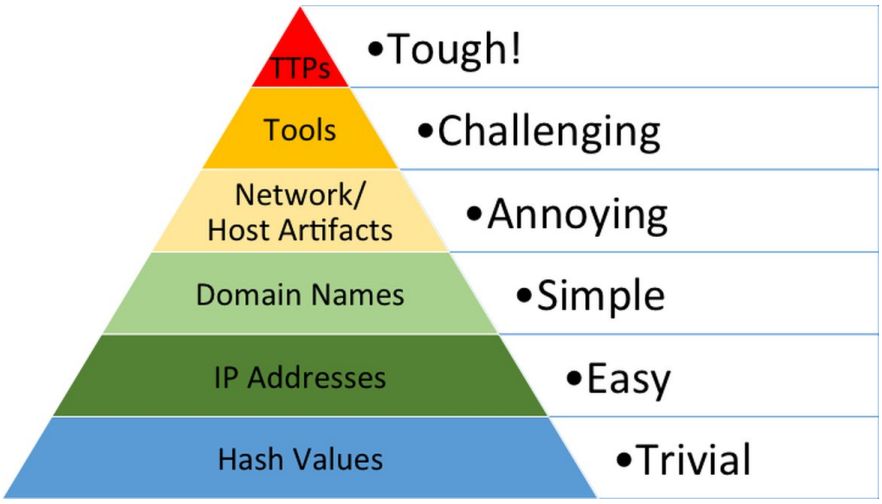
Projekt ATT&CK je široce uznávaný standard pro pochopení chování a technik, které hackeři aktuálně používají proti organizacím. Poskytuje společnou taxonomii pro odborníky zabývající se kybernetickou bezpečností s možností efektivně spolupracovat a diskutovat o metodách pomáhajících s bojem proti kybernetickým útokům. Z teoretické roviny plně přechází k praktickým aplikacím pro využití zejména bezpečnostními týmy. ATT&CK může poskytnout cenné informace pro jakékoliv organizace, které chtějí zvýšit znalosti o hrozbách a budovat komplexnější obranu v rámci kybernetické bezpečnosti. Scénáře používání této znalostní báze se odvíjejí od zaměření dané organizace a jejího specifického chování. Základní možné případy využití definují následující skupiny.

5.5.1 Cyber Threat Intelligence

Zajistit úplnou kybernetickou bezpečnost není v současné době reálné. Vzhledem k dostupným možnostem, jakými dnes útočníci disponují není možné zabránit veškerým útokům či narušením. Pro společnosti v roli obránců je tedy velmi důležité se cíleně zaměřit na aktivní ochranu před možnými hrozbami. K tomu, aby bylo možné obranu

realizovat však musí mít detailní informace a znalosti o kybernetických rizikách. Cyber Threat Intelligence dále jen CTI představuje způsob pro získávání, zpracování a aplikování dostupných informací o kybernetických hrozbách, které následně mohou pomoci při zajištění obrany proti útočníkům.

Zpracování získaných informací ovšem může představovat velmi zdlouhavý proces. Pokud jsou zprávy k analýze obsáhlé, vyhledání relevantních informací zabere jejich konzumentům mnoho času. Jako jeden z dalších možných problémů lze uvést špatně provedenou analýzu a následné prověřování určených identifikátorů. Některé z nich mohou uniknout nebo v případě jejich špatného zvolení vytvořit falešná vodítka pro obránce. Z pohledu CTI je hlavním parametrem efektivní detekce chování útočníka. Vhodný princip řešení ukazuje populární pyramida bolesti zobrazená na obrázku č.5 od specialisty na kybernetickou bezpečnost Davida Bianca.



Obrázek 5 - Pyramida „bolesti“
Zdroj: [40]

Pyramida reprezentuje typy indikátorů pomáhající k odhalení nežádoucích aktivit a zároveň míru „bolesti“, kterou útočníkovy způsobíme odepřením daného indikátoru. Rychlost a přesnost detekce škodlivého chování je zásadní pro narušení průběhu útoku a zároveň pro formování obranných mechanismů. Z principu pyramidy je patrné, že nejpodrobnějším identifikátorem útočníka jsou jeho taktiky, techniky a postupy. Pokud umí obránci tyto informace detekovat v nejkratším možném intervalu, hacker by musel změnit kompletně svoji strategii a principy, aby nebyl odhalen. [40][41]

ATT&CK rámec poskytuje z pohledu CTI strukturovaný, a především jednotný způsob, jak popsat chování útočníka pomocí taktik, technik a postupů. Analytici či obránci mohou na základě ATT&CK lépe porozumět chování útočníka a efektivněji se zaměřit na účinnou obranu, která zahrnuje různé typy hrozeb. Díky této struktuře lze také porovnávat skupiny protivníků a používaných nástrojů, během jejich útoku. Způsob využití znalostní báze v rámci CTI je individuální proces závislý na zaměření organizace, počtu lidských zdrojů nebo dostupnosti informací a dat pro analýzy. Velmi vhodným nástrojem pro začátek je ATT&CK Navigator představený v kapitole 5.4.1, kde lze pohodlně mapovat samostatné techniky nebo přímo celé skupiny. Postupným rozšiřováním a překrýváním technik shodujících se zaměřením organizace lze stanovit jejich prioritní výběr pro detekci a mitigaci.

V celkovém shrnutí ATT&CK poskytuje společný „jazyk“, který v rámci informování o možných kybernetických hrozbách umožňuje rychlé zpracování informací i když jsou z různých zdrojů.[41][42]

5.5.2 Detekce a analýza

Na základě překročení určitých indikátorů signalizujících kompromitaci, lze analýzou a následnou detekcí chování protivníka, identifikovat potenciálně škodlivé aktivity v rámci systému nebo sítě. Při splnění těchto podmínek, není nutné spoléhat na předchozí znalosti o jeho akcích. Pouze využijeme interakcí, které je s ním spojují skrze použitou platformu. Matici ATT&CK můžeme použít při konstrukci a testování behaviorální analýzy a následné detekci útočníkova chování v prostředí.

Tvorba analýz pro detekci použitých technik se může lišit přístupem k samotné detekci a dále množstvím poskytnutých dat k analýze. Pokud data v podobě protokolů a vykonaných událostí nejsou dostupná, identifikace je spíše orientovaná na známé škodlivé operace, které jsou následně blokovány. V druhém případě je analýza provedena nad kolekcí shromážděných dat a vyžaduje určitá specifika. V první fázi je zásadní pochopit typ dat, která máme k dispozici pro vyhledávání. Abychom byli schopni identifikovat podezřelé chování je důležité vidět akce, které se v systému odehrávají.

Jeden ze způsobů je prezentuje báze jako zdroje dat popsané v kapitole 5.2.6. Na jejich základě lze získat přehled o daných technikách a dobrý výchozí bod pro určení

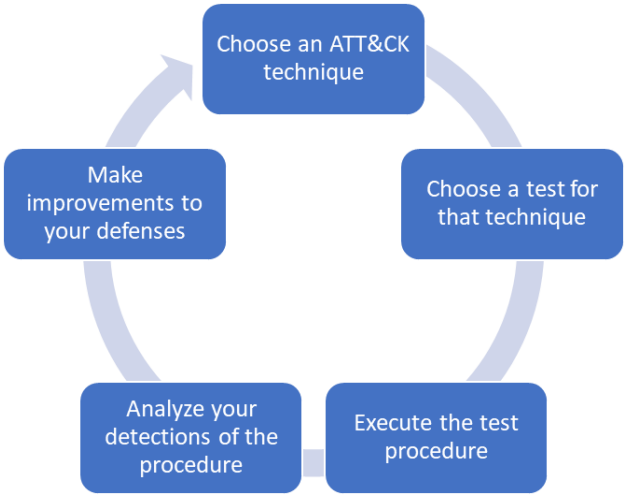
jaká data sbírat. Dalším krokem je využití některého ze softwaru SIEM, který bude data shromažďovat a umožní vytváření jednotlivých analýz vedoucích k detekci provedených technik. Při tvorbě analýzy je vhodné projít data vícekrát a v co největší míře jí specifikovat, čímž lze odfiltrovat falešně pozitivní výsledky. Na závěr je důležité provést její testování některým z dostupných softwarů z kapitoly 5.4 a dále rozvíjet, protože útočníkovým cílem je vyhnout se nastavené obraně. [43]

Obrázek 6 - Základní postup analýzy a detekce
Zdroj: Převzato a upraveno z [43]

5.5.3 Emulace protivníka a red teaming

Emulace protivníka představuje jeden z typů zapojení červeného týmu. Je zaměřena na schopnost ověřit detekci a mitigaci aktivity protivníka ve všech zjištěných bodech o jeho chování v rámci CTI. ATT&CK můžeme využít k vytvoření konkrétních scénářů napodobujících protivníka a jejich testování, kterým prověříme obranu proti jednotlivým technikám. Profily konkrétních skupin útočníků lze nadefinovat za pomoci informací obsažených ve znalostní bázi případně na základě mapování informací z CTI nebo dalších dostupných zdrojů.

S emulací protivníka úzce souvisí i provádění testů obsahujících jednotlivé techniky. Pro tento účel lze využít jeden z představených open source nástrojů a zkoumat reakce systému po provedení zvolených testů. Při odhalení problémů můžeme inkriminovaný nedostatek vyřešit opravou a opakovaným testem ověřit jeho funkčnost. Princip a postup testování zobrazuje diagram na obrázku č.7. [44]



Obrázek 7 – Testovací cyklus techniky
Zdroj: [44]

Red teaming se zaměřuje na dosažení konečného cíle útoku, aniž by došlo k jeho odhalení. Jedná se o týmy etických hackerů, kteří simulují domluvené útoky na organizace za pomoci sofistikovaných technik a svých osvědčených postupů a nástrojů. Hlavním účelem je ukázat nedostatky v rámci bezpečnosti, které mohou v případě reálného útoku zapříčinit provozní dopady. Na základě výstupu testování červených týmů poté obránci mapují, analyzují a detekují odhalené hrozby, čímž zvyšují ochranu proti reálným útokům. Matice ATT&CK v tomto ohledu může být podkladem k navržení plánů červeného týmu a definování technik, které použijí během cvičného útoku. Dále je možné ji použít jako plán pro výzkum a vývoj nových způsobů útoku, které nemusí být odhaleny běžnou obranou. [25][44]

5.5.4 Hodnocení obrany a SOC

Na základě hodnocení nastavené defenzivy mohou bezpečnostní architekti určit, které části systémů jsou kvalitně zabezpečeny, a naopak které vytváří potenciální slabá místa. I menší bezpečnostní mezery mohou umožnit protivníkovi získat některou z forem přístupu k systémům a datům, aniž by byl odhalen. Pomocí ATT&CK lze sestavit běžný model chování protivníka na jehož základě dojde k posouzení monitorování, detekce a zmírnění provedených technik. Z výsledného hodnocení mohou vzejít nezajištěná místa, která mohou vést ke zlepšení obranných mechanismů. Odborníci z MITRE stanovili pro proces hodnocení obecný postup v podobě následujících kroků:

1. Vyhodnocení aktuální obrany proti technikám útočníků v ATT&CK,
2. Identifikovat hrozby a určit jejich prioritu,
3. Upravit ochranu systémů.

V prvotní fázi vyhodnocování je vhodné vybrat jednu konkrétní techniku a provést příslušné kroky pro hodnocení. Pokud bude technika vhodně pokryta přecházíme plynule na přidání dalších odpovídajících technik a jejich posuzování. V opačném případě musí definovaná obrana projít úpravami a novým posouzením. Pro další a efektivnější zpracování, můžeme použít již zpracované analýzy a také nástroje jako například ATT&CK Navigator. Díky Navigatoru můžeme přehledně evidovat výsledky v matici a určit prioritu pokrytí jednotlivých technik pomocí teplotní mapy.

S hodnocením může být spojeno i posouzení centrálního bodu bezpečnosti (SOC), který může být kritickou součástí mnoha organizací. SOC se zaměřuje na nepřetržité monitorování, zajišťování i řízení bezpečnostních událostí a incidentů s cílem minimalizovat škody a reakční dobu. Rámec ATT&CK můžeme využít jako jeden z nástrojů pro zhodnocení, efektivity SOC při detekci, analýze a reakci na narušení. Obdobně jako u hodnocení ochrany a následném definování slabých míst je hodnocení centrálního bodu zejména z pohledu rychlosti řešení jedním z důležitých bodů zabezpečení. Nesmíme opomenout, že kybernetická bezpečnost je nekonečný proces a protivníci vytvářejí nové techniky, proto je důležité kromě rychlosti vyřešení incidentu mít i aktuální formy pro reakci. [25][45]

6 Definice taktik a technik pro platformy Windows a Linux

Po představení kompletní struktury znalostní báze a jejího využití lze přejít na výběr relevantních taktik a technik pro vybrané platformy Windows a Linux. Matice ATT&CK u obou platforem čítá 12 možných taktik a více než 100 technik a sub-technik. I když jsou techniky obsažené v rámci jednotlivé platformy, jejich cíle se mnohdy liší. Některé více zkoumají systémovou část a další se více specializují na napadení samotných aplikací. Z tohoto důvodu je v první fázi vhodné zvolit okruh, na který se je třeba při výběru změřit.

V případě této diplomové práce se jedná o definici technik, které útočníci využívají pro napadení základních systémových funkcionalit obou platforem. V praxi se jedná o jednotky využívané pro koncové uživatelské stanice nebo v případě serverových zařízení jako podklad pro instalaci služeb a aplikací v rámci modelového firemního prostředí. Další z faktorů napomáhající k relevantnímu výběru představují informace a data. Z tohoto pohledu nelze využít nashromážděných událostí již běžících systémů, neboť se pracuje s prostředím, které nebylo nikdy v reálném provozu. Naopak je záměrem vybrat formy napadení, které mohou být dopředu ošetřeny v rámci základního nastavení systému. Pro úspěšný výběr v případě absence interních zdrojů je vhodné najít a analyzovat dostupné externí zdroje. Proto byl autorem proveden průzkum, ze kterého pro výběr technik zvolil následující externí zdroje:

- zpráva NÚKIB o bezpečnostních hrozbách [46],
- výroční zprávy o stavu kybernetické bezpečnosti od agentury Evropské unie pro kybernetickou bezpečnost ENISA [47],
- report ohledně trendů v rámci používaných útoků od oborníků na bezpečnost společnosti FireEye [48],
- zpráva o detekci hrozeb od organizace Red Canary, která poskytuje detekci hrozeb pro organizace a využívá bázi MITRE ATT&CK [49].

Za pomoci informací z těchto zdrojů, konzultací s lidmi z praxe a autorovými praktickými zkušenostmi zvolil a zmapoval taktiky a techniky v nástroji ATT&CK Navigator. Kompletní výběr s doplňujícími informacemi ohledně postupu je představují následující kapitoly.

Initial Access

Z cílů taktiky počátečního přístupu shrnutých v kapitole 5.2.1 vyplývá, nutnost zohlednění techniky využívající možné slabiny pro přístup do systému. Mezi tyto slabiny patří například standardní služby jako SMB, SSH a další, které mají otevřené sockety pro připojení z internetu. Jednu z dalších možných hrozeb představují externí média obsahující škodlivý program, který může být spuštěn uživatelem nebo v případě návaznosti na jinou z technik automaticky po vložení. Poslední z řešených problémů s cílem přístupu zahrnuje neošetřené lokální a přednastavené účty. Autor zvolil z těchto důvodů vybrány techniky a dílčí techniky obsažené v tabulce č.1. 79[29]

TA0001 - Initial Access

T1190 - Exploit Public-Facing Application
T1133 - External Remote Services
T1091 - Replication Through Removable Media
T1078 - Valid Accounts
T1078.001 - Default Accounts
T1078.003 - Local Accounts

Legenda: Linux | Windows | obě platformy

Tabulka 1 - Zvolené techniky pro taktiku Initial Access
Zdroj: [29]

Execution

V této kategorii jsou zvoleny zejména nástroje, které umožňují provádět příkazy, spouštět skripty nebo jiné binární soubory. Tato rozhraní jsou společným rysem pro obě platformy, neboť jsou přímou součástí systému. Mezi vybranými technikami, tak nalezneme zneužívání standardních interpretů jako je Windows Command Shell nebo PowerShell, který při průzkumu patřil mezi jednu z nejvyužívanějších technik. I další vybrané formy útoku zneužívají již vestavěné funkce. Plánovače úloh jsou jednou ze základních funkcionalit Windows i Linux a poskytují protivníkovi nástroje k jednotlivému nebo opětovnému spuštění škodlivého kódu. Mezi dílčími technikami, tak figurují například programy At, Cron nebo Task Scheduler. Nutno podotknout, že zvolené techniky jsou ve většině případů navázány na ostatní taktiky jako například Intial Access nebo Privilege Escalation. Výběr zobrazuje tabulka č.2. [29]

TA0002 - Execution

T1059 - Command and Scripting Interpreter	T1053.003 - Cron
T1059.001 - Powershell	T1053.004 - Scheduled Task
T1059.003 - Windows Command Shell	T1569 - System Service
T1053 - Scheduled Task/Job	T1569.001 - Service Execution
T1053.001 - At (Linux)	

Legenda: Linux | Windows | obě platformy

Tabulka 2 - Zvolené techniky pro taktiku Execution
Zdroj: [29]

Persistence

Persistence se soustředí na zachování přístupu k systémům jakoukoliv formou. Vybrané techniky se z velké části zaměřují na konfiguraci v oblasti účtů a služeb. Vytváření účtů, úpravou jejich konfigurace nebo dalších zásad mohou útočníci zneužít pro trvalé spojení se systémy. Obdobnou kompromitaci představují úpravy procesů a služeb na úrovni systému. Tyto služby běží na pozadí a umožňují opakovaně spouštět škodlivé akce protivníka. Některé z technik jsou používány napříč více taktikami, proto výběr zahrnuje automaticky i ty z předešlých kategorii zde konkrétně z Intial Access. [29]

TA0003 - Persistence

T1098 - Account Manipulation	T1542 - Pre-OS Boot
T1098.001 - SSH Authorized Keys	T1053 - Scheduled Task/Job
T1136 - Create Account	T1053.001 - At (Linux)
T1136.002 - Local Account	T1053.003 - Cron
T1543 - Create or Modify System Process	T1053.004 - Scheduled Task
T1543.002 - Systemd Service	T1078 - Valid Accounts
T1543.003 - Windows Service	T1078.001 - Default Accounts
T1133 - External Remote Services	T1078.003 - Local Accounts

Legenda: Linux | Windows | obě platformy

Tabulka 3 - Zvolené techniky pro taktiku Persistence
Zdroj: [29]

Privilege Escalation

Zisk vyšších oprávnění umožňuje útočníkovi vykonávat další taktiky a dopad do systému může mít fatální následky. Vybrané techniky poukazují na obcházení mechanismů jako UAC nebo sudo, které zařizují eskalaci oprávnění. Tyto techniky jsou dále doplněny o některé z dalších taktik, neboť vyšší oprávnění je často potřeba pro jejich vykonání. [29]

TA0004 - Privilege Escalation	
T1548 - Abuse Elevation Control Mechanism	T1053 - Scheduled Task/Job
T1548.002 - Bypass User Account Control	T1053.001 - At (Linux)
T1548.003 - Sudo and Sudo Caching	T1053.003 - Cron
T1543 - Create or Modify System Process	T1053.004 - Scheduled Task
T1543.002 - Systemd Service	T1078 - Valid Accounts
T1543.003 - Windows Service	T1078.001 - Default Accounts
T1068 - Exploitation for Privilege Escalation	T1078.003 - Local Accounts

Legenda: Linux | Windows | obě platformy

Tabulka 4 - Zvolené techniky pro taktiku Privilege Escalation
Zdroj: [29]

Defense Evasion

Kategorie disponující technikami, které útočník používá pro maskování svých akcí patří mezi nejrozsáhlejší v matici. Mezi prvními z vybraných nalezneme vcelku standardní operace s oprávněními u složek a souborů, čímž se lze vyhnout seznamům s řízeným přístupem. Následují techniky, které se zaměřují na kompletní nebo částečnou deaktivaci obranných mechanismů jako například firewally nebo antivirové programy. Výběr zakončuje forma útoku, která se specifikuje na zcizení validních autentizačních materiálů, díky kterým mohou být obejity běžné kontroly přístupu v systému. Přehled všech technik zobrazuje tabulka č.5. [29]

TA0005 - Defense Evasion	
T1548 - Abuse Elevation Control Mechanism	T1562.004 - Disable or Modify System Firewall
T1548.002 - Bypass User Account Control	T1112 - Modify Registry
T1548.003 - Sudo and Sudo Caching	T1542 - Pre-OS Boot
T1222 - Files and Directory Permissions Modification	T1550 - Use Alternate Authentication Material
T1222.001 - Windows File and Directory Permissions Modification	T1550.002 - Pass the Hash
T1222.002 - Linux and Mac File and Directory Permissions Modification	T1078 - Valid Accounts
T1562 - Impair Defenses	T1078.001 - Default Accounts
T1562.001 - Disable or Modify tools	T1078.003 - Local Accounts

Legenda: Linux | Windows | obě platformy

Tabulka 5 - Zvolené techniky pro taktiku Defense Evasion
Zdroj: [29]

Credential Access

Krádež přihlašovacích údajů v podobě hesla a názvu účtu figuruje mezi nejznámějšími formami útoku. Z nabídky matice ATT&CK jsou zvoleny techniky, které spadají mezi často používané. První je klasická forma útoku hrubou silou, kdy dochází k hádání hesla bez předchozí znalosti například formou slovníku. Druhá metoda

v podobě dumpingu je již sofistikovanější, ale její záměr je stejný jako v prvním případě. Bližší specifikaci doplňují zvolené dílčí techniky, například v podobě operací s pamětí procesu LSASS na platformě Windows. Při výběru byl zohledněn i hojně využívaný nástroj na dumping Mimikatz. [29]

TA0006 - Credential Access
T1110 - Brutal Force
T1003 - OS Credential Dumping
T1003.001 - LSASS Memory
T1078.008 - /etc/passwd and /etc/shadow

Legenda: Linux | Windows | obě platformy

Tabulka 6 - Zvolené techniky pro taktiku Credential Access
Zdroj: [29]

Discovery

Průzkum v oblasti systémů může útočníkům poskytnout doplňující informace, díky kterým zvolí další postupy. Navržené techniky se zabývají objevováním dostupných účtu na systému, zejména těch lokálních. Další techniky se zabývají skenováním běžících služeb a jejich síťových portů nebo získáním informací o sdílených síťových jednotkách. [29]

TA0007 - Discovery
T1087 - Account Discovery
T1087.001 - Local Account
T1046 - Network Service Scanning
T1135 - Network Share Discovery

Legenda: Linux | Windows | obě platformy

Tabulka 7 - Zvolené techniky pro taktiku Discovery
Zdroj: [29]

Lateral Movement

I zde se nachází již velký podíl vybraných technik z předchozích taktik. Tento seznam je rozšířen hlavně o nástroje umožňující vzdálený přístup do systému. Z tohoto důvodu je výběr znázorněný v tabulce č.8 zacílen na služby jako vzdálená plocha, sdílení přes protokol SMB nebo standardní přístup přes SSH. [29]

TA0008 - Lateral Movement

T1210 - Exploitation of Remote Services	T1021.006 - Windows Remote Management
T1021 - Remote Services	T1091 - Replication Through Removable Media
T1021.001 - Remote Desktop Protocol	T1550 - Use Alternate Authentication Material
T1021.002 - SMB/Windows Admin Shares	T1550.002 - Pass the Hash
T1021.004 - SSH	

Legenda: Linux | Windows | obě platformy

Tabulka 8 - Zvolené techniky pro taktiku Lateral Movement
Zdroj: [29]

Command and Control

Útočníci při napadení a řízení systémů používají pro komunikaci po síti různé síťové protokoly, které jim v jisté míře mohou poskytnout maskování v rámci běžného síťového provozu. Proto je vhodné zabývat se protokoly aplikační vrstvy jako například RDP, SMB a další, ale samozřejmě i těch z nižších vrstev. Stejný případ představují i síťové porty, hlavně ty, které se standardně nevyužívají. [29]

TA0011 - Command and Control

T1071 - Application Layer Protocol
T1095 - Non-Application Layer Protocol
T1571 - Non-Standard Port

Legenda: Linux | Windows | obě platformy

Tabulka 9 - Zvolené techniky pro taktiku Command and Control
Zdroj: [29]

Impact

U poslední ze zvolených taktik v podobě dopadu jsou obsaženy techniky související s negativním dopadem na data a služby. Manipulací s daty může dojít k jejich smazání, ovlivnění případně ukrytí útočníkova chování. Závažný dopad představuje také špatná manipulace se službou sloužící k obnově systému, ať už jde o smazání záloh nebo její úplné deaktivaci. Zastavení této služby, ale i dalších kritických pro systém představuje výrazný problém. [29]

TA0040 - Impact

T1565 - Data Manipulation	T1490 - Inhibit System Recovery
T1561 - Disk Wipe	T1489 - Service Stop

Legenda: Linux | Windows | obě platformy

Tabulka 10 - Zvolené techniky pro taktiku Impact
Zdroj: [29]

7 Praktická část

Jak již bylo nastíněno v teoretické části, řízení kybernetické bezpečnosti je nekonečný cyklus a ve většině případů nelze zcela zabránit útočníkům v provedení útoku. Je ovšem důležité jim cestu proniknutí do systémů co nejvíce ztížit a případně je od škodlivé akce odradit. V návaznosti na provedenou analýzu a výběr technik se praktická část zaměřuje na návrh možných forem zabezpečení, které mají za úkol zmírnit dopad v případě použití dané techniky. Vzhledem k prolínání zmírňujících forem u jednotlivých technik, dochází pro zpracování tohoto úkolu k jejich rozřazení do oblastí jejich působení. U každé ze zkoumaných kategorií lze provést detailnější rozbor a navrhnout nejvhodnější formu mitigace. Konečná podoba řešení zahrnuje seznámení s implementačními kroky a aplikaci na vytvořeném modelovém prostředí. Výchozím zdrojem pro návrh řešení jsou jednotlivé metody zmírnění dopadu uvedené u každé techniky v rámci MITRE ATT&CK.

7.1 Charakteristika prostředí

Diplomová práce je zaměřena na platformy Windows a Linux, proto její vypracování zahrnuje vytvoření testovacího prostředí v podobě dvou virtuálních strojů. Obsazení za platformu výrobce Microsoft zastupuje operační systém Windows Server 2019, naproti tomu figuruje linuxová distribuce Ubuntu Server 20.04. Oba systémy jsou použity v serverové verzi, která je vhodnější jako zmíněný podklad pro instalaci dalších služeb, které by mohla případná firma používat. Nicméně provedené konfigurace jsou platné i na téměř všechny klasické klientské verze systémů. Oba systémy jsou ponechány ve výchozí konfiguraci, která se naskytne po jejich instalaci. Z pohledu firemního prostředí by bylo možné instalovat například doménovou službu, ovšem tyto služby nejsou předmětem zpracování diplomové práce, a proto je autor v prostředí nezahrnuje.

7.2 Řešené oblasti zvolených technik

Před zpracováním jednotlivých technik je vhodné připomenout fakt, že techniky se v matici mohou opakovat v rámci různých taktik. Způsob zpracování mitigace, ovšem zůstává stejný. Obdobné řešení se ale může vyskytnout i u více technik zároveň, neboť jejich princip útoku může mít podobné rysy.

7.2.1 Inicializace systému

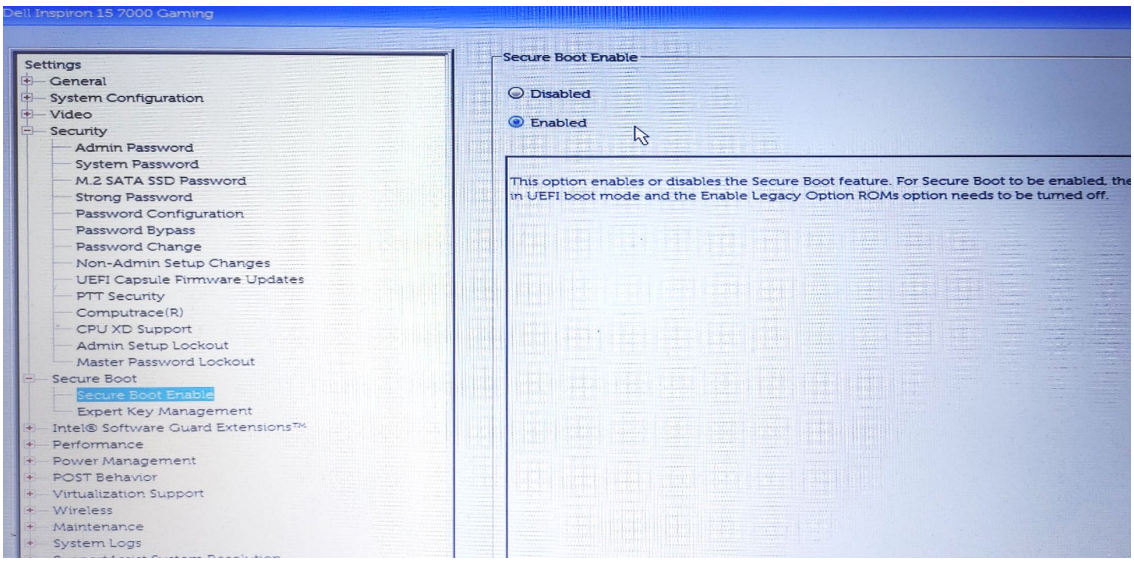
První kategorie zkoumá techniku **T1542 Pre-OS Boot** směřující na mechanismy, které se zabývají zavedením a startem operačního systému. Cílem této techniky je kompromitace dat samotného systému nebo dalších obslužných programů například v podobě ovladačů. Z pohledu rámce ATT&CK se na tuto techniku vztahuje mitigace s označením **M1046 Boot Integrity**, která vyzývá k využití zabezpečených metod pro bootování systému a ověření integrity operačního systému a zaváděcích mechanismů.

Start počítače je obecně rozdělen do několika po sobě jdoucích kroků, a právě některé z nich podléhají riziku kompromitace útočníkem. Po základních POST testech hardwarových komponent je spuštěno rozhraní UEFI, které umožňuje komunikaci mezi operačním systémem a firmwarem jednotlivých hardwarových komponent. Po provedení standardních rutin souvisejících se startem rozhraní je načten i program označován jako boot loader operačního systému, který se stará o jeho načtení. Pokud při zavedení systému nejsou aplikovány žádné ochranné mechanismy, zavaděč jednoduše aktivuje jakýkoliv operační systém uložený na disku, aniž by jej ověřil. Neověřený systém představuje potenciální riziko, neboť se může jednat o útočníkem podvržený software. Úplné zajištění důvěryhodnosti operačního systému a ovladačů je velmi obtížným úkolem, existují ovšem integrované obranné mechanismy, které mohou při neoprávněných operacích pomoci.

V rámci UEFI je pro tyto účely dostupná funkce **Secure Boot**. Na základě její aplikace zobrazené na obrázku č.8 firmware prozkoumá digitální podpis zavaděče, aby se ujistil, že nedošlo k jeho kompromitaci. Pokud není shledáno žádné porušení, firmware spustí bootloader za předpokladu, že platí jedna z následujících podmínek:

- zavaděč je podepsán pomocí důvěryhodného certifikátu společnosti Microsoft,
- ručně schválený digitální podpis zavedený do databáze.

Po úspěšném načtení zavaděče přechází proces do stavu nazvaného **Trusted Boot,** ve kterém je provedena kontrola integrity jádra operačního systému v podobě ověření spouštěcích procesů, zaváděcích jednotek, spouštěcích souborů a ELAM. Pokud je integrita porušena u některé z komponent, zavaděč ji odmítne načíst. Poslední možné nebezpečí hrozí od ovladačů jiných výrobců, než je Microsoft, které mohou být ve skutečnosti škodlivým malwarem. Pro tyto případy je k dispozici antimalwarový ovladač ELAM, jež všechny ovladače porovnává s důvěryhodným seznamem před spuštěním samotného operačního systému. [50]



Obrázek 8 - Nastavení Secure Boot v prostředí UEFI na testovacím stroji
Zdroj: vlastní zpracování

S integrací TPM čipu na základní desku počítače se otevřela možnost využít nový princip bootovacího procesu označovaný jako **Measured Boot**. TPM modul umožňuje bezpečné vytváření a ukládání kryptografických klíčů, ovšem v rámci funkčnosti počítače má více způsobů využití. Obecně je však spojován se zajištěním integrity platformy. Princip ochrany integrity z pohledu Measured Boot spočívá v měření parametrů každé komponenty od firmwaru až po ovladače pomocí hashovací funkce. Výsledné logovací soubory jsou na konci řetězce ukládány do TPM modulu.

Díky tomuto principu může před spuštěním zaváděcí sekvence dojít k lokálnímu či vzdálenému porovnání hash řetězců a ověření důvěryhodnosti všech komponent. Tento

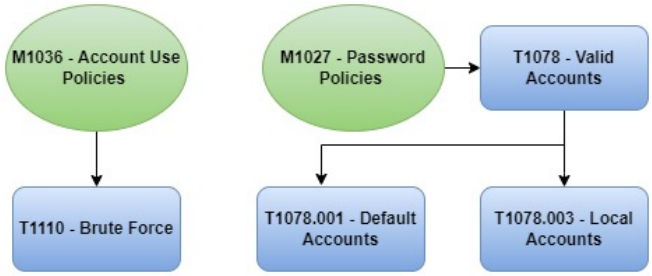
princip bootovací sekvence pomáhá identifikovat například skryté rootkit malwary v systému. [50]

Funkce zabezpečeného bootování vzhledem k využívání digitálních podpisů společnosti Microsoft představovala na počátku jejího uvedení jisté obtíže pro jednotlivé distribuce platformy Linux při jejich instalaci. Postupem času se však situace ohledně této problematiky vyjasnila a funkce Secure Boot již není pro většinu distribucí problémem. Aktivací funkce Secure Boot zmírníme dopady techniky **T1542 Pre-OS Boot** na procesy při spuštění systému. V rámci bezpečnosti je důležitý i samotný firmware UEFI opatřit komplexním heslem, aby standardní uživatel nemohl upravit jeho konfiguraci.

7.2.2 Uživatelské účty a hesla

Účet a heslo jsou základními parametry, díky kterým je umožněn přístup k systémům. Útoky cílené na prolomení těchto údajů figurují na předních příčkách a z hlediska náročnosti patří pokusy o jejich prolomení mezi ty nejzákladnější. Nejčastější používaná metoda tohoto typu napadení je označována jako brute force. Její činnost spočívá v odhadu hesla pomocí různých kombinací znaků, dokud není uhodnuta ta správná. Variantu s kombinací doplňuje i velmi častá metoda s využíváním volně dostupných databází obsahující nejčastěji používaná hesla.

Kromě samotných hesel a jejich složitosti může v rámci těchto útoku hrát významnou roli i nastavení samotného účtu. Například nastavením prodlevy mezi přihlášením můžeme útočníka zbrzdit, případně úplně odradit. Obecnými popisy zmírnění tohoto typu útoku se ve znalostní bázi věnují mitigace **M1036 Account Use Policies** a **M1027 Password Policies.** Tyto formy budou dále rozvedeny v konkrétní řešení pro obě platformy v následující části. Schéma na obrázku č.9 doplňuje vybrané techniky, které budou řešeny v kontextu těchto forem zmírnění.



Obrázek 9 - Schéma mitigací a technik v oblasti účtů a hesel
Zdroj: vlastní zpracování

7.2.2.1 Politika uživatelských účtů

Před konfigurací určitých zásad pro používání účtů je z pohledu zabezpečení vhodné zabývat se i existencí účtů samotných. Po čisté instalaci systémů jsou v rámci jejich nativní konfigurace již některé účty vytvořené. V operačním systému Windows jsou jimi například Administrator nebo Guest a na platformě Linux se jedná o standardně známý účet root. Tyto účty představují v případě jejich zmocnění útočníkem reálnou hrozbu. Zejména pokud dojde ke kompromitaci těch administrátorských, neboť ty mají k dispozici nejvyšší privilegia v rámci systému. Obecně pro jejich veřejnou známost je proto vhodné tyto účty zakázat. V případě, že systém není například připojený k spravující doméně je důležité před tímto krokem zhotovit nové administrátorské účty, tak aby byl zachován nejvyšší možný přístup k systému.

Po vytvoření potřebných účtů lze přejít na konfiguraci zásad, které mohou značně zpomalit provedení zvolených technik. Vzhledem k povaze útoků jako brute force nebo DoS se nabízí konfigurace omezující počet zadání nevalidních hesel. Po překročení limitu je účet zablokován na definovaný časový interval nebo natrvalo. Jednou z dalších možných zásad, která může být vhodná k aplikaci je interval pro přihlášení uživatele. V principu se jedná o časový rámec, kdy může uživatel daný počítač používat. Na první pohled se toto pravidlo zdá být více restriktivní, ovšem jeho uplatnění může mít negativní dopad na případný útok.

Pro konfiguraci výše zmíněných zásad a postupů jsou na platformě Windows využity nástroje PowerShell a standardní editor pro skupinové politiky GPO. Prvním krokem je založení nového uživatele s přiřazením do skupiny s nejvyššími právy dle následujících PowerShell příkazů:

```
#Proměnná account a password  pro zadání jména a hesla pro uživatele
$account  = Read-Host
$password = Read-Host -AsSecureString

#Založení uživatele
New-LocalUser $account -Password $password -FullName "Ondrej Danis" -
Description "Local admin account"

#Přidání nového uživatele do skupiny Administrators
Add-LocalGroupMember -Group "Administrators" -Member $account
```

Blokaci nativních uživatelů lze provést více způsoby, nejsofistikovanější metoda je využití lokálních politik. Tuto formu konfigurace využijeme i pro zásady v oblasti zamykání uživatele. Editor politik lze jednoduše spustit přes spouštěcí okno zadáním příkaz **gpedit.msc.** Zásady potřebné pro zvolenou kategorii se nachází v rámci

bezpečnostních nastavení **Account Policies** a **Local Policies** umístěných v následující cestě **Computer Configuration\Windows Settings\Security Settings.** Aplikovanou konfiguraci pravidel v rámci testovacího prostředí představuje tabulka č.11.

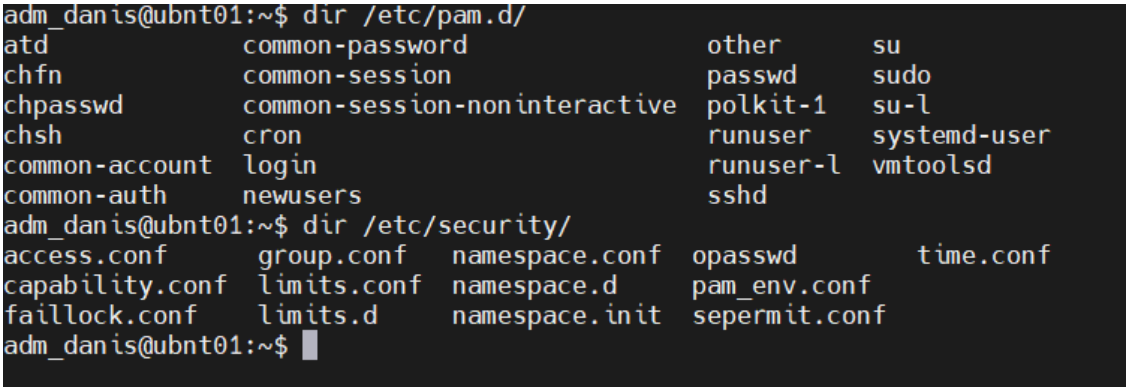
Local Settings\Security options		
Politika	**Nastavení**	**Informace**
Accounts: Administrator account status	Disabled	Zablokování nativního účtu Administrator
Accounts: Block Microsoft accounts	Users can't add Microsoft accounts	Zablokování přidávání účtů Microsoft
Accounts: Guest account status	Disabled	Zablokování nativního účtu Guest
Account Policies\Account Lockout Policy		
Politika	**Nastavení**	**Informace**
Account lockout duration	15 minutes	Časový interval blokace uživatele v případě překročení hranice pro špatně zadané heslo
Account lockout threshold	5 invalid logon attempts	Hranice špatně zadaného hesla, po které dojde k zablokování účtu
Reset account lockout counter after	15 minutes	Časový interval pro vynulování neúspěšných pokusů o přihlášení

Tabulka 11 - Politiky pro zabezpečení účtů na platformě Windows
Zdroj: vlastní zpracování

Obdobná konfigurace je aplikována také na platformě Linux. Vzhledem k odlišnosti mezi platformami je však provedení jednotlivých kroků rozdílné. Již při instalaci operačního systému vzniká nový uživatelský účet, který je zařazen do skupiny s možností využití provedení příkazu s vyššími právy pomocí příkazu **sudo**. Na rozdíl od platformy Windows je zde obdoba správcovského účtu s označením **root** nativně vypnuta. Hlavní myšlenka tohoto přístupu spočívá ve využívání vyšších oprávnění pouze v případech, kdy jsou nezbytné. Samozřejmě účet root lze kdykoliv aktivovat i deaktivovat. Obecně se tato varianta z bezpečnostního hlediska nedoporučuje, pokud k tomu nejsou dostatečné důvody.

K řízení a nastavení zásad pro uživatelské účty je využita sada knihoven PAM umožňující konfiguraci jednotlivých fází autentizačních kroků. Před manipulací s tímto nástrojem je vhodné důkladně prostudovat jeho dokumentaci, neboť v případě nevhodně umístěných pravidel, může být ohrožena některá z funkcionalit systému. Základní struktura PAM je umístěna v adresáři **/etc/pam.d/**, kde se nachází konfigurační soubory pro aplikace a služby, které tento nástroj podporují.

Důležitým adresářem pro nastavení je také **/etc/security/**, který obsahuje konfigurační soubory pro jednotlivé moduly. Přehledný výpis z těchto adresářů je zobrazený na obrázku č.10.



Obrázek 10 - Struktura konfiguračních souborů PAM
Zdroj: vlastní zpracování

Pro nastavení totožných politik pro blokaci uživatelského účtu jako na platformě Windows musí být dodány do souboru **faillock.conf** následující parametry:

- **deny = 5**
  - hranice neúspěšných pokusů o přihlášení,
- **unlock_time = 900**
  - časový interval 15 minut pro odemknutí účtu,
- **fail_interval = 300**
  - časový interval 5 minut pro naplnění hranice pokusů,
- **audit**
  - zapnutí logování událostí do systémového logu, pokud uživatelský účet není v systému nalezen,
- **silent**
  - vypnutí vypisování informačních zpráv o počtu pokusů.

Finální úprava konfigurace pro zajištění funkce blokace uživatele se musí provést v konfiguračním souboru **login,** kde musí dojít k doplnění autentizační služby a provázáním s výše uvedeným modulem faillock. Upravený soubor login s popisem doplněné funkcionality zobrazuje následující výpis.

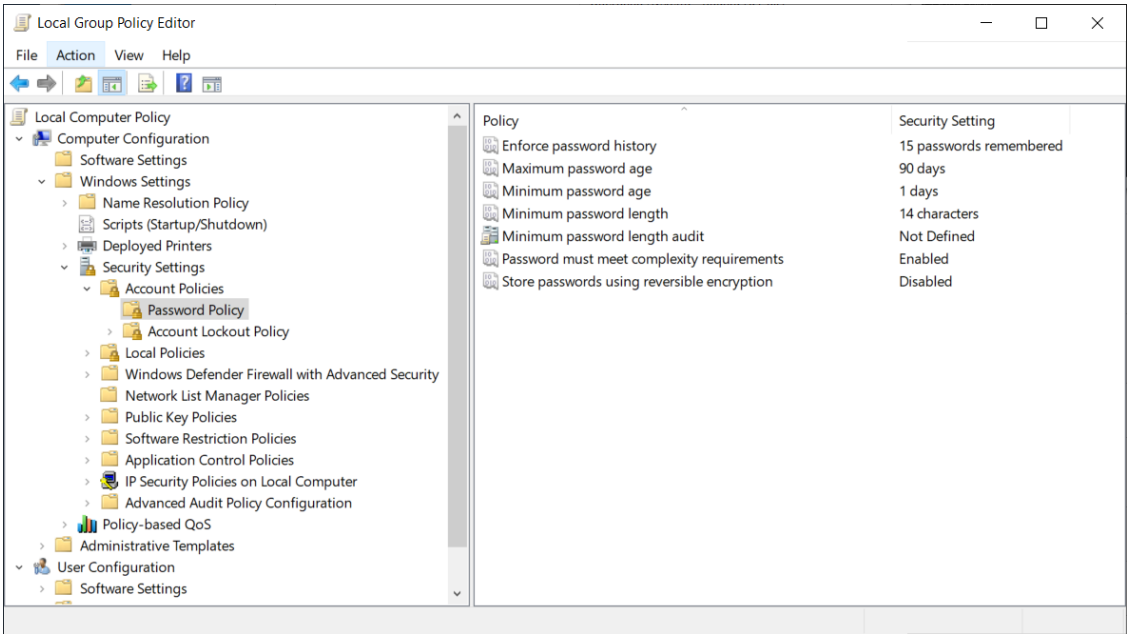
```
auth      optional   pam_faildelay.so  delay=3000000
auth      requisite  pam_nologin.so
#Vložená konfigurace
auth      required   pam_faillock.so # použití modulu pro kontrolu autentizace
auth      sufficient pam_unix.so #ověření hesla, pokud úspěšně ověří heslo ukončí proces
auth      [default=die]   pam_faillock.so authfail # vrácení chyby o selhání
auth      required        pam_deny.so # ukončení autentizace, pokud dojde k jejímu selhání
account   required        pam_faillock.so #použití modulu pro ověření uživatele
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so close
….
```

7.2.2.2 Politika hesel

Neexistuje žádné ustanovení, které by přesně specifikovalo, jaké parametry má obsahovat komplexní heslo a obecně politika řízení hesel. Názory na tyto parametry se často liší i mezi odbornými organizacemi, a proto se spíše jedná o individuálním uvážení jednotlivých administrátorů. Dostatečná síla hesla se odvíjí od počtu znaků, použití malých i velkých písmen, číslic a speciálních znaků. Je ovšem vcelku složitým úkolem propojit všechna tato kritéria, tak aby heslo vyhovovalo uživatelům systému například z pohledu délky a zároveň splnilo kritéria pro označení silného hesla. Další skloňované politiky se zaměřují na délku platnosti hesla nebo počet neopakujících se hesel. Po uvážení všech kritérii jsou na základě různých doporučení a autorovy zkušenosti z praxe stanoveny následující parametry:

- **Minimální délka hesla** - 14 znaků
- **Minimální stáří hesla** – 1 den
- **Maximální stáří hesla** – 90 dní
- **Obsahuje alespoň tři z následujících kategorií:**
  - Malá písmena (a - z)
  - Velká písmena (A - Z)
  - Obsahuje číslice 1 až 9
  - Speciální znaky (+, -, !, *, #)
- **Historie použitých hesel** - 15

Konfigurace na platformě Windows je opět zajištěna pomocí editace GPO politik, které jsou umístěny v následující cestě **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**. Výčet a nastavení jednotlivých politik zobrazuje obrázek č.11.



Obrázek 11 - Nastavení politiky hesel pomocí GPO
Zdroj: vlastní zpracování

Pro nastavení politiky hesla na Linux platformě se musí provést úprava tří konfiguračních souborů. Obdobně jako v podkapitole 7.2.2.1 vstupuje do hry sada modulů PAM, požadovaný modul s označením **libpam-pwquality** ovšem není obsažen v počátečním balíku a musí nejprve dojít k jeho instalaci přes standardní rozhraní **APT**. Po přidání modulu musí být postupně upraveny následující soubory:

- **/etc/login.defs,**
- **/etc/security/pwquality.conf,**
- **/etc/pam.d/common-password.**

Úpravu a přidání potřebných parametrů popisuje podrobně tabulka č.12.

Soubor /etc/login.defs	
Parametr	**Informace**
PASS_MAX_DAYS = 90	Maximální počet dnů pro využití hesla
PASS_MIN_DAYS = 1	Minimální počet dnů před změnou hesla
PASS_WARN_AGE = 7	Počet dnů pro upozornění před vypršením platnosti hesla
Soubor /etc/security/pwquality.conf	
Parametr	**Informace**
difok = 2	Počet znaků nového hesla, které nesmí být obsaženy ve starém hesle
minlen = 14	Minimální délka hesla
minclass = 3	Minimální počet požadovaných tříd znaků (číslice, malá a velká písmena, speciální znaky)
gecoscheck = 1	Kontrola nového hesla proti obsahu řetězců nastavených v profilu uživatele (jméno, příjmení atd.)
enforce_for_root	Aplikace kvality hesla pro zadávání přes příkaz sudo
Soubor /etc/pam.d/common-password	
Parametr	**Informace**
password requisite pam_pwquality.so retry=5	Aplikace nastavených politik pro hesla (parametr je po instalaci automaticky nastaven)

Tabulka 12 - Konfigurační parametry pro politiku hesel na platformě Linux
Zdroj: vlastní zpracování

7.2.3 Oprávnění a řízení přístupu

Řada technik, které útočníci používají je závislá na vyšším oprávnění, kterým ovšem zneužitý účet nemusí disponovat. V konečném důsledku může proto oprávnění uživatelů nebo aplikací a vhodné řízení jejich přístupů ke zdrojům zastávat významnou roli v zabezpečení. I na tuto problematiku je v rámci ATT&CK upozorněno některými formami mitigace, které apelují na restriktivní opatření vztahující se na využívání uživatelských účtu při přístupu k souborům, instalaci softwaru nebo úpravě registrů. Tato kapitola je zaměřena na představení dostupných způsobů, které se využívají pro řízení přístupu na obou platformách. Formy zmírnění a zvolené techniky, které se na tuto kapitolu podle znalostní báze vztahují zobrazuje tabulka č.13.

Zmírnění	Techniky
M1018 - User Account Management	T1110, T1543, T1562, T1021, T1053, T1489, T1550, T1047, T1490
M1022 - Restrict File and Directory Permissions	T1548, T1543, T1565, T1222, T1562, T1489
M1024 - Restrict Registry Permissions	T1562, T1112, T1489
M1026 - Privileged Account Management	T1548, T1059, T1136, T1543, T1222, T1003, T1542, T1021, T1053, T1569, T1550, T1078, T1047
M1033 - Limit Software Installation	T1091
M1034 - Limit Hardware Installation	T1543
M1052 - User Account Control	T1548, T1550

Tabulka 13 - Přehled zmírnění a technik v rámci oprávnění a řízení přístupu
Zdroj: vlastní zpracování

7.2.3.1 Řízení uživatelských účtů

Platforma Windows pro řízení přístupu uživatelských účtu již řadu let využívá **User Account Control** (UAC). Tato funkcionalita byla navržena pro zvýšení celkového zabezpečení v rámci operací, které uživatelé vykonávají a pomáhá tak například zabránit malwaru v poškození počítače. Pokud je UAC aktivováno aplikace a úlohy se vždy spouští v kontextu zabezpečení daného účtu, což přináší výhodu pro řízení přístupu. UAC umožňuje všem vytvořeným uživatelům přihlásit se k počítači pomocí standardního uživatelského účtu. Procesy spuštěné přes tento účet mohou provádět jen úkony na základě přidělených přístupových práv.

Většina aplikací, včetně těch, které jsou součástí samotného operačního systému, jsou proto navrženy, aby fungovaly správně v tomto režimu. V systému se vyskytují ovšem i funkcionality vyžadující vyšší oprávnění. Zejména jde o systémové aplikace, které mají dopad na celkový chod systému a zabezpečení. Pokud pak daný účet není správcem nebo jím není pověřen pro vykonání, nelze požadovanou akci provést. V praxi to znamená, že standardní uživatel není oprávněn provádět změny systémových funkcionalit, jako je například nastavení registrů, firewall brány a další.

Pokud aplikace potřebuje pro svůj chod vyšší oprávnění, kterým nedisponuje standardní uživatelský kontext, UAC umožňuje uživatelům spouštět aplikace s tokenem správce namísto jejich výchozího standardního uživatelského přístupového tokenu. Princip tohoto přístupu umožňuje zachovat většinu provedených operací ve standardním kontextu zabezpečení uživatelů, přičemž v případě potřeby umožní spuštění určitých aplikací se zvýšenými oprávněními. S aplikací vyšších oprávnění musí správci aktivně souhlasit nebo poskytnout přihlašovací údaje pro každý administrativní proces, čímž mají zároveň nad těmito procesy i určitou kontrolu. [51]

Základní konfiguraci UAC představují tyto možné míry řízení:

1. **Nikdy neupozorňovat**
    - Úplné vypnutí UAC,
2. **Informovat pouze v případě že se programy pokusí provést změny v počítači**
    - Upozorní pouze, že je snaha o pokus instalovat software nebo změnu v počítači, ale nepozastaví ostatní úlohy,
3. **Upozornit pouze pokud se programy pokusí provést změny v počítači**
    - Upozorní o pokusu instalovat software nebo změny v počítači a pozastaví ostatní úlohy. Neupozorňuje pouze při nastavení systému,
4. **Vždy upozornit**
    - Upozorňuje při každé akci.

Po výchozí instalaci operačního systému je UAC aktivováno a nastaveno na režim číslo tři. K finální podobě nastavení musí být provedena ještě kontrola a některé úpravy v rámci GPO politik. Tyto politiky se v editoru nachází v umístění **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options** a potřebné nastavení symbolizuje přehled v tabulce č.14.

Politika	Nastavení	Informace
Use Admin Approval Mode for the built-in Administrator account	Enabled	Schvalování pro nativní účet Administrator (pokud nedojde k zablokování)
Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled	Schvalování přes zabezpečenou plochu pro UI aplikace i při vzdáleném přístupu
Behavior of the elevation prompt for standard users	Automatically deny elevation	Schvalování vyššího oprávnění pro standardní účty bude automaticky odmítnuto
Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent on the secure desktop.	Schvalování na zabezpečené ploše, která chrání před falšováním vstupů a výstupů
Detect application installations and prompt for elevation	Enabled	Detekce instalace aplikace
Only elevate executable files that are signed and validated	Enabled	Časový interval pro vynulování neúspěšných pokusů o přihlášení
Only elevate UIAccess applications that are installed in secure locations	Enabled	Aplikace s UI musí být umístěna v bezpečném místě v systému souborů
Turn on Admin Approval Mode	Enabled	Zapnutí UAC
Switch to the secure desktop when prompting for elevation	Enabled	Přepnutí na zabezpečenou plochu pro výzvu k zvýšení oprávnění
Virtualize file and registry write failures to per-user locations	Enabled	Řízení zápisu při selhání aplikace na určitá místa

Tabulka 14 - Nastavení GPO politik pro UAC
Zdroj: vlastní zpracování

Obdobou UAC v linuxovém prostředí je využívání příkazu **sudo** zmíněného v kapitole 7.2.2 o uživatelských účtech, případně příkazu **su** (switch user)**.** Oba příkazy umožní uživateli provést akci s vyšším oprávněním, ale jejich princip je odlišný. V případě příkazu **sudo** je vykonán pouze daný příkaz s vyšším oprávněním, ale kontext uživatele zůstává ve standardním režimu. U příkazu **su „user“** (root = nejvyšší oprávnění) dochází k přihlášení terminálu pod jiným účtem a dochází k trvalému přístupu k nejvyšším oprávněním, pokud se přepneme do kontextu uživatele root. Kromě tohoto zásadního rozdílu je třeba doplnit fakt, že pro přepnutí kontextu uživatele je nutné znát i jeho heslo. V návaznosti na zmíněnou kapitolu o uživatelských účtech, nebyl uživatel root aktivován, a proto je dále spíše cíleno na příkaz **sudo**.

Aby mohl daný uživatel použít příkaz pro zvýšení svých oprávnění musí být zařazen konfiguračním souboru **/etc/sudoers** nebo figurovat ve skupině sudo, případně jiné skupině již přidané v tomto souboru. Používání tohoto příkazu spočívá v jeho přidání před požadovanou operaci. Před vykonáním akce musí volající uživatel zadat své heslo, čím se ověří podmínky pro využití suda. Úspěšným ověřením získává daný uživatel vyšší práva na nativně nastavený interval 15 minut, což je možné vnímat jako určité bezpečnostní riziko. Tento parametr lze ovšem přenastavit v zmíněném konfiguračním souboru. Operace a patřičná nastavení zobrazuje následující výčet.

Soubor /etc/sudoers

```
Defaults        env_reset, timestamp_timeout=0 # parametr pro časový interval platnosti oprávnění
Defaults        mail_badpass
Defaults   secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
# User privilege specification
root    ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

7.2.3.2 Oprávnění pro soubory a složky

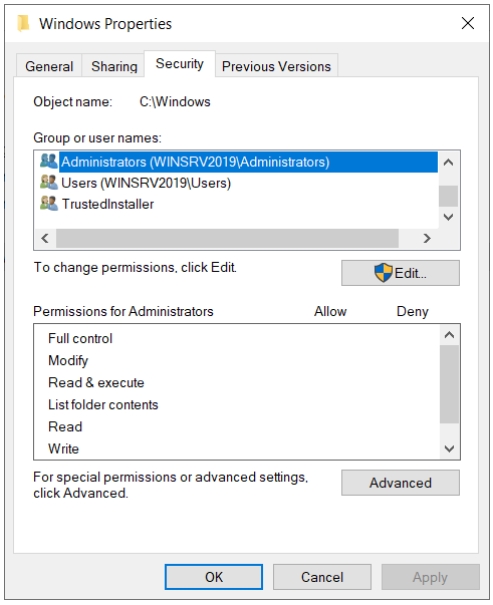
Udělení přístupu k určitým složkám a souborům u standardních uživatelů může být jednou z bezpečnostních mezer v rámci nastavení systémů. Zpravidla se jedná o systémové složky a soubory, které by měli mít pod správou pouze administrátor nebo účet systémové služby. Z pohledu standardního účtu to nemusí znamenat úplný zákaz přístupu, ale jen omezení práv na pouhé čtení, které je ovšem důležité pro chod služby

nebo obecně systému. U obou platforem je samozřejmostí udělovat na složky i soubory základní trojici oprávnění v podobě **čtení, zápisu a exekuce**. Řízení přístupu je i díky strukturalizované možnosti rozřazení uživatelů do určitých skupin vcelku variabilní záležitostí.

Operační systém Windows má aplikovaná základní oprávnění na systémové složky již po své instalaci. Pro základní kontrolu si lze ověřit oprávnění zejména u složek nacházejících se v kořenové složce C:

- C:\Windows,
- C:\Program Files,
- C:\ProgramData,
- C:\Users\%USERPROFILE%\AppData,
- C:\Windows\SysWOW64 – pro 64-bit verzi OS,
- C:\Windows\System32 – pro 32-bit verzi OS.

Tyto složky jsou pro standardního uživatele dostupné pouze pro čtení. V případě potřeby dodání jednotlivých práv pro uživatele nebo skupinu lze využít přehledné GUI zobrazené na obrázku č.12, které je dostupné přes vlastnosti v záložce **Security** dané složky nebo souboru.



Obrázek 12 - Přidání oprávnění na složku v prostředí Windows
Zdroj: vlastní zpracování

I na linuxové platformě se v rámci instalace implementují patřičná oprávnění. Ačkoliv jsou ve výchozím nastavení oprávnění aplikována, může dojít k jejich změně neúmyslně nebo škodlivým jednáním. Konkrétně je důležité se změřit na tyto kritické soubory:

- **/etc/passwd a /etc/passwd- -** soubor a záložní soubor s informacemi o uživatelích
- **/etc/group a /etc/group- -** soubor a záložní soubor s definicí skupin uživatelů
- **/etc/shadow a /etc/shadow- -** soubor a záložní soubor s informacemi o heslech pro účty
- **/etc/gshadow a /etc/gshadow- -** soubor a záložní soubor s informacemi o skupinových účtech

K těmto souborům musí mít zpravidla přístup pouze účet root, neboť v případě jejich kompromitace může dojít například k prolomení hesel jednotlivých účtů. Pokud se zaměříme na udělení práv a jiné složky nebo soubory v rámci platformy je pro tyto úkony využíván příkaz **chmod.** Způsob aplikace tohoto příkazu vysvětluje názorně následující výpis:

```
#Oprávnění read = 4, write = 2, execute = 1, finální oprávnění pomocí součtu
#Struktura chmod příkazu  chmod xyz soubor(složka), kde x=vlastník, y = skupina z= ostatní
#příklad
sudo chmod 744 priklad.txt
```

7.2.3.3 Řízení přístupu k aplikacím

Řízení účtů a oprávnění jejich přístupu k složkám a souborům zajisté reguluje značnou část možných forem zneužití. Tyto formy zmírnění dopadů v rámci zvýšení zabezpečení lze doplnit dalším způsobem v podobě řízení přístupu aplikací. Byť jsou pro chod některých akcí a aplikací potřebná vyšší oprávnění, stále existuje riziko spuštění softwarů nebo skriptů v rámci kontextu standardního uživatele. Z tohoto důvodu je vcelku podrobná kontrola nad chodem aplikací důležitým doplňkem pro bezpečnou manipulaci se systémy.

V rámci operačního systému Windows využijeme pro tuto problematiku implementovaný nástroj **AppLocker**. Princip funkčnosti je založen na definic sad

pravidel podle aspektů aplikací, které mají být kontrolovány administrátorem. Aspekty jsou hlavním kritériem, podle kterého je dané pravidlo vytvořeno a figurují mezi nimi tyto:

- **Certifikát aplikace** – při spuštění aplikace je kontrolován její digitální podpis,
- **Cesta k souboru** – aplikace je blokována na základě definované cesty k spustitelným souborům,
- **Hash souborů aplikace** – Windows nejprve vytvoří hash spustitelného souboru, který je při spuštění aplikace kontrolován.

Pravidla lze poté díky struktuře uživatelů aplikovat na vytvořené skupiny nebo konkrétní uživatele v systému. Mezi soubory, které lze pomocí AppLockeru kontrolovat spadají následující:

- Spustitelné soubory .exe a .com
- Skripty .ps, .bat, .cmd, .vbs, .js
- Instalační služby Windows .msi
- Knihovny DDL
- Archivy aplikací a instalačních souborů

Z pohledu aktivace AppLockeru musí na prostředí nejprve dojít k aktivaci služby **Application Identity**, která umožňuje ověřování identity aplikace a zároveň je kritická pro uplatnění definovaných zásad. Ve výchozím nastavení se musí tato služba spouštět manuálně, proto je vhodné provést úpravu pro automatický start například pomocí následujícího PowerShell příkazu.

```
#Změna konfigurace startování služby Application Identity
sc.exe config appidsvc start= auto
```

Samotné nastavení AppLockeru se nachází v obdobné konzoli pro správu politik a zásad využívanou v kapitole 7.2.2 na tomto umístění **Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker.** Jako vhodný startovací bod pro základní zabezpečení jsou v rámci modelovacího prostředí aplikována doporučená výchozí pravidla. Tato pravidla mohou být posléze v rámci rozvoje bezpečnosti a na základě provozu patřičně upravena. Výpis implementovaných pravidel zobrazuje tabulka č.15.

Spustitelné soubory			
Akce	**Uživatel**	**Pravidlo**	**Aspekt**
Povoleno	Everyone	All files located in the Program Files folder	Cesta k souboru
Povoleno	Everyone	All files located in the Windows folder	Cesta k souboru
Povoleno	BUILTIN\Administrators	All files	Cesta k souboru
Instalační služby systému Windows			
Akce	**Uživatel**	**Pravidlo**	**Aspekt**
Povoleno	Everyone	All digitally signed Windows Installer files	Certifikát vydavatele
Povoleno	Everyone	All Windows Installer files in %systemdrive%\Windows\Installer	Cesta k souboru
Povoleno	BUILTIN\Administrators	All Windows Installer files	Cesta k souboru
Skripty			
Akce	**Uživatel**	**Pravidlo**	**Aspekt**
Povoleno	Everyone	All scripts located in the Program Files folder	Cesta k souboru
Povoleno	Everyone	All scripts located in the Windows folder	Cesta k souboru
Povoleno	BUILTIN\Administrators	All scripts	Cesta k souboru
Zabalené aplikace			
Akce	**Uživatel**	**Pravidlo**	**Aspekt**
Povoleno	Everyone	All signed packaged apps	Vydavatel (*)

Tabulka 15 - Konfigurační pravidla pro AppLocker
Zdroj: vlastní zpracování

Na velmi podobné bázi operuje v rámci linuxové platformy software s názvem **AppArmor**. Tento systém umožňuje na základě definice profilů pro jednotlivé programy omezovat jejich práva. Program spuštěný v rámci kontextu uživatele, disponuje i jeho právy. Pomocí AppArmoru lze práva v rámci funkčnosti samotné aplikace dále omezit bez dopadnu na uživatele, který aplikaci spustil. V praxi to znamená, že pro spuštěnou aplikaci lze omezit práva například ke složkám, souborům nebo i síťovému připojení. Pomocí vhodně nastavených restrikcí, tak můžeme zvýšit bezpečnost systému v případě spouštění různých aplikací. Na druhou stranu je důležité omezení implementovat s jistou mírou ohleduplnosti ke komfortu používání aplikace ze strany uživatele.

Na distribuci Ubuntu je AppArmor integrován v rámci výchozí instalace operačního systému. Konfigurační soubory samotného softwaru jsou umístěny v adresáři **/etc/apparmor/**. Pro definici jednotlivých profilů existuje adresář **/etc/apparmor.d/**, kde také dochází k jejich rozřazení dle jejich stavu. Typy stavů jsou celkem tři:

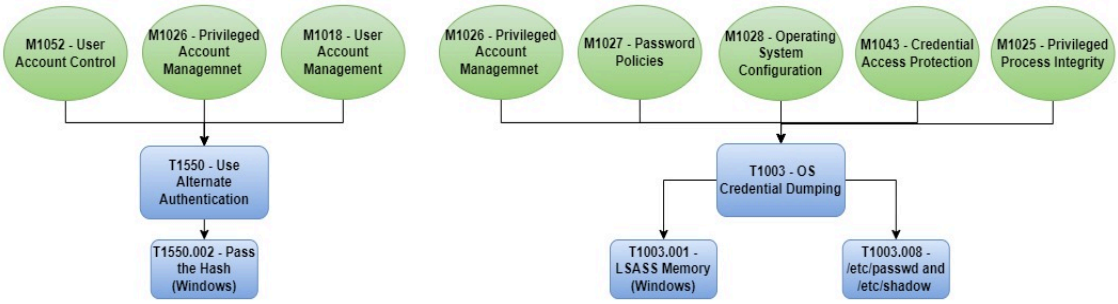
- **enforce** – profile je plně aplikovaný,
- **complain** – profil je pouze monitoruje a zapisuje do log souboru, ale neomezuje,
- **unconfined** – profil není aplikovaný.

Ve výchozím stavu jsou již integrovány i základní profily, které definují vhodnou počáteční konfiguraci. Proto z pohledu konfigurace je potřeba aplikovat pouze následující příkazy.

```
#Instalace doplňujících závislostí apparmor-utils
sudo apt-get install apparmor-utils
#Aplikace všech dostupných výchozích profilů
sudo aa-enforce /etc/apparmor.d/*
#Výpis o stavu profilů AppArrmoru
sudo aa-status
```

7.2.4 Autentizační materiály

Přihlašovací údaje jsou nejzásadnějšími parametry pro přístup a potenciální úspěšné provedení útoku. I proto útočníci hledají nedostatečně ošetřená místa v systému a vytvářejí techniky, které na tyto údaje cílí. Již v kapitole 7.2.2 o nastavení účtů a složitosti hesla byla představena technika brute force na prolomení hesla. Existují ovšem i jiné vcelku běžné útoky specializující se na krádež autentizačních údajů při jejich ukládání v systému nebo komunikaci skrze ověřovací protokoly. Je nutné zdůraznit, že při aplikaci dosud nastavených protekčních procesů by mělo těmto technikám být zabráněno, pokud se útočník ovšem nedostane k účtu s administrátorskými právy. Tuto skutečnost přitom nelze vyvrátit, a proto musí zabezpečení chápáno z celkového pohledu nikoli jen jedince. Zkoumané mitigační informace a zvolené techniky útoku z pohledu ATT&CK zobrazuje sestavené schéma na obrázku č.13.



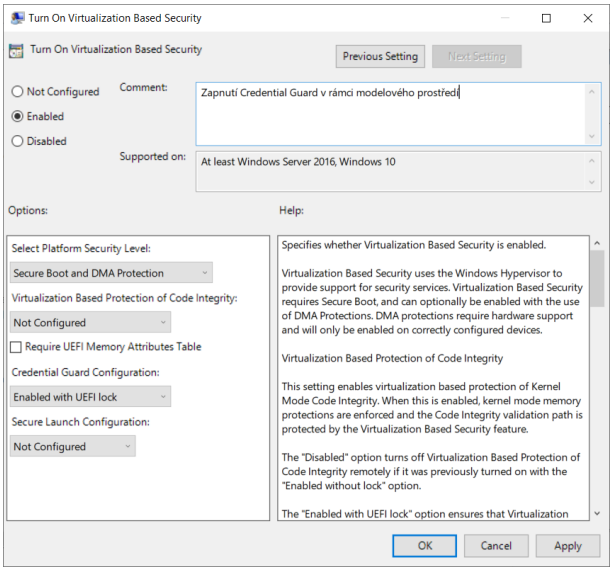
Obrázek 13 - Schéma mitigací a technik v oblasti autentizačních materiálů
Zdroj: vlastní zpracování

7.2.4.1 Paměť procesu LSASS

Autentizaci uživatelů v systému Windows zaopatřuje lokální bezpečnostní autorita LSA s integrovaným procesem LSASS, který slouží jako autentizační server. Účelem procesu LSASS je ověřování uživatelů proti lokální databázi s uloženými údaji o uživatelích SAM a ukládání autentizačních informací o uživatelích, kteří mají vytvořenou aktivní relaci k systému. V principu se jedná cache paměť obsahující informace s přihlášenými uživateli, aktivními službami, plánovanými úlohami. Kromě standardních informací účtu jsou zde umístěné i hesla v hashované podobě pro ověření účtů skrze autentizační protokoly LM, NTLM, Kerberos. Kompromitací této paměti může útočník získat ověřovací materiály všech přihlášených účtů a použít například pro přístup na další systémy v rámci organizace. [52]

Právě na základě zjištěných forem tohoto útoku jsou implementovány v rámci systému obranné mechanismy, které provedeme v rámci modelovacího prostředí. První z aplikovaných prvků představuje relativně nová funkcionalita **Credential Guard**. Princip této funkce spočívá v izolaci procesu LSA na izolovaném virtualizovaném procesu, který není přístupný pro zbytek operačního systému. V případě napadení paměti procesu LSASS, tak útočník nemůže odcizit zahashovaná hesla.

Zapnutí Credential Guardu probíhá pomocí aktivace GPO zásad z obrázku č.14 a vyžaduje aktivovaný **Secure Boot**, který je řešen v kapitole 7.2.1. Zmíněné zásady jsou dostupné v následující cestě **Computer Configuration\Administrative Templates\System\Device Guard.**



Obrázek 14 - Aktivace Credential Guardu
Zdroje: vlastní zpracování

7.2.4.2 Pass the Hash

Pass the Hash významně souvisí s předchozí kapitolou o ochraně paměti LSASS a patří mezi velmi oblíbenou techniku útočníků v kategorii laterálního pohybu. Tato technika se zaměřuje se na ukradení a zneužití zahashované podoby hesla uživatele. Na základě odcizeného hash řetězce získává útočník způsob umožňující úspěšnou autentizace vůči systému bez znalosti textové podoby hesla. K získání hashové podoby se hojně využívá například program Mimikatz, který kompromituje paměť procesu LSASS. Případně pokud je již útočník v síťové prostředí může zneužít nedostatečné zabezpečení autentizačních protokolů, zejména LM nebo NTLM a naslouchání při ověřovacím procesu hash zcizit. Velká část způsobů ochrany již byla představena, v rámci doplnění lze však uvést například vynechání nedostatečně chráněných autentizačních protokolů LM a NTLMv1. I pro tato omezení existují GPO zásady a jejich výčet představuje tabulka č.16. [52]

Local Settings\Security options		
Politika	**Nastavení**	**Informace**
Network security: Configure encryption types allowed for Kerberos	AES128_HMAC_SHA1 AES256_HMAC_SHA1 Future encryption types	Typy šifrování pro autentizační protokol Kerberos
Network security: LAN Manager authentication level	Send NTLMv2 response only\refuse LM & NTLM	Ověřování pouze pomocí NTLMv2
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security Require 128-bit encryption	Minimální zabezpečení pro relaci NTLM - klienti
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security Require 128-bit encryption	Minimální zabezpečení pro relaci NTLM - servery

Tabulka 16 - GPO pro nastavení autentizačních protokolů
Zdroj: vlastní zpracování

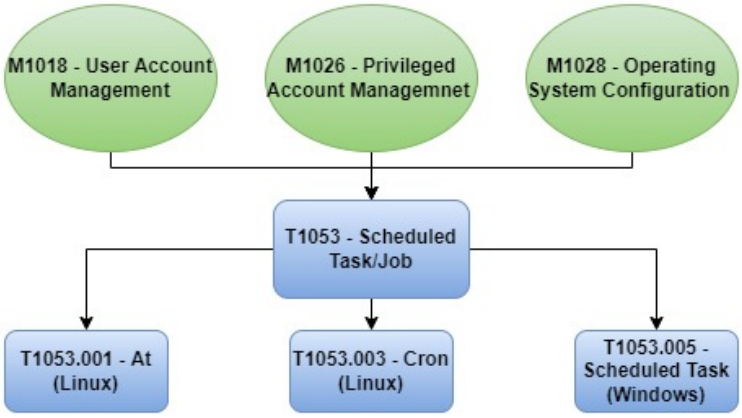
7.2.4.3 Soubory /etc/passwd a /etc/shadow

Přístup do složek /etc/passwd a /etc/shadow je z pohledu bezpečnosti přístupových údajů klíčovou záležitostí. V návaznosti na kapitolu 7.2.3 týkající se oprávnění je z pohledu linuxové platformy potřebné doplnit oprávnění pro uvedené soubory, aby nedošlo k jejich kompromitaci. Oprávnění se na základě jednotlivých souborů liší, neboť soubory **/etc/passwd** a **/etc/group** obsahují pouze informace o uživatelích, ale nikoliv jejich hesla, proto mohou být dostupné pro čtení. Naproti tomu jsou doplňující soubory s hesly v podobě **/etc/shadow** a **/etc/gshadow**, které má pod správou pouze uživatel root. Nastavení v souladu s bezpečností zobrazuje následující výpis.

```
# Nastavení vlastníka a skupiny na root u všech kritických souborů
sudo chown root:root /etc/passwd /etc/passwd- /etc/group /etc/group- /etc/shadow /etc/shadow- /etc/gshadow /etc/gshadow-
# Oprávnění pro soubory /etc/passwd, /etc/group
sudo chmod u-x,go-wx /etc/passwd /etc/passwd- /etc/group /etc/group-
# Oprávnění pro soubory /etc/shadow, /etc/gshadow
sudo chmod u-x,g-wx,o-rwx /etc/shadow /etc/shadow- /etc/gshadow /etc/gshadow-
```

7.2.5 Plánovací služby

Nástroje pro plánování úloh jsou nedílnou součástí téměř každého operačního systému, není tomu jinak ani u obou řešených platforem. Byť tato funkcionalita může ulehčit administrátorům správu jistých úkonů, útočníkům naopak poskytuje možnost pro aplikaci jejich škodlivých kódů nebo trvalý přístup k systémům. Právě z tohoto důvodu se o plánovače úloh zajímají i bezpečnostní týmy a figurují mezi technikami v bázi ATT&CK. Na základě odhalených případů této techniky jsou z pohledu báze navrženy určité formy zmírnění, které jsou z větší míry orientovány na řízení přístupu k těmto službám a obecnou konfiguraci operačního systému. Celkový přehled zúčastněných technik a mitigací zobrazuje schéma na obrázku č.15.



Obrázek 15 - Schéma mitigací a technik u plánovacích nástrojů
Zdroj: vlastní zpracování

Zabezpečení standardního Task Scheduler operujícího na systému Windows je spojeno s oprávněními standardního uživatele. V rámci předchozích nastavení v podobě UAC, oprávnění a implementovaných pravidel je uživatel schopen pro standardní plánování úloh bez možnosti využití vyšších privilegii. Existuje možnost kompletního vypnutí nástroje pro plánování, ale vzhledem k jeho užitečné funkcionalitě i pro standardní uživatele jsou aplikovaná opatření prozatím dostačující.

Z pohledu druhé platformy je variabilita plánovacích nástrojů integrovaných v systému vyšší. V rámci zvolených technik je konkrétně cíleno na plánovače **At** a **cron**. Před nastavením těchto služeb se nabízí otázka, zda je nutné mít oba plánovače v provozu, neboť plní téměř totožnou službu. Byť cron umožňuje komplexnější nastavení plánování. Nehledě na zvolenou variantu nástroje se musí pro formu ochrany před jejich zneužitím provést jisté ochranné kroky. V případě plánovače cron se nejprve musíme zaměřit na oprávnění k adresářům této služby. Práva vzhledem k možným nestandardním a kompromitujícím úpravám musí mít pouze uživatel root, který má být zároveň i jejich vlastníkem. Zasažené soubory a adresáře a příkazy pro potřebná oprávnění představuje následující výpis.

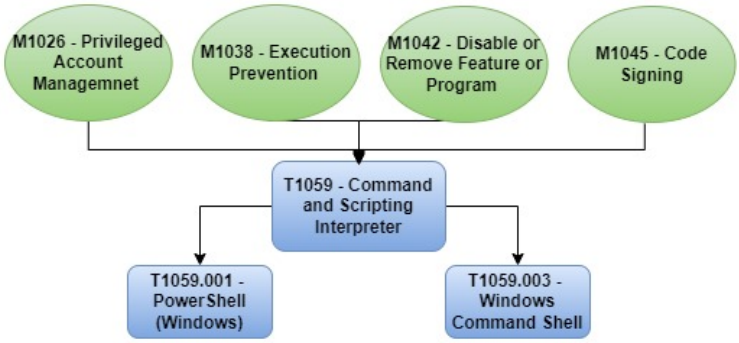
```
# Změna vlastníka a nastavení oprávnění pro /etc/crontab
sudo chown root:root /etc/crontab
sudo chmod og-rwx /etc/crontab
# Změna vlastníka a nastavení oprávnění pro /etc/cron.d/
sudo chown root:root /etc/cron.d/
sudo chmod og-rwx /etc/cron.d/
# Změna vlastníka a nastavení oprávnění pro /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly,
/etc/cron.monthly
sudo chown root:root  /etc/cron.hourly/  /etc/cron.daily/ /etc/cron.weekly/ /etc/cron.monthly/
sudo chmod og-rwx /etc/cron.hourly/  /etc/cron.daily/ /etc/cron.weekly/ /etc/cron.monthly/
```

Po nastavení oprávnění složkám a souborům už zbývá pouze řídit administrativní přístup pro vytváření a plánování úloh. V praxi to znamená zavést seznam oprávněných uživatelů pro správu úloh. Implicitně po instalaci plánovačů jsou vytvořeny seznamy **at.deny** a **cron.deny**, které fungují na opačném principu a obsahují seznam uživatelů kterým je správa zakázána. Z logického a bezpečnostního pohledu je vhodnější tento princip přístupu otočit, neboť při vytvoření nového uživatele může dojít k opomenutí jeho přidání na daný list a přístup mu tam bude umožněn. Proto dojde k smazání zakazujících listů, a naopak se přidají soubory **at.allow** a **cron.allow** pro definic oprávněných účtů. Na tento krok jsou i oba plánovače připravené, neboť z jejich pohledu se nejprve vyhledává a kontroluje soubor **.allow** a až posléze **.deny**. Pro finální konfiguraci musí proto dojít k následujícím příkazům.

```
# Odstranění zakazujících seznamů /etc/at.deny a /etc/cron.deny
sudo rm /etc/at.deny /etc/cron.deny
# Založení souborů pro oprávněné uživatele
sudo touch /etc/at.deny /etc/cron.deny
# Nastavení vlastníka souborů a přístupových práv
sudo chown root:root  /etc/cron.allow/  /etc/at.allow/
sudo chmod og-rwx /etc/cron.allow/  /etc/at.allow/
```

7.2.6 Shell a skripty

Používání skriptovacích jazyků a integrovaných interpretů patří mezi hojně využívané techniky útoku. Zejména v případě přístupu k PowerShellu s vyšším oprávněním se dostává do rukou kompromitující osoby velmi sofistikovaný nástroj pro ovládání systému. Proto je vhodné této kategorii věnovat patřičnou pozornost z pohledu správy systémů. Obdobný názor mají i odborníci z MITRE, neboť na základě této problematiky vytvořili patřičnou sadu technik a forem zmírnění dopadu útoků. V souvislosti s výše zmíněnou formou napadení se jeví jako možná opatření nastavit patřičná privilegia pro používání interpretů a pouštění pouze ověřených skriptů. Soupis vybraných řešení můžeme sledovat na obrázku č.16.



Obrázek 16 - Schéma mitigací a technik v oblasti shell a skriptů
Zdroj: vlastní zpracování

Řada potřebných akcí pro možnou ochranu se v rámci aplikace projevuje napříč ostatními řešenými kategoriemi. I v tomto případě již byla řada technik představena. Mezi základní omezující faktory určitě spadá přístup k interpretům s vyššími privilegii pouze pro správce systémů, tato oprávnění jsou řízena pomocí UAC aplikovaného v kapitole 7.2.3.1. Určitá část protekce je zastoupena při aktivaci nástroje AppLocker a nastavených pravidel z tabulky č.15. Zejména jde o kontrolu spouštění skriptů pouze z vybraných systémových složek. Nastavená pravidla však mohou doznat určitých restriktivnějších úprav, pokud to bude potřebné z pohledu detekovaných informací při provozu systému.

Z pohledu sofistikovanějšího interpreta PowerShell lze kromě výše uvedených způsobů ochrany, zhodnotit a případně aplikovat kroky následujících konfigurací. Mezi jedno z doplňujících nastavení patří exekuční politika pro načítání konfiguračních souborů a spouštění skriptů. Princip této funkcionality je ukryt v nastavení režimu

kontroly před vykonáním skriptu v kontextu počítače, relace nebo uživatele. V systému Windows jsou dostupné tyto politiky:

- **AllSigned** – všechny skripty a soubory musí být podepsány důvěryhodným vydavatelem,
- **Bypass** – bez blokace a kontroly všech souborů ,
- **RemoteSigned** – skripty musí být digitálně podepsány, pokud jsou staženy z internetu,
- **Restricted** – spuštění všech soborů a skriptů je zakázáno,
- **Unrestricted** – bez blokace a kontroly, ale uživatel je varován o původu skriptu.

Volba vhodného režimu je velmi individuální a závisí na provozovaném prostředí a operacích, které podnikají uživatelé a aplikace. Příliš restriktivní nastavení může mít opačný dopad na používání systému, na druhou stranu zajisté je vhodnější spíše využít restriktivnější opatření a v případě potřeby ho rozvolňovat, pokud to bude v souladu s bezpečností. K aplikaci nastavení z pohledu využití pro aktuálního uživatele a všechny uživatele stroje se používá editor zásad GPO. Ostatní skupiny lze nastavovat standardně přes terminál PowerShellu. Navržené GPO zásady jsou zobrazeny v tabulce č.17.

Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell		
Politika	**Nastavení**	**Informace**
Turn on Script Execution	Enabled – Allow local scripts and remote signed scripts	Povolení spouštění skriptů pro všechny uživatele počítače
User Configuration\Administrative Templates\Windows Components\Windows PowerShell		
Politika	**Nastavení**	**Informace**
Turn on Script Execution	Enabled – Allow local scripts and remote signed scripts	Povolení spouštění skriptů pro aktuálního uživatele

Tabulka 17 - GPO zásady pro interpreta PowerShell
Zdroj: vlastní zpracování

V rámci aktivní ochrany přístupnosti k PowerShellu na Windows platformě se lze například zaměřit na přístup PowerShellu k internetu nebo naopak přístup na tento nástroj přes službu pro vzdálenou správu Windows Remote Management. Vhodným opatřením pro zmíněné formy přístupu je aplikace příchozích a odchozích pravidel na straně brány Windows Firewall. Bezpečnost interpretů v rámci systému je zajisté potřebná, ovšem z pohledu funkcionalit, které tyto nástroje nabízejí je důležité najít optimální nastavení neomezující zasažené aktéry.

7.2.7 Brána Firewall a nativní služby

Počáteční přístup, objevování nebo laterální pohyb jsou kategorie úzce spojené s komunikací pomocí protokolů a služeb integrovaných v operačních systémech. V principu tak vytváří komunikační rozhraní vůči svému okolí, které může mít lokální nebo veřejný síťový charakter. Přestože většina takto publikovaných služeb má svá opodstatnění, očima útočníka se jedná o pouhou další možnost pro kompromitaci systémů. Proto je na uvážení administrátorů organizace, zda jsou schopni tato rozhraní zabezpečit dostatečnou formou či nikoliv. Nutno podotknout, že bezpečnost v tomto případě má dvojí charakter, neboť je spojena i nastavenými pravidly na síťové infrastruktuře. Kombinací zabezpečení sítě a operačních systému, tak může vzniknout silnější ochrana vůči aplikovaným technikám.

Z pohledu báze ATT&CK se pro autorem vybrané techniky prolíná mnoho způsobů pro řešení dané problematiky. V celkovém shrnutí je doporučeno zaměřit se na tyto body:

- limitování přístupu služeb do sítě,
- vypnutí nebo blokace nepotřebných služeb,
- řízení přístupu uživatelů k službám,
- úprava konfigurace a politik v rámci operačního systému.

Celkový přehled všech začleněných způsobů mitigace a mapovaných technik je zdokumentován tabulkou č.18.

Zmírnění	Techniky
M1030 - Network Segmentation	T1190, T1133, T1046, T1210, T1021.001, T1021.004, T1071, T1095, T1571
M1042 - Disable or Remove Feature or Program	T1133, T1091, T1046, T1210, T1021.001, T1021.004, T1021.004
M1035 - Limit Access to Resource Over Network	T1133, T1021.001, T1021.002
M1034 - Limit Hardware Installation	T1091
M1022 - Restrict File and Directory Permissions	T1098.004
M1028 - Operating System Configuration	T1087, T1087.001, T1135
M1026 - Privileged Account Management	T1190, T1210, T1021.001, T1021.002
M1018 - User Account Management	T1021.004

Tabulka 18 - Přehled zmírnění a technik v rámci oprávnění a řízení přístupu
Zdroj: vlastní zpracování

V obecném principu je síťová komunikace v rámci operačních systémů řízená bránami firewall, které umožňují aplikovat restriktivní pravidla na síťové pakety a komunikační porty. Na platformě Windows je tento nástroj vedený pod označením Windows Defender Firewall. Pro jeho nastavení lze využít přehledné GUI nebo případ PowerShell. V zásadě mezi prvotní nastavení patří aktivace brány pro všechny předdefinované profily v podobě **doménového**, **soukromého** a **veřejného**. Díky profilům lze rozlišovat a individuálně povolovat pravidla dle typu sítě, ke které jsme právě připojeni. Následně již dochází k aplikaci samotných výchozích a odchozích pravidel s možností pokročilejšího nastavení pravidel pro zabezpečení. Pro každé pravidlo můžeme aplikovat širokou škálu omezení jako například:

- aplikace pravidla na konkrétní porty, program, službu,
- povolení pouze pro některé uživatele nebo skupiny,
- povolení pouze pro vyjmenované lokální nebo veřejné IP,
- vyžádání ověření uživatele pomocí autentizačních protokolů.

V zásadě po výchozí instalaci operačního systému Windows Server jsou všechna příchozí připojení blokována kromě již aplikovaných pravidel a odchozí připojení povolena. Povolených služeb a otevřených portů ve výchozí podobě systému není mnoho, z pohledu bezpečnosti tak za zmínku stojí pouze porty 139 a 445 pro protokol SMB nebo 5985 pro službu Windows Remote Management. U těchto portů lze zvolit minimální strategii v přístupu pouze v lokální síti případně jejich úplné vypnutí.

Platforma Linux a její distribuce mají pro řízení síťové komunikace více možností jako například firewalld, ufw nebo univerzální iptables. Distribuce Ubuntu má ve výchozí instalaci integrované ufw i iptables. Pro běžnou správu příchozí a odchozí komunikace bohatě postačí ufw. V případě komplexnějšího hlídání síťových packetů je vhodnější využití iptables. Konfigurace firewallu probíhá standardními příkazy přes terminál, případně lze využít úpravu souborů v adresáři **/etc/ufw/**. Samotná nastavení pak mohou probíhat v rámci zadávání konkrétních portů a adres nebo pomocí zakládání profilů pro služby a aplikace nacházející se v adresáři **/etc/ufw/application.d**. Počáteční konfigurace zvolíme totožnou jako u platformy Windows, a to v podobě povolení odchozí a odmítnutí příchozí komunikace. Posléze už je nastavení čistě individuální záležitostí, neboť list povolených portů je prázdný. Konfigurace je zaznamenána v následujícím výpisu.

```
# Nastavení výchozího pravidla pro příchozí a odchozí komunikaci
sudo ufw default allow outgoing
sudo ufw default deny incoming

# Příklad povolení portu ssh
sudo ufw allow ssh  nebo  sudo ufw allow 22/tcp
# Uvedení ufw do provozu
sudo ufw enable
# Výpis konfigurace firewallu
sudo ufw status
```

V obecném principu zabezpečení síťové komunikace na obou platformách je vhodné povolit vždy pouze potřebné síťové porty do internetu, v lepším případě pouze do vnitřní sítě. Pro jistou formu zabezpečení je vhodné aplikovat například omezení dostupnosti na konkrétní IP adresy a uživatele, pokud to je možné. Velmi často se také setkáváme se záměnou standardně využívaných portů za nestandardní, což ale musí být doplněno některou z dalších způsobů zabezpečení. Nejvhodnější metodu pro přístup na systémy a služby interního charakteru poskytuje například připojení přes VPN. Následující podkapitoly doplňují zvýšení ochrany v případě přístupu a komunikace přes často využívané protokoly na systém.

7.2.7.1 Autorun

Zastoupení v oblasti fyzického přístupu útočníků k systému reprezentuje z pohledu Windows funkce autorun. Principem tohoto útoku je kompromitace vyměnitelného média malwarem, při jehož fyzického vložení do počítače dojde k automatickému spuštění škodlivého kód přes funkci autorun. Účinnou obranou proti této formě útoku je zakázání této funkce. Případně úplné zakázání vyměnitelných médií, které v dnešní době nejčastěji zastupuje USB flash disk. Potřebná nastavení lze jednoduše aplikovat pomocí GPO politik z tabulky č.19.

Computer Configuration\Administrative Templates\Windows Components\AutoPlay Policies		
Politika	**Nastavení**	**Informace**
Set the default behavior for AutoRun	Enabled – Do not execute any autorun commands	Zákaz provedení všech autorun příkazů
Computer Configuration \Administrative Templates\System\Removable Storage Access		
Politika	**Nastavení**	**Informace**
All Removable Storage classes: Deny all access	Enabled	Zakázání všech vyměnitelných médií

Tabulka 19 - GPO pro vypnutí funkce AutoRun
Zdroj: vlastní zpracování

7.2.7.2 SMB

Síťový protokol SMB patří mezi často používané protokoly v rámci firemních prostředí, neboť zajišťuje přístup k sdíleným zařízením, složkám nebo souborům. Na druhou stranu se ovšem stává terčem útoků, pokud je veřejně přístupný bez aplikovaných opatření. Reálným příkladem je nechvalně známý ransomwarový útok WannaCry. Jeho standardní komunikace probíhá na TCP portu 445 a 139 ve starší verzi komunikující přes rozhraní NetBIOS. Z pohledu bezpečnosti u komunikace SMB, tak nastávají dva možné případy, kdy první představuje zablokování těchto portů a vypnutí služby, pokud není potřeba. Druhý případ představuje používání SMB s určitým nastavením, které ztíží jeho zneužití. Mezi těmito kritérii figurují:

- nevyužívat starší verzi protokolu SMBv1 - nedostatečné šifrování,
- nepoužívat SMB v rámci veřejné sítě,
- nastavit vhodná příchozí a odchozí pravidla SMB (omezení uživatelů, počítačů),
- využít podepisování SMB - Umožnuje chránit zprávy během jejich přenosu a pomáhá odhalit, zda je někdo nekompromitoval.

7.2.7.3 RDP

Remote Desktop Protocol neboli vzdálená plocha poskytuje připojení na vzdálený počítač v podobě standartní uživatelské plochy a nahrazuje tak fyzickou přítomnost u stroje. RDP patří mezi jeden z nejběžněji používaných protokolů v komunitě platformy Windows. Míra zapojení tohoto protokolu do standardního pracovního procesu eskalovala v poslední letech vzhůru, neboť spousta zaměstnanců začala pracovat formou home office. Právě díky velké popularitě, není vhodné komunikační TCP port 3389 této služby propagovat volně do internetu, neboť pravděpodobně v nejbližším časovém horizontu se stane oběti některé z technik napadení.

Obdobně jako u protokolu SMB patří mezi nejúčinnější možnou ochranu tento protokol úplně deaktivovat. Existují ovšem i parametry pomocí nichž lze RDP relativně bezpečně provozovat. Mezi potřebnými nastaveními figurují GPO politik z tabulky č.20 a následující kritéria:

- **VPN –** způsob pro bezpečné používání RDP služby,
- **aplikovat příchozí pravidla pro připojení** – specifikace veřejných i lokálních IP adres, ze kterých se lze připojit,
- **nastavení uživatelských účtu** – potřebná nastavení jsou shrnuta v kapitole 7.2.2.1 o politice účtů,
- **specifikace uživatelů** – pro využívání lze pomocí GPO politik specifikovat uživatele nebo skupiny, které mohou přes službu RDP připojit,
- **využít NLA** – Network Layer Authentication umožnuje ověření uživatele před navázáním spojení,
- **aktualizace OS** – Vzhledem k objevování zranitelností mohou být pro tuto službu vydány opravné balíčky.

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Right Assignment		
Politika	**Nastavení**	**Informace**
Allow log on through Remote Services	Administrators, Remote Desktop Users	Povolení definovaných uživatelů k připojení přes RDP
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security		
Politika	**Nastavení**	**Informace**
Set client connection enrycption level	Enabled – High Level	Úroveň šifrování dat při komunikaci mezi klientem a serverem
Always prompt for password upon connection	Enabled	Vyžadování hesla při každém vyvolání nové relace
Require user authentication for remote connections by using NLA	Enabled	Zapnutí funkce NLA

Tabulka 20 - GPO politiky pro zabezpečení RDP protokolu
Zdroj: vlastní zpracování

7.2.7.4 SSH

Zabezpečený komunikační protokol Secure Shell konkuruje RDP protokolu, ovšem na platformě Linux. Jde o nejběžnější způsob pro vzdálenou správu počítačů postavených na této platformě. I když tento protokol poskytuje šifrovanou komunikaci, jeho publikace v rámci veřejné sítě nezůstane bez povšimnutí útočníků. Právě z těchto důvodů jsou pro jeho užívání provést několik úprav v konfiguraci SSH serveru a zvýšit jeho ochranu vůči nežádoucím vlivům. Samozřejmě i v případě tohoto protokolu platí obdobná forma nejvyšší formy bezpečnosti v podobě neprovozování tohoto protokolu nebo v druhém případě umístění v rámci VPN sítě.

Navrhované úpravy začínají u změny komunikačního portu, neboť standardní port 22 na protokolu TCP je celosvětově známý a jeho odhalení je příliš snadné. Ze síťového

pohledu ještě zbývá nastavení restrikcí na konkrétní IP adresy, kterou lze provést přímo v konfiguračním souboru SSH serveru a aplikací pravidla na firewallu. Jisté úpravy doznává i autentizační část. Nejzásadnější změnou je samotné ověřování uživatele, kdy místo jména a hesla je bezpečnější použít autentizační klíče. Na klientské stanici je vygenerována privátní a veřejná část klíče. Privátní zůstává na klientském počítači a veřejná je umístěna na SSH server. Při připojení na server pak jednoduše dochází k ověření podpisu na serverové straně pomocí náhodně vygenerovaných a podepsaných dat na klientovi. V rámci autentizace dále specifikujeme uživatele i skupiny, které mohou se mohou pomocí SSH přihlásit a deaktivujeme přístup účtu root. Finální podoba konfigurace je dále doplněna o další bezpečností parametry relace.

Konfigurační soubor služby SSH je umístěný v adresáři **/etc/ssh/sshd_config**. Výše zmíněné úpravy konfigurace, včetně generování klíčů jsou představeny v následujícím výčtu.

```
# Příkaz pro vygenerování autentizačních klíčů. Uložení probíhá do adresáře .ssh v uživatelském
adresáři. Například /home/danis/.ssh/.
#Generování vzniknou klíče id_rsa (privátní klíč) a id_rsa.pub (veřejný klíč).
# Veřejný klíč musí být umístěn na server do souboru authorized_keys v adresáři .ssh.
ssh-keygen -t rsa

# Úprava konfiguračního souboru SSH serveru /etc/ssh/sshd_config.

# Nový port pro službu
Port 52022
# List uživatelů, kteří jsou oprávněni používat SSH.
AllowUsers   adm_danis
# Zablokování uživatele root
PermitRootLogin   no
# Povolené IP adresy pro navázání komunikace.
ListenAddress  192.168.0.100
# Vypnutí autentizace pomocí standardního hesla.
PasswordAuthnetication  no
# Maximální počet konkurenčních připojení k SSH.
MaxStartups   5
# Zakázání přesměrování portů.
AllowTcpForwarding  no
X11Forwarding  no
# Nastavení intervalu pro nečinnost klienta. Po uplynutí dojde k jeho odhlášení.
ClientAliveInterval   900
ClientAliveCountMax 0
```

7.2.8 Antivirová ochrana

Antivirová ochrana může v řadě situací pomoci s detekcí škodlivého softwaru ještě před jeho spuštěním nebo umístěním do systému. Ve své podstatě to je doplňující mechanismus k zvýšení ochrany systému společně s dosud navrženou konfigurací. Tento bezpečnostní prvek je zařazen i do báze ATT&CK, jako možná forma mitigace s označením **M1049 - Antivirus/Antimalware.** Z pohledu zvolených technik figuruje u oblasti týkající se skriptování. Uplatnění však lze brát komplexně napříč systémem.

Použití antivirové ochrany je spojeno zejména s platformou Windows, neboť počet škodlivých programů je pro tento systém mnohonásobně větší než pro Linux. Nelze konstatovat, že platforma Linux je vůči napadení virem stoprocentně zabezpečená. Nicméně koncept platforem se v mnoha procesech odlišuje a většině útoků lze u Linuxu předejít vhodnou konfigurací. Samozřejmě i pro Linux existují antivirové programy doplňující bezpečnostní složku, ovšem podstatnější formu ochrany plní u systému od firmy Microsoft.

Spektrum antivirových programů pro Windows zahrnuje velké množství komerčních i volně dostupných řešení. Vhodnou variantu představuje již integrovaný Windows Defender Antivirus, který je celkově propojený s operačním systémem a nabízí velkou škálu protekčních mechanismů zejména proti malwaru. Ke správě Defenderu je k dispozici GUI rozhraní v aplikaci Windows Security nebo GPO politiky. V rámci základního nastavení je třeba mít aktivované následující moduly:

- **Ochrana v reálném čase** – zajišťuje vyhledávání škodlivých softwarů a znemožní jejich instalaci,
- **Cloudová ochrana a odesílání vzorků** – umožnuje komunikaci a odesílání podezřelého soubor, který antivirus nerozezná k analýze. Soubor je blokován do doby, než se dostaví patřičné informace,
- **Ochrana před falšováním** – zabraňuje malwaru v manipulaci s důležitými funkcionalitami.

Pro správnou funkčnost a úspěšnost detekce škodlivého kódu je důležité neopomenout instalaci průběžně vydaných aktualizací pro tento nástroj. Aktualizace lze aplikovat v rámci služby Windows Update nebo pomocí manuálního vyvolání například přes PowerShell.

7.2.9 Systémové aktualizace

Jedna z možností, jak útočníci mohou kompromitovat systém je nalezení zranitelností na straně systémových funkcí nebo nainstalovaných aplikací dříve, než je jejich vydavatel opraví a vydá novou verzi softwaru. Právě proto by mělo docházet k pravidelný kontrolám publikovaných aktualizací a jejich aplikaci dříve, než dojde k prolomení ochrany. Na danou problematiku se vztahuje i několik zanalyzovaných útočných technik a mitigace s označením **M1051 - Update Software**, která apeluje na pravidelnost aktualizace softwarů.

Pro řízení aktualizací v operačním systému Windows je k dispozici služba Windows Update, která se zaměřuje výhradně na aktualizaci operačního systému, bezpečnostní záplaty nebo aktualizaci antiviru Windows Defender Antivirus. Dále pak nabízí i volitelné aktualizace hardwarových komponent. Nastavení této služby je ryze individuální záležitostí, neboť každá organizace může preferovat svoji politiku pro aktualizaci systémů. Velmi často se tak kromě automatického režimu, uplatňuje manuální řízení a instalace pouze aktualizací, které uznají správci za důležité. V principu je však hlavním cílem udržet systém a aplikace plně ošetřené vůči škodlivým vlivům.

Linuxová platforma nabízí v tomto směru opět větší variabilitu a pro aplikaci aktualizací je dostupných hned několik nástrojů. V modelovém prostředí distribuce Ubuntu se nachází předinstalovaný balíkovací systém **apt.** Scénáře pro nasazení aktualizací jsou totožně jako u Windows a rozhoduje u nich individualita organizace. Ovládání **apt** probíhá standardně přes terminál pomocí příkazů, nejzákladnější z nich pro manuální instalaci jsou uvedeny v následujícím výpisu.

```
# Vyhledání nových verzí instalovaných balíčků
sudo apt-get update
# Instalace všech nalezených verzí nových balíčků
sudo apt-get upgrade
# Individuální instalace balíčku
sudo apt-get install „název balíčku“
# Individuální odstranění nainstalovaného balíčku
sudo apt-get remove „název balíčku“
```

7.2.10 Ochrana dat

Vyjma narušení dostupnosti nebo ovládnutí správy nad systémy, se mezi cíle technik útočníků řadí porušení integrity dat. V praxi to znamená jejich poškození určitou formou manipulace nebo dokonce jejich úplné odstranění. Narušení integrity může mít fatální dopady na chod systému a aplikací nebo způsobit finanční ujmu pro organizace a jejich uživatele. Právě z těchto důvodů pro označenou techniku **T1561 – Disk Wipe** figuruje mezi zmírňujícími způsoby forma **M1053 – Data Backup**, která upozorňuje na nastavení zálohování dat jako opatření proti jejich poškození. Zálohování dat je v rámci IT prostředí často konzultovaným tématem, neboť mnohokrát již došlo k jejich nenávratné ztrátě na základě kompromitace útočníkem. Například v posledních letech lze poukázat na využívání ransomware útoků WannaCry, který šifruje data a pro jejich odblokování požaduje zaplatit určitý obnos.

Politika zálohování je velmi individuální, v principu závisí na důležitosti systému a uložených dat. V rámci kritických systému lze spíše aplikovat striktní plánování na denní bázi. U uživatelských stanic pak lze operovat například na týdenních intervalech. Z pohledu systému Windows jsou pro zálohování dat integrované nástroje s označením **Záloha a obnovení** v klientské verzi systému a pro serverovou podobu **Windows Server Backup**. Pomocí těchto nástrojů lze provádět zálohování dat na externí lokální nebo sdílené uložiště v rámci nastavení určitého intervalu. Lze také přímo vybrat jaká data se budou zálohovat nebo tvořit klon celého systému v podobě bitové kopie. V rámci ochrany samotných záloh je používání těchto nástrojů povoleno jen pro určité účty s vyšším oprávněním. Platforma Linux nabízí k zálohování mnoho nástrojů, pro standardní uživatelskou zálohu souborů lze využít například nástroj rsync a kopírovat potřebné soubory do vzdáleného uložiště.

Jako další formu ochrany před manipulací s daty lze zmínit využití nástrojů pro šifrování disků. Pomocí těchto nástrojů lze šifrovat zvolená data nebo celé diskové oddíly před neoprávněným přístupem a ochránit jejich integritu. Vzhledem k dnes už běžné integraci TPM čipů do počítačů je využití šifrování vcelku komfortní funkcionalitou poskytující jistou formu zabezpečení. Operační systém Windows má pro tyto účely, téměř ve všech svých verzí přístupnou aplikaci BitLocker. Z pohledu Linuxu je dostupných více možností, lze například uvést multiplatformní nástroj VeraCrypt.

7.2.11 Školení uživatelů

Všechny předchozí kapitoly jsou zaměřeny na konfiguraci ochrany proti škodlivým technikám v kontextu systémů, a tedy s virtuálním prostorem. Nebyl ovšem zmíněn velmi důležitý faktor v kybernetické bezpečnosti v podobě samotných uživatelů. Lidé nejsou stroje a svým nekorektním chováním mohou útočníkům přístup k systému velmi usnadnit. Způsobem, jakým alespoň do jisté míry můžeme potenciální riziko lidské složky zmírnit je v rámci organizace uskutečnit školení ohledně bezpečného chování v rámci kybernetického prostoru. Školení by mělo být posléze průběžně doplňováno informacemi o nových hrozbách a postupech v rámci organizace, aby se míra rizika nezvyšovala. I školení uživatelů má svou podobu mitigace s označením **M1017 – User Training** a uplatnění se nachází především u technik spojených s hesly a uživatelskými účty. V rámci doplnění výše zmíněných faktů je vhodné doplnit několik základních pravidel pro chování uživatele:

- používat komplexní a odlišná hesla pro každou službu,
- zamykat zařízení v případě nepřítomnosti,
- nezveřejňovat svá hesla,
- nepřipojovat neznámá externí zařízení,
- kontrola důvěryhodnosti zdrojů,
- nepoužívat soukromé zařízení k pracovním účelům a opačně.

8 Shrnutí

Na základě přiřazení zvolených technik k doporučeným formám zmírnění z pohledu znalostní báze ATT&CK, došlo k jejich rozdělení na kategorie směřující na konkrétní oblast z pohledu nastavení systémů. V jednotlivých kategoriích bylo provedeno podrobnější rozpracování obecných informací u definovaných mitigací v podobě návrhu vhodných ochranných mechanismů či nastavení v rámci platforem Windows a Linux.

První řešená kategorie cílila na inicializaci systému a aplikaci ochranné možnosti startu systému v podobě funkcionality Secure Boot. V kontextu této problematiky autor představil jednotlivé fáze, v nichž se systém při startu nachází a na které jsou útoky směřovány. Následující kapitola byla věnována managementu uživatelů systému a politikám pro uživatelské účty a hesla. V rámci nastavení uživatelských účtů autor uvedl jednotlivé zásady zamykání účtů v podobě GPO politik na straně Windows a začlenění knihoven PAM pro obdobnou konfiguraci v Linuxu. Danou kategorii uzavírá řešení komplexní politiky hesel v kontextu techniky útoku brute force.

V návaznosti na uživatelské účty následuje kapitola vztahující se na oprávnění a řízení přístupu v rámci systému, neboť privilegia jsou důležitá pro vykonání velkého množství vybraných technik. Úvod je věnován způsobu řízení uživatelských účtu. Na systému Windows je aplikována funkcionalita UAC s nasazením doplňujících zásad. Jako protějšek u druhé platformy je uveden příkaz sudo a náležitosti s ním spojené. V druhé podkapitole je shrnut postup pro aplikaci oprávnění pro soubory i složky a dále zmíněny důležité adresáře z pohledu udělení přístupu. Celou sérii zakončuje řízení přístupu k aplikacím, kde jsou postupně představeny nástroje AppLocker a AppArmor. U obou programů je doplněn důvod zařazení do zmírňujících forem a potřebná nastavení k uvedení do provozu.

Celkově čtvrtá kategorie řeší problematiku ochrany autentizačních materiálů v reakci na známé typy útoků jako je kompromitace paměti procesu LSASS a související technika Pass the Hash nebo rizikovost systémových adresářů /etc/passwd a /etc/shadow na linuxové platformě. V rámci řešení jsou techniky blíže specifikovány a doplněny o potřebné akce vedoucí k snížení potenciálního rizika. Pátá kapitola se zabývá integrovanými plánovači úloh, které mohou útočníci použít zejména v oblasti trvalého přístupu nebo spuštěním škodlivých skriptů. Postupně jsou vyjmenovány některé

z dostupných plánovačů pro obě platformy a potřebná nastavení, týkající se hlavně omezeného přístupu k těmto nástrojům.

Po sérii s plánovači bylo došlo na kategorii směrovanou výhradně na interprety a jejich skripty v operačním systému Windows. Cíleno je hlavně na operace skriptovacího jazyku PowerShell, neboť se jedná o velmi sofistikovaný nástroj pro ovládání celého systému. Navržené formy ochrany pro tuto problematiku se zabývají omezeným přístupem nebo digitálním podepisováním skriptů.

Sedmá kapitola se orientuje na zmírnění technik zneužívajících nedostatečně zabezpečený lokální, a především vzdálený přístup na systémy. Z těchto důvodů jsou úvodní řádky této kategorie věnovány firewallovým branám v zastoupení Windows Defender Firewall a ufw. Zmíněna je zejména jejich počáteční konfigurace. Kapitola je následně rozdělena na menší podkapitoly obsahující nejpoužívanější protokoly pro vzdálený přístup a lokální riziko externích médií. Sérii zahajuje funkcionalita Autorun, která hrozí v případě vložení kompromitovaného externího média. V rámci nastavení jsou definovány politiky, které tuto funkci omezují. Následně jsou představena rizika při používání protokolu SMB pro sdílení složek a souborů. Celou kapitolu zakončují potřebné úpravy konfigurací dvou nejpoužívanějších síťových protokolů pro vzdálený přístup, a to RDP a SSH.

Závěrečné kapitoly směřují na obecné oblasti, které ovšem plní v rámci zabezpečení systému důležitou roli. V první z nich se představuje výhoda integrace antivirové ochrany pro hledání a odstranění malwarů, zejména pro operační systém Windows. Následuje připomenutí důležitosti aktivace aktualizací proti bezpečnostním mezerám v systému nebo aplikacích. Není opomenuta ani problematika zálohování dat, neboť jejich ztráta může mít negativní dopad na chod organizace. Finální kapitola již zasahuje mimo virtuální prostor a apeluje na dostatečnou informovanost uživatelů systému, kteří svým chováním mohou výrazně pomoci ke zlepšení celkové ochrany.

9 Závěr

Řízení kybernetické bezpečnosti zahrnuje velké množství procesů, které je důležité dodržovat a neustále kontrolovat. Jen za takových podmínek lze udržet dostatečnou ochranu virtuálního prostoru pro organizaci nebo jednotlivce. Bezpečnostní experti a správci systémů, tak často řeší otázku, jaké kroky provést, aby v maximální možné míře zabezpečili své systémy před kompromitací útočníkem. Vzhledem k velmi proměnlivému prostředí, které kybernetická bezpečnost představuje, jim v rozhodování může výrazně pomoci sdílení informací o útočnících a příslušných technikách.

Cílem práce bylo představit a následně použít projekt znalostní báze MITRE ATT&CK jako prvek pro efektivní řízení kybernetické bezpečnosti na platformách Windows a Linux. Aby mohlo dojít k naplnění zadaného cíle, muselo dojít k prozkoumání dané problematiky. První část práce se proto věnuje základním informacím, které jsou spojeny s kybernetickou bezpečností. V zásadě jsou uvedeny nejdůležitější termíny a správní orgány, díky kterým se lze v tomto oboru orientovat.

Po uvedení do kontextu problematiky byl představen projekt MITRE ATT&CK. V první fázi byly postupně popsány všechny prvky tvořící strukturu znalostní báze a postup mapování určující útočníkovi techniky. Následně došlo na představení nástrojů sloužících pro využívání rámce při definici strategie nebo emulaci protivníka. Ve finální fázi celé teoretické části jsou představeny principy používání matice ATT&CK pro účely zvýšení ochrany proti kybernetickým útokům.

Před zpracování praktické části práce musely dojít k výběru relevantních technik, zaměřených na základní zabezpečení obou platforem. K tomuto kroku jsou využity materiály renomovaných organizací pro kybernetickou bezpečnost.

V praktické části už došlo k naplnění potenciálu znalostní báze. Vybrané techniky musely být nejprve propojeny s dostupnými formami zmírnění dopadu útoku. Právě na základě tohoto mapování autor specifikoval i jednotlivé oblasti zkoumání. V jednotlivých kapitolách jsou následně rozpracovány obecné informace z rámce ATT&CK na finální řešení v podobě postupů a konfiguračních parametrů. Postupně, tak za účelem zvýšení bezpečnosti byly probrány procesy jako například inicializace systému, management a politika uživatelských účtů, řízení lokální i vzdáleného přístup nebo aktualizace systémů.

Závěrem lze konstatovat, že projekt MITRE ATT&CK nabízí z pohledu řízení kybernetické bezpečnosti velmi užitečný nástroj. Vzhledem ke kompletní provázanosti všech komponent poskytuje společné rozhraní pro efektivní dohledání cílů a technik, které útočníci využívají. Zároveň však doplňuje i obecnou formu řešení, která pomáhá bezpečnostní mezeru elimininovat. Řízení kybernetické bezpečnosti je velmi rozsáhla problematika zahrnující mnoho konfiguračních procesů. Proto by na základě zpracování této práce bylo možné navázat v jejím doplnění. Například by bylo vhodné integrovat nástroj pro management log souborů (SIEM), který umožní analýzu aplikovaných opatření a případně detekci jejich nedostatků. Dalším zajímavým tématem by bylo například využití představených nástrojů pro testování zavedených opatření formou red teamingu.

10 Seznam použitých zdrojů

[1] OOSTHOEK, Kris a Christian DOERR. SoK: ATT&CK Techniques and Trends in Windows Malware. CHEN, Songqing, Kim-Kwang Raymond CHOO, Xinwen FU, Wenjing LOU a Aziz MOHAISEN, ed. *Security and Privacy in Communication Networks* [online]. Cham: Springer International Publishing, 2019, 2019-12-13, s. 406-425 [cit. 2022-01-05]. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. ISBN 978-3-030-37227-9. Dostupné z: doi:10.1007/978-3-030-37228-6_20

[2] AL-SHAER, Rawan, SPRING, Jonathan M. a CHRISTOU, Eliana, 2020. *Learning the Associations of MITRE ATT&CK Adversarial Techniques.* arXiv:2005.01654 [online],2020-05-12, [cit. 2022-01-05]. Získáno z: http://arxiv.org/abs/2005.01654arXiv: 2005.01654

[3] KARAGIANNIS, Stylianos, Alexandros TOKATLIS, Sotiris PELEKIS, Michael KONTOULIS, George DOUKAS, Christos NTANOS a Emmanouil MAGKOS. *A-DEMO: ATT&CK Documentation, Emulation and Mitigation Operations.* In: 25th Pan-Hellenic Conference on Informatics [online]. New York, NY, USA: ACM, 2021, 2021-11-26, s. 328-333 [cit. 2022-01-06]. ISBN 9781450395557. Dostupné z: doi:10.1145/3503823.3503884

[4] LIU, Changwei, Anoop SINGHAL a Duminda WIJESEKERA. Forensic Analysis of Advanced Persistent Threat Attacks in Cloud Environments. PETERSON, Gilbert a Sujeet SHENOI, ed. *Advances in Digital Forensics XVI* [online]. Cham: Springer International Publishing, 2020, 2020-08-06, s. 161-180 [cit. 2022-01-06]. IFIP Advances in Information and Communication Technology. ISBN 978-3-030-56222-9. Dostupné z: doi:10.1007/978-3-030-56223-6_9

[5] AJMAL, Abdul Basit, Munam Ali SHAH, Carsten MAPLE, Muhammad Nabeel ASGHAR a Saif Ul ISLAM. *Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation. IEEE Access* [online]. 2021, 9, 126023-126033 [cit. 2022-01-10]. ISSN 2169-3536. Dostupné z: doi:10.1109/ACCESS.2021.3104260

[6] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

[7] VON SOLMS, Rossouw a Johan VAN NIEKERK. *From information security to cyber security. Computers & Security* [online]. 2013, 38, 97-102 [cit. 2022-02-01]. ISSN 01674048. Dostupné z: doi:10.1016/j.cose.2013.04.004

[8] Fortinet. *What is the CIA Triad and Why is it important?* Fortinet, Inc. [online]. [cit. 2022-02-01]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/cia-triad

[9] WALKOWSKI, Debbie. *What Is The CIA Triad?*. F5, Inc [online]. [cit. 2022-02-01].Dostupné z: https://www.f5.com/labs/articles/education/what-is-the-cia-triad#:~:text=These%20three%20letters%20stand%20for,objectives%20for%20every%20security%20program.

[10] KLONOFF, David C. *Cybersecurity for Connected Diabetes Devices*. Journal of Diabetes Science and Technology [online]. 2015, 9(5), 1143-1147 [cit. 2022-02-03]. ISSN 1932-2968. Dostupné z: doi:10.1177/1932296815583334

[11] *Základní pojmy*. Platforma kybernetické bezpečnosti [online]. [cit. 2022-02-05]. Dostupné z: https://www.kybez.cz/

[12] DAZAHRA, M. N., F. ELMARIAMI, A. BELFQIH a J. BOUKHEROUAA. *A Defense-in-depth Cybersecurity for Smart Substations*. International Journal of Electrical and Computer Engineering (IJECE) [online]. 2018, 8(6), 4423-4431 [cit. 2022-02-06]. ISSN 2088-8708. Dostupné z: doi:10.11591/ijece.v8i6.pp4423-4431

[13] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978–80–7251–397–0.

[14] DONALDSON, Scott E., Stanley G. SIEGEL, Chris K. WILLIAMS a Abdul ASLAM. *Enterprise Cybersecurity* [online]. Berkeley, CA: Apress, 2015 [cit. 2022-02-11]. ISBN 978-1-4302-6082-0. Dostupné z: doi:10.1007/978-1-4302-6083-7

[15] ROSS, R. , MCEVILLEY, M. and OREN, J. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [online], Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2018, [cit. 2022-02-12]. Dostupné z: doi:10.6028/NIST.SP.800-160v1

[16] CICHONSKI, Paul R., MILLAR, Thomas, GRANCE, Timothy a SCARFONE, Karen, 2012. *Computer Security Incident Handling Guide.* [online]. 2012. [cit. 2022-02-13]. Dostupné z: https://www.nist.gov/publications/computer-security-incident-handling-guide

[17] HANÁČEK, Petr a Jan STAUDEK. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií.* Praha: Úřad pro státní informační systém, 2000. ISBN 80-238-5400-3.

[18] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[19] NÚKIB. *Legislativa*. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2022-02-21] Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[20] HRŮZA, Petr. *Kybernetická bezpečnost*. Brno: Univerzita obrany, 2012. ISBN 978-80-7231-914-5.

[21] NÚKIB. *O úřadu*. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2022-02-21] Dostupné z: https://nukib.cz/cs/o-nukib/o-uradu/

[22] NÚKIB. *Vládní CERT*. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2022-02-21] Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/

[23] NBU. *NBÚ vybral provozovatele národního CERT (CSIRT.CZ), je jím CZ.NIC*. [online]. [cit. 2022-02-21] Dostupné z: https://www.nbu.cz/cs/aktualne/820-621-nbu-vybral-provozovatele-narodniho-cert-csirtcz-je-jim-cznic/

[24] ŠEFČÍK, Antonín a KVASNICOVÁ Barbora. *Sepsali jsme pro vás přehled doposud vydaných norem řady ISO/IEC 27000. Kybernetická bezpečnost na internetu a zákon.* NGSS [online]. Praha: NEXT GENERATION SECURITY SOLUTIONS s.r.o., 2019 [cit. 2022-02-21]. Dostupné z: https://www.ngss.cz/clanek/46-sepsali-jsme-pro-vas-prehled-doposud-vydanych-norem-rady-iso-iec-27000

[25] STROM, Blake E. *MITRE ATT&CK: Design and Philosophy* [online]. 2. US: McLean, VA, 2020 [cit. 2022-02-23]. Dostupné z: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

[26] MITRE ATT&CK. *Matrix – Enterprise*. MITRE ATT&CK® [online]. Copyright © 2015 [cit. 2022-02-24]. Dostupné z: https://attack.mitre.org/matrices/enterprise/

[27] STROM, Blake E., BATTAGLIA, Joseph A., KEMMERER, Michael S., KUPERSANIN, William, MILLER, Douglas P., WAMPLER, Craig, WHITLEY, Sean M. a WOLF, Ross D., 2017. *Finding Cyber Threats with ATT&CK-Based Analytics*. [online]. 2017. [cit. 2022-02-25]. Dostupné z: https://www.mitre.org/publications/technical-papers/finding-cyber-threats-with-attck-based-analytics

[28] WALKOWSKI, Debbie. *MITRE ATT&CK: What It Is, How it Works, Who Uses It and Why. F5 Labs*.[online]. 2021. [cit. 2022-02-26]. Dostupné z: https://www.f5.com/labs/articles/education/mitre-attack-what-it-is-how-it-works-who-uses-it-and-why

[29] MITRE ATT&CK. *Tactics - Enterprise*. MITRE ATT&CK® [online]. Copyright © 2015 [cit. 2022-02-26]. Dostupné z: https://attack.mitre.org/tactics/enterprise/

[30] STROM, Blake E. *ATT&CK Sub-Techniques Preview*[online]. MITRE ATT&CK®. 2019 [cit. 2022-02-27]. Dostupné z: https://medium.com/mitre-attack/attack-sub-techniques-preview-b79ff0ba669a

[31] MITRE ATT&CK. *Groups*. MITRE ATT&CK® [online]. Copyright © 2015 [cit. 2022-03-01]. Dostupné z: https://attack.mitre.org/groups/

[32] MITRE ATT&CK. *Software*. MITRE ATT&CK® [online]. Copyright © 2015 [cit. 2022-03-02]. Dostupné z: https://attack.mitre.org/software/

[33] RODRIGUEZ, JL. *Defining ATT&CK Data Sources, Part I: Enhancing the Current State*. MITRE ATT&CK®[online]. 2020 [cit. 2022-03-02]. Dostupné z: https://medium.com/mitre-attack/defining-attack-data-sources-part-i-4c39e581454f

[34] NICKELS, Katie. *Getting Started with ATT&CK: Threat Intelligence*. MITRE ATT&CK® [online]. 2019 [cit. 2022-03-04]. Dostupné z: https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f

[35] Cybersecurity and Infrastructure Security Agency | CISA. *Best Practices for MITRE ATT&CK® Mapping* [online]. [cit. 2022-03-05]. Dostupné z: https://www.cisa.gov/uscert/best-practices-mitre-attckr-mapping

[36] MITRE ATT&CK. *Working with ATT&CK*. MITRE ATT&CK® [online]. [cit. 2022-03-07]. Dostupné z: https://attack.mitre.org/resources/working-with-attack/

[37] Anomali. *What Is MITRE ATT&CK and How Is It Useful?*. Anomali® [online]. [cit. 2022-03-07]. Dostupné z: https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful

[38] STROM, David. *4 open-source Mitre ATT&CK test tools compared.* CSO [online]. 2018 [cit. 2022-03-08]. Dostupné z: https://www.csoonline.com/article/3268545/4-open-source-mitre-attandck-test-tools-compared.html

[39] MITRE. *CALDERA™*. MITRE Corporation [online]. 2018 [cit. 2022-03-08]; Dostupné z: https://www.mitre.org/research/technology-transfer/open-source-software/caldera%E2%84%A2

[40] CHENETTE, S. *Emulating Attacker Activities and The Pyramid of Pain*. AttackIQ [online]. 2019 [cit. 2022-03-10]. Dostupné z: https://attackiq.com/2019/06/26/emulating-attacker-activities-and-the-pyramid-of-pain/

[41] NICKELS, Katie. Getting Started with ATT&CK: Threat Intelligence. MITRE ATT&CK® [online]. 2019 [cit. 2022-03-10]. Dostupné z: https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f

[42] NICKELS, Katie. *Using ATT&CK to Advance Cyber Threat Intelligence — Part 1*. MITRE ATT&CK® [online]. 2019 [cit. 2022-03-10]. Dostupné z: https://medium.com/mitre-attack/using-att-ck-to-advance-cyber-threat-intelligence-part-1-c5ad14d59724

[43] WUNDER, J. *Getting Started with ATT&CK: Detection and Analytics*. MITRE ATT&CK® [online]. 2019 [cit. 2022-03-11]. Dostupné z: https://medium.com/mitre-attack/getting-started-with-attack-detection-a8e49e4960d0

[44] STROM, Blake E. *Getting Started with MITRE ATT&CK: Adversary Emulation and Red Teaming*. MITRE ATT&CK® [online]. 2020 [cit. 2022-03-11]. Dostupné z: https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3

[45] APPLEBAUM, A. *Getting Started with ATT&CK: Assessments and Engineering*. MITRE ATT&CK® [online]. 2019 [cit. 2022-03-13]. Dostupné z: https://medium.com/mitre-attack/getting-started-with-attack-assessment-cc0b01769cb4

[46] NÚKIB. *Analýzy*. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2022-03-17]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/analyzy/

[47] ENISA. *ENISA Threat Landscape 2021*. European Union Agency for Cybersecurity© [online]. 2021 [cit. 2022-03-17]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[48] FireEye. *M-Trends 2021*. FireEye© [online]. [cit. 2022-03-17]. Dostupné z: https://content.fireeye.com/m-trends/rpt-m-trends-2021

[49] Red Canary. *Threat Detection Report: Introduction*. Red Canary© [online]. [cit. 2022-03-17]. Dostupné z: https://redcanary.com/resources/guides/threat-detection-report/

[50] Microsoft. *Secure the Windows boot process - Windows security*. Microsoft© [online]. [cit. 2022-03-20]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process

[51] Microsoft. *How User Account Control works (Windows) - Windows security*. Microsoft© [online]. [cit. 2022-03-23]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/how-user-account-control-works

[52] GRAFNETTER, Michael. *Pass-the-Hash útoky a obrana proti nim*. Directory Services Internals [online]. 2015. [cit. 2022-03-30]. Dostupné z: https://www.dsinternals.com/sk/slajdy-pass-the-hash-utoky/

11 Seznam obrázků

12 Seznam tabulek

13 Seznam použitých zkratek

AD – Active Directors

APT – Advanced persistent threat

ATT&CK – Adversarial Tactics, Techniques, and Common Knowledge

CERT – Computer Emergency Response Team

CIA – Confidentiality, Integrity, Availability

COBIT – Control Objectives for Information and Related Technologies

CTI – Cyber threat intelligence

DDoS – Distributed denial of service

DoS – Denial of service

ELAM – Early Launch Anti-Malware

ENISA – European Union Agency for Cybersecurity

GPO – Group Policy Object

GUI – Graphical User Interface

HW – hardware

ICS – Induistrial Control Systems

ICT – Information and Communications Technology

IEC – International Electrotechnical Commission

ISMS – Information security management

ISO – International Organization for Standardization

ITU – International Telecommunication Union

LM – LAN Manager

LSASS – Local Security Authority Server Service

MITM – Man in the middle

NIS – Network & Information Systems

NLA – Network Level Authentication

NTLM – NT LAN Manager

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OS – operační systém

PAM – Pluggable authentication module

POST – Power-on self-Test

RDP – Remote Desktop Protocol

SIEM – Security information and event management

SMB – Server Message Block

SOC – Security Operations Center

SSH – Secure Shell

STIX – Structured Threat Information Expression

SW – software

TPM – Trusted Platform Module

UAC – User Account Control

UEFI – Unified Extensible Firmware Interface

VNC – Virtual Network Computing

14 Seznam příloh

Příloha 1 – Podklad pro zadání diplomové práce

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2020/2021

Studijní program: Aplikovaná informatika
Forma studia: Kombinovaná
Obor/kombinace: Aplikovaná informatika (ai2-k)

Podklad pro zadání DIPLOMOVÉ práce studenta

Jméno a příjmení:	**Bc. Ondřej Daniš**
Osobní číslo:	**I2000304**
Adresa:	Tylova 1082, Jičín – Valdické Předměstí, 50601 Jičín 1, Česká republika
Téma práce:	Využití MITRE ATT&CK pro efektivní řízení kybernetické bezpečnosti
Téma práce anglicky:	Use of MITRE ATT&CK for effective cyber security management
Vedoucí práce:	Mgr. Josef Horálek, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Cílem práce je podrobně popsat projekt MITRE ATT&CK, jeho strukturu a možnosti využití pro efektivní řízení kybernetické bezpečnosti.

V teoretické části autor představí projekt MITRE ATT&CK s důrazem na definici taktik a technik pro řešení zajištění aktuálnosti nastavení kybernetické bezpečnosti pro platformy Windows a Linux.

V praktické části pak autor navrhne řešení pro využití MITRE ATT&CK v procesu zajištění kybernetické bezpečnosti s důrazem na platformy Windows a Linux. Návrh bude řešen formou případové studie implementace MITRE ATT&CK v modelovém firemním prostředí.

Osnova:
1. Úvod do kybernetické bezpečnosti
2. Představení projektu MITRE ATT&CK
3. Definice taktik
4. Definice technik
5. Nastavení pro platformy Windows a Linux
6. Řešení implementace v modelovém firemním prostředí

Seznam doporučené literatury:

STROM, Blake E. *MITRE ATT&CK®: Design and Philosophy* [online]. 2. US: McLean, VA, 2020 [cit. 2021-01-05]. Dostupné z: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
STROM, Blake E. *Finding Cyber Threats with ATT&CK™-Based Analytics* [online]. 2. US: McLean, VA, 2017 [cit. 2021-01-05]. Dostupné z: https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats%20with%20att%26ck-based-analytics.pdf

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: