Monitorování bezpečnostních hrozeb v síťové infrastruktuře založené na Microsoft Windows

Daniela Zedníčková

Bakalářská Práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Daniela Zedníčková**
Osobní číslo:	**A21104**
Studijní program:	**B0613A140020 Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Monitorování bezpečnostních hrozeb v síťové infrastruktuře založené na Microsoft Windows**
Téma práce anglicky:	**Monitoring Security Threats in a Microsoft Windows-Based Network Infrastructure**

Zásady pro vypracování

1. Nastudujte a popište potřebnou terminologii a teorii v kontextu tématu práce.
2. Popište aktuální stav řešení.
3. Navrhněte možná vylepšení a řešení monitorování bezpečnosti v rámci firmy.
4. Zvolte a popište vhodné technologie a prostředky.
5. Realizujte navržené řešení.
6. Řešení vhodně otestujte a porovnejte se stávajícím.

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

Seznam doporučené literatury:

1. *Zabezpečení počítačových sítí bez předchozích znalostí*. 1. Brno: CP Books, 2005. ISBN 8025104176.
2. *Computer security : principles and practice*. Third edition. Boston: Pearson, 2015. ISBN 9781292066172 1-292-06617--2.
3. *Analýza sítí a řešení problémů v programu Wireshark*. Brno: Computer Press, 2012. ISBN 9788025137185.
4. *Informační bezpečnost*. 1. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 8086898385.
5. *TCP/IP v kostce*. Druhé upravné a rozšířené vydání. Kopp, 2009. ISBN 978-80-7232-388-3.
6. *Tribe of hackers : cybersecurity advice from the best hackers in the world*. 1. Wiley: Wiley, 2019. ISBN 9781119643395.
7. *CyberSecurity*. 1. Edice CZ.NIC, 2019. ISBN 978-80-88168-31-7.
8. MICROSOFT. Security auditing. *Security auditing* [online]. 2022 [cit. 2023-09-25]. Dostupné z: https://learn.microsoft.com

Vedoucí bakalářské práce: **Ing. Petr Žáček, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **5. listopadu 2023**
Termín odevzdání bakalářské práce: **13. května 2024**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 6.5.2024

Daniela Zedníčková v.r.
…….
podpis studenta

ABSTRAKT

V této bakalářské práci je vytvořen program pro monitorování uživatelských aktivit na platformě Windows pro firmu X9 s.r.o. Práce začíná výčtem možných kybernetických útoků a vymezením terminologie. Následuje hlavní část práce, tedy zpracování sběru bezpečnostně relevantních dat s využitím kombinací vlastního agenta, dostupných technologií Windows a open-source nástrojů jako OpenSearch. V rámci práce je rozebrána i etika monitoringu uživatelů, či porovnání se softwary třetích stran. Na závěr jsou uvedeny ukázky agregace dat z výstupů programu.

Klíčová slova:

Active Directory, bezpečnostní logy, kybernetická bezpečnost, Logstash, OpenSearch, PowerShell, Python, sdílené soubory, uživatelské aktivity, Windows, Winlogbeat.

ABSTRACT

In this bachelor's thesis, a program for monitoring user activities on the Windows platform is developed for X9 s.r.o. The work begins with a list of potential cyber-attacks £and the definition of terminology. This is followed by the main part of the thesis, which involves the processing of collecting security-relevant data using a combination of a proprietary agent, available Windows technologies, and open-source tools like OpenSearch. The ethics of user monitoring are also discussed, along with comparisons to third-party software. The conclusion presents examples of data aggregation from the program's outputs.

Keywords:

Active Directory, cybersecurity, Logstash, OpenSearch, PowerShell, Python, security logs, shared files, user activity, Windows, Winlogbeat.

Poděkování

Ráda bych poděkovala Ing. Filipovi Zubíkovi za inspirativní nápad, poskytnutí prostředků a jeho trpělivou podporu během zpracování mé bakalářské práce. Taktéž bych ráda poděkovala Ing. Petru Žáčkovi, Ph.D. za vstřícnost a odborné vedení mé práce. A v neposlední řadě patří velké poděkování mé rodině a přátelům, kteří mě maximálně podporují po celou dobu studia.

Motto

"If We knew what we were doing, it would not be called research, would it?"

-- Albert Einstein --

OBSAH

ÚVOD

Pro většinu lidí představuje kybernetická bezpečnost abstraktní koncept, pro manažery firem je to jedna z nejtěžších výzev. Nová pravidla, jako je EU směrnice NIS2, vede firmy nejen k posílení bezpečnostních opatření, ale i k pravidelnému monitorování svých systémů a uživatelů, aby se firma mohla účinně bránit proti rostoucím kybernetickým hrozbám. Je tedy nezbytné, aby měl management k dispozici informace, které pomohou v plnění této odpovědnosti. Monitoring hrozeb související s uživatelskými aktivitami v rámci sítě má mnoho řešení v podobě kvalitních komerčních i open-source softwarů, které hravě zvládnou komplexní úkoly. Na druhou stranu jsou takové nástroje pro firmy často finančně náročné, nesplňují požadované funkcionality, či vyžadují specializovaného pracovníka, který by ho uměl ovládat. Cílem této bakalářské práce v kooperaci s firmou X9 s.r.o. je výzkum řešení monitoringu uživatel čistě na platformě Windows a není koncipované jako hotový produkt pro komerční užití.

Teoretická část této práce popisuje kybernetickou bezpečnost a příklady útoků související s koncovými stanicemi společně s nezbytnou terminologií k pochopení praktické části. Také se zabývá etickým faktem sledování uživatel ve firmě.

Praktická část se zabývá monitoringem uživatelů v síti. Výsledný program splňuje požadavky firmy, tedy monitoruje přihlášení na počítače, přístupy ke sdíleným složkám včetně jejich modifikací, prohlížení webových stránek, přičemž výstupy anonymizuje (pomocí IP adres). Program také sbírá informace o datových tocích z firewallu a poskytuje přehled o právech uživatelů ke sdíleným složkám. Dále kontroluje připojení externích zařízení a zaznamenává základní informace o AD, operačním systému a hardwaru stanic a serverů. Sběr dat probíhá centralizovaně na jednom počítači s využitím protokolů Windows, nástrojů jako Winlogbeat a Logstash, a také vlastního agenta spouštěného na stanicích. Data a logy jsou ukládány do NoSQL databáze OpenSearch, což umožňuje budoucí rozvoj aplikace, například implementaci strojového učení, což by mohlo být součástí navazující diplomové práce.

Dalším cílem, a to nemálo důležitým, je zisk hlubšího vhledu do fungování sítě Windows a interakcí a požadavků v tomto prostředí. Pochopení a zkoumání je více méně podstata celé práce. Přeci i při vývoji systémů, jako je Zabbix, museli vývojáři nejprve porozumět základům a vyzkoušet jistě několik způsobů, než nalezli ten stávající.

Touto cestou, věřím, se dá celá podstata technologií použitých v rámci monitoringů dobře pochopit. Využití už vynalezeného nástroje přináší jistě velké výhody, ale dle mého názoru

nemůže nikdy plně nahradit zkušenosti získané vlastním vývojem a řešením úskalí v rámci vlastních pokusů.

Moje motivace spočívá tedy především v hlubším porozumění komunikaci počítačů na platformě Windows a výzkumu technologií, jako je OpenSearch a přidružených nástrojů. Cílem je najít efektivní způsob, jak tyto systémy implementovat a poskytnout data, o která firma požádala a ověřit, zda je možné tento postup a nástroje v praxi úspěšně použít.

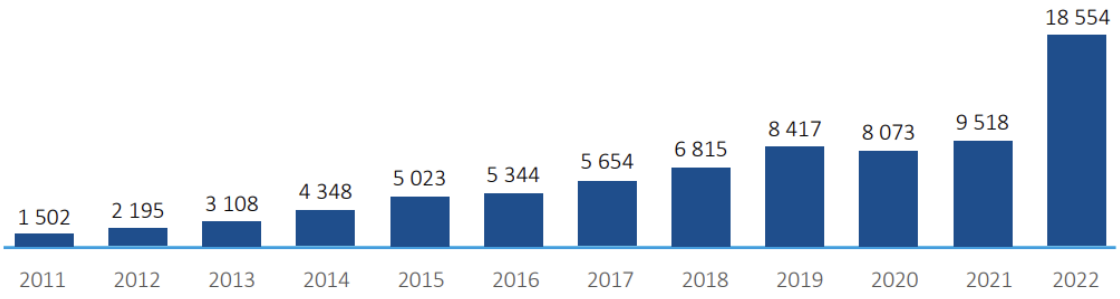
I. TEORETICKÁ ČÁST

1 BEZPEČNOST A MONITORING UŽIVATELŮ

V oblasti kybernetické bezpečnosti se lze setkat s pojmy hrozba a zranitelnost. Nejen tyto pojmy jsou zásadní pro pochopení, jak se bránit proti potenciálním útokům a zabezpečit koncové stanice, které jsou často cílem kybernetických zločinců. Monitoring hrozeb spjatý s aktivitami uživatelů patří mezi důležité prvky celé kybernetické bezpečnosti a společně s dalšími (jako jsou například technologie pro detekci a prevenci úniku informací, správa identit a přístupů, šifrování dat, či pokročilé ochranné systémy proti malwaru) pak může tvořit obranný systém organizace.

1.1 Definice kybernetické bezpečnosti

„*Cílem kybernetické bezpečnosti je zajištění dostupnosti počítačů a jejich sítí, zajištění důvěrnosti a integrity uchovávaných zpracovaných a přenášených dat.*“ (Šulc 2018: 19) [1] Firmy zavádí technická, organizační ale i personální opatření ve snaze bránit se hrozbám, které v posledních letech nabírají na síle. Jen v meziročním porovnání let 2021 a 2022 zaznamenal Národní úřad pro kybernetickou bezpečnost nárůst nahlášených útoků o více, než 55 %. V České republice jsou organizace povinné dodržovat Zákon o kybernetické bezpečnosti č. 181/2014. [2] Tento zákon stanovuje povinnosti a opatření týkající se kybernetické bezpečnosti, aby organizace ochránily své informační systémy a data před kybernetickými hrozbami. Nedávno došlo ke změně tohoto zákona, tato novela byla schválena a vešla v platnost jako Zákon č. 226/2022 Sb. [3]



Obrázek 1. Vyšetřované kyberkriminální případy v ČR mezi lety 2011 až 2022 [4]

1.2 Základní principy

Kybernetická bezpečnost je klíčovým prvkem ochrany dat a informačních systémů vůči vlivům, které mohou vést k jejich zneužití, ztrátě nebo poškození. Tento oddíl se zaměřuje na

vysvětlení tří základních principů kybernetické bezpečnosti: dostupnosti, důvěrnosti a integrity, které jsou nezbytné pro ochranu a správnou funkci informačních systémů ve stále více propojeném světě.

1.2.1 Dostupnost

Zajištění dostupnosti dat či informačních systémů je jedním z hlavních principů. Mezi typické incidenty, které narušují dostupnost, patří ransowarový útok. Jeden ze známých případů napadení ransomwarem posledních let se stal útok v benešovské nemocnici. Došlo k němu v prosinci roku 2019. Jednalo se o virus Ryuk, vstupním bodem byl malware Emotet, který se do počítače dostal nejčastěji otevřením příloh. Škodlivý kód se pak z pohledu běžného uživatele nechoval nijak podezřele. Šířící se trojský kůň vytvářel infikované soubory na lokálním, ale i síťovém úložišti. [5] Po získání důležitých dat chybí už jen jediný krok, a to uzamknout, resp. zašifrovat počítač. Za obnovení přístupu útočníci obvykle požadují výkupné, které se v případě strategicky důležitých firem, či státních sektorů může vyšplhat až do řádu milionů korun.

1.2.2 Důvěrnost

Zajištění důvěrnosti, jak napovídá samotný název, se týká ochrany citlivých informací před neoprávněným přístupem. K narušení důvěrnosti dochází v případě, kdy organizace nedbají na dostatečnou ochranu dat využitím šifrování, monitoringu přístupů, či selhaly jejich autentizační metody. A právě porušení důvěrnosti se stalo osudným pro firmu Sony Pictures Entertainment. V roce 2014 unikly desítky tisíc informací o zaměstnancích a jejich členech rodiny. Nasazený malware využíval vlastnosti správy a síťového sdílení souborů Microsoft Windows SMB k šíření, vypínání síťových služeb a restartování počítače. Navíc pojmenoval infikované soubory podle klíčových komponent Windows, aby provedly většinu špinavé práce při komunikaci s uživatelem a ničení systémů, které infikuje. [6] Cena za porušení důvěrnosti se pro Sony vyšplhala do desítek milionů korun.

1.2.3 Integrita

Narušením integrity se rozumí jakékoliv narušení či pozměnění dat. V případě integrity je ale potřeba si uvědomit, že pokud dojde k nežádoucí změně dat, nemusí být tato změna odhalena včas. „*Čím později se na tento bezpečnostní incident přijde, tím vážnější bude jeho dopad. Problém spočívá v tom, že je velice obtížné dohledat, jaká byla původní hodnota, jelikož nebudeme vědět, kdy přesně ke změně došlo. Navíc oněch změn může být mezitím*

provedeno několik; v takové situace bude zhola nemožné dohledat, jaká byla původní hodnota. Na tomto místě je třeba také zdůraznit, že opatření určené pro zajištění dostupnosti jako je zálohování a archivace nám příliš nepomohou, protože daná poslední změna se bude pravděpodobně nacházet také na záložních a archivních médiích, a pokud nebudeme mít k dispozici logy o činnostech v systému, nebudeme vědět k jakému dni máme data obnovit." (Šulc 2018: 22)[1] Často dochází ke zkreslování digitální reality. Mezi techniky patří například manipulace s časovými razítky prostřednictvím Chronos útoků, nebo nasazení deepfake obsahu v obchodní komunikaci. Útočníci mohou získat přístup k aplikacím pro komunikaci nebo k e-mailovým účtům a využít tak předstírání cizí identity. [7]

1.3 Hrozba

„*Hrozbu můžeme definovat jako náhodnou nebo úmyslně vyvolanou událost, která může mít negativní dopad na důvěrnost, integritu a dostupnost aktiv."* (Šulc 2018: 22) [1] Jedním z hlavních problémů jsou hrozby spojené právě s koncovými stanicemi, jako jsou počítače, chytré telefony, tablety a další zařízení.

1.4 Zranitelnost

„*Zranitelnost představuje vlastnost aktiva, a tudíž se nemusí nacházet pouze v software, nýbrž také v hardware, v procesu a lidech, kteří tvoří informační systém.*" (Šulc 2018: 22) [1] Takové zranitelnosti může útočník využít k realizaci svých cílů a infiltrovat se do systému.

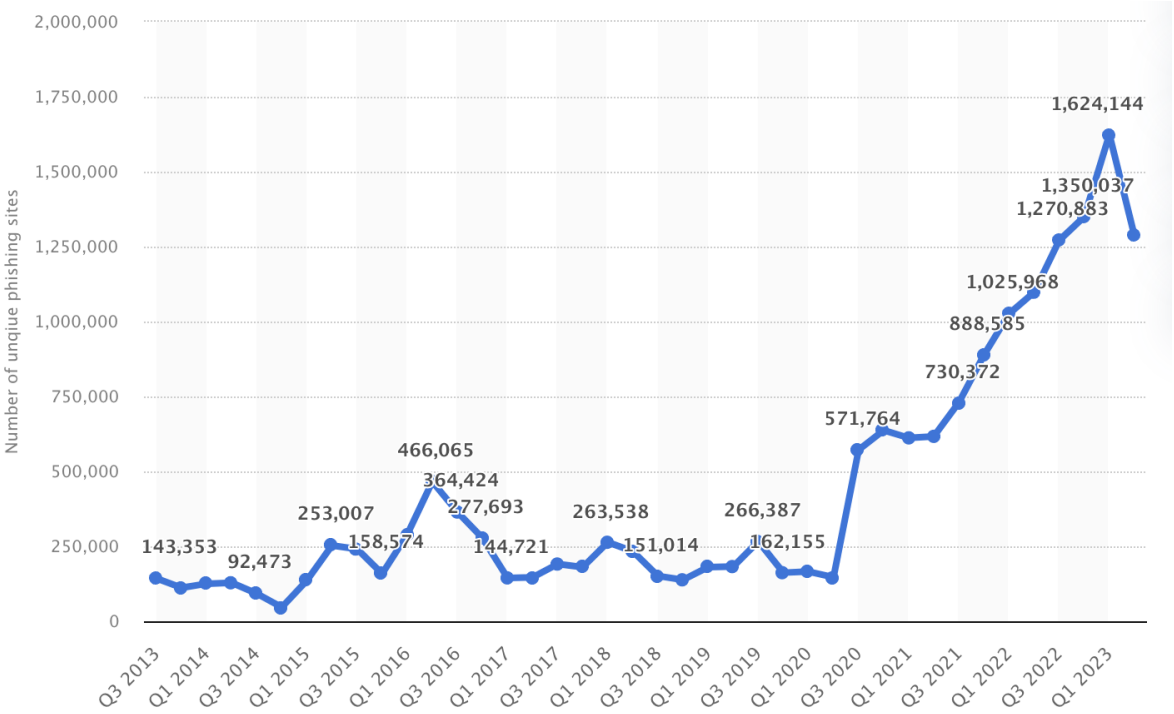
1.5 Typy hrozeb a zranitelností v kontextu stanic

Zákon zdůrazňuje, že je klíčové, aby organizace prováděly identifikaci různých aspektů, které mohou ohrozit bezpečnost jejich dat a systémů. Mezi ty důležité patří nedostatečné povědomí o aktivitách uživatelů a správců, stejně jako zanedbávání aktualizací softwaru a operačních systémů. Jednou z hlavních priorit pro zajištění bezpečnosti dat a systémů je identifikace a řešení těchto potenciálních rizik. Důraz na tyto aspekty je klíčový pro efektivní ochranu dat a systémů organizace. [2]

1.5.1 Phishingové útoky

V dnešní době se jedná o nejčastěji používanou techniku. Podvržený email, textová zpráva, vzkaz na sociálních sítích, či podvržená webová stránka mají za úkol přelstít uživatele. Obvykle ve snaze, aby klikl na odkaz, zadal citlivé údaje, či stáhl přílohu, která slibuje např.

náhled na platy nadřízených. V posledním desetiletí lze pozorovat trend vzrůstu těchto nekalých technik, což potvrzuje i graf počtu známých phishingových stránek, které se na internetu objevily za poslední dekádu.



Obrázek 2. Počet globálních phishingových webů mezi lety 2013–2023 [9]

1.5.2 Neaktualizovaný software

Jedná se o nápravu zranitelností v systému, které mohou vyústit v hrozbu. Například v lednu roku 2024 vydal Microsoft soubor aktualizací a patchů, které měly za úkol ochránit proti Remote Execution code. Bylo objeveno několik zranitelností v produktech běžně používaných uživateli, jako jsou i Microsoft Office. Jedna z nich dokázala umožnit vzdálené provedení kódu v kontextu přihlášeného uživatele. V závislosti na oprávněních přiřazených uživateli by útočník mohl nainstalovat programy a zobrazit, změnit nebo smazat data, či dokonce vytvořit nové účty s plnými uživatelskými právy. [10]

1.5.3 Síťová bezpečnost

Síťová bezpečnost má za hlavní cíl zabránit neoprávněnému přístupu k síťovým prostředkům, detekovat a zastavit kybernetické útoky, či zajistit, že autorizovaní uživatelé mají bezpečný přístup k relevantním zdrojům. [11] Pokud kyberzločinec využije zranitelnosti sítě, může to mít nedozírné následky. Jak vypovídá například útok ransomware z roku 2017, který

využil zranitelnosti v implementaci protokolu pro sdílení souborů Microsoft Windows (SMB). Prostřednictvím zranitelnosti ExternalBlue nainstalovali na počítače zadní vrátka, nástroj vyvíjený americkou Národní bezpečnostní agenturou nazvaný DoublePulsar. Ten umožňuje vzdálenou správu serveru a přes ně se šířil ransomware WannaCry rychle a automaticky na další počítače ve stejné síti. Pravdou je, že to bylo všechno do značné míry předvídatelné Microsoft vydal bezpečnostní záplatu několik měsíců před útokem. Mnoho počítačů však nemělo tuto záplatu aplikovanou. [12]

1.5.4 Sociální inženýrství

Sociální inženýrství je technika, kterou podvodníci využívají k získání citlivých osobních informací, jako jsou hesla, nebo bankovní údaje, od důvěřivých uživatelů. Cílem je získat přístup k jejich počítačům a nainstalovat škodlivý software. To je často jednodušší než překonávat technická zabezpečení počítačů. K velmi rozšířenému phishingu se připojují i další techniky. Například vyvolání strachu může vést k tomu, že potenciální oběť otevře e-mail s varováním o exekuci a klikne na škodlivý odkaz. Objevují se i případy, kdy útočníci slibují různé výhry v loterii nebo nový telefon výměnou za poskytnutí osobních údajů. Vzbuzení zvědavosti se projevuje také prostřednictvím falešných e-mailů od přepravních společností s oznámením chybné adresy. Objevuje se i zneužití empatie, či nekalých praktik v podobě vydávání se za pracovníka IT, který se potřebuje dostat například do serverovny. Jedním z nejznámějších hackerů využívající sociálního inženýrství je Kevin Mitnick. Jako jedné z nejhledanějších osob v historii americké FBI mu za jeho neoprávněné průniky do počítačových systémů velkých společností hrozil trest několika set let odnětí svobody. V průběhu 80. a 90. let pronikl do mnoha počítačových systémů firem, jako jsou Motorola, DEC, Nokia, Sun Microsystems, či Fujitsu Siemens. Mitnick ve skutečnosti nebyl nijak zvlášť dobrým počítačovým hackerem, dokázal však své technické znalosti dokonale kombinovat s technikami sociálního inženýrství a díky tomu byl tak úspěšný.[13]

1.5.5 Nedostatečný monitoring uživatelských aktivit

Mezi základní problémy dle zákona o kybernetické bezpečnosti lze považovat právě nedostatečné monitorování činnosti uživatelů a administrátorů a tedy neschopnost odhalit včas jejich nevhodné, nebo závadné způsoby chování. [2] Pokud nemá vedení povědomí o tom, kam a kdy mají uživatelé přístup, stává se infrastruktura chaotická, o čemž vypovídá například incident z roku 2022. Organizace obvykle mají mnoho uživatelů s rozšířenými

oprávněními, jako jsou administrátoři, techničtí specialisté a manažeři. Někteří mohou mít přístup pouze k určitým kritickým zdrojům, jako jsou specifické databáze nebo aplikace. Jiní mohou mít plný přístup ke každému systému v síti, a dokonce mohou vytvářet nové privilegované účty, aniž by na sebe upoutali pozornost. Pokud mají privilegovaní uživatelé zlé úmysly, nebo byli kompromitováni, může to vést k únikům dat, finančnímu podvodu, sabotáži a dalším vážným následkům. Což se stalo v lednu 2022 Mezinárodnímu výboru Červeného kříže. Jednalo se o kybernetický útok, který způsobil masivní únik dat. Vyšetřování ukázalo, že došlo ke zneužití privilegovaných účtů. Útočníci použili techniky pro eskalaci svých oprávnění a vystupovali v přestrojení za administrátory, aby získali citlivá data. [14]

1.5.6 Staré, nebo žádné zálohy

Pokud k útoku dojde, jsou zálohy doslova záchranou. Nedostatečná zálohovací politika, nebo zastaralé, nefunkční zálohy mohou znamenat katastrofu. V případě útoku může být návrat k běžnému stavu bez aktuálních záloh velmi náročný, nákladný a někdy i nemožný, což může mít za následek ztrátu důležitých dat a finanční ztráty. Ty se mohou vyšplhat až k desítkám milionů korun, jak tomu bylo v případě útoku na Ředitelství silnic a dálnic ČR v roce 2022. Útok způsobil výpadek webových stránek a dalších IT systémů. Důležitým aspektem řešení situace bylo rozhodnutí neplatit požadované výkupné a zaměřit se na obnovení systémů ze záloh. Celkové náklady spojené s touto obnovou nakonec vyčíslili na desítky milionů korun. [15]

2 SÍŤOVÁ INFRASTRUKTURA A SPRÁVA ÚČTŮ

Microsoft Windows organizační struktura je postavena na Active Directory. Společně s doménovým kontrolorem tvoří základní stavební kameny síťové infrastruktury organizace, která využívá implementaci organizace založené na technologiích Microsoft Windows.

2.1 Virtualizace

Virtualizace je klíčovou součástí počítačového prostředí již téměř půl století. V 60. a 70. letech společnost IBM vyvinula systémy Control Program/Cambridge Monitor Systém, které vedly k vývoji VM/370. Tyto systémy umožňovaly uživatelům spouštět izolovaně působící systémy na jednom sdíleném počítači s časově omezeným prostředím. Virtuální stroje jsou výrazným příkladem virtualizace. [16] Dnešní virtualizační technologie tvoří základ pro cloud computing. Tento vývoj umožňuje poskytovatelům cloudu nabízet širokou škálu služeb. Ty zahrnují virtuální servery, aplikace a úložiště, které jsou dostupné odkudkoliv a kdykoliv.

2.2 Struktura sítě Windows

Pro porozumění monitorování v síti Windows je důležité se seznámit s několika základními pojmy spojenými s infrastrukturou postavenou na AD. Tato část poskytuje přehled klíčových prvků, které hrají roli v síti Windows a jsou důležité pro správu a monitorování.

2.2.1 Koncová stanice

V kontextu této práce se jedná o koncová zařízení typu počítač s operačním systémem Windows 10/11, který je propojený s doménou na základě AD. Pokud je tedy zařazený do domény, umožňuje uživateli centrálně zajistit například práci s interním softwarem, přístup k dokumentům a sdílení informací prostřednictvím celé sítě organizace.

2.2.2 Server

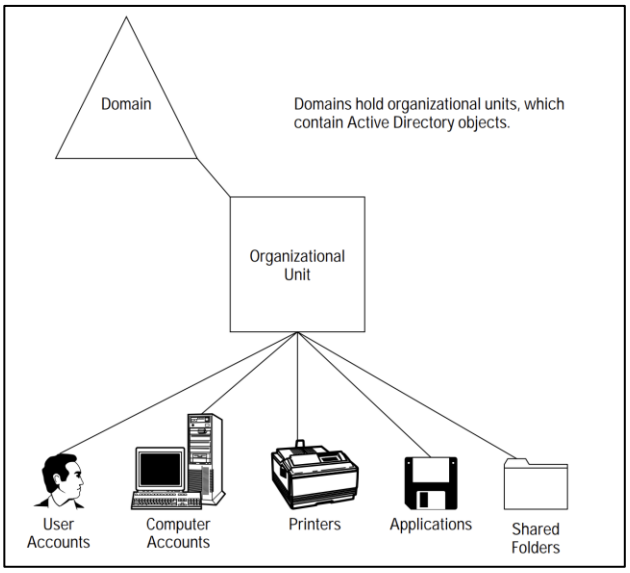
Server je počítačový systém, který poskytuje služby a zdroje pro ostatní zařízení v síti. V kontextu infrastruktury založené na AD jeden ze serverů plní roli doménového řadiče, což je speciální typ serveru, který spravuje a udržuje databázi AD obsahující informace o uživatelích, skupinách, počítačích a dalších objektech v síti. Odpovídá také za autentizační požadavky uživatelů a umožňuje jim přístup k síťovým zdrojům v organizaci.

2.2.3 Active Directory

Active Directory je adresářová služba, poskytující komplexní řešení pro organizované ukládání síťových zdrojů. Jedná se o databázi správy identit umožňující uchovávat informace o uživatelích, která obvykle běží na doménovém řadiči. [17]

2.2.4 Logická struktura AD

Domény v AD jsou organizovány do struktur zvaných doménové stromy. V organizaci může být těchto struktur několik. Doména obsahuje organizační jednotky (Organizational Units), ty drží důležité informace o uživatelích, počítačích, tiskárnách, či sdílených složkách. [17]



Obrázek 3. Logická struktura Active Directory [17]

2.2.5 LDAP

LDAP je založen na protokolu DAP (Directory Access Protocol), který byl implementací sítí X.500, což je standard popisující, jak se organizují a spravují informace v adresářové službě. Ta ukládá informace, jako jsou uživatelská jména, hesla, e-maily a další údaje o lidech a zařízeních. LDAP umožňuje provádět veškeré úpravy těchto objektů v AD. [17] LDAP může být náchylný k různým bezpečnostním rizikům, včetně injekčních útoků, při nichž útočník vkládá škodlivý kód do systému prostřednictvím například webových aplikací.

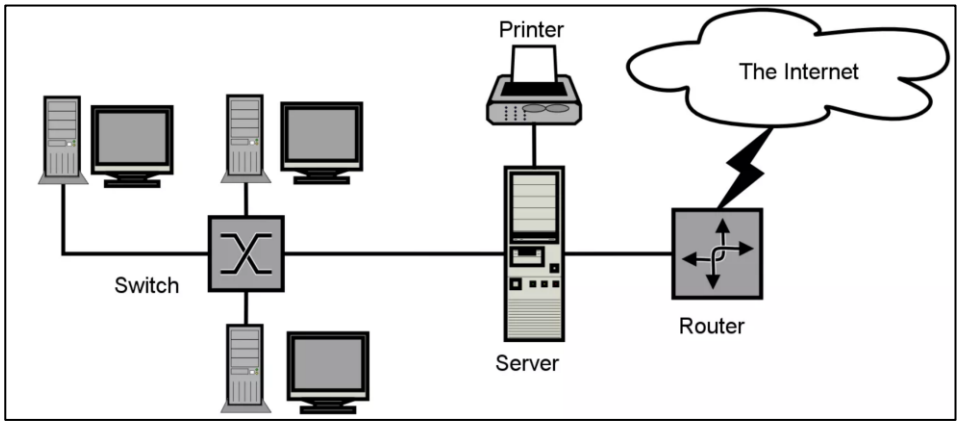
2.2.6 DNS

S Active Directory je úzce spojen pojem DNS. Ve skutečnosti nemůže být AD bez DNS funkční. Úkolem DNS služby je překlad IP adres na název, což je mimo jiné i princip

fungování dnešního internetu. Počítače se mezi sebou rozeznávají pomocí IP adres, lidé ovšem používají názvy, tedy řetězce. Aby tato komunikace fungovala hladce a rychle, DNS se stará o překlad názvu do IP adresy a zpět. V předchozích verzích systému Windows byla pro převod jména počítače na IP adresu používána síťová jména NetBIOS ve spojení se službou WINS (Windows Internet Name Service). [17] DNS v Active Directory slouží tedy také k překladu jmen počítačů a serverů na IP adresy a naopak. To umožňuje lidem i strojům v síti lokalizovat a komunikovat s ostatními zařízeními v síti.

2.2.7 Síť a její segregace

Síťová infrastruktura je klíčová pro efektivní provoz a komunikaci ve stávajících organizacích, a bez ní by bylo spravování AD bezpředmětné. Lokální síť neboli LAN, tvoří omezený prostor, ve kterém jsou umístěna všechna síťová zařízení, jako jsou servery, počítače a další síťové komponenty. Tato zařízení jsou schopná vzájemné komunikace. Struktura lokálních sítí je založená na referenčním modelu OSI, ale zároveň obsahuje specifika, která odlišují LAN od širších síťových struktur typu WAN. Zásadní charakteristikou LAN je možnost přímého propojení každého uzlu v síti s ostatními, což odstraňuje potřebu směrování dat prostřednictvím síťové vrstvy. [18]



Obrázek 4. Obrázek 5. Schéma LAN [19]

2.3 Účty a uživatelé Windows a oprávnění

Bezpečná a efektivní správa účtů je v dnešní době klíčová pro zajištění plynulého chodu počítačových systémů. V prostředí domény se pak počet účtů a připojených zařízení pohybuje v desítkách až stovkách, což zdůrazňuje důležitost obezřetného spravování účtů a jejich oprávnění. Následující kapitola se věnuje principům oprávnění a přístupového řízení, které

jsou zásadní pro správu přístupu k systémovým zdrojům a ochranu citlivých informací před neoprávněným přístupem.

2.3.1 Lokální účty

Lokální uživatelské účty na zařízeních Windows mají různé úrovně oprávnění a jsou definované přímo na jednotlivých počítačích. Každý počítač obsahuje administrátorský účet, který umožňuje uživateli plný přístup a správu systému. Existuje také systémový účet určený pro automatické operace systému (Default System Managed Account), který nemá interakci s koncovým uživatelem. Účet Guest, obvykle deaktivovaný pro zvýšení bezpečnosti, poskytuje omezený přístup pro občasné uživatele bez stálého účtu na počítači. Systémový účet, označovaný jako SYSTEM, je využívaný přímo operačním systémem a službami Windows a není viditelný a nelze ho přidat do uživatelských skupin. Network Service je lokální účet určený pro správu služeb a identifikaci pomocí vlastních přihlašovacích údajů při komunikaci s vzdálenými servery, což vyžaduje správné nastavení oprávnění pro bezpečnou operaci. Nakonec, Local Service je účet s minimálními oprávněními používaný pro spouštění služeb s cílem zajištění bezpečnosti a oddělení funkcí. Tyto účty hrají klíčovou roli ve správě a zabezpečení systému Windows, každý s jasně definovanou rolí a omezeními.[20]

2.3.2 Active Directory účty

Výchozí lokální účty jsou předdefinované účty, které jsou automaticky vytvořené při instalaci doménového řadiče systému Windows Server a při vytváření domény. Tyto účty jsou specifické pro celou doménu a existují nezávisle na ostatních lokálních uživatelských účtech. Jejich účel spočívá v poskytování základních oprávnění a služeb potřebných pro správu a provoz doménového řadiče a celého prostředí domény. Uživatelské účty v Active Directory jsou pak vytvářené pro jednotlivé uživatele v síti. Tyto účty umožňují uživatelům přihlásit se do domény, přistupovat k síťovým prostředkům a využívat různé služby a aplikace. [21]

2.3.3 Principy oprávnění a přístupového řízení

Principy oprávnění a přístupového řízení zahrnují několik klíčových konceptů a mechanismů, jako jsou ACL (Access Control Lists) a RBAC (Role-Based Access Control) případně i UAC (User Access Control). Tyto mechanismy jsou zásadní pro správu přístupu k systémovým zdrojům, jako jsou soubory, aplikace a databáze, a pro ochranu informací před neoprávněným přístupem.

2.3.4 Řízení přístupů

V rámci politiky řízení přístupu se musí definovat pravidla a postupy potřebné pro omezení a kontrolu používaného softwaru a hardwaru, který by mohl narušit systémovou a aplikační bezpečnost. [22] Jeden z konceptů, který popisuje řízení účtů se nazývá Principle of Least Privilege, který zdůrazňuje udělování uživatelům pouze těch oprávnění, která jsou nezbytná pro jejich práci. Identifikace uživatelů a jejich rolí je zásadní pro správnou definici přístupových práv v systému. Tyto role by měly být pečlivě stanovené na základě pracovních funkcí, odpovědností a potřebného přístupu k systémovým zdrojům.

2.3.5 ACL

ACL jsou tabulky, které vymezují, kterým uživatelům je povolený přístup k určitým objektům a jaké akce mohou s těmito objekty provádět. ACL jsou často používané v tradičních systémech DAC, kde vlastník zdroje rozhoduje o přístupových právech. [23] Nejčastěji je s nimi nakládáno v případě řešení přístupů ke sdíleným složkám na úrovní filesystému NTFS. Pomocí řízení přístupů ACL je možné určit, jakým skupinám, či uživatelům bude složka jak lokálně, tak i ve sdílené síti přístupná.

2.3.6 RBAC

RBAC (je metoda řízení přístupu založená na rolích, které jsou přiřazeny uživatelům. Tento model umožňuje efektivně spravovat oprávnění uživatelů tím, že je seskupuje do rolí na základě jejich pracovních funkcí nebo úkolů. [23] Například, pokladníci mohou mít přístup k pokladně a účetním souborům, zatímco manažeři mají přístup k finančním reportům a personálním údajům. Tímto způsobem se uživatelé přiřazují do rolí podle jejich pracovních funkcí, což usnadňuje správu oprávnění a zlepšuje bezpečnost systému.

2.3.7 UAC

Uživatelský účet řízení (UAC) snižuje riziko malware útoku tím, že omezuje schopnost škodlivého kódu spouštět se s administrátorskými oprávněními. Windows chrání procesy označováním jejich úrovní integrity. Úrovně integrity jsou měřením důvěry. Aplikace s vysokou integritou může být například softwarový firewall, který spravuje síťová pravidla a blokuje nebo povoluje přístup k síťovým prostředkům na základě definovaných pravidel. Taková aplikace má schopnost měnit konfigurační data a ovlivňovat chování systému, aby zajistila bezpečnost a ochranu sítě před neoprávněným přístupem nebo škodlivými útoky.

Aplikace s nižšími úrovněmi integrity nemohou modifikovat data v aplikacích s vyššími úrovněmi integrity. Když se standardní uživatel pokusí spustit aplikaci, která vyžaduje přístupový token správce, UAC vyžaduje, aby uživatel poskytl platné přihlašovací údaje. [24]

2.4 Vzdálený přístup RDP

Vzdálený přístup, často realizovaný pomocí protokolu Remote Desktop Protocol (RDP), umožňuje uživatelům připojit se ke vzdálenému počítači nebo serveru a pracovat s ním, jako by byl fyzicky přítomen u zařízení. Monitorování síťového provozu RDP (Remote Desktop Protokol) je zásadní z hlediska zajištění bezpečnosti a efektivity sítě. Pomáhá identifikovat neobvyklé aktivity, jako jsou podezřelé pokusy o přihlášení, neautorizované přístupy nebo neobvyklé objemy datového přenosu. V rámci této práce není monitoring RDP přímo zpracovaný, mohl by být zahrnutý v rozšířené verzi systému v rámci diplomové práce společně s analýzou sbíraných událostí. Řešením by mohl být například agent sledující provoz na portu 3389, případně s využitím jiného nástroje třetích stran pro zachycení a analýzu datových toků.

2.5 Logy

„Windows záznam událostí je nejdůležitějším zdrojem důkazů během digitálního forenzního vyšetřování Windows systému, protože záznamy událostí spojují určité události s konkrétním časovým bodem.“ [25] Logování hraje klíčovou roli v identifikaci zranitelností jak v aplikačním, tak v systémovém a bezpečnostním kontextu. Pravidelným prohlížením záznamu událostí může systémový administrátor identifikovat problémy předtím, než způsobí škodu. [26] Existuje několik typů událostí.

2.5.1 Error

Událost signalizující významný problém, který může ovlivnit provoz systému nebo aplikace. Například se jedná o selhání operací, výpadky služeb, selhání hardware, problémy se softwarem, neúspěšné pokusy o přístup k zabezpečeným zdrojům a další kritické události, které vyžadují okamžitou pozornost.

2.5.2 Info

Informační záznamy jsou používané pro zaznamenání rutinních operací a událostí, které neindikují žádný problém. Patří sem například úspěšné dokončení operace, zahájení nebo

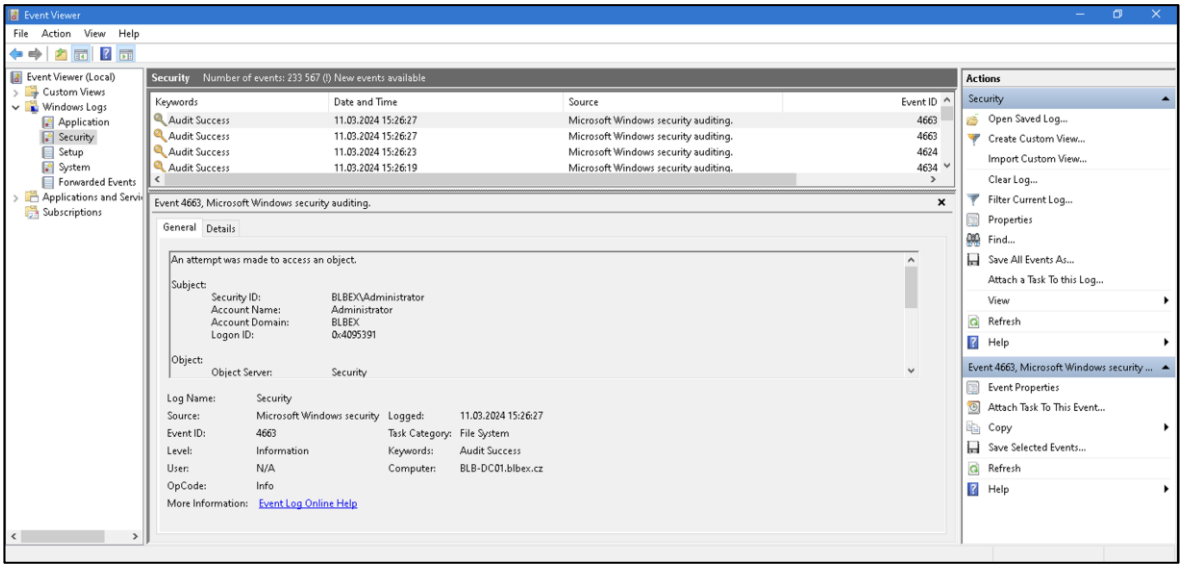
ukončení služby, nebo jiné události, které signalizují normální chod systému. Informační logy jsou užitečné pro potvrzení, že konfigurace a operace proběhly podle očekávání. Přesto, že neinformují o žádném problému, je důležité je sledovat. Monitorují totiž například korektní a autorizované přístupy do složek a její modifikaci, úspěšně provedená přihlášení uživatelů a další.

2.5.3 Warning

Jedná se o události, které nejsou kritické, ale mohou mít i vážné následky, a tak je potřeba zasáhnout. Varování mohou zahrnovat například dočasné nedostatky zdrojů, konfigurační nastavení, které nejsou optimální, nebo neobvyklé, ale ne nezbytně škodlivé aktivity. Cílem logování těch to událostí je upozornit administrátory, aby mohli provést preventivní opatření a zabránit tak možným budoucím problémům.

2.5.4 Event Log

Windows logy se nachází ve Správci událostí (Event Viewer), a logy rozděluje do několika kategorií.



Obrázek 5. Prohlížeč události systému Windows

2.5.4.1 Aplikační log

Zaznamenává události vytvořené aplikacemi, které jsou nainstalované na počítači. Mohou obsahovat informace o chybách aplikace, informace o spuštění nebo ukončení a jiné významné události související s aplikacemi.

2.5.4.2 Systémové logy

Obsahují informace a události generované operačním systémem Windows a jeho komponentami, jako jsou ovladače zařízení a vestavěné systémové služby. Tyto logy mohou zahrnovat události, jako jsou chyby systému, varování, informace o spuštění a vypnutí systému a problémy s hardwarem.

2.5.4.3 Logy zabezpečení

Evidují události související se zabezpečením, jako jsou pokusy o přihlášení, změny oprávnění, použití skupinových politik a další bezpečnostní události. Tyto logy jsou klíčové pro sledování a analýzu bezpečnosti systému. V rámci této bakalářské práce probíhá monitoring právě těchto událostí.

2.5.4.4 Setup logy

Zaznamenávají události, jako jsou spuštění instalačních programů, detekce a vyřešení konfliktů během instalace, změny v systémových konfiguracích provedené instalátorem a další související události. Záznamy tohoto typu jsou užitečné pro diagnostiku a řešení problémů s instalací softwaru a sledování změn v konfiguraci systému.

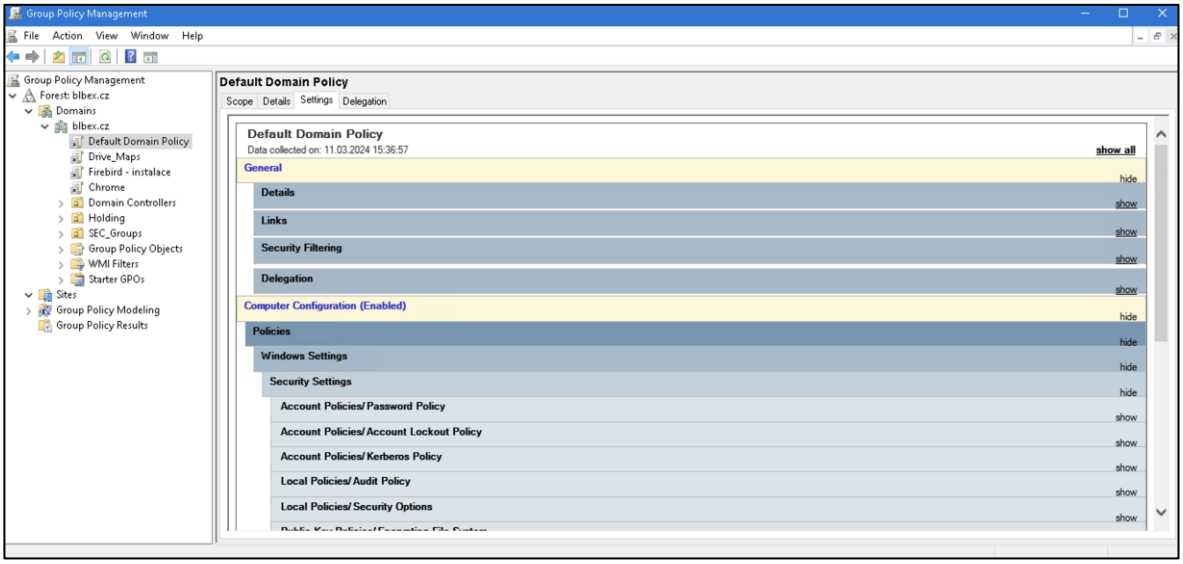
2.6 Politiky systému Windows

Základem pro centralizovanou správu počítačů v doméně jsou skupinové politiky (Group Policy), které umožňují řídit nastavení, bezpečnost a chování pracovních stanic a serverů. [27] Active Directory poskytuje hierarchickou strukturu, která uspořádává GPO politiky, což usnadňuje vyhodnocování a aplikaci správy. Pro správu skupinových politik se používá Group Policy Management konzole, která může být nainstalovaná buď na doménovém řadiči, nebo na samostatném systému určeném pro správu domény. K tomu slouží Remote Server Administrator Tools, což je sada nástrojů vyvinutých společností Microsoft, umožňující správu vzdálených serverů z jakéhokoli počítače s operačním systémem Windows.

2.6.1 GPO

Jedná se o virtuální objekty, které mají své GUID a jsou uložené na úrovni domény v GPC kontejnerech a GPT předlohách. Skupinové politiky se uplatňují v určitém pořadí s tím, že v první vrstvou je místní úroveň (Local Policy), které je nadřazená síťová úroveň (Site Level Policy) a následuje doménová úroveň (Domain Level) a nakonec vnořená politika

jednotlivých organizačních jednotek AD. Politiky na vyšší úrovni mají vyšší prioritu a jejich nastavení přepíše nastavení na nižší úrovni, pokud jsou v rozporu. Tento koncept umožňuje hierarchické řízení nastavení.[28]



Obrázek 6. GPO management konzole pro správu politik

2.6.2 GPC

Jedná se o kontejner, který drží informace o aplikovaných skupinových politikách pro danou doménu nebo organizační jednotku. GPC (Group Policy Container) umožňuje centrální správu a distribuci konfigurací politik v rámci síťové infrastruktury založené na AD. Každé GPO je pak přiřazeno ke GPC, který určuje, kde a jak jsou tyto politiky v síti aplikované. [28]

2.6.3 GPT

GPT (Group Policy Template) je složka souborového systému, která obsahuje datové informace o politikách specifikovaných soubory s příponou „.adm“, resp. “admx”, nastavení zabezpečení, skriptovací soubory a informace o aplikacích, které jsou k dispozici k instalaci. GPT se nachází ve složce systémového svazku, tedy v souboru SYSVOL. [28]

2.7 Firewall

Firewall je klíčovým prvkem zabezpečení počítačové sítě, jehož hlavním účelem je chránit interní síť před neoprávněným přístupem a škodlivými útoky z vnějšího prostředí, tedy z internetu. Virtuální firewall implementovaný pomocí open-source softwaru PfSense

poskytuje efektivní ochranu sítě prostřednictvím analýzy a řízení toku dat. Firewall sleduje síťový provoz a vytváří komplexní pravidla pro filtrování a řízení přístupu dat. Tímto způsobem může identifikovat potenciálně nebezpečné komunikace a reagovat na ně odpovídajícím způsobem. Například blokováním přístupu nebo vytvořením bezpečných zón v síti. Díky virtuální implementaci v rámci této práce je možné firewall snadno spravovat a konfigurovat bez nutnosti fyzického hardwaru. To umožňuje flexibilitu při přizpůsobování firewallu specifickým potřebám a požadavkům sítě. Také lze snadno provádět testování a ladění konfigurace bez výrazných nákladů na hardware či reálné prostředky.

3 MONITORING

Pro zaznamenání událostí souvisejících s činností uživatelů lze využít procesů logování nebo auditování (formální název prostředí Windows). Existuje několik integrovaných nástrojů a metod, které umožňují sledování uživatelů v síti. Záznamy poskytují základní, ale v mnoha ohledech efektivní a ekonomickou alternativu k implementaci drahých systémů detekce, které vyžadují například nasazení agentů. Pro sběr záznamů systému Windows je třeba definovat, které typy systémových objektů budou sledované (soubory, registry, přihlášení), jaké akce na těchto objektech budou zaznamenány (čtení, zápis, změny oprávnění apod.) a kdo bude monitorován (uživatelé, systém, všichni atd.). [29]

3.1 Logy událostí zabezpečení

Logy událostí zabezpečení Windows (Windows Security Audit), poskytují informace o aktivitách, které mohou pomoci identifikovat neobvyklou činnost, což naznačuje možný neoprávněný přístup k systémům nebo síťovým zařízením. Microsoft vyvinul funkci auditu zabezpečení Windows, která umožňuje sledování uživatelských aktivit, provádění forenzní analýzy a vyšetřování incidentů. [30] Existují dva typy těchto logů, přístup povolen (Audit Success) a přístup odepřen (Audit Failure) nastavit se přitom dají dva typy auditních politik, a to základní audit (Basic Security Audit) a rozšířený (Advanced Security Audit). Základní audit bezpečnosti, kterou Windows nazývá Basic Security Audit, definuje kategorie bezpečnostních událostí, které lze sledovat v systému Windows, čemuž se věnuje následující kapitola.

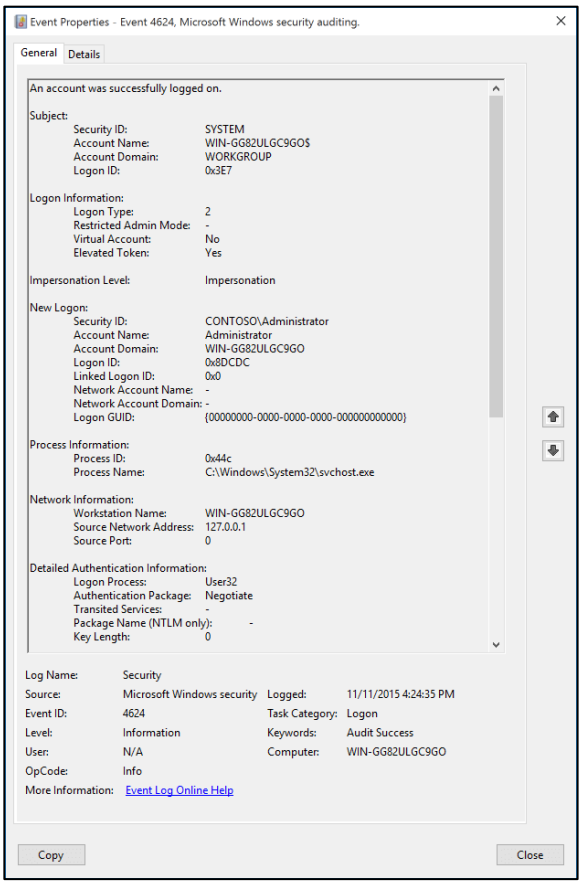
V této práci jsou v kontextu výkladu použita slova 'monitoring' nebo 'sledování' místo slova 'audit', aby nedošlo k záměně významu slova 'audit' z hlediska právní terminologie.

3.1.1 Audit událostí přihlášení uživatelů

Monitoring události přihlášení uživatelů (Audit Account Logon Events) je způsob, který zaznamenává každou instanci přihlášení nebo odhlášení bezpečnostního subjektu (například uživatele, počítače nebo účtu služsby), který se přihlašuje nebo odhlašuje z jednoho počítače, když je použit jiný počítač k ověření účtu. [31] Pokud je aktivní toto nastavení, systém bude sledovat, když se uživatel přihlásí na jiném zařízení pomocí svého účtu a toto zařízení použije aktuální zařízení (například doménový kontrolér) k ověření tohoto účtu. [32]

3.1.2 Audit přihlašovacích událostí

Sledování přihlašovacích událostí (Audit Logon Events) přináší úspěšné a neúspěšné pokusy o přihlášení nebo odhlášení z lokálního počítače. Což může být užitečné pro detekci útočníků a forenzní analýzu po incidentu. Lze pak sledovat události s Event ID 4624 - Uživatel úspěšně přihlášen k počítači, či Event ID 4625 - Neúspěch přihlášení. Pokus o přihlášení byl provedený s neznámým uživatelským jménem nebo s známým uživatelským jménem a špatným heslem.



Obrázek 7. Událost přihlášení uživatele [33]

Události přihlášení se generují na řadičích domény pro aktivitu účtů v doméně a na místních zařízeních pro aktivitu místních účtů. Při nastavování je možné specifikovat, jestli chceme monitorovat úspěšné přihlášení, nebo neúspěšné. Po nastavení politiky lze sledovat několik událostí, jako například, jestli se uživatel přihlásil úspěšně, zda použil přesně určené (explicitní) přihlášení, nebo se naopak odpojil od terminálového serveru bez odhlášení. [30]

Logon events	Description
4624	A user successfully logged on to a computer. For information about the type of logon, see the Logon Types table below.
4625	Logon failure. A logon attempt was made with an unknown user name or a known user name with a bad password.
4634	The logoff process was completed for a user.
4647	A user initiated the logoff process.
4648	A user successfully logged on to a computer using explicit credentials while already logged on as a different user.
4779	A user disconnected a terminal server session without logging off.

Obrázek 8. Přehled auditních událostí [34]

3.1.3 Audit správy uživatelských účtů

Možnost sledování správy uživatelských účtů (Audit Account Management) určuje, zda se sleduje aktivita související s uživatelskými účty a skupinami. Například zda došlo k vytvoření, smazání nebo změně uživatele, či účtu. Případně generuje i události, pokud došlo k zakázání, nebo povolení uživatelského účtu. Události spojené s monitorováním správy uživatelských účtů v systému [31]

3.1.4 Audit přístupu k službám adresářů

Tento proces zahrnuje systematické sledování a záznam úkonů a událostí spojených s přístupem k adresářovým službám, jako jsou například AD nebo LDAP.

3.1.5 Audit přístupu k objektům

Generuje události v momentě, kdy uživatel přistupuje k objektu, například k souboru, složce, klíči v registru, tiskárně a podobně, který má svůj vlastní seznam řízení přístupu systému specifikovaný. Monitoring přístupů k objektům (Audit Object Access) může generovat události, pokud jsou následně definované objekty s povoleným přístupem ke sledování. [35]

3.1.6 Audit změn politiky

Sledování změn politik (Auditing Policy Change), určuje, zda monitorovat každý případ změny v přiřazení uživatelských práv, politikách Windows Firewall, důvěrných politikách nebo změnách v politice. [31]

3.1.7 Audit oprávnění

Monitoring oprávnění (Audit Privilege Use) je nastavení politiky, které určuje, zda se mají zaznamenávat veškeré případy, kdy je využíváno uživatelské právo nebo oprávnění. Jinými slovy, tato funkce sleduje každou událost, kdy uživatel využívá své privilegia nebo oprávnění v systému. [31]

3.1.8 Audit sledování procesů

Monitoring sledování procesů (Audit Process Tracking). Toto nastavení politiky určuje, zda sledovat podrobné informace o sledování procesů, jako jsou aktivace programu, ukončení procesu, duplikace handle a nepřímý přístup k objektům. Je užitečné pro sledování škodlivých uživatelů a programů, které používají. [31]

3.1.9 Rozšířené politiky

Každá hlavní kategorie má svou podkategorii, tedy rozšíření politik (Advacne Audit Policy), které umožňují provádět monitoring mnohem podrobněji, než by bylo možné pouze pomocí hlavních kategorií. Případně lze povolit pouze určité způsoby monitoringu a tím lépe určovat, jaké události jsou pro sledování v dané organizaci relevantní. [31] Jedním z možných nastavení v rámci rozšířené politiky je sledování událostí souvisejících s filesystémem a manipulací s ním.

3.2 Doporučení pro monitoring

Nastavení monitorovacích politik je závislé na potřebách dané organizace. Přestože existují základní doporučení, nelze aplikovat žádné univerzální řešení pro všechny. Doporučení pro běžné počítače použité v podnikání, které Microsoft definuje jako počítače s průměrnými požadavky na zabezpečení, vyžadují vysokou úroveň provozní funkčnosti. Entity potřebující vyšší požadavky na zabezpečení by měly zvážit agresivnější politiky v prostředí Windows. Častou chybou je pouze monitorovat servery nebo řadiče domény. Útok totiž obvykle začíná právě na pracovních stanicích a ignorování monitorování pracovních stanic tak znamená opomíjení nejlepšího a nejčasnějšího zdroje informací. Největší pozornost by měly vzbudit právě ty události, které naznačují, že došlo k hrubým porušením pravidel, nebo ty, které mají zásadní změnu trendu v počtu výskytů. Příkladem může být přihlášení uživatele na počítač, na který by neměl mít přístup, nebo neustálé generování události o selhání přihlášení, což by mohlo naznačovat útok. [36]

3.3 Přehled technik a nástrojů pro monitorování

Kromě nativních nástrojů operačního systému Windows existuje mnoho dalších technik a nástrojů pro monitorování událostních záznamů a reakci na bezpečnostní hrozby. Mezi ně patří specializované softwarové aplikace, open-source řešení a vlastní vyvinuté skripty a systémy. Tyto nástroje nabízejí různé funkce, jako je sledování síťového provozu, detekce anomálií, analýza chování uživatelů nebo monitorování aplikací a služeb.

3.3.1 Nativní nástroje

Microsoft nabízí hned několik základních nástrojů pro monitoring a správu událostí v systému. Pro sledování procesů lze využít správce úloh (Task Manager) a správce prostředků (Resource Manager), které umožňují efektivní správu a monitoring systémových či hardwarových prostředků. Správce událostí nabízí (Event Viewer) nabízí možnost procházení událostí v celém systému. Pro automatizaci a monitoring lze použít i pokročilé skriptování pomocí Powershellu či jiného programovacího jazyka.

3.3.2 Řešení třetích stran

Softwary třetích stran mohou být řešením pro efektivní monitoring a zabezpečení IT infrastruktury ve firmách. Tyto systémy umožňují sledování, sběr a analýzu dat, která jsou nezbytná pro identifikaci a reakci na potenciální bezpečnostní hrozby a incidenty. Mezi těmito nástroji je SIEM (Security Information and Event Management), který poskytuje komplexní řešení pro analýzu a reakci na bezpečnostní události v reálném čase, což firmám umožňuje efektivně čelit kybernetickým hrozbám. Na druhé straně Syslog server se primárně zaměřuje na sběr a archivaci logů z různých zařízení, což usnadňuje monitorování událostí. Dalším důležitým nástrojem je software jako Zabbix, který se soustředí na sledování výkonnosti a dostupnosti IT komponent, poskytující detailní analýzu a optimalizaci systémového provozu.

3.3.3 Protokoly a způsoby komunikace mezi vzdálenými systémy

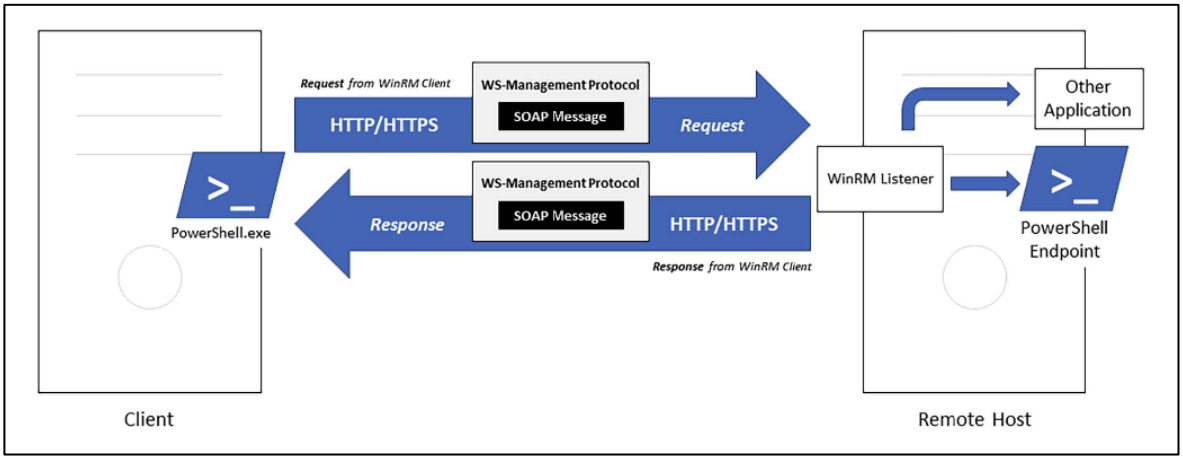
Existují specializované nástroje pro správu, jako jsou Sysinternals, framework WMI, či speciální knihovny Powershellu. Umožňují spouštění operací vzdáleně, vyžadují však komplexnější znalosti v dané oblasti. Různé nástroje ovšem přistupují k vzdálené správě odlišně, používají jiné protokoly, byť v mnoha ohledech spolu mohou spolupracovat.

Remote Connection Method	Protocol Used
PowerShell Remoting via WinRM (default)	WS-Management
WMI	DCOM/RPC
CIM Cmdlets	WS-Management
SSH Remoting	SSH

Obrázek 9. Přehled připojovacích metod a používaných protokolů [38]

3.3.3.1 WinRM

Windows Remote Management (WinRM) je implementace protokolu WS-Management, což je standardní protokol založený na jednoduchém protokolu přístupu k objektům (SOAP). Pro získání správných dat z lokálních a vzdálených počítačů, lze použít objekty skriptování WinRM, nebo nástroj příkazového řádku Windows Remote Shell. [39] Například ve výchozím nastavení PSRemoting používá jako transportní protokol právě WinRM. [38]



Obrázek 10. Schéma použití WinRM a WS-Management s PSRemoting [38]

3.3.3.2 WMI

Windows Management Instrumentation (WMI) je framework pro správu dat a operací v operačních systémech založených na platformě Windows. Mnoho správců a IT profesionálů přistupuje k WMI prostřednictvím nástroje Windows PowerShell. [40] Používá DCOM/RPC komunikační protokoly. Je třeba si ale uvědomit, že příkazy Powershellu pro práci s WMI jsou od verze PowerShell Core 6 označené jako zastaralé a neměly by být používané v novějších verzích PowerShell. Což ale neznamená, že nejsou v současné době podporované v určitých starších verzích, jako je například PowerShell 5.1 na Windows 10, a budou nadále

využívané po dobu podpory těchto operačních systémů. Pokud je to ale možné, doporučuje se místo nich používat novější cmdlety pro práci s CIM, protože mohou být použité na operačních systémech Windows i mimo ně. [38]

3.3.3.3 Sysinternals

Sysinternals je kolekce nástrojů pro správu a diagnostiku systému Windows. Nástroje Sysinternals pomáhají při řešení potíží, diagnostice, výkonu a optimalizaci systému. Umožňují uživatelům hluboký náhled a kontrolu nad svými systémy založenými na Windows. Jedním z nástrojů je i PsExec. Jedná se o lehkou náhradu za Telnet, která umožňuje provádět procesy na jiných systémech s plnou interaktivitou pro konzolové aplikace, aniž by bylo třeba na daného klienta manuálně instalovat software. [41]

3.3.3.4 PowerShell Remote Control

PowerShell je skriptovací rámec a příkazová řádka postavená na .NET. Je implementovaný ve výchozím nastavení v operačních systémech Windows a založený na objektech, což znamená, že vše, s čím se pracuje (například proměnné, vstupy a další), má vlastnosti a metody. To otevírá mnoho možností při práci s PowerShell. [38] Relace PowerShell Remoting jsou v základu povolené jen pro administrátory a spouští je pod kontextem uživatele. Jedná se o funkce v PowerShellu, které umožňují správci ovládat a provádět příkazy na vzdálených počítačích pomocí síťového připojení. To znamená, že příkazy a skripty lze spouštět na vzdálených počítačích a získat výsledky zpět na svůj lokální počítač. V závislosti na velikosti organizace, lze PSRemoting povolit několika způsoby.

Action	Enable-PSRemoting	Group Policy	Manual Configuration
Set the WinRM to Auto-Start	Yes	Yes	Yes
Configure HTTP Listener	Yes	Yes *(No Custom Listeners)*	Yes
Configure HTTPS Listener	No	No	Yes
Configure Endpoints	Yes	No	Yes
Configure Firewall	Yes	Yes	Yes

Obrázek 11. Metody nastavení PSRemotingu [38]

3.3.3.5 CIM

WMI je implementace společnosti Microsoft pro Common Information Model (CIM) a definuje, jak jsou prvky IT systému reprezentované jako objekty a jak se vzájemně propojují. To by mělo nabídnout dobrý způsob správy IT systémů, bez ohledu na výrobce nebo platformu. CIM příkazy jsou tedy novější náhradou známých, zastaralých, ale v některých systémech stále používaných WMI příkazů. [38] Umožňují provádět operace jako získávání informací o hardwaru a softwaru, správu služeb a procesů a mnoho dalšího.

3.3.3.6 Agent-based řešení

Jedná se o speciální typ řešení monitoringu pomocí samostatně fungujících agentů, kteří jsou instalovaní na koncových stanicích a mají specifické role. Mohou být velmi flexibilní a napsané na míru tomu, co organizace potřebuje. Ať už se jedná o monitoring sítě, koncových stanic, či dílčích úkonů. Může komunikovat s centrálním systémem pomocí HTTPS (Hypertext Transfer Protocol Secure), ale i jiným způsobem, záleží na přístupu k řešení. Jelikož se jedná ve většině případů instalovaný software, vyžaduje také údržbu a patch management.

3.3.3.7 Administrativní sdílení

Administrativní sdílení jsou výchozí sdílení každého pevného disku na počítači v síti. Umožňují místním správcům spravovat více počítačů a přistupovat k diskům a složkám na vzdálených počítačích, aniž by tyto vzdálené disky byly explicitně sdílené. Ve výpisu sdílených souborů lze tyto poznat pomocí přidaného dolaru na konci názvu. Jedná se o Admin$, což je vzdálený správce, C$ je sdílený systémový disk, IPC$ se používá ke komunikaci s programy a například Print$ je publikovaný při sdílení tiskárny.

3.3.4 Invoke-ADEnum nástroj

Sběr informací z AD může být v první fázi seznámení se s firemním prostředním velký pomocník. Invoke-ADEnum je nástroj vývojářů z Github repositáře a nabízí už vyvinutý nástroj pro enumeraci AD s využitím funkcí PowerView. Umožňuje rychlou a efektivní enumeraci AD, včetně domén, důvěryhodných vztahů, řadičů domény, uživatelů, skupin, počítačů, sdílených složek, podsítí, ACL, organizačních jednotek, GPO a dalších. Mimo jiné nástroj nabízí generování zpráv ve formátu HTML (Hypertext Markup Language). [42] Pokrývá tedy velmi širokou škálu informací z AD, pro svou jednoduchou použitelnost byl v mé práci upřednostněný před vlastním enumeračním řešením pomocí jiných technik.

3.3.5 Informace o hardware a operačním systému

Informace o hardwaru, operačních systémech, IP adresách a posledních restartech jsou klíčové pro správu sítě. Tato data umožňují také rychle identifikovat zranitelná zařízení, která nemají nejnovější aktualizace a plánovat potřebné údržby. Což, jak už bylo zmíněné v několika případech útoků na začátku této práce, je velmi důležitou částí v obraně proti kybernetickým hrozbám. Poslouží také v obecném přehledu, jaký hardware, počítače a jejich IP adresy v síti vůbec jsou.

3.4 Ukládání logů a událostí ze stanic

Při ukládání logů a bezpečnostních dat se nabízí několik typů databázových systémů, či řešení, z nichž každý má své specifické vlastnosti a nejvhodnější využití závisí na konkrétních potřebách organizace. Pro potřeby bakalářské práce byl vybraný OpenSearch.

3.4.1 OpenSearch

OpenSearch je open-source vyhledávací a analytický nástroj založený na Apache Lucene, který nabízí širokou škálu funkcí pro práci s daty. Není vhodný jen pro použití jako backend pro vyhledávací aplikace, ale také pro analýzu logů. V případě logování lze tedy získat události z aplikace, či systému a vložit je všechny do OpenSearch. [43] Jedná se o systém NoSQL databáze, SQL dotazy jsou částečně podporované. Hlavní výhodou je, že dokáže pracovat s daty různého typu, délky a návaznosti na sebe. Lze v něm tedy držet variabilní data s různou strukturou, což je v rámci práce s logy a měnícími se zdroji informací klíčové. Primárním dotazovacím jazykem pro OpenSearch je pak DSL, který je zvolený v této práci pro svoji jednoduchost a podobnost JSON formátu. Lze se setkat ale i s využitím dotazovacích jazyků jako jsou SQL, který je částečně podporovaný.

3.4.1.1 Indexace

OpenSearch uspořádává data do indexů, které obsahují kolekci dat formátu JSON. Indexy také zahrnují mapování a nastavení. Mapování definuje pole, která dokumenty v indexu obsahují, zatímco nastavení obsahuje informace jako název indexu, datum vytvoření a počet fragmentů. [43]

3.4.1.2 OpenSearch Dashboard

Umožňuje vizualizaci dat v OpenSearch databázi. Pomocí vyhledávacího pole v záložkách Discover a Dashboard lze vyhledávat data. Existuje více jazyků pro dotazování: DQL a Lucene. DQL umožňuje použití hvězdičky (wildcard), rozsahů, logických operací a dotazů na vnořená pole. Jazyk Lucene obsahuje regulární výrazy, fuzzy vyhledávání, dotazy na blízkost a zvýhodňování.[43]

3.4.2 Logstash

Logstash je open-source program, kterým lze načítat data z mnoha zdrojů a dále podle potřeby transformovat a odesílat dál. V případě této práce je odesílá přímo do OpenSearch databáze, a to bez ohledu na formát nebo složitost. Z neuspořádaných dat odvozuje strukturu například pomocí filtru Grok, dešifruje geografické souřadnice z IP adres, nebo modifikuje názvy a pole a usnadňuje celkové zpracování. [44] Logstash má ve své konfiguraci tři důležité části. Jednou z nich je input, který se stará o zisk dat zvenčí, například na základě naslouchání na určitých portech. V případě logů z přístrojů a síťových zařízení lze totiž použít formu syslogu, který očekává data ve formátu RFC3164. Poskytuje pak předem definované typy dat, jako například port, timezone a jiné. [48] Další částí jsou tak zvané filtry, tedy způsoby zpracování v rámci pipeline Logstash. Lze je kombinovat s podmínkami a provést akci na události, pokud splňují určitá kritéria. Poté, co jsou data filtrem zpracovaná, jdou do OpenSearch databáze. V sekci output je možné opět použít logiku podmínek. Každý typ logu má své zpracování a dynamicky přidělený název indexu. V případě problémů existuje způsob debugu pomocí `stdout rubydebug`, který při spuštění vypisuje jednotlivé JSON formáty logů ukládaných do OpenSearche.

3.4.3 Winlogbeat

Winlogbeat je nástroj pro přenášení Windows událostí do OpenSearch, či Logstash a může být nainstalovaný jako služba ve Windows. Čte data z jednoho nebo více logů pomocí Windows API (Application Programming Interface), následně je filtruje podle kritérií konfigurovaných uživatelem a odesílá je dál. [45] Umožňuje tak sběr bezpečnostních logů bez potřeby přeposílání logů z jednoho na druhý počítač (Event Forward). Lze ho nastavit dle potřeb organizace, může tak sbírat jen předem určená data. Vyžaduje však samostatnou instalaci na jednotlivé stanice. Obdobně jako Winlogbeat, i služba Event Forwarding může přenášet logy, ale vznikají potíže, zejména při odesílání bezpečnostních logů (Security Logs).

Nastavení pro přeposílání těchto logů může vyžadovat úpravy v registrech a kvůli přenosu rozsáhlých dat existuje možnost, že bude docházet k problémům s latencí. Například jednou z výhod Winlogbeat je jeho schopnost ignorovat starší logy a specifikovat konkrétní ID událostí k monitorování přímo v konfiguraci.

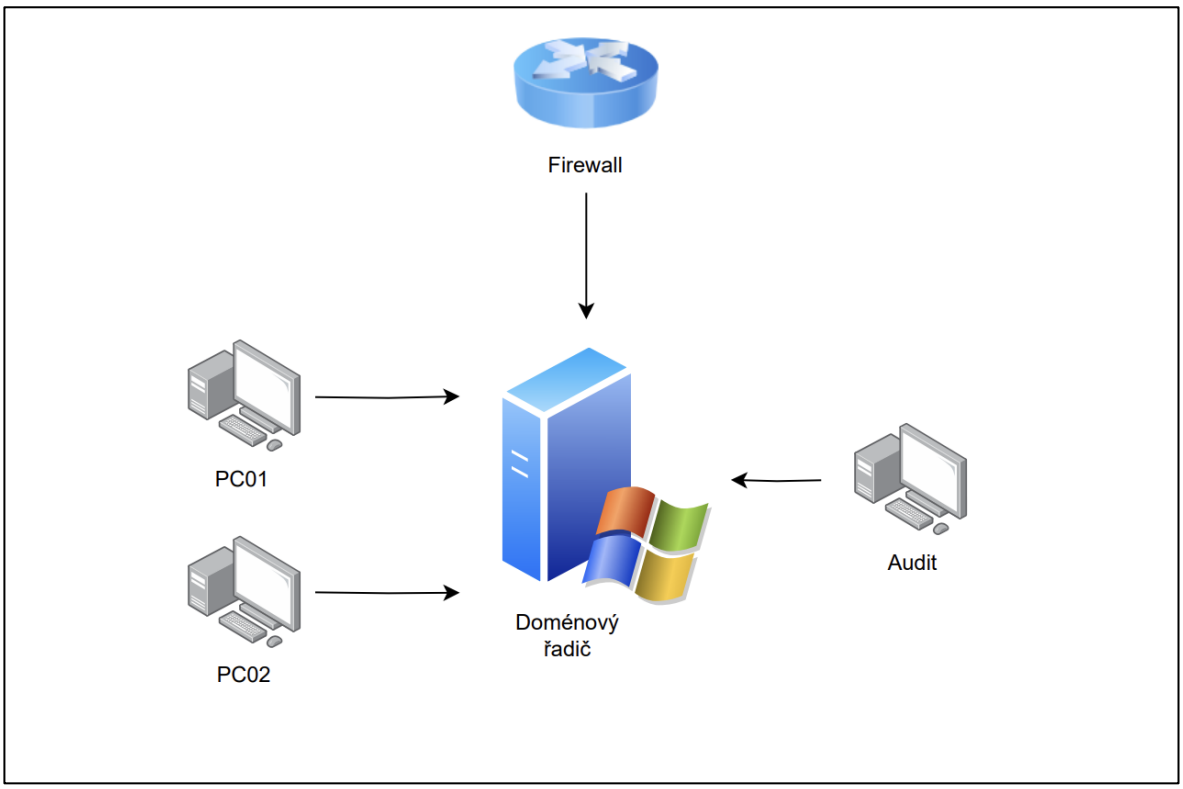
3.5 Právní a etické aspekty monitorování dat

Monitoring zaměstnanců a pracovníků organizace je velmi citlivé téma, a ne každý postup je v souladu se zákonem. Zejména se musí dbát na dodržení podmínek uvedených v zákoníku práce. Zákoník práce stanovuje, že zaměstnanci nemohou používat pracovní nástroje jako počítače nebo telefony pro své soukromé účely bez souhlasu svého zaměstnavatele. Zaměstnavatel má právo kontrolovat dodržování tohoto pravidla, ale nesmí bez vážného důvodu narušovat soukromí zaměstnanců na pracovišti, například sledováním jejich telefonních hovorů nebo čtením jejich emailů, pokud k tomu není dobrý důvod, jako je zvláštní povaha práce. Pokud je takový důvod, zaměstnavatel musí zaměstnance informovat o rozsahu kontroly a způsobech provádění této kontroly. [46] Etická stránka monitoringu vyžaduje jasné informování všech uživatelů a hlavně jejich souhlas. Monitoring jakékoliv činnosti bez vědomí uživatele je nezákonný. Organizace tak musí zpracovat politiky, které budou tyto činnosti jasně popisovat a vysvětlovat zejména důvod celého monitoringu, který by měl být prováděn jen v krajních nezbytných situacích. V této práci je použitý zejména kontroverzní monitoring historie ve vyhledávači. Uživatelé by měli ke své práci v rámci politik firmy používat výhradně prohlížeč Microsoft Edge. Ke svým osobním účelům mají pak možnost mít jiné prohlížeče, a právě monitoring historie Edge prohlížeče je do monitoringu zahrnuta. Hlavní důvod vyplývá z detekce a prevence potenciálně nebezpečných situací, jako je škodlivý hacking, útoky na síť nebo šíření škodlivého softwaru. Analyzování historie prohlížeče může pomoci identifikovat podezřelé vzory chování, jako je neobvyklé stažení souborů, přístup k podezřelým webovým stránkám nebo pochybné komunikace. Identifikace přístupu k citlivým dokumentům nebo webovým stránkám může pomoci minimalizovat riziko úniku dat nebo nedovoleného přístupu. Může sloužit také k ověření, zda zaměstnanci dodržují stanovená pravidla v oblasti bezpečnosti dat. Data z prohlížeče jsou v rámci řešení představeného v této práci anonymizovaná. Při monitoringu je tedy možné zjistit navštívené IP adresy a čas, případně zhruba určit, odkud IP adresa pochází. Nelze však přímo zjistit, jaké stránky uživatel navštívil. Každý uživatel musí být o monitoringu informovaný předem.

II. PRAKTICKÁ ČÁST

4 AKTUÁLNÍ STAV FIRMY

Struktura testovacího prostředí je založená na technologiích Microsoft Windows, což je hlavním kritériem celého projektu. Jedná se o prostředí bez předchozích nastavení a s minimálním provozem uživatelů, což má zajistit přehlednost výsledků a ověřit důvěryhodnost monitorovaných dat. Tato laboratoř je tedy nainstalovaná tak, jak je to běžné u skutečných zákazníků. Důvodem je, že testování a zkoušení nenarušuje integritu a chod sítě u žádného skutečného zákazníka. Nelze si dovolit manipulovat s nastavení GPO, firewally či doménovými řadiči u zákazníků pro experimentální účely. Nehledě na to, že v živé síti je velmi vysoký ruch, který by mohl zkreslit výsledky a snížil by účinnost testování dat.



Obrázek 12. Rozvržení sítě testovacího prostředí

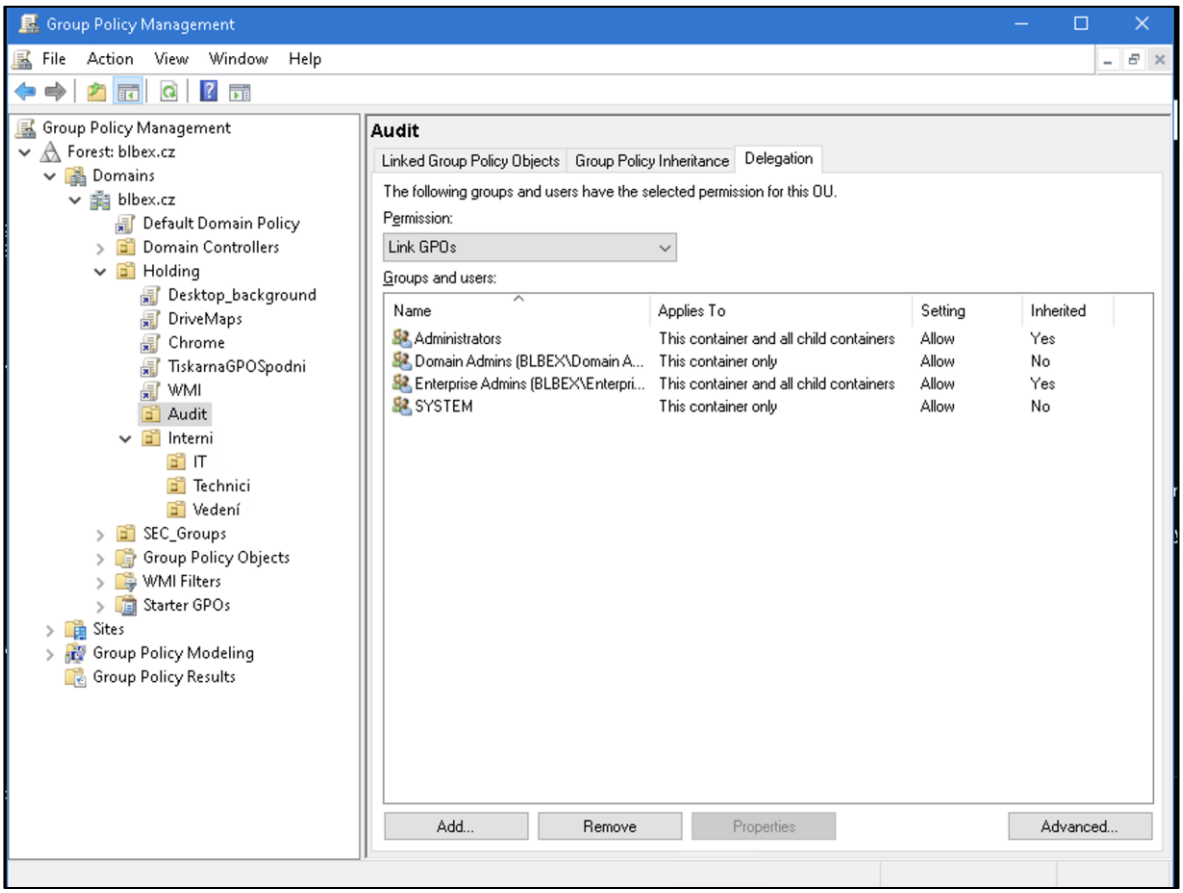
4.1 Servery a stanice

Virtuální počítače a servery jsou v základním stavu. Tento přístup zajišťuje přesnou simulaci potřebných konfigurací na čistém systému. Díky virtualizaci VMware lze rychle nasadit a flexibilně spravovat celou síť bez nutnosti fyzické infrastruktury. Laboratoř zahrnuje také virtuální firewall s open-source softwarem PfSense, jehož funkce odpovídají klasickému hardwarovému řešení. Tyto prvky patří mezi běžné komponenty implementované u

zákazníků firmy. Následující kapitola se věnuje nastavení domény, serverů a celé sítě, včetně začlenění auditního počítače.

4.1.1 Doménový řadič

Základním prvkem sítě testovací laboratoře je doménový řadič, který umožňuje nastavení politik, monitoringu a centrální správy uživatelů a počítačů v síti. Tento řadič také slouží jako filesystém pro sdílení souborů a složek v síti. Po instalaci serveru a přiřazení role doménového řadiče vzniká hierarchická struktura podniku, kterou lze spravovat pomocí Nástroje pro správu uživatelů, skupin, počítačů a dalších objektů v Active Directory (Active Directory Users and Computers). Testovací prostředí se skládá z organizačních jednotek interních uživatelů, jako je vedení a technici, a speciální skupiny Audit, do které patří uživatel určený speciálně pro monitoring. Doménový řadič zatím nemá nastavené žádné politiky GPO.



Obrázek 13. Přehled AD struktury testovacího prostředí

4.1.2 Stanice

V síti jsou aktuálně k dispozici dva virtuální uživatelské počítače s operačním systémem Windows 10 PRO. Na tyto počítače má přístup každý doménový uživatel nebo správce v síti, aniž by byly jejich přístupy sledované, nebo omezené. Jedná se o počítače s výchozím nastavením, bez instalace jakéhokoliv softwaru třetích stran. Uživatelé a stanice mají přístup k síti a mohou vidět sdílené složky.

4.1.3 Auditní počítač

Auditní počítač je jediným fyzickým zařízením v celé infrastruktuře, na kterém běží operační systém Windows 10 PRO. Tato volba odráží zaměření na práci v prostředí Microsoft a zároveň je finančně efektivní. Rozhodnutí použít klasický operační systém na koncové stanici namísto serverové licence nemá žádný vliv na zamýšlenou funkcionalitu. Klíčovým faktorem je také zohlednění finančních aspektů, protože náklady na serverovou licenci jsou v porovnání s licencí pro běžný operační systém koncových stanic značně vyšší. Pro účely sběru dat je vytvořený speciální doménový účet "Audit", který má povolení přihlásit se pouze na vybraný počítač, čímž je zajištěna bezpečnost přístupu k důležitým datům a zdrojům. Počítač název dostal dle pojmenování nastavení politik Windows, tedy (Basic Audit Policy) v GPO.

4.2 Uživatelé

Pro účely testování je vytvořeno několik uživatelských účtů. V analyzovaném prostředí zatím chybí jakékoli metody a technologie pro sledování aktivit uživatelů, monitoringu hrozeb nebo neobvyklého provozu na síti. Následující kapitola se věnuje organizaci firmy v rámci AD a nastavení přístupů uživatelů.

4.2.1 Organizace firmy

V AD je vytvořená organizační jednotka: holding. Uživatelé jsou rozdělení do skupin: Interní zaměstnanci a Audit, což splňuje doporučení Microsoftu následovat organizační uspořádání firmy. Ve skupině interních zaměstnanců jsou podskupiny rozdělené na Vedení, Technici a IT oddělení. Skupina Audit slouží právě pro potřeby monitoringu. V rámci testování vzniklo několik uživatelů – Jan Kulička a Jan Svoboda a IT technik Roman Ajťák. Do skupiny vedení byl zařazený účet uživatele a vedoucího Pavla Nováka.

4.3 Politiky a procesy

V prostředí zatím chybí jakékoli metody a technologie pro detekci neobvyklého provozu. Proto se následující kapitola věnuje nastavení politik v prostředí Windows, správě práv na sdílených složkách, ukládání logů a dalším důležitým aspektům zabezpečení a sledování v prostředí sítě.

4.3.1 Nastavení monitoringu

Není nastavené žádné základní ani pokročilé monitorování pomocí GPO, tedy nesledují se události jako přihlášení a odhlášení uživatele, ani změny ve sdílených složkách, nebo kontroly oprávnění ke sdíleným složkám.

4.3.2 NTFS a SMB práva na sdílené složky

V rámci firmy je politika přidělování práv na složky zajištěná nastavením práv na úrovni souborového systému NTFS. SMB práva sdílení jsou tedy povolená pro všechny. NTFS práva pak určují, jaká skupina, či jednotlivec může do složky přistoupit. Jediná možnost, jak si vylistovat nastavená pravidla přístupu, je jít složku po složce a vyčíst informace z jednotlivých konfigurací NTFS práv.

4.3.3 Nastavení sdílení složek

Na doménovém řadiči je vytvořená složka C:\SHARES, nasdílená v síti. Obsahuje testovací podsložky, avšak monitoring přístupů k těmto složkám není prováděný, a proto nejsou zaznamenaná žádná data o jejich modifikaci. Pomocí skupinových politik (GPO) jsou tyto složky připojené jako disky. Každá podsložka má přidělená specifická práva, což umožňuje řízení přístupu k jednotlivým složkám.

1. C:\SHARES\Folder_Share - sdílená pro všechny doménové uživatele jako disk S:\.
2. C:\SHARES\INSTALL - sdílená pro všechny, přístup mají jen technici, kteří mohou číst a spouštět, nemohou zapisovat a mazat, připojená je jako I:\.
3. C:\SHARES\Vedeni – připojenou ji mají všichni, vstup, zápis, čtení má však výhradně vedení

4.3.4 Ukládání logů

Logy jsou na jednotlivých zařízení v případě procházené ručně a nejsou nijak archivované či uchovávané. Každý logovací soubor má maximální velikost 128 MB a jakmile tuto velikost dosáhne, dochází k automatickému přepisování nejstarších záznamů.

4.3.5 Vzdálená správa

Na počítačích ani serverech nejsou povolené žádné speciální porty pro vzdálenou komunikaci v síti. Nejsou nastavené a spuštěné služby protokolů, či sběru dat ze stanic. Ovšem kvůli povaze celé sítě, která je virtualizovaná, jsou nastavené komunikace pro vzdálené připojení pomocí Microsoft Remote Desktop. Vzdáleně se lze tedy připojit jak na servery, tak stanice.

4.3.6 Software

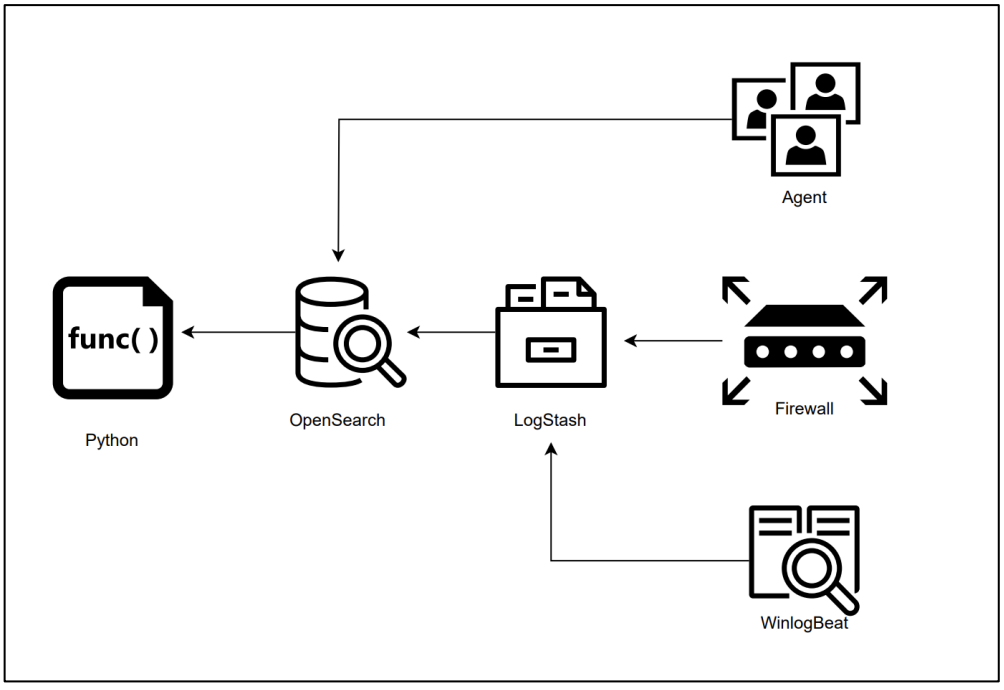
Po instalaci kromě nezbytně nutných programů není na stanicích ani serverech nainstalovaný žádný software, který by monitoroval uživatele. Vzhledem k budoucímu nastavení firewallu a testování není nainstalovaný ani antivirus.

4.4 Firewall

Základní nastavení firewallu zahrnuje implementaci routovacích pravidel na úrovni L3 i L4. Tato pravidla jsou základem pro povolování, či zakazování spojení na základě zdrojových a cílových IP adres a portů. Specifikum těchto nastavení spočívá v možnosti regulace přístupu z vnějších sítí (WAN rozhraní), kde je přípustná komunikace povolená pouze pro určité služby, a to výhradně z území České republiky. K dosažení této geografické selektivity je využívaný balíček pfBlocker společně s volně dostupnou licencí MaxMind GeoIP, což umožňuje efektivní filtrování nepovolených nebo nežádoucích přístupů z jiných zemí. Pomocí NAT (Network Address Translation) pravidel se pak řeší vnitřní routování provozu. Jakmile přichází provoz na určitou veřejnou IP adresu a port, NAT je schopný vnitřně přesunout tento provoz na další určenou IP adresu a příslušný port. V rámci PfSense softwaru navíc platí, že jakékoliv pravidlo, které není explicitně povolené, je defaultně zakázané. Provoz firewallu není aktuálně sledovaný, firma nemá záznamy, kolik provozu probíhá na různých portech a z jakých IP adres. Logy firewallu nejsou ukládané.

5 NÁVRH MONITORINGU

Důležité je si uvědomit, že monitorování infrastruktury Windows má širokou škálu možných přístupů. Způsob, který je popsaný v této práci, není jedinou variantou, kterou lze obecně použít. Hlavním cílem je sledovat události, které jsou účelově simulované. Důvode je, že lze lépe sledovat integritu dat a odhalovat případné problémy a nesrovnalosti. Výsledkem tohoto úsilí bude sada kódů a dokumentace nastavení, které umožňují centrální sběr informací z logů stanic a dalších zdrojů. Tento systém lze nadále rozvíjet a rozšiřovat, například implementací strojového učení. To by mohlo být součástí dalšího výzkumu, zahrnujícího analýzu nasbíraných událostí a vytvoření uživatelského rozhraní v rámci navazující diplomové práce. Následující část popisuje návrh monitoringu, jednotlivá nastavení a použité technologie a postupy. Nabízí také srovnání vlastního řešení s komplexnějšími nástroji, jako je Zabbix. Nakonec také popisuje, jaké funkcionality má tedy vlastní monitoring na základě zadání firmy splňovat.



Obrázek 14. Struktura použití technologií

5.1 Vlastní návrh versus řešení třetích stran

Cílem této bakalářské práce je nejenom monitorování infrastruktury, jak bylo zmíněné už výše, ale především hlubší pochopení fungování systémů na platformě Windows, jejich spolupráce a síťové komunikace. Volba vyvinout vlastní řešení, místo využití komerčních

nástrojů jako například Zabbix, vychází především z touhy získat praktické zkušenosti a lepší porozumění těmto technologiím.

Zabbix je robustní open-source platforma pro monitorování, která nabízí široké možnosti konfigurace a škálovatelnost. Umožňuje monitorování sítí, serverů, virtuálních strojů a cloudových služeb. Díky svým rozsáhlým možnostem je ideální pro velké podniky s komplexními sítěmi a potřebou detailního dohledu nad rozmanitými aktivitami. V rámci monitoringu Zabbix sleduje dostupnost a výkon koncových stanic, využití systémových zdrojů jako CPU, RAM a diskový prostor, a také běžící procesy a služby. Dále umožňuje sledování aplikací, zabezpečení systémů včetně detekce bezpečnostních aktualizací a posílá upozornění administrátorům v případě detekce problémů.

Dynamický vývoj vlastního řešení přináší možnost neustálého rozvoje a rozšiřování. Díky otevřené a modulární struktuře jazyku Python je snadné implementovat nové funkce a adaptovat systém na měnící se požadavky. To umožňuje flexibilní a dynamický rozvoj, což je ideální pro organizace, které potřebují pružně reagovat na nové výzvy a změny v technologickém prostředí. Vlastní monitoring nabídne hlubší náhled na aktivity uživatelů, jako je sledování jejich přihlášení a odhlášení, modifikace souborů, práva v souborovém systému a další funkcionality, které například Zabbix neposkytuje a muselo by se například sáhnout po placeném řešení softwarů jiných třetích stran. Málo jaký open-source poskytuje monitoring pokrývající požadavky firmy jako jsou výše zmíněné funkcionality s centrálním ukládáním logů a filtrací dat. Výhodou je zejména možný budoucí rozvoj celého řešení, technologie k tomu zvolené (jako je například OpenSearch), nabízí například i implementaci strojového učení.

Řešení ctí také rozhodnutí firmy prozkoumat tyto možnosti výhradně na platformě Windows. Cílem je zjistit, jak efektivně lze na této platformě implementovat monitorovací řešení a jaká dílčí nastavení jsou k tomu potřebná.

5.2 Návrh funkcionalit

Tato kapitola se podrobně věnuje specifikaci funkcionalit, které jsou od systému vyžadované v rámci aktuálních požadavků firmy. Detailně popisuje, jaké konkrétní operace a úkoly musí systém umět, aby odpovídal očekáváním a potřebám organizace. Na základě těchto informací bude možné systém správně nakonfigurovat a optimalizovat tak, aby co nejefektivněji sloužil svému účelu a zároveň zajišťoval bezpečnost a efektivitu pracovních procesů.

5.2.1 Přihlášení uživatele

Tento modul zabezpečí sledování a analýzu přihlašování a odhlašování uživatelů. Systematicky zdokumentuje jak úspěšné, tak neúspěšné pokusy o přihlášení, což umožní identifikaci potenciálních bezpečnostních hrozeb, či zneužití přihlašovacích údajů. Data budou filtrovaná na základě uživatele, času přihlášení a odhlášení, pracovní stanice, úspěšnosti pokusu a typu přístupu, což poskytuje komplexní přehled o uživatelské aktivitě v síti.

5.2.2 Monitoring přístupů do složek

Často je třeba, aby mohlo vedení firem nahlédnout, kdo manipuloval s daným souborem nebo složkou. Sledování přístupů do sdílených složek je tak klíčové pro zajištění integrity a bezpečnosti firemních dat. Tento modul zachycuje všechny pokusy o přístup k souborům, a to jak úspěšné, tak neúspěšné, což umožní reagovat na neautorizované pokusy o přístup. Filtrace dat se provede podle cesty k složce, identifikace uživatele, úspěšnosti pokusu o přístup a typu přístupu. Monitoring složek lze nastavit pomocí GPO, tudíž informace budou získané pomocí zpracování logů z doménového řadiče, který slouží pro testovací účely i jako filesystém.

5.2.3 Sledování historie prohlížečů

Tato funkce zahrne shromažďování a anonymizaci údajů o webových stránkách navštívených pomocí prohlížeče Edge, který je primárně určený politikami firem pro veškerou práci s interním softwarem, intranetem a dalšími nástroji firmy. Cílem je poskytnout přehled o online aktivitách uživatelů za účelem zabezpečení a dodržování firemních politik. Data jsou dostupná pro analýzu podle konkrétního uživatele, IP adresy a geografické lokace. Sledování nebude probíhat v reálném čase, ale s určitou prodlevou.

5.2.4 Aktivita firewallu

Monitoring aktivit firewallu poskytne cenné informace o veškeré komunikaci mezi interní sítí a vnějším světem. Logy z firewallu se zaznamenají v databázi a nadále se budou filtrovat podle typu komunikace, použitých portů, geografické lokace a IP adres, což umožňuje identifikovat potenciální bezpečnostní rizika.

5.2.5 Práva přístupů ke sdíleným složkám

Tato funkce poskytne podrobný přehled o aktuálních přístupech ke sdíleným složkám a umožňuje správu přístupových práv. Díky možnosti filtrovat data podle cesty k složce nebo podle uživatele a skupiny je možné efektivně koordinovat přístupy a zabezpečení dat v rámci firmy. Data budou sbíraná pomocí logů ze stanic, k tomu je třeba nastavit speciální GPO politiky.

5.2.6 Připojení externího zařízení

Sledování připojení externího zařízení k počítačům je klíčové pro prevenci úniku dat a zajištění bezpečnosti informací. Tento modul zahrnuje detekci všech externích zařízení připojených k síťovým stanicím. Sledování bude provedené pomocí nastavení GPO. Bohužel Windows neumožňuje nativní sledování odpojení externího zařízení. Pro tento účel je by bvlo vhodné nasadit speciální software na stanicích, který umožní monitorovat jak připojení, tak i odpojení USB zařízení. Toto řešení není ale v současné době firmou požadované a touto prací zpracované. Počítá se s ním však v budoucím vývoji.

5.2.7 Hardware a informace o AD

Tato funkce poskytuje informace o hardware a operačních systémech na vzdálených počítačích a zahrnuje nastavení a správu Active Directory. Monitoring AD zahrnuje politiky hesel, uživatelské účty a počítače v síti, což je nezbytné pro správu uživatelských identit a přístupových práv. Informace o HW poskytnou název počítače, poslední restart, verzi operačního systému a také IP adresu dané stanice. V rámci AD jsou dostupné informace hlavně o nastavení politiky hesel, výpisu stanic, uživatelů a administrátorů. Tyto informace nebudou přímo ukládané do OpenSearch.

5.2.8 Návrh vizualizace pomocí grafů

Na závěr chci demonstrovat možnost vizualizace dat prostřednictvím grafů, které však zatím nejsou začleněné do dynamického výběru pro uživatele. Nejprve je totiž nutné provést analýzy, na nichž by závisela agregace a určení, co by mělo být sledované a proč. Grafy jsou pouze ukázkou toho, jak lze s celým systémem pracovat a jak lze data prezentovat.

5.2.9 Možná budoucí rozšíření monitoringu

V současné fázi vývoje bakalářské není požadovaná implementace sledování externích zařízení, především co se týče monitorování jejich odpojování. Plánované rozšíření tohoto monitoringu zahrnuje vývoj a nasazení specializovaného softwarového agenta, který bude instalovaný na jednotlivých pracovních stanicích. Tento agent by měl schopnost detekovat jak připojení, tak odpojení USB zařízení, a poskytovat tak úplný přehled o všech externích zařízeních používaných v síti. Tato funkce je zásadní pro zajištění bezpečnosti dat, neboť umožní rychle reagovat na neautorizované přístupy a potenciální úniky informací.

Dalším důležitým aspektem monitoringu, který byl identifikovaný, ale zatím neimplementovaný, je sledování RDP. To je často využívané pro vzdálenou správu a přístup, což ho činí atraktivním cílem pro útočníky. Monitorování RDP by umožnilo identifikovat neobvyklé nebo neautorizované přístupy, což je klíčové pro ochranu proti vnějším útokům a interním hrozbám. Implementace této funkcionality by zahrnovala sledování všech RDP pokusů o připojení, včetně času, datumu, trvání sezení a identifikace uživatelů. Takový monitoring by poskytl cenný náhled do toho, jak jsou firemní zdroje využívané.

Obě tato rozšíření by přinesla významné zlepšení kybernetické bezpečnosti organizace tím, že by poskytla hlubší a detailnější pohled na uživatelské aktivity, což je nezbytné pro moderní proaktivní obranu proti kybernetickým hrozbám.

5.3 Seznam technologií

Následující kapitola se zaměřuje na představení a rozbor technologií použitých v rámci bakalářské práce. Popis jednotlivých nástrojů zde uvedených vysvětluje jejich roli a specifické využití v kontextu této práce, přičemž zdůrazňuje, jakým způsobem každý z nich přispívá k dosažení cílů práce.

5.3.1 Logstash

Logstash je nástroj pro zpracování a převedení logovacích dat do strukturovaného formátu pro jednodušší analýzu a vizualizaci. V tomto případě bude použitý pro zpracování dat ze stanic a firewallu. Umožní filtraci a modifikaci dat ještě před uložením do databáze, lze tak řídit jejich strukturu.

5.3.2 OpenSearch

OpenSearch je distribuovaný a škálovatelný vyhledávací a analytický nástroj. V této práci je využitý hlavně pro svou jednoduché ukládání dat s různou strukturou. Data bude možné indexovat, lehce v nich vyhledávat a archivovat po delší dobu na jednom místě. OpenSearch umožní v budoucnu vývoj například implementací strojového učení.

5.3.3 Winlogbeat

Winlogbeat je komponenta ze sady Elastic Stack, lehký agent pro Windows, který v tomto případě sbírá a přenáší události z Windows Event Logu do počítače AUDIT-SONDA. Tohoto agenta lze jakkoliv nakonfigurovat, v případě bakalářské práce bude sbírat hlavě bezpečnostní logy stanic a serverů. To zahrnuje události jako jsou přihlášení uživatelů, pokusy o přístup, změny v politikách a další bezpečnostně relevantní informace, které jsou klíčové pro detekci a analýzu bezpečnostních hrozeb.

5.3.4 Docker

Docker je populární platforma pro kontejnerizaci aplikací, která umožňuje vývojářům a systémovým administrátorům snadno vytvářet, nasazovat a spouštět aplikace v izolovaných kontejnerech. V této bakalářské práci Docker hostí instance OpenSearch a OpenSearch Dashboard, což jsou nástroje pro vyhledávání, analýzu a vizualizaci dat. Použití Dockeru zde znamená, že instalace a správa těchto komponent je zjednodušená a standardizovaná, což vede k vyšší efektivitě a snadnější správě systémových prostředků.

5.3.5 PsExec

PsExec je nástroj pro vzdálené spouštění programů nebo příkazů na vzdálených počítačích v prostředí Windows. Je často využíván pro automatizaci a správu vzdálených počítačů. V rámci tohoto řešení se bude podílet na testování a případně zajištění informací o HW a AD.

5.3.6 PowerShell Remote

PowerShell Remote umožňuje vzdálené spouštění PowerShell skriptů a příkazů na vzdálených počítačích v síti. V tomto řešení je využívaný pro automatizaci daných úkolů, jako je třeba sběr dat o právech sdílených složek.

5.3.7 Python

Python je vysokoúrovňový programovací jazyk, který se vyznačuje jednoduchostí a přehledností syntaxe. Je široce využívaný pro automatizaci úloh a komplexní analýzu dat. V rámci bakalářské práce je klíčová knihovna pro komunikaci s OpenSearch, která poskytuje intuitivní rozhraní pro interakci s tímto vyhledávacím systémem, umožňující integraci pokročilých vyhledávacích funkcí. Kromě toho Python nabízí bohaté možnosti pro vizualizaci dat například pomocí knihovny Matplotlib. Tyto nástroje umožňují efektivně prezentovat výsledky analýz, což je v této práci využité k ukázce zpracování a prezentace shromážděných dat.

5.4 Nastavení vzdálené správy a komunikace v síti

Pro celý proces je velmi důležité, aby byly počítače schopné spolu komunikovat. Respektive, aby správa celého monitoringu mohla probíhat z jednoho centrálního bodu. Tedy počítače, na kterém poběží OpenSearch, do kterého se data budou sbírat a naopak a ze kterého je lze strukturovaně i získávat a dále zpracovávat. Pro komunikaci a sdílení informací mezi počítači existují různé metody. V této práci se využívá povolení a nastavení protokolů Windows, které umožňují vzdálenou správu a spuštění kódu na vzdálených stanicích. Další možností je nasazení agenta přímo na stanici, které je využité v rámci sběru dat z prohlížeče, či logů ze stanic.

5.5 Natavení politik GPO

Jedná se o vytvoření pravidel pro sledování určitých událostí na stanicích a serverech pomocí GPO. Konkrétně je cílem nastavit monitoring přihlášení uživatelů, změn ve sdílených složkách na síti, či připojení externího zařízení. Pro účely sledování přihlášení je možné nastavit GPO tak, aby se ukládaly události přihlášení a odhlášení uživatelů na dané stanici. Pokud jde o zaznamenávání změn ve sdílených souborech, GPO umožní nastavení sledování přístupu k souborům a složkám na síťovém úložišti. Tím lze získávat události, jako jsou otevření, zápis nebo odstranění souborů, a identifikace uživatelů, kteří k těmto objektům přistupují.

5.6 Návrh databázového systému

NoSQL databáze je vhodný nástroj na práci s různou strukturou dat, proto je pro účely této bakalářské práce navržené použití OpenSearch. Vyniká totiž ve flexibilní manipulaci s daty,

umožňuje indexování každého typu logu pod unikátním pojmenováním, které zajistí Logstash. Například, logy z firewallu budou ukládané pod specifickým názvem, který reflektuje jejich obsah a strukturu, podobně bude postupováno i s logy ze stanic, kde každá stanice bude mít svůj jasně definovaný index označený názvem a datem zápisu. Všechna data jsou ukládána ve formátu JSON. Speciální požadavky na formátování dat jsou pečlivě ošetřené, aby odpovídaly specifikacím potřebným pro analýzu a vyhledávání.

5.7 Návrh sběru a ukládání dat

Na začátku se inicializuje spojení s OpenSearch, k čemuž slouží konfigurační soubor, který je uchovávaný odděleně od ostatních kódů a knihoven. Tento přístup umožní snadné provádění změn v nastavení bez nutnosti úpravy více kódů najednou.

Pro interakci s OpenSearch se využívá knihovna jazyka Python s názvem OpenSearch, která umožňuje vytvoření klienta na základě definované konfigurace. Tímto klientem se naváže spojení a zpracuje všechny požadavky na databázi OpenSearch pomocí jazyka DSL.

Pro sběr a zpracování dat z různých zdrojů, včetně logů z Windows a firewallu, se navrhuje využít nástroje Logstash. Dokáže naslouchat na určitých portech a aplikovat definované filtry na příchozí data. Pro přenos logů ze stanic bude využitý Winlogbeat, který umožňuje flexibilní zpracování a přímé odesílání dat na Logstash.

Na stanice bude nasazený také agent, který se stará o automatický sběr a odesílání dat, zejména z prohlížeče přímo do OpenSearch.

Data z firewallu se automaticky přesměrují na určené místo pomocí nastavení v jeho rozhraní.
V případě zisku práv NTFS se použijí příkazy PowerShell. Pomocí funkcí napsaných v jazyce Python lze data jednoduše zapsat také do databáze s příslušným indexem.

Jediná data, která nebudou ukládaná do OpenSearch, jsou data o HW a AD.

5.8 Zpracování dat

V této práci se data zpracovávají z OpenSearch s důrazem na flexibilitu a kontrolu nad celým procesem. Pro tento účel je využívaný jazyk Python, který poskytuje možnosti vizualizace dat pomocí grafů a organizace do tabulek, to zajistí knihovna Pandas a DataFrame. Každý úkol monitoringu bude mít vlastní sadu knihoven s funkcemi, které mají za úkol postupně načítat data z OpenSearch podle požadavků, zpracovávat a filtrovat je. Některá data nejsou

ukládána do OpenSearch, jako například informace o hardwaru a AD, a proto bude jejich zpracování probíhat aktuálně, když to bude potřeba. V budoucnu se plánuje vytvoření uživatelsky přívětivého rozhraní nad celou logickou sekcí.

5.9 Hardware a AD

Přehled o Active Directory, a případně o operačním systému a hardwaru počítačů uživatelů, je doplňkovou funkcí. K tomu účelu vyl vybraný i PowerShell open source nástroj Invoke-ADEnum, který je schopný generovat XML soubor obsahující relevantní informace. Tyto údaje mohou být klíčové při prvotním seznámení se strukturou neznámého zákazníka, protože poskytují přehled o počtu uživatelů, nastavených politikách hesel a dalších důležitých informacích.

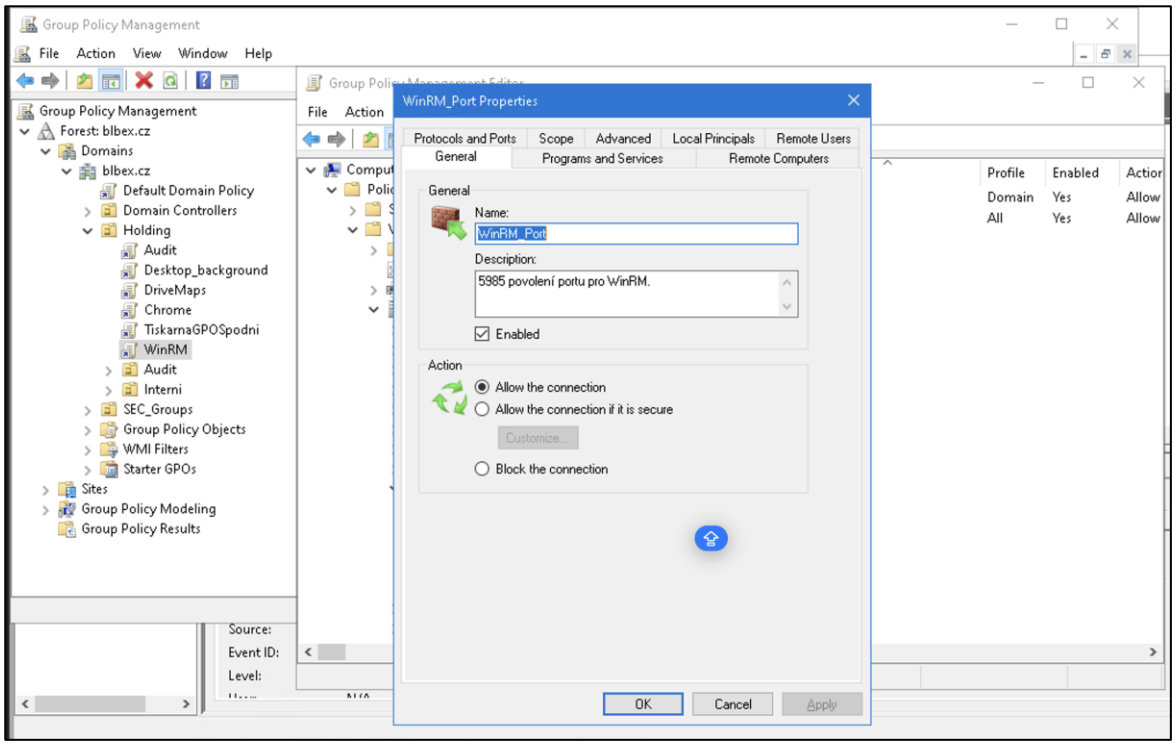
6 IMPLEMENTACE

V následující kapitole je popsané nastavení konfigurace pro nástroje a protokoly, jako jsou WinRM, PsExec a PowerShell Remote Control, které umožňují efektivní vzdálenou správu a komunikaci v síti. Tato sekce tedy podrobně popisuje kroky pro implementaci bezpečného a efektivního vzdáleného přístupu, zahrnující nastavení příslušných portů a politik skrze GPO a další nástroje pro správu Windows.

6.1 WinRM

Protokol WinRM umožňuje vzdáleně na stanicích a serverech získávat informace o hardware a celém systému a často jej ke své funkčnosti potřebují i další služby, jako PSRemoting. Pro nastavení je nutné povolit příchozí port číslo 5985 na firewallu, který umožňuje nešifrovanou komunikaci vhodnou pro testovací účely. Toto lze provést pomocí GPO na všech serverech a stanicích. Nastavení portu lze konfigurovat v editoru GPO pod politikou Windows Defender Firewall. Pro zjednodušení pozdější správy je vytvořená speciální politika s názvem WinRM, která je aplikovaná na celý holding. Vše lze nastavit v následujících krocích:

`Computer-> Windows Settings-> Security Settings-> Windows Defender Firewall with Advanced Security -> Inbound Rules`

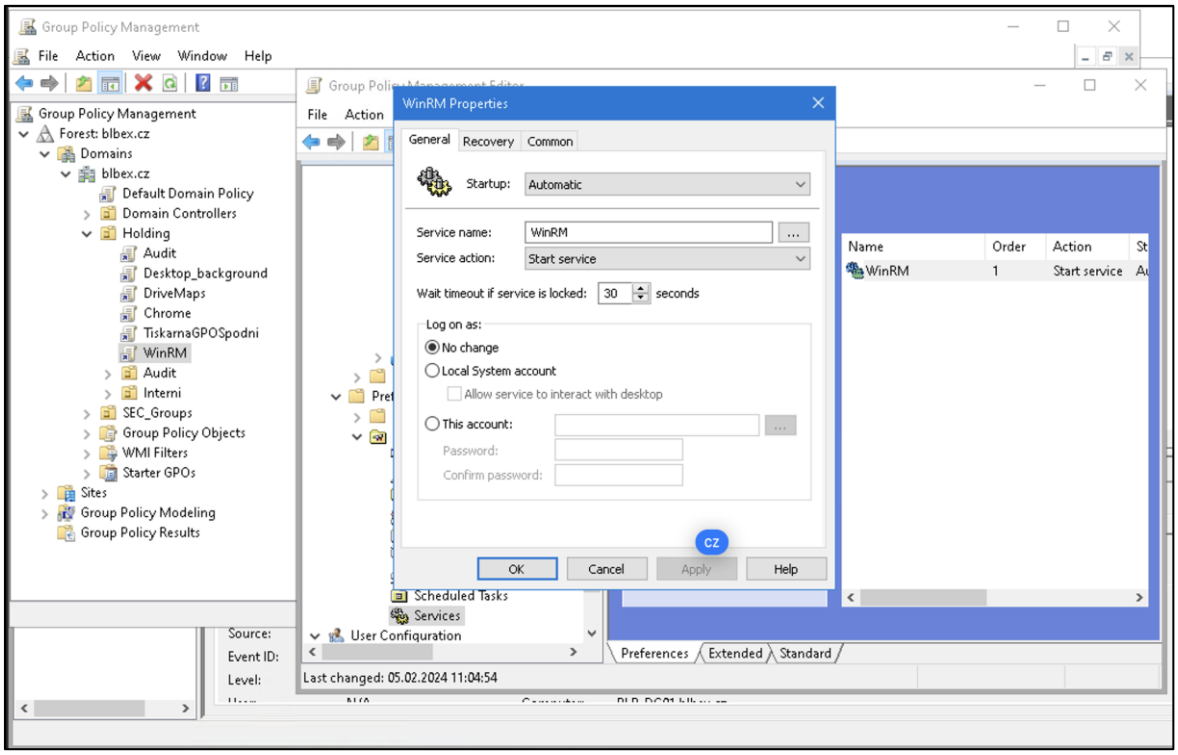


Obrázek 15. Povolení příchozího portu 5985 pomocí GPO

Lze také nastavit omezení, jako je specifikace IP adres, ze kterých je povolený přístup. Pro testovací účely se ale používá nastavení "wildcard" (*), což povoluje připojení z jakékoliv IP adresy. Následující nastavení umožňuje vzdálenou správu serverů prostřednictvím Windows Remote Management (WinRM). Když je tato možnost nastavena na "Povoleno", umožňuje konfiguraci serverů tak, aby akceptovaly příchozí požadavky na správu přes WinRM. WinRM je protokol Microsoftu pro správu a údržbu počítačů v síti Windows. Lze jej nastavit tímto způsobem:

`Computer Configuration-> Policies-> Administrative Templates -> Windows Components-> Windows Remote Management-> WinRM Service ->Allow remote server management through WinRM-> Enabled`

Dalším důležitým krokem pro efektivní fungování WinRM je aktivace služby WS-Management, která umožňuje komunikaci prostřednictvím WinRM. Tím lze realizovat operace na vzdálených počítačích. Je důležité, aby bylo nastavení této služby konfigurované na automatický start.
`Computer-> Preferences-> Control Panel-> Service-> Start WinRM & Automatic`



Obrázek 16. Povolení služby WinRM

6.2 PsExec

Tento nástroj může být využitý k zisku, či k administrativním účelům a spouštění jednoduchých příkazů na všech stanicích. PsExec využívá služby SMB k přenášení a spouštění binárního kódu na vzdálených počítačích. Je tedy nutné povolit port komunikace opět pomocí GPO, konkrétně příchozího portu 445, případně pravidla s názvem Sdílení Souborů a tiskáren SMB.

6.3 PowerShell Remote Control

Jedná se o další z popsaných metod spouštění skriptů a administrace na vzdálených počítačích v síti. Jak bylo zmíněno výše (3.4.4), tato služba může být spuštěná hned několika způsoby. V této bakalářské práci se přistoupilo k povolení provedené přes WinRM manuálně. Respektive pro takové úkony lze použít nástroj PsExec, kterým lze spustit příkaz na všech požadovaných koncových stanicích. V případě, že je služba již zapnutá, systém o daném nastavení podá zprávu. Příkaz vypadá následovně:

```
PS C:\X9\PSTools> .\psexec \\BLB-PC02 powershell -Command "Enable-PSRemoting -Force"

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Služba WinRM je již v tomto počítači nastavena pro příjem požadavků.
Služba WinRM je již v tomto počítači nastavena pro vzdálenou správu.
powershell exited on BLB-PC02 with error code 0.
```

Obrázek 17. Znovu spuštění PSRemotingu pomocí nástroje PsExec

V případě prověření, zda služba WinRM na dané stanici běží, lze použít opět PsExec, který tentokrát vzdáleně spustí příkazovou řádku a vylistuje konfiguraci WinRM:

```
.\PsExec.exe \\BLB-PC01 -s cmd /c "winrm get winrm/config"
```

Ale to, zda PSRemoting na vzdáleném počítači skutečně funguje, lze ověřit jednoduchým příkazem. Příklad je v následující ukázce:

```
PS C:\X9\PSTools> Enter-PSSession -ComputerName BLB-PC01 -ConfigurationName "microsoft.powershell32"
[BLB-PC01]: PS C:\Users\audit\Documents> ipconfig

Windows IP Configuration


Ethernet adapter LAN:

   Connection-specific DNS Suffix  . : blbex.cz
   Link-local IPv6 Address . . . . . : fe80::dc58:353c:7535:b437%4
   IPv4 Address. . . . . . . . . . . : 10.253.253.51
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.253.253.254
```

Obrázek 18. Demonstrace spojení se vzdáleným počítačem

Důležité také je si uvědomit, že některé Cmdlety disponují integrovanými technologiemi pro vzdálené spouštění na stanicích, které lze využít. Tyto příkazy obvykle obsahují parametr nazývaný `-ComputerName` pro specifikaci vzdáleného cílového zařízení. Jedná se například o příkazy `Invoke-Command`, nebo zmíněné `Enter-PSSession`. První zmíněný spustí daný příkaz na vzdáleném počítači, `Enter-PSSession` odstartuje interaktivní spojení se vzdáleným počítačem, což umožňuje spouštět jakékoliv skripty, jako po přihlášeni přímo na vzdáleném systému.

6.4 Nastavení sledování událostí

Monitoring v prostředí Windows se nastavuje pomocí vytvoření pravidel pro sledování určitých událostí, které většinou nejsou v základním nastavení povolené. Pro přehlednost je na doménovém řadiči v konzoli GPO vytvořená speciální politika s názvem Audit, která v sobě nese veškerá nastavení tohoto druhu. Tudíž ji lze jednoduše odlišit od jakýchkoliv jiných nastavení v síti.

6.5 Sledování událostí přihlášení

Pro sledování přihlášení je třeba povolit GPO politiku logování (Audit Account Logon Events). Což lze udělat následujíce:

```
Computer-> Policy-> Windows Policy-> Security setting-> Local Policy-> Audit Account Logon events
```

Zároveň je velmi důležité nezapomenout zapnout rozšířenou politiku, konkrétně přihlášení odhlášení a zachycení úspěšných i neúspěšných pokusů. Nastavení lze provést tímto způsobem:

```
Computer-> Policy-> Windows Policy-> Security setting-> Advanced Audit Policy Setting-> Logon/Logoff
```

V rámci bakalářské práce je kladený důraz na monitoring logů, které zahrnují jak úspěšné, tak neúspěšné pokusy o přihlášení. Konkrétně se zkoumají události Event ID 4624, signalizující úspěšné přihlášení uživatele, Event ID 4625, označující neúspěšné pokusy o přihlášení, a Event ID 4634, indikující odhlášení uživatele.

6.6 Výpis NTFS a SMB práv přístupů

Přístupy k sdíleným složkám lze nastavit v samotných NTFS ve vlastnostech (Properties), což se nachází v rozšířených možnostech zabezpečení (Securitu) v podsložce sdílení (Share). Explicitně lze definovat, zda má ke složce NTFS práva všichni, či vybraní uživatelé a o jaký typ práv se jedná. Tyto složky jsou připojené jako disky pro všechny uživatele pomocí GPO a práva NTFS určují, kdo může na disk přistoupit a co na něm může dělat.

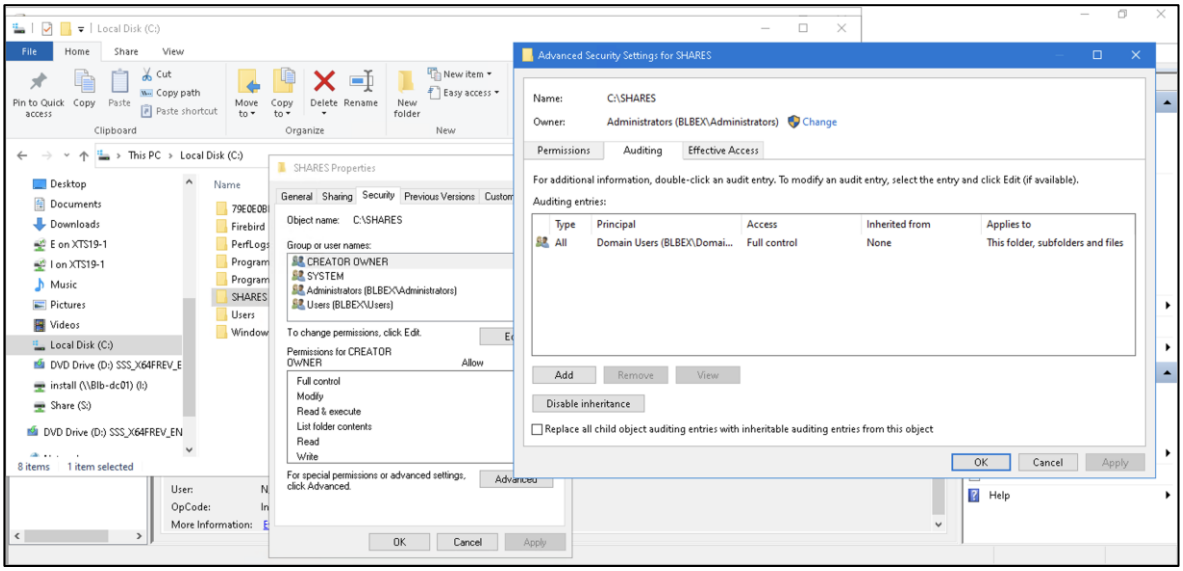
6.7 Sledování změn sdílených souborů

Pro monitorování změn v souborovém systému je nutné přistoupit k rozšířeným nastavením politik, kde lze nastavit sledování aktivit. Toto umožní zaznamenávat, kdo, kdy a k jakým souborům nebo složkám přistupoval, a zda došlo k vytvoření nebo smazání souborů či složek. Přístup k nastavení lze najít zde:

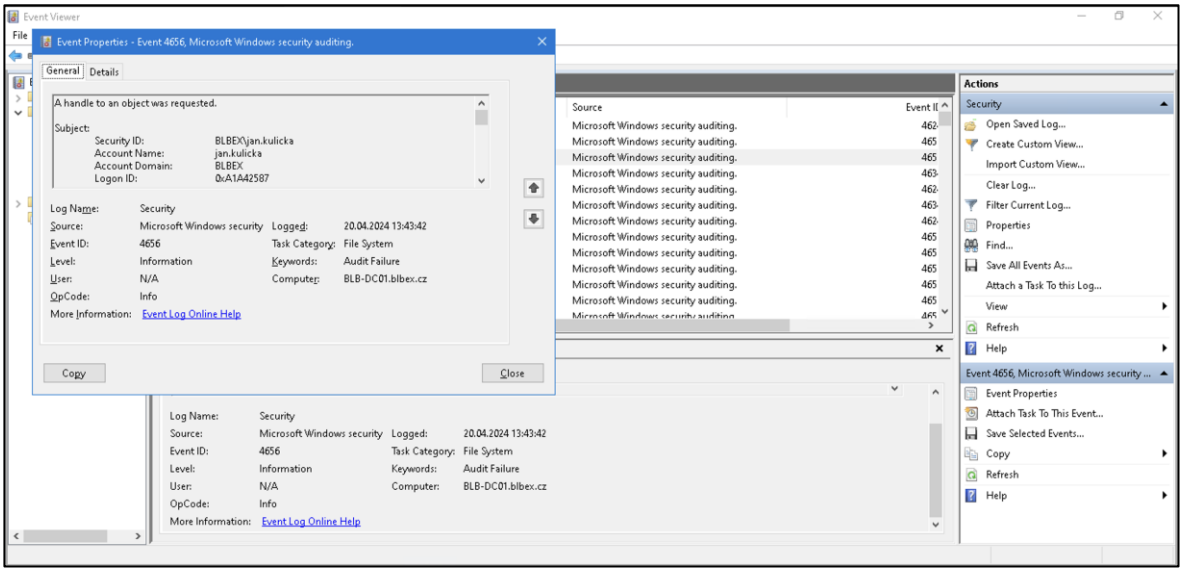
```
Computer Configuration-> Windows setting-> Security Setting-> Advanced Audit Policy-> Audit Policies-> Object Access-> Audit File Sysetem Success and Filure
```

Je rovněž důležité specifikovat v NTFS pravidlech, které složky podléhají monitoringu. V tomto případě se jedná o sdílené složky na doménovém řadiči, umístěné v C:\SHARES. Monitoring lze nastavit přímo v rozšířených nastaveních na záložce zabezpečení (Security) ve vlastnostech složky (Properties). Dále je třeba zvolit specifického uživatele nebo skupinu (Principal), u kterých budou události zaznamenávané. Dále je možné nastavit rozsah monitorování. V tomto případě byl zvolený monitoring plného přístupu pro všechny doménové uživatele. Kromě toho je třeba nastavit další politiku, aby bylo možné monitorovat i neúspěšné pokusy o přístup, které se zaznamenávají pod Event ID 4656. Nastavení lze provést tímto způsobem:

```
Computer Configuration-> Windows setting-> Security Setting-> Advanced Audit Policy-> Audit Policies-> Object Access-> Handle Manipulation
```



Obrázek 19. Nastavení auditu pro sdílenou složku C:\SHARES.



Obrázek 20. Log neúspěšného pokusu o přístup ke sdílené složce

6.8 Sledování připojení externího zařízení

GPO umožňuje monitorovat události v systémovém logu, jako je ID 4663 (Removable Storage), což se týká například připojení externího zařízení, jako USB nebo externí disk. Avšak nativní monitoring politik nepodporuje sledování odpojení zařízení. Přestože odpojení zařízení není nativně sledované, jeho monitorování bylo zařazené do konfigurace monitoringu kvůli jeho důležitosti.

Konfigurace probíhá prostřednictvím GPO:

```
Computer Configuration->Policies->Windows Settings->Security Settings->Advanced Policy Configurations->Audit Policy->Object Accesses->Audit Removable Storage
```

Což ale není vše, v dalším kroku se musí nastavit Active Directory Service Interfaces (ADSI), pro což lze využít nástroj Server Manager. Po otevření aplikace ADSI Edit je nutné navázat připojení a vybrat Výchozí kontext názvů (Default Naming Context). Poté je třeba přejít do uzlu DC, kde se nachází potřebná nastavení. V novém okně je záložka Zabezpečení (Security) v ní lze kliknout na možnost rozšířených nastavení (Advanced), aby mohlo být provedeno nastavení monitoringu. Důležité je správně zvolit skupinu uživatelů, na kterou se monitoring bude vztahovat. Při nastavování monitoringu připojení externích zařízení se zahrnují všichni uživatelé, včetně doménových a lokálních, na všech zařízeních v síti. Sledování lze dále upravit pomocí rozbalovacího seznamu, kde si můžete vybrat, zda se mají sledovat úspěšné nebo neúspěšné události. Pro každý typ přístupu je možné dále specifikovat typ kontroly (List Contents, Read All Properties, Read Permissions).

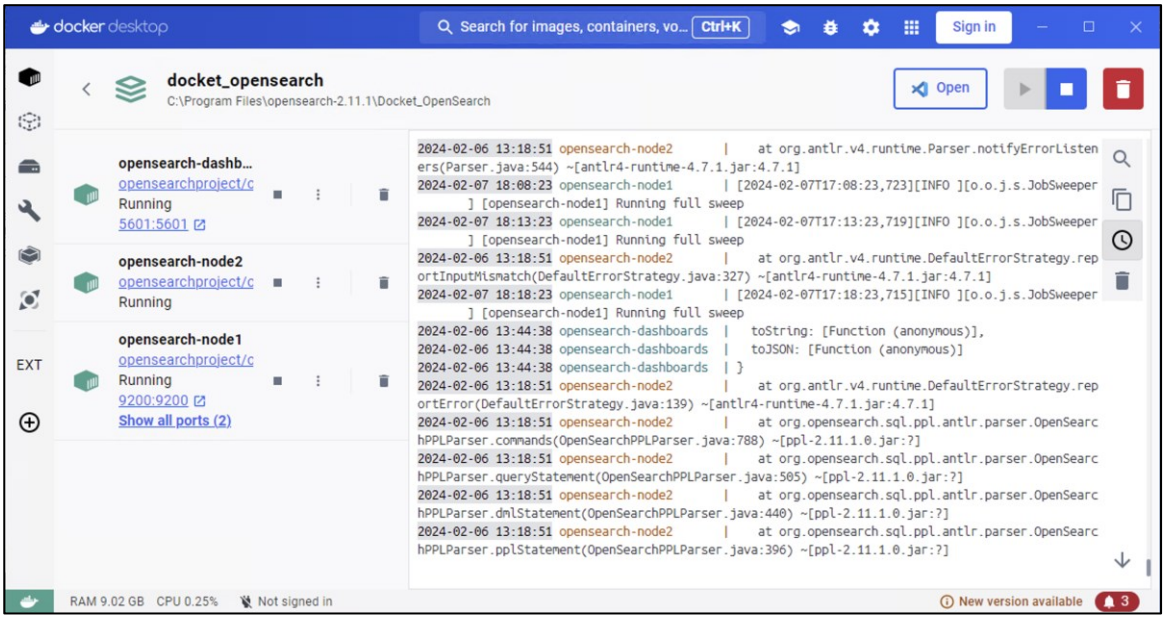
Události s ID 4663 (Removable Storage, An Attempt Was Made To Access An Object) jsou stejné pro oba typy výše zmíněných akcí. Při následném zpracování je proto důležité analyzovat další informace v každé události. Tyto informace se liší zejména podle systémů, na kterých byly události spuštěny.

6.9 Konfigurace databázového systému

OpenSearch shromažďuje data posílaná nástroji jako Logstash a Winlogbeat nebo přímo od agentů na stanicích. Uložená data jsou ve formátu JSON, což zajišťuje efektivní indexaci a snadné procházení.

6.9.1 Docker instalace

Pro usnadnění správy systému je vhodná instalace Docker Desktop manageru, který umožňuje jednoduchou správu kontejnerů prostřednictvím uživatelského rozhraní. Spuštění veškeré potřebné konfigurace OpenSearch je možné provést pomocí YML souboru v příkazové řádce. Pro účely testování je v YML rovněž zahrnutá konfigurace na instalaci OpenSearch Dashboard, jeho primární využití v rámci práce souvisí s testováním důvěryhodnosti dat.



Obrázek 21. Docker kontejnery OpenSearch a Dashboardu

6.9.2 Porty OpenSearch

OpenSearch vyžaduje komunikaci na specifických portech pro svou funkčnost. Port 5601 umožňuje přístup k OpenSearch Dashboardu přes síť, zatímco port 9200 je určený pro příjem dat od stanic nebo nástroje Logstash pro další zpracování. Ověření portů na počítači lze provést mimo jiné i příkazem PowerShellu, konkrétně `Test-NetConnection`. Pokud parametr `TcpTestSucceed` vypíše `True`, znamená to, že počítač naslouchá na portu a komunikace s ním byla úspěšná.

```
PS C:\Users\audit> Test-NetConnection -ComputerName localhost -Port 5601


ComputerName     : localhost
RemoteAddress    : ::1
RemotePort       : 5601
InterfaceAlias   : Loopback Pseudo-Interface 1
SourceAddress    : ::1
TcpTestSucceeded : True
```

Obrázek 22. Ověření otevření portu 5601

Po nastavení portů a instalaci se lze kdekoliv v síti připojit na Dashboard pomocí IP adresy auditního počítače s portem 5601 a v případě odesílání dat do databáze OpenSearch využít IP a port 9200.

6.10 Winlogbeat

Každá stanice musí mít nainstalovanou službu Winlogbeat. Stažené binární soubory obsahují instalační skript, který stačí spustit pomocí PowerShell příkazu. Ještě před nainstalováním služby je třeba upravit konfigurační soubor. Winlogbeat je velmi flexibilní nástroj, nabízí zpracování logů mnoha způsoby, dokáže komunikovat přímo nejen s OpenSearch databází, ale i s Logstash případně s mnoha dalšími systémy.

```
###################### Winlogbeat Configuration Example #########################
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h
  - name: Syste
  - name: Security

processors:
  - include_fields:
      fields: ["winlog.event_data.accesses"]

# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.109.60:5044"]

# ================================ Processors =====================================
processors:
  - add_host_metadata:
      when.not.contains.tags: forwarded
  - add_cloud_metadata: ~
```

Obrázek 23. Nastavení Winlogbeats na stanicích

Pro tuto práci byl zvolen přístup přímé komunikace s Logstash na portu 5044, port může být ale jakýkoliv. Podmínkou je, aby byl stejný pro Logstash konfiguraci i Winlogbeat. Tento port se navíc musí povolit na straně auditního počítače ve Windows Firewall. Pro potřeby bakalářské práce je zvolená jednoduchá konfigurace pro odesílání logů zabezpečení a systémových přímo na IP adresu auditního počítače. Ten má otevřený zmíněný port a pokud je Logstash spuštěný, události se začnou okamžitě přeposílat. Po uložení nastavení je třeba Winlogbeat spustit jako službu buď v rozhraní služeb, případně pomocí příkazu v PowerShell `Start-Service winlogbeat`.

6.11 Logstash

Primárním využitím programu Logstash je sběr dat z různých zdrojů, které dále zpracovává. V případě této bakalářské práce se jedná o logy z prostředí Windows a firewallu. Logstah se musí po stažení binárních souborů přemístit do složky C:\ProgramFiles. Lze ho spustit buď jako službu, či pomocí PowerShell příkazu, tedy jako smyčku. Naslouchá pak na portech dle své konfigurace a informace zpracovává na základě zadaných filtrů. Konfigurace Logstash je v souboru `/bin/logstash.conf` a skládá se ze tří důležitých částí.

6.11.1 Input

Určuje, co je zdrojem zpracování, tedy co se má uložit do OpenSearch. Data z Winlogbeat agenta z jednotlivých stanic se zpracovávají na portě 5044, pro který je opět třeba vytvořit výjimku ve firewallu auditního počítače.

```
input {
  beats {
    port => 5044
    tags => ["beats_log"]
    type => "beats"
  }

  tcp {
    type => "syslog"
    port => 5140
  }
  udp {
    type => "syslog"
    port => 5140
  }
}
```

Logy, které budou přicházet z firewallu přijímá Logstash na portu 5140. Formát TCP a UDP je zvolený z důvodu, že se nad těmito logy musí postavit vlastní parsování, aby bylo možné získat z firewallu relevantní data. Ke konfiguraci inputu se mohou doplnit tagy, popisy, typy, nad kterými bude spuštěna další filtrovací logika.

6.11.2 Filtr

Dalším krokem je filtr. Filtr Grok nabízí více než 120 šablon a je jedním z nejúčinnějších nástrojů pro filtrování logů v Logstash. Filtr Mutate umožňuje provádět široké transformace na polích událostí, jako je přejmenování, odstranění, nahrazení a úprava.

```
filter {
  if [type] == "beats" {
    grok {
      match => { "message" => "(?<Accesses>Accesses:\s+%{WORD:Access_type})
      " }
    }

    mutate {
      add_field => { "[@metadata][temp_hostname]" => "%{[host][name]}" }
    }

    mutate {
      lowercase => [ "[@metadata][temp_hostname]" ]
    }
  } else if [type] == "syslog" {
    ruby {
      code => "
        message = event.get('message')
        if message
          fields = message.split(',')
          fields.each_with_index do |field, index|
            event.set('field' + index.to_s, field.strip)
          end
        end
      "
    }
  }
}
```

V rámci kódu lze použít i podmínku, ta v tomto případě zahrnuje vyhodnocení, zda se jedná o příchozí log z firewallu, nebo z Winlogbeat. Jelikož hlavní složkou monitorování v rámci Windows jsou logy zabezpečení a stěžejní je monitoring přístupů ke sdíleným složkám (Delete, Read, Write), je nutné právě tuto část vytáhnout ze zprávy celého logu a parsovat pomocí filtru grog. Tím v databázi vzniká nová kolonka, která zahrnuje i informaci o způsobu přístupu uživatelů do složek. V případě zpracování logů z firewalu je nutné použít pokročilý typ filtru, tak zvaný Ruby. Důvodem je formát logu, který přichází z firewallu. Jedná se prakticky o jeden řetězec, který v sobě nese všechny potřebné údaje, jako zdrojovou IP adresu, příchozí porty, časovou známku, zda komunikace prošla přes bránu, případně jestli se jedná o TCP či UDP a další. Ruby filtr v Logstash umožňuje provádět transformace událostí pomocí spouštění Ruby kódu. Tento filtr přijímá buď inline Ruby kód, který se vykoná pro každou událost, nebo odkaz na Ruby soubor. Tímto uvedeným způsobem je schopný vzít řetězec (log firewallu) a pomocí rozdělovače (v tomto případě čárky), jednoduše rozdělit

zprávu do jednotlivých sloupců. Další zpracování pomocí Python kódu a dokumentace firewallu umožňuje přesně identifikovat typy dat.

6.11.3 Output

```
filter {
  if [type] == "beats" {
    grok {
      match => { "message" => "(?<Accesses>Accesses:\s+%{WORD:Access_type})
      " }
    }

    mutate {
      add_field => { "[@metadata][temp_hostname]" => "%{[host][name]}" }
    }

    mutate {
      lowercase => [ "[@metadata][temp_hostname]" ]
    }
  } else if [type] == "syslog" {
    ruby {
      code => "
        message = event.get('message')
        if message
          fields = message.split(',')
          fields.each_with_index do |field, index|
            event.set('field' + index.to_s, field.strip)
          end
        end
      "
    }
  }
}
```

Logstash pracuje jako smyčka, tudíž sbírá data během celého dne kontinuálně. Odchozí data po filtraci se rozdělují a přidává se jim příslušný název. Pokud mají označení beats, což jsou logy z Windows prostředí, přiřazuje se jim název počítače či stanice, odkud jsou a datum zpracování. Jako syslog jsou označené logy z firewallu. V případě, že by se jakýmkoliv vlivem dostal do zpracování log bez dalších informací, je označený za neznámý.

6.12 OpenSearch Dashboard

OpenSearch Dashboard poskytuje možnost vizualizace dat pomocí různých agregací a nastavení. V této práci je využitý především jako nástroj pro kontrolu, zatímco získávání a agregaci dat zajišťují vlastní funkce v jazyce Python. Například v záložce Discover webového rozhraní umožňuje nastavit prefix indexu pro zobrazení uložených dat a aplikovat filtry pro výběr specifických dat, ty pak lze porovnat se ziskem dat z vlastního řešení. Celé uživatelské rozhraní je dostupné na IP adrese auditního počítače a portu 5601 v rámci interní sítě.

6.13 Sběr a zpracování dat

Po připojení k OpenSearche pomocí klienta se lze dotazovat na daná data pomocí specifických funkcí. Následně proběhne další zpracování.

6.14 Komunikace s OpenSearch

```
from opensearchpy import OpenSearch
host = 'localhost'
port = 9200
auth = ('admin', 'admin')

client = OpenSearch(
    hosts=[{'host': host, 'port': port}],
    http_auth=auth,
    use_ssl=True,
    verify_certs=False,
    ssl_show_warn=False
)
```

Python obsahuje knihovnu speciálně určenou ke komunikaci s OpenSearch. K navázání spojení se vytvoří klient, který zpracuje vstupní údaje, jako je IP adresa OpenSearch a port, na kterém probíhá komunikace spolu s ověřením jména a hesla. Pro přehlednost kódu je konfigurace uchovaná v samostatném souboru a dle potřeby ji lze použít. Pro testovací účely bylo v této práci odpuštěno od zabezpečení komunikací pomocí SSL certifikátů a změny přihlašovacích údajů. V produkčním prostředí pak OpenSearch tuto možnost zabezpečení nabízí.

6.15 Funkce a knihovny

Knihovny používané pro úlohy často sdílejí podobné funkce, což je dáno jejich společným zdrojem dat a způsobem, jakým data uchovávají. Typicky zahrnují načítání dat, jejich

zpracování, vytváření datových rámců, filtrování a spuštění procesů, které jsou si navzájem podobné. Některé úlohy však vyžadují specifické přístupy k datům, což vede k rozdílným řešením. V jednotlivých případech se také využívají skripty PowerShell. V následující části jsou popsané jednotlivé funkce a jejich využití.

6.15.1 Funkce fetchData

```
def fetchData(client, index, query):
    """
    Získejte data z OpenSearch pomocí zadaného dotazu a indexu.
    """
    return client.search(body=query, index=index)
```

Funkce se stará o vytvoření spojení pomocí konfiguračního souboru OpenSearch. Volá funkci `client.search()` s parametry dotazu a hledaného indexu. Vytvoří tím instanci OpenSearch a spustí hledání. Parametr index je řetězec, který specifikuje jméno indexu v OpenSearch, ze kterého se získávají data. Query je slovník (dictionary), který obsahuje dotaz pro vyhledávání dat. Struktura tohoto dotazu se řídí syntaxí, kterou jazyk DSL vyžaduje. Funkce pak řeší i specifikace jaká data získat, jak je filtrovat či řadit.

6.15.2 Funkce procesHits

```
def processHits(hits):
    data = []
    for hit in hits:
        isInherited = hit['_source'].get('IsInherited', 'false')
        identityReference = hit['_source'].
            get('IdentityReference','Neznámý')
        folderPath = hit['_source'].get('FolderPath', 'Neznámý')
        accessControlType = hit['_source'].
            get('AccessControlType','Neznámý')
        propagationFlags = hit['_source'].get('PropagationFlags', 'Neznámý')
        shareName = hit['_source'].get('ShareName', 'Neznámý')
        fileSystemRights = hit['_source'].get('FileSystemRights', 'Neznámý')

        data.append({
                'IsInherited': isInherited,
                'IdentityReference': identityReference,
                'FolderPath': folderPath,
                'AccessControlType': accessControlType,
                'PropagationFlags': propagationFlags,
                'ShareName': shareName,
                'FileSystemRights': fileSystemRights,
        })    return data
```

Zpracovává výsledky dotazů získané z OpenSearch a převede je na seznam slovníků pro snazší manipulaci a analýzu. Ve smyčce prochází list výsledků (hits) a vytahuje data uložená pod klíčem(source), což je konvence OpenSearch pro uchování záznamu. Podle definice funkce extrahují specifické informace, jako je například cesta ke složce, a další údaje. Pro každý záznam tato funkce vytvoří slovník obsahující vybrané informace, který poté přidává do seznamu. V některých případech provádí funkce i práci s časovými razítky, převádí formát UTC do časové zóny středoevropského času a poté jej formátuje do čitelnějšího stavu. V ukázce kódu je vybraná funkce pro zpracování NTFS práv. Jiné řešení ovšem vyžaduje zpracování záznamů z firewallu. PfSense má totiž jasně daný formát logů, do Logstash data přichází jako řetězec, který následně parsuje Grok filtr, do databáze OpenSearch se dostávají nepojmenované kolonky. Funkce má v tomto případě ještě speciální úkol, a to pojmenovat neznámá data, která z OpenSearche dostává. Jednoduše vyhledá nepojmenované sloupce a dá jim název.

6.15.3 Funkce createDataFrame

```
def createDataFrame(data):
    """
    Dynamické vytvoření DataFrame z dat.
    """
    if data:
        # Získání klíčů ze prvního záznamu pro definici sloupců
        columns = data[0].keys()
        df = pd.DataFrame(data, columns=columns)
    else:
      # Pokud nejsou data, vytvoří prázdný DataFrame s předem
      definovanými sloupci
        df = pd.DataFrame(columns=[
            'IsInherited', 'IdentityReference', 'FolderPath',
             'AccessControlType', 'PropagationFlags', 'ShareName',
            'FileSystemRights'
        ])
    return df
```

Funkce přijímá jako vstup list dat z výše zmíněné funkce. Převede je do formy datové struktury DataFrame, což je tabulková struktura knihovny Pandas, čímž data získají čitelnou formu pro další manipulaci. Výsledkem je tabulka se sloupci, ty jsou vytvořené na základě sloupců v OpenSearch, ale v případě, že by nastal problém, dokáže si je vytvořit explicitně. Tímto způsobem funkce poskytuje užitečný nástroj pro přípravu dat získaných z OpenSearch pro další analýzu, vizualizaci, nebo reportování, zatímco zároveň zachovává nezbytné informace v přehledné a strukturované formě. Následující ukázka kódu pochází ze zpracování NTFS práv.

6.15.4 Funkce filterDataFrame

```
def filterDataFrame(df, filterCriteria):
    """
    Filtruje DataFrame na základě více kritérií od uživatele.
    """
    filteredDf = df
    for column, value in filterCriteria.items():
        if column in filteredDf:
            filteredDf = filteredDf[filteredDf[column].str.contains(value,
            case=False, na=False)]
    return filteredDf
```

Funkce je určena k filtraci už poskládaných dat do DataFrame na základě uživatelských kritérií, ta jsou předána funkci ve formě slovníku. Klíče interpretují názvy sloupců, do hodnot

se zadává předmět hledání. Výsledkem je nový DataFrame, který obsahuje pouze řádky odpovídající všem zadaným filtrům. Tato metoda je obzvláště užitečná pro zúžení na záznamy splňující specifická kritéria, což umožňuje uživatelům provádět cílenější analýzy nebo vizualizace dat.

6.15.5 Funkce pro zpracování jednotlivých aktivit

```
def ntfsActivity(client, indexPrefix, filterNtfsWatcher):
    indexList = client.indices.get_alias("*").keys()
    combined_df = pd.DataFrame()
    query = {
        'size': 1000,
        'query': {
            'bool': {
                'must': [{'match_all': {}}]
            }
        }
    }
    for indexName in indexList:
        if indexName.startswith(indexPrefix):
            response = fetchData(client, indexName, query)
            data = processHits(response['hits']['hits'])
            if data:
                df = createDataFrame(data) combined_df =
                  pd.concat([combinedDf, df], ignore_index=True)
    if not combinedDf.empty:
        filteredDf = filterDataFrame(combinedDf, filterNtfsWatcher)
        return filteredDf
    else:
        return pd.DataFrame()
```

Funkce skládá celou logiku dohromady a pro každý úkol je jedinečná. Prochází ve smyčce všechny indexy, které začínají na zadaný vzor od uživatele a pro každý vykoná dotaz pomocí funkce `fetchData`. Výsledky dotazu jsou zpracovány funkcí `processHits`, která převede surová data na seznam slovníků připravených pro analýzu. Tyto seznamy jsou postupně kombinovány do jednoho DataFrame. Funkce využívá explicitního výběru dat z OpenSearch, a to pomocí DSL dotazů. Lze tak například předejít čerpání potencionálně nechtěných dat. Uvedený příklad je opět součástí řešení pro NTFS práva, DSL dotaz zde není nijak omezený.

6.16 Agent historie prohlížečů

Historie prohlížeče vyžaduje zcela odlišný přístup. Data se nedostávají do OpenSearch pomocí Logstash, ani Winlogbeat. Historie prohlížeče Edge je totiž databázový soubor uložený v dané cestě.

`%APPDATA%\Local\Microsoft\Edge\User Data\Default\History`

Data lze získat pomocí SQL dotazu, což je řešené samostatným agentem (browser_agent.exe), kompilovaným souborem python kódu. Naplánovaná úloha spouští PowerShell skript, který vkládá dynamicky parametry do kompilovaného python kódu, oba se nachází ve sdílené složce SYSVOL. Zde může zapisovat jen doménový administrátor, nikoliv uživatel. Jednotlivé stanice z něj mohou soubor spouštět. V první řadě PowerShell skript kontroluje, zda byl během dne skript spuštěný, a to pomocí souboru uloženého v dočasné složce systému %TMP%. Obsahem tohoto souboru je datum posledního spuštění. Pokud skript běžel během dne, už se nespustí. Jinak aktualizuje soubor s aktuálním datem a spustí hlavní příkaz. Jediná pevná konstanta je IP adresa OpenSearch, ta je na rozdíl od počítačů a účtu vždy stejná. Hlavní příkaz spustí kompilovaného agenta (browser_agent.exe) s předanými argumenty, včetně dynamicky zjištěného jména uživatele a názvu počítače, a zmíněnou IP adresou OpenSearch.

```
$flagFile = Join-Path $env:TEMP "browser_agent_last_run.txt"
# Získá dnešní datum
$today = Get-Date -Format "yyyyMMdd"
# Kontrola, zda skript již běžel dnes
if (Test-Path $flagFile) {
    $lastRun = Get-Content $flagFile
    if ($lastRun -eq $today) {
        Write-Host "Skript byl již dnes spuštěn."
        exit
    }
}
# Aktualizace souboru s datem posledního spuštění
Set-Content -Path $flagFile -Value $today
# Spuštění hlavního příkazu s dynamickým jménem uživatele a počítače
$computerName = $env:COMPUTERNAME.ToLower()
$username = $env:USERNAME
$command = "\\blb-dc01\SYSVOL\browser_agent.exe -u $username -c
$computerName -o 192.168.109.60"
Invoke-Expression $command
```

Plánovač úloh hlídá událost přihlášení uživatele na počítač. Jakmile se uživatel přihlásí, skript se spustí a kontroluje výše zmíněný soubor v dočasné složce, což omezuje duplikaci dat v OpenSearch. Pro testovací účely však agent odesílá data za posledních pět dní, důvodem je, že laboratoř není mimo bakalářskou práci využívaná a pro demonstrace je třeba vytvářet data uměle. V produkční verzi by tento interval byl nastavený na jeden den z důvodů předpokladu, že uživatel se přihlašuje na svůj počítač a využívá prohlížeč na denní bázi. Dat by tak bylo dostatek. Důležité je zdůraznit, že přenos není prováděný v reálném čase. Navíc je nemožné číst data přímo z databáze SQL, pokud má uživatel otevřený prohlížeč, což je běžná situace v průběhu pracovní doby. Skript řeší tento integritní problém tím, že kopíruje soubor historie do dočasného umístění. Ta není procesem prohlížeče Edge zamčená a může číst konzistentní data. Ty pak načte pomocí SQL dotazu, přidá sloupec s uživatelským jménem, nastaví klienta a přenese data do OpenSearch v JSON formátu pro každý záznam. Po úspěšném nahrání skript odstraní dočasné soubory.

6.16.1 Zisk dat z OpenSearch

Získaná data jsou zaobalená do geolokačních IP adres pomocí DNS vyhledávání. K čemuž je použitá lokálně uložená databáze Geoip2. Lze tedy získat základní informace jako název stránky, čas poslední návštěvy, IP a uživatele, a doplní je o IP adresu serveru. Čas poslední návštěvy je korigován z epochálního času prohlížeče na lidsky čitelný formát a převeden do lokálního časového pásma. Výsledné data jsou transformovaná do DataFrame. Výstupem je tak čistější a specificky zaměřená sada dat.

6.17 Invoke AD-Enum a HW info

Tento kód kombinuje použití PowerShell skriptů a Pythonu k získávání a zpracování informací o počítačích v síti. Skript v PowerShellu je navržen tak, aby se spustil na více vzdálených počítačích a shromáždil z nich detailní informace o hardwaru, operačním systému a IP adresách. Python kód následně parsuje výstup z PowerShell skriptu, který je zformátovaný a rozdělený do bloků. Každý blok reprezentuje data z jednoho počítače. Výstup je pak uložený do DataFrame, tento DataFrame je poté možné dále zpracovávat. Například, je možné filtrovat počítače podle doby od posledního restartu, funkce převede textovou reprezentaci času posledního spuštění do datového formátu a vypočítá, kolik dní uplynulo od té doby.

6.18 Výsledky monitorování

S využitím filtrovacího pole s klíči a hodnotami program získá požadovaná data. Filtrování je zakomponováno do výše zmíněné logiky v kódech, vyžaduje však znalost jednotlivých tabulek, tedy, jaké obsahují názvy a položky. V budoucím rozvoji systému by byla například tato logika uživateli skrytá a filtrování by mělo dynamickou podobu. Program tak umožní jen výběr z hodnot, které jsou relevantní. Následující ukázky nepokrývají všechny možné kombinace filtrů a uložených dat. Vizualizace dat pomocí grafů balíčku Matplotlib jazyka Python je ukázkou možných agregací, lze si tak snadněji představit, co je program schopný nabídnout, není to však aktuální cíl. Data nejsou agregována na základě žádné analýzy.

6.18.1 Přihlašování uživatele

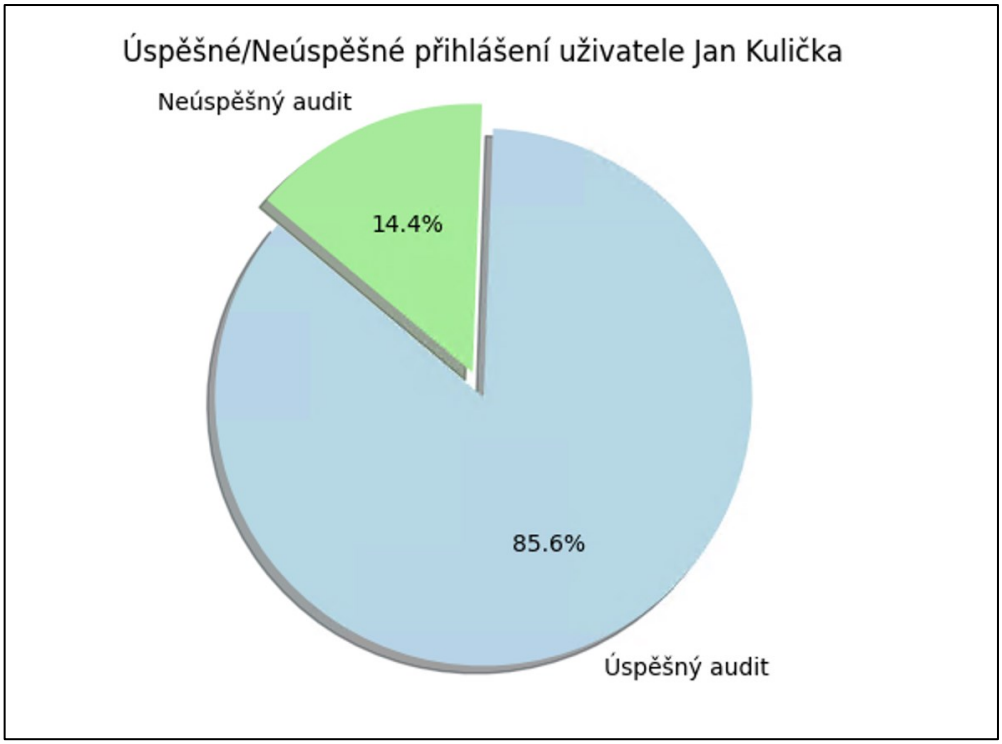
Události přihlášení se zapisují do logů zabezpečení a po zápisu do databáze je hlavním úkolem v nich umět vyhledávat dle jména uživatele, zda se přihlásil či odhlásil, nebo o jaké přihlášení se jedná (úspěšné, neúspěšné). Filtr dat je závislý na názvech sloupců, což umožňuje dotaz ještě více zpřesnit, pokud je potřeba. Následující ukázka filtruje data na základě jména a typů události.

```
# LogOn a LogOff události
filterlogonWatcher = {
    "TargetUserName": "jan.kulicka",
    "Task": "Logoff", # Filtruji podle přihlášení či odhlášení
    "LogonType": "3", # Typ události
}
logonActivity = logevent.logonActivity(setup.client, "log-blb-pc01",
        filterlogonWatcher)
print("=== Logon Activity Data ===")
print(logonActivity)
```

```
=== Logon Activity Data ===
      Task TargetUserName      Keywords           Timestamp  Hostname LogonType
20   Logoff    jan.kulicka  Úspěšný audit  09.04.2024 08:49:40  BLB-PC01         3
30   Logoff    jan.kulicka  Úspěšný audit  09.04.2024 08:49:59  BLB-PC01         3
65   Logoff    jan.kulicka  Úspěšný audit  09.04.2024 11:47:25  BLB-PC01         3
73   Logoff    jan.kulicka  Úspěšný audit  09.04.2024 18:11:11  BLB-PC01         3
91   Logoff    jan.kulicka  Úspěšný audit  06.04.2024 18:32:01  BLB-PC01         3
101  Logoff    jan.kulicka  Úspěšný audit  06.04.2024 18:32:59  BLB-PC01         3
112  Logoff    jan.kulicka  Úspěšný audit  06.04.2024 19:41:28  BLB-PC01         3
120  Logoff    jan.kulicka  Úspěšný audit  07.04.2024 16:09:58  BLB-PC01         3
128  Logoff    jan.kulicka  Úspěšný audit  08.04.2024 21:42:04  BLB-PC01         3
138  Logoff    jan.kulicka  Úspěšný audit  27.03.2024 12:06:24  BLB-PC01         3
150  Logoff    jan.kulicka  Úspěšný audit  27.03.2024 12:07:51  BLB-PC01         3
178  Logoff    jan.kulicka  Úspěšný audit  12.04.2024 08:00:10  BLB-PC01         3
190  Logoff    jan.kulicka  Úspěšný audit  12.04.2024 09:37:26  BLB-PC01         3
224  Logoff    jan.kulicka  Úspěšný audit  11.04.2024 08:26:01  BLB-PC01         3
242  Logoff    jan.kulicka  Úspěšný audit  11.04.2024 15:54:05  BLB-PC01         3
```

Obrázek 24. Výsledky spuštění kódu výše

Data z datagramu lze použít ke tvorbě koláčového grafu pro ukázku úspěšných a neúspěšných přihlášení uživatele Jana Kuličky na všech počítačích. Kód v tomto případě filtruje data jen na základě jména uživatele a graf ukazuje agregaci počtu úspěšných a neúspěšných přihlášení ze všech uložených událostí.



Obrázek 25. Úspěšné a neúspěšné přihlášení

6.18.2 Historie prohlížeče Edge

Funkce získává data z prohlížeče, které lze filtrovat pomocí uživatele, případně přesné IP adresy, nebo státu. Data jsou na pozadí převedená pouze do IP adres, čehož je docíleno použitím knihovny GeoLite2. Podle IP se pak každému záznamu přidává kolonka státu, ze kterého prohlížené stránky pochází.

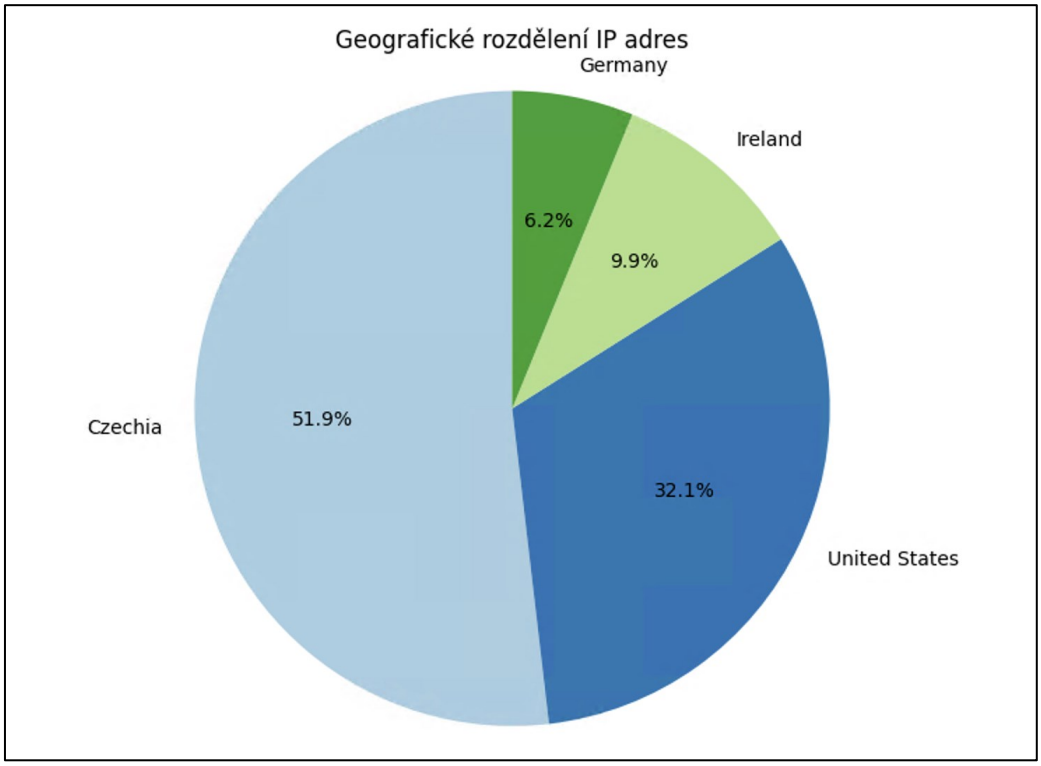
```
# Historie prohlížení Edge
filterBrowserWatcher = {
    "user": "pavel.novak",
    "Country": "United States",


}
browserWatcherData= bh.browserHistoryActivity(setup.client,
    "browser_history", filterBrowserWatcher)
print("=== Browser History Data ===")
print(browserWatcherData)
```

Výsledkem kódu výše jsou všechny prohlížená data uživatele Pavla Nováka. Vzor (index) specifikuje pouze název indexace, tudíž jsou výsledkem všechna historicky procházené stránky uživatele.

```
=== Browser History Data ===
       lastVisitTime         user       ipAddress        Country  id
20  2024-04-02 15:31  pavel.novak  204.79.197.203  United States  38
21  2024-04-02 15:31  pavel.novak   142.251.36.99  United States  57
22  2024-04-02 15:31  pavel.novak   142.251.36.99  United States  56
27  2024-04-02 15:31  pavel.novak   35.208.115.57  United States  60
32  2024-04-02 15:31  pavel.novak   35.208.115.57  United States  61
```

Obrázek 26. Stránky procházené uživatelem Pavlem Novákem

K agregaci a vizualizaci dat lze využít opět sestavení grafu, například na základě zemí, ze kterých pochází webové stránky prohlížené všemi uživateli v síti za celou dobu sběru logů.



Obrázek 27. Rozdělení prohlížených stránek pomocí IP adres

6.18.3 Sledování přístupů ke sdíleným souborům

Přístupy uživatelů ke sdíleným souborům kód filtruje na základě uživatele, druhu přístupu (Delete, ReadAttributes, Write) ke sdílené složce, nebo podle cest ke složkám a indexu. Pokud je třeba zjistit informace o více uživatelích, lze zadat pole se jmény. Pokud je to ovšem potřebné, lze sledovat i nepovedené pokusy o přístup ke složkám.

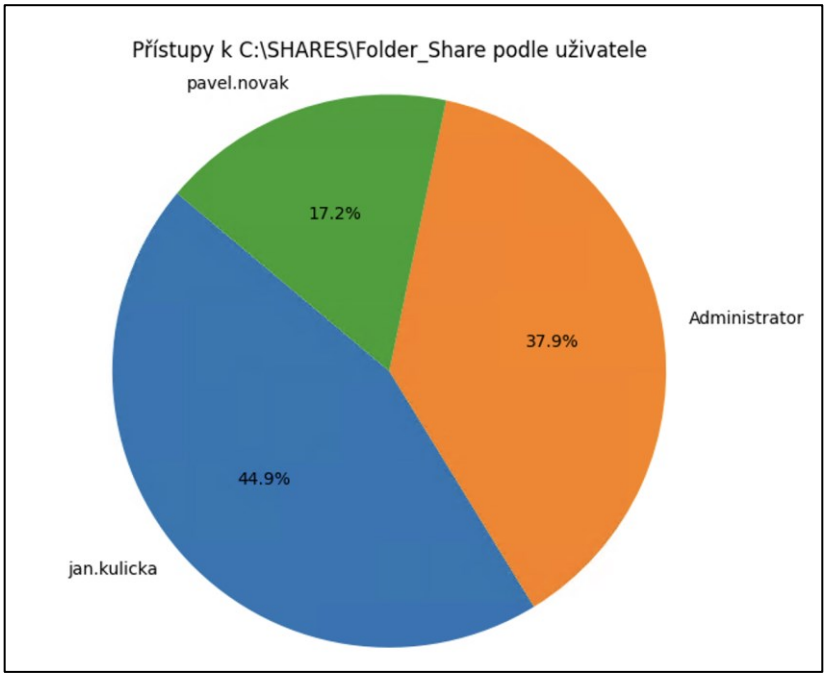
```
# Data přístupů ke sdíleným složkám
filterFileWatcher = {
      "User": ["Administrator", "jan.kulicka"],
      "File": "C:\\SHARES\\Folder_Share"
      # "Access": "DELETE",
      # "Keywords": "Audit Failure",

}
fileWatcherData = fwa.fileWatcherActivity(
    setup.client, "log-blb-dc01.blbex.cz-2024", filterFileWatcher)
print("\n" * 2)
print("=== File Watcher Data ===")
print(fileWatcherData}
```

Výsledkem kódu výše je souhrn přístupů ke složce C:\SHARES\Folder_Share od uživatelů Administrátor a Jan Kulička.

```
=== File Watcher Data ===
                    Slozka       Uzivatel        Pristup          Pokus                  Cas  ID Udalosti
3     C:\SHARES\Folder_Share  Administrator  ReadAttributes  Audit Success  27.03.2024 12:03:58        4663
4     C:\SHARES\Folder_Share  Administrator  ReadAttributes  Audit Success  27.03.2024 12:04:01        4663
5     C:\SHARES\Folder_Share  Administrator  ReadAttributes  Audit Success  27.03.2024 12:04:01        4663
6     C:\SHARES\Folder_Share  Administrator  ReadAttributes  Audit Success  27.03.2024 12:04:01        4663
15    C:\SHARES\Folder_Share  Administrator      AppendData  Audit Success  27.03.2024 12:04:14        4663
...                      ...            ...             ...            ...                  ...         ...
2067  C:\SHARES\Folder_Share    jan.kulicka  ReadAttributes  Audit Success  10.04.2024 12:41:26        4663
2070  C:\SHARES\Folder_Share    jan.kulicka  ReadAttributes  Audit Success  10.04.2024 12:41:27        4663
2071  C:\SHARES\Folder_Share    jan.kulicka  ReadAttributes  Audit Success  10.04.2024 12:41:27        4663
2072  C:\SHARES\Folder_Share    jan.kulicka  ReadAttributes  Audit Success  10.04.2024 12:41:27        4663
2077  C:\SHARES\Folder_Share    jan.kulicka  ReadAttributes  Audit Success  10.04.2024 16:08:38        4663

[347 rows x 6 columns]
```

Obrázek 28. Výsledek přístupů dvou uživatelů k jedné složce

Jak často a kdo přistupuje do určité složky se dá taktéž vizualizovat pomocí koláčového grafu. V tomto případě kód filtruje přístupy všech uživatelů do sdílené složky C:\SHARES\Folder_Share.



Obrázek 29. Jednotliví uživatelé pracující se sdílenou složkou

6.18.4 Firewall logy

Logy z firewallu nabízí spoustu informací, které lze agregovat, či filtrovat. Funkce navíc nabízí možnost vyloučení. Následující grafy jsou ukázkami provozu na portech firewallu, či sběr přijatých a blokovaných komunikací.

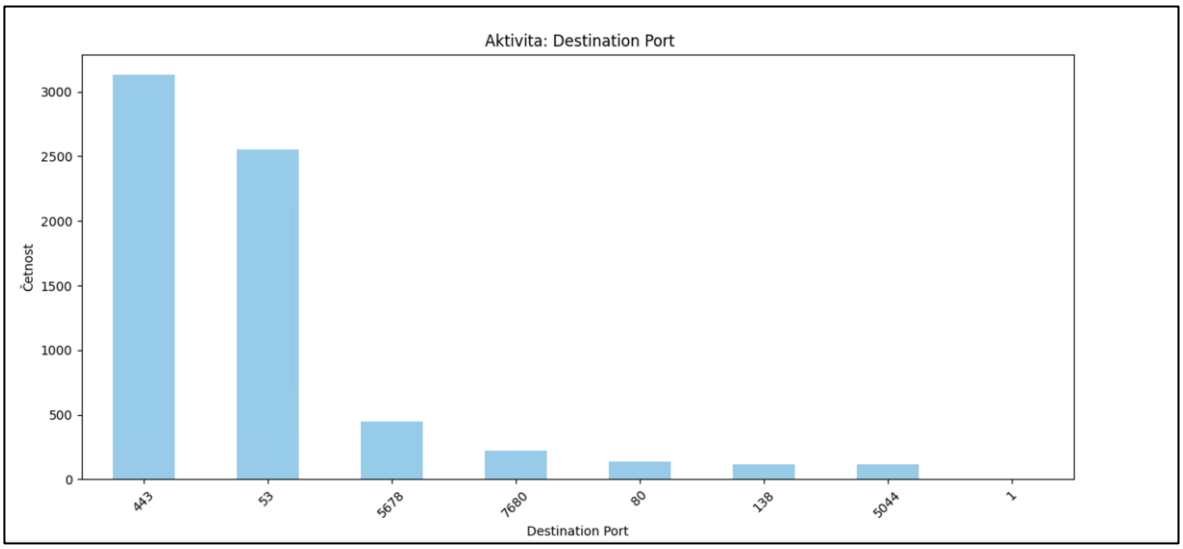
```
# Data z firewallu
indexPrefix = "logstash-pfsense-2024."
print("=== Firewall Activity Data ===")
filters = {
        "Type": "tcp",
        "Country": ["not:Místní síť", "not:Broadcast"],
        "Destination Port": ["not:443"]
}
firewallData = fw.firewallActivity(setup.client, indexPrefix, filters,
db_path)
print(firewallData)
```

Výsledkem kódu jsou data, která splňují všechny výše zmíněné podmínky ,tedy typ TCP, cílový port nesmí být 443 a nejedná se o Broadcast ani Místní síť. Takový výsledek by mohl být předmětem další analýzy.

```
=== Firewall Activity Data ===
           Source IP Source Port Actions Direction Type  Destination IP Destination Port         Timestamp       Country      Continent        Timezone Subdivisions
77     146.75.118.172       54078    pass        in  tcp   10.253.253.52              80  03-04-2024, 22:33       Germany         Europe    Europe/Berlin        Hesse
230     34.104.35.123       55716    pass        in  tcp   10.253.253.51              80  03-04-2024, 22:51 United States  North America  America/Chicago      Unknown
279     34.104.35.123       55735    pass        in  tcp   10.253.253.51              80  03-04-2024, 22:57 United States  North America  America/Chicago      Unknown
370      92.122.48.35       55759    pass        in  tcp   10.253.253.51              80  03-04-2024, 23:07       Czechia         Europe    Europe/Prague       Prague
479    146.75.118.172       49821    pass        in  tcp  10.253.253.101              80  03-04-2024, 23:19       Germany         Europe    Europe/Berlin        Hesse
...               ...         ...     ...       ...  ...             ...             ...                 ...           ...           ...              ...          ...
12464     10.6.66.53       63683    pass        in  tcp   10.253.253.51            7680  13-04-2024, 01:06       Unknown       Unknown       Unknown      Unknown
12519    92.122.48.99       58616    pass        in  tcp  10.253.253.101              80  13-04-2024, 01:12       Czechia         Europe    Europe/Prague       Prague
12935  192.229.221.95       59057    pass        in  tcp  10.253.253.101              80  13-04-2024, 02:26 United States  North America  America/Chicago      Unknown
12988    92.122.48.99       58632    pass        in  tcp   10.253.253.52              80  13-04-2024, 02:39       Czechia         Europe    Europe/Prague       Prague
13065    92.122.48.48       54407    pass        in  tcp  10.253.253.101              80  27-03-2024, 16:30       Czechia         Europe    Europe/Prague       Prague

[305 rows x 12 columns]
```

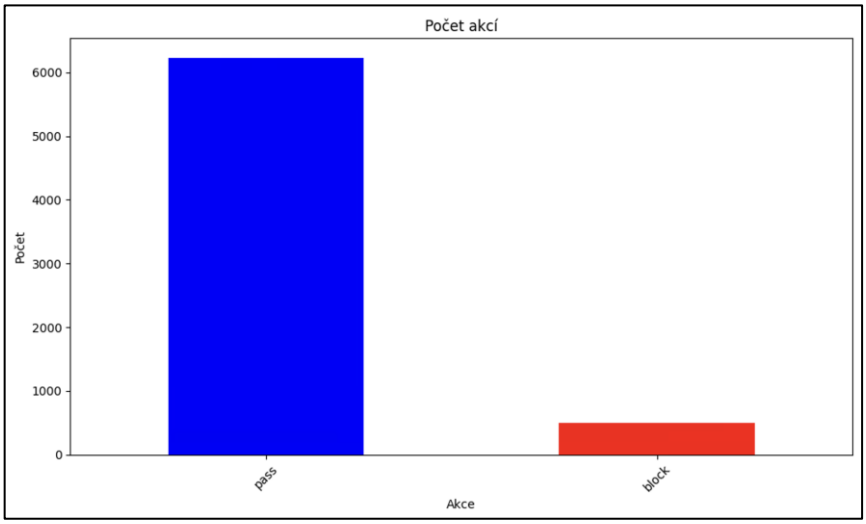
Obrázek 30. Filtrovaná data firewallu

Provoz na těchto cílových portech je získaný agregací všech logů z firewallu bez filtrů.



Obrázek 31. Provoz na portech firewallu

Stejným způsobem lze získat agregace toku, které firewall povolil nebo blokoval.

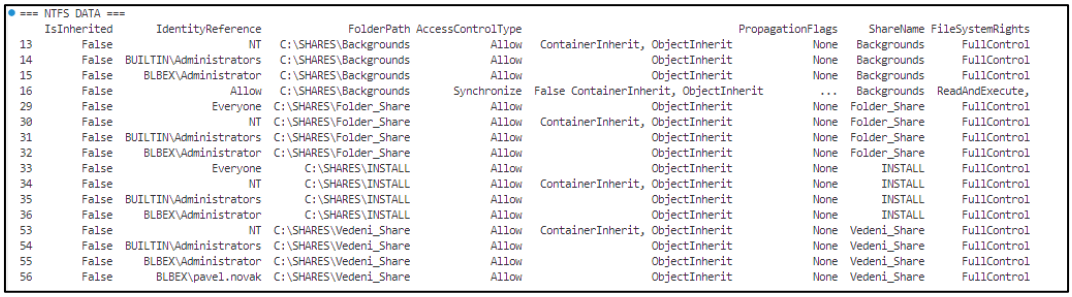


Obrázek 32. Blokovaná a povolená komunikace na firewallu

6.18.5 NTFS přístupová práva

Organizace mají obvykle několik sdílených složek, často rozdělených dle účelu práce samotných pracovníků. Je tedy velmi důležité mít přehled, kdo má kam vlastně přístup, což určují NTFS práva. Kód je schopný úhledně vypsat a filtrovat zadané složky, případně nastavená práva. V ukázce je vidět filtr pro sdílené složky doménového řadiče, konkrétně pro C:\SHARES\Vedení_Share. Do složky má přístup jen uživatel pavel.novak.

```
# NTFS data přístup
print("=== NTFS DATA ===")
filterNtfsWatcher = {
    "FolderPath": r"C:\\SHARES",
}
index_prefix = 'log-ntfs-shares-2024-04-11'
filtered_df = ntfs.ntfsActivity(setup.client, index_prefix,
      filterNtfsWatcher)
print(filtered_df)
```



```
=== NTFS DATA ===
    IsInherited      IdentityReference            FolderPath AccessControlType                                PropagationFlags     ShareName FileSystemRights
13        False                     NT  C:\SHARES\Backgrounds             Allow  ContainerInherit, ObjectInherit             None   Backgrounds      FullControl
14        False  BUILTIN\Administrators  C:\SHARES\Backgrounds             Allow                    ObjectInherit             None   Backgrounds      FullControl
15        False     BLBEX\Administrator  C:\SHARES\Backgrounds             Allow                    ObjectInherit             None   Backgrounds      FullControl
16        False                   Allow  C:\SHARES\Backgrounds       Synchronize False ContainerInherit, ObjectInherit         ...   Backgrounds  ReadAndExecute,
29        False                Everyone  C:\SHARES\Folder_Share             Allow                    ObjectInherit             None  Folder_Share      FullControl
30        False                      NT  C:\SHARES\Folder_Share             Allow  ContainerInherit, ObjectInherit             None  Folder_Share      FullControl
31        False  BUILTIN\Administrators  C:\SHARES\Folder_Share             Allow                    ObjectInherit             None  Folder_Share      FullControl
32        False     BLBEX\Administrator  C:\SHARES\Folder_Share             Allow                    ObjectInherit             None  Folder_Share      FullControl
33        False                Everyone       C:\SHARES\INSTALL             Allow                    ObjectInherit             None       INSTALL      FullControl
34        False                      NT       C:\SHARES\INSTALL             Allow  ContainerInherit, ObjectInherit             None       INSTALL      FullControl
35        False  BUILTIN\Administrators       C:\SHARES\INSTALL             Allow                    ObjectInherit             None       INSTALL      FullControl
36        False     BLBEX\Administrator       C:\SHARES\INSTALL             Allow                    ObjectInherit             None       INSTALL      FullControl
53        False                      NT  C:\SHARES\Vedeni_Share             Allow  ContainerInherit, ObjectInherit             None  Vedeni_Share      FullControl
54        False  BUILTIN\Administrators  C:\SHARES\Vedeni_Share             Allow                    ObjectInherit             None  Vedeni_Share      FullControl
55        False     BLBEX\Administrator  C:\SHARES\Vedeni_Share             Allow                    ObjectInherit             None  Vedeni_Share      FullControl
56        False       BLBEX\pavel.novak  C:\SHARES\Vedeni_Share             Allow                    ObjectInherit             None  Vedeni_Share      FullControl
```

Obrázek 33. NTFS data získaná pro složky začínající vzorem C:\SHARES

6.18.6 Připojení USB

Připojení USB nelze plnohodnotně sledovat pomocí sběru nativních logů v prostředí Windows. Proto je zde uvedený alespoň způsob, který zahrnuje vytvoření události v momentě, kdy se do sítě připojí USB zařízení počítače AUDIT-SONDA. Jedná se o jediný počítač v testovací laboratoři, který má svůj vlastní hardware, tudíž bylo možno toto nastavení přímo otestovat.

```
# USB data
USBWatcherData = usb.logonActivity(setup.client,
      "log-audit-sonda.blbex.cz-2024.")
print("=== USB Watcher Data ===")
print(USBWatcherData)
```

```
=== USB Watcher Data ===
          Host  EventID               ObjectName               Task            Timestamp
0  audit-sonda     4663  \Device\HarddiskVolume13  Removable Storage  11.04.2024 15:51:53
1  audit-sonda     4663  \Device\HarddiskVolume12  Removable Storage  11.04.2024 15:51:53
```

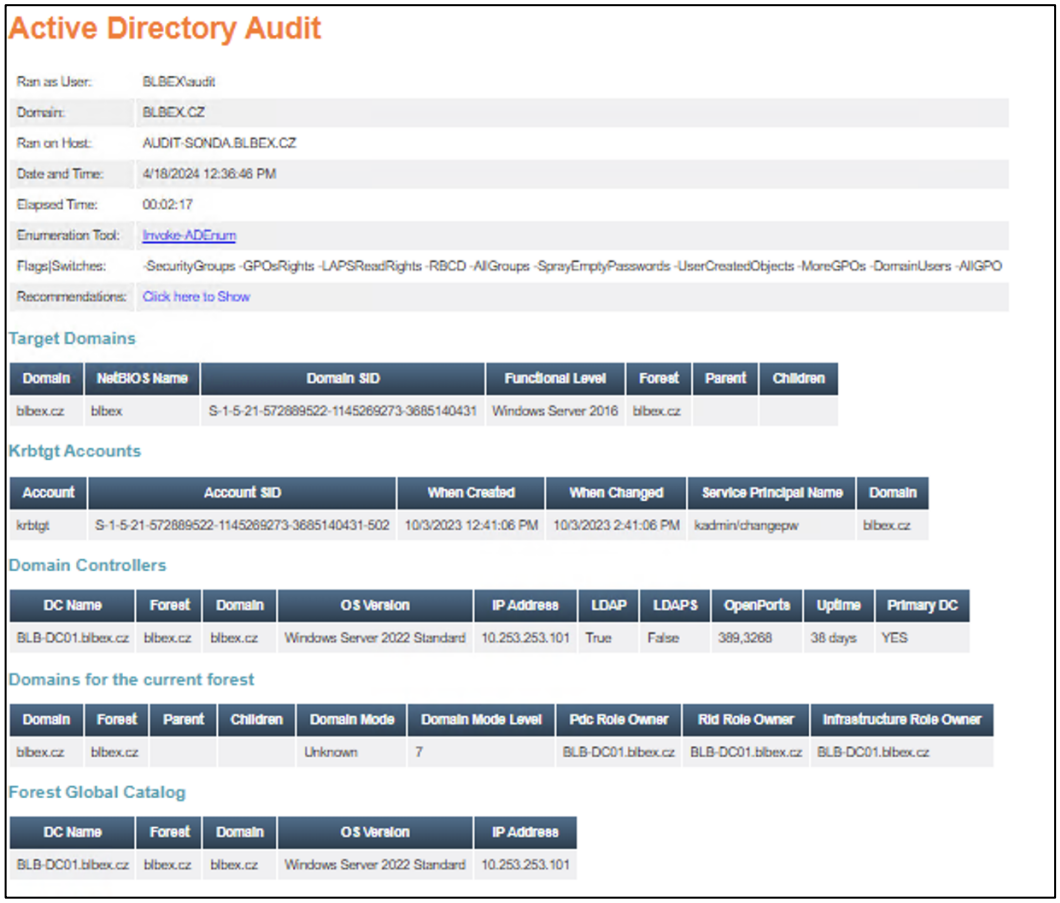
Obrázek 34. USB připojená na počítač auditu

6.18.7 Informace o AD

Jak bylo zmíněno v kapitole 3.4.5 Ivoke-ADEnum, enumerace informací z AD může hrát významnou roli při prvotním zjišťování aktuálního stavu v síti. Tedy, kolik má uživatelů, jaké jsou politiky hesel. Zprávy je možné vyexportovat v CSV formátu, nebo v XLSX.

```
Enterprise Administrators:

Member Name   Enabled Active Last Logon                          Member SID                                    Group Domain
-----------   ------- ------ ----------                          ----------                                    ------------
Administrator True    True   4/6/2024 4:15:03 PM                 S-1-5-21-572889522-1145269273-3685140431-500  blbex.cz
audit         True    True   {4/17/2024 3:23:35 PM, $null, $null} S-1-5-21-572889522-1145269273-3685140431-1112 blbex.cz
```

Obrázek 35. Příklad výpisu Invoke-ADEnum v příkazové řádce



Active Directory Audit

Ran as User:	BLBEX\audit
Domain:	BLBEX.CZ
Ran on Host:	AUDIT-SONDA.BLBEX.CZ
Date and Time:	4/18/2024 12:36:46 PM
Elapsed Time:	00:02:17
Enumeration Tool:	Invoke-ADEnum
Flags|Switches:	-SecurityGroups -GPOsRights -LAPSReadRights -RBCD -AllGroups -SprayEmptyPasswords -UserCreatedObjects -MoreGPOs -DomainUsers -AllGPO
Recommendations:	Click here to Show

Target Domains

Domain	NetBIOS Name	Domain SID	Functional Level	Forest	Parent	Children
blbex.cz	blbex	S-1-5-21-572889522-1145269273-3685140431	Windows Server 2016	blbex.cz		

Krbtgt Accounts

Account	Account SID	When Created	When Changed	Service Principal Name	Domain
krbtgt	S-1-5-21-572889522-1145269273-3685140431-502	10/3/2023 12:41:06 PM	10/3/2023 2:41:06 PM	kadmin/changepw	blbex.cz

Domain Controllers

DC Name	Forest	Domain	OS Version	IP Address	LDAP	LDAPS	OpenPorts	Uptime	Primary DC
BLB-DC01.blbex.cz	blbex.cz	blbex.cz	Windows Server 2022 Standard	10.253.253.101	True	False	389,3268	38 days	YES

Domains for the current forest

Domain	Forest	Parent	Children	Domain Mode	Domain Mode Level	Pdc Role Owner	Rid Role Owner	Infrastructure Role Owner
blbex.cz	blbex.cz			Unknown	7	BLB-DC01.blbex.cz	BLB-DC01.blbex.cz	BLB-DC01.blbex.cz

Forest Global Catalog

DC Name	Forest	Domain	OS Version	IP Address
BLB-DC01.blbex.cz	blbex.cz	blbex.cz	Windows Server 2022 Standard	10.253.253.101

Obrázek 36. Invoke-ADEnum export do HTML

6.18.8 Hardware a operační systém

Informace o hardware, operačním systému a případně i IP adresu jde získat pomocí PowerShell skriptů. Informace nejsou aktivně ukládané do OpenSearch, pouze se aktuálně vypisují na konzoli. Pro přehledné zobrazení je použité zpracování do DataFrame tabulky, navíc lze filtrovat počítače, které byly naposledy restartované před určeným dnem. Jelikož počet laboratorních počítačů je poměrně malý, od dalších filtrů bylo upuštěno z důvodů nedostatečného počtu dat pro testování.

```
# HW informace
hwinfo.setupPandasDisplay()
output = hwinfo.runPowershellScript()
df=[]
if output:
    df = hwinfo.parseOutputToDataFrame(output)
    print(df[['PSComputerName', 'Caption', 'Version',
            'LastBootUpTime','IP']])
    filtered_df = hwinfo.filter_by_reboot_days(df, 2)
    print(filtered_df[['PSComputerName', 'Caption', 'Version',
      'LastBootUpTime','IP']])
```

Výsledek kódu, který demonstruje možnost filtrace na počítače, které nebyly restartovány před dvěma dny. První tři řádky v ukázce jsou vypsané bez filtru, následující ukazuje vyfiltrované počítače, které ještě nebyly

```
  PSComputerName                          Caption     Version        LastBootUpTime                      IP
0       BLB-DC01  Microsoft Windows Server 2022 Standard  10.0.20348   3/10/2024 1:05:33 PM  10.253.253.101, 127.0.0.1
1       BLB-PC01               Microsoft Windows 10 Pro  10.0.19045   4/19/2024 9:45:03 AM   10.253.253.51, 127.0.0.1
2       BLB-PC02               Microsoft Windows 10 Pro  10.0.19045  4/10/2024 11:38:30 PM   10.253.253.52, 127.0.0.1
  PSComputerName                          Caption     Version      LastBootUpTime                      IP
0       BLB-DC01  Microsoft Windows Server 2022 Standard  10.0.20348 2024-03-10 13:05:33  10.253.253.101, 127.0.0.1
2       BLB-PC02               Microsoft Windows 10 Pro  10.0.19045 2024-04-10 23:38:30   10.253.253.52, 127.0.0.1
```

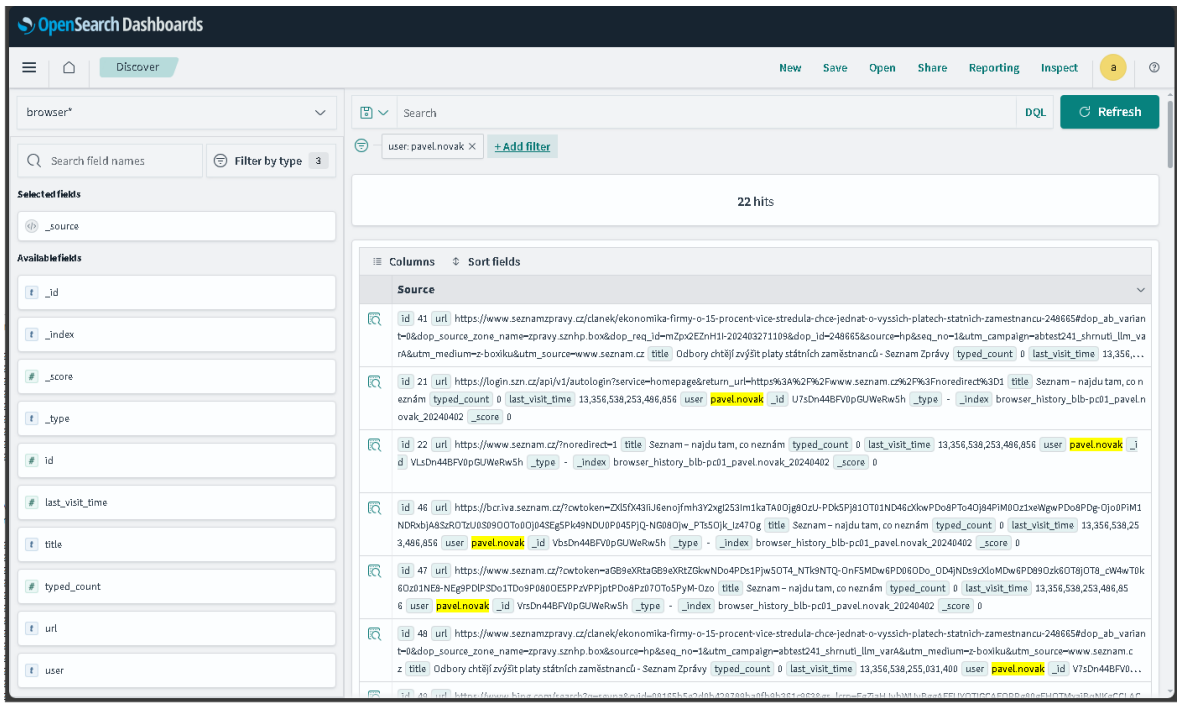
Obrázek 37. Informace o hardware a jeho filtrace na základě restartu

6.19 Testování dat

Pomocí OpenSearch Dashboard se lze přesvědčit, jestli filtrování, případně sběr dat a následné parsování opravdu funguje. Jako příklad jsou uvedená data z historie prohlížeče. V Dashboard lze navolit vlastní vzor indexu (Index Pattern).

`Dashboard Manager->Index patterns`

Ten na základě zadaného počátku indexu vyhledá všechny, které jsou s ním spojené. Což je stejný systém, který je používaný v rámci vyhledávání pomocí python kódů. To znamená, že při zadání počátku prefixu indexu „browser“ najde všechny indexy začínající tímto pravidlem. V záložce Discovery se zvolí tento předem nakonfigurovaný vzor, což zobrazí všechna data, která jsou v indexech uložena. Data, která poskytne Dashboard jsou porovnána s těmi, která nabídne python kód. Takto byl OpenSearch Dashboard využívaný v rámci celého vývoje. Umožňuje i filtraci, což ukazuje demo níže. Při zadání DQL dotazu Dashboardu a specifikaci, že je třeba nalézt všechny záznamy, které mají uživatele jménem Jan Kulička, najde dashboard 59 výsledků, totéž najde i python kód.



Obrázek 38. Výsledek dotazu na historii prohlížeče uživatele Pavla Nováka

```
=== Browser History Data ===
       lastVisitTime        user       ipAddress        Country  id
11  2024-04-02 15:30  pavel.novak   185.66.189.31        Czechia  41
12  2024-04-02 15:30  pavel.novak    77.75.78.104        Czechia  21
13  2024-04-02 15:30  pavel.novak    77.75.77.222        Czechia  22
14  2024-04-02 15:30  pavel.novak     77.75.79.3         Czechia  46
15  2024-04-02 15:30  pavel.novak    77.75.77.222        Czechia  47
16  2024-04-02 15:30  pavel.novak   185.66.189.31        Czechia  48
17  2024-04-02 15:30  pavel.novak  23.212.110.209        Czechia  49
18  2024-04-02 15:31  pavel.novak  23.212.110.209        Czechia  58
19  2024-04-02 15:31  pavel.novak  23.212.110.209        Czechia  59
20  2024-04-02 15:31  pavel.novak  204.79.197.203  United States  38
21  2024-04-02 15:31  pavel.novak   142.251.36.99  United States  57
22  2024-04-02 15:31  pavel.novak   142.251.36.99  United States  56
23  2024-04-02 15:31  pavel.novak   185.66.189.31        Czechia  55
24  2024-04-02 15:31  pavel.novak     77.75.79.3         Czechia  53
25  2024-04-02 15:31  pavel.novak   185.66.189.31        Czechia  50
26  2024-04-02 15:31  pavel.novak   185.66.189.31        Czechia  52
27  2024-04-02 15:31  pavel.novak   35.208.115.57  United States  60
28  2024-04-02 15:31  pavel.novak   185.66.189.31        Czechia  54
29  2024-04-02 15:31  pavel.novak    77.75.77.222        Czechia  20
30  2024-04-02 15:31  pavel.novak    77.75.79.222        Czechia  19
31  2024-04-02 15:31  pavel.novak    77.75.78.104        Czechia  51
32  2024-04-02 15:31  pavel.novak   35.208.115.57  United States  61
```

Obrázek 39. Výsledek stejného dotazu pomocí Python kódu

6.20 Porovnání řešení oproti počátečnímu stavu

Původní stav testovacího prostředí byl charakterizovaný minimálním provozem a absencí jakýchkoliv předchozích nastavení specifických pro monitorování, což mělo za cíl zajistit přehlednost a důvěryhodnost výsledků. V síti byly pouze základní virtuální stanice a servery bez speciálního řešení pro sledování činností, což odpovídalo běžným podmínkám u skutečných zákazníků. Doménový řadič neměl nastavené žádné monitorovací politiky prostředí Windows, což omezovalo možnosti pro hloubkový monitoring bezpečnostních rizik.

Implementace monitorovacího řešení představuje přechod od základního nastavení k řešení, které je schopno sledovat různé aspekty síťové aktivit. Změny zahrnují zavedení pokročilých funkcionalit, jako jsou sledování přihlášení a odhlášení uživatelů, monitoring přístupů do sdílených složek a jejich modifikací, a sběr dat o aktivitách na firewallových pravidlech. Tato nová řešení umožňují získat hlubší vhled do chování uživatelů a potenciálních bezpečnostních hrozeb.

ZÁVĚR

Tato práce zahrnuje postup, nástroje a řešení monitoringu aktivit uživatelů na platformě Windows, který pomohl firmě s řešením zadaných požadavků. Sledování přihlašování uživatelů, změny ve sdílených souborech na síti, výpis oprávnění přístupů k těmto souborům, komunikace na firewallech či výpis nastavení v AD nevyžadují nadále manuální procházení. Bezpečnostní logy ze všech stanic a serverů jsou centrálně sbírané na jedno místo a mohou být archivované, nebo posloužit k následující analýze. Vše lze filtrovat dle požadavků zadání firmy pomocí úprav parametrů jednotlivých funkcí. Navíc je řešení podpořené grafickým znázorněním dat, byť analýza není předmětem této práce.

V rámci práce jsem měla možnost seznámit se způsoby komunikace počítačů v síti Windows a vyzkoušet v praxi několik technologií, které jsem mohla vyzkoušet včetně WinRM, PsExec a PowerShell. Což platí i o využití nástrojů jako OpenSearch, Logstash a Winlogbeat pro automatizované zpracování a indexaci logů. Zkusila jsem si napsat svého vlastního agenta na stanice, který se automaticky spouští a dokáže komunikovat přímo s databází OpenSearch a odesílat požadovaná data. Navíc právě díky základu postavenému na OpenSearch a implementaci v Docker kontejnerech, je systém připravený na budoucí rozvoj a integraci dalších technologií, jako je strojové učení, což může být předmětem výzkumu a vývoje v rámci diplomové práce.

Jak již bylo uvedeno v úvodu, hlavním cílem bylo zjistit, zda je možné pomocí této metody efektivně sbírat výše zmíněná klíčová data. Odpověď je jednoznačně kladná. Pro budoucí rozvoj systému by však bylo nutné implementovat komplexnější řešení, které by zahrnovalo rozšíření agenta na stanicích a serverech, včetně automatické instalace na jednotlivé stanice. Rozvoj by umožnil zahrnout i pokročilé monitorování RDP komunikace a používání externích zařízení. Zároveň je v budoucím vývoji zahrnuto i přívětivé uživatelské prostředí. Tím by mohl vzniknout lehký, ale mocný nástroj na monitoring základních aktivit uživatelů firmy.

Softwary třetích stran bez pochyby nabízí komplexnější řešení, s hlubším vhledem, ale i takové nástroje jako Zabbix musely projít fází vývoje, při které vývojáři zkoumali detaily, aby pochopili, jakým směrem se vydat. Zkoumání vývoje a možností implementace svého řešení bylo hlavním cílem této práce a věřím, že byl náležitě splněn.

SEZNAM POUŽITÉ LITERATURY

[1] ŠULC, Vladimír. *Kybernetická bezpečnost.* 1. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

[2] ČESKÁ REPUBLIKA, 2014. Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: 181/2014. 75/2014.

[3] ČESKÁ REPUBLIKA, 2022. Zákon 226/2022 Sb., Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů. In: 226/2022 Sb. částka 104/2022.

[4] NÁRODNÍ ÚŘAD KYBERNETICKÉ BEZPEČNOSTI, 2024. *Zpráva o stavu kybernetické bezpečnosti České Republiky za rok 2022.* Online. In: Národní Úřad pro Kybernetickou Bezpečnost. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/2073-nukib-v-roce-2023-zaznamenal-rekordni-pocet-kybernetickych-incidentu/. [cit. 2024-02-21]

[5] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU BEZPEČNOST, 2020. *Aktualizace informací o hrozbě Emotet-Trickbot-Ryuk.* Online. Národní Úřad pro Kybernetickou bezpečnost. Dostupné z: https://nukib.gov.cz/cs/infoservis/hrozby/1483-aktualizace-informaci-o-hrozbe-emotet-trickbot-ryuk/. [cit. 2024-02-21

[6] GALLAGHER, Sean, 2014. *Inside the "wiper" malware that brought Sony Pictures to its knees [Update].* Online. Cyber Law. Dostupné z: https://arstechnica.com/information-technology/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/. [cit. 2024-02-21]

[7] SKELTON, Sebastian Klovig, 2021. *Destruction and integrity cyber attacks on the rise.* Online. Computer Weekly. Dostupné z: https://www.computerweekly.com/news/252504825/Destruction-and-integrity-cyber-attacks-on-the-rise. [cit. 2024-02-21]

[8] *CVE Details Microsoft Windows 10 22h2*, 2024. Online. In: CVE Details. Dostupné z: https://www.cvedetails.com/version-list/26/125376/1/Microsoft-Windows-10-22h2.html?sha=5686228450d7ec74f12190900963f263d16c3998&order=1&trc=98. [cit. 2024-02-28]

[9] PETROSYAN, Ani, 2024. *Number of phishing domain names worldwide: Number of unique phishing sites detected worldwide from 3rd quarter 2013 to 2nd quarter 2023*. Online. In: Statista. Dostupné z: https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/. [cit. 2024-02-21]

[10] Critical Patches issued for Microsoft Products January 2024, 2024. Online. Cisecurity. Dostupné z: https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products-january-09-2024_2024-002. [cit. 2024-02-21].

[11] IBM, 2024. *What is network security?* Online. IBM. Dostupné z: https://www.ibm.com/topics/network-security. [cit. 2024-02-25]

[12] *Today's Massive Ransomware Attack Was Mostly Preventable; Here's How To Avoid It*, 2017. Online. Gizmodo International. Dostupné z: https://gizmodo.com.au/2017/05/todays-massive-ransomware-attack-was-mostly-preventable-heres-how-to-avoid-it/. [cit. 2024-02-25]

[13] BUDAI, David, 2012. *Sociální inženýrství v praxi: Když si hacker o heslo prostě řekne.* Online. CNews. Dostupné z: https://www.cnews.cz/clanky/socialni-inzenyrstvi-v-praxi-kdyz-si-hacker-o-heslo-proste-rekne/. [cit. 2024-02-28]

[14] STORCHAK, Yana, 2023. *Top 10 Best-Known Cybersecurity Incidents and What to Learn from Them.* Online. Ekran System. Dostupné z: https://www.ekransystem.com/en/blog/top-10-cyber-security-breaches. [cit. 2024-02-28]

[15] DOLEJŠÍ, Milan, 2022. *Obnova systémů ŘSD po kyberútoku stála desítky milionů. Brzy má opět fungovat i web s dopravními informacemi.* Online. Česká Televize. Dostupné z: https://ct24.ceskatelevize.cz/clanek/domaci/obnova-systemu-rsd-po-kyberutoku-stala-desitky-milionu-brzy-ma-opet-fungovat-i-web-s-dopravnimi-info-17479. [cit. 2024-02-29]

[16] DOUGLIS, F. a KRIEGE, O. Virtualization. Online. Roč. 2013, č. 2, s. 6-9. ISSN 1941-0131. Dostupné z: https://doi.org/10.1109/MIC.2013.42. [cit. 2024-03-25].

[17] SIMMONS, Curt, 2001. *Active Directory™ Bible*. 1. IDG Books Worldwide. ISBN 0-7645-4762-3

[18] PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009. ISBN 978-80-7232-388-3.

[19] WHITEHEAD, Coletta Teske, 2022. *What is LAN: The definition of and uses for a local area network.* Online. In: Life Wire. Dostupné z: https://www.life-wire.com/what-is-lan-4684071. [cit. 2024-03-03]

[20] MICROSOFT, 2023. *Local Accounts.* Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts. [cit. 2024-03-06]

[21] MICROSOFT, 2023. *Active Directory accounts.* Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-default-user-accounts. [cit. 2024-03-06]

[22] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU BEZPEČNOST, 2023. Minimální bezpečnostní standard. 1. 1. NUKIB.

[23] Role-Based Access Control (RBAC), 2022. Online. Impreva. Dostupné z: https://www.imperva.com/learn/data-security/role-based-access-control-rbac/. [cit. 2024-03-06]

[24] MICROSOFT, 2023. How User Account Control works. Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/en-us/windows/security/application-security/application-control/user-account-control/how-it-works. [cit. 2024-03-13]

[25] BASHROUSH, Rabih; JAHANKHANI, Hamid a AL-NEMRAT, Ameer Al-Nemrat, 2012. *Sufficiency of Windows Event Log as Evidence in Digital Forensics.* Online. In: Global Security, Safety and Sustainability & e-Democracy. 1. University of East London, s. 253–262. ISBN 978-3-642-33447-4. Dostupné z: https://link.springer.com/book/10.1007/978-3-642-33448-1. [cit. 2024-03-13]

[26] MICROSOFT, 2021. *Audit logon events.* Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/cs-cz/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/basic-audit-logon-events. [cit. 2024-03-12]

[27] Auditování bezpečnostních událostí windows v doméně. Samuraj [online]. 2018 [cit. 2024-03-11]. Dostupné z: https://www.samuraj-cz.com/clanek/auditovani-bezpecnostnich-udalosti-windows-v-domene/

[28] Group Policy Storage. Learn Microsoft [online]. 2018 [cit. 2024-03-11]. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-storage

[29] BERLIN, Konstantin; SLATER, David a SAXE, Joshua, 2015. *Malicious Behavior Detection using Windows Audit Logs*. Pracovní studie. Ithaca: Cornell University Library arXiv.org.

[30] Security for Microsoft Windows System Administrators [online]. 1. Syngress, 2011 [cit. 2024-03-13]. ISBN 978-1-59749-594-3. Dostupné z: doi:https://doi.org/10.1016/C2009-0-64311-7

[31] MICROSOFT, 2023. Monitoring Active Directory for Signs of Compromise. Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise. [cit. 2024-03-14]

[32] MICROSOFT, 2021. Audit account logon events. Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/basic-audit-account-logon-events. [cit. 2024-03-14]

[33] MICROSOFT, 2021. 4624(S): An account was successfully logged on. Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624. [cit. 2024-03-14].

[34] MICROSOFT, 2021. Audit logon events. Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/cs-cz/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/basic-audit-logon-events. [cit. 2024-03-12]

[35] MICROSOFT, 2021. Audit object access. Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/basic-audit-object-access. [cit. 2024-03-14].

[36] MICROSOFT, 2023. Audit Policy Recommendations. Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations. [cit. 2024-03-15]

[37] VILLANUEVA, Mark Sheldon, 2021. Pros and Cons of Implementing SIEM. Online. ITASAP. Dostupné z: https://www.itsasap.com/blog/pros-cons-siem. [cit. 2024-03-15].

[38] WIESNER, MIRIAM C., 2023. PowerShell Automation and Scripting for Cybersecurity. Pdf. 2023. Packt Publishing. ISBN 978-1-80056-637-8. Dostupné z:

https://www.packtpub.com/product/powershell-automation-and-scripting-for-cybersecurity/9781800566378. [cit. 2024-03-26].

[39] MICROSOFT, 2023. Windows Remote Management. Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/en-us/windows/win32/winrm/portal. [cit. 2024-04-02].

[40] MICROSOFT, 2023. Windows Management Instrumentation. Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/en-us/windows/win32/wmisdk/using-wmi. [cit. 2024-03-26].

[41] MICROSOFT, 2023. PsExec. Online. Learn Microsoft. Dostupné z: https://learn.microsoft.com/en-us/sysinternals/downloads/psexec. [cit. 2024-03-26].

[42] LP, Rob, 2024. Invoke-ADEnum. Online. Github Repository. Dostupné z: https://github.com/Leo4j/Invoke-ADEnum. [cit. 2024-04-18].

[43] OPENSEARCH, 2024. Introduction to OpenSearch. Online. OpenSearch. Dostupné z: https://opensearch.org/docs/latest/intro/. [cit. 2024-04-02].

[44] ELASTIC, 2024. Logstash. Online. Elastic Stack. Dostupné z: https://www.elastic.co/logstash. [cit. 2024-04-02].

[45] ELASTIC, 2024. Winlogbeat. Online. Elastic Stack. Dostupné z: https://www.elastic.co/guide/en/beats/winlogbeat/current/_winlogbeat_overview.html. [cit. 2024-04-02].

[46] ČESKÁ REPUBLIKA, 2006. Zákon zákoník práce: č. 262/2006 sb. In: 2006.

[47] OPENSEARCH, 2024. Installing OpenSearch. Online. OpenSearch. Dostupné z: https://opensearch.org/docs/latest/install-and-configure/install-opensearch/docker/. [cit. 2024-04-03].

[48] ELASTIC, 2023. Syslog input plugin. Online. Elastic Stack. Dostupné z: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-syslog.html. [cit. 2024-04-03].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory
DNS	Domain Name System
DQL	Data Query Language
DSL	Domain-Specific Language
GPC	Group Policy Container
GUID	Globally Unique Identifier
HW	Hardware
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation
NTFS	New Technology File System
NÚKIB	Národní Kybernetický Úřad
OSI	Open Systems Interconnection
RDP	Remote Desktop Protocol
SIEM	Security Information and Event Management
SMB	Server Message Block
SQL	Structured Query Language
TCP	Transmission Control Protoco
UAC	User Acces Control
WinRM	Windows Remote Management
WINS	Windows Remote Management
WMI	Windows Management Instrumentation

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: NÁZEV PŘÍLOHY

Struktura obsahu přiloženého CD:

- Adresář Text bakalářské práce – obsahuje text bakalářské práce ve formátu PDF/A
- Adresář Monitoring – obsahuje programovou část práce