Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Group policy security baseline pro OS Windows

Bakalářská práce

Autor: Jiří Obst
Studijní obor: Informační management

Vedoucí práce: Ing. Tomáš Svoboda Ph.D.

Hradec Králové Duben 2024

Prohlášení:

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

V Hradci Králové dne 14.4.2024 Jiří Obst

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Tomáši Svobodovi, Ph.D. za metodické vedení práce a profesionální přístup.

Anotace

Tato bakalářská práce se zabývá tvorbou bezpečnostních politik GPO ve Windows Serveru 2022 a Windows 11 od společnosti Microsoft. Teoretická část práce přináší přehled historického vývoje operačních systémů Windows a Linux, konceptů bezpečnosti a principů GPO politik. Praktická část je pak zaměřena na analýzu a implementaci 5 konkrétních případů užití (dále jen usecase). Každý usecase je detailně popsán prostřednictvím postupů a ověření funkčnosti, které jsou ilustrovány obrázky z prostředí Windows Serveru a operačního systému Windows. Každý usecase obsahuje 3 až 5 bodů, které jsou pečlivě zpracovány, ověřeny a zdokumentovány. Text poskytuje komplexní pohled na problematiku, kterou daný usecase řeší. Pro tvorbu praktické části byly vybrány nejběžněji používané bezpečnostní politiky GPO. Praktická část práce je rozčleněna do kapitol, přičemž každá kapitola se věnuje konkrétnímu tématu. V práci jsou popsány využité prostředky a softwarová řešení použitá při tvorbě praktické části.

Klíčová slova: Microsoft Azure, Windows Server, Operační systémy, Microsoft Windows, Active Directory

Annotation

Title: Group Policy Security Baseline for Windows OS

This bachelor's thesis examines the creation of GPO security policies in Windows Server 2022 and Windows 11 from Microsoft. The theoretical part of the thesis provides an overview of the historical development of Windows and Linux operating systems, security concepts and principles of GPO policies. The practical part then focuses on the analysis and implementation of 5 specific use cases (usecases). Each usecase is described in detail through procedures and functional verification, which are illustrated with images from Windows Server and Windows environments. Each usecase contains 3 to 5 points that are carefully developed, verified and documented. The text provides a comprehensive view of the

issues addressed by the usecase. The most commonly used GPO security policies were selected for the practical part. The practical part of the thesis is divided into chapters, with each chapter focusing on a specific topic. The thesis describes the resources used and the software solutions used in the development.

Keywords: Microsoft Azure, Windows Server, Operating Systems, Microsoft Windows, Active Directory

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Tato bakalářská práce se zaměřuje na oblast IT a kyberbezpečnosti. V dnešní době se informační technologie a jejich využití rozšířily do všech oborů lidské činnosti. Použití IT technologií nese i rizika kybernetických útoků s cílem zajistit nedostupnost dat nebo jejich zneužití. Moderní operační systémy podporují spoustu mechanismů, jak těmto problému předcházet. Existují různé mechanismy, jak zajistit bezpečnost IT systému, respektive OS. Jedním z mechanismů zajištění bezpečnosti jsou GPO (skupinové politiky). GPO je soubor různých nastavení politik, které umožňují centralizovaně řídit chování počítačů a uživatelů v rámci domény systému Windows. Pro účely práce byly použité Windows Server 22 a Windows 11, jedná se o nejnovější verze systému od společnosti Microsoft. Bakalářská práce podrobně představuje úvod do OS, informační a kybernetické bezpečnosti s důrazem na využití GPO pro zajištění bezpečnosti. Dále pracuje s konfiguracemi samotných lokálních a globálních politik (GPO) na předem definovaných use cases.

2 Cíl práce

Cíle teoretické část

- Představit problematiku OS a jejich využití:
    - Představit historii operačních systémů s důrazem na platformu Windows a Linux.
- Představit problematiku informační a kybernetické bezpečnosti:
    - Požadavky na důvěrnost, dostupnost a integritu dat.
- Představit modely zajištění ochrany dat:
    - Představení možností pro řešení ochrany dat.
- Představení GPO:
    - Typy politik dle úrovně použití (domain, forest, organizational unit).
    - Lokální a globální politiky.

Praktická část

Výstupem praktické části je ověření nasazení GPO na předem definovaných use cases. V této práci je použito celkem pět use cases. Každý use cases cílí na jinou problematiku v rámci celé kyberbezpečnosti ve Windows Server 22 a Windows 11.

3 Operační systémy

Operační systém je v dnešní době běžnou součástí každého počítače. Primárním účelem operačního systému je komunikace mezi hardwarem a uživatelem prostřednictvím uživatelského rozhraní. Sekundárním účelem je zajištění komunikace mezi Hardware a firmware. Firmware je software hardwaru, jedním z příkladů je BIOS (UEFI).

Předchůdcem současných moderních operačních systémů byly děrné štítky, které nebyly vždy spolehlivé. V průběhu vývoje IT techniky, hardware a software, kam spadají i operační systémy došlo k výraznému zdokonalení těchto komponent z hlediska výkonových parametrů, poskytovaných služeb a samozřejmě i uživatelského rozhraní. Většina současných moderních operačních systémů podporuje základní potřebné nástroje, služby a aplikace využitelné pro uživatele i administrátory. Mezi hlavní uživatelské funkce spadá využívání přehrávače audia, videa, kodeky, aplikace a služby. Vše musí být kvalitně zoptimalizováno, aby bylo dosaženo nejvyššího výkonu. [1]

Aktuální situace na trhu s operačními systémy je silně konkurenční. Můžeme vybírat podle poskytovaných služeb, podpory ze strany výrobce, naplnění uživatelských požadavků, bezpečnosti a ceny. Na trhu jsou serverové či desktop distribuce. Každá z těchto distribucí je zaměřena na poskytování odlišných služeb a jejich využití.

3.1 Windows

Windows je grafický operační systém vyvinutý a spravovaný společností Microsoft. Nejnovější verzí je NT 10.0. V této verzi se nachází Windows 11, určený pro desktopové řešení. Sekundárním produktem je Windows Server 2022. [2]

Desktopová verze Windows má různé druhy licencování. Existují tři typy licencí. První licence je takzvaná FPP (Full Packaged Product) licence. Tuto licenci kupuje běžný zákazník, který chce licenci Windows na svoje zařízení. Licence je dostupná i po upgradu mezi Windows (z Windows 10 na Windows 11). Hlavní výhodou je její přenositelnost mezi zařízeními. Druhou licencí je OEM licence (Original Equipment Manufacturer). Druh této licence se váže s hardwarem zařízení,

kde je Windows použit. Toto řešení používají především společnosti, který vyrábí počítače nebo laptopy. Mezi takové společnosti spadají například společnosti DELL, HP, Asus či Lenovo. Na zařízení je předinstalovaný Windows, který si zákazník přizpůsobí či nastaví vlastním predikcím. Třetím a zároveň posledním typem licencí je Volume Licenses (Multilicencování). Tento typ licence má určení ve velkých společnostech, školách či organizacích. Společnost musí být registrována, aby měla přístup k těmto licencím. Z pravidla se používá jeden klíč na více zařízeních pomocí serveru KMS popřípadě MAK. [3]

Serverová verze Windows má tři druhy licencí. První licencí je Datacenter edition. Tato licence je využívaná pro cloudová či datacentrová řešení, předpokládá se i vysoká míra virtualizace. Licencování se opírá o počet jader (pouze fyzických jader) na serveru. V základu je počítáno s 16 jádry. Druhou licencí je Standard edition. Tato edice je určena pro fyzické prostředí ale lze využít i minimálně virtualizované prostředí. Licencování je stejné jako u verze Datacenter edition, rozdíl je jen v cenách. Poslední verzí licencování je Essentials edition. Určené pro menší společnosti. Zohledňuje se 25 uživatelů a maximálně 50 zařízení. V této licenci se licencuje dle počtu jader (max 10 jader) a jeden virtuální počítač. [4,5]

Tabulka 1 Licence Windows Server 22

Edice	Licencování	Cena
Datacenter	Dle počtu jader	6 155 USD
Standart	Dle počtu jader	1 069 USD
Essentials	Speciální servery	501 USD

Zdroj: vlastní. Upraveno dle [5]

Desktopové verze se nerozdělují jen dle licence. Dělí se na edice. Edice jsou různé a záleží na zákazníkovi, kterou si zvolí. Jsou rozděleny do třech skupin. Každá skupina má specifické funkce a využití. První je edice Home. Jedná se základní verzi Windows. Používá se na většině koupených zařízení v rámci OEM licence. Zároveň se jedná o nejlevnější edici. Pokročilou a druhou edicí je Pro. Tato edice je rozšířením základní verze. Podporuje spoustu rozšířených, pokročilých vlastností. Příkladem

je vzdálená plocha, Bitlocker či Group policy management. Poslední třetí edicí je Business, pracovně nazvané Professional. Určení je pro pracovní stanice. Nachází se zde pokročilé funkce pro velké společnosti, podniky. [6]

3.1.1 Historie

Prvním produktem společnosti Microsoft byl takzvaný MS-DOS, který byl vydaný v roce 1981. Jeho primárním účelem byla komunikace uživatele se systémem pomocí příkazové řádky. V následujících letech Microsoft vyvinul aplikaci s názvem Windows ve verzi 1.0. Tato verze byla vyvinuta v roce 1985. Windows fungoval jako aplikace na starším systému MS-DOS. Tyto systémy byly označovány jako Windows pro MS-DOS. V roce 1995 byl vydán Windows 95. Tato verze se přiblížila k dnešním moderním operačním systémům od Microsoft. Bylo přidáno tlačítko start a celá nabídka start. Dalším velkým krokem bylo představení, dnes již mrtvého, Internetu Exploreru. O tři roky později, rok 1998, Microsoft vydává Windows 98. Hlavní výhodou je přidaná podpora USB a vylepšení funkčnosti. Posledním Windows z řady pro MS-DOS se stal Windows Millennium Edition. Tento Windows byl velmi problémový a neoblíbený. [7,8]

Microsoft přechází na NT (New technology – nová technologie). Tato technologie bylo uvedena v roce 1993. Měla vyšší hardwarové nároky než MS-DOS Windows. Primárním účelem této technologie byla použitelnost bez MS-DOS. Microsoft tuto technologii původně zamýšlel pro použití ve firemních prostředích. Tato technologie byla využívána do roku 1996, poté její vývoj Microsoft zastavil. V roce 2000 se Microsoft k NT technologii vrací a vydává Windows s názvem Windows 2000 neboli Windows NT 5.0. Ve verzi je i přítomný Windows Server. V roce 2001 Microsoft oznamuje a vydává Windows XP neboli Windows NT 5.1. Jedná se o 32bitovou verzi, 64bitová verze je vydána až v roce 2005 z důvodu nových procesorů (64bitové procesory). Hlavní výhodou byl moderní a nadčasový vzhled a především funkčnost. Tento systém lze označit jako „legendární“. V roce 2007 vychází Windows Vista s pracovním názvem Windows NT 6.0. Jeho silnou stránkou je nový vzhled. Slabou stránkou je nekompatibilita se staršími aplikacemi. Proto Microsoft v roce 2009 vydal Windows 7 s pracovním názvem Windows NT 6.1.

Jeho silnou stránkou je zpětná kompatibilita s programy, aplikacemi a hardwarem. V roce 2012 byl uveden na trh Windows 8 s pracovním názvem Windows NT 6.2. Tato verze byla založená na velkých uživatelských změnách. Byla odebrána nabídka start, která byla nahrazena takzvaným „metrem“. Cílem Microsoftu bylo vytvoření operačního systému, který by byl kompatibilní s celou řadou zařízení (mobil, počítač, Xbox či tablet). O rok později přišel bezplatný upgrade na Windows 8.1, kde byla vrácena nabídka start. V roce 2015 Microsoft vydal Windows 10 s pracovním názvem Windows NT 10.0. Zákazníkům byla přidána možnost upgradu z předchozích verzích na tuto verzi zcela zdarma. Jediná podmínka byla mít aktivovaný Windows. Cílem bylo shrnout všechny platformy do jedné. V roce 2021 byl oznámen a vydán Windows 11 s pracovním názvem Windows NT 10.0. Jedná se o nejaktuálnější verzi Windows. [7,8]

Microsoft rozdělil v letech 2000 až 2003 Windows na dva typy (podle účelu). Windows a Windows Server. V roce 2003 vychází první samotná verze Windows Server. Její výhodou bylo přizpůsobení se specifickým úlohám, například DNS Serveru. O dva roky později vyšla verze s přídavkem R2. Jednalo se víceméně o bezpečnostní update/verzi. V roce 2008 vyšel v pořadí druhý Windows Server 2008. Zásadní změnou bylo vylepšení Active Directory. Byl zde přidán prohlížeč událostí či správce serveru. O déle byla opět vydána verze s přídavkem R2. V roce 2012 vyšla další verze Windows Serveru. Název byl Windows Server 2012. V této verzi Microsoft pracoval na zlepšení práce s cloudem. O rok později byla vydána verze s přídavkem R2, která rozšířila prostředí PowerShell. Cíl zůstal stejný, a to cloudové služby. V roce 2016 vyšla další verze s názvem Windows Server 2016. K této verzi nikdy nevyšla verze s přídavkem R2. Měla dvojí rozdělení. První byla Standart edition, která měla menší kapacitu operací než druhá edice s názvem Datacenter edition. V říjnu roku 2018 vyšel Windows Server 2019. Založen je na Windows 10. Byl vylepšen Windows Defender a přidán OpenSSH. V roce 2021

vyšel aktuální Windows Server 2022. Výhodu je podpora TPM 2.0 a cloudu s názvem Azure.[9]

3.1.2 Rozdělení Windows

Do roku 2000 se používal Windows s potřebou MS-DOS, v dnešní době se už používá pouze větev s názvem NT. Technologie NT byla vytvořena v roce 1994 s předpokladem využití u velkých firem. Následující dva roky byly klíčové pro tuto verzi. Microsoft se rozhodl tuto větev pozastavit. Obnovil ji až v roce 2000 s příchodem Windows 2000, který byl desktopový a zároveň i serverový. V roce 2003 došlo k rozdělení na klasický desktopový Windows a serverový Windows. Tuto podobu Microsoft zachoval do současné doby.

3.2 Linux/Unix

Unix je rodina operačních systémů. Tyto systémy dokážou provozovat multitasking, obsluhu více uživatelů s různými úrovněmi přístupu. Byly vyvinuté v 70. až 80. letech minulého století. Výhodou je, že jsou volně dostupné a mají otevřené kódy. Jsou navržené pro jednoduchost, přenositelnost mezi platformami a účinnost.

Linux je založený na principech jádra operačního systému Unix. Jádro vytvořil Linus Torvalds v roce 1991. Operační systém je málo náročný, tohoto se dá využívat v různých platformách. Linux je vyvíjen velkou základnou lidí, protože se jedná o svobodný software. Má takzvanou GNU General Public License (GNU GPL). Operační systém má distribuce pro server ale i pro klasickou desktopovou verzi. Z toho důvodu existuje spousta distribucí pro každou jednu problematiku. Existují stovky distribucí. [10]

Tabulka 2 Nejpoužívanější edice Linuxu

	Distrowatch	**Tecmint**
1.	MX Linux	MX Linux
2.	Mint	Manjaro
3.	EndeavourOS	Linux Mint

Zdroj: vlastní. Upraveno dle [53,54]

3.2.1 Historie, licencování

V roce 1983 Richard Stallman založil projekt s názvem GNU. Hlavní myšlenkou bylo vytvořit svobodný a otevřený operační systém. GNU se podařilo vyvinout s nástroji a knihovnami. Zásadní problematikou bylo, že systému chybělo jádro. V roce 1991 Linus Torvalds začal pracovat na vlastním jádře. Jádro dostalo název Linux. O rok později se povedlo jádro Linux propojit s knihovnami a nástroji z projektu GNU. Tímto krokem vznikl operační systém GNU/Linux. V roce 1993 vyšla první oficiální verze Linuxu. Byla vedená pod licencí GNU General Public License (GPL). Pod touto licencí šlo svobodně experimentovat, sdílet či modifikovat a distribuovat tento software. V průběhu následujících let začaly vznikat různé distribuce. Mezi ně patřily Debian, Slackware či Red Hat Linux. Pomocí těchto distribucí se začal Linux stávat populárnější na trhu serverů. Bylo to z důvodu malé náročnosti, a především malým pořizovacím nákladům. Největší posun Linux zaznamenal při vstupu na trh s mobilními telefony. Všechny chytré mobilní telefony, které pracují na Androidu jsou uživateli Linuxu. Linux se začal rozšiřovat i do chytrých zařízení, jako jsou ledničky, televize a tak dále. Ve většině distribucí je i volně šířen otevřený software. Jedná se o ekosystém. [10,11]

V aktuální době Linux spadá do licence GNU General Public License (GNU GPL). Licence byla představena v roce 1989 Richardem Stallmanem, tvůrce projektu GNU. Od té doby byla několikrát aktualizovaná (3 verze). Základními principy této licence jsou:

- Používat – Svobodně používat pro jakýkoliv účel bez omezení.
- Studovat – Uživatel má přístup ke zdrojovému kódu. Jeho právo je studovat či modifikovat kód.
- Modifikovat – Software lze upravovat pro svoje účely. Tímto krokem lze podporovat vývoj softwaru pod touto licencí.
- Kompatibilita s dalšími licencemi – Tato licence umožňuje spolupracovat s dalšími licencemi.
- Copyleft – Další distribuce modifikovaného kódu musí být distribuovány pod stejnou licencí.

3.2.2 Využití Linuxu

Linux má díky své nenáročnosti, jednoduchosti a modifikovatelnosti velkou škálu využití. Existuje nepřeberné množství distribucí s různým účelem použitelnosti. Využívá se v síťových prvcích, stolních počítačích, serverech, mobilních zařízení a superpočítačích. Každá z těchto platforem řeší odlišnou problematiku. [12]

- *Serverové systémy* – V této kategorii je Linux velmi často používán. Mnoho služeb jako jsou datové centra, cloudové služby či internetové služby využívají Linuxu. Pro tyto účely se používají edice Debian či CentOS.
- *Webové systémy* – Využívá se zde malé náročnosti. Webový server Apache také funguje na Linuxu. Využití se najde i u hostingových služeb.
- *Desktopové počítače* – Tyto edice jsou určeny pro běžného uživatele, který používá počítač k „základním“ potřebám (internet, kancelářská práce).
- *Superpočítače* – Používá se pro výhodu práce s velkým objemem dat a výpočetních prostředků. V této kategorii jsou tyto potřeby rozhodujícím faktorem.
- *Bezpečnost* – Linux má kvalitní zpracování práce s různými viry. Díky tomu he vůči nim velmi odolný. Tohoto se využívá v bezpečnostních aplikacích, popřípadě firewallových systémech.
- *Embeded systémy* – Tento bod využití je pro normálních spotřebního uživatele, který se nezajímá o hardware, software. Embeded systémy jsou myšleny set-top boxy, chytré domácnosti (chytré televize, ledničky, hodinky, světelné systémy, pračky). Důvodem využití je opět malá náročnost na daný čip v daném zařízení. [12,13]

4 Bezpečnost

Bezpečnost v operačních systémech je prioritním bodem. Primárním bodem bezpečnosti je samotné zabezpečení operačního systému, popřípadě softwaru třetích stran. Sekundárním bodem je chování uživatele. Chování silně ovlivňuje bezpečnost. Definování bezpečnosti je tedy silně různorodé a náročné. V moderních operačních systémech uživateli pomáhá samotný systém. I přes tuto výpomoc lze najít chybu či pochybení v bezpečnosti.

Zanedbání bezpečnosti může mít různé následky. Mezi největší hrozby lze přiřadit ztrátu dat, neoprávněný přístup k zařízení, ztrátu stability či nedodržování právních předpisů. [14]

- *Ochrana dat* – Ve většině operačních systémech se uchovává spoustu dat. Data mohou mít podobu například osobních informací, bankovních údajů či firemních údajů. Zde je potřeba vytvořit bezpečnostní kroky. Tato data jsou citlivá ke zneužití.
- *Virové hrozby* – Jedná se o škodlivý software, který je potřeba podchytit. Bezpečnostní opatření cílí na software, který tyto hrozby dokáže detekovat a zneškodnit. [14]
- *Integrita systému* – Jedná se o bezpečnostní prvek, který zajišťuje očekávanou funkcionalitu operačního systému.
- *Síťová bezpečnost* – V moderní době jsou operační systémy připojeny k síti. Nutností je bezpečnostní rámec pro útoky venku z internetu, který zabrání zneužití dat. [15]
- *Stabilita a dostupnost* – Jedná se o bezpečnostní rámec, který generuje udržitelnost operačního systému. Stabilita je důležitá pro udržení dostupnosti operačního systému. Jinak může docházet k výpadkům či nedostupnosti systému.
- *Právní zákony* – Firmy jsou povinné dodržovat zákony v této problematice. Bez nenastavených právních zákonů bezpečnosti tyto zásady nejdou zaručit. Klíč této problematiky je v nastavených právních zákonech bezpečnosti. [15]

4.1 Zranitelnosti operačních systémů

Zranitelnost operačního systému jsou místa, která jsou lehce zranitelná či zneužitelná. Důležitým prvkem je správné nastavení systému, abychom těmto hrozbám předešli. Většinu těchto prvků lze ovlivnit svým vlastním nastavením či chováním. Zbytek jsou neovlivnitelné námi ale stranou výrobce/vývojáře operačního systému. Při ignoraci těchto parametrů může dojít k poškození systému, ztrátě dat či zneužití citlivých informací. [16,17]

Chyby v kódu – Tento druh zranitelnosti běžný uživatel nemá, jak opravit. Chyby v kódu ovlivní jen v případě čekání na aktualizace. Za tuto zranitelnost nese odpovědnost vývojář daného operačního systému. Následky mohou být pro uživatele nepříjemné. Operační systém nemusím fungovat správně. [17]

Neaktualizovaný software – Za aktuálnost softwaru nese zodpovědnost samotný uživatel. Tento bod se vztahuje k předešlému bodu. Aktualizace mají za účel opravy chyb v kódu, vylepšení a bezpečnost daného operačního systému. Neaktuální systém zvyšuje riziko zneužití.

Slabá autorizace – Jedná se o druh zranitelnosti, kterou nespravuje sám operační systém. Uživatel si musí nastavit autorizaci dle svého uvážení. Obecně v moderních operačních systémech platí pravidlo administrátora, který má přístup ke všemu. Zbytek uživatelů se musí „ptát“ administrátora.

Škodlivý software – Této problematice lze předejít dvěma způsoby. Primární způsob je předcházení těmto hrozbám. Potřebná dávka pozornosti a opatrnosti je nutná. Sekundární způsob je používání softwaru třetích stran, který škodlivý software dokáže rozpoznat.[16]

Síťové služby – Prvky síťových služeb v operačních systémech také nese hrozbu. Hrozbou může být vzdálený útok pomocí sítě.[17]

Nastavení firewallu – Pro běžného uživatele je firewall defaultně nastavený po čisté instalaci operačního systému. V případě serverových služeb je potřeba firewall nastavit, aby fungoval správně dle našich požadavků. Pomocí firewallu lze blokovat určitý provoz v síti a tím předcházet hrozbám. [16,17]

4.2 Parametry bezpečnosti

Pokud není uvedeno jinak, vychází následujících kapitola ze zdrojů.[18]

Parametry bezpečnosti v operačních systémech jsou souhrnem pravidel a opatření, který zajistí určitý stupeň bezpečnosti a ochrany. Parametry se rozdělují podle toho, jaké využití bude mít operační systém. Správné nastavení parametrů bezpečnosti vede k zajištění stability, integrity, důvěrnosti, ochrany dat a dostupnosti operačního systému. [18]

Uživatelské účty – Tento parametr je základem bezpečnosti. Určujeme tím, kdo bude administrátor. Administrátor má přístup k celému operačnímu systému. Zbytek účtů jsou běžní uživatele, kteří nemají takové oprávnění.

Oprávnění – Oprávnění se váže k předešlému bodu (uživatelské účty). Oprávněním můžeme kontrolovat běžné účty, popřípadě jim dávat určitá privilegia. Privilegia mohou mít různé podoby. Úplný přístup či částečný. Podstatným parametrem je, jaký operační systém používáme.

Aktualizace – Podstatné je udržovat aktuální verze operačního systému. Aktualizace zajišťují bezpečností parametry pro správnou funkčnost, stabilitu, důvěryhodnost.

Šifrování – Šifrování je pokročilý způsob parametrů bezpečnosti. Používá se pro šifrování dat na disku a práci s nimi. Cílem je utajit citlivá, důležitá data před určitou hrozbou.

Antivirový software – Jedná se software třetích stran. Detekuje a odstraňuje škodlivý software. Pro plnou funkčnost, musí být plně aktualizován

Správa hesel – Pro primární parametr bezpečnosti jsou potřebná kvalitní a silná hesla. Sekundární parametr je po určité pravidelné časové době změna hesla. Lze jimi ochránit před neoprávněným přístupem.

Biometrická ověření – Zavedením biometrického ověřování lze ochránit data a operační systém. Jedná se o otisky prstů nebo rozpoznání obličeje. Primární využití je u mobilních zařízení nebo laptopů.

Síťová bezpečnost – Zabezpečení je potřebné mít i na úrovni sítě, kde je možnost šifrování komunikace. Nutnost je používat bezpečnostní síťové protokoly, které jsou většinou šifrované.

Dvoufázové ověření – Tento parametr bezpečnosti funguje na principu dvojitého ověření. Primární funkce je samotné zadání hesla. Sekundární funkce je ověření dle mobilu či SMS zprávy.

Záloha a obnova dat – Záloha dat pomáhá k možnosti obnovy operačního systému. V případě nějakého virového útoku, lze operační systém obnovit. Nedochází ke ztrátě citlivých dat, jsou zálohované. [18]

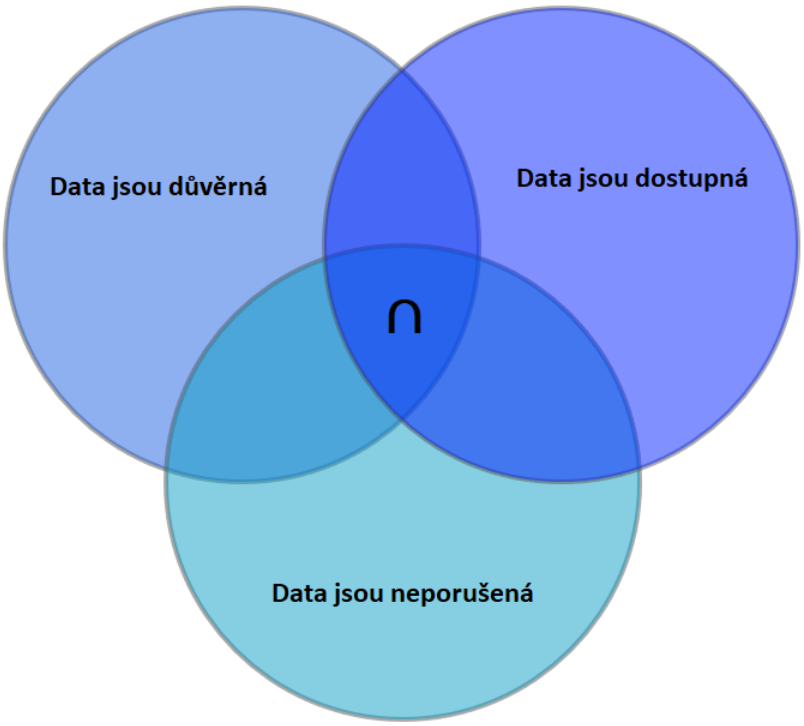
4.2.1 CIA Triáda

CIA triáda je koncept informační bezpečnosti. Zkratka CIA představuje tři anglické výrazy (Confidentiality, Integrity a Availability). V češtině mluvíme o důvěrnosti, integritě a dostupnosti. Popisuje tři základní charakteristiky rizik, které mohou nastat. Projevuje se v kybernetické bezpečnosti. Poskytuje vysokou úroveň bezpečnosti, která je základním stavebním kamenem. Jedná se o účinný způsob, jak rozpoznat slabá místa v operačních systémech a sítích. [19]

Důvěrnost (Confidentiality) – Pojem důvěrnost reprezentuje ochranu dat v soukromí. Neoprávnění uživatelé by neměli mít přístup k citlivým datům. Cílem je přístup k citlivým datům ověřeným a oprávněným uživatelům. Pro zajištění této bezpečnosti v rámci firmy využíváme šifrování dat a další potřebné prostředky.

Integrita (Integrity) – Pojem integrita reprezentuje správnost a konzistenci citlivých dat. Primárním použití je kontrola informace, zda není poškozená a jestli je důvěryhodná. Sekundární použití se stará o neoprávněné změny dat, které nejsou potřebné a chtěné. Udržování integrity je důležité, protože je potřeba mít přístup k přesným informacím.

Dostupnost (Availability) – Pojem dostupnost reprezentuje, zda jsou data přístupné v jakékoliv situaci pro oprávněného uživatele. Cílem je zamezit výpadků dat a zajistit odolnost dat. Pro splnění těchto požadavků se používá záloha dat, různé RAID systémy a software pro obnovení. Tvorba těchto podmínek není lehká, protože se nemůže ovlivnit integrita a důvěryhodnost. [19]



Obr. 1 CIA Bezpečnost
Zdroj: vlastní. Upraveno dle [25]

4.2.2 Parkerian hexad

Parkerian hexad je koncept informační bezpečnosti. Byl navržen Donnem B. Parkerem v roce 1998. Jeho součástí jsou tři prvky (důvěrnost, integrita, dostupnost) z CIA triády. Oproti CIA triádě je rozšířený o další tři prvky. Jedná se o soubor šesti prvků, které přispívají k bezpečnosti (důvěrnost, integrita, dostupnost, autenticita, důvěryhodnost, odpovědnost). Tímto rozšířením modulu dochází i k lepšímu komplexnějšímu rámci v bezpečnosti. Organizace dokáží lépe reagovat na bezpečnost jejich dat a lépe pracovat s virovými hrozbami či útoky z internetového prostředí.

Důvěrnost (Confidentiality) – Pojem důvěryhodnost je stejný jako v CIA triádě. Reprezentuje ochranu dat v soukromí. Chrání před neoprávněným přístupem uživatelů k citlivým datům

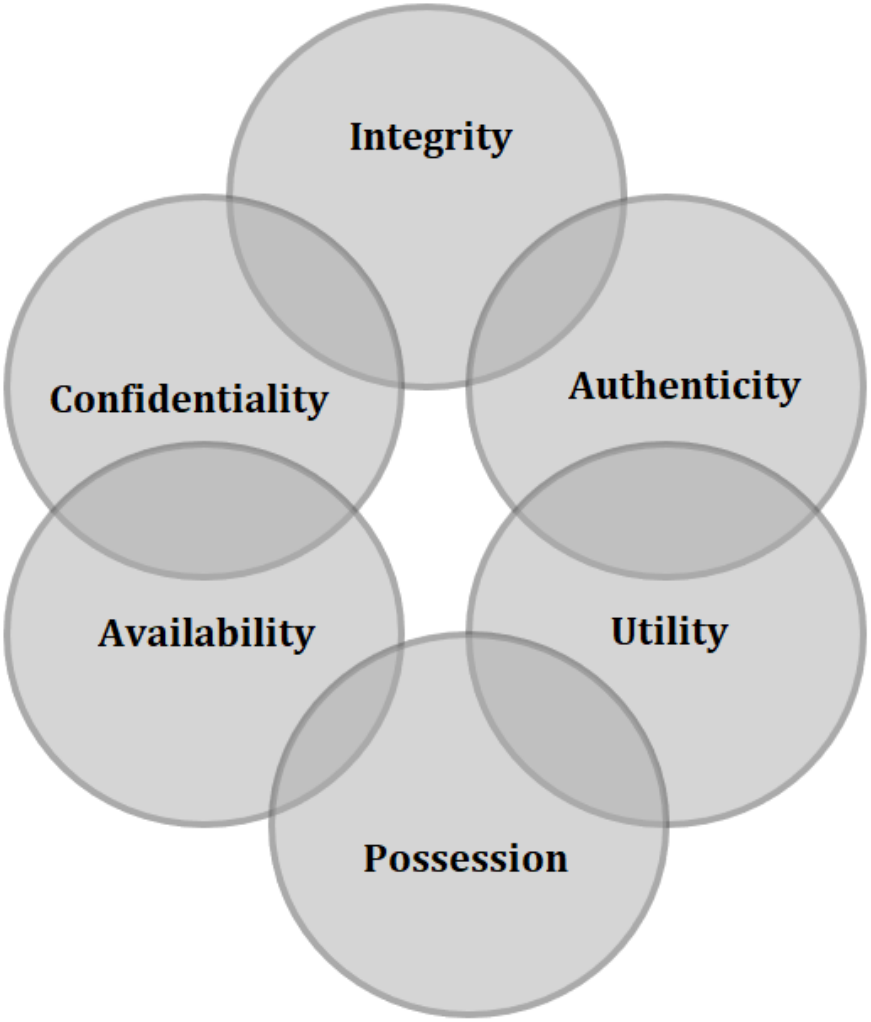
Integrita (Integrity) – Pojem integrita je podobný jako v CIA triádě. Reprezentuje správnost a konzistenci dat pro ověřeného uživatele. Stará se o to, aby informace byla nepoškozená.

Dostupnost (Availability) – Pojem dostupnost je také stejný jako v CIA triádě. Reprezentuje zajištění přístupu oprávněného uživatele. Dále dostupnost dat v jakémkoliv případě.

Autenticita (Authenticity) – Pojem autenticita je prvním přidaným prvkem v Parkerian hexad. Autenticita se stará se o původu informace či autorství. Cílem je mít ověřená data, které nejsou falešně zadaná. Autenticita dat pomáhá i s bojem proti fake news. Příkladem je elektronický podpis na smlouvě.

Důvěryhodnost (Utility) – Pojem utility je druhým přidaným prvkem v Parkerian hexad. Utility znamená kontrolovat stav dat. Může dojít ke ztrátě klíče k zašifrovaným datům. Data jsou uchována ale nejdou použít.

Odpovědnost (Possession)– Pojem odpovědnost je třetím přidaným prvkem v Parkerian hexad. Odpovědnost znamená ilustrace ztráty kontroly či držení informací. Jedná se o ztrátu vlastnictví daných dat. [19,20]



Obr. 2 Parkerian hexad
Zdroj: vlastní. Upraveno dle [26]

4.2.3 Řešení zranitelnosti, hrozeb

Operační systémy jsou kritickou částí moderních počítačových technologií. Důležitým prvkem je samotná bezpečnost (hrozby a zranitelnosti) operačního systému. Kvalitně vytvořená bezpečnost zajišťuje ochranu před kybernetickými útoky. Řešení zranitelnosti a hrozeb je individuálním nastavením osoby nebo společnosti dle potřeby užití a funkčnosti. Existují základní postupy, které pomáhají určit úroveň zabezpečení. [24]

- **CVSS (Common Vulnerability Scoring System)** – Jedná se o systém, který hodnotí zranitelnosti v operačním systému. Používá standardizovaný způsob hodnocení zranitelnosti a hrozeb na základě určitých faktorů. Z toho vypočítá číselnou hodnotu, která odráží závažnost situace. Existuje pět druhů skóre (žádné, nízké, střední, vysoké a kritické). Hodnocení se udává na stupnici 0 až 10. Hodnota 0 určuje nulové riziko. Hodnocení 10 ukazuje maximální riziko. [27]

Tabulka 3 CVSS Skóre
Zdroj: vlastní. Upraveno dle [27]

Vážnost	Hodnocení vážností
Žádná	0,0
Nízká	0,1 - 3,9
Střední	4 - 6,9
Vysoká	7 - 8,9
Kritická	9 - 10

- **CVE Zranitelnosti** – Zkratka CVE znamená (Common Vulnerabilities and Exposures). Jedná se o slovník zranitelností. Každá zranitelnost má svoje jedinečné číslo. Identifikátory jsou tvořeny ve formátu CVE-YYYY-NNNN. Na místě „YYYY“ se udává rok, kdy byla zranitelnost objevena. Na místě „NNNN“ je číslo zranitelnosti (nesmí být dvě stejná čísla). Díky CVE jsou zaznamenávány podrobnosti k dané zranitelnosti. CVE seznam je tvořen a spravován společností MITRE corporation. [28]

Mezi standardní bezpečností opatření patří dle zdroje [24]

Pravidelné aktualizace politik – Pro dodržování a funkčnost bezpečnostních politik je nutné stále udržovat aktuální postupy pro tvorbu bezpečnosti. Pravidelně je potřebné přezkoumávat, upravovat a používat CVSS či CVE.

Politika hesel – Nutností je vytvořit silný autorizační koncept. Autorizační koncept je tvořený pomocí identifikace uživatele (silné heslo), přidělování oprávnění uživatelů, řízení přístupu a ověřování oprávnění. [24]

Šifrování dat – Šifrování dat zajistí ochranu citlivých dat před zneužitím či krádeží. V případě, že by se útočník k datům dostal, není schopen je přečíst. Existují různé formy šifrovacích algoritmů a obecně kryptografie.

- **Symetrická kryptografie** – Symetrická kryptografie používá jeden společný klíč pro šifrování a dešifrování dat. Při použití této metody je nutné klíč udržovat v bezpečí. Příkladem symetrického algoritmu je AES. [29]

- **Asymetrická kryptografie** – Forma asymetrické kryptografie spočívá v používá dvou klíčů. Veřejný klíč je používán k šifrování dat. Soukromý klíč je používán k dešifrování dat a je nutné udržovat v bezpečí. Příkladem asymetrického algoritmu je RSA. [29]

- **Šifrovací algoritmy** – Šifrovací algoritmy jsou matematické kroky, které transformují data do nečitelného zápisu. Cílem je ochrana dat před zneužitím a neoprávněným přístupem k datům. Existuje spousta druhů algoritmů. [29]
    1. **AES (Advanced Encryption Standard)** – Symetrický šifrovací algoritmus, vyniká svojí rychlostí a silnou bezpečností. Používá klíče o velikosti 128, 192 a 256 bitů.
    2. **RSA (Rivest-Shamir-Adleman)** – Asymetrický šifrovací algoritmus. Využívá se pro šifrování dat a digitalizaci podpisu. Používá dva klíče veřejný a soukromý.
    3. **Twofish** – Symetrický šifrovací algoritmus, který nahrazuje zastaralý DES a 3DES. Jeho vlastnostmi je bezpečnosti a rychlost.

Antivirový software – Dalším důležitým softwarem je antivirový software. Dokáže rozpoznávat škodný software, který by mohl ohrozit funkčnost operačního systému.[24]

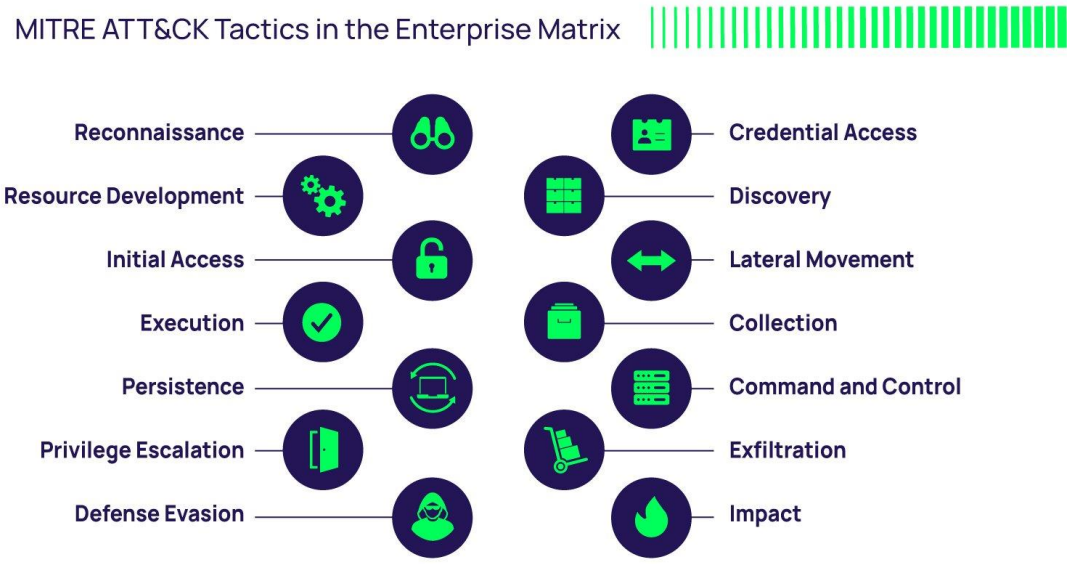
- **Signatury (rozpoznávání)** – Jsou používány v antivirových softwarech pro identifikaci škodlivých softwarů. Součástí jsou speciální vzory, které jsou potřebné pro rozpoznávání hrozeb (většinou známých hrozeb).

EDR (Endpoint Detection and Response) vs XDR (Extended Detection and Response) – Oba tyto koncepty zahrnují monitorování, detekci hrozeb a automatickou reakci na kybernetické hrozby. EDR je omezený jen na koncové body. XDR je komplexnější a obsáhlejší něž samotný EDR. V reálném využití je XDR lépe připravený na hrozící kyberútok. XDR má pohled na integraci dat (cloudy, identity) což EDR chybí, a proto není tak komplexní. Díky tomu jsou vyplněny všechny mezery na integraci dat. [32]

Bezpečnostní školení – V organizacích je potřeba školit zaměstnance. Vědomí zaměstnanců o bezpečnosti je důležitým bezpečnostní kritériem. Tento druh školení má za účel zvyšovat bezpečností povědomí uživatelů a tím snížit zranitelnost. Cílem může být ochrana proti phishingu či dalším hrozbám. [24]

Sledování trendů a hrozeb – Přehled o trendech hrozeb a zranitelností přináší organizaci připadnou hodnotu, neboť může efektivně plánovat investice do bezpečnostních opatření, které jsou cílené na konkrétní hrozby a zranitelnosti. Existuje spousta zdrojů, ze kterých lze čerpat kvalitní data.

- **MITRE ATT&CK matrix** – Jedná se o nástroj, který popisuje kybernetickou bezpečnost. Součástí je ukázka taktik, postupů a technik, které jsou používány. Existuje několik bodů, které jsou potřebné využívat.



Obr. 3 MITRE ATT&CK Matice
Zdroj: vlastní. Upraveno dle [45]

Průzkum (Reconnaissance) – Shromažďování informací pro plánování budoucích akcí proti soupeři.

Vývoj zdrojů (Resource Development) – Vytváření zdrojů k podpoře provádění operací.

Počáteční přístup (Initial Access) – Snaha proniknout do sítě.

Realizace (Execution) – Snaha o spuštění škodlivého kódu.

Perzistence (Persistence) – Usiluje o udržení své pozice.

Zvýšení oprávnění (Privilege Escalation) – Snaží se získat oprávnění na vyšší úrovni.

Vyhýbání obraně (Defense Evasion) – Snaha vyhnout se odhalení.

Přístup k pověření (Credential Access) – Zneužití nebo odcizení přihlašovacích údajů.

Zjištění (Discovery) – Snaha o porozumění svého okolí.

Boční pohyb (Lateral Movement) – Navigace svým prostředím pomocí legitimních oprávnění k průchodu mezi více systémy.

Shromažďování (Collection) – Sběr dat, která jsou cílem zájmu protivníka.

Velení a řízení (Command and Control) – Komunikace s napadenými systémy s cílem jejich ovládání.
Exfiltrace (Exfiltration) – Krádež dat
Dopad (Impact) – Manipulace, přerušování nebo ničení systémů a dat. [46]

- **NUKIB** – „Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo.“ [30]

- **APT skupiny** – „APT je zkratka pro Advanced Persistent Threat (pokročilé trvalé hrozby), přičemž APT Groups jsou subjekty odpovědné za iniciování těchto hrozeb a následných kybernetických útoků. Tyto skupiny jsou občas synonymem pro Cyber Threat Actors.“ [31]

4.2.4 Kyberútoky

Cílem kyberútoků je poškodit či ukrást citlivá data, která lze zneužít. Dále získat kontrolu či přístup na základě citlivých dat. Tato problematika postihuje nejen organizace ale i osobní počítače běžných uživatelů. Kyberútoky se volně distribuují internetem, jednotlivci či organizacemi, a generují trestnou činnost. Existuje spoustu druhů těchto softwarů a hrozeb. Dělí se do čtyř skupin. [21]

Cyber Espionage (Kybernetická špionáž) – Kybernetická špionáž je typ kybernetického útoku. Tento kybernetický útok se pokouší získat přístup k citlivým datům za účelem ekonomického zisku, konkurenční výhody či z politických důvodů. Cílem tohoto kyberútoku jsou velké korporátní firmy, vládní agentury či akademické instituce. Nevylučuje se, že cíl může být jednotlivec (vládní představitelé, celebrity, pracovníci či vládní úředníci). Útoky se řadí do pokročilých trvalých hrozeb APT.

APT je kyberútok, který velice sofistikovaný. Většinou je dopředu pečlivě připravený a naplánovaný. Mezi formy běžných technik útoků spadá sociální inženýrství (získat potřebné informace od cíle, aby útok byl úspěšný), škodlivé odkazy, stáhnutí malwaru či ransomware. [33]

Hactivism (Aktivisté a skupiny útočníků) – Hacktivismus využívá hackerské techniky pro politické či sociální účely. Využívá digitální nástroje pro tvorbu protestů a jiných přímých akcí. Hacktivisté pracují na svobodě projevu, lidských právech či informační etice pomocí kyberútoků. Mezi formy běžných technik útoků spadají DoS útoky (narušení činnosti organizací, proti nimž vystupují), poškozování webových stránek (změna vzhledu za účelem politického prohlášení nebo protestu), úniky dat (přístup k důvěrným informacím) či doxing (poškodit pověst organizace či jednotlivce). [34]

Cyber Warfare (Kybernetická válka) – Kybernetická válka je typ kybernetických útoků. Může se jednat o jeden útok či o sérii útoků jdoucích po sobě. Pro tento kyberútok je vybraná nějaká země, na kterou se poté útočí. Tento druh kyberútoků nemusí být jen cílem nějaké země ale také konkurence organizací. Cílem je tvorba zmatku ve vládní a civilní infrastruktuře (narušení důležitých systémů), což vede k velkým škodám ve státu či organizaci. Následkem může být i ztráta na životech. Mezi formy běžných technik útoků spadají špionáž (sledování jiných zemí či organizací za účelem krádeže citlivých dat – phishing), sabotáž (ukradnutí citlivých dat, využití vnitřní hrozny – nedbalí zaměstnanci), DoS útoky. [35]

Cyber Prime (Kybernetická kriminalita) – Kybernetická kriminalita je trestná činnost. Zaměřuje se na počítače, počítačové sítě či síťové zařízení. Je páchaná kyberzločinci nebo hackery za účelem vydělání peněz. Důvodem tohoto kyberútoku můžou být i politické a osobní spory. Kyberkriminalitu páchají jednotlivci ale i organizace. V případě organizace se jedná o organizovanou skupinu, která používá pokročilé technologie a její členové jsou technicky zdatní. Mezi formy běžných technik útoků se řadí malware útok (počítačový systém nebo síť je infikována

počítačovým malwarem), phishing (nevyžádané e-maily nebo jiné formy komunikace), útoky DoS (vyřazení systému nebo sítě z provozu). [36]

Definice kyberútoků:

Malware – Jedná se o formu útoků, které se rozšiřují pomocí škodlivého softwaru. Prezentuje se buďto jako důvěryhodná emailová adresa nebo program. Příloha je většinou šifrovaná, aby se program mohl nainstalovat. Existuje několik typů malwaru.

- Viry – Využívají chyby v kódech aplikací, které používáme. Pomocí nich pak infikují celý operační systém. Po infikaci je vir dál distribuovaný bez vědomí uživatele.
- Trojský kůň – Trojské koně jsou skryté v softwaru, který je běžně používán. Využívá se pro tvorbu takzvaných backdoors (zadních vrátek). Pomocí zadních vrátek útočník poté zaútočí na daný operační systém.
- Spyware – Spyware je typ malwaru, který sleduje aktivitu uživatele. Shromažďuje o uživateli citlivá data.
- Ransomware – Uzamkne citlivá data uživatele a znemožní přístup k nim. Přístup je vymáhán finanční odměnou pod hrozbou nebo zveřejnění dat. Data nelze odemknout, protože jsou zašifrovaná. [22,23]

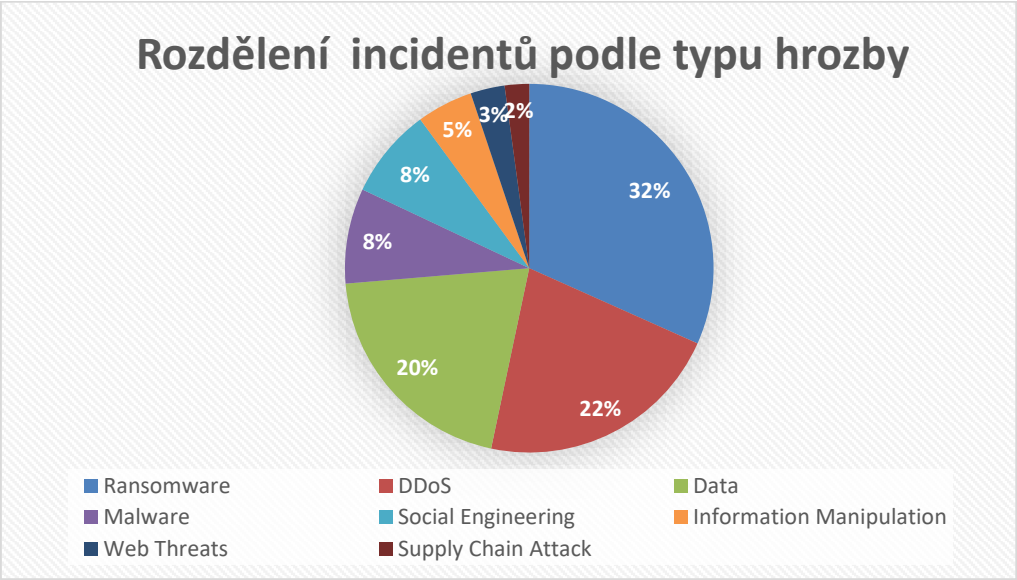
DOS (Denial of Service) a DDOS (Distributed Denial of Service) – Jedná se o typ kyberútoku, který má za cíl pomocí zahlcení sítě vyřadit systém. Rozděluje se na dva typy DoS a DDoS. Dos je útok z jednoho zařízení na druhé s cílem vyřadit systém pomocí zahlcení. DDoS má identický cíl s tím, že používá více zařízení pro vyřazení a zahlcení služby.

Phishing – Jedná se o kyberútok, který je svoji náročnost nejjednodušší. Pomocí podvodných emailů, podvodných stránek či zpráv dokáže ukrást citlivá data a informace nejenom z organizací ale i od běžných uživatelů. Podvodné maily mohou být velice důvěryhodné, vydávají za legitimní organice. Po otevření jednoho mailu dochází k napadnutí celé sítě, a tedy celý systém je v ohrožení. [22,23]

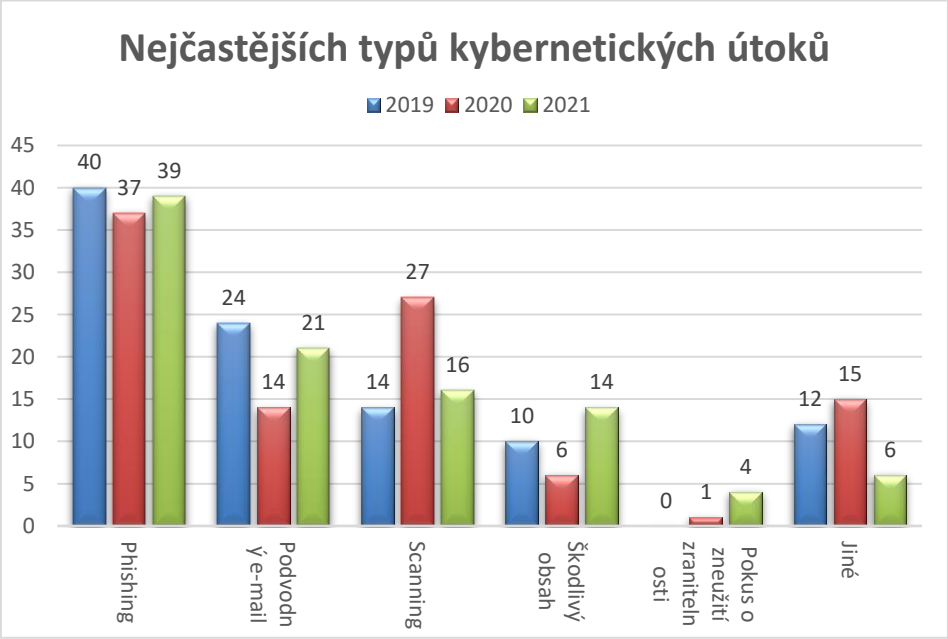
Statistiky kyberútoků

V následujícím grafu jsou znázorněná procentuální zastoupení kyberútoků. Jedná se o období od července 2022 až po červen 2023. Největší zastoupení kyberútoků má ransomware a DDoS útoky.

V druhém grafu jsou znázorněny nejčastější typy kybernetických útoků v České republice v procentech za roky 2019 až 2021.



Obr. 4 Rozdělení incidentů podle typu hrozby ENISA
Zdroj: vlastní. Upraveno dle [37]



Obr. 5 Nejčastějších typů kybernetických útoků NÚKIB
Zdroj: vlastní. Upraveno dle [38]

5 Zajištění bezpečnosti v OS Windows

Zabezpečení operačního systému Windows vyžaduje komplexní strategii, která zahrnuje široké spektrum opatření a technologií. Existuje mnoho přístupů k řešení této problematiky, přičemž účinnost závisí na použití pokročilých metod a technik. Mezi základní prvky patří pravidelné aktualizace, aktivní firewall, spolehlivý antivirový software, šifrování citlivých dat, pravidelné zálohování a důkladné školení uživatelů. Hlavním cílem je ochrana samotného systému před hrozbami kybernetických útoků a identifikování zranitelností. Sekundárně se klade důraz na ochranu citlivých informací a uživatelských dat. [39]

Group Policy Objects (GPO) – Skrze skupinovou politiku (GPO) se provádí centralizovaná správa a konfigurace politik v operačním systému Windows. Nutné je použití features Active Directory. Tento nástroj umožňuje definovat politiky, práva uživatelů a počítačů v síti. Díky tomu lze efektivně zavést a udržovat silné heselné politiky a regulovat přístup k souborům a citlivým informacím. [39]

Lokální politiky – GPO lokální politiky je mechanismus umožňující správcům konfigurovat a řídit nastavení v rámci celé sítě pouze na úrovni lokálního prostředí, tedy jednotlivých počítačů. Tato politika není závislá na doméně a umožňuje konzistentní správu a zabezpečení počítačů bez nutnosti centrálního řízení pomocí GPO v rámci služby Active Directory. GPO lokální politiky zahrnují následující. [48]

- **Nastavení bezpečnostních pravidel** – Možnost správy umožňuje nastavení bezpečnostní politiky pro počítače v místní síti, například požadavky na hesla, pravidla pro uzamykání účtů apod.
- **Konfigurace síťových nastavení** – Správci mohou nastavit síťová nastavení. Příkladem jsou síťové adaptéry, firewall a síťové protokoly.
- **Správa uživatelských práv** – Správa uživatelských práv a oprávnění na jednotlivých počítačích v rámci lokální sítě.
- **Nastavení systémových politik** – Možnost nastavení různých nastavení a politik pro počítače a bezpečnost.

- **Aktualizace a správa GPO** – Možnost správy a aktualizace politik přímo na jednotlivých počítačích.
- **Monitoring a auditování** – Schopnost sledovat změny a auditovat nastavení politik.

Globální politiky – Jedná se o soubor konfiguračních nastavení v operačním systému Windows. Tyto nastavení umožňují správcům organizací centralizovaně řídit a upravovat chování počítačů v síti. Mohou být aplikovány na uživatelské, počítačové účty a ovlivňují různé aspekty operačního systému. Součástí politik je zabezpečení, síťových nastavení, softwarových omezení a dalších konfiguračních parametrů. Globální politiky umožňují administrátorům definovat a vynucovat standardizované politiky a postupy v celé organizaci. Cílem je usnadnění správy sítě, zlepšení bezpečnosti a zajištění konzistenci prostředí pro uživatele.

Group Policy Management Console – Konzole pro správu zásad skupiny (GPMC) je kompletní nástroj pro řízení zásad skupiny. Správci ho využívají k plnění všech úkolů souvisejících s řízením zásad skupiny. Výjimkou jsou konfigurace jednotlivých nastavení zásad přímo v objektech zásad skupiny. Provádí se pomocí Editoru místních objektů zásad skupiny.[52]

GPO na úrovni domény – GPO na úrovni domény představují soubor nastavení, která se aplikují na všechny objekty uvnitř dané domény. Administrátorům poskytují centralizovanou možnost řídit konfigurace a chování počítačů a uživatelů v rámci této domény. Politiky na úrovni domény mají obecně nižší prioritu než ty na úrovni organizační jednotky (OU). Politiky definované na úrovni OU mohou přepsat nebo upřesnit nastavení definované na úrovni domény.

Pomocí těchto politik mohou správci nastavit bezpečnostní pravidla pro ochranu systému a dat v rámci této domény. Toto zahrnuje nastavení hesel, zabezpečení sítě, správu účtů a další. Umožňují auditovat a monitorovat provedené změny a události v rámci domény. [51]

GPO na úrovni lesa – GPO na úrovni lesa představují soubor nastavení, která ovlivňují všechny domény uvnitř daného lesa. Správcům umožňují definovat a distribuovat konfigurační politiky z jednoho centrálního místa pro všechny domény v rámci lesa. Tímto způsobem lze zajistit konzistenci a standardizaci konfigurace napříč organizací. Usnadňují centralizovanou správu a dodržování standardů a pravidel organizace v celém lesu. Politiky na úrovni lesa mají vyšší prioritu než politiky na úrovni domény. Pomocí těchto kroků lze nastavit globální bezpečnostní a konfigurační politiky, které se aplikují na všechny domény v lesu. To zahrnuje nastavení zabezpečení, auditování, správu certifikátů. [51]

GPO na úrovni organizační jednotky – V úrovni organizační jednotky se nacházejí konfigurační nastavení a politiky v Active Directory. Tyto prvky jsou aplikovány na objekty, umístěné v dané organizační jednotce. Tato úroveň umožňuje správcům definovat a aplikovat specifická nastavení a politiky na konkrétní skupinu uživatelů, počítačů nebo dalších objektů v rámci organizace.

Application Whitelisting – Jedná se o proces, který umožňuje omezení používání pouze schválených aplikací na operačním systému Windows. Všechny ostatní aplikace jsou blokovány a nedovolí se jejich spuštění. Dále je možné nastavit blokování spouštění neznámých aplikací. Tento typ zabezpečení lze implementovat pomocí skupinové politiky nebo skriptů v PowerShellu. [39]

- **Privileged Access Management (PAM)** – Toto řešení se zaměřuje na zabezpečení identit. Pracuje s managementem a sledováním privilegovaných účtů a operací, aby organizace byla chráněna před kybernetickými hrozbami. Správa přístupu k těmto funkcím je zajištěna kombinací lidských faktorů, procesů a technologií. Omezení počtu uživatelů s přístupem k funkcím správy zvyšuje celkovou bezpečnost systému. Samotný Windows zajišťuje tuto operaci pomocí správy práv a účtů. Nastavení lze dále upravovat prostřednictvím skupinových politik (GPO). [40]

- **Continuous Monitoring** – Continuous monitoring průběžně monitoruje a v případě potřeby vyhodnocuje stav bezpečnosti systému a sítě. Jedná se o klíčové řešení, které identifikaci nových hrozeb a útoků rychle potlačí. [41]

Endpoint Detection and Response (EDR) – Endpoint Detection and Response (EDR) představuje klíčový nástroj pro sledování a reakci na chování koncových bodů či zařízení v síti. Tento mechanismus umožňuje detekci podezřelých aktivit a hrozeb v reálném čase a poskytuje podrobné informace o probíhajících kybernetických útocích. Díky EDR je možné rychle a efektivně reagovat na identifikované bezpečnostní incidenty. [32]

Host-based Intrusion Prevention Systems (HIPS) – HIPS nástroje sledují aktivitu na koncových bodech. Jejich hlavním úkolem je předcházet nebo alespoň upozorňovat na potenciálně škodlivé činnosti. Tyto činnosti mohou zahrnovat pokusy o manipulaci se systémovými soubory nebo spouštění neznámých aplikací či procesů. [42]

Advanced Threat Protection (ATP) – ATP představuje integrované řešení, které se specializuje na ochranu e-mailů a prohlížení webových stránek. Prostřednictvím pokročilé analýzy těchto komunikačních kanálů aktivně identifikuje a blokuje potenciální hrozby kybernetických útoků a škodlivého obsahu.

5.1 Windows Update

Následující podkapitola vychází z tohoto zdroje, pokud není řečeno jinak [43].

Windows Update představuje integrovanou součást operačního systému Windows (včetně Windows Server) od společnosti Microsoft. Tato služba umožňuje uživatelům snadno stahovat a instalovat aktualizace do svých operačních systémů. Obsah těchto aktualizací zahrnuje nové verze softwaru od Microsoftu, bezpečnostní záplaty a opravy chyb. Jedná se o zásadní prvek pro udržení bezpečnosti a stability systému. Zajišťuje, že operační systém zůstává aktuální a chráněný před potenciálními bezpečnostními hrozbami a kyberútoky. Existuje několik parametrů,

pomocí kterých se rozdělují aktualizace dle potřeby. Aktualizace lze také spravovat podle určených nástrojů ve Windows prostředí (WSUS a Microsoft Endpoint Configuration Manager).

Aktualizace funkcí – Tyto aktualizace jsou pravidelně vydávány každoročně a přinášejí nové funkce a vylepšení do operačního systému Windows. Díky této častější aktualizaci je správa systému mnohem jednodušší, než je tomu u aktualizací vydávaných jednou za 3 až 5 let.

Aktualizace kvality – Tento druh aktualizací přináší bezpečnostní i nezabezpečené opravy. Jsou tvořeny zabezpečením, kritickými aktualizacemi, aktualizacemi zásobníku služeb a aktualizacemi ovladačů. Microsoft je vydává každé druhé úterý v měsíci. V případě potřeby jsou vydány kdykoliv. Aktualizace kvality jsou kumulativní. Stačí nainstalovat nejnovější aktualizace kvality, všechny předešlé aktualizace jsou součástí té nejnovější.

Servicing stack updates – Servisní zásobník je klíčovou součástí kódu, který zajišťuje instalaci aktualizací systému Windows. Jeho aktualizace jsou nezbytné pro bezproblémový chod operačního systému a zabezpečení zařízení. Je důležité pravidelně aktualizovat servisní zásobník, protože nové bezpečnostní opravy od společnosti Microsoft jsou součástí těchto aktualizací. Tyto aktualizace nejsou vždy vydávány s každou měsíční aktualizací kvality. Někdy jsou zveřejněny mimo plánovaný aktualizační cyklus, aby vyřešily naléhavé problémy. Abychom zajistili úplnost aktualizací servisního zásobníku, je důležité instalovat všechny dostupné aktualizace kvality. Kromě toho obsahuje servisní zásobník také zásobník servisních služeb založený na komponentách (CBS), který je důležitou součástí pro mnoho funkcí systému Windows, jako je DISM, SFC a opravy komponent. Aktualizace CBS jsou obvykle vydávány méně často než servisní zásobník.

Aktualizace ovladačů – Tento druh aktualizací je přímo závislý na určitém zařízení uživatele. Jsou specifikované podle druhu hardwaru. Aktualizace ovladačů jsou defaultně vypnuté v aktualizační službě Windows Server Update Services (WSUS).

V případě cloudových metod může aktualizace ovlivnit, zda se nainstalují nebo nikoliv.

Aktualizace produktů Microsoft – Tyto aktualizace jsou určeny pro jiné produkty od společnosti Microsoft. Například celé sady Microsoft Office. Tento druh aktualizací lze povolit či zakázat pomocí zásad řízených různými servisními nástroji.

5.2 Security Baseline

Následující podkapitola vychází z tohoto zdroje, pokud není řečeno jinak [44].

Organizace čelí různým formám kybernetických útoků a bezpečnostních hrozeb, které se mohou v závažnosti i povaze lišit. Microsoft definuje soubor standardů, postupů a konfigurací. Soubor slouží jako referenční bod pro zajištění bezpečnosti informačních systémů v rámci dané organizace. Tato nastavení jsou vytvořena na základě zpětné vazby od bezpečnostních inženýrů, produktových skupin, partnerů a zákazníků. Cílem je, aby efektivně odpovídala měnícím se potřebám a hrozbám v kybernetickém prostředí.

Základní linie zabezpečení představují klíčový přínos pro zákazníky, neboť spojují odborné znalosti společnosti Microsoft, partnerů a zákazníků. Pro operační systém Windows 10 existuje více než 3 000 nastavení zásad skupiny. K tomu souboru se přidává dalších přes 1 800 nastavení pro aplikaci Internet Explorer 11. Z těchto 4 800 nastavení se pouze některá týkají bezpečnosti, a prozkoumání každého z nich může být zdlouhavé. Organizace se musí neustále přizpůsobovat měnícím se bezpečnostním hrozbám, a proto poskytuje Microsoft základní bezpečnostní nastavení ve snadno použitelných formátech. Cílem je usnadnění nasazení a správy produktů.

Doporučení se řídí jednoduchým a efektivním přístupem k definici základních hodnot, které jsou:

- Základní linie jsou navrženy pro spravované organizace, které staví důraz na bezpečnost. Standardní koncoví uživatelé nemají administrátorská práva.
- Základní linie prosazují nastavení pouze v případech, kdy snižují současné bezpečnostní riziko a nezpůsobují provozní problémy.

- Základní linie vynucují výchozí nastavení pouze v případě, kdy je pravděpodobné, že oprávněný uživatel nastaví nastavení do nezabezpečeného stavu.

5.2.1 Baseline logování

Následující podkapitola vychází z tohoto zdroje, pokud není řečeno jinak [47].

Baseline logování představuje základní úroveň sběru a uchovávání logovacích dat v informačním systému organizace. Organizace si stanovují minimální požadavky na sběr a ukládání událostí. Cílem je poskytnout základní úroveň bezpečnosti a monitorování prostředí a zároveň dodržovat předpisy v oblasti kybernetické bezpečnosti. Správná implementace a konfigurace jsou klíčové pro úspěšné odhalování a reakci na kybernetické hrozby v organizaci.

Event Viewer

Event Viewer je nástroj pro správu událostí (Event logs) v operačním systému Windows. Hlavním účelem tohoto nástroje je sledování a analýza událostí, které se vyskytly během provozu daného zařízení. Kromě toho je klíčovým prvkem pro diagnostiku, monitorování a řešení problémů v prostředí Windows. Existuje několik druhů event logů, různých typů a porozumění jednotlivých událostí.

Kategorie protokolu událostí:

Protokol aplikace – Jakákoli událost zaznamenaná aplikací, kterou určují vývojáři při tvorbě aplikace. – např: chyba při spuštění aplikace.

Systémový protokol – Jakákoli událost zaznamenaná operačním systémem. – např: neschopnost spustit jednotku během startu.

Bezpečnostní protokol – Jakákoli událost, která má význam pro zabezpečení systému. – např: platná a neplatná přihlášení a odhlášení

Protokol adresářové služby – Zaznamenává události Active Directory. Tento protokol je přístupný pouze na řadičích domény.

Protokol serveru DNS – Zaznamenává události související se servery DNS a rozlišováním názvů. Tento protokol je přístupný pouze pro servery DNS.

Protokol služby replikace souborů – Zaznamenává události replikace řadiče domény. Tento protokol je dostupný pouze na řadičích domény.

Typy protokolů událostí:

Informace – Událost popisující úspěšnou aktivitu úlohy, jako je aplikace, ovladače nebo služby. – např: úspěšné načtení ovladačů síťové karty.

Varování – Událost, která nemusí být zásadní, ale může naznačovat možný budoucí problém. – např: oznámení docházení místa na disku.

Chyba – Událost, která signalizuje vážný problém, jako je ztráta dat nebo funkcionality. – např: nenačtení hardwaru při spuštění.

Audit úspěšnosti (protokol zabezpečení) – Událost, která oznamuje úspěšné dokončení auditované bezpečnostní události. – např: úspěšné přihlášení.

Audit selhání (bezpečnostní protokol) – Událost popisující neúspěšné dokončení auditované bezpečnostní události. – např: neúspěšné přihlášení.

Porozumění události:

Datum – Datum, kdy událost nastala.

Čas – Čas, kdy k události došlo.

Uživatel – Uživatel, který byl v dobu události přihlášen.

Počítač – Počítač, na kterém k události došlo.

ID události – Číslo události, které identifikuje typ události.

Zdroj – Zdroj, který událost vygeneroval.

Typ – Typ události (Informace, Varování, Chyba, Audit úspěchu a Audit neúspěchu).

5.2.2 Baseline Active Directory

Následující podkapitola vychází z těchto zdrojů, pokud není řečeno jinak [49,50].

Active Directory Domain Services (AD DS) poskytuje hierarchickou strukturu pro ukládání a správu informací o různých objektech v síti. Součástí jsou uživatelské účty, sdílené prostředky a další. Tato služba usnadňuje vyhledávání a využívání těchto dat a zajišťuje jejich zabezpečení prostřednictvím ověřování a řízení přístupu. Díky konceptu jediného síťového přihlášení mohou správci účinně

spravovat celou síť. Uživatelé mají snadný přístup k potřebným zdrojům, a to bez ohledu na to, kde se nacházejí v rámci sítě.

Při návrhu logické struktury služby AD DS je klíčové definovat vztahy mezi kontejnery v adresáři, které odpovídají požadavkům správy a provozním potřebám sítě. Před samotným návrhem je nutné porozumět logickému modelu služby Active Directory, který organizuje prvky sítě do hierarchické struktury. Tato struktura zahrnuje domény, organizační jednotky a další prvky. Každý z nich má svůj specifický účel a roli v celkovém uspořádání dat. Logický model je nezávislý na fyzických aspektech nasazení, což umožňuje flexibilitu a efektivní správu sítě.

Active Directory forest – Doménová struktura je skupina jedné nebo více domén v rámci služby Active Directory, které sdílejí společné vlastnosti a nastavení. Tato struktura zahrnuje společné schéma adresáře, konfiguraci adresáře a globální katalog. Všechny domény v jedné doménové struktuře jsou propojeny obousměrnými a tranzitivními vztahy důvěryhodnosti.

Active Directory domain – Doména v rámci služby Active Directory představuje segment dat, který umožňuje organizacím replikovat informace jen tam, kde jsou potřebné. To usnadňuje škálování adresáře v celé síti, zejména v situacích s omezenou šířkou pásma. Kromě toho doména poskytuje řadu klíčových funkcí souvisejících se správou.

- Identita uživatele v celé síti
- Ověřování
- Vztahy důvěryhodnosti
- Replikace

Active Directory organizational units – Organizační jednotky (OU) poskytují hierarchickou strukturu pro seskupování objektů v rámci domény služby Active Directory. Tato struktura umožňuje efektivní správu prostřednictvím aplikace zásad skupiny a delegování pravomocí. Správa nad jednotkou OU a obsaženými objekty je řízena pomocí seznamů řízení přístupu (ACL). Delegování pravomocí

je klíčovým konceptem, který umožňuje vlastníkům přenést správu nad objekty na jiné uživatele či skupiny. Tato funkcionalita je zásadní pro efektivní rozdělení úkolů správy v prostředí s velkým množstvím objektů.

6 Praktická část

V praktické části této práce bude představeno 5 užitkových případů nastavení skupinových politik. Cílem (GPO) je zvýšit bezpečnost prostředí MS Windows. Skupinové politiky jsou klíčovým nástrojem pro správu a zabezpečení síťových prostředí postavených na operačním systému Windows. V rámci této části práce se zaměříme na specifické nastavení a konfiguraci GPO. Konfigurace a nastavení umožní efektivní ochranu proti různým hrozbám a útokům. Hrozby a útoky mohou ohrozit integritu, dostupnost a důvěrnost dat v uživatelských prostředích. Každý z těchto případů bude detailně analyzován a popsán. Cílem této práce bude vygenerovat bezpečné prostředí na základě předem vytvořených problematik.

Architektura sítě

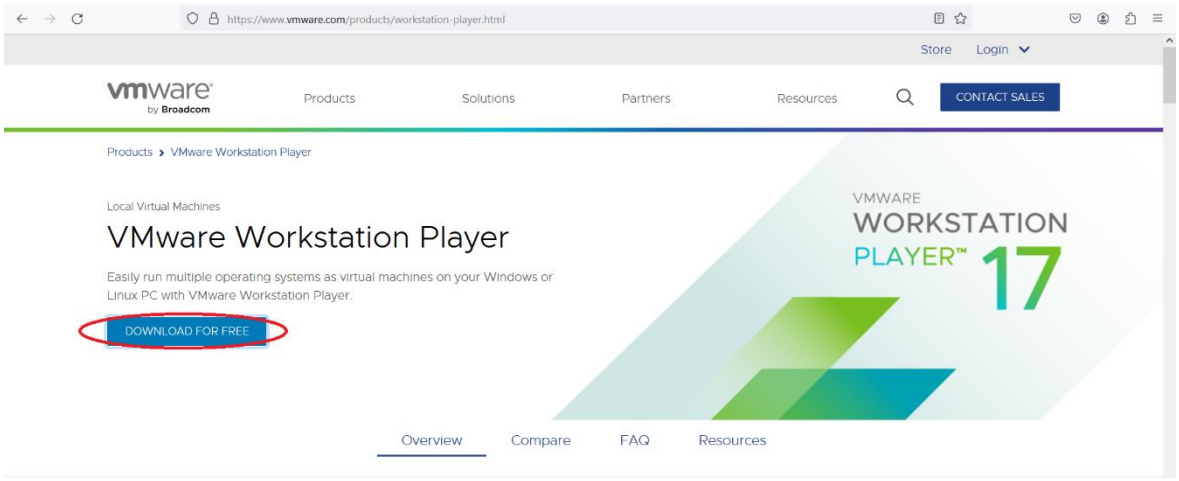
Architektura sítě zahrnuje centrální serverovou infrastrukturu založenou na MS Windows Server 2022 a klienta Windows 11 připojeného k této síti. MS Windows Server je nasazen jako doménový kontrolér, který poskytuje služby autentizace, autorizace a správy uživatelů. Díky této architektuře je možné řídit přístup uživatelů k síťovým prostředkům a aplikacím pomocí skupinových politik. Klienti v síti jsou pracovní stanice a notebooky, které jsou připojeny k doméně a využívají autentizaci a autorizaci poskytovanou serverem. Tímto je možné spravovat GPO. Na následujícím obrázku je zobrazená celá topologie sítě s IP adresací a názvy. V případě serveru je zobrazen i název domény.

Obr. 6 Topologie sítě. Zdroj: Vlastní.

6.1 Příprava prostředí

Instalace VMware Workstation 17 Player

Pro instalaci VMware Workstation 17 Player budeme postupovat následovně. Nejprve navštívíme oficiální stránky společnosti VMware a stáhneme instalační soubor. Instalační soubor stáhneme na následujícím URL linku https://www.vmware.com/products/workstation-player.html.

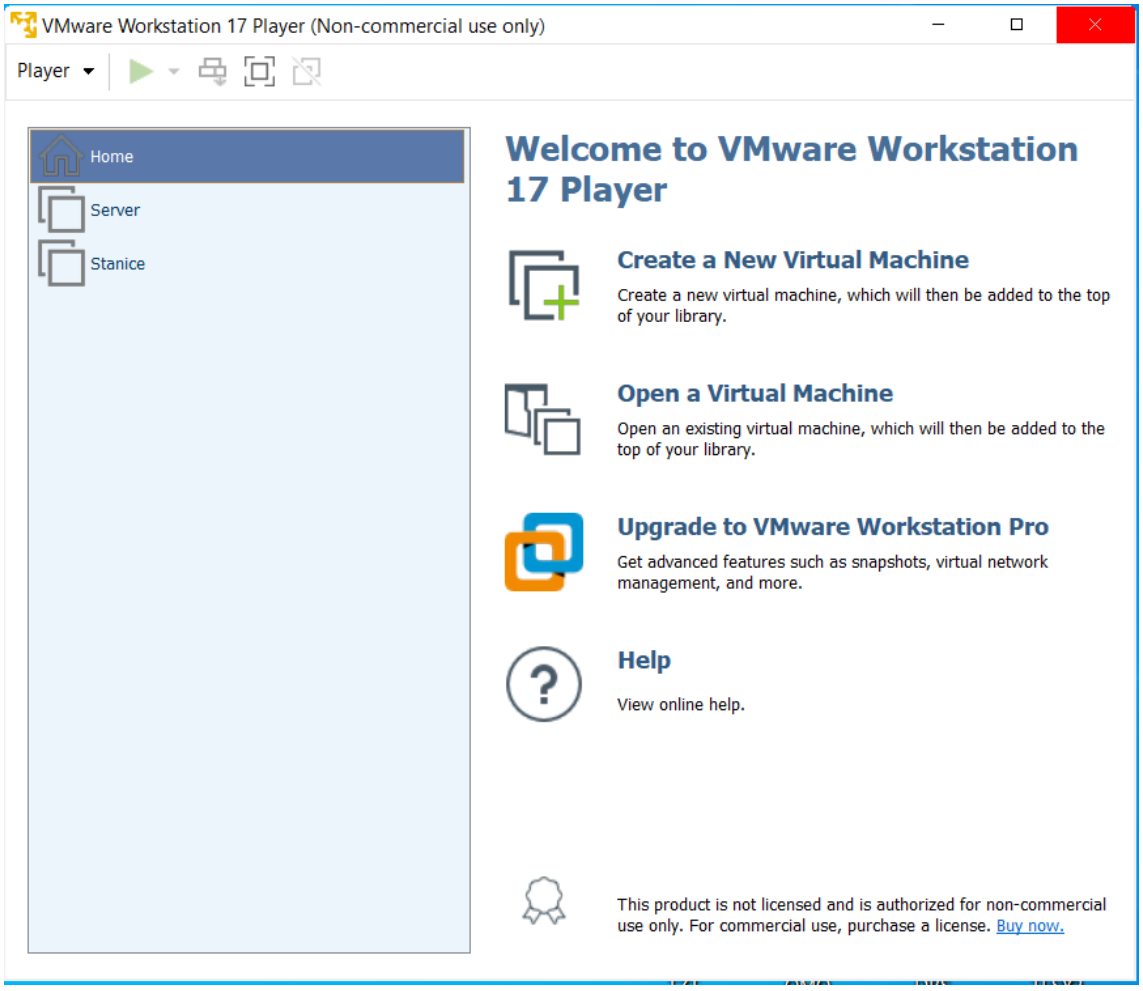


Obr. 7 Webová stránka VMware. Zdroj: Vlastní.

Po stažení instalačního souboru VMware Workstation 17 Player pokračujeme spuštěním instalace dvojitým kliknutím na stažený soubor. Během tohoto procesu nás čeká několik důležitých rozhodnutí. Začneme výběrem jazyka, který bude použit během instalace a následně i při práci s programem. Poté budeme vyzváni k akceptaci licenčních podmínek. Je důležité vybrat licenční podmínky odpovídající našemu záměru využití softwaru. Pokud se jedná o nekomerční využití pouze pro osobní účely, vybereme licenční podmínky určené pro tento účel.

Samotná instalace může trvat delší dobu. To je způsobeno potřebou nainstalovat různé důležité frameworky a součásti, které VMware Workstation 17 Player vyžaduje pro svůj provoz. Během tohoto procesu je důležité trpělivě počkat, dokud není instalace úplně dokončena.

Po dokončení instalace nás program pravděpodobně vyzve k restartování počítače. Tento krok je důležitý, aby se veškeré změny provedené během instalace mohly správně aplikovat. Poté je program připraven na plné využívání. V dalším kroku lze už virtualizovat operační systémy.



Obr. 8 Program WMware Workstation 17 Player. Zdroj: Vlastní.

Instalace serveru a stanice

Proces instalace začíná tím, že máme připravené instalační médium Windows Serveru a Windows 11, nejlépe ve formátu ISO. Instalační média se dají stáhnout pomocí cloudové aplikace Microsoft Azure, popřípadě pomocí Windows media creation tool.

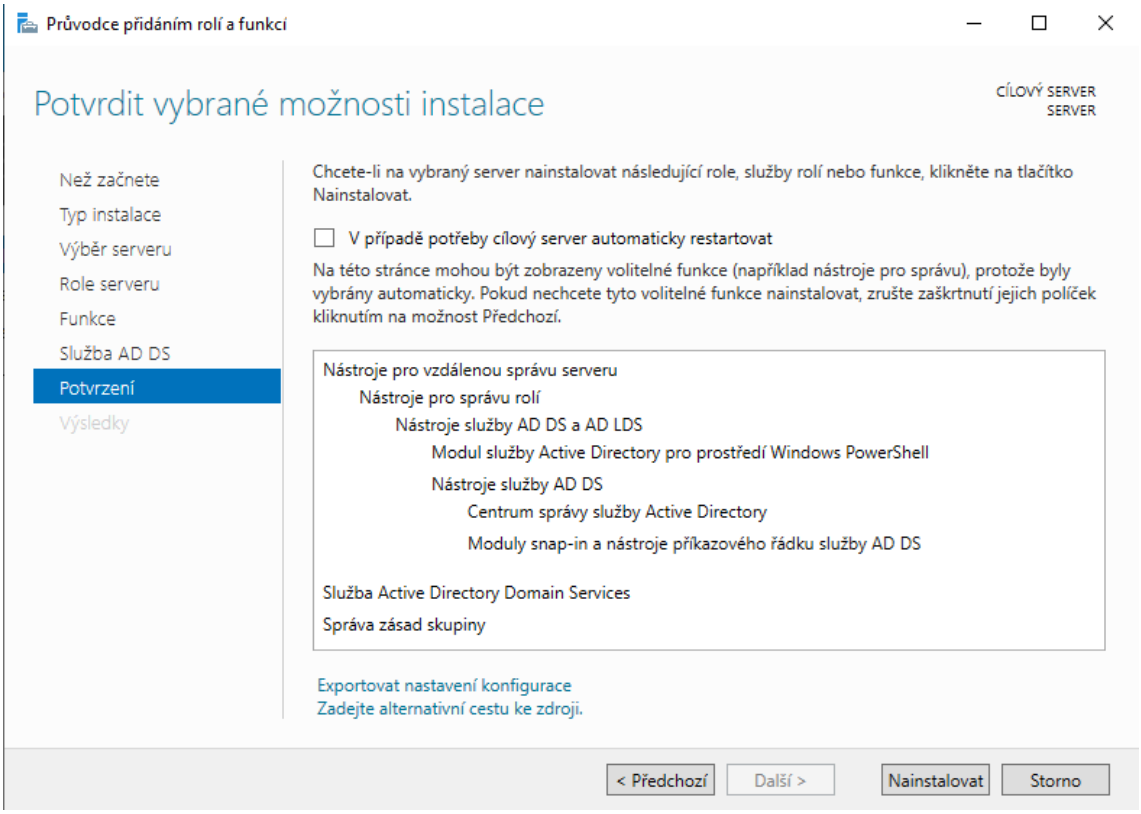
V dalším kroku je třeba vytvořit virtuální stroj v aplikaci VMware Workstation 17 Player. Je důležité mít na paměti, že požadavky na vytvoření virtuálního stroje se mohou lišit mezi serverovými a klientskými zařízeními. Jedním z klíčových rozdílů jsou požadavky na operační paměť. Serverové prostředí vyžaduje obvykle větší alokaci paměti než klientské stanice.

Instalace serveru a klientské stanice sdílí podobný postup. Začínáme kliknutím na tlačítko "Instalovat nyní", následně vybíráme jazyk, formát klávesnice

a zemi nebo region. Poté znovu klikneme na "Instalovat nyní" a pokračujeme zadáním produktového klíče. Případně je možné produktový klíč přeskočit a zadat ho později. Následně souhlasíme s licenčními podmínkami a vybíráme typ instalace. Poté vybereme disk pro instalaci a provedeme instalaci operačního systému Windows. Po dokončení instalace se počítač automaticky restartuje a můžeme pokračovat v konfiguraci nově nainstalovaného systému.

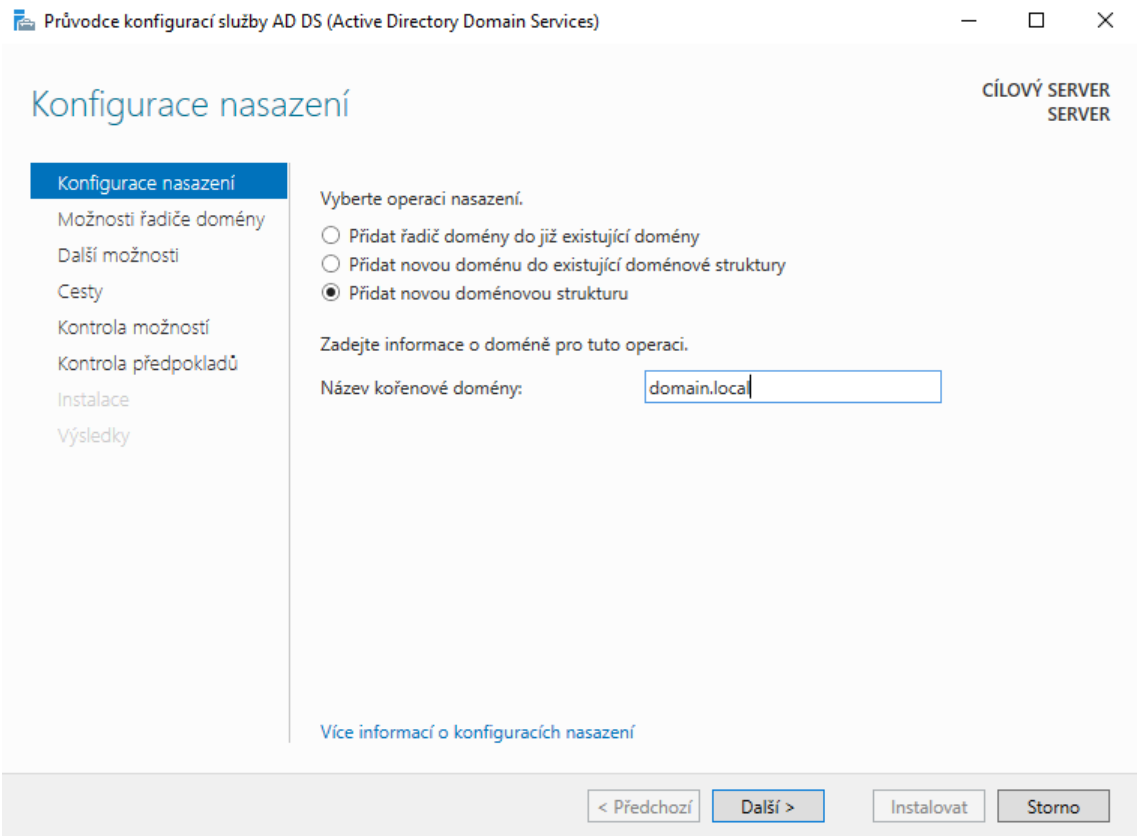
Instalace AD-DS, DNS, GPO Management

Po úspěšné instalaci serveru je důležité doinstalovat další komponenty, tzv. features. V našem případě je klíčové nainstalovat Active Directory Domain Services (AD-DS). Tímto balíčkem jsou automaticky zahrnuty další součásti, jako je například DNS a správa zásad skupiny (GPO Management). V nastavení serveru vybereme možnost "Přidat role a funkce" a poté zvolíme instalaci AD-DS. Viz. - Obrázek s číslem 9.



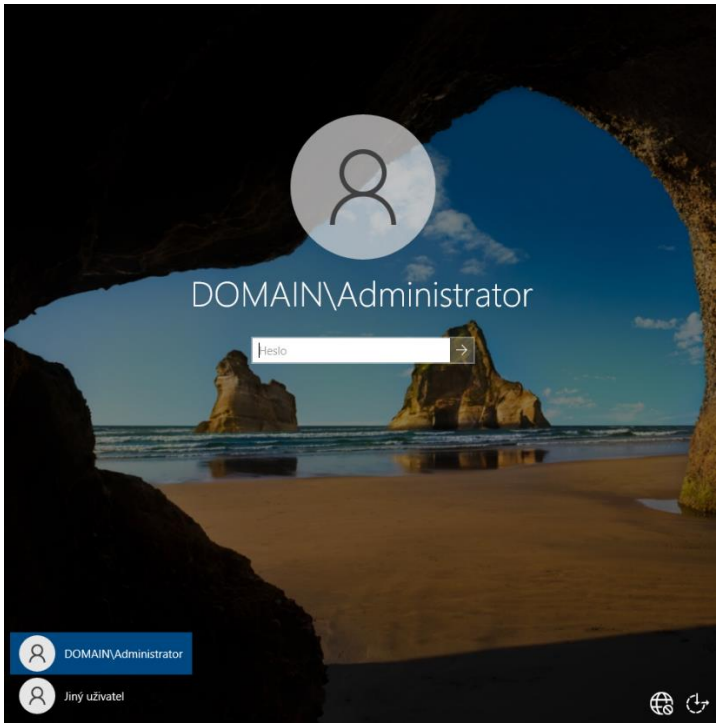
Obr. 9 Potvrzení instalace AD-DS. Zdroj: Vlastní.

Po zajištění těchto kroků jsme připraveni nainstalovat roli doménového řadiče. V mezičase je nutností nastavit IP adresaci síťové karty. Server bude mít adresu 172.16.1.1. Dalším krokem je konfigurace této funkce po její úspěšné instalaci. Při konfiguraci je třeba vytvořit nový les (forest) a specifikovat název domény, kterou chceme vytvořit a používat. V našem případě je název domény domain.local.



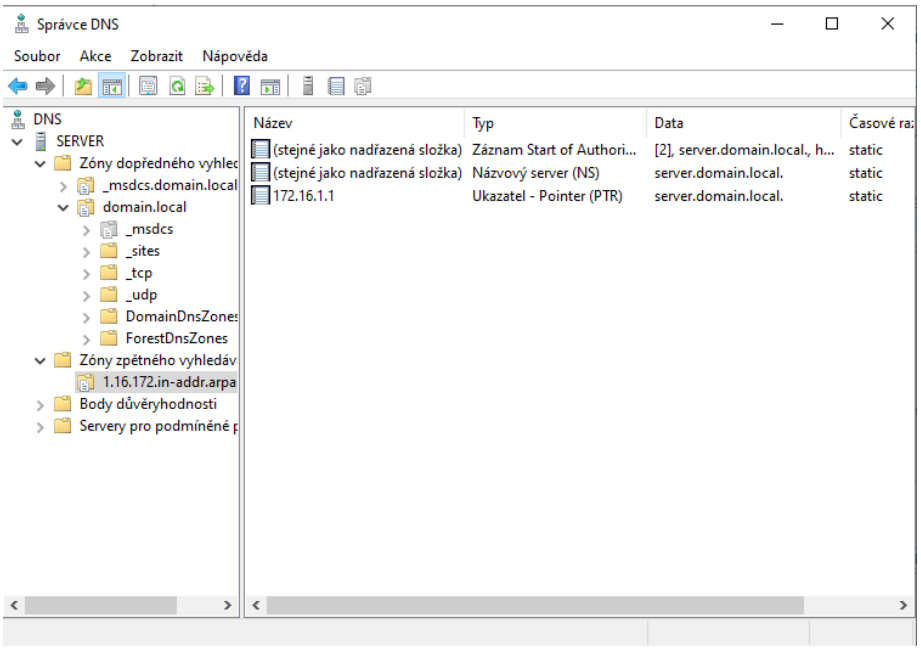
Obr. 10 Konfigurace AD-DS. Zdroj: Vlastní.

Během konfigurace AD-DS je nutný restart serveru, který může trvat delší dobu. Cílem tohoto procesu je vytvoření nezbytných podmínek pro správné fungování služby AD-DS. Po úspěšném restartu se objeví přihlašovací obrazovka, kde je možné vybrat možnost přihlášení, buď pomocí účtu DOMAIN\Administrator nebo jiného uživatele registrovaného v doméně. V této fázi je vhodné použít heslo, které bylo určeno při instalaci serveru. Po přihlášení by mělo být v Server Manageru vidět, že služba AD-DS je správně nakonfigurována a všechny potřebné prvky pro její správné fungování jsou aktivní.



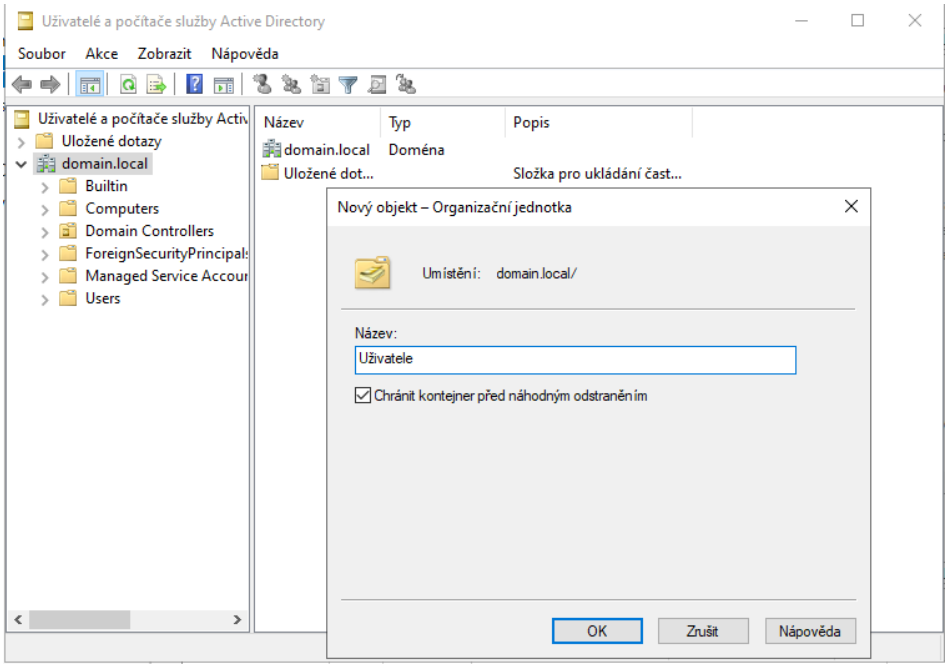
Obr. 11 Přihlašovací obrazovka po restartu serveru. Zdroj: Vlastní.

Dalším krokem je nastavení DNS serveru. To zahrnuje vytvoření nové zóny, což umožní konfiguraci této služby. Po vytvoření primární zóny je důležité založit také zónu zpětného vyhledávání, což je nezbytné pro správné fungování serveru.

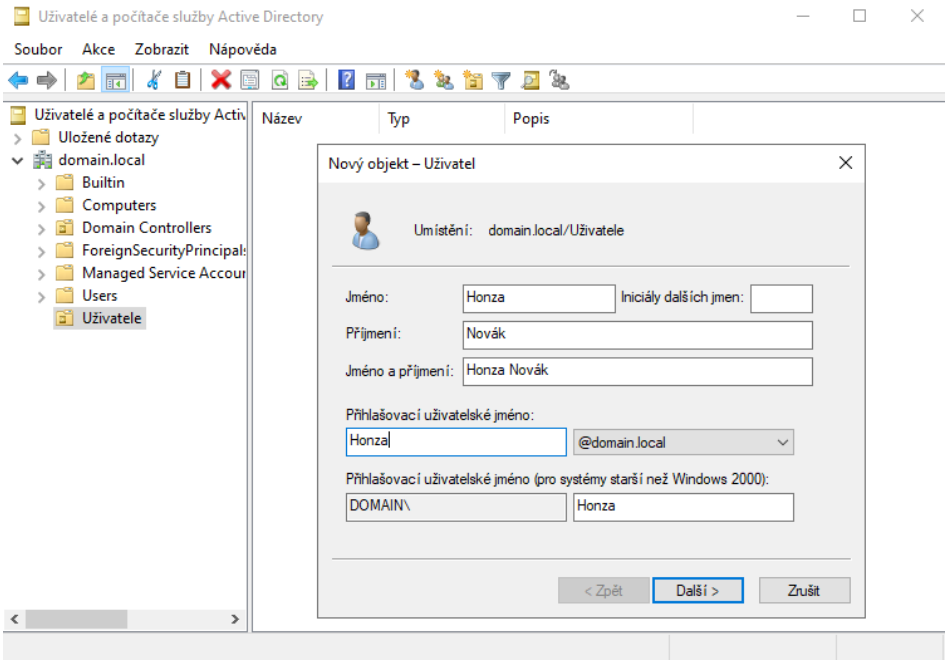


Obr. 12 Konfigurace DNS. Zdroj: Vlastní.

V dalším kroku se zaměříme na vytvoření jednotky v Active Directory. Po vytvoření jednotky budeme pokračovat přidáním uživatelů. Přidání uživatelů je nezbytné pro jejich správu a umožní jim přihlášení k jejich účtům na počítačích, které jsou členy domény. Takto vytvořené uživatelské účty budou mít přístup k sdíleným souborům, aplikacím a dalším síťovým zdrojům v rámci doménového prostředí.

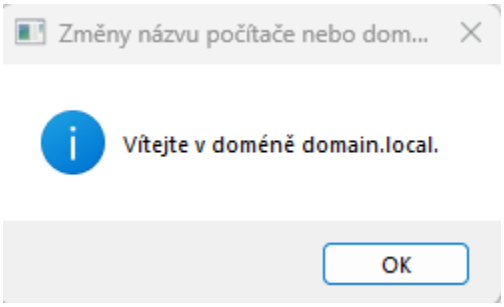


Obr. 14 Tvorba jednotky v AD-DS. Zdroj: Vlastní.

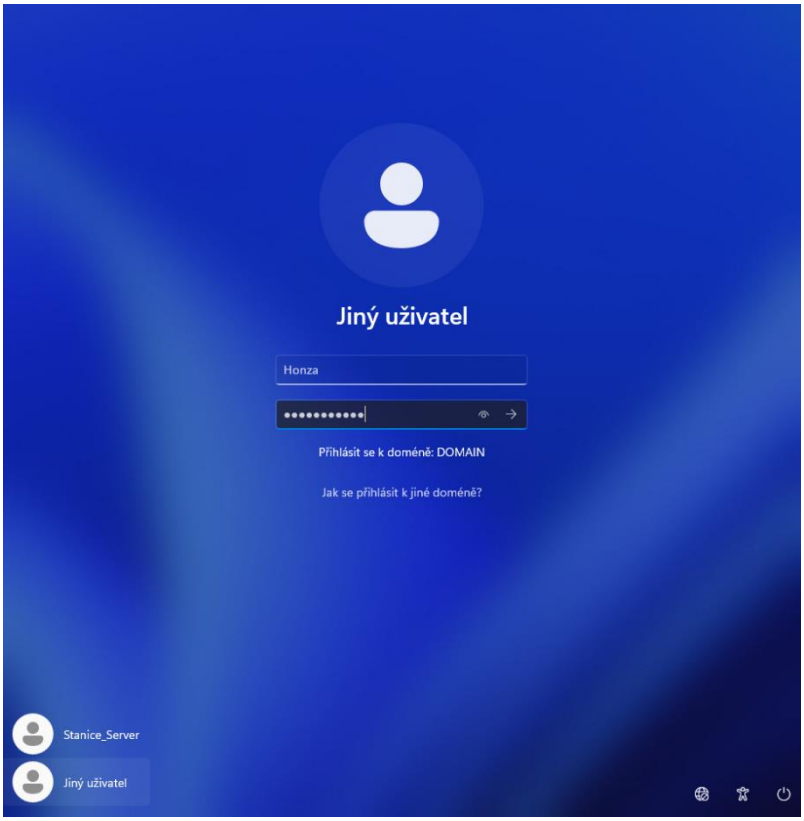


Obr. 13 Tvorba uživatele v AD-DS. Zdroj: Vlastní.

Po dokončení konfigurace serveru máme základní kámen naší síťové infrastruktury. Nyní je nezbytné přidat stanici do sítě a integrovat ji do domény. Stanice bude přiřazena IP adresa 172.16.1.10. Důležité je zajistit, aby mezi stanicí a serverem fungoval ping, což je základní test komunikace v síti. Dále je třeba nastavit DNS tak, aby odkazovalo na IP adresu serveru, aby proces přidání do domény proběhl bez problémů. S těmito přípravami je stanice připravena být zařazena do domény.

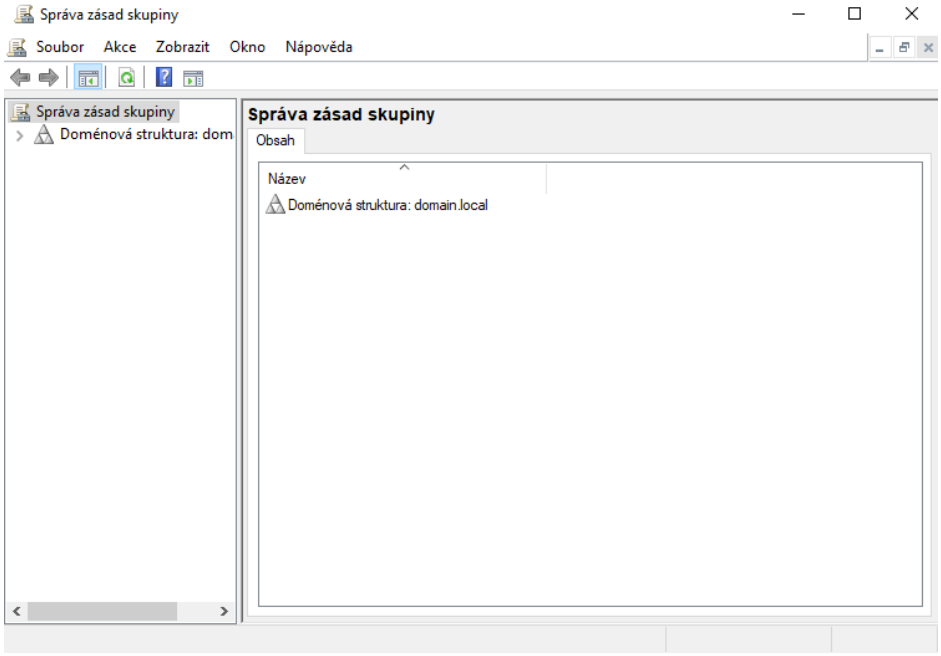


Obr. 15 Přidání stanice do domény. Zdroj: Vlastní.



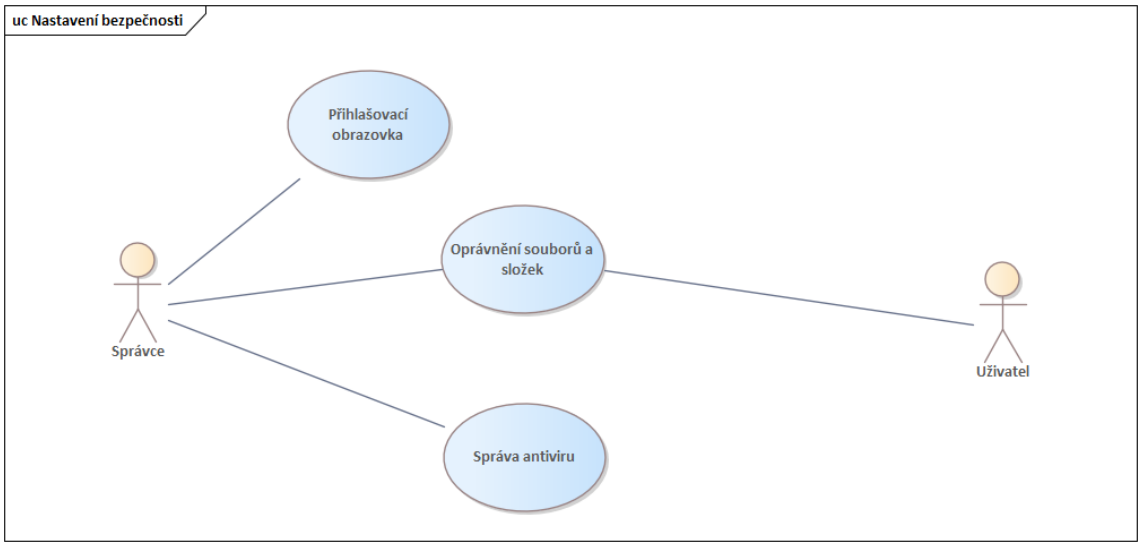
Obr. 16 Přihlašovací obrazovka stanice po přidání do domény. Zdroj: Vlastní.

Po úspěšném přidání stanice do domény se vracíme zpět k serveru a správě skupinových politik (GPO). Správa GPO byla nainstalována spolu s AD-DS. Tento nástroj je potřebný k nastavení všech politik pro servery a stanice v doméně.



Obr. 17 GPO Management. Zdroj: Vlastní.

6.2 Use case 1 – Bezpečnost



Obr. 18 Use case 1. Zdroj: Vlastní.

Use case je složen z 3 dílčích kroků, které budou konfigurovány v rámci jednotlivých GPO a následně ověřena jejich funkčnost.

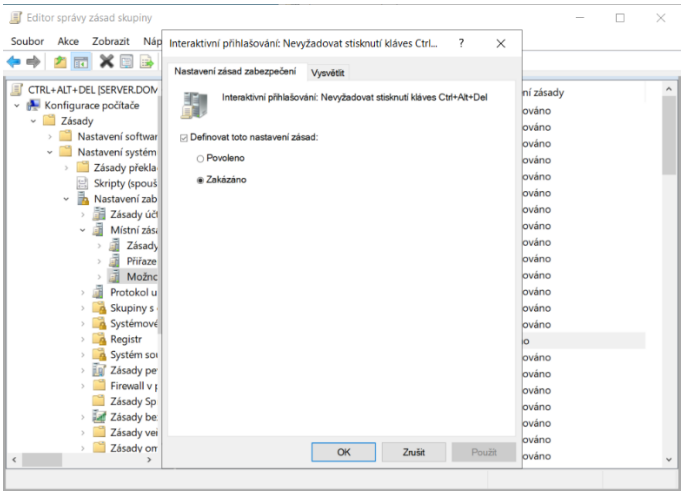
6.2.1 Přihlašovací obrazovka

Cílem tohoto kroku je nastavení GPO tak, aby uživatel při každém přihlášení na koncovou stanici musel zadat kombinaci kláves ctrl+alt+delete pro přístup na přihlašovací obrazovku. Tato funkcionalita je doporučená i Microsoftem jako best-practise pro zamezení zadání uživatelského hesla na podvrženou přihlašovací obrazovku útočníkem.

Konfigurace GPO:

Pro zajištění správného fungování tohoto nastavení je nezbytné vytvořit novou politiku v nástroji pro správu GPO (Group Policy Objects).

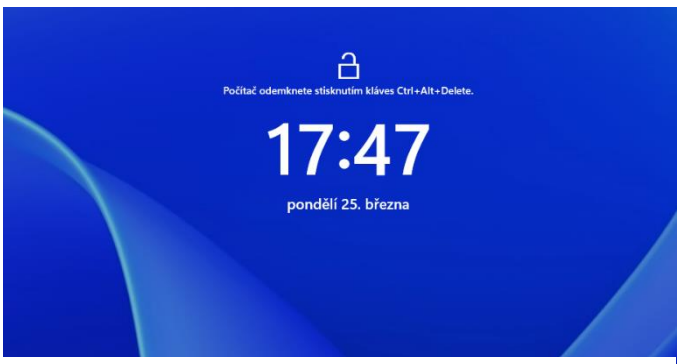
Konfigurace uživatele -> Zásady -> Šablony pro správu -> Systém -> Možnosti klávesové zkratky Ctrl + Alt + Delete.



Obr. 19 Nastavení CTRL+ALT+DEL. Zdroj: Vlastní.

Ověření:

Uživatel se hlásí do PC a je mu zobrazen požadavek na zadání kombinace kláves.



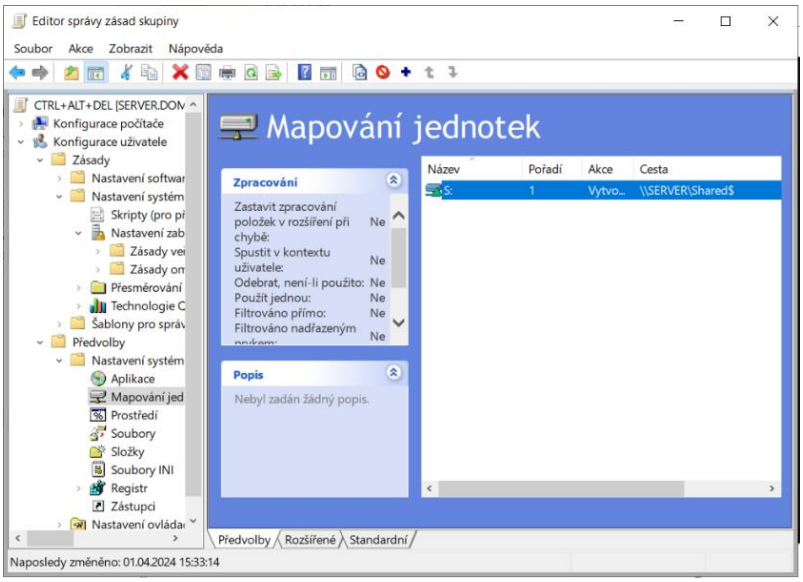
Obr. 20 Funkčnost CTRL+ALT+DEL. Zdroj: Vlastní.

6.2.2 Oprávnění souborů a složek

Cílem tohoto kroku je určení oprávnění pro přístup k souborům a složkám. GPO budou nastaveny, aby uživatel nemohl odstranit složky či soubory, které jsou sdíleny v rámci sítě.

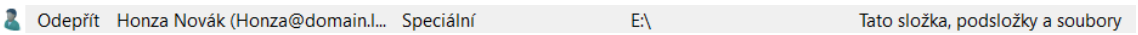
Konfigurace GPO:

Konfigurace uživatele -> Předvolby -> Nastavení systému Windows -> Mapování jednotek. Nejprve vytvoříme disk a poté ho sdílíme. Vytvoříme data abychom mohli otestovat funkčnost.

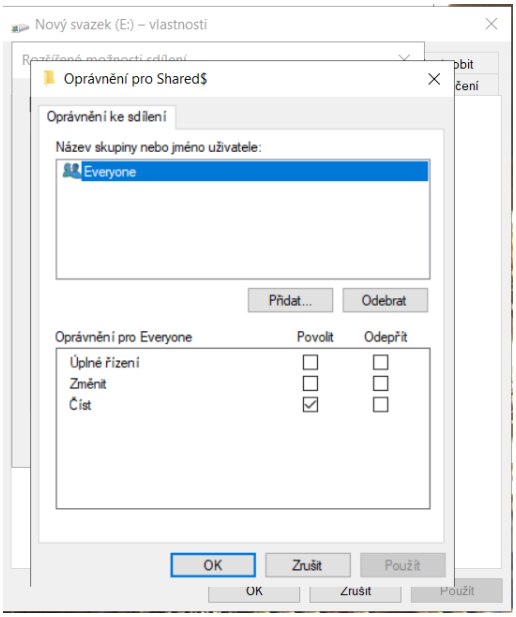


Obr. 21 Tvorba jednotek. Zdroj: Vlastní.

Obr. 22 Sdílení disku. Zdroj: Vlastní.



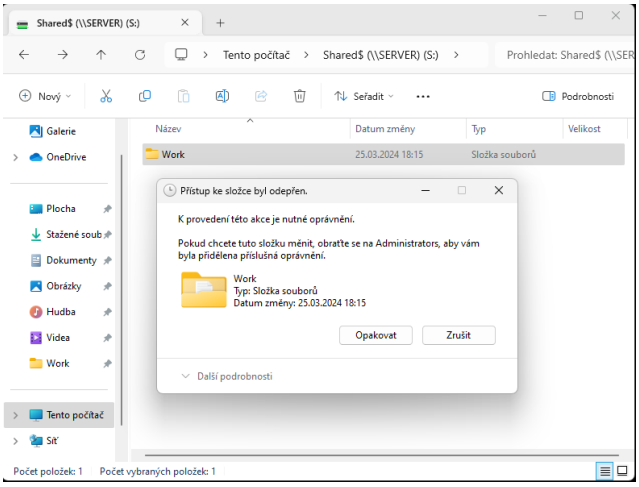
Obr. 23 Oprávnění uživatele. Zdroj: Vlastní.



Obr. 24 Oprávnění složky. Zdroj: Vlastní.

Ověření:

Po úspěšném nastavení a aktualizování politik ověříme. Na následujícím obrázku měníme složku a Windows nás zastaví.



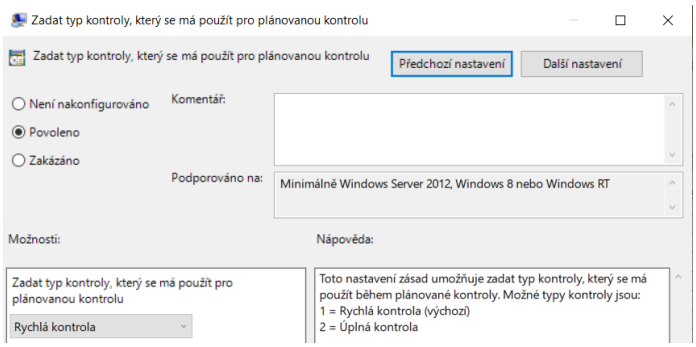
Obr. 25 Ověření politik sdílení. Zdroj: Vlastní.

6.2.3 Správa antiviru

Cílem tohoto kroku je nastavení GPO tak, aby byl správně konfigurovaný antivir. V případě Windows se jedná o Microsoft Defender. Cílem bude plánované skenování.

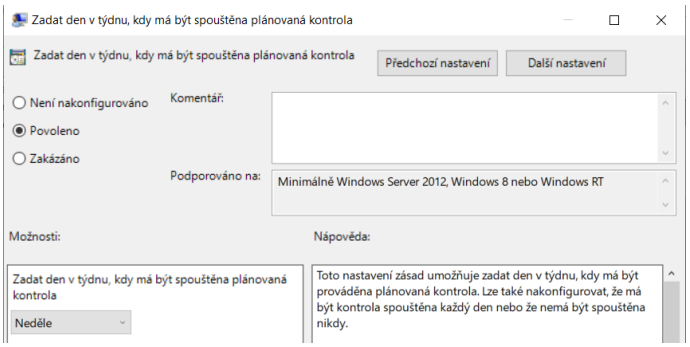
Konfigurace GPO:

Konfigurace počítače –> Zásady –> Šablony pro správu –> Součásti systému Windows –> Microsoft Defender –> Kontrola. Nejdříve je třeba určit typ kontroly, následně specifikovat, který den se bude kontrola provádět, a nakonec stanovit čas, kdy bude provedena.



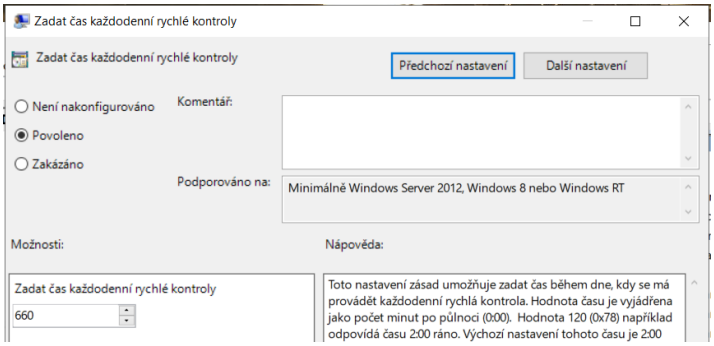
Obr. 26 Nastavení typu kontroly. Zdroj: Vlastní.

Na následujícím obrázku je natavení dne kontroly.



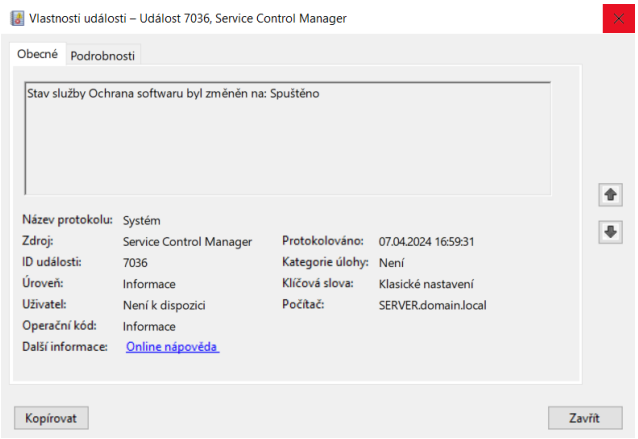
Obr. 27 Nastavení dne kontroly. Zdroj: Vlastní.

Na posledním obrázku se řeší čas, kdy kontrola bude probíhat. Nastavuji čas 660. To znamená, že se bude kontrolovat v čase 11:00.



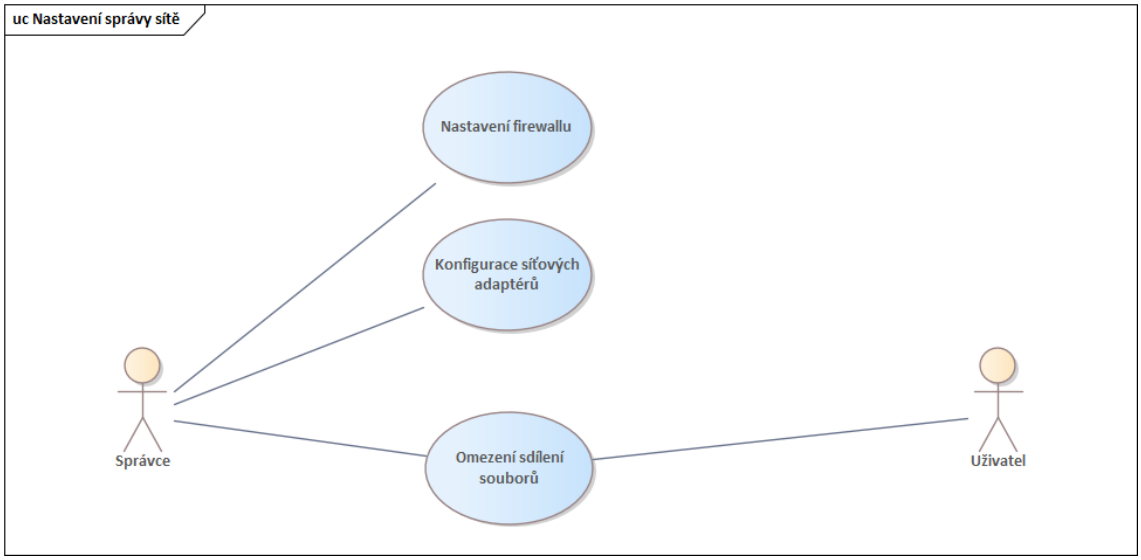
Obr. 28 Nastavení času. Zdroj: Vlastní.

Ověření:



Obr. 29 Funkčnost kontroly. Zdroj: Vlastní.

6.3 *Use case 2 – Správa sítě*



Obr. 30 Use case 2 - Správa sítě. Zdroj: Vlastní.

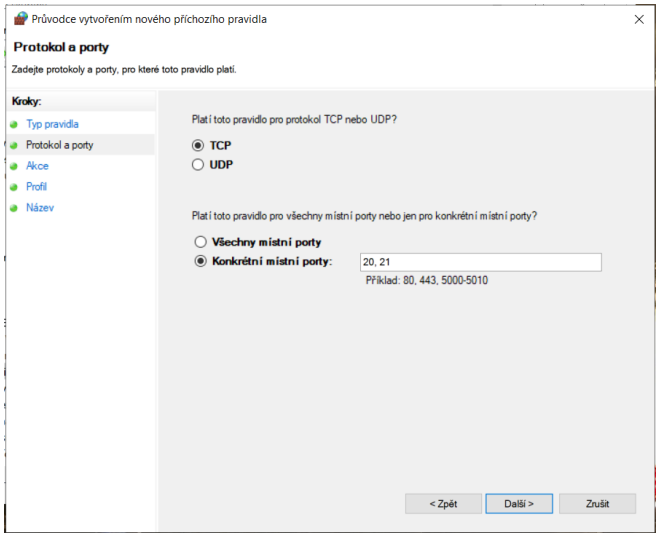
Use case je složen z třech dílčích kroků, které budou konfigurovány v rámci jednotlivých GPO a následně ověřena jejich funkčnost.

6.3.1 Nastavení firewallu

Cílem této konfigurace bude blokování komunikace protokolu FTP. Protokol FTP funguje na portech 20 a 21. Zakazujeme z důvodu nezabezpečeného přístupu.

Konfigurace GPO:

Konfigurace počítače –> Zásady –> Nastavení systému Windows –> Nastavení zabezpečení –> Firewall v programu Windows Defender s pokročilým zabezpečením. Nutné rozkliknout poslední bod. Pro správnou konfiguraci je nezbytné nastavit jak příchozí, tak odchozí pravidlo v bezpečnostním nastavení. V obou typech pravidel se vytvářejí dva stejné druhy pravidel.



Obr. 31 Tvorba pravidla. Zdroj: Vlastní.

Ověření:

Po správné konfiguraci a aktualizování politik ověříme toto pravidlo pomocí příkazové řádky a služby telnet.

```
C:\Windows\System32>telnet 172.16.1.1 20
Připojování k 172.16.1.1...Nelze navázat spojení s hostitelem. na portu 20: Připojení se nezdařilo

C:\Windows\System32>telnet 172.16.1.1 21
Připojování k 172.16.1.1...Nelze navázat spojení s hostitelem. na portu 21: Připojení se nezdařilo
```

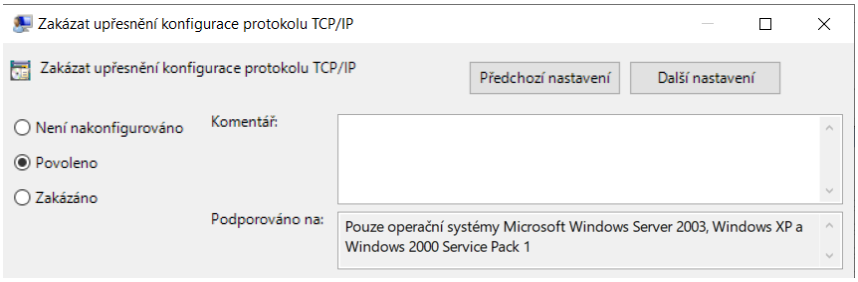
Obr. 32 Blokace portu 20 a 21. Zdroj: Vlastní.

6.3.2 Konfigurace síťových adaptérů

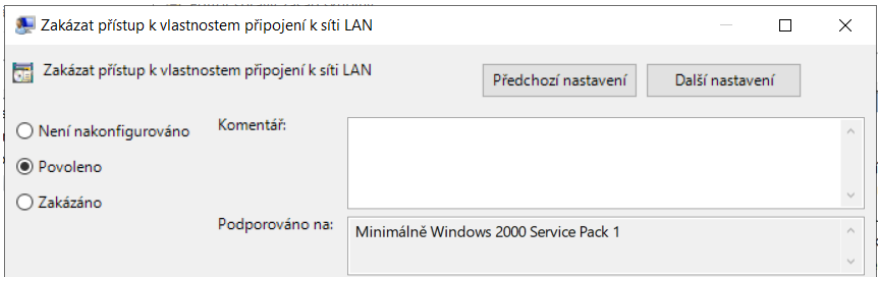
Cílem této konfigurace bude zakázání přístupu k vlastnostem připojení k síti LAN a zakázání upřesnění konfigurace protokolu TCP/IP.

Konfigurace GPO:

Konfigurace uživatele –> Zásady –> Šablony pro správu –> Síť –> Síťová připojení. Obě nastavení jsou nutná povolit.



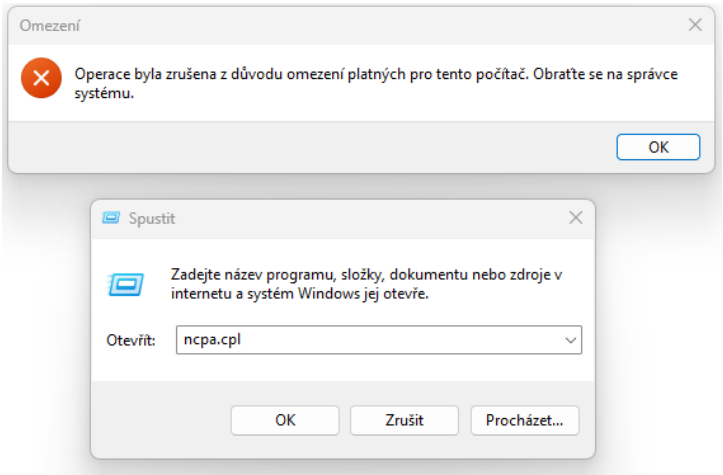
Obr. 33 Konfigurace TCP/IP. Zdroj: Vlastní.



Obr. 34 Konfigurace vlastností LAN. Zdroj: Vlastní.

Ověření:

Po úspěšném nastavení a následném aktualizování politik nás Windows nepustí do vlastností LAN a není možná další konfigurace.



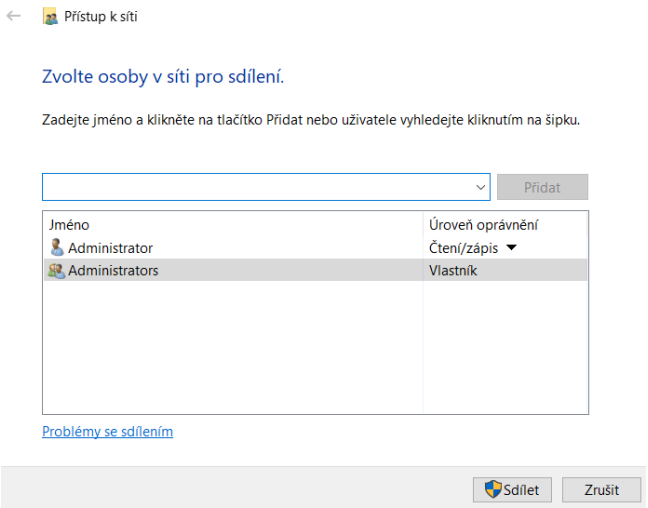
Obr. 35 Chybová zpráva ověření. Zdroj: Vlastní.

6.3.3 Omezení sdílení souborů

Cílem této konfigurace bude omezení přístupu k určitým adresářům nebo souborům pro specifické uživatele nebo skupiny.

Konfigurace GPO:

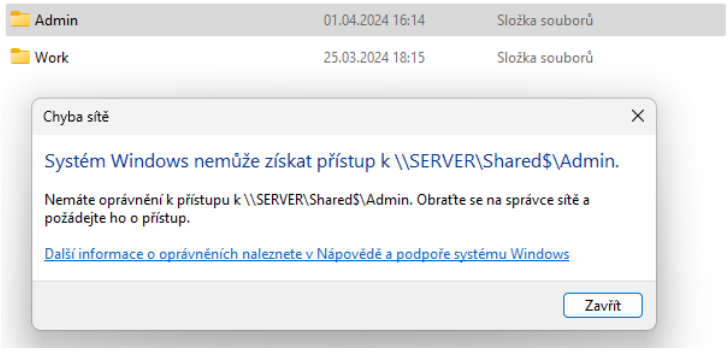
Na sdíleném disku vytvoříme novou složku a specifikujeme přístup pouze pro administrátora. Ostatní uživatelé budou mít tuto složku viditelnou, ale nebudou mít možnost k ní přistupovat. Tato situace názorně ukazuje, že ne každá konfigurace vyžaduje použití GPO politik.



Obr. 36 Nastavení přístupu. Zdroj: Vlastní.

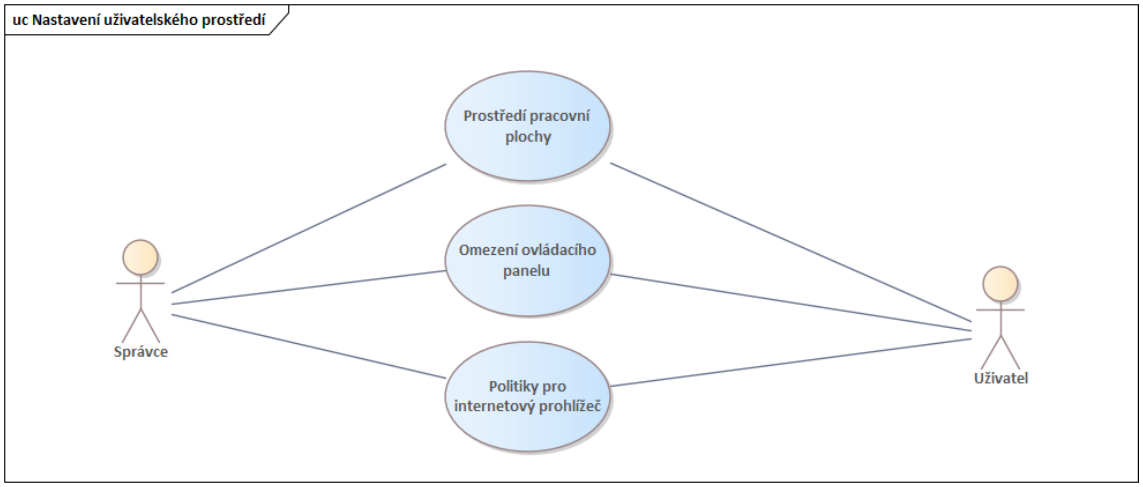
Ověření:

Ověření proběhne na stanici, kde se pokusíme otevřít danou složku (popřípadě ji zkusíme upravovat).



Obr. 37 Odepření přístupu. Zdroj: Vlastní.

6.4 Use case 3 – Uživatelské prostředí



Obr. 38 Use case 3 – Uživatelské prostředí. Zdroj: Vlastní.

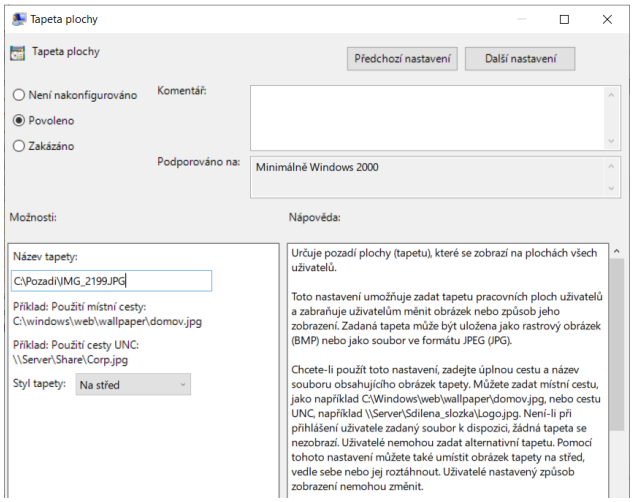
Use case je složen ze 3 dílčích kroků, které budou konfigurovány v rámci jednotlivých GPO a následně ověřena jejich funkčnost.

6.4.1 Prostředí pracovní plochy

Cílem tohoto nastavení bude zamezit uživatelům v používání vlastních pozadí na jejich účtech, což může přispět k udržení jednotného firemního vzhledu a zvýšení bezpečnosti systému.

Konfigurace GPO:

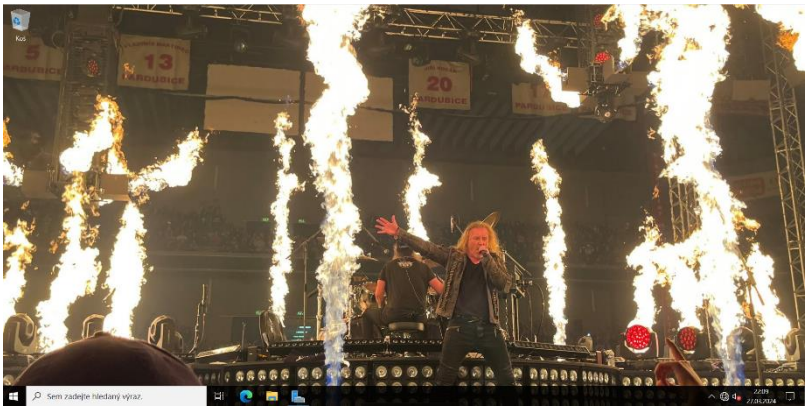
Konfigurace uživatele –> Zásady –> Šablony pro správu –> Plocha –> Tapeta plochy –> Povoleno. Tímto krokem určíme jednotné pozadí na stanicích a účtech. Nutností je vybrat obrázek, který se bude využívat.



Obr. 39 Nastavení jednotného obrázku na ploše. Zdroj: vlastní.

Ověření:

Po aktualizaci politik a nového přihlášení se nastaví daný obrázek, který jsme si zvolili.



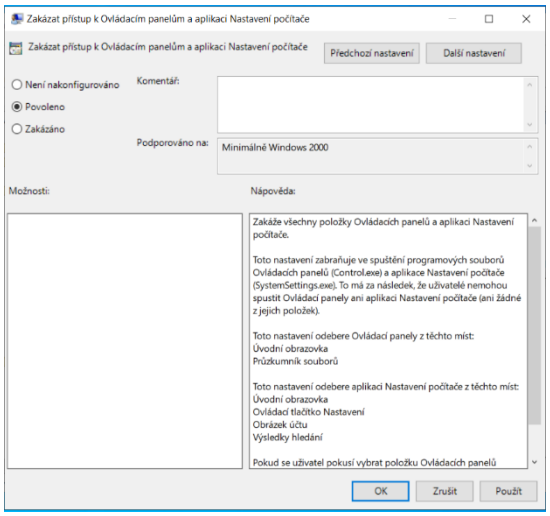
Obr. 40 Ukázka obrázku. Zdroj: Vlastní.

6.4.2 Omezení ovládacího panelu

Cílem tohoto nastavení bude zakázání přístupu uživatelů k funkcím ovládacího panelu a nastavení.

Konfigurace GPO:

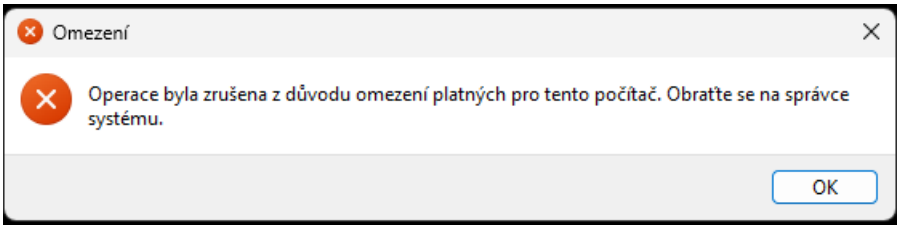
Konfigurace uživatele –> Zásady –> Šablony pro správu –> Ovládací panely –> Povolit



Obr. 41 Povolení zakázaní nastavení a OP. Zdroj: Vlastní.

Ověření:

Po aktualizaci politik a přihlášení uživatele se při otevření Ovládacích panelů zobrazí varovná tabulka. V případě, nastavení se však neotevře vůbec.



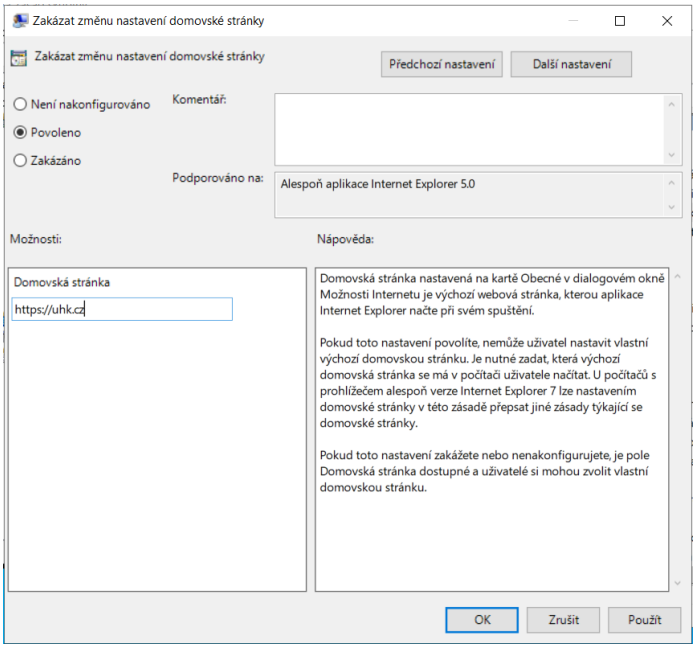
Obr. 42 Omezení ovládacích panelů. Zdroj: Vlastní.

6.4.3 Politiky pro internetový prohlížeč

Cílem tohoto nastavení bude nastavení hlavní stránky v Internet Explorer pomocí GPO politiky.

Konfigurace GPO:

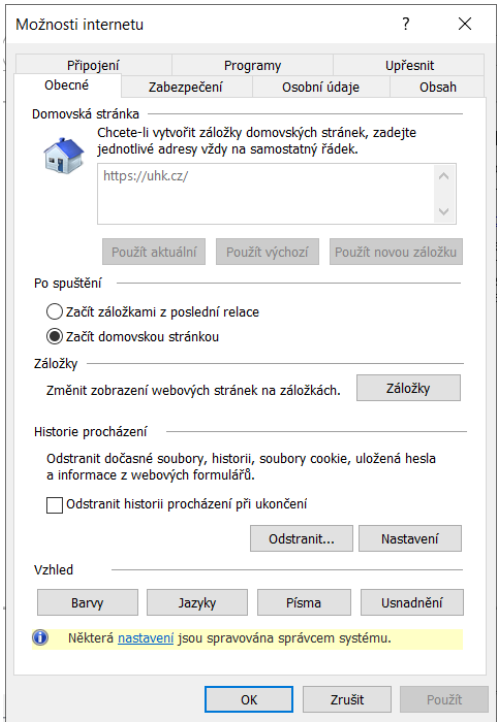
Konfigurace uživatele –> Zásady –> Šablony pro správu –> Součásti systému Windows –> Internet Explorer –> Zakázat změnu nastavení domovské stránky –> Povolit. Potřebné je definovat webovou stránku. V tomto případě to budou webové stránky UHK.



Obr. 43 Nastavení Webové stránky. Zdroj: Vlastní.

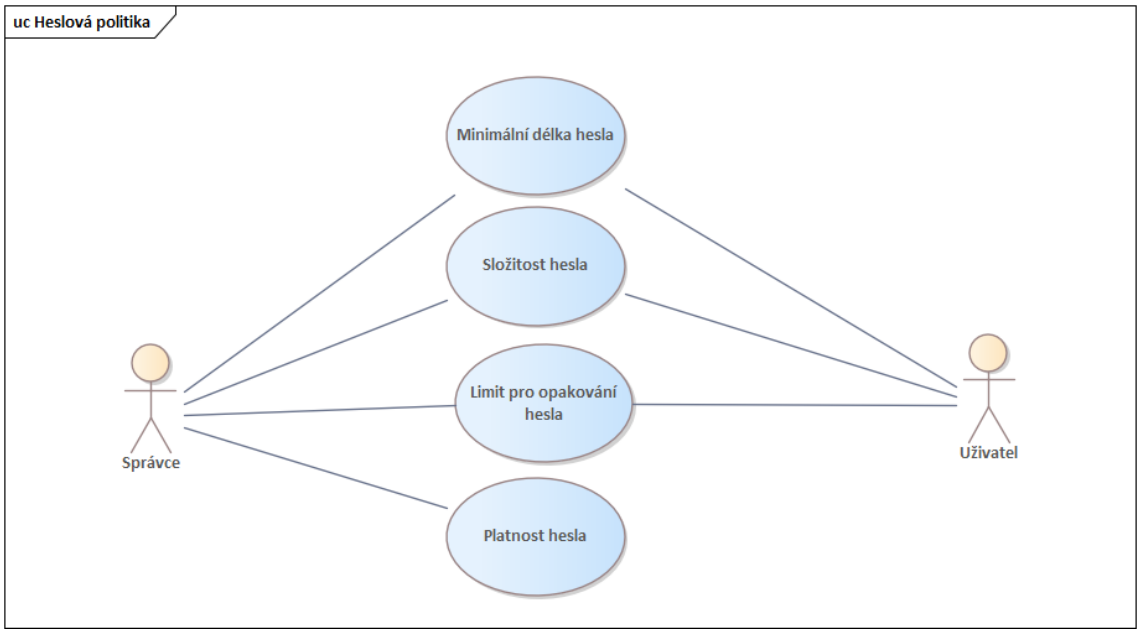
Ověření:

Po úspěšném konfiguraci a aktualizaci politik otevřeme Internet Explorer a je nutné zkontrolovat předem určenou webovou stránku.



Obr. 44 Ověření webové stránky. Zdroj: Vlastní.

6.5 Use case 4 – Heslová politika



Obr. 45 Use case 4 – Heslová politika. Zdroj: Vlastní.

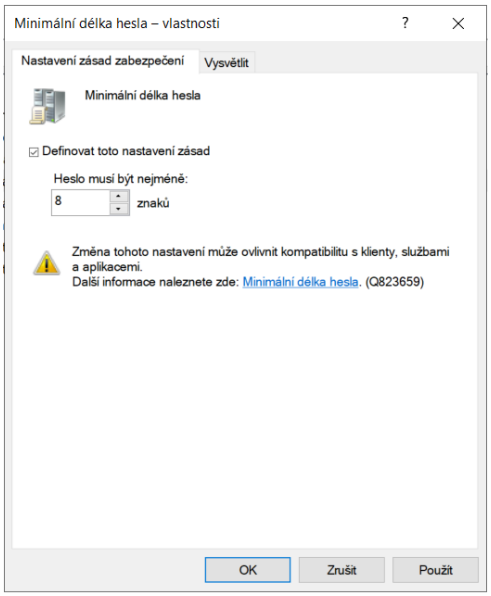
Use case je složen ze čtyřech dílčích kroků, které budou konfigurovány v rámci jednotlivých GPO a následně ověřena jejich funkčnost.

6.5.1 Minimální délka hesla

V tomto kroku se zaměříme na nastavení minimální délky hesla na 8 znaků, což je jedno ze základních bezpečnostních opatření pro ochranu uživatelských účtů. Tato délka zajistí, že hesla budou dostatečně složitá a odolná proti útokům.

Konfigurace GPO:

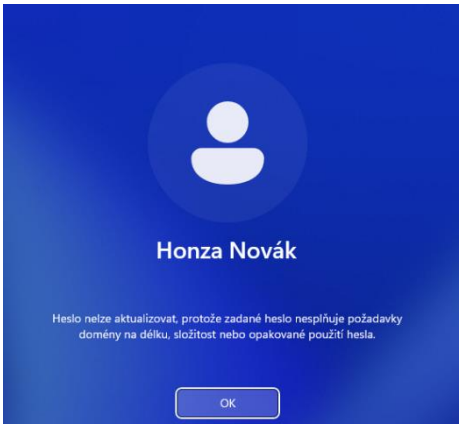
Konfigurace počítače –> Zásady –> Nastavení systému Windows –> Nastavení bezpečnosti –> Zásady účtu –> Zásady hesel –> Minimální délka hesla.



Obr. 46 Definování délky hesla. Zdroj: Vlastní.

Ověření:

Po úspěšné aktualizaci politik a požadavku na nové heslo je vyžadováno, aby heslo obsahovalo minimálně 8 znaků. Pokud uživatel nezadá heslo splňující tuto podmínku, zobrazí se následující chybová zpráva.



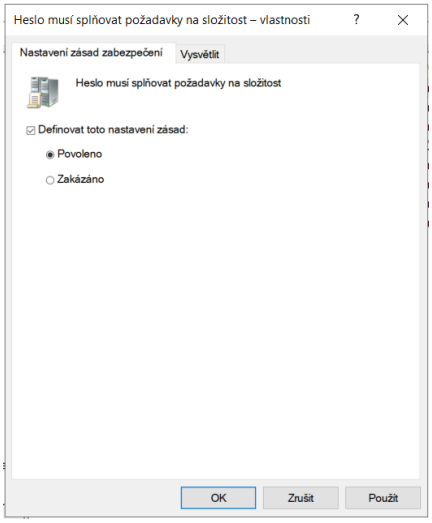
Obr. 47 Chybová hláška hesla. Zdroj: Vlastní.

6.5.2 Složitost hesla

Cílem tohoto kroku bude nastavení složitosti hesla, aby mohlo být používané. Heslo musí obsahovat číslice, velká a malá písmena a speciální znaky. Tato funkcionalita je dnešní standard.

Konfigurace GPO:

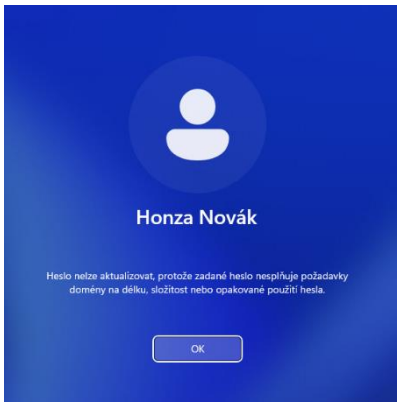
Konfigurace počítače –> Zásady –> Nastavení systému Windows –> Nastavení bezpečnosti –> Zásady účtu –> Zásady hesel –> Heslo musí splňovat požadavky na složitost –> Povoleno.



Obr. 48 Definování složitosti hesla. Zdroj: Vlastní.

Ověření:

Po úspěšné aktualizaci politik a požadavku na nové heslo je vyžadováno, aby heslo obsahovalo složitost. Pokud uživatel nezadá heslo splňující tuto podmínku, zobrazí se následující chybová zpráva.



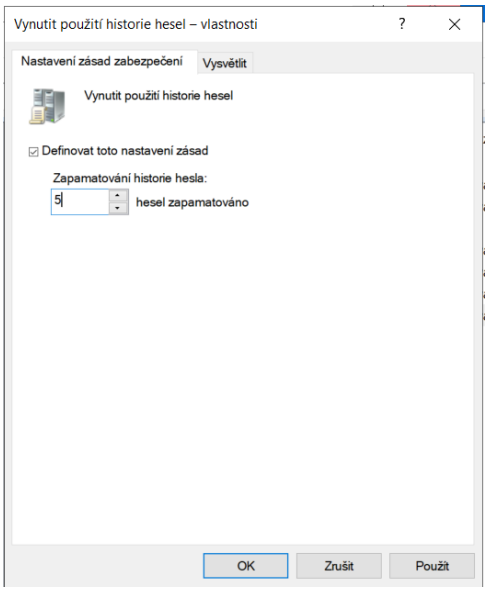
Obr. 49 Chybová hláška hesla. Zdroj: Vlastní.

6.5.3 Limit pro opakování hesla

Cílem tohoto opatření bude nastavení počtu zapamatovaných hesel. V tomto případě bude použito 5 hesel.

Konfigurace GPO:

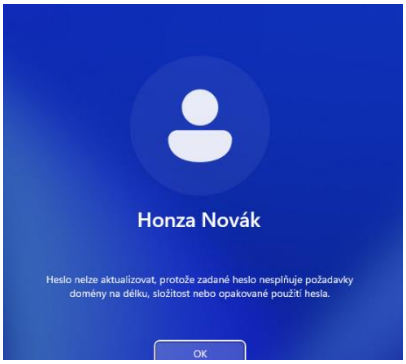
Konfigurace počítače –> Zásady –> Nastavení systému Windows –> Nastavení bezpečnosti –> Zásady účtu –> Zásady hesel –> Vynutit použití historii hesla



Obr. 50 Nastavení počtu zapamatovaných hesel. Zdroj: Vlastní.

Ověření:

Po úspěšné aktualizaci politik je vyžadováno, aby si server pamatoval posledních 5 hesel. Pokud uživatel nezadá heslo splňující tuto podmínku, zobrazí se následující chybová zpráva.



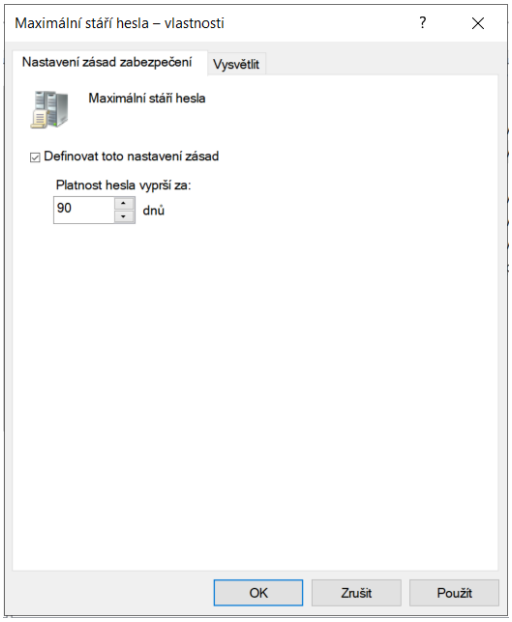
Obr. 51 Ověření pravidla. Zdroj: Vlastní

6.5.4 Platnost hesla

Cílem tohoto opatření bude nastavení délky platnosti daného hesla. Určení doby, po kterou může být heslo používáno. V tomto případě budeme používat kratší interval z důvodu bezpečnosti.

Konfigurace GPO:

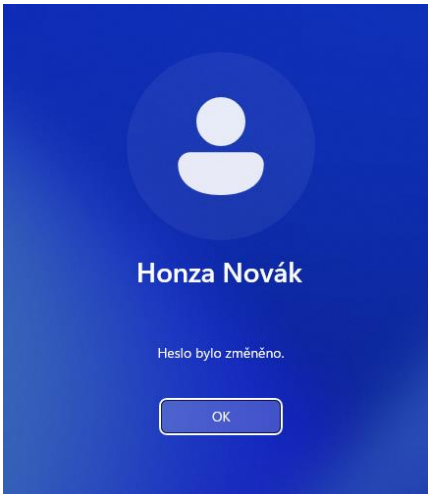
Konfigurace počítače –> Zásady –> Nastavení systému Windows –> Nastavení bezpečnosti –> Zásady účtu –> Zásady hesel –> Maximální stáří hesla.



Obr. 52 Nastavení délky životnosti hesla. Zdroj: Vlastní.

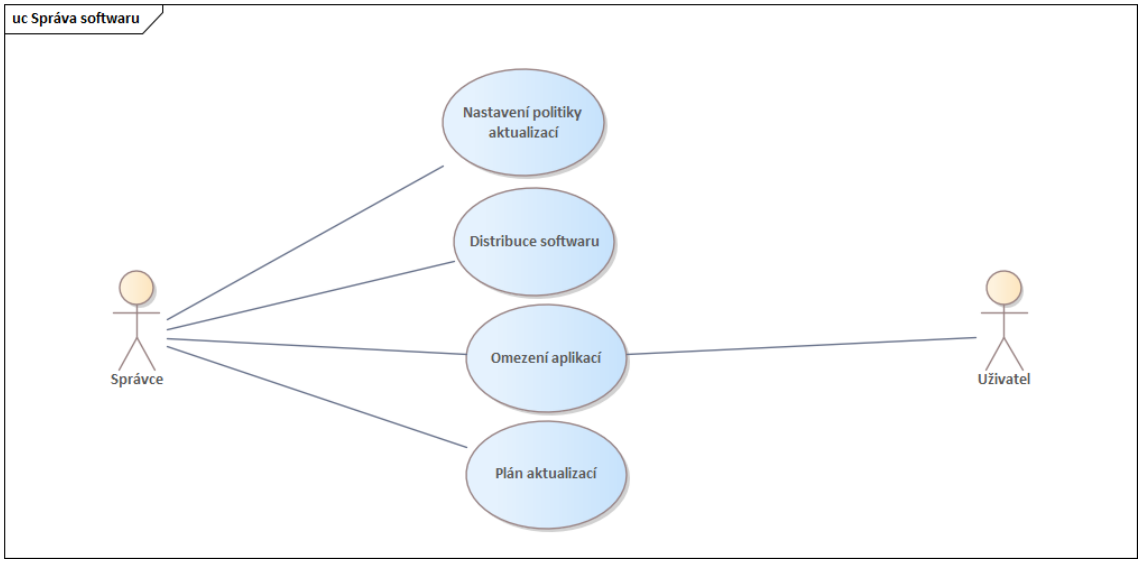
Ověření:

Po uplynutí doby si Windows vyžádá sám změnu hesla.



Obr. 53 Změna hesla po uplynutí doby. Zdroj: Vlastní

6.6 Use case 5 – Správa softwaru



Obr. 54 Use case 5 – Správa softwaru. Zdroj: Vlastní.

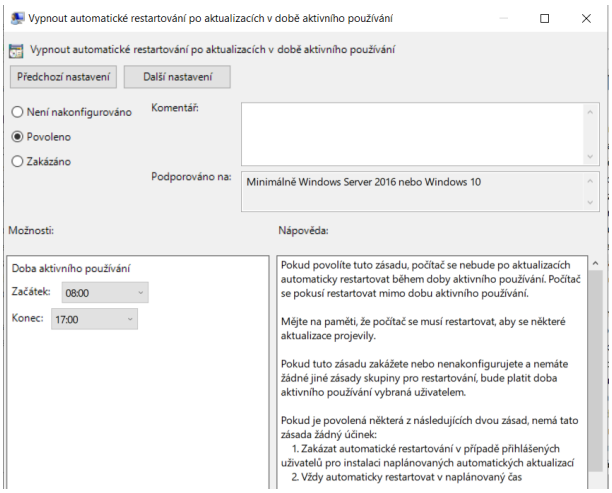
Use case je složen ze čtyřech dílčích kroků, které budou konfigurovány v rámci jednotlivých GPO a následně bude ověřena jejich funkčnost.

6.6.1 Nastavení politiky aktualizací

Cílem této konfigurace bude nastavení fungování aktualizací na stanicích. Příkladem je automatické aktualizování v době aktivního používání.

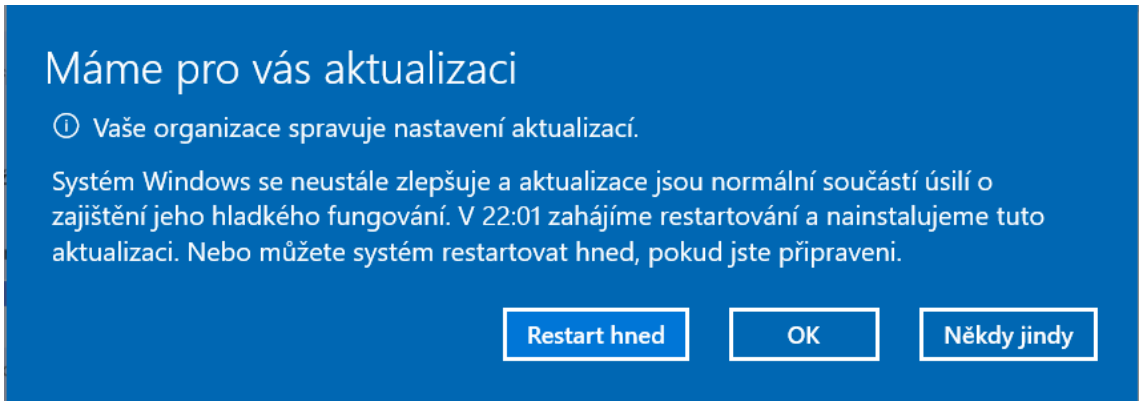
Konfigurace GPO:

Konfigurace počítače –> Zásady –> Nastavení systému Windows –> Nastavení zabezpečení –> Šablony pro správu –> Součásti systému Windows –> Windows Update –> Povolit. Poté se nastaví jen rozmezí času.



Obr. 55 Nastavení politiky Windows Update. Zdroj: Vlastní.

Ověření:



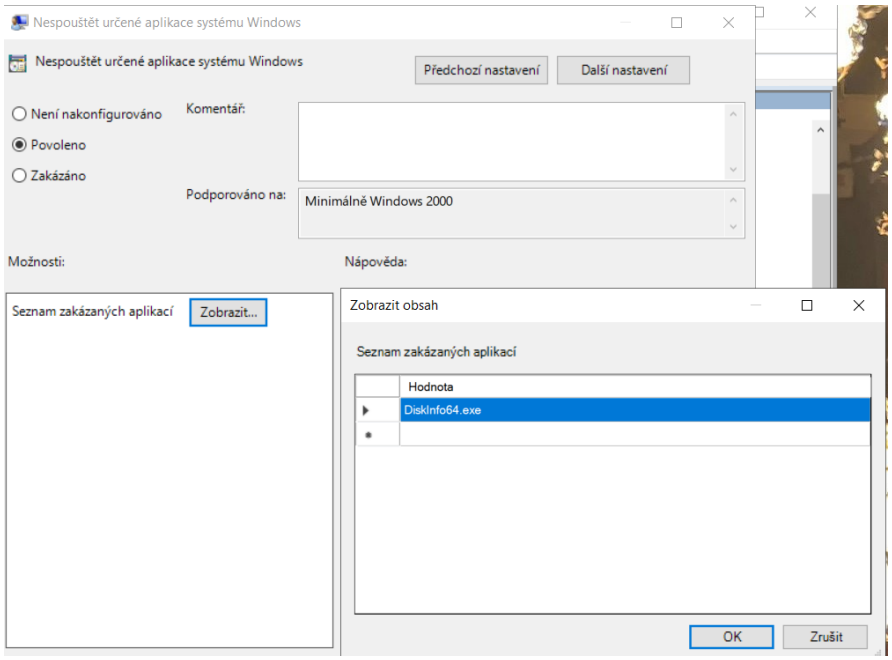
Obr. 56 Funkčnost aktualizací po daném čase. Zdroj: Vlastní.

6.6.2 Distribuce softwaru

Cílem této konfigurace bude zakázat instalované softwary třetích stran na stanicích s běžnými uživateli.

Konfigurace GPO:

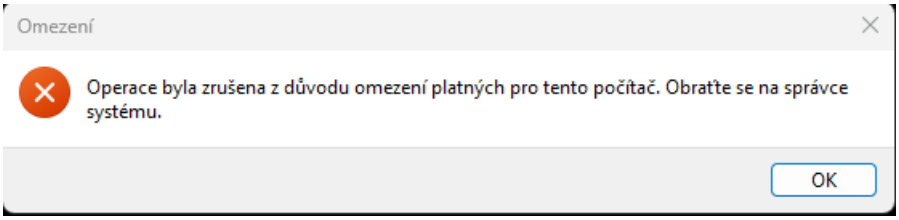
Konfigurace uživatele –> Zásady –> Šablony pro správu –> Systém –> Nespouštět určené aplikace systému Windows –> Povolit. Na seznam zakázaných aplikací je nutné dávat aplikace s koncovkou .exe.



Obr. 57 Konfigurace zakázání aplikaci. Zdroj: Vlastní.

Ověření:

Po úspěšném aktualizování politik na serveru i na stanici je určený software zakázaný a ukazuje chybovou zprávu omezení.



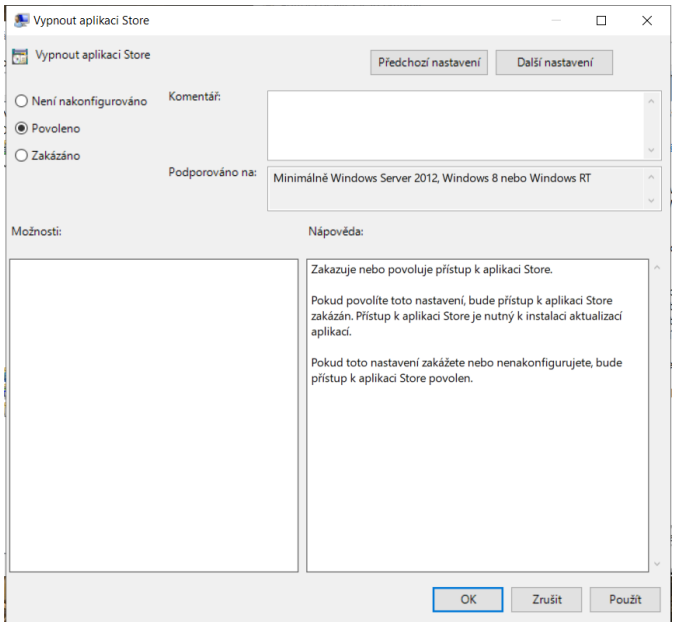
Obr. 58 Omezení. Zdroj: Vlastní.

6.6.3 Omezení aplikací

Cílem tohoto nastavení bude zakázání spouštění aplikací na základě uživatelských stanic. Konkrétně deaktivujeme aplikace Store od Microsoft.

Konfigurace GPO:

Konfigurace uživatele –> Zásady –> Šablony pro správu –> Součásti systému Windows –> Store –> Vypnout aplikaci store –> Povolit.



Obr. 59 Deaktivace aplikace Store. Zdroj: Vlastní.

Ověření:

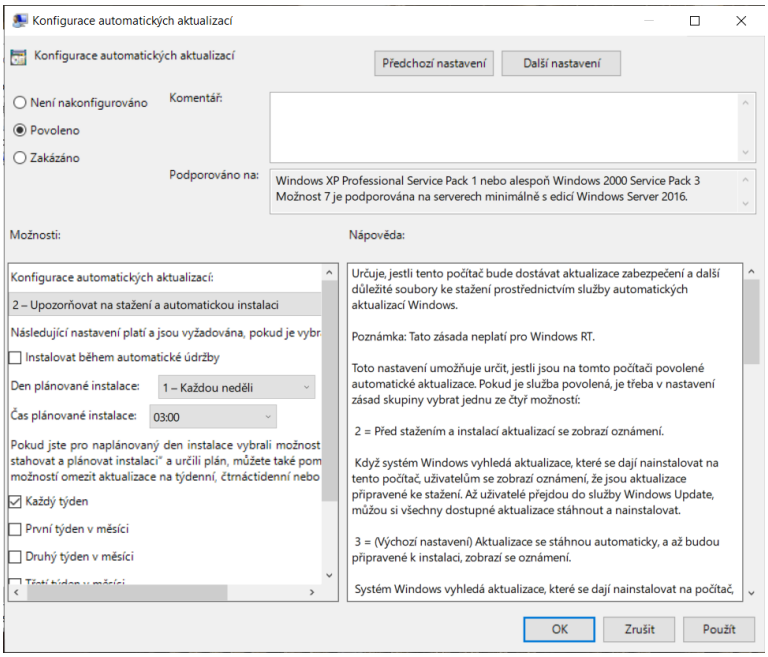
Po úspěšné aktualizaci politik se aplikace Store nespustí.

6.6.4 Plán aktualizací

Cílem tohoto nastavení bude definování plánu pro stahování a instalaci aktualizací systému Windows.

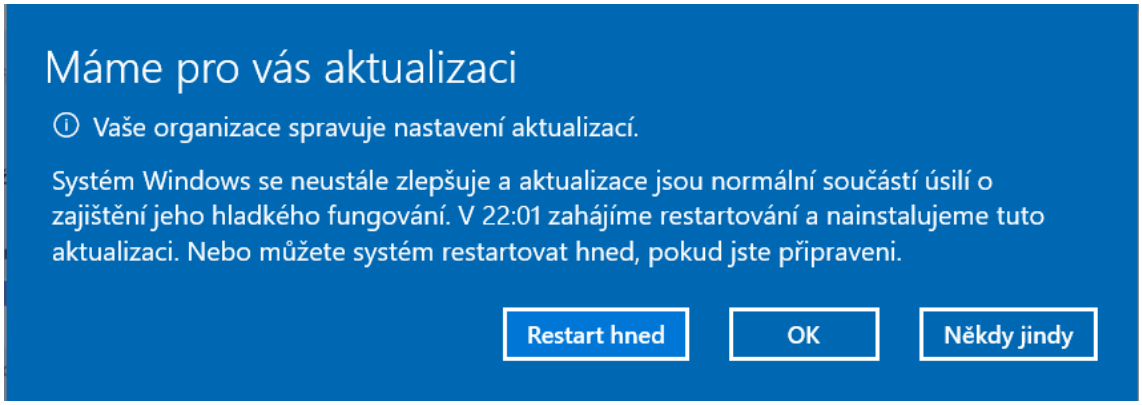
Konfigurace GPO:

Konfigurace uživatele –> Zásady –> Šablony pro správu –> Součásti systému Windows –> Windows Update –> Konfigurace automatických aktualizací –> Povolit V následném kroku je potřebné nastavit podrobnosti – viz. Obrázek.



Obr. 60 Konfigurace automatických aktualizací. Zdroj: Vlastní.

Ověření:



Obr. 61 Funkčnost aktualizací. Zdroj: Vlastní.

7 Shrnutí výsledků

V praktické části této práce bylo řešeno pět předem definovaných use cases pro tvorbu a zajištění kybernetické bezpečnosti v prostředí Windows od společnosti Microsoft. K vytvoření byl použitý Windows Server 22 a Windows 11, oba v nejnovějších verzích. Každý use cases obsahuje 3 až 4 body. Body v use cases jsou vypracované a ověřené. Témata (okruhy bezpečnosti), která byla řešena:

- Nastavení bezpečnosti
    - Přihlašovací obrazovka
    - Oprávnění souborů a složek
    - Správa antiviru
- Nastavení uživatelského prostředí
    - Prostředí pracovní plochy
    - Omezení ovládacího panelu
    - Politiky pro internetový prohlížeč
- Nastavení správy sítě
    - Nastavení firewall
    - Konfigurace síťových adaptérů
    - Omezení sdílení souborů
- Heslová politika
    - Minimální délka hesla
    - Složitost hesla
    - Limit pro opakování hesla
    - Platnost hesla
- Správa softwaru
    - Nastavení politiky aktualizací
    - Distribuce softwaru
    - Omezení aplikací
    - Plán aktualizací

Praktická část byla zaměřena na řešení problematiky kyberbezpečnosti a předcházení této problematiky. Všechna nastavení jsou plně funkční.

8 Závěry a doporučení

Tvorba funkčních a potřebných politik pomocí GPO (skupinové politiky) je velmi rozsáhlý a komplexní soubor nastavení. Soubor je rozdělený do spousty podkategorií. Každá podkategorie se zabývá specifickou problematikou. Tato práce je zaměřena na podstatné a doporučené způsoby použití GPO.

V teoretické části je vysvětlená historická linie operačních systému Windows a Linux včetně licencování a edic. Dále je rozebrána bezpečnost včetně parametrů bezpečnosti, které jsou nejčastěji používané pro zajištění bezpečnosti v operačních systémech. V posledním bodě je řešeno zajištění bezpečnosti v operačním systému Windows. Součástí tohoto bodu je Windows update, nejpodstatnějším bodem je GPO (skupinové politiky) na který navazuje praktická část této bakalářské práce.

Výsledkem této bakalářské práce je souhrn nastavení politik pro zajištění bezpečnosti v operačním systému Windows pomocí pěti use cases. Politiky jsou tvořené pro Windows Server 22, Windows 11 a jsou vytvořené v české jazyce (byla použitá česká verze operačního systému). Instalační média byla použita z webu Microsoft Azure (jedná se o službu společnosti Microsoft, která pomocí cloudu hostuje a škáluje webové aplikace).

Případným možným rozšířením práce by mohla být práce s dalšími rozšířeními samotného Windows Serveru 2022. Ve features je velké množství rolí, které jsou potřebné a tím pádem zajímavé i pro samostatné GPO skupinové politiky.

9 Seznam použité literatury

[1] ČERNÁ, Bc. Monika Černá a RNDr. Michal Černý Ph.D. ČERNÝ PH.D. Historie operačních systémů: Sálové počítače, Unix, DOS. *RPV* [online]. 2013 [cit. 2023-10-27]. Dostupné z: https://clanky.rvp.cz/clanek/c/g/15439/HISTORIE-OPERACNICH-SYSTEMU-SALOVE-POCITACE-UNIX-DOS.html

[2] CONTRIBUTOR, TechTarget. What is a window? Whatls [online]. 2021 [cit. 2023-10-27]. Dostupné z: https://www.techtarget.com/whatis/definition/window

[3] GICHUKI, Kenny. What Are the 3 Types of Windows Licensing? *Make Use Of* [online]. 2021 [cit. 2023-10-27]. Dostupné z: https://www.makeuseof.com/what-are-the-3-types-of-windows-licensing/

[4] COJOCARU, Alex, Ciprian GRIGORE a Chris ALLEN. Microsoft Windows Server 2022 licensing guide. Licenseware [online]. 2023 [cit. 2023-10-27]. Dostupné z: https://www.licenseware.io/microsoft-windows-server-2022-licensing-guide/

[5] Přehled cen a licencování pro Windows Server 2022. *Microsoft* [online]. [cit. 2024-03-08]. Dostupné z: https://www.microsoft.com/cs-cz/windows-server/pricing [6] HOPE, Computer. Windows. *Computer Hope* [online]. 2023 [cit. 2023-10-18]. Dostupné z: https://www.computerhope.com/jargon/w/windows.htm

[6] HOPE, Computer. Windows. Computer Hope [online]. 2023 [cit. 2023-10-18]. Dostupné z: https://www.computerhope.com/jargon/w/windows.htm

[7] KEJDUŠ, Radomír. Stručná historie operačních systémů: od UNIXu přes Windows k Mac OS X. CNEWS [online]. 2012 [cit. 2023-10-27]. Dostupné z: https://www.cnews.cz/clanky/strucna-historie-operacnich-systemu-od-unixu-pres-windows-k-mac-os-x/

[8] Windows OS History: Evolution of Windows Operating System from 1 to 11. AKURA, Rick. Softwarekeep [online]. 2024 [cit. 2024-01-03]. Dostupné z: https://softwarekeep.com/blog/history-of-windows-operating-system

[9] Ultimate Guide to Windows Server Including Versions & Dev History. COOPER, Stephen. *Comparitech* [online]. 2023 [cit. 2024-01-07]. Dostupné z: https://www.comparitech.com/net-admin/guide-windows-server/

[10] A Brief History of Linux. JUELL, Kathleen. Digitalocean [online]. 2023 [cit. 2024-01-07]. Dostupné z: https://www.digitalocean.com/community/tutorials/brief-history-of-linux

[11] The Complete History of Linux: Everything You Need to Know. HARZ, Tyler Von Harz. History-computer [online]. 2023, 202-09-02 [cit. 2024-01-07]. Dostupné z: https://history-computer.com/the-complete-history-of-linux-everything-you-need-to-know/

[12] Who Uses Linux? Companies That Use Linux and What Linux Is Used For. WAMBUA, Daisy Waithereo Wambua. *Careerkarma* [online]. 2022, 2023-02-04 [cit. 2024-01-25]. Dostupné z: https://careerkarma.com/blog/who-uses-linux/

[13] 11 surprising ways you use Linux every day. WATKINS, Don Watkins. *Opensource* [online]. 2019, 2019-09-30 [cit. 2024-01-25]. Dostupné z: https://opensource.com/article/19/8/everyday-tech-runs-linux

[14] What is Operating System Security? FRANÇOIS, Alexandre. *Techslang* [online]. 2024, 2024-01-01 [cit. 2024-01-31]. Dostupné z: https://www.techslang.com/definition/what-is-operating-system-security/

[15] Protection and Security in Operating System. TWINKLE, Sharma. *Scaler* [online]. 2023, 2023-10-15 [cit. 2024-01-31]. Dostupné z: https://www.scaler.com/topics/protection-and-security-in-operating-system/

[16] Five OS Vulnerabilities. EDIMO, Hilda. *Medium* [online]. 2021, 2021-02-23 [cit. 2024-01-31]. Dostupné z: https://laki-edimo.medium.com/five-os-vulnerabilities-1d9fafb1c87b

[17] Vulnerability in Security: A Complete Overview. KELLEY, Karin. *Simplilearn* [online]. 2020, 2020-10-20 [cit. 2024-01-31]. Dostupné z: https://www.simplilearn.com/vulnerability-in-security-article

[18] Windows operating system security. *Learn.microsoft* [online]. 2023, 2023-08-03 [cit. 2024-02-01]. Dostupné z: https://learn.microsoft.com/en-us/windows/security/operating-system-security/

[19] What Is the CIA Triad? , Coursera Staff. *Coursera* [online]. 2023, 2023-11-29 [cit. 2024-02-01]. Dostupné z: https://www.coursera.org/articles/cia-triad

[20] CIA: Je důvěrnost, integrita a dostupnost dostačující? ČERMÁK, Miroslav. *Cleverandsmart* [online]. 2018, 2018-12-02 [cit. 2024-02-01]. Dostupné z: https://www.cleverandsmart.cz/cia-je-duvernost-integrita-a-dostupnost-dostacujici/

[21] Co je kybernetický útok? *Microsoft* [online]. 2024, 2024-01-01 [cit. 2024-02-01]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-a-cyberattack

[22] 10 nejčastějších typů kybernetických útoků. DUBINSKÁ, Mgr. Lída. *Datasys* [online]. 2022, 2022-03-08 [cit. 2024-02-01]. Dostupné z: https://www.datasys.cz/10-nejcastejsich-typu-kybernetickych-utoku/

[23] Jaké jsou nejčastější typy kybernetických útoků? KRESA, Dan. *Kybez* [online]. 2018, 2018-03-08 [cit. 2024-02-01]. Dostupné z: https://kybez.cz/jake-jsou-nejcastejsi-typy-kybernetickych-utoku/

[24] Operating Systems: Types and Security. VARMA, Deepankar. *Towardsai* [online]. 2023, 2023-03-22 [cit. 2024-02-01]. Dostupné z: https://pub.towardsai.net/operating-systems-types-and-security-f319bec1078b

[25] Co je CIA triáda informační bezpečnosti. In: *Aptien* [online]. 2023 [cit. 2024-02-11]. Dostupné z: https://aptien.com/cs/kb/articles/what-is-cia-triad

[26] The Parkerian Hexad A More Complete Set of Information Security Elements. In: *Mósse Cyber Security Institute* [online]. 2022 [cit. 2024-02-11]. Dostupné z: https://library.mosse-institute.com/articles/2022/07/the-parkerian-hexad-a-more-complete-set-of-information-security-elements/the-parkerian-hexad-a-more-complete-set-of-information-security-elements.html

[27] Vulnerability Metrics. *Nvd.nist.gov* [online]. 2023 [cit. 2024-02-11]. Dostupné z: https://nvd.nist.gov/vuln-metrics/cvss

[28] What is a CVE? *Redhat* [online]. 2023 [cit. 2024-02-11]. Dostupné z: https://www.redhat.com/en/topics/security/what-is-cve

[29] What Is Data Encryption: Types, Algorithms, Techniques and Methods. , Simplilearn. *Simplilearn* [online]. 2023 [cit. 2024-02-11]. Dostupné z: https://www.simplilearn.com/data-encryption-methods-article

[30] NÚKIB. *NÚKIB* [online]. 2024 [cit. 2024-02-17]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/

[31] Origin & Evolution: An In-Depth Exploration of Advanced Persistent Threat (APT) Groups. , Simplilearn. Av-comparatives [online]. 2024 [cit. 2024-02-11]. Dostupné z: https://www.av-comparatives.org/origin-evolution-an-in-depth-exploration-of-advanced-persistent-threat-apt-groups/

[32] EDR vs XDR: What's the Difference? , Simplilearn. Blackberry [online]. 2024 [cit. 2024-02-11]. Dostupné z: https://www.blackberry.com/us/en/solutions/endpoint-security/extended-detection-and-response/xdr-vs-edr

[33] What is Cyber Espionage? BAKER, Kurt. *Crowdstrike* [online]. 2023 [cit. 2024-02-11]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

[34] Hacktivism. *Imperva* [online]. 2024 [cit. 2024-02-11]. Dostupné z: https://www.imperva.com/learn/application-security/hacktivism/

[35] Cyber Warfare. *Imperva* [online]. 2024 [cit. 2024-02-11]. Dostupné z: https://www.imperva.com/learn/application-security/cyber-warfare/

[36] What is cybercrime? How to protect yourself from cybercrime. *Kaspersky* [online]. 2024 [cit. 2024-02-11]. Dostupné z: https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

[37] *ENISA THREAT LANDSCAPE 2023* [online]. Enisa, 2023 [cit. 2024-02-19]. ISBN 978-92-9204-645-3. Dostupné z: doi:10.2824/782573

[38] *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2021* [online]. NÚKIB, 2021 [cit. 2024-02-19]. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf

[39] Group Policy Overview. *Learn.microsoft* [online]. 2016, 2016-08-31 [cit. 2024-02-11]. Dostupné z: https://learn.microsoft.com/en-us/previous-

versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v=ws.11)

[40] Co je Privileged Access Management (PAM)? *Microsoft* [online]. 2024 [cit. 2024-02-11]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-privileged-access-management-pam

[41] Important Group Policy Settings & Best Practices to Prevent Security Breaches. MURPHY, Danny. *Lepide* [online]. 2024, 2024-02-23 [cit. 2024-02-11]. Dostupné z: https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/

[42] Host-based Intrusion Prevention System (HIPS). *Help.eset* [online]. 2022, 2022-09-05 [cit. 2024-02-11]. Dostupné z: https://help.eset.com/ees/8/en-US/idh_hips_main.html

[43] Windows client updates, channels, and tools. *Learn.microsoft* [online]. 2023, 2023-08-24 [cit. 2024-02-11]. Dostupné z: https://learn.microsoft.com/en-us/windows/deployment/update/get-started-updates-channels-tools

[44] Security baselines. *Learn.microsoft* [online]. 2023, 2023-07-12 [cit. 2024-02-11]. Dostupné z: https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines

[45] MITRE ATT&CK Tactics in the Enterprise Matrix. In: *Delinea* [online]. 2024 [cit. 2024-03-01]. Dostupné z: https://delinea.com/blog/what-is-the-mitre-attack-framework

[46] What Is the MITRE ATT&CK Framework? *Trellix* [online]. 2024 [cit. 2024-02-11]. Dostupné z: https://www.trellix.com/security-awareness/cybersecurity/what-is-mitre-attack-framework/

[47] EventLog Tutorial Part I. *Manageengine* [online]. 2024 [cit. 2024-02-11]. Dostupné z: https://www.manageengine.com/network-monitoring/Eventlog_Tutorial_Part_I.html

[48] Group Policy Objects (GPOs): How They Work & Configuration Steps. HARRINGTON, David. *Varonis* [online]. 2023, 2023-06-12 [cit. 2024-03-08]. Dostupné z: https://www.varonis.com/blog/group-policy-objects

[49] Active Directory Domain Services Overview. *Learn.microsoft* [online]. 2022, 2022-08-17 [cit. 2024-03-08]. Dostupné z: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

[50] Understanding the Active Directory Logical Model. *Learn.microsoft* [online]. 2021, 2021-07-29 [cit. 2024-03-08]. Dostupné z: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model

[51] Understanding Group Policy & Group Policy Objects (GPOs). BLACKWELL, Jonathan. *Netwrix* [online]. 2023, 2023-09-28 [cit. 2024-03-08]. Dostupné z: https://blog.netwrix.com/group-policy/

[52] Group Policy Management Console. *Learn.microsoft* [online]. 2023, 2016-08-31 [cit. 2024-03-08]. Dostupné z: https://learn.microsoft.com/cs-cz/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn265969(v=ws.11)

[53] DistroWatch Page Hit Ranking. *Distrowatch* [online]. [cit. 2024-03-08]. Dostupné z: https://distrowatch.com/dwres.php?resource=popularity

[54] 10 Top Most Popular Linux Distributions of 2023. CÁNEPA, Gabriel. *Tecmint* [online]. 2023, 2023-05-18 [cit. 2024-03-08]. Dostupné z: https://www.tecmint.com/top-most-popular-linux-distributions/

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor: **Jiří Obst**

Studium: I2100532

Studijní program: B0688A140001 Informační management

Studijní obor: Informační management

Název bakalářské práce: **Group policy security baseline pro OS Windows**

Název bakalářské práce AJ: Windows group policy security baseline

Cíl, metody, literatura, předpoklady:

Cílem bakalářské práce je představení problematiky group policy v operačních systémech Windows pro zajištění parametrů důvernosti, dostupnosti a integrity dat, tedy základním stavebním kamenům zajištění bezpečnosti operačních systémů. V teoretické části autor představí a podrobně popíše principy group policy a jejich využití pro zajištění bezpečnosti OS s vazbou na security baseline Microsoft. V praktické části pak autor vytvoří praktická řešení dílčích úloh nastavení group policy dle předem definovaných usecase v organizaci ze soukromého sektoru.

KRAUSE, Jordan. *Mastering Windows Group Policy*. Birmingham: Packt Publishing Limited, 2018. ISBN 1789347394.

Zadávající pracoviště: Katedra informačních technologií,
Fakulta informatiky a managementu

Vedoucí práce: Ing. Tomáš Svoboda, Ph.D.

Datum zadání závěrečné práce: 15.10.2021