VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

IMPLEMENTACE ZÁKLADNÍCH BEZPEČNOSTNÍCH STANDARDŮ MATEŘSKÉ SPOLEČNOSTI

IMPLEMENTATION OF BASIC SECURITY STANDARDS OF THE PARENT COMPANY

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Jakub Valný

AUTHOR

VEDOUCÍ PRÁCE — Ing. Viktor Ondrák, Ph.D.

SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Jakub Valný**
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2022/23
Studijní program:	Informační management

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Implementace základních bezpečnostních standardů mateřské společnosti

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout Implementaci základních bezpečnostních standardů mateřské společnosti

Základní literární prameny:

SMITH, Ben a Brian KOMAR. Zabezpečení systému a sítě Microsoft Windows. Přeložil David KRÁSENSKÝ, přeložil Anna RYCHETSKÁ. Brno: Computer Press, 2006. ISBN 978-80-251-1260-1.

STANEK, William R. Microsoft Windows Server 2012: kapesní rádce administrátora. Přeložil Jiří HUF. Brno: Computer Press, 2015. ISBN 9788025138175.

SANTHOSH, Sivarajan. Getting Started with Windows Server Security. Birmingham: Packt Publishing, 2015. ISBN 1784398721.

JORDAN, Krause. Mastering Windows Server 2019. 2nd edition. Birmingham: Packt Publishing, 2019. ISBN 978-1789804539.

FRANCIS, Dishan. Mastering Active Directory. 3rd ed. Birmingham: Packt Publishing, 2021. ISBN 978-1801070393.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2022/23

V Brně dne 5.2.2023

L. S.

doc. Ing. Miloš Koch, CSc. garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Tato práce se zabývá implementací základních bezpečnostních standardů mateřské společnosti. První částí této práce jsou teoretická východiska, ve kterých jsou popsány a vysvětleny všechny potřebné pojmy. Druhou částí této práce je analýza současného stavu, ve které je rozebrán současný stav bezpečnosti v rámci domény dceřiné společnosti a také požadavky mateřské společnosti. Třetí částí této práce je vlastní návrh řešení, ve kterém je podrobně rozepsán návrh na implementaci všech požadavků. V rámci návrhu řešení je také management zavádění a ekonomické zhodnocení s přínosy.

Klíčová slova

Active Directory, Zabezpečení, Politika, Organizační jednotka, Tier Model, Doménový řadič, Doména, Správce

Abstract

This thesis deals with the implementation of the basic security standards of the parent company. The first part of this thesis is the theoretical starting point, in which are described and explained all the necessary concepts. The second part of this thesis is an analysis of the current state, in which is discussed the current state of security within the domain of the subsidiary company and also the requirements of the parent company. The third part of this thesis is the actual design of the solution, in which is detailed my proposal for the implementation of all requirements. Implementation management, economic evaluation and benefits are parts of the solution design as well.

Keywords

Active Directory, Security, Policy, Organizational Unit, Tier Model, Domain Controller, Domain, Administrator

Bibliografická citace

VALNÝ, Jakub. *Implementace základních bezpečnostních standardů mateřské společnosti* [online]. Brno, 2023 [cit. 2023-05-13]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/148698. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 13. 5. 2023

Bc. Jakub Valný

autor

Poděkování

Chtěl bych poděkovat svému vedoucímu Ing. Viktorovi Ondrákovi, Ph.D. za vedení a odborné rady při psaní této diplomové práce. Dále bych chtěl poděkovat zvolené společnosti za možnost psát tuto diplomovou práci právě v jejím prostředí.

Obsah

Úvod

V dnešní době je bezpečnost velké téma a čím dál více se dostává i do podvědomí firem, které o něj zatím nejevily moc velký zájem. Každý den proběhne obrovské množství plošných i cílených útoků všech různých druhů za účelem poškodit společnosti.

Bezpečnost se postupně začíná řešit ve všech společnostech, protože je jen otázkou času, kdy bude nějaký úspěšný útok zrealizován právě na ně. Nicméně navzdory všem hrozbám a možným dopadům se společnostem nechtějí vydávat velké náklady na bezpečnost, protože většina opatření je velmi nákladná a na první pohled není nikde vidět.

Bezpečnost je velmi rozsáhlé téma, které zahrnuje širokou škálu opatření, mezi které patří například různé konkrétní softwarové a hardwarové nástroje, stejně tak jako školení uživatelů a organizační opatření.

Ve své diplomové práci se zaměřím na návrh implementace základních bezpečnostních standardů mateřské společnosti. Návrh bude převážně zaměřen na obecná nastavení týkající se Active Directory a organizační opatření z několika důvodů. Hlavním důvodem je fakt, že jsem vázán smlouvou o mlčenlivosti a nemohu popisovat například konkrétní síťové prostředí a konfiguraci. Naproti tomu výhodou je, že můj návrh je z velké části univerzální a dá se aplikovat na širokou škálu společností. Hlavní výhodou je podle mého názoru fakt, že navrhovaná opatření výrazně zvyšují úroveň bezpečnosti v daném prostředí za vynaložení velmi nízkých nákladů.

Cíle práce, metody a postupy zpracování

Cílem této diplomové práce je zpracovat návrh na implementaci základních bezpečnostních standardů mateřské společnosti do prostředí dceřiné společnosti, obě zmíněné společnosti budou v rámci celé diplomové práce anonymizovány. Účelem implementace bezpečnostních standardů je zvýšení úrovně bezpečnosti v prostředí organizace dceřiné společnosti. Zaváděná opatření se soustředí převážně na zabezpečení Active Directory.

V rámci teoretické části práce jsou vysvětleny všechny potřebné pojmy k pochopení a vypracování analýzy současného stavu a vlastního návrhu řešení.

V analýze současného stavu je stručně představena anonymizovaná společnost a vysvětleno, co předcházelo implementaci bezpečnostních standardů. Dále je v rámci této kapitoly rozebrán současný stav prostředí a bezpečnosti v organizaci společně s požadavky mateřské společnosti.

Kapitola vlastní návrhy řešení obsahuje kompletní návrh a postupy implementace bezpečnostních požadavků z technického pohledu. Dále je v rámci této kapitoly navrhnut také management zavádění požadavků. Tato kapitola také zahrnuje ekonomické zhodnocení a přínosy řešení.

1 Teoretická východiska

V této části diplomové práce se budu zabývat pojmy, které jsou důležité pro zpracování a pochopení zbylých kapitol. V první podkapitole jsou rozebrány základní pojmy týkající se bezpečnosti, dále se ve většině teoretické části věnuji počítačové doméně a pojmům, které s ní souvisí. Na konci teoretické části se věnuji pojmům, které jsou obsaženy v rámci ekonomického zhodnocení a managementu zavádění.

1.1 Základní pojmy bezpečnosti

Následující body vysvětlují základní pojmy v kontextu informační bezpečnosti.

1.1.1 Informační bezpečnost

Informační bezpečnost se zabývá opatřeními a procesy, které mají minimalizovat rizika a hrozby spojené se ztrátou, zneužitím nebo poškozením informací. Informační bezpečnost se věnuje ochraně informací, bez ohledu na to, zda jsou uloženy v elektronické nebo jiné formě. (6)

1.1.2 Kybernetická bezpečnost

Kybernetická bezpečnost je oblast zabezpečení, která úzce souvisí s informační bezpečností, ale zaměřuje se především na ochranu digitálních systémů, sítí, zařízení a infrastruktury před kybernetickými hrozbami. Cílem kybernetické bezpečnosti je minimalizovat rizika a škody, které by mohly být způsobeny kybernetickými útoky a zajistit ochranu dat a informací v kyberprostoru. (6)

1.1.3 Aktivum

Aktiva v kontextu bezpečnosti jsou informace, technologie a další prvky, které organizace vlastní nebo spravuje a mají pro ni určitou hodnotu. Příklady aktiv jsou například informační systémy, soubory dat, databáze, software, hardware, telekomunikační zařízení, fyzická zařízení a další prvky, které jsou pro organizaci klíčové. Aktiva musí být chráněna před neoprávněným přístupem, zneužitím, poškozením nebo ztrátou. (6)

1.1.4 Hrozba

Hrozbu definujeme jako jakýkoliv vnitřní nebo vnější faktor, který má potenciál nežádoucím způsobem ovlivnit aktivum. Hrozba může způsobit například negativní změny ve struktuře, vlastnostech nebo vazbách aktiva, či jakékoliv jiné poškození. (6)

1.1.5 Riziko

Riziko je pravděpodobnost vzniku nežádoucí události, která může mít negativní dopad na aktiva. (6) (7)

1.1.6 Zranitelnost

Zranitelnost lze definovat jako potenciální slabé místo v aktivu, které může být zneužito a ohrozit tak bezpečnost aktiva, objektů nebo osob. Zranitelnost může být přítomna v různých oblastech, jako je například fyzická bezpečnost, informační bezpečnost nebo bezpečnost procesů. (6) (7)

1.1.7 Bezpečnostní událost

Jedná se o událost, která může mít vliv na bezpečnost, dostupnost nebo integritu aktiv. Bezpečnostní událost jako taková nemusí způsobit žádný dopad, může například pouze způsobit narušení bezpečnosti. (6)

1.1.8 Bezpečnostní incident

Bezpečnostní incident je specifickou formou bezpečnostní události, která se stala skutečným problémem. Jedná se o incident, který narušuje bezpečnost, dostupnost nebo integritu aktiv, mezi příklady patří například úspěšné útoky hackerských skupin, krádeže dat, narušení firemní politiky bezpečnosti a další. (6)

1.1.9 Dopad

Jedná se o důsledek bezpečnostního incidentu, může mít vážné důsledky pro organizaci, jako jsou ztráta důvěryhodnosti u zákazníků, finanční ztráty, ztráta dat, narušení obchodních procesů a další. (6) (7)

1.1.10 Bezpečnostní opatření

Bezpečnostní opatření jsou kroky, procesy nebo technologie, které jsou navrženy a implementovány za účelem minimalizace rizika v oblasti bezpečnosti. Cílem je ochrana aktiv před neoprávněným přístupem, ztrátou, poškozením nebo zneužitím. Bezpečnostní opatření mohou být implementována pro různé úrovně, jako jsou hardware, software, procesy, nebo politiky. (6) (7)

1.1.11 Útok

Útok je jakýkoli neoprávněný pokus o porušení bezpečnosti, například úmyslné vniknutí do počítačových systémů, sítí nebo aplikací za účelem získání neoprávněného přístupu k informacím, poškození nebo ukradení citlivých dat. Útoky mohou být cílené, nebo plošné. (6) (7)

1.2 Doména

Doména je logická struktura v počítačové síti, která umožňuje organizovat počítače a uživatele do jednotného systému. Účelem domény je poskytnout jednotné prostředí pro správu uživatelů, počítačů a dalších prvků v síti. Doména se skládá z jednoho nebo více počítačů, které spolu spolupracují, aby poskytovaly služby autentizace, autorizace a umožnily správu sítě. Tyto počítače nazýváme doménové řadiče (Domain Controller – DC). (2) (5)

a) **Autentizace**: ověření identity uživatele nebo počítače před přístupem k síťovým zdrojům
b) **Autorizace**: určení, zda má uživatel nebo počítač oprávnění k přístupu k určitým zdrojům nebo k provádění určitých operací
c) **Správa**: jednotná a centralizovaná správa uživatelů, počítačů a dalších zdrojů v síti (5)

1.2.1 Struktura

Struktura domény se skládá z hierarchického uspořádání objektů, které reprezentují jednotlivé prvky v síti. Hlavním prvkem je sama doména, která je nejvyšším prvkem v hierarchii a obsahuje všechny ostatní objekty. (2) (5)

1.2.2 Strom

Strom je seskupení nebo hierarchická organizace jedné nebo více domén. V síti existuje pouze jedna kořenová doména, kterou také nazýváme rodičovská doména, v případě že se v síti nachází další domény, nazýváme je podřízené domény. Všechny domény v doménovém stromu sdílejí stejný jmenný prostor. (2) (5)

1.2.3 Les

Les je seskupení jednoho nebo více oddělených nezávislých stromů. Všechny domény v lese sdílí stejné schéma a globální katalog. Domény jsou propojeny pomocí vztahů důvěry. Jednotlivé stromy domén mají vlastní jmenný prostor. (2) (5)

1.3 Windows server

Windows Server je operační systém od společnosti Microsoft určený pro poskytování služeb v síti. Windows Server nabízí širokou škálu funkcí a nástrojů pro správu, virtualizaci, zabezpečení a ukládání dat, díky kterým umožňuje organizacím lépe využívat své zdroje. Mezi klíčové funkce a služby patří Active Directory, Group Policy, Virtualizace, Remote Desktop Services (připojení ke vzdálené ploše) a Serverové role (file server, print server, web server, DNS server, DHCP server a další). (2) (4)

1.3.1 Registry

Registry jsou součástí operačního systému Microsoft Windows a slouží k ukládání informací o konfiguraci a nastavení systému, aplikací a služeb v počítači. Registry jsou hierarchické struktury, skládají se z klíčů a hodnot, přičemž každý klíč může obsahovat další klíče a hodnoty. (4) (8)

1.3.2 Služby

Služby ve Windows jsou programy, které běží v pozadí a poskytují funkce a podporu pro operační systém a aplikace. Mezi nejběžnější služby, které jsou ve Windows, patří například služby síťového připojení, zabezpečení, tisku, správy aktualizace systému, správy hardwaru a mnoho dalších. (4) (8)

1.3.3 Úlohy

V operačním systému Windows je pojem úloha obvykle spojen s různými činnostmi nebo akcemi, které provádí uživatel nebo systém. (4) (8)

1.3.4 RSAT

RSAT (Remote Server Administration Tools) jsou nástroje pro vzdálenou správu serverů a služeb v prostředí Windows. RSAT poskytuje sadu nástrojů pro správu různých funkcí a služeb Windows Serveru z jiného počítače v síti, což umožňuje správcům snadno a efektivně spravovat vzdálené servery a služby. RSAT zahrnují nástroje pro správu Active Directory, DNS, DHCP, Remote Desktop Services a dalších funkcí a služeb. (4) (8)

1.4 Active Directory

Active Directory (AD) je systém pro správu identit a přístupu, který se používá v sítích postavených na operačním systému Microsoft Windows. Je to hierarchická databáze, která uchovává informace o uživatelích, skupinách, počítačích a dalších objektech v síti. Primární role AD je poskytování centrálních služeb pro autentizaci a autorizaci, AD ale také poskytuje služby pro správu domény, mezi které patří například skupinové politiky a další funkce pro správu sítě. (2) (5) (8)

Active Directory umožňuje:

- Centralizovanou správu uživatelů a skupin, včetně jejich hesel a oprávnění
- Automatickou správu počítačů v síti
- Správu aplikací a služeb, které jsou v síti dostupné
- Správu síťových zdrojů, jako jsou tiskárny nebo síťové disky
- Autentizaci a autorizaci uživatelů v síti
- Správu bezpečnostních politik v síti (5)

1.4.1 Vlastnosti AD

AD má následující vlastnosti:

- **Hierarchická organizace** – AD umožňuje organizaci objektů (uživatelé, skupiny, počítače a jiné) do hierarchické struktury
- **Replikace dat** – AD využívá mechanismy replikace dat mezi doménami a doménovými řadiči, to umožňuje efektivní distribuci informací v celé síti
- **Škálovatelnost** – AD může být používána v malých sítích i v rozsáhlých korporátních prostředích, její architektura a možnosti konfigurace umožňují snadnou škálovatelnost podle potřeb organizace

- **Bezpečnost** – AD zahrnuje rozsáhlé bezpečnostní funkce, včetně autentizace a autorizace uživatelů, správy oprávnění k objektům v síti a auditování přístupových práv
- **Integrace** – AD lze snadno integrovat s dalšími produkty od společnosti Microsoft, jako je například Exchange Server, SharePoint a další (5)

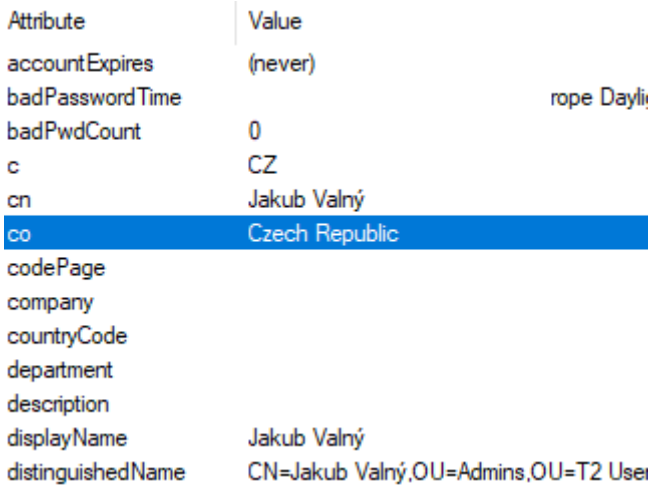
1.4.2 Objekty

Objekt v AD představuje ve většině případů nějaký prvek v síti, ale může se jednat také o logickou entitu. V AD existuje několik typů objektů, které slouží k různým účelům. (5)

- **Uživatel**: Objekt uživatel (user) představuje uživatele v síti, obsahuje informace o uživateli, jako je jméno, heslo, telefonní číslo a další
- **Skupina**: Objekt skupina (group) představuje skupinu uživatelů v síti, umožňuje spravovat oprávnění pro skupinu uživatelů najednou
- **Počítač**: Objekt počítač (computer) představuje počítač v síti, obsahuje informace o počítači, jako je jméno, operační systém a další
- **Tiskárna**: Objekt tiskárna (printer) představuje tiskárnu v síti, obsahuje informace o tiskárně, jako je jméno, typ tiskárny a další
- **Organizační jednotka**: Objekt organizační jednotka (Organizational Unit – OU) představuje logický adresář v síti, umožňuje organizovat objekty v síti do logických skupin a struktur
- **Další objekty**: Další typy objektů, které mohou být v doméně, jsou například kontakty, služby, aplikace nebo jiné specifické objekty vytvořené pro specifické potřeby (5)

1.4.3 Atributy

Atribut je informace o objektu, která je uložena v AD. Každý objekt v AD má několik atributů, které popisují různé aspekty objektu. Například uživatelský účet má atributy jako jméno, heslo, e-mailová adresa a další. Atributy objektů AD mohou být upravovány a spravovány pomocí nástrojů jako je Active Directory Users and Computers, Active Directory Administrative Center, nebo pomocí nástroje PowerShell. (5)



Attribute	Value
accountExpires	(never)
badPasswordTime	rope Dayli
badPwdCount	0
c	CZ
cn	Jakub Valný
co	Czech Republic
codePage	
company	
countryCode	
department	
description	
displayName	Jakub Valný
distinguishedName	CN=Jakub Valný,OU=Admins,OU=T2 User

Obrázek 1: Atributy objektu (vlastní)

1.4.5 Schéma

AD schéma je sada pravidel a definic, které určují, jaké objekty a atributy jsou v AD povoleny a jakým způsobem jsou mezi sebou propojeny. Schéma AD obsahuje řadu tříd objektů, které reprezentují různé typy objektů v AD, například uživatelské účty, skupiny, počítače a další. Každá třída objektu má svůj seznam atributů, které určují, jaké informace o objektu jsou v AD uloženy. Schéma také definuje vztahy mezi jednotlivými objekty. Například mezi objektem User a objektem Group existuje vztah "memberOf", který určuje, ve kterých skupinách je uživatel členem. Schéma AD může být upravováno pomocí nástrojů jako je Active Directory Schema snap-in v MMC (Microsoft Management Console) nebo pomocí nástroje PowerShell. (5)

1.4.6 FSMO role

FSMO (Flexible Single Master Operations) role jsou speciální role v AD, které jsou přiřazeny jednomu nebo několika doménovým řadičům v rámci stromu, nebo celého lesu. Tyto role zajišťují, že jednotlivé operace v rámci AD jsou koordinovány a řízeny, aby se zabránilo konfliktům a chybám. (5)

Existují následující FSMO role:

- **PDC Emulator** (Primary Domain Controller Emulator) – stará se o synchronizaci časových údajů a o řešení konfliktů hesla u uživatelů, kteří se přihlašují na starší verze operačních systémů

- **RID Master** (Relative ID Master) – řídí generování unikátních identifikátorů pro objekty v doméně
- **Infrastructure Master** – stará se o aktualizaci informací o objektech v doméně, když dochází ke změnám v jiných stromech v rámci lesa
- **Domain Naming Master** – řídí přidávání nebo odstraňování domén v rámci lesa
- **Schema Master** – řídí změny v AD schéma (5)

1.4.7 Globální katalog

Globální katalog (Global Catalog – GC) je distribuovaný adresářový systém používaný v AD. Jedná se o typ doménového řadiče, který uchovává repliku části informací z celého stromu AD. Jinými slovy je to centrální úložiště, které obsahuje vybrané informace o objektech z celého stromu či lesa. GC tedy uchovává kopie atributů uživatelů, skupin, počítačů a dalších objektů ze všech domén v celém AD lese, to umožňuje rychlé vyhledávání a přístup k informacím o objektech v celé síti bez nutnosti komunikace se vzdálenými doménovými řadiči. (2) (5)

1.5 Vztahy důvěry

Vztah důvěry mezi doménami je způsob, jakým se propojují dvě nebo více domén v AD, za účelem poskytnutí uživatelům v jedné doméně přístup k prostředkům v jiné doméně. (5)

1.5.1 Směr důvěry

Vztah důvěry může mít několik směrů:

- **Jednosměrná důvěra** – uživatelé v doméně A mohou přistupovat k prostředkům v doméně B, ale uživatelé v doméně B nemohou přistupovat k prostředkům v doméně A
- **Obousměrná důvěra** – uživatelé v obou doménách mohou přistupovat k prostředkům v obou doménách
- **Stromová důvěra** – speciální typ obousměrné důvěry, která propojuje domény ve stejném stromě, stromová důvěra umožňuje uživatelům v jedné doméně přistupovat k prostředkům v kterékoli doméně ve stejném stromě, bez ohledu na to, ve které doméně se nachází (5)

1.5.2 Možnosti průchodnosti

Vztah důvěry může mít nastaven několik typů průchodnosti:

- **Transitive** – umožňuje přístup uživatelům v jedné doméně ke zdrojům v jiné doméně, i když existuje řada dalších domén mezi nimi, vztah důvěry tedy není omezen na dvě přímo propojené domény, ale může se přenést na další domény
- **Non-transitive** – umožňuje přístup uživatelům v jedné doméně k zdrojům v jiné doméně, ale není přenositelný na další domény (5)

1.5.3 Typy vztahů důvěry

Vztahy důvěry rozdělujeme na několik typů:

- **Parent-child** – vztah důvěry mezi rodičovskou a podřízenou doménou, je vytvářen automaticky bez nutnosti manuálního nastavení. Jedná se o obousměrný tranzitivní vztah důvěry.
- **Tree-Root** – je obousměrný tranzitivní vztah důvěry podobný Parent-child. Při vytváření nového doménového stromu v rámci lesa je automaticky vytvořen vztah důvěry mezi kořenem stromu a všemi již existujícími doménovými stromy.
- **Forest Trust** – je tranzitivní vztah důvěry, který může být jednosměrný nebo obousměrný, vztah důvěry mezi dvěma lesy je vytvářen manuálně a záměrně, cílem je umožnit přístup k zdrojům mezi těmito lesy.
- **Shortcut Trust** – je ručně vytvářený jednosměrný, tranzitivní vztah důvěry. Mohou existovat pouze v rámci lesa. Tyto vztahy důvěry jsou vytvářeny za účelem optimalizace procesu ověřování a zkrácení cesty důvěry. Tyto důvěry jsou vytvářeny, když jedna doména potřebuje důvěřovat druhé doméně, aniž by se musela spoléhat na hierarchii.
- **External Trust** – jedná se o jednosměrný netranzitivní vztah důvěry. Tento vztah důvěry je vytvářen manuálně s externí doménou mimo les důvěřující domény
- **Realm Trust** – je vztah důvěry mezi doménou nebo lesem a jinou doménou nebo lesem, který není založen na Windows Active Directory, Realm Trust tedy umožňuje komunikaci mezi doménami různých platforem. Tento vztah důvěry je defaultně nastaven jako jednosměrný. Pro vytvoření obousměrného vztahu důvěry je nutné vytvořit trust i v opačném směru. (5)

1.5.4 Autentizace

Vztahy důvěry umožňují dva základní typy autentizace:

- **Domain-wide authentication** – je nastavení vztahu důvěry mezi doménami v prostředí AD, které umožňuje přístup k zdrojům v cílové doméně s použitím přihlašovacích údajů zdrojové domény, uživatelé zdrojové domény mohou přistupovat ke všem zdrojům v cílové doméně.
- **Selective authentication** – je nastavení vztahu důvěry mezi dvěma doménami, které umožňuje omezit přístup pouze na vybrané uživatele nebo skupiny uživatelů. Uživatelé z jedné domény nemají automaticky přístup k prostředkům v druhé doméně, každý uživatel nebo skupina uživatelů musí mít manuálně povolený přístup ke zdrojům v druhé doméně. (5)

1.6 Skupinové politiky

Skupinové politiky (Group Policy) je funkce operačního systému Windows, která umožňuje spravovat a konfigurovat různá nastavení počítačů v síti z centrálního umístění. Skupinové politiky jsou součástí AD a umožňují správcům nastavit politiky (Group Policy Object – GPO) pro různá omezení a nastavení vztahující se na skupiny uživatelů a počítačů. Skupinové politiky se používají k řízení bezpečnosti, konfiguraci systému, instalaci a aktualizaci softwaru, konfiguraci síťových připojení a mnoho dalšího. Skupinové politiky jsou uloženy na serveru a mohou být aplikovány na klienty, kteří jsou členem dané domény. (2) (5)

1.7 Fine-Grained Password Policy

Fine-Grained Password Policy (FGPP) je funkce v operačním systému Windows, která umožňuje správcům nastavit rozsáhlejší a podrobnější požadavky na hesla uživatelů v prostředí Active Directory. FGPP umožňuje správcům definovat více heslových politik v rámci jedné domény Active Directory a aplikovat je na různé skupiny uživatelů nebo jednotlivé uživatele podle potřeb organizace. (8)

1.8 DNS

DNS (Domain Name System) je decentralizovaný systém pro překlad doménových jmen na IP adresy. Jeho základní funkcí je tedy mapování doménového jména na odpovídající IP adresu, aby bylo možné efektivně komunikovat mezi počítači a dalšími síťovými zařízeními pomocí internetového protokolu IP. Mezi hlavní výhody používání doménových jmen patří lepší zapamatovatelnost, další výhodou je například možnost změny fyzického umístění počítače a jeho IP adresy a přesto zachovat stejné doménové jméno. DNS se využívá pro překlady doménových jmen na IP adresy v globálním prostoru internetu i v lokálních sítích, princip je stejný. AD využívá DNS pro několik doménových služeb. (2) (5)

1.8.1 Struktura

DNS funguje na základě hierarchické struktury, ve které jsou domény rozděleny na poddomény, které jsou dále rozděleny na další poddomény, tato struktura je známá jako strom DNS. Na vrcholu DNS stromu se nachází kořenové servery, které obsahují informace o nejvyšších úrovních domén (.com, .org a další), tyto servery odkazují na další servery, které obsahují informace o konkrétních doménách. (2) (5)

1.8.2 Princip

Princip DNS na jednoduchém příkladě zobrazení webové stránky v prohlížeči: Když zadáme název domény, například "microsoft.com", do adresního řádku webového prohlížeče, odešle se dotaz na DNS server, aby získal odpovídající IP adresu, na kterou se má připojit. Pokud DNS server zná odpověď, vrátí IP adresu, na kterou se má prohlížeč připojit. Prohlížeč se následně spojí s tímto serverem, aby získal požadovanou webovou stránku. Pokud DNS server nemá odpověď na daný dotaz, odešle dotaz na další server v hierarchické struktuře DNS, dokud není odpověď nalezena. (2) (5)

1.9 LDAP

LDAP (Lightweight Directory Access Protocol) je protokol pro přístup k adresářovým službám, který umožňuje vyhledávání, čtení a zápis informací v adresáři. LDAP byl vyvinut v roce 1993 a od té doby se stal standardem pro komunikaci se širokou škálou adresářových služeb, jako je například AD. LDAP definuje způsob, jak objekty reprezentovat, jak s nimi pracovat a jak s nimi komunikovat. LDAP umožňuje klientům připojit se k adresářové službě a provádět různé operace. (2) (5)

LDAP definuje základní operace pro práci s adresářovou službou, jako jsou:

- **Bind** – přihlášení k serveru pomocí uživatelského jména a hesla
- **Search** – vyhledávání informací v adresáři pomocí filtrování a hledání v hierarchické struktuře
- **Add** – přidání nového objektu do adresáře
- **Delete** – odstranění objektu z adresáře
- **Modify** – úprava existujícího objektu v adresáři (2) (5)

LDAP signing zajišťuje, že komunikace mezi klientem a serverem je podepsána a šifrována, snižuje se tak možnost úspěšně podvrhnout nebo upravit komunikaci. (8)

Channel binding zajišťuje, že klient a server komunikují pouze na již dříve ověřených kanálech, což minimalizuje riziko úspěšných útoků. (8)

1.10 Kerberos

Kerberos je bezpečnostní protokol, který se používá k ověřování identity uživatelů a klientů v síti. Jeho hlavním cílem je zajistit, aby se pouze ověření uživatelé mohli připojit k síťovým zdrojům a aby komunikace mezi klienty a servery byla zabezpečena před útoky třetích stran. Kerberos využívá symetrické kryptografie a používá tzv. "tickety" k ověření identity uživatele. (5) (8)

1.10.1 Princip protokolu Kerberos

Princip protokolu Kerberos je založen na třech základních krocích:

- **Autentizace klienta**: Klient se pokouší připojit k síťovému zdroji a posílá svou identitu autentizačnímu serveru, ten ověřuje identitu klienta pomocí uživatelského jména a hesla, nebo jiného ověřovacího mechanismu, pokud je ověření úspěšné, autentizační server vygeneruje tzv. ticket-granting ticket (TGT) a pošle ho klientovi.
- **Získání ticketu pro konkrétní službu**: Klient posílá TGT a svou identitu Ticket Granting Serveru (TGS), na který se chce připojit, TGS ověřuje TGT a když je ověření úspěšné, vygeneruje ticket pro konkrétní službu (tzv. service ticket) a zasílá ho klientovi.

- **Ověření identity pomocí ticketu**: Klient posílá service ticket a svou identitu serveru služby, na který se chce připojit, server služby ověřuje service ticket a pokud je ověření úspěšné, umožní klientovi připojit se k požadovanému síťovému zdroji. (5) (8)

Celý tento proces se odehrává v pozadí, klient se nemusí zabývat jednotlivými kroky, ale pouze posíláním své identity a získaných ticketů. (5) (8)

1.10.2 Kerberos Armoring

Kerberos Armoring zvyšuje bezpečnost při používání protokolu Kerberos tím, že zabezpečuje autentizaci a autorizaci při přenosu informací mezi klientem a serverem pomocí šifrování. (8)

1.10.3 KRBTGT

KRBTGT je výchozí účet služby Kerberos v operačním systému Windows. Tento účet se používá k zašifrování a ověřování přihlašovacích údajů v prostředí sítě Windows. KRBTGT účet je vytvářen při instalaci služby Active Directory a je zodpovědný za vytváření klíčů pro přenos autentizačních údajů. (5) (8)

1.11 SMB

Protokol SMB (Server Message Block) je komunikační protokol, který umožňuje sdílet soubory, tiskárny a další prostředky v síti mezi různými zařízeními, jako jsou například počítače, servery a tiskárny. Protokol SMB je založen na modelu klient-server, kde klient požaduje určitou akci nebo zdroj od serveru, který následně odpoví daty, které klient požadoval. Tyto požadavky a odpovědi jsou přenášeny v rámci tzv. SMB paketů, které jsou přenášeny pomocí síťového protokolu TCP/IP. (3) (8)

SMB podporuje různé funkce, jako jsou:

- Sdílení souborů a tiskáren mezi různými zařízeními v síti
- Zabezpečení přenosu dat pomocí šifrování a autentizace
- Možnost práce s různými typy souborů, včetně souborů s velkou kapacitou
- Možnost práce se zařízeními v síti a vzdálenou správu těchto zařízení (8)

V průběhu let byl protokol SMB aktualizován a vylepšen. Například verze SMB2 přinesla vylepšenou podporu pro velké soubory a lepší výkon při práci se soubory na síti. Verze SMB3 zase přinesla podporu pro šifrování přenosu dat, zlepšení výkonu a další vylepšení zabezpečení. (8)

1.11.1 SMB signing

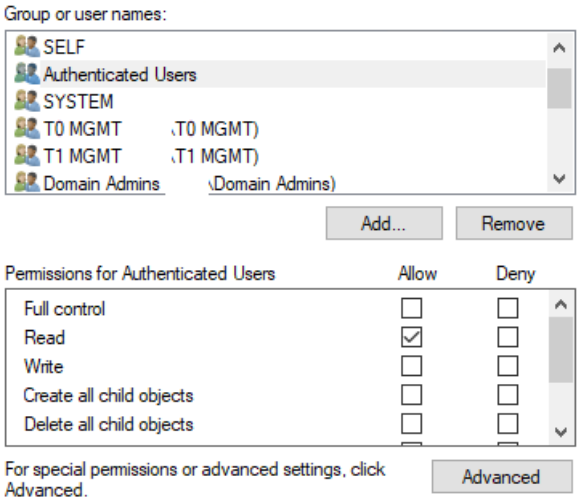
SMB signing je zabezpečovací mechanismus, který slouží ke kontrole integrity a autenticity dat přenášených mezi klientem a serverem v sítích. SMB signing zajišťuje, že data přenášená mezi klientem a serverem nejsou během přenosu modifikována a že jsou odesílána od důvěryhodného zdroje. Při použití SMB signing jsou data šifrována a podepsána digitálním certifikátem, což umožňuje ověřit, že data byla vyslána skutečným serverem a nebyla modifikována během přenosu. (5) (8)

1.12 LLMNR

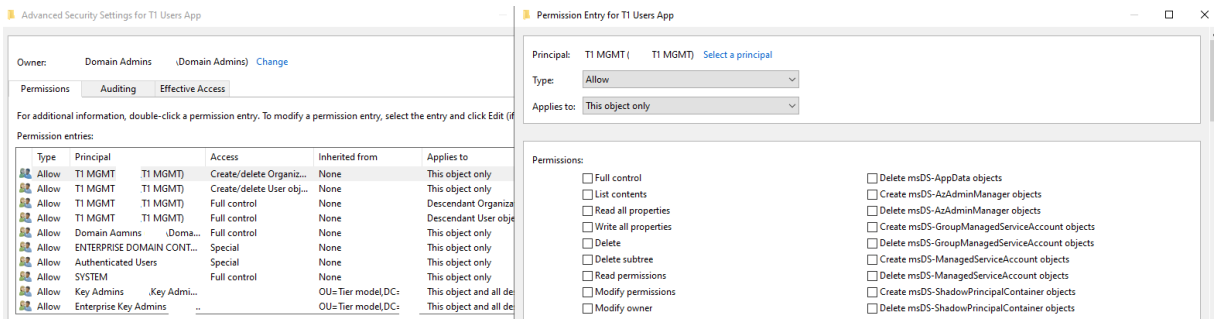
LLMNR (Link-Local Multicast Name Resolution) je síťový protokol, který slouží ke zjišťování síťových adres zařízení v lokální síti pomocí jména počítače. Když počítač potřebuje zjistit adresu jiného zařízení v lokální síti, zašle broadcast zprávu s dotazem na jméno daného zařízení, pokud se v síti nachází zařízení se stejným jménem, odpoví na tuto zprávu s vlastní IP adresou. (2)

1.13 Řízení oprávnění

AD používá pro správu oprávnění nad objekty ACL, stejně jako operační systém Windows. ACL v AD obsahuje seznam ACE, které definují oprávnění. Oprávnění v AD mohou být nastavena pro různé typy objektů, jako jsou uživatelé, skupiny, počítače, tiskárny, organizační jednoty a další. Například uživatelský účet může mít oprávnění pro přihlašování do domény, změnu vlastního hesla, nebo změnu informací o sobě v AD. Kromě nastavení oprávnění pro samotné objekty může být v AD také nastaveno dědění oprávnění, což umožňuje automatické předávání oprávnění z nadřazených objektů na podřízené. Tento princip umožňuje snadné spravování velkého počtu objektů v rámci domény. (3) (4)



Obrázek 2: Oprávnění nad objektem (vlastní)



Obrázek 3: Pokročilé nastavení oprávnění (vlastní)

1.13.1 ACL

ACL (Access Control List) je seznam práv přístupu pro určitý objekt (například soubor, složka, tiskárna, AD objekt a jiné), který umožňuje správci systému přidělit a řídit přístup uživatelů a skupin k tomuto objektu. ACL je v podstatě seznam s položkami, kde každá položka reprezentuje jednoho uživatele, skupinu, nebo roli a definuje práva, která mají přidělena pro daný objekt. Tyto práva mohou být například přístup k objektu, jeho editace, smazání nebo vytváření dalších objektů. (3) (4)

1.13.2 ACE

ACE (Access Control Entry) je základním prvkem ACL a reprezentuje jedno přidělené oprávnění pro uživatele, skupinu, nebo roli pro konkrétní objekt. ACE definuje, jaké konkrétní práva má uživatel, skupina nebo role k danému objektu a jak se tato práva aplikují. ACE může například určovat, zda uživatel má právo na čtení, zápis, spouštění, mazání nebo vytváření daného objektu. (3) (4)

Každý ACE se skládá ze tří hlavních částí:

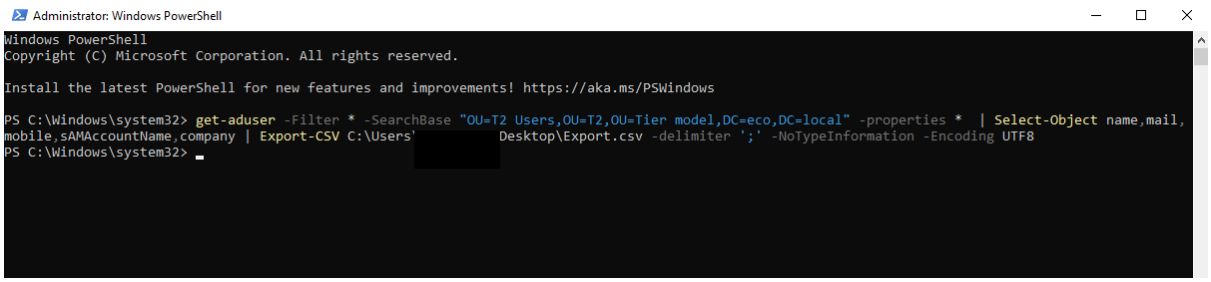
- **Identita** – určuje na kterého uživatele, skupinu nebo roli se toto oprávnění vztahuje
- **Typ oprávnění** – určuje, jaké právo je přiděleno, například čtení, zápis, spouštění, mazání nebo vytváření
- **Pravidlo aplikace** – určuje, jak se mají práva aplikovat, například zda se mají oprávnění dědit do podřízených objektů, nebo se mají aplikovat pouze na konkrétní objekt (3) (4)

1.14 Základní nástroje pro správu

V rámci prostředí Windows je k dispozici několik nástrojů pro správu.

1.14.1 PowerShell

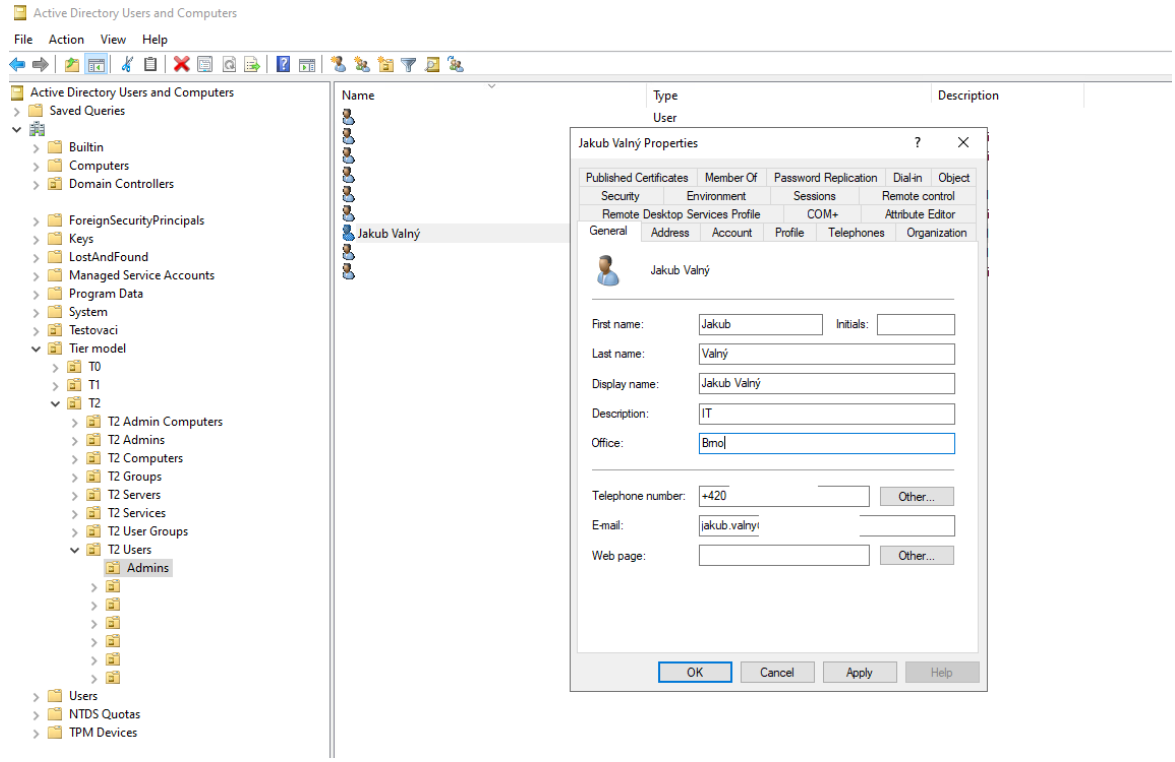
PowerShell je nástroj a skriptovací jazyk od společnosti Microsoft, který slouží k automatizaci úloh a správě systémů a aplikací v různých prostředích. PowerShell nabízí vysokou interaktivitu a flexibilitu při práci s daty a skripty. PowerShell obsahuje mnoho vestavěných příkazů, které slouží k práci s různými systémovými objekty, jako jsou soubory, registry, služby, uživatelé, skupiny a mnoho dalších. PowerShell nabízí také možnost práce s externími moduly, které umožňují rozšířit jeho funkce a zpřístupnit další příkazy pro specifické úkoly a aplikace. (4)



Obrázek 4: Příklad příkazu na export v nástroji PowerShell (vlastní)

1.14.2 Konzole Active Directory Users and Computers

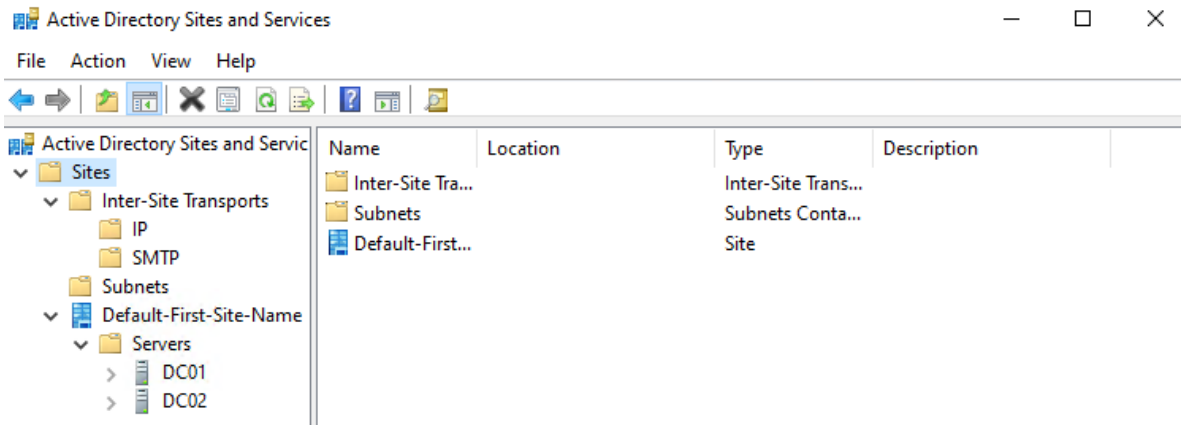
Konzole Active Directory Users and Computers (ADUC) je nástroj pro správu objektů v AD. V konzoli ADUC je možné vytvářet a upravovat uživatele, skupiny a počítače, měnit jejich vlastnosti, resetovat hesla, přidávat uživatele do skupin, měnit oprávnění a provádět další úkony týkající se správy. (4)



Obrázek 5: Konzole ADUC (vlastní)

1.14.3 Konzole Active Directory Sites and Services

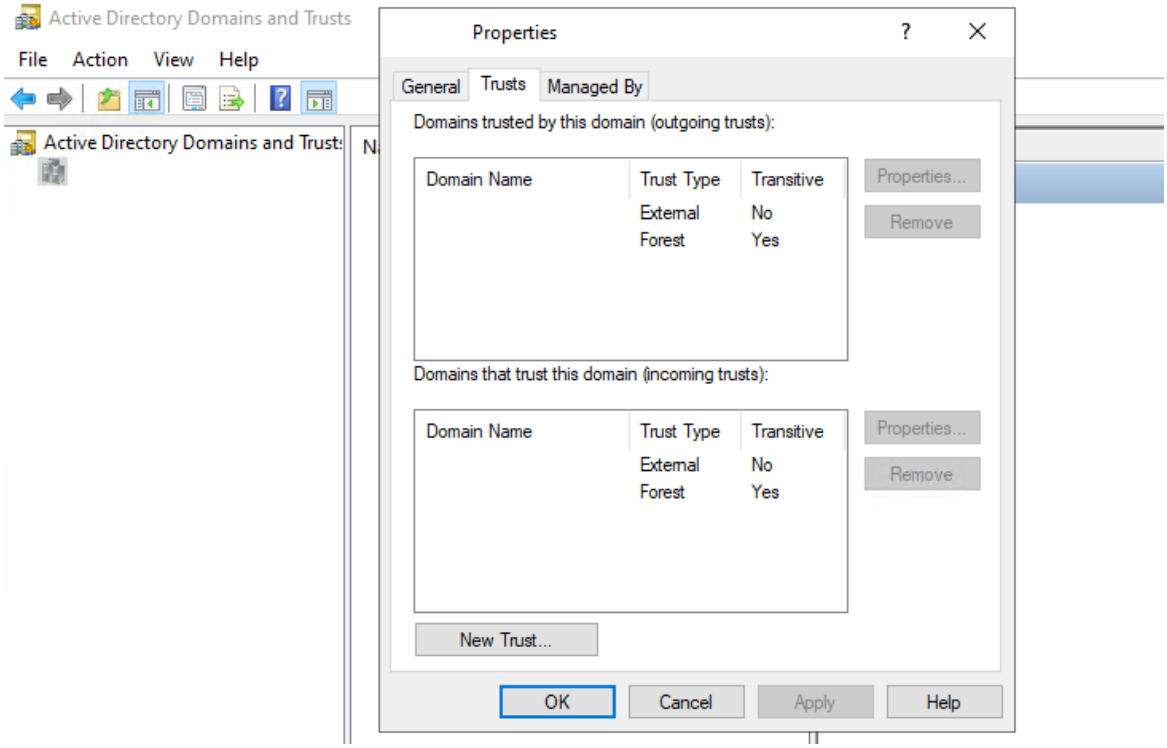
Konzole Active Directory Sites and Services (ADSS) je nástroj, který umožňuje spravovat a konfigurovat topologii sítě a umístění doménových řadičů. Tato konzole je nezbytná pro správu velkých a rozsáhlých sítí, které obsahují více doménových řadičů v různých lokalitách. Tato konzole také umožňuje spravovat replikace dat mezi doménovými řadiči v různých lokalitách a umožňuje řídit, jak se informace replikují. (4)



Obrázek 6: Konzole ADSS (vlastní)

1.14.4 Konzole Active Directory Domains and Trusts

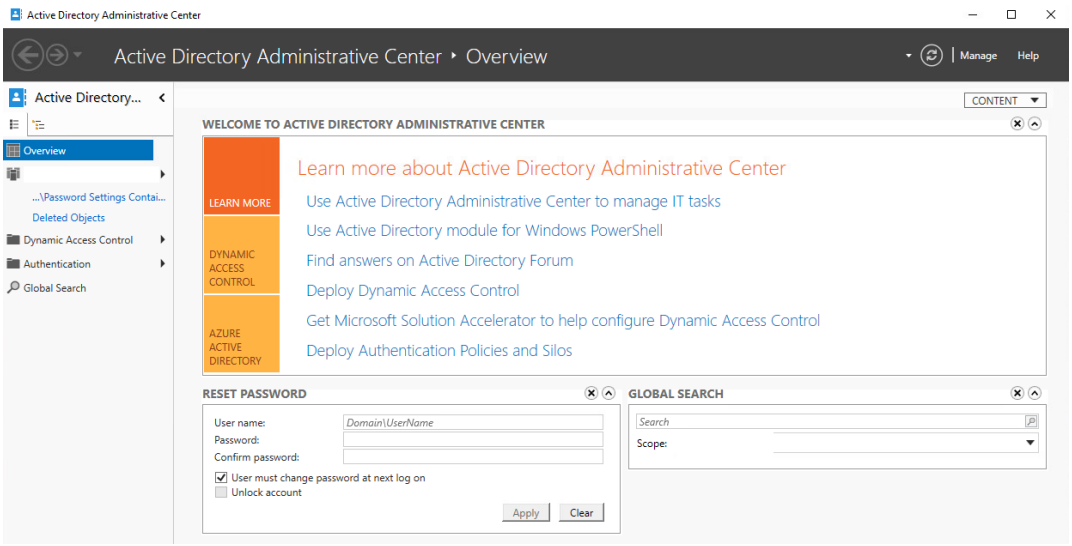
Konzole Active Directory Domains and Trusts (ADDT) je konzole, která umožňuje spravovat vlastní domény a především vztahy důvěry mezi různými doménami. Konzole ADDT umožňuje řídit, jak jsou vztahy důvěry mezi doménami a stromy vytvářeny a spravovány. Zahrnuje například nastavení úrovně důvěry, způsob autentizace a řízení oprávnění. ADDT umožňuje také správu vlastní domény, včetně správy globálních katalogů, zón DNS, řízení funkcí a další. (4)



Obrázek 7: Konzole ADDT (vlastní)

1.14.5 Konzole Active Directory Administrative Center

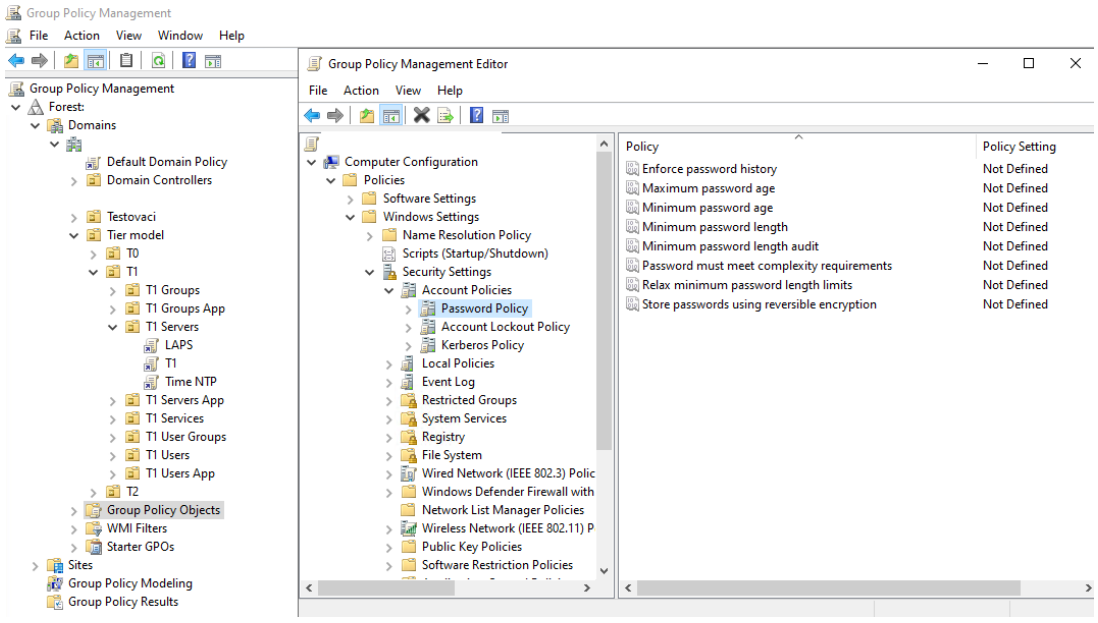
Konzole Active Directory Administrative Center (ADAC) je konzole pro správu a řízení prostředí AD, která umožňuje správu všech funkcí AD z jednoho místa. Konzole ADAC kombinuje funkce nástrojů, jako jsou například ADUC a ADSS. Konzole ADAC poskytuje tedy mnoho funkcí, mezi které patří například správa uživatelů a skupin, správa počítačů, správa zabezpečení, správa certifikátů a správa zdrojů. Konzole ADAC poskytuje různé filtry a vyhledávání pro snadnou správu a řízení AD a umožňuje vytvářet vlastní úkoly pro automatizaci správy. (4)



Obrázek 8: Konzole ADAC (vlastní)

1.14.6 Group Policy Management

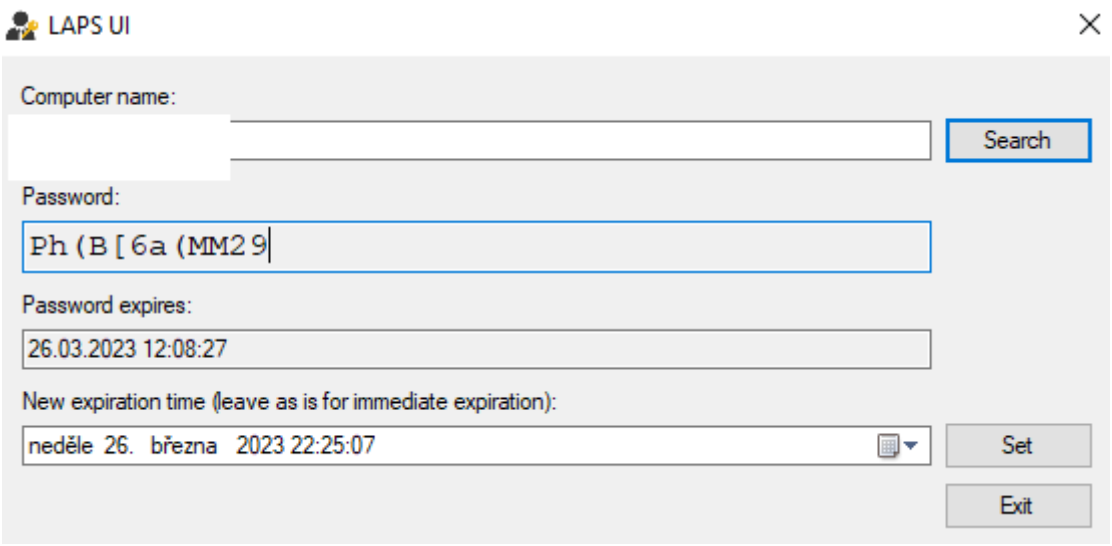
Konzole Group Policy Management (GPMC) je nástroj, který umožňuje centrální správu a konfiguraci skupinových politik v prostředí AD. GPMC umožňuje správcům centralizovat správu skupinových politik, což umožňuje rychle a efektivně provádět změny v politikách v celé organizaci. GPMC poskytuje nástroje pro vytváření, upravování, správu, audit, zobrazování, zálohování a propojování skupinových politik. V jednotlivých skupinových politikách můžeme pro počítače a uživatele v síti nastavovat různé faktory týkající se například bezpečnosti, aplikací, preferencí a další nastavení. (8)



Obrázek 9: Konzole GPMC (vlastní)

1.15 LAPS

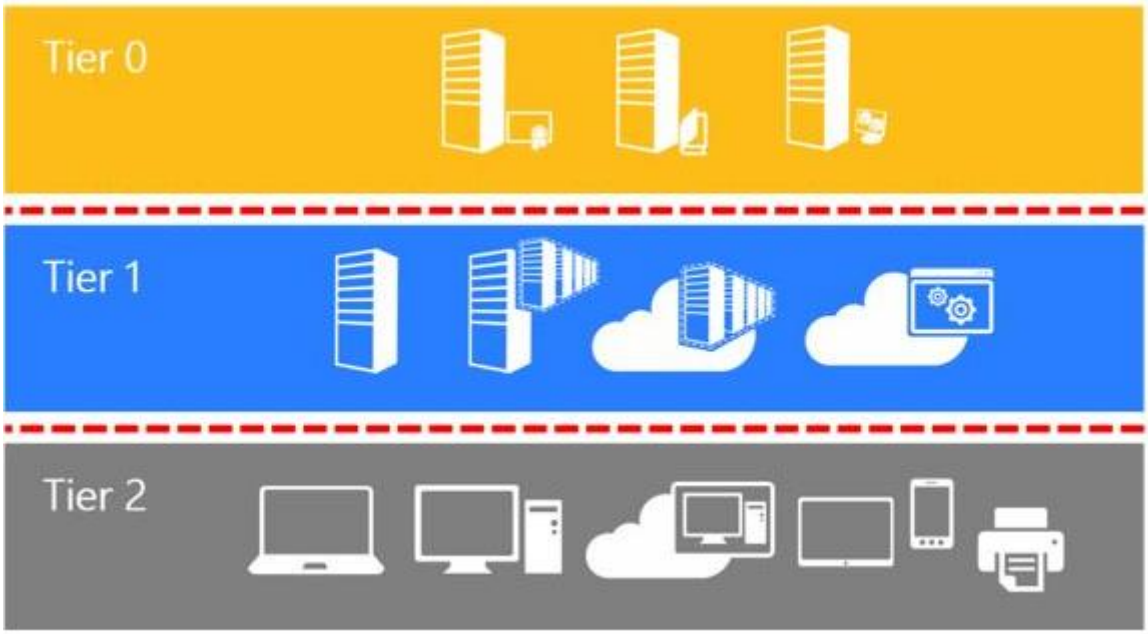
Nástroj LAPS (Local Admin Password Solution) je bezplatný doplněk od společnosti Microsoft, který umožňuje centrální správu a rotaci hesel účtů lokálních správců na počítačích v rámci AD domény. Lokální správce je lokální účet s administrátorským oprávněním, který je při instalaci operačního systému vytvořen na každém počítači. Tyto účty mohou představovat velké bezpečnostní riziko, pokud se jejich hesla dostanou mimo oprávněné osoby, jsou používána opakovaně, nebo jsou příliš slabá. LAPS řeší tento problém tím, že každý počítač v doméně má jedinečné heslo pro lokálního správce, které je generováno a uloženo do zabezpečeného umístění v AD. LAPS umožňuje rotovat hesla pro lokální správce na počítačích v určených intervalech, což zvyšuje bezpečnost sítě. Správci IT mohou přistupovat k heslům pomocí nástroje LAPS UI, který umožňuje vyhledávání hesel pro konkrétní počítač a hledání počítačů, které používají určité heslo. (8)



Obrázek 10: Heslo v nástroji LAPS (vlastní)

1.16 Tier Model

Jedná se o vrstvený model vytvořený pomocí základních administrativních nástrojů a prvků AD, který si klade za cíl lépe zabezpečit prostředí. Model definuje tři úrovně, které vytvářejí vertikální sadu zón pro oddělení aktiv podle jejich důležitosti. V rámci jednotlivých úrovní lze dělit aktiva horizontálně do dalších zón, které umožňuje ještě větší diverzifikaci. (8)



Obrázek 11: Úrovně Tier Modelu (8)

1.16.1 Definice úrovně 0

Úroveň 0 (Tier 0 - T0) je nejvyšší úrovní a zahrnuje nejkritičtější aktiva jakými jsou například doménové řadiče a certifikační autority. T0 zahrnuje účty a skupiny, které mají přímou nebo nepřímou kontrolu nad AD lesem, doménami nebo doménovými řadiči. Správci T0 mohou spravovat a ovládat aktiva na všech úrovních, interaktivně se však mohou přihlásit pouze k aktivům T0. (8)

1.16.2 Definice úrovně 1

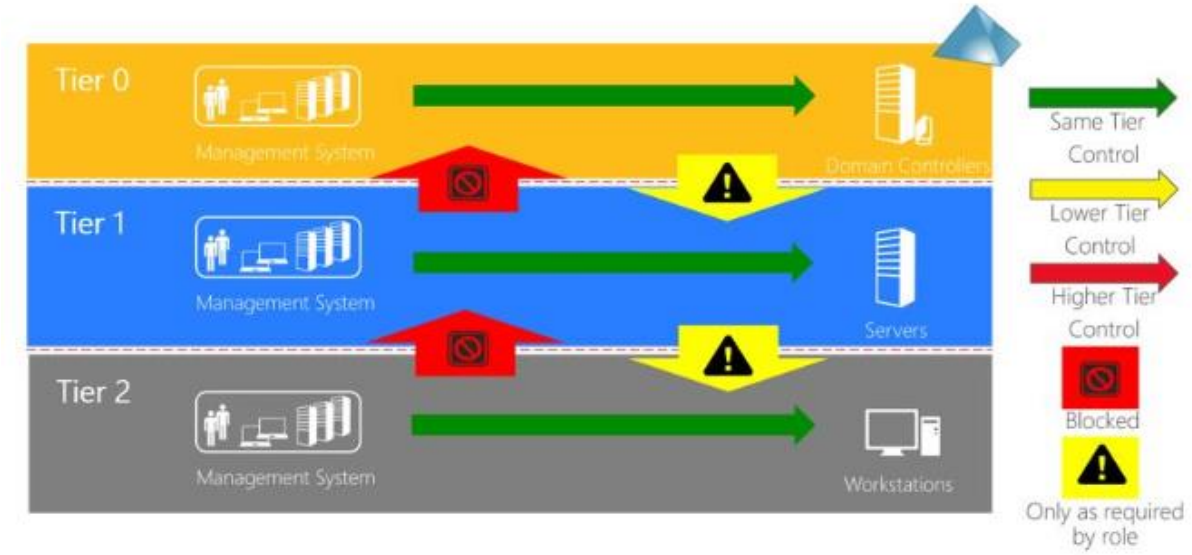
Úroveň 1 (Tier 1 - T1) zahrnuje převážně servery na kterých jsou provozovány aplikace, systémy a služby organizace. Účty v T1 mají přístup k citlivým datům organizace. Správci T1 mohou spravovat aktiva T1 a T2, interaktivně se však mohou přihlásit pouze k aktivům T1. (8)

1.16.3 Definice úrovně 2

Úroveň 2 (Tier 2 - T2) zahrnuje stanice na které přistupují koncoví uživatelé, jedná se například o počítače, notebooky a terminálové servery. T2 také zahrnuje samotné uživatelské účty a skupiny. Správci T2 se mohou interaktivně přihlásit k aktivům T2 a spravovat je. (8)

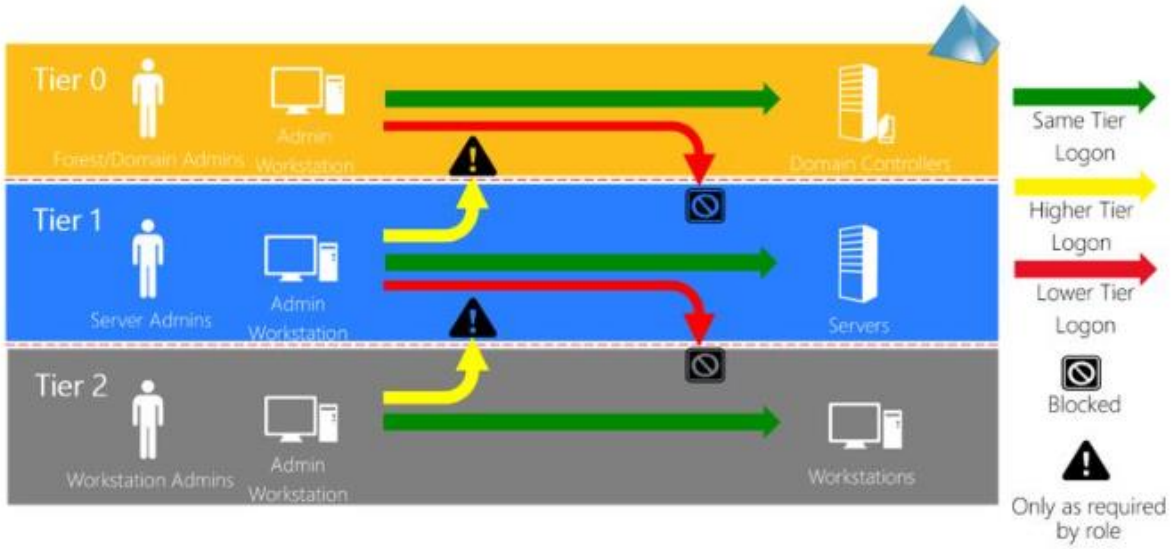
1.16.4 Restrikce a oprávnění

Následující obrázek znázorňuje restrikce mezi jednotlivými vrstvami modelu z hlediska oprávnění nad objekty. (8)



Obrázek 12: Restrikce oprávnění v Tier Modelu (8)

Následující obrázek znázorňuje oprávnění přihlášení k aktivům v rámci jednotlivých vrstev modelu. Interaktivně je možné se účtem z dané úrovně přihlásit pouze v rámci dané úrovně. Přihlašování v rámci úrovní směrem dolů je kompletně zablokováno převážně z důvodu možného odposlechnutí účtu vyšší úrovně na rizikovějším aktivu nižší úrovně. Přihlášení v rámci úrovní směrem nahoru je povoleno pouze pokud to vyžaduje role. (8)



Obrázek 13: Restrikce přihlášení v Tier Modelu (8)

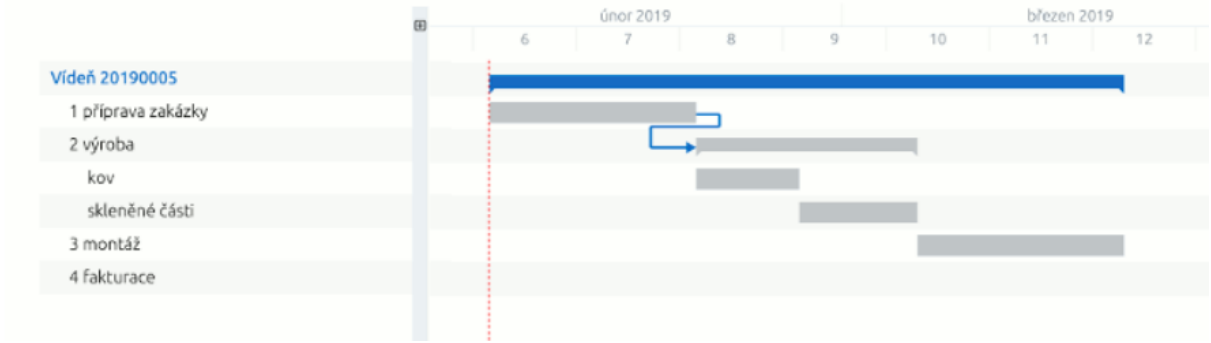
1.16.5 Princip

Konstrukce Tier modelu se skládá ze tří základních prvků, kterými jsou organizační jednotky, skupiny a skupinové politiky. Pomocí skupin se v jednotlivých úrovních modelu rozdělují účty podle jejich účelu, například se mohou dělit na uživatelské, správcovské a další. Jednotlivé skupiny se používají pro řízení všech oprávnění v modelu.

Tier model má hierarchicky uspořádanou strukturu organizačních jednotek, které mají speciálně upravené zabezpečení. Toto zabezpečení definuje oprávnění nad objekty umístěnými v daných organizačních jednotkách. Právě upravené zabezpečení organizačních jednotek rozděluje model do pomyslných úrovní z hlediska oprávnění v AD. Posledním prvkem modelu jsou skupinové politiky, které definují různá oprávnění na stanicích a serverech v jednotlivých úrovních modelu. Jejich úkolem je především zamezení přístupu účtů jiných vrstev v rámci dané vrstvy. (8)

1.17 Ganttův diagram

Ganttův diagram je grafický nástroj pro plánování a řízení projektů, který obsahuje časovou osu, na které jsou znázorněny činnosti projektu. Každá činnost je v Ganttově diagramu znázorněna jako vodorovná čára, která začíná v okamžiku, kdy začíná daný úkol, a končí v okamžiku, kdy je dokončen. Časová osa může být rozdělena do dnů, týdnů nebo měsíců, a umožňuje vizualizovat plánovaný průběh projektu. Ganttův diagram umožňuje sledovat průběh projektu a porovnávat plánovaný čas s aktuálním průběhem. Ganttův diagram zobrazuje nejen jednotlivé činnosti, ale také jejich vzájemné závislosti. Tyto závislosti mohou být zobrazeny pomocí šipek, které spojují jednotlivé činnosti. (9)



Obrázek 14: Ganttův diagram (11)

1.18 Návratnost investice do zabezpečení

Návratnost investice do zabezpečení (Return On Security Investment – ROSI) je metodika, která se používá k měření efektivity investic do bezpečnosti. Cílem metodiky je vyčíslit, zda jsou investice do bezpečnosti výhodné z finančního hlediska a zda poskytují přidanou hodnotu pro organizaci. ROSI spočívá v porovnání nákladů na bezpečnostní opatření s potenciálními úsporami z minimalizace rizik a škod způsobených bezpečnostními incidenty. ROSI vyjadřuje poměr návratnosti vynaložených nákladů na snížení rizika (10)

1.18.1 Jednotková očekávaná ztráta

Jednotková očekávaná ztráta (Single Loss Expectancy – SLE) vyjadřuje očekávaný finanční objem ztráty, v případě, že se zrealizuje určité bezpečnostní riziko. V kalkulaci by měly být zahrnuty všechny faktory, které mají vliv na konečnou cenu ztráty. (10)

1.18.2 Roční míra výskytu

Roční míra výskytů (Annual Rate of Occurrence – ARO) představuje pravděpodobnosti, že se dané riziko zrealizuje v období jednoho roku. (10)

1.18.3 Roční očekávaná ztráta

Roční očekávaná ztráta (Annual Loss Expectancy – ALE) se počítá z předchozích dvou hodnot. (10)

$$ALE = SLE \times ARO$$

1.18.4 Redukce rizika

Redukce rizika (Mitigation Ratio, MR) vyjadřuje, o jaký relativní poměr dokáže dané opatření snížit nebezpečí dopadu rizika. (10)

1.18.5 Finančně vyjádřená redukce ztráty

Finančně vyjádřená redukce ztráty (Monetary Loss Reduction, MLR) vyjadřuje o kolik zavedená opatření snižují potenciální ztráty. (10)

$$MLR = ALE \times MR$$

1.18.6 Výpočet ROSI

Výpočet ROSI zahrnuje finančně vyjádřenou redukci ztráty a náklady na opatření.

$$\text{ROSI} = \frac{\text{Finančně vyjádřená redukce ztráty} - \text{Náklady na opatření}}{\text{Náklady na opatření}}$$

Výsledek je kvalifikovaný odhad, je možné ho dále zpřesňovat úpravami vstupních hodnot. Je důležité si uvědomit, že ROSI tedy není dokonalým měřítkem a může být ovlivněn různými faktory, jako jsou například stanovaní nákladů a úspor, nebo neustálé změny v prostředí bezpečnosti. (10)

2 Analýza současného stavu

V této části diplomové práce uvedu základní informace o instituci a následně popíšu současný stav domény a bezpečnostních politik. Dále se budu zabývat rozborem požadavků mateřské společnosti a dalšími body, které s nimi souvisí.

2.1 Základní informace o instituci

Společnost, pro kterou budu zpracovávat tuto práci, budu držet ze smluvních důvodů v anonymitě. Nebudu zde uvádět ani odvětví podnikání, protože je velmi specifické a působí v něm velmi málo firem. Vzhledem k dominantnímu postavení a velikosti této firmy v České republice by byla snadno odhalitelná.

Společnost má několik desítek provozů a kanceláří rozesetých po celé České republice. Ve firmě je přibližně 400 digitálně aktivních uživatelů, kteří obsluhují přibližně 600 koncových stanic. Společnost působí v České republice již několik desetiletí a v minulosti si prošla několikrát změnou názvu a také jednou akvizicí, při které byla celá odkoupena zahraniční korporátní společností. Nyní si prošla druhou akvizicí a další změnou názvu, protože byla znovu odkoupena ještě větší zahraniční korporátní společností.

Změna názvu společnosti byla nutná, protože název obsahoval jméno bývalé mateřské společnosti. Společnost vlastnila několik domén s jmény bývalých názvů firmy. Všechny tyto domény musely být odevzdány bývalé mateřské společnosti, protože spadaly do jejího duševního vlastnictví. Mezi tyto domény patřila i lokální doména anonymizované společnosti. Z důvodu odevzdání všech těchto domén proběhl projekt migrace domén, ve kterém byly přemigrovány do nově vytvořené domény všechny potřebné prvky.

2.2 Současný stav

Výchozím stavem této práce je nově vybudovaná doména, do které byly přemigrovány všechny stanice, servery, skupiny a uživatelské účty pomocí nástroje Microsoft Active Directory Migration Tool. Aktuálně se jedná o jedinou doménu jediného stromu, která nemá žádné vztahy důvěry s jinou doménou. V doméně se nachází dva doménové řadiče, primární a sekundární. Doménové řadiče mají verzi Windows Server 2022, Forest Function Level domény a Domain Function Level domény je na úrovni Windows 2016.

Všechny objekty v doméně jsou umístěny v jedné OU, v rámci této OU jsou v dalších rozděleny na skupiny, účty uživatelů, objekty serverů a objekty stanic. Žádná z těchto OU nemá nijak upravené oprávnění.

2.2.1 Skupinové politiky

V současné době se v doméně, kromě základních automaticky vytvořených politik, nachází malé množství skupinových politik. Všechny vytvořené politiky mají za úkol pouze zajištění funkčnosti různých systémů, distribuci odkazů a úpravu vizuální stránky prostředí. Jsou zde tedy například skupinové politiky na distribuci záložek v prohlížeči, úpravu důvěrných webů a kořenových certifikačních autorit, nebo zamykací obrazovku s různými texty. Žádná z těchto skupinových politik nijak neupravuje oprávnění ani nezvyšuje úroveň zabezpečení.

2.2.2 Politika hesel doménových účtů

Aktuálně je nastavení hesel všech účtů v doméně řízeno pouze prostřednictvím defaultní doménové politiky, účty tedy nejsou žádným způsobem rozděleny a na všechny se vztahuje stejné nastavení. Minimální požadovaná délka hesla je pouze 8 znaků a nevyžaduje použití speciálních znaků. Doba platnosti hesla je nastavena na 90 dní, při změně hesla se heslo nesmí opakovat a musí být odlišné od 20 posledních použitých hesel. Několik účtů má zvolenou možnost Password never expires.

2.2.3 Lokální správci

Všechny uživatelské stanice mají jeden účet lokálního správce, heslo tohoto účtů je stejné na všech stanicích a znají ho pouze správci v rámci IT oddělení. Všechny servery mají také jeden účet lokálního správce, heslo tohoto účtů je stejné na všech serverech. Heslo pro účet lokálního správce na serverech je odlišné od hesla na uživatelské stanice. Toto heslo zná jen vybraná skupina správců v rámci IT oddělení. Lokální správce se používá ve většině případů pouze kvůli operacím vyžadujícím zvýšená oprávnění, například tedy instalacím aplikací.

2.2.4 Administrátorská oprávnění v doméně

V doméně není zavedena žádná struktura ani systém v řízení oprávnění na stanicích a serverech, stejně jako v řízení oprávnění nad objekty v AD. Z tohoto důvodu účet s administrátorským oprávněním v doméně mají všichni správci IT včetně prvotní podpory. Dále z tohoto důvodu mají administrátorské oprávnění v doméně také někteří externisti, kteří přistupují do vnitřní sítě za účelem správy dodávaných systémů. Nakonec bych zde chtěl zmínit, že administrátorské oprávnění v doméně mají dokonce i některé servisní účty systémů. Tyto účty se používají na všech zařízení včetně uživatelských stanic. Riziko odposlechnutí a zneužití administrátorských oprávnění je extrémně vysoké.

2.2.5 Přístup k Active Directory

Aktuálně se k AD za účelem správy účtů a dalších objektů přistupuje pouze skrze doménový řadič. Na doménový řadič se přistupuje standardně prostřednictvím vzdálené plochy, k připojení a následně i ke správě se používá doménový administrátor. Zde bych chtěl znovu zmínit, že takto přistupuje k AD i prvotní podpora.

2.2.6 Opatření proti hrozbám

Aktuálně v doméně není zavedeno žádné opatření proti známým hrozbám. Nejsou tedy například zakázány žádné rizikové protokoly, ani není upravena konfigurace.

2.3 Požadavky mateřské společnosti

V této části práce se zaměřím na požadavky mateřské společnosti. Mateřská společnost provádí akvizice relativně pravidelně, takže pro ni není žádnou novinkou a má již osvědčený postup i jasně daný seznam požadavků.

2.3.1 Forest a Domain Functional Level

Mateřská společnost požaduje, aby Forest Function Level domény byl minimálně na úrovni Windows 2012 R2 ideálně však na 2016. Dále požaduje, aby Domain Function Level domény byl minimálně na úrovni Windows 2012 R2 ideálně však na 2016. Díky nově vybudované doméně tyto požadavky dceřiná společnost splňuje a nebudou zahrnuty v návrhu.

2.3.2 Active Directory Tier Model

Mateřská společnost požaduje, aby ve všech doménách společností, které vlastní byl implementován Active Directory Tier Model ve všech vrstvách dle definované politiky. Specifikace Tier modelu mateřské společnosti jsou rozebrány v předposlední podkapitole analýzy současného stavu. V rámci tohoto bodu požaduje také izolaci doménových řadičů.

2.3.3 Password policy

Politika hesel mateřské společnosti rozděluje účty do několika skupin, požadovaná obtížnost se stupňuje s oprávněním a důležitostí účtu. Konkrétní požadované nastavení popisují tabulky níže. Nastavení v druhé tabulce již počítá s vytvořeným Tier Modelem.

Tabulka 1: Defaultní politika hesel (vlastní)

Název	Délka hesla	Maximální stáří hesla	Pokusů do uzamčení	Doba resetu	Doba zamčení
Default Policy	12	180	10	15	15

Tabulka 2: Speciální politiky hesel (vlastní)

Název	Délka hesla	Preference	Maximální stáří hesla	Pokusů do uzamčení	Doba resetu	Doba zamčení	Skupiny
T2 ADM Password Policy	15	9	180	10	15	15	T2 ADM, T2 AD TECH, T2 ADM VIP
T1 Password Policy	15	7	180	10	15	15	T1 All Accounts
T0 ADM Password Policy	16	5	180	10	30	30	Domain Admins, T0 All Accounts
SVC Password Policy	20	3	365	5	30	30	T0 All SVC, T1 All SVC, T2 SVC

2.3.4 Konfigurace protokolů a služeb

Mateřská společnost požaduje v rámci zvýšení zabezpečení pracovních stanic, serverů a doménových řadičů provést několik změn v nastavení protokolů a služeb.

- **Mitigace SMB –** Mateřská společnost požaduje několik úprav v nastavení a používání protokolu SMB za účelem eliminace zranitelností. V rámci tohoto bodu požaduje:
  - Vypnutí SMBv1
  - Vypnutí komprese v SMBv3
  - SMB Signing
- **Vypnutí LLMNR –** Mateřská společnost požaduje vypnutí LLMNR za účelem eliminace potenciálních hrozeb spojenými převážně s útoky typu name poisoning a man-in-the-middle.

- **LDAP signing a Channel binding –** Mateřská společnost požaduje využívat LDAP signing a channel binding za účelem zvýšení bezpečnosti při komunikaci s AD. Cílem je minimalizace rizika man-in-the-middle útoků.
- **Kerberos Armoring –** Mateřská společnost požaduje využívat Kerberos Armoring na všech stanicích, které ho podporují. Cílem je minimalizovat riziko útoků spojenými s protokolem Kerberos typu pass the ticket a pass the hash.
- **Vypnutí služby Print Spooler na doménových řadičích –** Mateřská společnost požaduje vypnout službu Print Spooler na doménových řadičích.

2.3.5 Propojení domén

Mateřská společnosti požaduje napojení všech domén společností, které vlastní na svou hlavní doménu za účelem poskytování aplikací a služeb společně s implementací systémů a monitorovacích systémů. K vytvoření důvěrnosti mezi doménami požaduje použít obousměrný selektivní vztah důvěry.

2.3.6 LAPS

Mateřská společnost požaduje nasazení nástroje Local Administrator Password Solution na všech koncových stanicích a serverech. V nastavení nástroje požaduje platnost hesla 30 dní a délku 12 znaků s použitím velkých a malých písmen, číslic i znaků.

2.4 Technická specifikace a pravidla Tier Modelu mateřské společnosti

V následující části rozeberu technické specifikace a pravila Tier Modelu definované mateřskou společností.

2.4.1 Úroveň 0

Jedná se o vrstvu obsahující nejkritičtější aktiva. Přístup k této vrstvě by měl mít omezený počet administrátorů. **Složení a účel OU v T0 je následující:**

- **T0 Groups** – Základních skupiny T0, pomocí kterých se řídí oprávnění
- **T0 Servers** – Počítačové objekty v T0
- **T0 Groups App** – V podřízených OU jsou skupiny pro řízení oprávnění v nasazených aplikacích
- **T0 Servers App** – V podřízených OU jsou počítačové objekty nasazených aplikací
- **T0 Services** – Servisních účty, které se používají pro chod služeb a spouštění úloh

- **T0 Users** – Účty uživatelů v T0
- **T0 User Groups** – Umístění skupin, které přímo souvisí s T0, ale nesouvisí s chodem Tier modelu
- **T0 Users App** – V podřízených OU jsou účty uživatelů spojené s danou nasazenou aplikací

Složení a účel skupin v T0 je následující:

- **T0 ADM** – Skupina uživatelů, kteří mají práva lokálního administrátora na serverech
- **T0 SVC** – Skupina servisních účtů, které mohou být použity pro spuštění služeb a úloh
- **T0 SVC ADM** – Skupina servisních účtů, které mají práva lokálního administrátora, účty musí být zároveň obsaženy i ve skupině T0 SVC, protože ta zajišťuje oprávnění pro spuštění služeb a úloh
- **T0 USR** – Skupina uživatelů, kteří mají právo interaktivního přihlášení přes RDP na servery T0, ale nemají administrátorské oprávnění
- **T0 SVC Trust** – V případě potřeby použít účet z důvěryhodné domény
- **T0 SVC ADM Trust** – V případě potřeby použít účet z důvěryhodné domény
- **T0 All Accounts** – Do této skupiny se agregují všechny účty z vrstvy T0. Členy jsou skupiny T0 ADM, T0 SVC, T0 USR z OU T0 Groups a také ze všech nasazených aplikací v rámci T0 Groups App
- **T0 ALL SVC** – Skupina všech servisních účtů v T0. Narozdíl od T0 SVC jsou v ní i účty ze všech T0 Groups App servisních skupin
- **T0 MGMT** – Členové této skupiny mají právo vytvářet a spravovat objekty v celém Tier Modelu

2.4.2 Úroveň 1

Jedná se o vrstvu obsahující podnikové aplikace a systémy. Složení a účel organizačních jednotek vrstvy 1 je stejné jako u vrstvy 0. Složení a účel skupin vrstvy 1 je až na skupinu T1 MGMT také stejný jako u vrstvy 0. Členové skupiny T1 MGMT mohou spravovat pouze objekty v T1 a T2, nemohou také spravovat strukturu těchto úrovní.

2.4.3 Úroveň 2

Jedná se o nejrizikovější vrstvu obsahující koncové uživatele a jejich stanice.

Složení a účel OU v T2 je následující:

- **T2 Groups** – Základní skupiny T2, pomocí kterých se řídí oprávnění
- **T2 Servers** – Počítačové objekty serverů v T2
- **T2 Computers** – Počítačové objekty uživatelských stanic
- **T2 Admin Computers** – Počítačové objekty stanic správců IT
- **T2 Services** – Servisních účty, které se používají pro chod služeb a spouštění úloh
- **T2 Users** – Uživatelské účty
- **T2 User Groups** – Skupiny, které přímo souvisí s T2, ale nesouvisí s chodem Tier modelu
- **T2 Admin** – Umístění administrátorských účtů v T2

Složení a účel skupin v T2 je následující:

- **T2 ADM** – Skupina uživatelů, kteří mají práva lokálního administrátora na koncových uživatelských stanicích a serverech v T2
- **T2 SVC** – Skupina servisních účtů, které mohou být použity pro spuštění služeb a úloh
- **T2 SVC ADM** – Skupina servisních účtů, které mají práva lokálního administrátora. účty musí být zároveň obsaženy i ve skupině T2 SVC, protože ta zajišťuje oprávnění pro spuštění služeb a úloh
- **T2 IT USR** – Skupina pro uživatelské účty správců IT
- **T2 SVC Trust** – V případě potřeby použít účet z důvěryhodné domény
- **T2 SVC ADM Trust** – V případě potřeby použít účet z důvěryhodné domény
- **T2 All Accounts** – Do této skupiny se agregují všechny účty z vrstvy T2. Členy jsou skupiny T2 ADM, T2 SVC a T2 IT USR
- **T2 MGMT** – Členové této skupiny mají právo vytvářet a spravovat objekty v rámci T2, kromě OU T2 Admin Computer a T2 Groups

V T2 jsou následující pravidla:

- Administrátoři na svých stanicích používají pro operace vyžadující zvýšená oprávnění vlastního lokálního administrátora
- Žádný účet kromě účtu lokálního administrátora nemá administrátorské oprávnění na stanicích správců IT

- Správci IT se svými běžnými uživatelskými účty nemohou přihlásit na žádné uživatelské stanici

2.4.4 Aplikace

Mateřská společnost doporučuje T0 a T1 dělit horizontálně, například dle služeb, nebo systémů. Obzvlášť v T1 se obvykle nachází velké množství systémů a je vhodné omezit přístupy na menší skupinu uživatelů. Díky tomuto rozdělení můžeme lépe udělovat přístup lokálním uživatelům, nebo externím dodavatelům. K tomuto účelu slouží OU Tx Groups App, Tx Servers App a Tx Users App. V těchto OU se vytváří OU pro jednotlivé aplikace. Každá aplikace má svou vlastní strukturu skupin, která řídí oprávnění, podobně jak je tomu u základních skupin nějaké z úrovní.

- **Tx ADM název_aplikace** – Skupina uživatelů, kteří mají práva lokálního administrátora na serverech v dané aplikaci
- **Tx SVC název_aplikace** – Skupina servisních účtů, které mohou být použity pro spuštění služeb a úloh v rámci dané aplikace, tato skupina musí být členem Tx All SVC
- **Tx SVC ADM název_aplikace** – Skupina servisních účtů, které mají práva lokálního administrátora na serverech v dané aplikaci, účty musí být zároveň obsaženy i ve skupině Tx SVC název_aplikace, protože ta zajišťuje oprávnění pro spuštění služeb a úloh
- **Tx USR název_aplikace** – Skupina uživatelů, kteří mají právo interaktivního přihlášení přes RDP na servery v dané aplikaci, ale nemají administrátorské oprávnění
- **Tx All Accounts název_aplikace** – Do této skupiny se agregují všechny účty z dané aplikace, členové musí být skupiny Tx ADM JménoApp, Tx SVC JménoApp, Tx USR JménoApp. Skupina musí být členem sk. Tx All Accounts

2.4.5 Jmenná konvence

Kromě uživatelských a servisních účtů musí všechny účty dodržovat následující jmennou konvenci. Písmeno X v jmenné konvenci představuje číslo vrstvy.

- Jméno: Tx
- Příjmení: Příjmení
- Logon: tx.prijmeni

- Display Name: Příjmení Tx

2.4.6 Pravidla

V rámci Tier modelu je nutné dodržovat následující pravidla:

- Je nutné dodržovat třídění objektů podle pravidel
- Každý účet v Tier Modelu musí být členem nějaké skupiny ve vrstvě
- V popisu servisního účtu je potřeba uvádět odpovědnou osobu a účel
- V popisu skupin je potřeba uvádět odpovědnou osobu a účel
- Neobcházet politiky, například hesla

Všechna pravidla je důležité dodržovat z několika důvodů, mezi které patří například usnadnění administrátorům řešit případné potíže s účty, ale také například usnadnění práce při auditu.

2.5 Shrnutí současného stavu

V předešlých kapitolách bylo rozebráno aktuální obecné nastavení a konfigurace v doméně společně s různými organizačními politikami. Na základě této analýzy můžeme konstatovat, že úroveň zabezpečení v rámci domény je extrémně nízká a volnost organizačních politik i konfigurace představuje velmi vysoké riziko a je na dnešní poměry nevyhovující.

Největší problém osobně vidím v riziku odposlechnutí či jiného způsobu zmocnění významných účtů a následného zneužití těchto účtů. Volnost oprávnění přístupů společně s množstvím doménových administrátorů v kombinaci s nastavenou politikou hesel toto riziko definuje extrémně vysoké.

V doméně chybí především struktura, která by lépe definovala a rozdělovala oprávnění, dále řád definující používání významných účtů a v neposlední řadě přísnější politika hesel. Jinými slovy v doméně chybí jakákoliv ochrana, která by snižovala riziko zmocnění účtů a také ochrana, která by snižovala dopady v případě zmocnění nějakého účtu. Dále zde chybí úprava konfigurace, která by snižovala riziko již známých hrozeb, například zakázání rizikových a zastaralých protokolů.

Vybrané požadavky mateřské společnosti jsou na velmi vysoké úrovni z hlediska on permise řešení a definují přísnou a efektivní bezpečnostní politiku, která vyplní téměř všechny aktuální bezpečnostní mezery. Vybrané požadavky, respektive opatření výrazně snižují riziko především útoků spojenými se sociálním inženýrstvím a využitím známých hrozeb v prostředí Windows.

3 Vlastní návrhy řešení

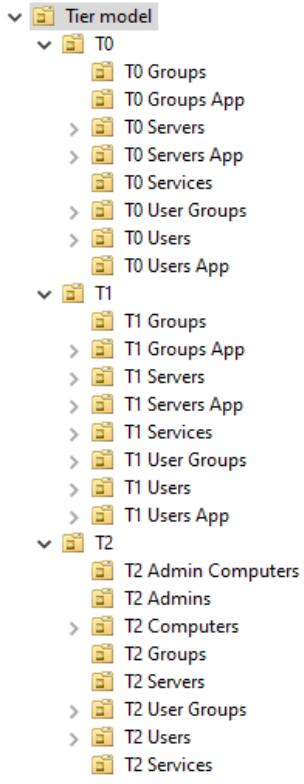
V této kapitole se zaměřím na vlastní návrh řešení. Ve většině návrhu se věnuji technické implementaci požadavků, na konci návrhu rozebírám management zavádění změn a ekonomické zhodnocení.

3.1 Tier model

Jako první krok navrhuji vytvořit Tier model. Zde bych chtěl hned na začátek podotknout, že model není standardizovaný a je ohebný, jinými slovy v každé společnosti se mohou různé detaily v konkrétním nastavení lišit. V našem případě je nutné dodržovat názvy OU a dalších objektů AD stejné jako v materiálech dodané mateřskou společností. Jednotná prostředí umožňují lepší podporu a také jsou na ně navázány další procesy například v SIEM, SCCM (MECM) a dalších systémech.

3.1.1 Struktura organizačních jednotek

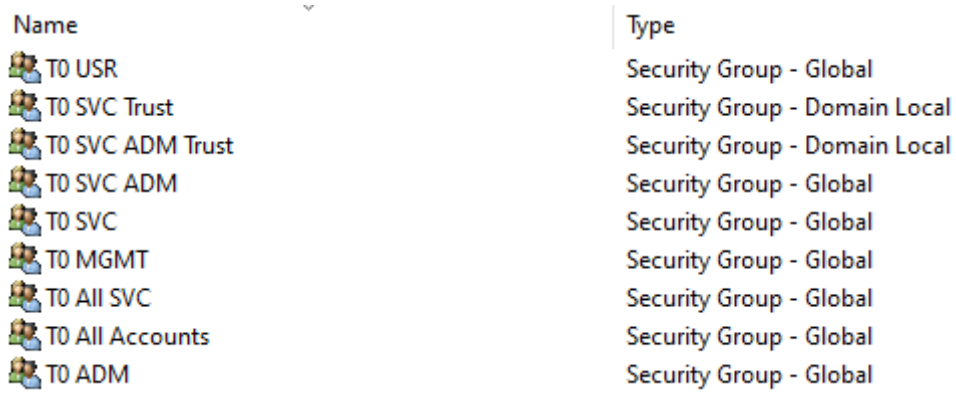
V kořenovém adresáři organizační struktury AD vytvoříme novou OU nazvanou Tier model. V rámci této OU dále vytvoříme další OU pro jednotlivé vrstvy T0, T1 a T2. V OU jednotlivých vrstev následně vytvoříme další strukturu OU, ve které budou objekty tříděny pro lepší organizaci a správu. Struktura jednotlivých vrstev se mírně liší.



Obrázek 15: Struktura OU Tier Modelu (vlastní)

3.1.2 Základní skupiny

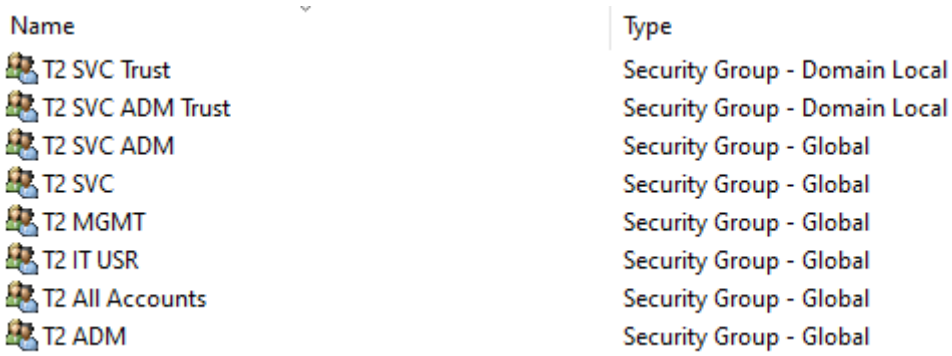
Dalším krokem při tvorbě Tier Modelu je vytvoření základních skupin jednotlivých úrovní, pomocí kterých se řídí oprávnění. Základní skupiny pro jednotlivé úrovně budeme vytvářet v OU Tx Groups. Je nutné dodržet členství skupin, všechny skupiny až na skupinu Tx MGMT jsou členem skupiny Tx All Accounts.



Name	Type
T0 USR	Security Group - Global
T0 SVC Trust	Security Group - Domain Local
T0 SVC ADM Trust	Security Group - Domain Local
T0 SVC ADM	Security Group - Global
T0 SVC	Security Group - Global
T0 MGMT	Security Group - Global
T0 All SVC	Security Group - Global
T0 All Accounts	Security Group - Global
T0 ADM	Security Group - Global

Obrázek 16: Základní skupiny T0 (vlastní)

T1 má stejnou strukturu skupin jako T0, struktura skupin se mírně liší u T2.



Name	Type
T2 SVC Trust	Security Group - Domain Local
T2 SVC ADM Trust	Security Group - Domain Local
T2 SVC ADM	Security Group - Global
T2 SVC	Security Group - Global
T2 MGMT	Security Group - Global
T2 IT USR	Security Group - Global
T2 All Accounts	Security Group - Global
T2 ADM	Security Group - Global

Obrázek 17: Základní skupiny T2 (vlastní)

3.1.3 Zabezpečení organizačních jednotek

Po vytvoření základní struktury OU Tier Modelu a skupin v jednotlivých úrovních je nutné upravit zabezpečení OU. Jako první krok je nutné zrušit dědění práv z nadřazené struktury.

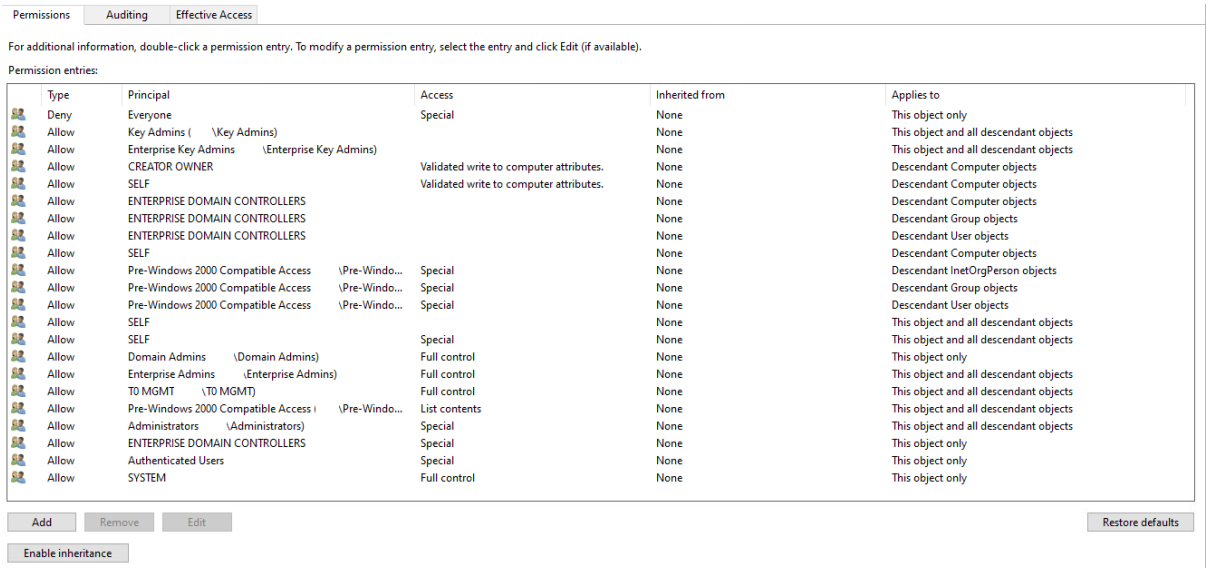
V podrobnostech OU Tier model v záložce "Security" zvolíme "Advanced", kde dědění práv zrušíme. Systém nás vyzve, zda práva, která byla zděděna z nadřazené struktury chceme odstranit, nebo je chceme převést do námi vybrané OU, zvolíme možnost "Convert inherited permissions into explicit permissions on this object". Tím zajistíme, že práva, která v nastavení zůstávají, nebudeme muset znovu vkládat.

V dalším kroku odstraníme práva, které nejsou žádoucí a přidáme ty potřebné. Odebereme skupiny, které by neměly mít práva nad objekty v Tier Modelu. Skupiny, které budou odebrány, je nutné vybrat s ohledem na konfiguraci a používané služby v doméně.

Skupiny, které by měly být odstraněny v každé doméně jsou:

- Organization Management
- Account Operators
- Print Operators

Jako poslední bod nastavíme nad celým OU Tier Model práva Full control skupině T0 MGMT, tím zajistíme, že spravovat Tier Model budou moct pouze členové této skupiny.



Obrázek 18: Zabezpečení OU Tier Model (vlastní)

V dalších krocích budeme nastavovat oprávnění pro T1 a T2, ve kterých budeme definovat, kdo bude moct spravovat objekty v těchto úrovních. Skupině T1 MGMT budeme nastavovat v pokročilém nastavení specifické oprávnění pouze nad některými OU.

OU T1 Groups App

Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Delete all child objects	None	This object only
Allow	T1 MGMT (T1 MGMT)	Create/delete Group objects	None	This object only
Allow	T1 MGMT (T1 MGMT)	Create/delete Organizational Unit objects	None	This object only
Allow	T1 MGMT (T1 MGMT)	Full control	None	Descendant Group objects
Allow	T1 MGMT (T1 MGMT)	Full control	None	Descendant Organizational Unit objects

Obrázek 19: Zabezpečení OU T1 Groups App (vlastní)

OU T1 Servers

Type	Principal	Access	Inherited from	Applies to
Allow	T1 MGMT (T1 MGMT)	Create/delete Computer obje...	None	This object only
Allow	T1 MGMT (T1 MGMT)	Full control	None	Descendant Computer objects

Obrázek 20: Zabezpečení OU T1 Servers (vlastní)

OU T1 Servers App

Type	Principal	Access	Inherited from	Applies to
Allow	T1 MGMT (\T1 MGMT)	Create/delete Computer obj...	None	This object only
Allow	T1 MGMT (\T1 MGMT)	Create/delete Organizational...	None	This object only
Allow	T1 MGMT (\T1 MGMT)	Full control	None	Descendant Computer objects
Allow	T1 MGMT (\T1 MGMT)	Full control	None	Descendant Organizational Unit objects

Obrázek 21: Zabezpečení OU T1 Servers App (vlastní)

OU T1 Services

Type	Principal	Access	Inherited from	Applies to
Allow	T1 MGMT (T1 MGMT)	Create/delete User objects	None	This object only
Allow	T1 MGMT (T1 MGMT)	Full control	None	Descendant User objects

Obrázek 22: Zabezpečení OU T1 Services (vlastní)

OU T1 User Groups

Type	Principal	Access	Inherited from	Applies to
Allow	T1 MGMT (T1 MGMT)	Create/delete Group objects	None	This object only
Allow	T1 MGMT (T1 MGMT)	Create/delete Organizational Unit ...	None	This object only
Allow	T1 MGMT (T1 MGMT)	Full control	None	Descendant Group objects
Allow	T1 MGMT (T1 MGMT)	Full control	None	Descendant Organizational Unit objects

Obrázek 23: Zabezpečení OU T1 User Groups (vlastní)

OU T1 Users App

Type	Principal	Access	Inherited from	Applies to
Allow	T1 MGMT (T1 MGMT)	Create/delete Organizational Unit objects	None	This object only
Allow	T1 MGMT (T1 MGMT)	Create/delete User objects	None	This object only
Allow	T1 MGMT (T1 MGMT)	Full control	None	Descendant Organizational Unit objects
Allow	T1 MGMT (T1 MGMT)	Full control	None	Descendant User objects

Obrázek 24: Zabezpečení OU T1 User App (vlastní)

Skupině T2 MGMT nastavíme práva Full control na všech OU T2 až na OU T2 Admin a T2 Groups. Je to dáno tím, že celý T2 je brán jako rizikový, protože se v něm nachází koncoví uživatelé. Není tedy potřeba v této vrstvě nějak složitě rozlišovat oprávnění. Oprávnění nad zmíněnými OU nastavíme skupině T1 MGMT.

OU T2 Admin

Type	Principal	Access	Inherited from	Applies to
Allow	T1 MGMT (T1 MGMT)	Create/delete Computer objects	None	This object only
Allow	T1 MGMT (T1 MGMT)	Full control	None	Descendant Computer objects

Obrázek 25: Zabezpečení OU T2 Admin (vlastní)

OU T2 Groups

Type	Principal	Access	Inherited from	Applies to
Allow	T1 MGMT (T1 MGMT)	Create/delete Group objects	None	This object only
Allow	T1 MGMT (T1 MGMT)	Full control	None	Descendant Group objects

Obrázek 26: Zabezpečení OU T2 Groups (vlastní)

3.1.4 Skupinové politiky

Posledním krokem při tvorbě Tier Modelu je nasazení skupinových politik, které upravují oprávnění na stanicích. V základním Tier Modelu je potřeba vytvořit 3 politiky pro jednotlivé úrovně a jednu dodatečnou v T2. V případě nasazení aplikací v rámci T0 a T1 je potřeba vytvořit další politiky jednotlivých aplikací.

- Vytvoříme GPO s názvem T0 a nasadíme ji na OU T0 Servers. Konfigurace GPO je znázorněna v **Příloha 1**.
- Vytvoříme GPO s názvem T1 a nasadíme ji na OU T1 Servers. Konfigurace GPO je znázorněna v **Příloha 2**.
- Vytvoříme GPO s názvem T2 a nasadíme ji na OU T2 Computers a T2 Servers. Konfigurace GPO je znázorněna v **Příloha 3**.
- Vytvoříme GPO s názvem T1 ADM a nasadíme ji na OU T2 Admin Computers. Konfigurace GPO je znázorněna v **Příloha 4**.

3.2 Nasazení Tier Modelu

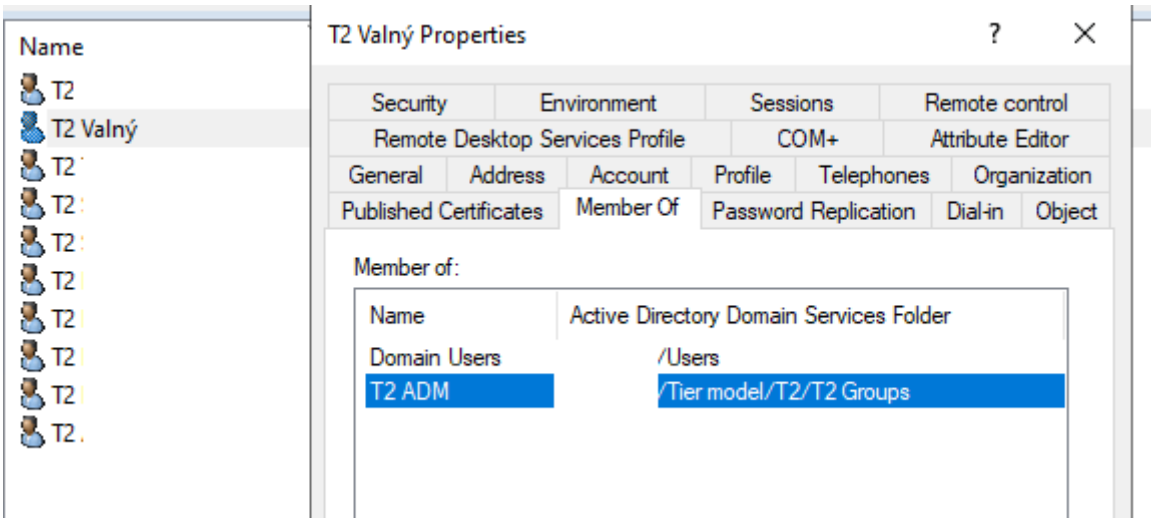
V tomto bodě se zaměřím na ostré nasazení Tier Modelu v prostředí organizace a další úkoly spojené s tímto požadavkem. Jedná se o relativně složitý proces, který ovlivní hlavně práci zaměstnanců IT oddělení.

3.2.1 Nasazení T2

Cílem tohoto bodu je odizolovat nejrizikovější vrstvu modelu od zbytku domény. Navrhuji nasadit T2 jako první, protože zahrnuje pouze koncové stanice uživatelů, navíc z jejich strany nijak neovlivní používání těchto stanic. Změna ovlivní pouze správce v IT oddělení a používání citlivých účtů.

Potřebné body k dosažení cílového stavu:

a) Vytvoření T2 admin účtů v OU T2 Admins a přidání členství v potřebných skupinách



Obrázek 27: T2 administrátorský účet (vlastní)

b) Vytvoření lokálních účtů "admin" na stanicích správců v IT oddělení

c) Přidání uživatelských účtů správců do skupiny T2 IT USR

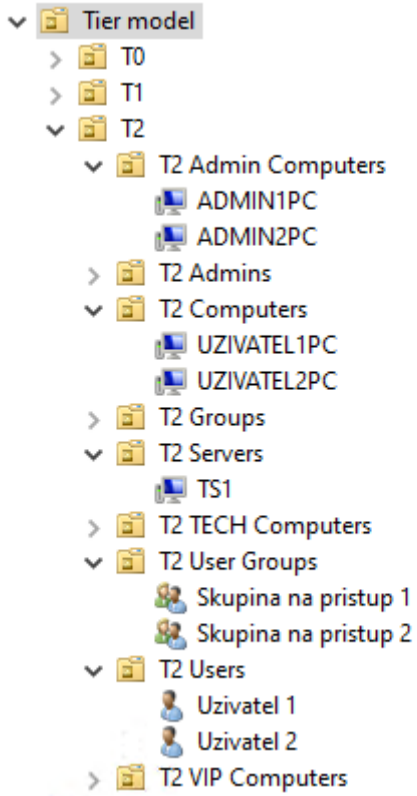
d) Přesunutí objektů stanic zaměstnanců IT oddělení do OU T2 Admin Computers

e) Přesunutí objektů stanic uživatelů do OU T2 Computers

f) Přesunutí objektů skupin do OU T2 User Groups

g) Přesunutí objektů uživatelských účtů do T2 Users

h) Přesunutí objektů serverů do T2 Servers



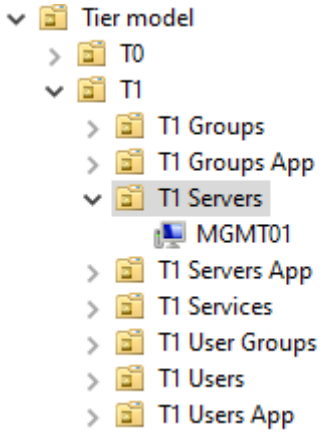
Obrázek 28: Nasazený T2 (vlastní)

3.2.2 Vzdálená správa Active Directory

Jako další bod navrhuji vytvořit Jump server, přes který se bude přistupovat do AD. Na tomto serveru budou nainstalovány RSAT a bude již umístěn v T1. Cílem tohoto bodu je vytvořit nový způsob přístupu do AD pro správce v IT oddělení za účelem základní správy objektů, díky němu se již nebude muset pro správu AD přistupovat přes doménový řadič a používat doménový administrátor.

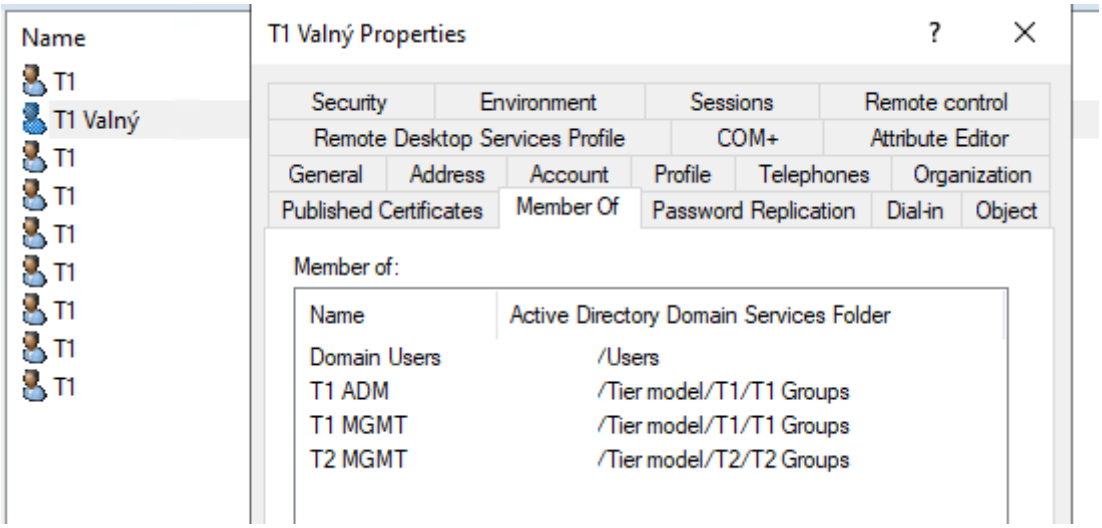
Potřebné body k dosažení cílového stavu:

a) Vytvoření čistého serveru
b) Instalace RSAT
c) Přesunutí objektu serveru do OU T1 Servers



Obrázek 29: Objekt serveru v T1 (vlastní)

d) Vytvoření T1 účtů v OU T1 Users a přidání členství v potřebných skupinách



Obrázek 30: T1 administrátorský účet (vlastní)

3.2.3 Nasazení T1

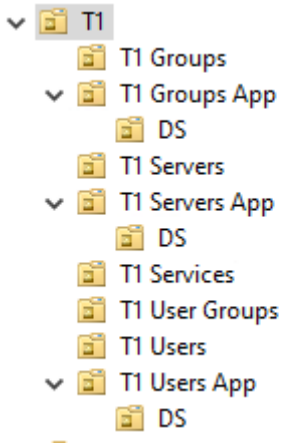
Cílem tohoto bodu je vytvořit vrstvu ve které bude efektivně řízeno oprávnění nad servery společnosti, na kterých jsou provozovány aplikace, systémy a služby. Téměř všechny servery v rámci T1 navrhuji nasadit jako aplikaci, protože tím dosáhneme ještě většího rozdělení v rámci vrstvy a také budeme moct snadněji řídit přístupy, například u externistů. Každý server nebo skupinu serverů na kterých je provozován nějaký systém je potřeba implementovat do úrovně velmi opatrně a ověřovat funkčnost tohoto systému.

Nasazení aplikace

V následujících bodech rozeberu nasazení aplikace datových schránek (DS) do T1 jako aplikaci. Před nasazením aplikace budeme muset vytvořit strukturu pro aplikaci.

Potřebné body k nasazení aplikace

a) Vytvoření OU aplikace

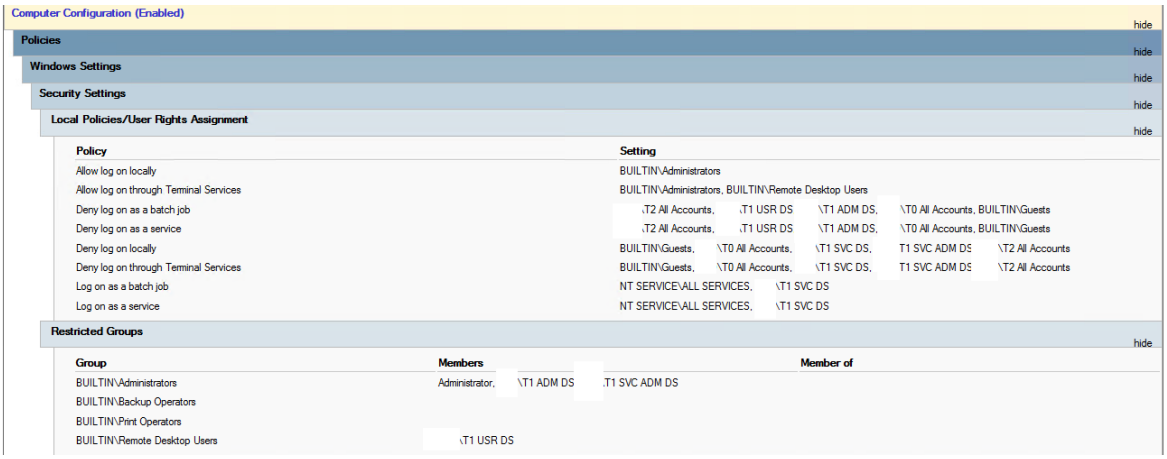


Obrázek 31: OU aplikace DS (vlastní)

b) Vytvoření skupin aplikace v T1 Groups App/DS

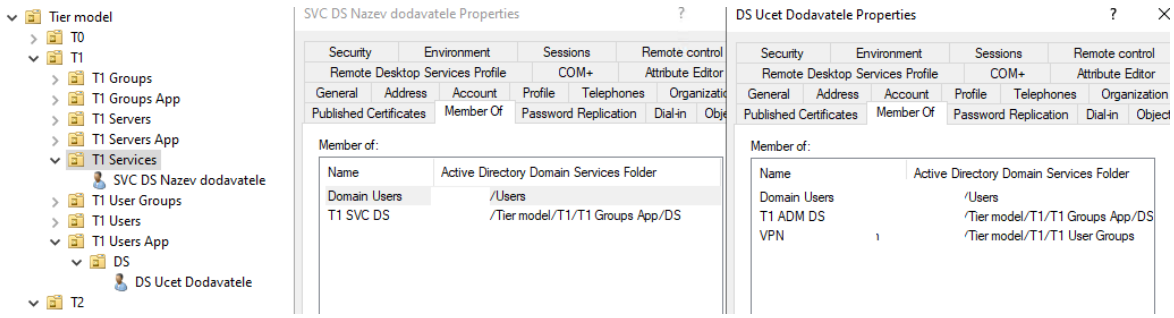
Obrázek 32: Skupiny aplikace DS (vlastní)

c) Vytvoření a nasazení GPO aplikace na OU T1 Servers App/DS



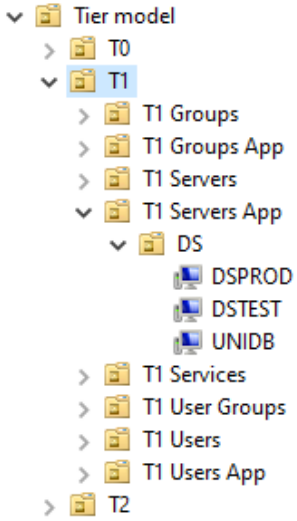
Obrázek 33: GPO pro aplikaci DS (vlastní)

d) Vytvoření / přesunutí potřebných T1 aplikačních účtů a přidělení skupin podle účelu



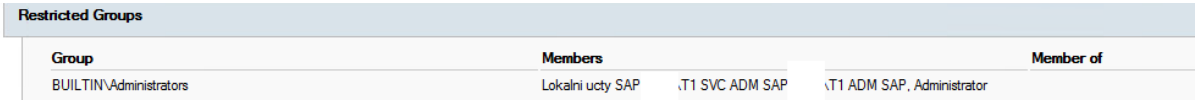
Obrázek 34: Servisní účet a účet dodavatele DS (vlastní)

e) Přesunutí objektů serverů do T1 Server App/DS



Obrázek 35: Nasazená aplikace DS (vlastní)

Při nasazování citlivých aplikací je někdy potřeba provést lehké úpravy na straně aplikace nebo Tier Modelu. To může zahrnovat například reorganizaci servisních účtů a jiné operace. V našem případě budeme muset při nasazování systému SAP lehce upravit politiku takovým způsobem, aby povolovala další lokální účty a administrátory.

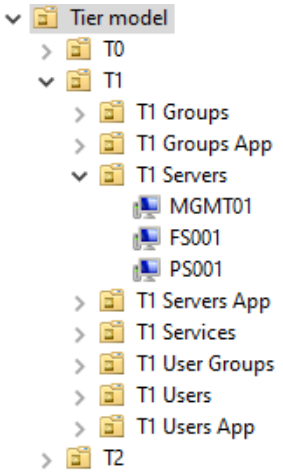


Obrázek 36: Úprava Tier Modelu (vlastní)

Všechny ostatní servery a systémy, které nebudou nasazovány do T1 jako aplikace budou umístěny v OU T1 Servers. Navrhuji, aby zde byly pouze obecné servery, které nevyžadují žádný přístup externistů a přistupují na ně pouze správci v IT oddělení. Jedná se například o file servery, print servery a další.

Potřebné body k plnému nasazení T1:

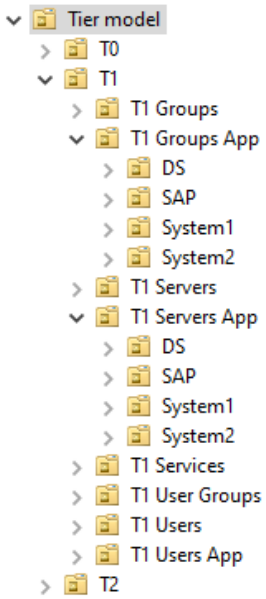
a) Přesunutí objektů serverů, které nebudou nasazeny jako aplikace do OU T1 Servers



Obrázek 37: Nasazení serverů v T1 (vlastní)

b) Kontrola již vytvořených T1 účtů a úprava oprávnění podle potřeby

c) Nasazení aplikací



Obrázek 38: Nasazení aplikací v T1 (vlastní)

3.2.4 Nasazení T0

V našem případě nebudeme nasazovat žádné aplikace ani služby v T0. Jediná služba v našem prostředí, která patří do T0, je certifikační autorita, ale po vytvoření vztahu důvěry s doménou mateřské společnosti je naplánováno postupně přejít na její certifikační autoritu a aktuální certifikační autoritu zrušit. T0 navrhuji využívat pro umísťování citlivých účtů a skupin.

3.2.5 Izolace T0 a doménových řadičů

Po splnění všech předchozích bodů dosáhneme všech predispozicí k izolaci T0 a doménových řadičů. Tento bod navrhuji provést jako poslední bod v rámci nasazení Tier Modelu po ověření, že všichni správci v IT oddělení jsou seznámeni se změnami a hlavně se v nich orientují. V rámci tohoto bodu navrhuji vytvořit administrátorům nové účty a smazat všechny staré z důvodu hrozby zneužití Kerberos golden ticketu. Cílem tohoto bodu je izolovat nejkritičtější vrstvu modelu a omezit množství administrátorů.

Potřebné body k dosažení izolace:

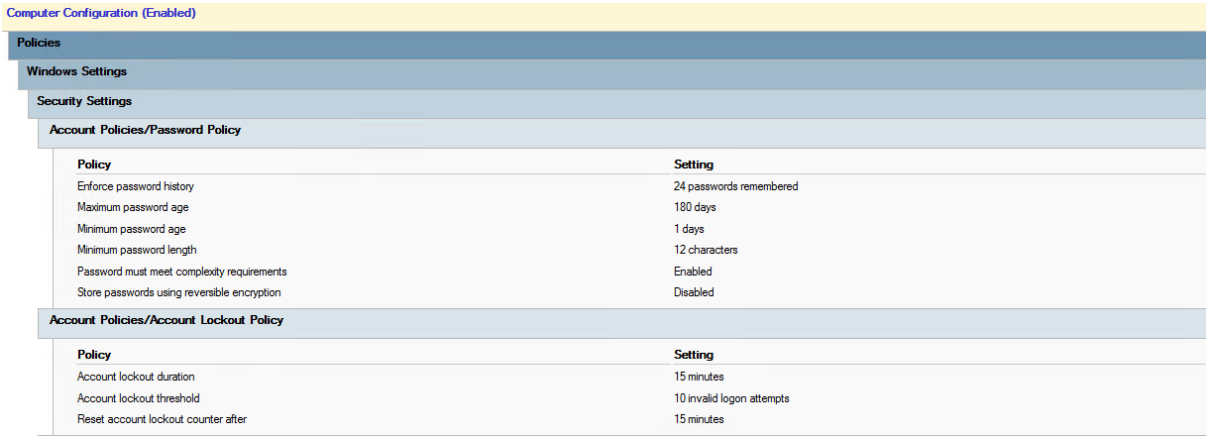
a) Vytvoření nových účtů
b) Smazání všech starých administrátorských účtů v doméně
c) Reset hesla KRBTGT

3.3 Politika hesel

Po vytvoření Tier Modelu navrhuji nasadit novou politiku hesel podle mateřské společnosti. Tato změna musí být komunikována k uživatelům, navrhuji pro to použít interní mailovou komunikaci. V komunikaci budou vysvětlena nová pravidla a také datum do kterého si musí uživatelé změnit heslo. Po stanoveném termínu navrhuji vynutit změnu hesla těch uživatelů, kteří změnu ještě neprovedli.

3.3.1 Defaultní politika hesel

Základní politiku pro hesla nastavíme v defaultní doménové politice. Tato politika bude platit na všechny objekty, na které nebude nasazena Fine-Grained Password Policy.



Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	180 days
Minimum password age	1 days
Minimum password length	12 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

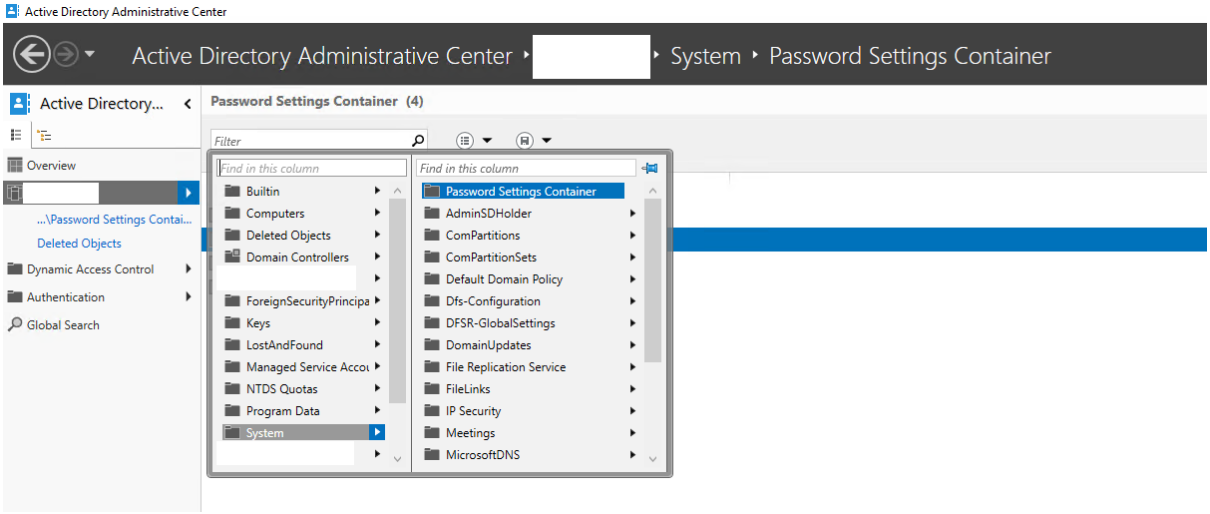
Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

Obrázek 39: Defaultní politika hesel (vlastní)

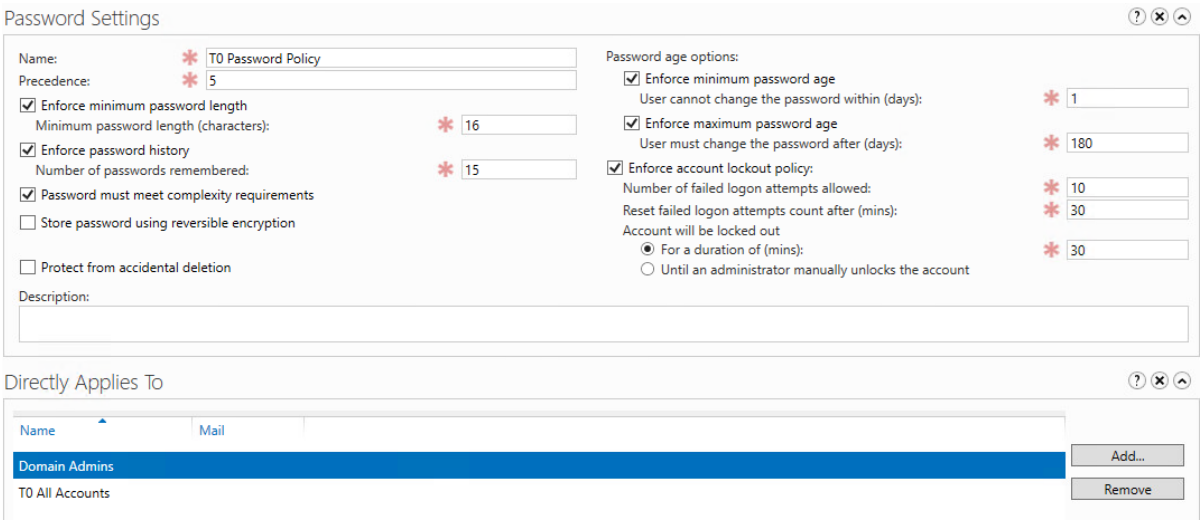
3.3.2 Fine Grained Password Policy

Dále budeme nasazovat již zmíněnou Fine-Grained Password Policy, všechny potřebné skupiny byly vytvořeny při vytváření Tier modelu. V konzoli ADAC se přepneme do stromového zobrazení a přejdeme do (AD Root)/ System / Password Settings Container.



Obrázek 40: Cesta k nastavení speciální politiky hesel (vlastní)

V této složce vytvoříme 4 politiky pro hesla podle požadavků.



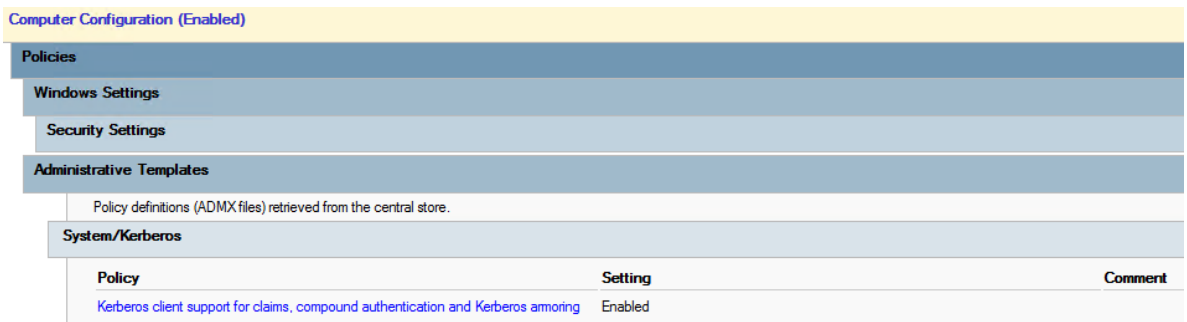
Obrázek 41: Speciální politika hesel (vlastní)

3.4 Konfigurace protokolů a služeb

Všechny požadované změny v nastavení navrhuji implementovat prostřednictvím GPO. Některé změny navrhuji provádět v defaultních doménových politikách, pro zbylé požadavky navrhuji vytvořit 3 politiky (Obecná, testovací a DC) do kterých budeme postupně přidávat všechny body. Používání pouze dvou (ostrých) politik usnadní správu a případné aktualizace. Při úpravách konfigurace je potřeba postupovat opatrně, protože mohou ovlivnit funkčnost systémů a aplikací. Z tohoto důvodu navrhuji jednotlivé požadavky nasazovat postupně a důkladně testovat, díky tomu se mohou snadněji identifikovat a napravovat jakékoli chyby vzniklé při implementaci před ostrým nasazením v rámci celé domény.

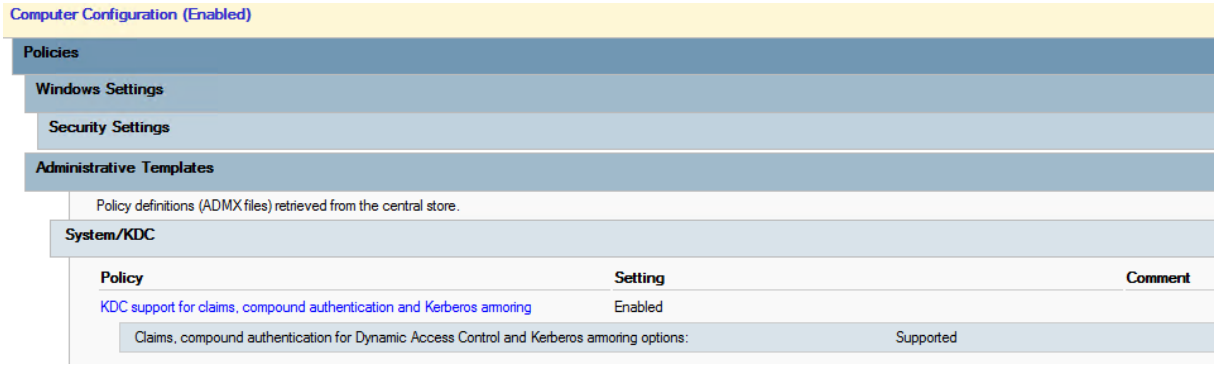
3.4.1 Kerberos Armoring

Jako první navrhuji nasadit Kerberos Armoring, nastavení navrhuji implementovat prostřednictvím úpravy defaultních doménových politik. Všichni klienti nemusí podporovat Kerberos Armoring, z tohoto důvodu nastavení zatím nebudeme vynucovat, ale pouze zapneme jeho podporu. V GPO Default Domain Policy povolíme Claims a Kerberos Armoring.



Obrázek 42: Nasazení Kerberos Armoring Default Domain Policy (vlastní)

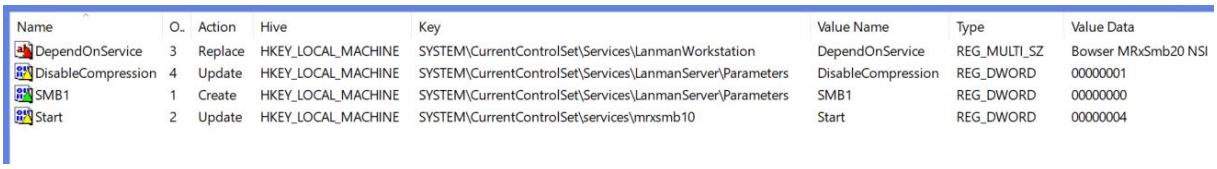
Dále budeme muset zvlášť upravit nastavení na doménových řadičích, v GPO Default Domain Controllers Policy povolíme používání Claims a Kerberos Armoring, v rozbalovacím menu nastavíme "Supported".



Obrázek 43: Kerberos Armoring v Default Domain Controllers Policy (vlastní)

3.4.2 Mitigace SMB

Jako další bod navrhuji upravit konfiguraci protokolu SMB. Navrhuji vytvořit nové politiky Politika1 a Politika1Test, ve kterých v cestě Computer Configuration – Preferences – Registry vytvoříme 4 položky registru s následujícím nastavením:



Obrázek 44: Položky registu v rámci GPO pro mitigaci SMB (vlastní)

Položka DisableCompression zakazuje kompresi v SMBv3 a eliminuje tak známou zranitelnost, zbylé položky zakazují protokol SMBv1. Dále v cestě Computer configuration – Policies – Windows Settings – Security Settings – Local Policies – Security Options povolíme SMB Signing.

Obrázek 45: SMB signing v GPO (vlastní)

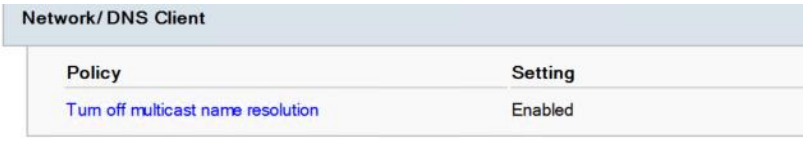
Vytvořenou politiku Politika1Test navrhuji nasadit pouze na IT oddělení, v našem případě tedy na OU T2 Admin Computers. V případě úspěšného nasazení a testování navrhuji nasadit politiku Politika1 na kořen domény mimo pracovní dobu a opět provést testování, obzvláště na serverech.

3.4.3 Vypnutí LLMNR

Jako další bod navrhuji vypnout LLMNR, před vypnutím je potřeba ověřit, zda některé aplikace, nebo stanice tento protokol nevyžadují. Pokud správně funguje DNS, neměl by být protokol LLMNR potřebný. LLMNR mohou využívat například následující aplikace:

- Systémy pro sdílení souborů a tiskáren v lokální síti
- Nástroje pro správu sítě, jako je například Network Explorer
- Aplikace pro sdílení multimédií v lokální síti
- Různé aplikace a služby pro vzdálenou správu a monitorování sítě

V GPO Politika1Test, kterou jsme vytvořili v rámci minulého bodu LLMNR vypneme v Computer Configuration -> Administrative Templates -> Network -> DNS Client



Obrázek 46: Vypnutí LLMNR v GPO (vlastní)

V případě úspěšného nasazení a testování navrhuji provést zmíněné nastavení také v politice Politika1 mimo pracovní dobu a opět provést testování, obzvláště na serverech.

3.4.4 Vypnutí služby Print Spooler na doménových řadičích

V rámci tohoto bodu navrhuji zakázat spouštění služby prostřednictvím GPO. Jelikož tato GPO bude nasazena pouze na doménových řadičích, navrhuji vytvořit novou GPO DCPolitika1, kterou budeme používat i pro následující bod. V cestě Computer Configuration – Preferences – Registry vytvoříme novou položku registru s následujícím nastavením:

Obrázek 47: Položka registru pro zakázání služby v GPO (vlastní)

Vytvořenou politiku nasadíme na OU Domain Controllers v kořenu domény. Nasazení této politiky zakáže spouštění služby, ale aktuálně běžící službu nevypne. Službu je nutné vypnout manuálně, nebo provést restart doménového řadiče. Nasazení této GPO neovlivní funkčnost žádného systému.

3.4.5 LDAP signing a Channel binding

LDAP Signing a Channel binding navrhuji nasadit jako poslední bod, protože pravděpodobnost, že ovlivní funkčnost nějakého systému nebo aplikace je vyšší než u předchozích požadovaných bodů. Tento bod lze realizovat dvěma způsoby, postupně, nebo okamžitou změnou. V rámci postupné implementace bychom odpovídající nastavení v GPO postupně upravovali přes možnosti "When Supported" a jiné až po "Require Signing". Navrhuji tento bod implementovat formou okamžité změny mimo pracovní dobu, ideálně před víkendem. Tím zaručíme, že nenastanou žádné komplikace během přechodu a snížíme tak čas strávený na testování funkčnosti systémů a aplikací. V politice DCPolitika1 pro doménové řadiče provedeme následující nastavení:

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/ Security Options

Domain Controller

Policy	Setting
Domain controller: LDAP server signing requirements	Require signing

Other

Policy	Setting
Domain controller: LDAP server channel binding token requirements	Always

Obrázek 48: LDAP signing a Channel binding GPO pro DC (vlastní)

V politice Politika1 provedeme v stejné cestě následující nastavení:

Network Security

Policy	Setting
Network security: LDAP client signing requirements	Require signing

Obrázek 49: LDAP signing a Channel binging pro kořen domény (vlastní)

Po konfiguraci GPO navrhuji vynutit aktualizaci skupinových politik na doménových řadičích a následně je postupně restartovat. Po restartu navrhuji provést krátký test funkčnosti základních služeb. Jako poslední bod je potřeba vynutit aktualizaci skupinových politik na potřebných serverech a stanicích a důkladně otestovat funkčnost všech systémů a aplikací.

3.5 Vztah důvěry

Nyní se zaměřím na vytvoření vztahu důvěry mezi doménou mateřské společnosti a doménou dceřiné společnosti. Tomuto bodu předchází síťová konfigurace a další nastavení, které není předmětem této práce.

3.5.1 Vytvoření vztahu důvěry

V konzoli ADDT otevřeme podrobnosti naší domény a přepneme se do záložky "Trusts". V této záložce spustíme průvodce "New Trust".

V průvodci provedeme následující kroky:

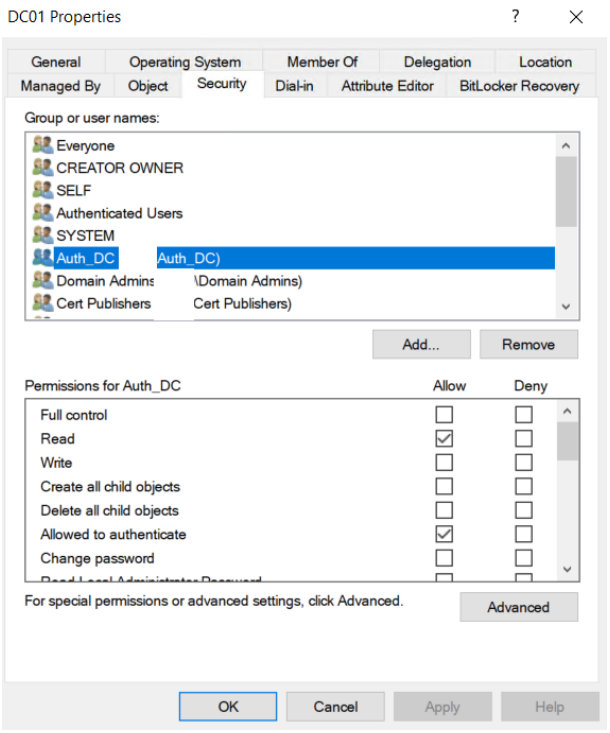
a) Zadáme jméno cílové domény
b) Zvolíme možnost Forest Trust
c) Ponecháme Two way
d) Ponecháme This domain only
e) Zvolíme Selective Authentication
f) Použijeme silné vygenerované heslo

Těmito kroky nachystáme vztah důvěry na naší straně, stejné kroky se budou muset provést také na straně domény mateřské společnosti. Po nachystání vztahu důvěry je potřeba ho validovat, to provede administrátor ze strany mateřské společnosti, který má účet doménového administrátora v obou doménách.

3.5.2 Selektivní vztah důvěry

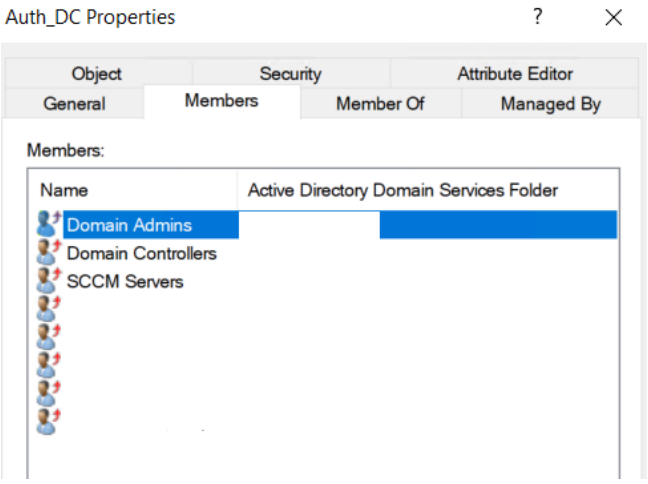
Po vytvoření vztahu důvěry je nutné nastavit základní strukturu pro ověřování v rámci selektivního vztahu důvěry. Zmíněné kroky je potřeba ve většině případů provést v obou doménách, budu zde rozebírat pouze kroky potřebné na naší straně. V OU T0 User Groups vytvoříme OU Auth. V této OU budeme vytvářet skupiny potřebné k provozu selektivního vztahu důvěry. Dále vytvoříme security domain local skupinu s názem Auth_DC, která bude sloužit pro autentizaci na doménové řadiče dceřiné společnosti. Vytvořenou skupinu vložíme

do zabezpečení na všechny doménové řadiče s oprávněními "Read" a "Allowed to authenticate". Členové této skupiny tedy budou moct číst z doménových řadičů a autentizovat se na nich.



Obrázek 50: Oprávnění v rámci selektivního vztahu důvěry (vlastní)

Nyní do skupiny Auth_DC přidáme skupiny Domain Admins a Domain Controllers z domény mateřské společnosti. Dále se zde budou selektivně vkládat další prvky a systémy, které budou potřebovat dříve zmíněná oprávnění na doménových řadičích, na příkladu lze vidět, že zde budou například SCCM (MECM) servery. Stejné kroky jsou potřeba provést i na ostatních objektech v doméně, které potřebují nějaké oprávnění spojené s doménou mateřské společnosti.



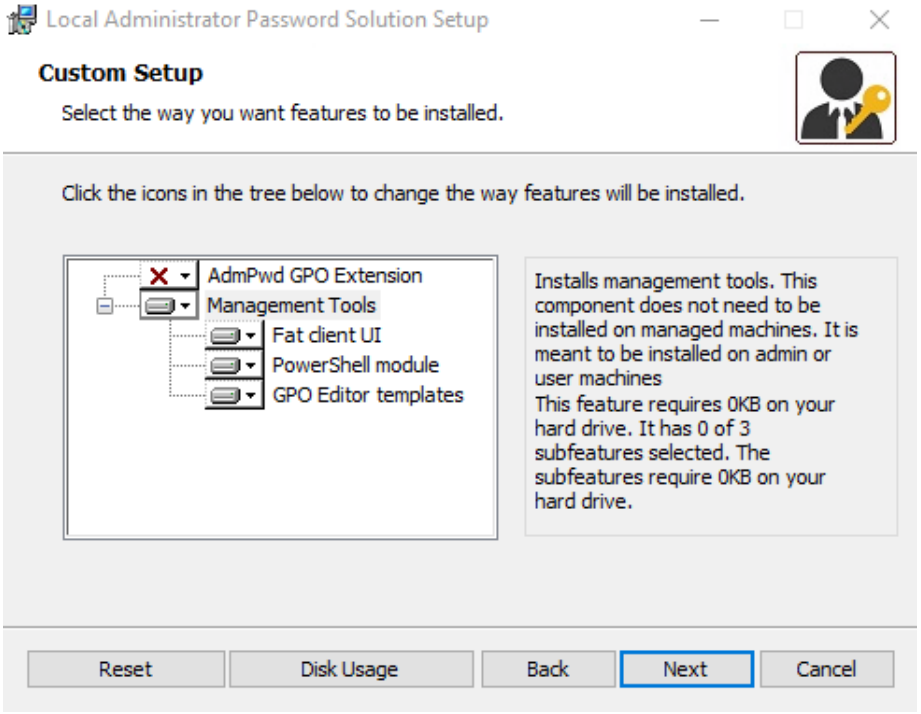
Obrázek 51: Členství ve skupině pro ověřování (vlastní)

3.6 LAPS

Jako poslední bod navrhuji nasadit nástroj LAPS, v následujících bodech je rozebrán postup jeho nasazení.

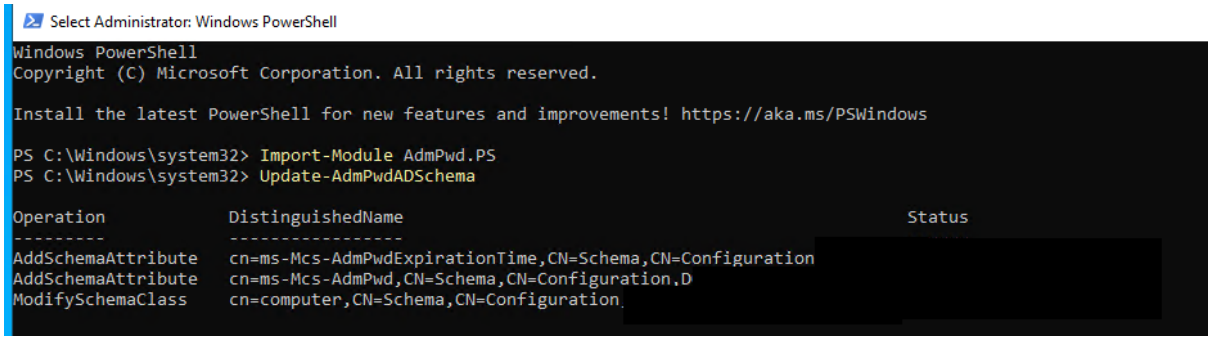
3.6.1 Instalace

Pomocí instalačního souboru nainstalujeme na primárním doménovém řadiči kompletní balíček Management Tools nástroje LAPS.



Obrázek 52: Instalace LAPS (vlastní)

Po úspěšné instalaci provedeme restart doménového řadiče. V dalším kroku upravíme schéma domény, spustíme aplikaci PowerShell jako správce a použijeme dva příkazy. Prvním příkazem importujeme modul AdmPwd.PS abychom s ním mohli pracovat a pomocí druhého příkazu upravíme schéma domény.



Obrázek 53: Import modulů a rozšíření schéma domény PowerShell (vlastní)

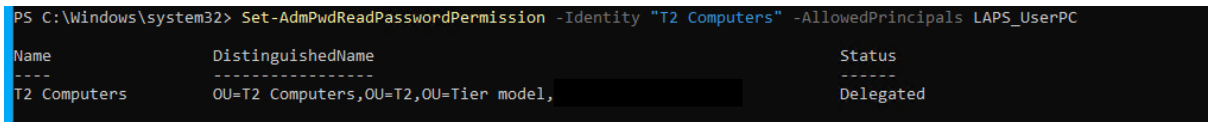
Pro provedení této operace je nutné být Schéma administrátorem. Podle "best practices" by neměl být žádný účet v doméně Schéma administrátorem, pokud to nevyžaduje nějaká jednorázová změna jako je například náš případ. Pokud tedy náš účet není členem skupiny Schema Admins, přidáme ho do ní z důvodu provedení této operace. Po úpravě schématu domény odstraníme všechny účty ze skupiny Schema Admins. Členství ve skupině se projeví až po novém přihlášení.

3.6.2 Oprávnění

V následujících bodech budeme nastavovat oprávnění pro operace spojené s hesly lokálních administrátorů. Navrhuji vytvořit dvě skupiny, které budou oddělovat oprávnění podle důležitosti. První skupina bude mít oprávnění pouze nad uživatelskými stanicemi a druhá skupina bude mít oprávnění nad všemi stanicemi a servery. Větší diverzifikace oprávnění nad zbylými stanicemi není nutná, protože se jedná o citlivé stanice, na kterých není potřeba často využívat účet lokálního správce a možnost zobrazit si toho heslo by měla mít pouze úzká skupina správců. Skupiny budou umístěny v OU T0 User Groups, aby je mohli spravovat pouze nejvyšší administrátoři.

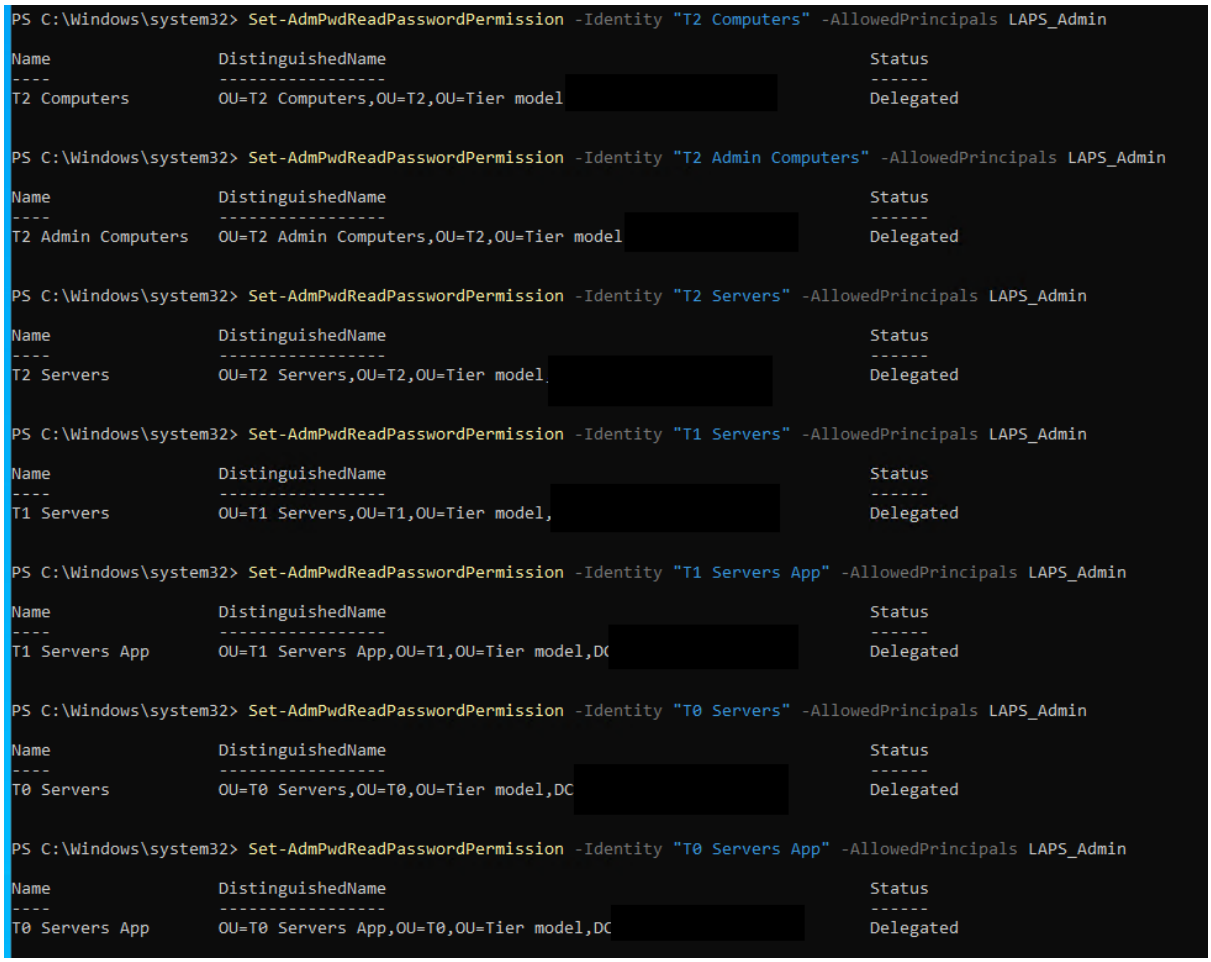
Obrázek 54: Skupiny pro LAPS (vlastní)

Pro přidělení oprávnění navrhuji použít příkazy v modulu PowerShell, které výrazně usnadní práci. Skupině LAPS_UserPC nastavíme oprávnění číst heslo lokálního administrátora na OU T2 Computers.



Obrázek 55: Nastavení oprávnění pro skupinu LAPS_UserPC (vlastní)

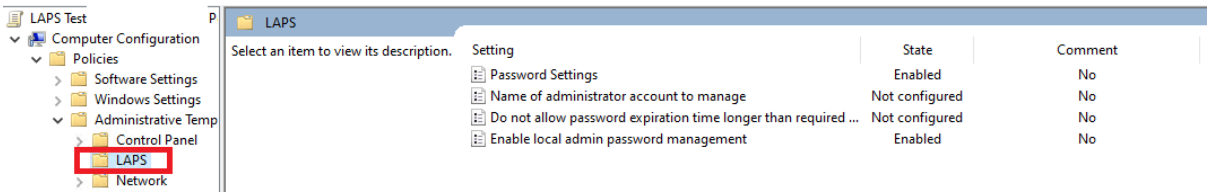
Skupině LAPS_Admin nastavíme oprávnění číst heslo lokálního administrátor na všech OU v Tier Modelu, ve který se nachází počítačové objekty.



Obrázek 56: Nastavení pro oprávnění pro skupinu LAPS_Admin (vlastní)

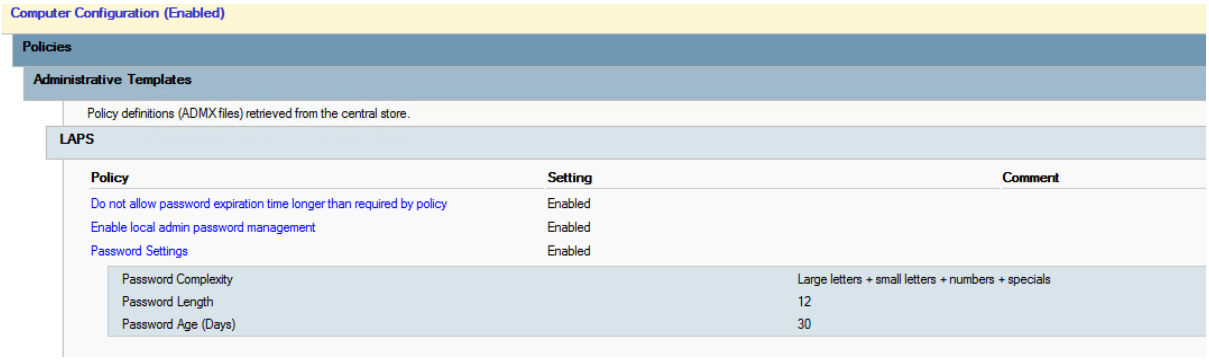
3.6.3 Skupinová politika pro LAPS

Posledním krokem v nastavení nástroje LAPS je vytvoření GPO, pomocí které budeme definovat konkrétní nastavení pro hesla lokálních správců na stanicích. Před vytvořením samotné GPO je nutné rozšířit šablony pro správu, abychom mohli nastavení vůbec spravovat. Potřebné soubory pro rozšíření šablon pro správu byly vytvořeny při instalaci nástroje na doménovém řadiči. První soubor má název "AdmPwd.admx" a je umístěn v "C:\Windows\PolicyDefinitions", druhý soubor má název "AdmPwd.adml" a je umístěn v "C:\Windows\PolicyDefinitions\en-US". Tyto soubory je nutné zkopírovat a vložit do "C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions" v případě prvního souboru a do "C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions\en-US" v druhém případě, aby se v šablonách pro správu zobrazila nová šablona LAPS. Tento krok platí v případě, že je používáno centrální uložiště skupinových politik.



Obrázek 57: LAPS šablona pro správu (vlastní)

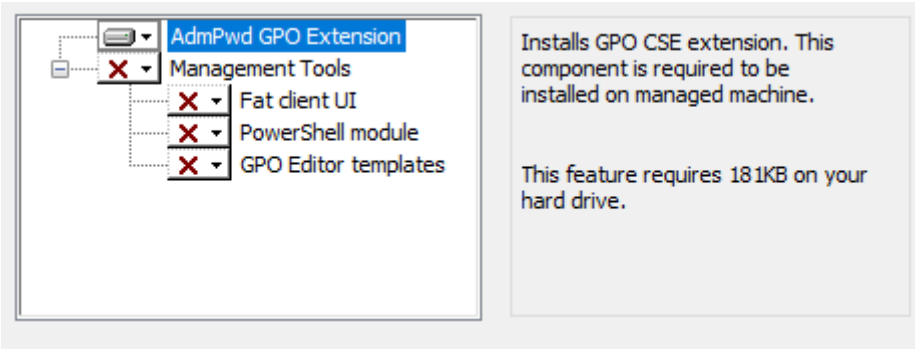
Po rozšíření šablon pro správu vytvoříme novou GPO, ve které definujeme obtížnost a platnost hesla společně s názvem účtu lokálního správce. Vytvořenou GPO nasadíme na všechny OU v rámci Tier Modelu, ve kterých se nachází počítačové objekty.



Obrázek 58: LAPS GPO (vlastní)

3.6.4 Instalace klienta na stanicích

Posledním krokem v implementaci nástroje LAPS je instalace klienta na spravované stanice. Klient musí být na všech spravovaných stanicích, instaluje se pouze vlastnost AdmPwd GPO Extension.



Obrázek 59: Distribuce LAPS na klienty (vlastní)

Klienta lze instalovat hromadně na velké množství stanic několika způsoby. Pro distribuci klientů navrhuji použít nástroj SCCM (MECM) mateřské společnosti, který bude implementován společně s vytvořením vztahu důvěry s mateřskou společností. Implementace

nástroje MECM není předmětem této práce. Distribuce pomocí tohoto nástroje poskytuje několik výhod jako je například informace o aktuálním stavu instalací. Hromadnou distribuci lze provést také pomocí skupinových politik.

3.7 Management zavedení

V této kapitole se budu zabývat managementem zavádění požadavků mateřské společnosti. Nejdříve stručně popíšu jednotlivé části integrace dceřiné společnosti a jak na sebe tyto části navazují pro lepší pochopení celého projektu. Ve zbytku se budu věnovat samotnému managementu zavádění změn. Management zavádění je pouze doplňkem této diplomové práce, z tohoto důvodu nebude příliš rozsáhlý a nebude obsahovat například podrobný popis a rozklad jednotlivých činností. Cílem je především stanovení hlavních činností, naplánování harmonogramu zavádění změn, určení reálných termínů a dalších informací. Stanovené hlavní činnosti zahrnují všechny kroky popsané v technické části návrhu.

3.7.1 Integrace

Jak již bylo naznačeno v úvodu, návrh se zabýval jednou z několika částí integrace dceřiné společnosti, převážně obecnou konfigurací týkající se AD za účelem zvýšení úrovně bezpečnosti. Celý proces integrace dceřiné společnosti zahrnuje různá síťová nastavení a úpravy konfigurace, dále zahrnuje fyzické propojení sítí a implementaci systémů pro správu a monitorování sítě. Všechny body po bod vytvoření vztahu důvěry probíhají souběžně se síťovým nastavením a realizací fyzického propoje mezi sítěmi společností. Tyto faktory jsou nutnou predispozicí k vytvoření vztahu důvěry, na který navazují implementace systémů pro správu a monitorování, které nejsou předmětem této diplomové práce. Jeden z těchto nástrojů navrhuji využít v rámci posledního požadavku, konkrétně distribuci nástroje LAPS. Termín dokončení integrace je konec listopadu.

3.7.2 Harmonogram

V harmonogramu navrhuji jednotlivé hlavní činnosti společně s termíny a dalšími informacemi. Jednotlivé činnosti mají výrazně nižší časovou náročnost, než jaký mají alokovaný prostor v rámci harmonogramu. Je to dáno tím, že vytvoření propoje mezi sítěmi společností je naplánováno realizovat až 14.8.2023, je tedy dostatečný prostor na realizaci změn (do bodu vztah důvěry) a seznámení se s nimi. Mezi další důvody patří například fakt, že na straně dceřiné společnosti bude všechny změny realizovat pouze jeden IT specialista, který má za úkol také další činnosti v rámci integrace. V neposlední řadě mateřská společnost záměrně poskytuje

dostatečný prostor na implementaci změn, aby měli všichni dostatečný prostor na to se s nimi seznámit a také aby byl dostatečný prostor na případné řešení vzniklých problémů.

Harmonogram je znázorněn v **Příloha 5**.

3.7.3 Časová náročnost a zdroje

V této části odhaduji časovou náročnost jednotlivých hlavních činností za účelem získání celkové časové náročnosti, která je nutná pro ekonomické zhodnocení.

Tabulka 3: Časová náročnost

	Činnost	Časová náročnost
1	Vytvoření Tier Modelu	8 h
2	Nasazení Tier Modelu	20,5 h
3	Nasazení nové politiky hesel	3 h
4	Konfigurace protokolů	19,5 h
5	Propojení domén	3 h
6	Nasazení LAPS	6 h
Celkem		60 h

Celková odhadovaná časová náročnost implementace všech požadavků je 60 hodin. Jelikož jednotlivé činnosti (kromě školení) vyžadují pouze jeden interní zdroj, kterým se rozumí IT specialista provádějící změny, není v této části řešeno alokování zdrojů. Dalším důvodem je fakt, že na provedení změn je dostatek prostoru a mateřská společnost je schopna akceptovat případný posun termínů.

3.7.4 Ganttův diagram

Ganttův diagram, ve kterém jsou znázorněny jednotlivé hlavní činnosti a jejich návaznosti, je znázorněn v **Příloha 6**.

3.8 Ekonomické zhodnocení

V této části se budu zabývat ekonomickým zhodnocením. Vyčíslení nákladů nebude moc rozsáhlé, protože všechen požadovaný software pro realizaci požadavků již společnost vlastní (Windows Server), nebo se jedná o freeware (LAPS). Ve vyčíslení nákladů tedy budu rozebírat pouze projektové odměny, které se promítnou ve mzdových nákladech, které v našem případě budou i celkové náklady. Školení bude provádět IT specialista, který bude implementovat změny, proto není obsaženo v nákladech. Mateřská společnost si za konzultace ani společné úkoly nic neúčtuje, protože jsou v jejím zájmu, z tohoto důvodu tato položka v rámci vyčíslení nákladů také není zahrnuta.

3.8.1 Vyčíslení nákladů

V závislosti na časové náročnosti jsme schopni pomocí hodinové sazby za odměny vypočítat projektové odměny.

Tabulka 4: Projektové odměny

Časová náročnost	60 h
Odměna za hodinu	500 Kč
Projektové odměny	30 000 Kč

Hrubé projektové odměny činí 30 000 Kč.

Tabulka 5: Celkové náklady

Projektové odměny	30 000 Kč
Sociální pojištění	7 440 Kč
Zdravotní pojištění	2 700 Kč
Mzdové náklady	40 140 Kč
Celkové náklady	40 140 Kč

Celkové náklady na projekt činí 40 140 Kč.

3.8.2 Návratnost investice do zabezpečení

Teoretickou návratnost investice se pokusím vyčíslit na příkladu pomocí ukazatele Return On Security Investment. V příkladu budu počítat s dopady a pravděpodobností nejčastějších typů útoků jako jsou například útoky typu Man-in-the-middle, Malware, Brute force a Social engineering.

Zavedená opatření jsou proti zmíněným typům útoků velmi účinné, z tohoto důvodu je hodnota efektivity zavedených opatření u těchto typů relativně vysoká. Méně obvyklé sofistikované útoky v příkladu rozebírat nebudu, zavedená opatření proti nim mají samozřejmě menší efektivitu, ale jsou také velmi specifické a mají menší výskyt.

Zmíněné útoky mohou způsobit různé škody od lehkého poškození dat až po únik citlivých informací a poškození infrastruktury. V očekáváné finanční ztrátě v případě incidentu zahrnuji všechny známé faktory, výsledná potenciální cena ztráty tedy zahrnuje významné dopady.

Management stanovil, že náklady na jeden den mimo provoz se pohybují kolem hranice 600 000 Kč, tato částka se každým dalším dnem mimo provoz výrazně zvyšuje. Odhadovaná doba potřebná k obnově infrastruktury v případě vážného incidentu jsou 3 dny, náklady na 3 dny mimo provoz jsou odhadovány na 2 100 000 Kč. Další náklady spojené s vážnějším incidentem (zahrnuje únik informací, pokuty a další) jsou odhadovány na 800 000 Kč. Celková očekávaná ztráta v případě realizace incidentu je tedy 2 900 000 Kč.

Určit roční míru výskytu incidentu je složitý proces, který vyžaduje pečlivou analýzu dat a faktorů ovlivňujících bezpečnost. Tato míra se každým dnem zvyšuje, protože útoků a hrozeb přibývá. V rámci příkladu budu počítat s roční mírou výskytu incidentu 0,6.

$$SLE = 2\ 900\ 000\ Kč$$

$$ARO = 0{,}6$$

$$ALE = 2\ 900\ 000 \times 0{,}6 = 1\ 740\ 000\ Kč$$

Roční očekávaná ztráta zahrnující jednotkovou očekávanou ztrátu a roční míru výskytu incidentu je 1 740 000 Kč. Jak již bylo zmíněno, zavedená opatření jsou proti zvoleným typům útoku velmi efektivní, v příkladu tedy budeme počítat, že zavedená opatření redukují míru rizika zmíněných útoků o 75 %.

$$MR = 75\ \%$$

$$MLR = 1\ 740\ 000 \times 0{,}75 = 1\ 305\ 000\ Kč$$

Finančně vyjádřená redukce ztráty je 1 305 000 Kč, zavedená opatření tedy redukují finanční ztráty o velmi významnou částku.

$$\text{ROSI} = \frac{1\,305\,000 - 40\,140}{40\,140} = 31{,}51 => 3151\ \%$$

Očekávaná návratnost investice do bezpečnostních opatření je 3151 %. Zmíněné výstupy jsou pouze kvalifikovaný odhad, skutečné hodnoty vstupů mohou nabývat rozdílných hodnot. Navzdory tomuto faktu se investice jednoznačně vyplatí realizovat. I kdyby hodnoty vstupů byly výrazně nižší, vzhledem k nízkým nákladům by byly výstupy i tak přesvědčivé.

3.9 Přínosy

Hlavní přínos zavedení nových bezpečnostních standardů je samozřejmě zvýšení úrovně bezpečnosti v organizaci. Zavedená bezpečnostní opatření výrazně snižují rizika úspěšných útoků, některé z nich také snižují i jejich případné dopady. Zavedená opatření tedy snižují nebo eliminují potenciální finanční dopady mezi které patří například ztráty vzniklé z narušení provozu, ztráty zákazníků nebo ztráty vzniklé z porušení smluvních podmínek. To stejné platí i pro nefinanční dopady mezi které patří například poškození dobrého jména organizace, ztráta důvěry zákazníků, potenciální právní řízení a sankce ze strany regulátorů.

Dalším přínosem navrhovaného řešení může být například rozvoj zaměstnanců IT oddělení. Rozšiřování znalostí v kontextu bezpečnosti, která je v dnešní době čím dál více rozebírané téma, může vést k osobnímu rozvoji zaměstnanců, který povede k zvýšení jejich motivace a touze po dalším osobním rozvoji.

Závěr

Cílem této diplomové práce bylo vytvořit návrh na implementaci základních bezpečnostních standardů mateřské společnosti. Požadavky se týkaly převážně Active Directory, nebo s ní nějakým způsobem souvisely.

V první části jsem se věnoval teorii potřebné k realizaci analýzy současného stavu a vlastního návrhu řešení.

V analýze současného stavu jsem stručně představil anonymizovanou společnost, posoudil současný stav bezpečnosti a představil požadavky mateřské společnosti. Ze současného stavu vyplývalo, že úroveň bezpečnosti je velmi nízká a konfigurace v doméně i organizační politiky jsou nastaveny špatně.

Hlavní částí této práce byl vlastní návrh řešení, ve kterém jsem podrobně popsal a odůvodnil vlastní návrhy řešení a doporučení týkající se technické stránky implementace požadavků. Dále jsem v rámci této kapitoly navrhnul a objasnil management zavádění zahrnující definici a výběr hlavních činností pro sledování a dalších faktorů. Na závěr návrhu jsem se věnoval ekonomickému zhodnocení, ve kterém jsem vyčíslil náklady a zpracoval návratnost investice.

Zavedená opatření výrazně zvyšují úroveň bezpečnosti v organizaci, díky tomu také výrazně snižují riziko spojené s nejčastějšími typy útoků. Na základě výstupů z ekonomického zhodnocení můžeme konstatovat, že zavedená opatření jsou také velmi efektivní a mají velmi významné přínosy v poměru s náklady na jejich zavedení. Návratnost investice je tedy velmi vysoká a má široké spektrum přínosů od snižování rizika a dopadů až po potenciální zlepšení motivace a rozvoj zaměstnanců.

Výstupem této práce je kompletní návrh na implementaci bezpečnostních standardů mateřské společnosti obsahující technickou stránku, management zavádění i ekonomické zhodnocení.

Seznam použitých zdrojů

1. SMITH, Ben a Brian KOMAR. *Zabezpečení systému a sítě Microsoft Windows*. Přeložil David KRÁSENSKÝ, přeložil Anna RYCHETSKÁ. Brno: Computer Press, 2006. ISBN 978-80-251-1260-1.
2. STANEK, William R. *Microsoft Windows Server 2012: kapesní rádce administrátora*. Přeložil Jiří HUF. Brno: Computer Press, 2015. ISBN 9788025138175.
3. SANTHOSH, Sivarajan. *Getting Started with Windows Server Security*. Birmingham: Packt Publishing, 2015. ISBN 1784398721.
4. JORDAN, Krause. *Mastering Windows Server 2019*. 2nd edition. Birmingham: Packt Publishing, 2019. ISBN 978-1789804539.
5. FRANCIS, Dishan. *Mastering Active Directory*. 3rd ed. Birmingham: Packt Publishing, 2021. ISBN 978-1801070393.
6. KOLOUCH, Jan, Pavel BAŠTA a Josef POŽÁR. CyberSecurity: Cyber security glossary. Třetí aktualizované vydání. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-34-8.
7. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
8. Dokumentace Microsoft Learn: *Microsoft Learn* [online]. [cit. 2023-02-03]. Dostupné z: https://learn.microsoft.com/en-us/
9. SVOZILOVÁ, Alena. *Projektový management*. 2., aktualiz. a dopl. vyd. Praha: Grada, 2011. Expert (Grada). ISBN 978-80-247-3611-2.
10. ENISA: *Introduction to Return on Security Investment* [online]. [cit. 2023-01-19]. Dostupné z: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment
11. Projektove.cz: *Ganttův diagram* [online]. [cit. 2023-01-21]. Dostupné z: https://www.projektove.cz/vlastnosti/ganttuv-diagram

Seznam zkratek

AD	Active Directory
OU	Organizational Unit
GPO	Group Policy Object
T0	Tier 0
T1	Tier 1
T2	Tier 2
DC	Domain Controller
GC	Global Catalog
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
RSAT	Remote Server Administration Tools
FGPP	Fine-Grained Password Policy
IP	Internet Protokol
LDAP	Lightweight Directory Access Protocol
TGT	Ticket Granting Ticket
TGS	Ticket Granting Server
SMB	Server Message Block
ACL	Access Control List
ACE	Access Control Entry
GPMC	Group Policy Management Console
ADAC	Active Directory Administrative Center
ADUC	Active Directory Users and Computers
ADSS	Active Directory Sites and Services
ADDT	Active Directory Domains and Trusts
LAPS	Local Admin Password Solution
DS	Datové Schránky
IT	Information Technology
SCCM	System Center Configuration Manager

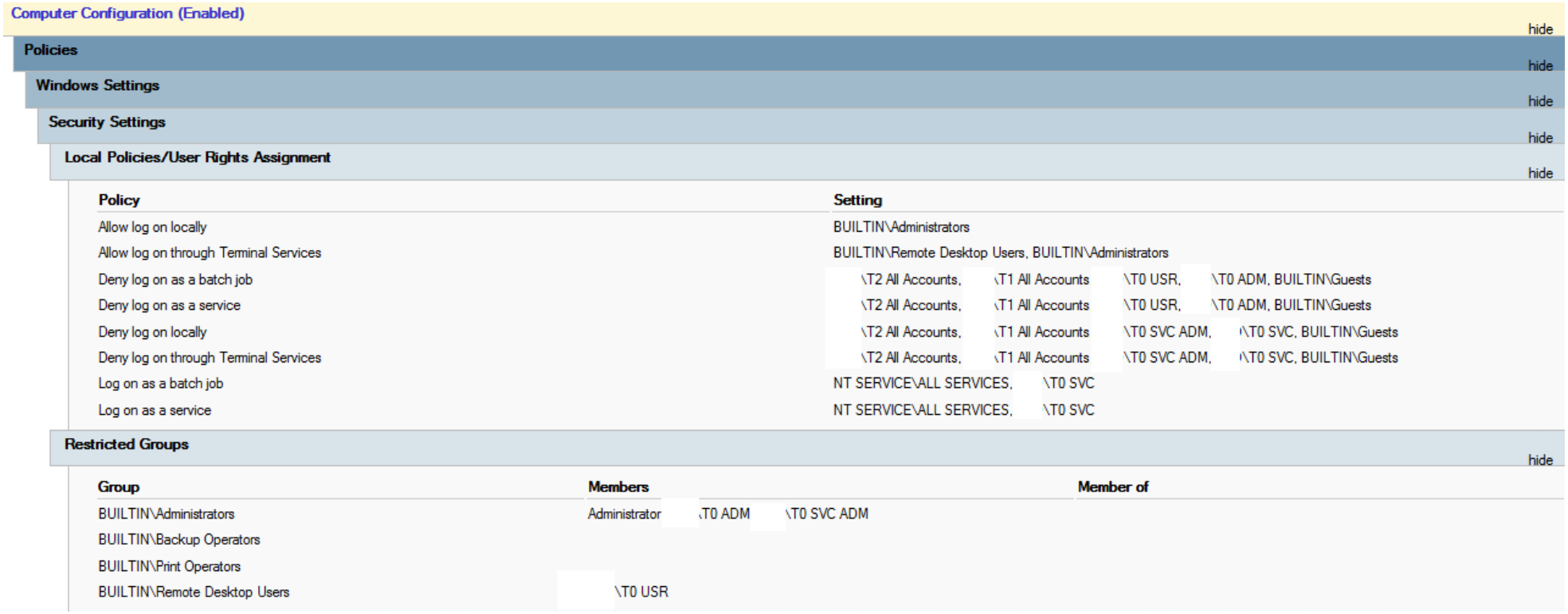
MECM	Microsoft Endpoint Configuration Manager
LLMNR	Link-Local Multicast Name Resolution
ROSI	Return On Security Investment
SLE	Single Loss Expectancy
ARO	Annual Rate of Occurrence
ALE	Annual Loss Expectancy
MR	Mitigation Ratio
MLR	Monetary Loss Reduction
FSMO	Flexible Single Master Operations

Seznam obrázků

Seznam tabulek

Seznam příloh

Příloha 1: T0 GPO



Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

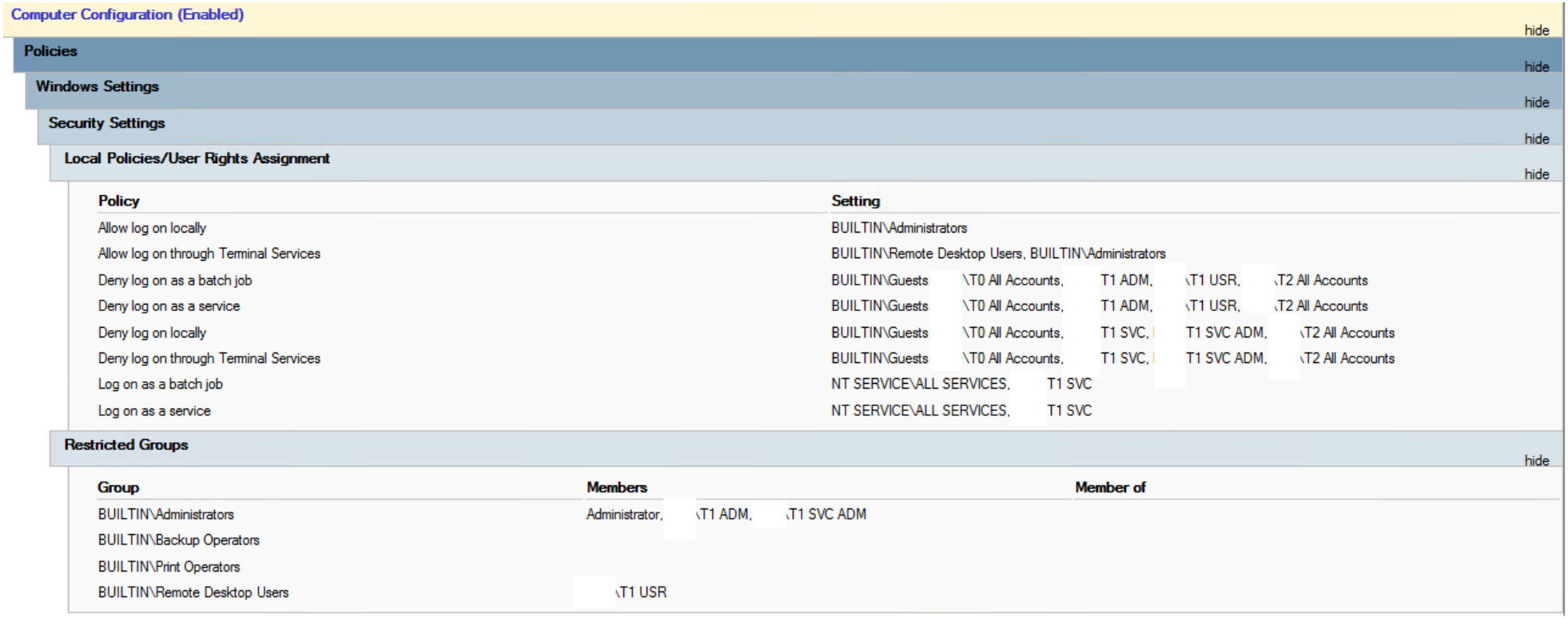
Local Policies/User Rights Assignment hide

Policy	Setting
Allow log on locally	BUILTIN\Administrators
Allow log on through Terminal Services	BUILTIN\Remote Desktop Users, BUILTIN\Administrators
Deny log on as a batch job	\T2 All Accounts, \T1 All Accounts \T0 USR, \T0 ADM, BUILTIN\Guests
Deny log on as a service	\T2 All Accounts, \T1 All Accounts \T0 USR, \T0 ADM, BUILTIN\Guests
Deny log on locally	\T2 All Accounts, \T1 All Accounts \T0 SVC ADM, \T0 SVC, BUILTIN\Guests
Deny log on through Terminal Services	\T2 All Accounts, \T1 All Accounts \T0 SVC ADM, \T0 SVC, BUILTIN\Guests
Log on as a batch job	NT SERVICE\ALL SERVICES, \T0 SVC
Log on as a service	NT SERVICE\ALL SERVICES, \T0 SVC

Restricted Groups hide

Group	Members	Member of
BUILTIN\Administrators	Administrator \T0 ADM \T0 SVC ADM	
BUILTIN\Backup Operators		
BUILTIN\Print Operators		
BUILTIN\Remote Desktop Users	\T0 USR	

Příloha 2: T1 GPO



Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

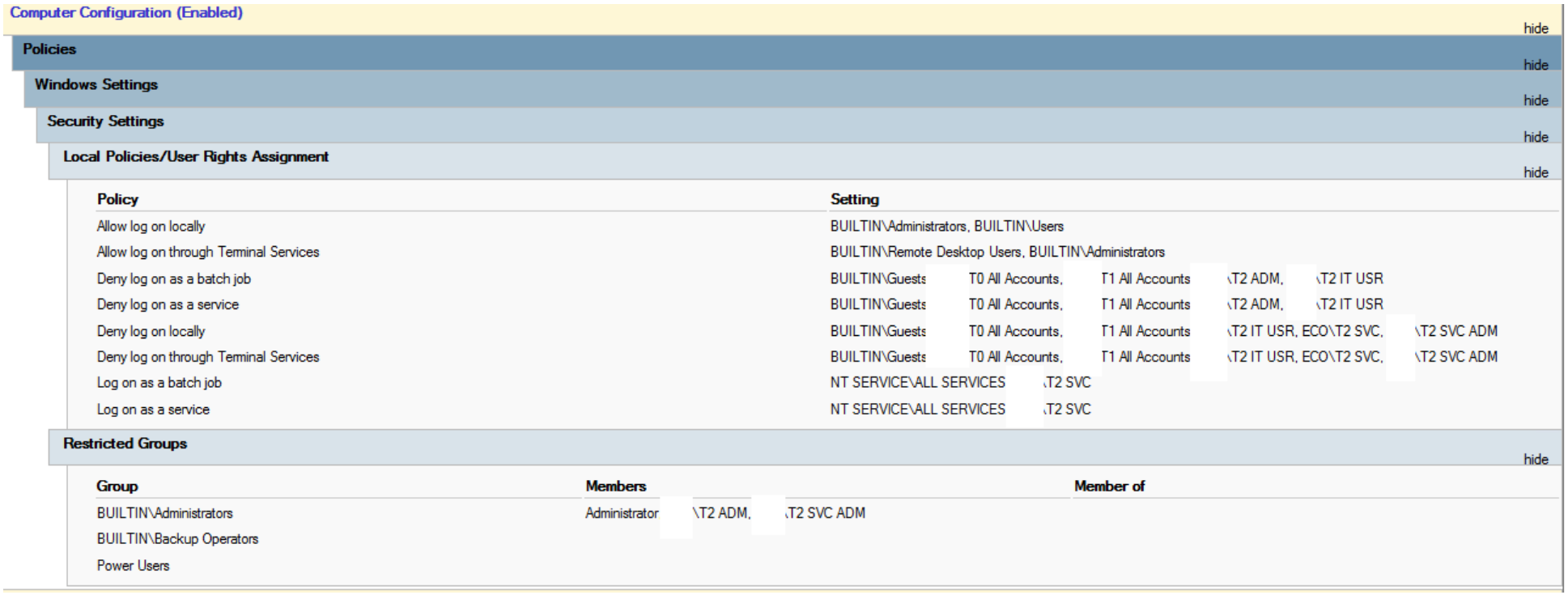
Local Policies/User Rights Assignment hide

Policy	Setting
Allow log on locally	BUILTIN\Administrators
Allow log on through Terminal Services	BUILTIN\Remote Desktop Users, BUILTIN\Administrators
Deny log on as a batch job	BUILTIN\Guests \T0 All Accounts, T1 ADM, \T1 USR, \T2 All Accounts
Deny log on as a service	BUILTIN\Guests \T0 All Accounts, T1 ADM, \T1 USR, \T2 All Accounts
Deny log on locally	BUILTIN\Guests \T0 All Accounts, T1 SVC, T1 SVC ADM, \T2 All Accounts
Deny log on through Terminal Services	BUILTIN\Guests \T0 All Accounts, T1 SVC, T1 SVC ADM, \T2 All Accounts
Log on as a batch job	NT SERVICE\ALL SERVICES, T1 SVC
Log on as a service	NT SERVICE\ALL SERVICES, T1 SVC

Restricted Groups hide

Group	Members	Member of
BUILTIN\Administrators	Administrator, \T1 ADM, \T1 SVC ADM	
BUILTIN\Backup Operators		
BUILTIN\Print Operators		
BUILTIN\Remote Desktop Users	\T1 USR	

Příloha 3: T2 GPO



Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

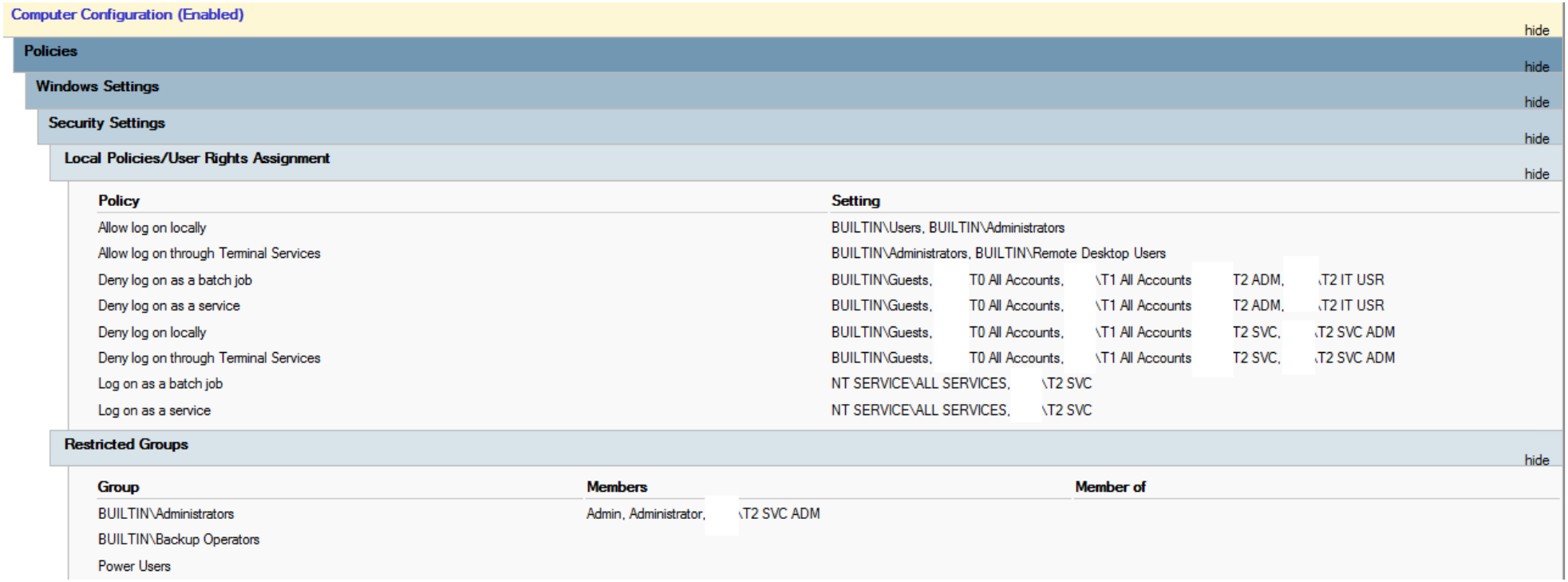
Local Policies/User Rights Assignment hide

Policy	Setting
Allow log on locally	BUILTIN\Administrators, BUILTIN\Users
Allow log on through Terminal Services	BUILTIN\Remote Desktop Users, BUILTIN\Administrators
Deny log on as a batch job	BUILTIN\Guests T0 All Accounts, T1 All Accounts \T2 ADM, \T2 IT USR
Deny log on as a service	BUILTIN\Guests T0 All Accounts, T1 All Accounts \T2 ADM, \T2 IT USR
Deny log on locally	BUILTIN\Guests T0 All Accounts, T1 All Accounts \T2 IT USR, ECO\T2 SVC, \T2 SVC ADM
Deny log on through Terminal Services	BUILTIN\Guests T0 All Accounts, T1 All Accounts \T2 IT USR, ECO\T2 SVC, \T2 SVC ADM
Log on as a batch job	NT SERVICE\ALL SERVICES \T2 SVC
Log on as a service	NT SERVICE\ALL SERVICES \T2 SVC

Restricted Groups hide

Group	Members	Member of
BUILTIN\Administrators	Administrator \T2 ADM, \T2 SVC ADM	
BUILTIN\Backup Operators		
Power Users		

Příloha 4: T2 ADM GPO



Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

Local Policies/User Rights Assignment hide

Policy	Setting
Allow log on locally	BUILTIN\Users, BUILTIN\Administrators
Allow log on through Terminal Services	BUILTIN\Administrators, BUILTIN\Remote Desktop Users
Deny log on as a batch job	BUILTIN\Guests, T0 All Accounts, \T1 All Accounts T2 ADM, \T2 IT USR
Deny log on as a service	BUILTIN\Guests, T0 All Accounts, \T1 All Accounts T2 ADM, \T2 IT USR
Deny log on locally	BUILTIN\Guests, T0 All Accounts, \T1 All Accounts T2 SVC, \T2 SVC ADM
Deny log on through Terminal Services	BUILTIN\Guests, T0 All Accounts, \T1 All Accounts T2 SVC, \T2 SVC ADM
Log on as a batch job	NT SERVICE\ALL SERVICES, \T2 SVC
Log on as a service	NT SERVICE\ALL SERVICES, \T2 SVC

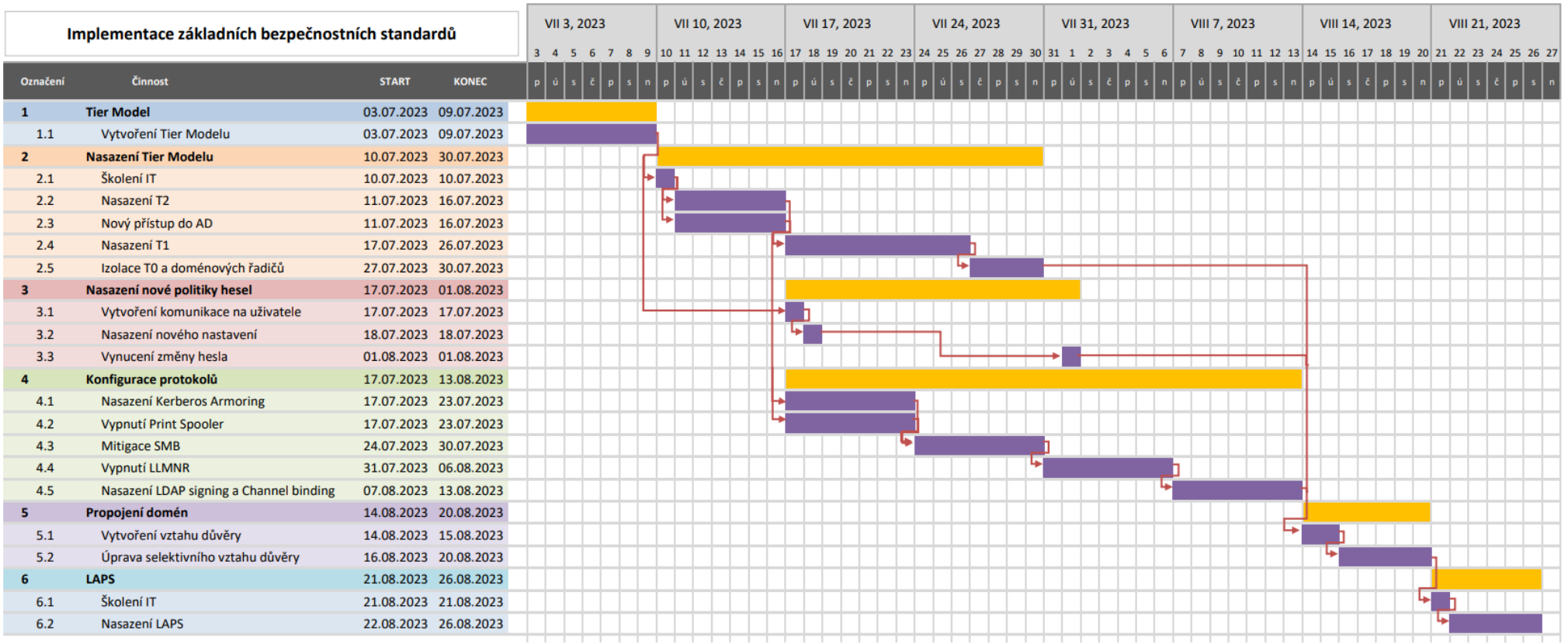
Restricted Groups hide

Group	Members	Member of
BUILTIN\Administrators	Admin, Administrator, \T2 SVC ADM	
BUILTIN\Backup Operators		
Power Users		

Příloha 5: Harmonogram hlavních činností

	Činnost	Trvání	Termín zahájení	Termín ukončení	Zodpovědná osoba	Popis
1	Tier Model	7	03.07.2023	09.07.2023	Jakub Valný	Všechny činnosti spojené s tvorbou Tier Modelu
1.1	Vytvoření Tier Modelu	7	03.07.2023	09.07.2023	Jakub Valný	Vytvoření Tier Modelu
2	Nasazení Tier Modelu	21	10.07.2023	30.07.2023	Jakub Valný	Všechny činnosti spojené s nasazením Tier Modelu
2.1	Školení IT	1	10.07.2023	10.07.2023	Jakub Valný	Školení zaměstnanců IT jak používat účty, nový přístup do AD
2.2	Nasazení T2	6	11.07.2023	16.07.2023	Jakub Valný	Vytvoření účtů, testování a ostré nasazení
2.3	Nový přístup do AD	6	11.07.2023	16.07.2023	Jakub Valný	Instalace a konfigurace serveru pro přístup do AD
2.4	Nasazení T1	11	17.07.2023	27.07.2023	Jakub Valný	Vytvoření účtů, testování, úpravy, vytvoření aplikací a ostré nasazení
2.5	Izolace T0 a doménových řadičů	4	27.07.2023	30.07.2023	Jakub Valný	Vytvoření nových účtů, smazání starých administrátorských účtů a reset KRBTGT
3	Nasazení nové politiky hesel	16	17.07.2023	01.08.2023	Jakub Valný	Všechny činnosti spojené s nasazením nové politiky hesel
3.1	Vytvoření komunikace na uživatele	1	17.07.2023	17.07.2023	Jakub Valný	Příprava a odeslání mailové komunikace o změnách
3.2	Nasazení nového nastavení	1	17.07.2023	17.07.2023	Jakub Valný	Vytvoření a nasazení nových politik
3.3	Vynucení změny hesla	1	01.08.2023	01.08.2023	Jakub Valný	Vynucení hesla u účtů, které nemají změněné heslo
4	Konfigurace protokolů	28	17.07.2023	13.08.2023	Jakub Valný	Všechny činnosti spojené s úpravou konfigurace protokolů a služeb
4.1	Nasazení Kerberos Armoring	7	17.07.2023	23.07.2023	Jakub Valný	Úprava základních doménových politik
4.2	Vypnutí Print Spooler	7	17.07.2023	23.07.2023	Jakub Valný	Vytvoření potřebné politiky a restart doménových řadičů nebo manuální vypnutí služby
4.3	Mitigace SMB	7	24.07.2023	30.07.2023	Jakub Valný	Vytvoření potřebné politiky, testování a ostré nasazení
4.4	Vypnutí LLMNR	7	31.07.2023	06.08.2023	Jakub Valný	Vytvoření potřebné politiky, testování a ostré nasazení
4.5	Nasazení LDAP signing a Channel binding	7	07.08.2023	13.08.2023	Jakub Valný	Vytvoření potřebné politiky, testování a ostré nasazení
5	Propojení domén	7	14.08.2023	20.08.2023	Jakub Valný	Všechny činnosti spojené s propojením domén společností
5.1	Vytvoření vztahu důvěry	2	14.08.2023	15.08.2023	Jakub Valný, Administrátor mateřské společnosti	Vytvoření vztahu důvěry na obou stranách a validace
5.2	Úprava selektivního vztahu důvěry	6	15.08.2023	20.08.2023	Jakub Valný, Administrátor mateřské společnosti	Konfigurace všech potřebných oprávnění v rámci selektivního vztahu důvěry
6	LAPS	7	21.08.2023	27.08.2023	Jakub Valný	Všechny činnosti spojené s nasazením nástroje LAPS
6.1	Školení IT	1	21.08.2023	21.08.2023	Jakub Valný	Školení zaměstnanců IT jak se dostat k heslům lokálních správců
6.2	Nasazení LAPS	6	22.08.2023	27.08.2023	Jakub Valný	Instalace nástroje, konfigurace, testování a nasazení

Příloha 6: Ganttův diagram činností



Implementace základních bezpečnostních standardů			
Označení	Činnost	START	KONEC
1	**Tier Model**	03.07.2023	09.07.2023
1.1	Vytvoření Tier Modelu	03.07.2023	09.07.2023
2	**Nasazení Tier Modelu**	10.07.2023	30.07.2023
2.1	Školení IT	10.07.2023	10.07.2023
2.2	Nasazení T2	11.07.2023	16.07.2023
2.3	Nový přístup do AD	11.07.2023	16.07.2023
2.4	Nasazení T1	17.07.2023	26.07.2023
2.5	Izolace T0 a doménových řadičů	27.07.2023	30.07.2023
3	**Nasazení nové politiky hesel**	17.07.2023	01.08.2023
3.1	Vytvoření komunikace na uživatele	17.07.2023	17.07.2023
3.2	Nasazení nového nastavení	18.07.2023	18.07.2023
3.3	Vynucení změny hesla	01.08.2023	01.08.2023
4	**Konfigurace protokolů**	17.07.2023	13.08.2023
4.1	Nasazení Kerberos Armoring	17.07.2023	23.07.2023
4.2	Vypnutí Print Spooler	17.07.2023	23.07.2023
4.3	Mitigace SMB	24.07.2023	30.07.2023
4.4	Vypnutí LLMNR	31.07.2023	06.08.2023
4.5	Nasazení LDAP signing a Channel binding	07.08.2023	13.08.2023
5	**Propojení domén**	14.08.2023	20.08.2023
5.1	Vytvoření vztahu důvěry	14.08.2023	15.08.2023
5.2	Úprava selektivního vztahu důvěry	16.08.2023	20.08.2023
6	**LAPS**	21.08.2023	26.08.2023
6.1	Školení IT	21.08.2023	21.08.2023
6.2	Nasazení LAPS	22.08.2023	26.08.2023