Bezpečnosť operačného systému MS Windows

It is estimated that ninety-nine per cent of all reported intrusions result through exploitation of known vulnerabilities or configuration errors, for which safeguards and countermeasures were available (NIST SP 800-53)

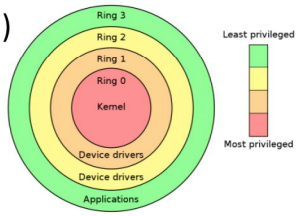
Na základe učebných materiálov doc. Ing. Ladislava Hudeca, CSc. rozšíril a aktualizoval Ing. Martin Pavelka

OS MS Windows

- Najrozšírenejší OS na pracovných staniciach – prečo?
  - Podpora HW, cena, skúsenosti používateľov, administrátorov, možnosť centralizácie správy, dostatok aplikácií, prepojenie na cloudové služby, ...
- Využitie
  - Osobné počítače – samostatné pracovné stanice, s prístupom do LAN a internetu
  - Doménové počítače – využívané v podnikovom a školskom prostredí na centralizáciu prístupových práv, implementovaná adresárová služba LDAP, opatrenia prevádzkového aj bezpečnostného charakteru
  - Servery – Windows Server Desktop Experience / Core Edition, Standard / Datacenter
- Funkcionality a nastavenia OS Windows možno rozdeliť na tri základné druhy:
  - Integrálne – esenciálne súčasti OS Windows, bez ktorých by nebol OS funkčný – napr. zavádzací súbor, registre, knižnice DLL
  - Prevádzkové – funkcie a nastavenia v OS, ktoré spríjemňujú používateľský zážitok – napr. grafické efekty, zvuky, ...
  - Bezpečnostné – funkcie a nastavenia vytvorené primárne s cieľom zaistiť želanú úroveň bezpečnosti – napr. politika hesla (povinnosť zadať heslo), oddelenie používateľského a administrátorského konta a pod.
- Prednáška sa skladá z dvoch častí
  - 1. časť – architektúra OS Windows – opakovanie a rozšírenie poznatkov získaných z prednášok Operačné systémy
  - 2. časť – výklad o konkrétnych nástrojoch v OS Windows, ktoré môžu slúžiť na zaistenie súladu s bezpečnostnými štandardami

Architektúra systému MS Windows

- OS pracuje v dvoch režimoch (podobne ako UNIX)
  - **Používateľský režim** (user mode) – typicky v chránenom okruhu 3 (najnižšom)
  - **Režim kernel** (kernel mode) – typicky v chránenom okruhu 0 (najvyššom)



- Hlavné služby OS vrátane **Windows executive** sa vykonávajú v režime kernel. Executive tiež zahŕňa **Bezpečnostný referenčný monitor** (Security Reference Monitor - SRM), ktorý je zodpovedný za riadenie prístupu.

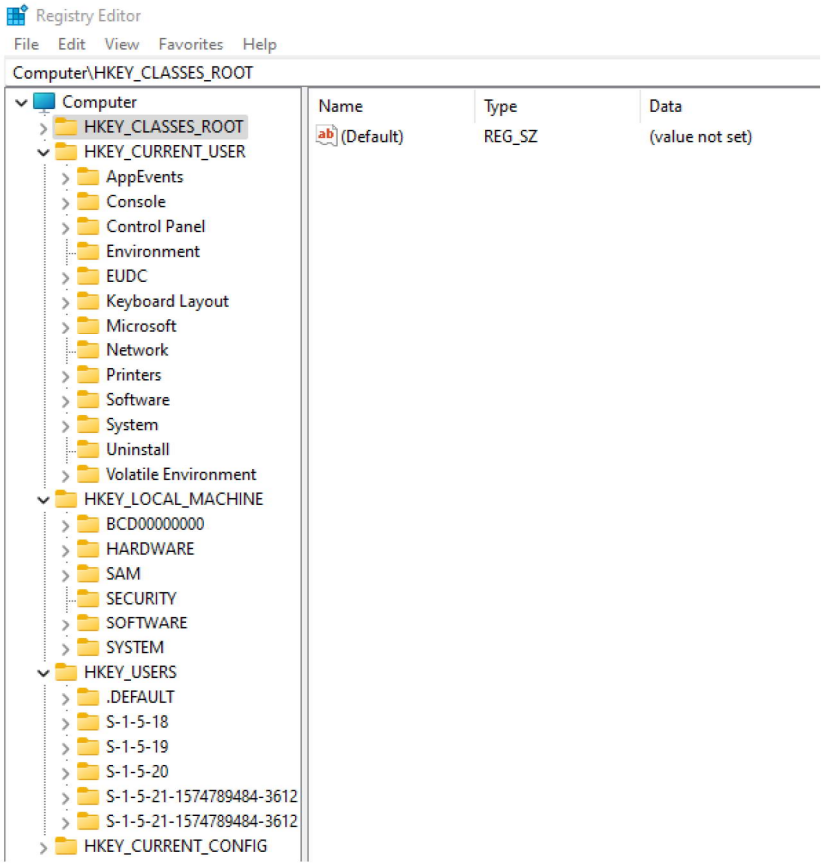
- Používateľský program prostredníctvom API (Application Program Interface) vykonáva volania služieb OS.
- Vrstva Hardware Abstraction Layer (HAL) poskytuje interfejs OS na hardvér.
- Ovládače zariadení (často ovládače tretej strany) sa vykonávajú v režime kernel. Ovládače tretích strán môžu mať **bezpečnostné problémy** (napr. pretečenie vyrovnávacej pamäti), čo môže využiť útočník napr. na získanie plnej kontroly OS.

Registry

- **Registry** je centrálna databáza pre konfiguračné údaje OS

- V registroch sú odložené informácie o nastavení ovládačov, boote, aplikácií
  - Položky databázy sa nazývajú **keys** (kľúče, pozor nie šifrovacie!)
  - Organizujú sa v tzv. hives – ako keby separátne súborové systémy
  - Pomocou **Registry Editor** (regedit.exe, regedt32.exe) je možné modifikovať databázu a zobrazovať položky **pomocou GUI, príp. pomocou príkazu reg v príkazovom riadku a ekvivalentu v PowerShell-i**

Editor Registrov v systéme MS Windows 11



- Na najvyššej úrovni majú Registre OS Windows päť dôležitých preddefinovaných kľúčov:
  - HKEY_CLASSES_ROOT – obsahuje asociáciu na názov rozšírenia súboru, je možné špecifikovať, že .docx súbory budú spracovávané MS Wordom 2019
  - HKEY_CURRENT_USER – obsahuje konfiguračné údaje práve prihláseného používateľa – **aktuálne prihlásený používateľ má možnosť neobmedzeného čítania aj zápisu**, tu si môžu programy typu Outlook, VLC, ... ukladať nastavenia
  - HKEY_LOCAL_MACHINE – obsahuje konfiguračné údaje o lokálnom stroji
  - HKEY_LOCAL_MACHINE\SAM – obsahuje používateľské účty, vrátane ich hešov hesiel a vyrovnávaciu pamäť prihlásení v doméne
  - HKEY_USERS – obsahuje všetky aktívne zavedené používateľské profily na systéme (v podstate HKEY_CURRENT_USER pre každého používateľa)
  - HKEY_CURRENT_CONFIG – obsahuje informácie o hardvérovom profile používanom na lokálnom stroji pri štartovaní systému

Registry

- **Modifikovaním kľúčov registry** môže útočník modifikovať správanie OS
  - Útočník môže nastaviť Debugger – program na ladenie, ktorý sa spustí automaticky pri volaní iného programu (napr. na prihlasovacej obrazovke **nahradiť** nástroje pre hendikepovaných programom cmd.exe, ktorý sa spustí s právami SYSTEM)
  - Kľúč z registry môže ukazovať na lokáciu (path – cesta), kde OS automaticky hľadá určité vykonateľné súbory
  - Ak nastavené prístupové práva k tomuto kľúču sú slabé (prístup zápisu pre Everyone), potom útočník môže modifikovaním kľúča vložiť škodlivý kód
  - Je absolútna nevyhnutnosť chrániť integritu údajov registry, **predovšetkým v doméne**
  - Odstavenie / zakázanie editora registry zo všetkých strojov, ktoré nie sú používané na manažment systému, je dobrá bezpečnostná prax – prostredníctvom skupinových politík
  - Niektoré bezpečnostne relevantné kľúče dokonca nie je možné zmeniť editorom registri, ale iba špecifickou utilitou
  - V prípade potreby je možnosť exportu a importu do registrov (napr. preinštalovanie programu a zálohovanie si jeho aktuálnej konfigurácie) – **opatrnosť pri importovaní – najprv otvorím cez notepad, až potom importujem /merge.**

Služby

- **Paralela s Unix - Daemon**
- Procesy bežiace (spravidla) na pozadí, bez GUI, bez potreby interakcie používateľa, „dlhodobo bežiace procesy“
- Služba = spustiteľný súbor obohatený o funkcionalitu umožňujúcu komunikovať so správcom služieb (HKLM\SYSTEM\CurrentControlSet\Services)
- Spúšťané zvyčajne so štartom OS
- Ovládanie: services.msc
- Viacero stavov:
  - Automatic
  - Automatic – Delayed Start
  - Manual
  - Disabled

PowerShell
- Get-Service
- New-Service
- Restart-Service
- Resume-Service
- Set-Service
- Start-Service
- Stop-Service
- Suspend-Service

- Hardening:
  - Ako možno vypnúť službu?
  - Ktoré služby vieme vypnúť bez ovplyvnenia prevádzky PC pre zlepšenie zabezpečenia?
  - V akom kontexte bežia služby?
  - Kam má prístup kontext služby?

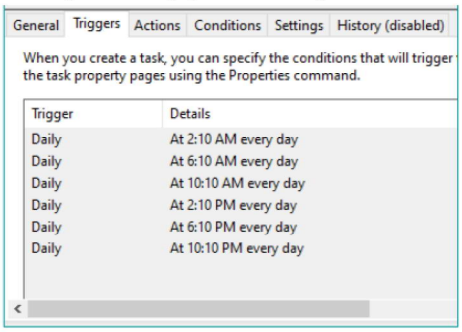
Plánované úlohy

- **Paralela s Unix – CRON JOB**
- Proces spustený pri výskyte určenej udalosti, napr.:
  - Nastala určená hodina/deň/týždeň...
  - Nastala určitá udalosť – Event ID
  - Používateľ sa prihlásil
  - Počítač sa zapol
  - Počítač sa prebudil
- Plánované úlohy na úrovni systému spravujú administrátori, avšak aj bežní používatelia majú (zbytočne) možnosť vytvoriť svoje plánované úlohy
- Podobne ako služby – musíme dbať na KONTEXT
- Možnosti perzistencie – skrývanie či nahrádzanie plánovaných úloh – logická bomba (plánovaná úloha sa môže spustiť aj o týždeň)
- Legitímne využitie – závierky programov, zálohovacie rituály, reakcia na určitú udalosť (event)
- Settings – napr. čo v prípade ak sme zmeškali trigger, NTB na batérií...
- Škodlivé využitie – exfiltrácia, malware, Command and Control a pod.
- Umiestnenie : C:\Windows\System32\Tasks; C:\Windows\SysWOW64\Tasks; C:\Windows\Tasks - jobs

PowerShell

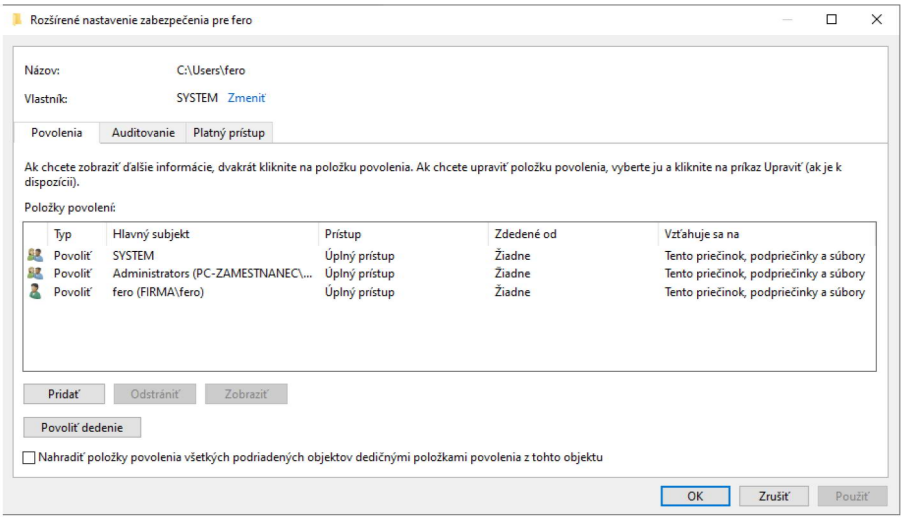
- Get-ScheduledTask
- Get-ScheduledTaskInfo
- New-ScheduledTask
- New-ScheduledTaskAction
- New-ScheduledTaskPrincipal
- New-ScheduledTaskSettingsSet
- New-ScheduledTaskTrigger

Komponenty plánovaných úloh



Riadenie prístupu - komponenty

- Riadenie prístupu v OS Windows je komplexnejšie než je riadenie prístupu v typickom súborovom systéme (objekty sú súbory, kľúče registry, tlačiarne, objekty LDAP, AD, atď).
- OS Windows umožňuje DAC (voliteľné riadenie prístupu) a RBAC (riadenie prístupu založeného na rolách).
- Nástroje na riadenie prístupu v MS Windows sú **skupiny, role a dedenie**.
- **Principals** (pomenované subjekty) v OS sú: **lokálny používateľ, alias, doménový používateľ, skupina alebo stroj**.
  - Subjekty (principals) majú človeku zrozumiteľné **meno** (username) a stroju zrozumiteľné meno **SID** (Security IDentifier)



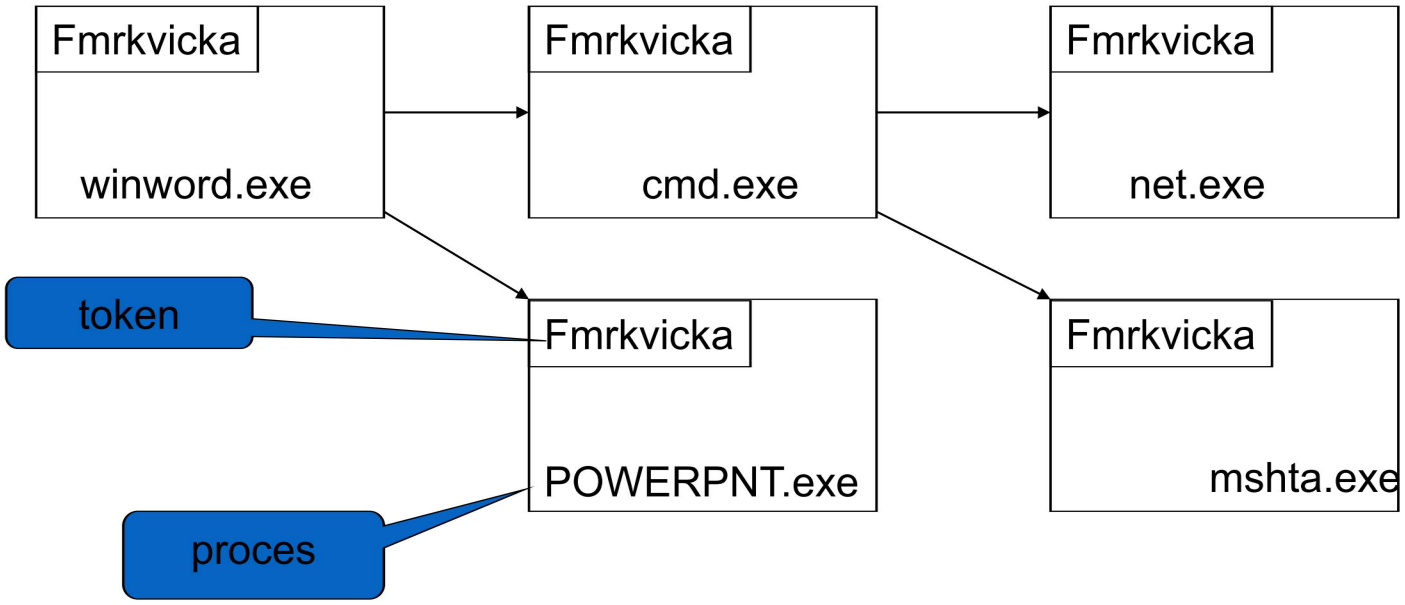
Riadenie prístupu - komponenty

- **Subjekty** sú aktívne entity (nie principals) v operačnom systéme. V OS Windows subjekty sú **Procesy a Vlákna**.
- Bezpečnostné doklady (credentials) procesu alebo vlákna sú uložené v **prístupovom tokene** (access token). Štruktúra prístupového tokenu obsahuje:
  - **User SID, Group and Alias SID** (security identifier) – slúži ako identifikačné a autorizačné atribúty
  - **Privilégiá** – riadi prístup k systémovým zdrojom, obsahuje zjednotenie všetkých privilégií pridelené uvedeným SID
  - **Prednastavenia pre nové objekty** – nový objekt získa prednastavenia podľa rodičovského tokenu, token nezmení členstvo a privilégia
  - **Rôzne** – obsahuje logon session ID a ID tokenu
- **Privilégiá** riadia prístup k systémovým zdrojom.
  - Privilégium je jednoznačne identifikované jeho programovým menom
  - Privilégiá sú pridelené používateľom, skupinám a aliasom podľa strojov
  - Privilégiá sú cachované v tokenoch (access tokeny pre procesy a vlákna) ako **LUID** (Locally Unique Identifiers)
  - Privilégiá sú iné ako prístupové práva. Typické privilégiá sú: **backup files and directories**, **debug programs**, **shut down the system**

Riadenie prístupu - komponenty

- **Objekty** sú pasívne entity v prístupových operáciách. OS Windows pozná
  - Vykonateľné objekty ako procesy a vlákna
  - Objekty súborového systému ako súbory alebo adresáre
  - Ďalšími objektami sú kľúče registry a zariadenia ako tlačiareň
  - Objekty majú Security Descriptor – **bezpečnostný deskriptor**
- **Bezpečnostný deskriptor** pozostáva z:
  - Owner SID – indikuje vlastníka objektu. Objekty dostávajú vlastníka pri vytváraní. Vlastník je subjekt (principal), ktorý má vždy oprávnenia READ_CONTROL a WRITE_DAC. Vlastníctvo môže byť získané tiež prostredníctvom privilégií (Take ownership of files and other objects).
  - Primary group – je zahrnutá k vôli kompatibilite so štandardom POSIX. Aj napriek tom u sa využíva v špecifických situáciách (predovšetkým v doménovom prostredí)
  - **DACL** – Discretionary Access Control List – určuje komu je pridelený a komu je zamietnutý prístup k objektu.(Toto pole môže byť prázdne alebo nie je zriadené.)
  - SACL – System Access Control List – určuje auditnú politiku pre objekt.
- **Oprávnenie** je autorizácia na vykonanie určitej operácie nad objektom.
  - Oprávnenia sú kódované v 32 bitovej maske.
  - Zobraziť oprávnenia pre súbor je možné kliknutím na *File*, potom na *Properties* a nakoniec na *Security*.

Riadenie prístupu - komponenty



- Štandardne sa programy vykonávajú v bezpečnostnom kontexte prihláseného používateľa. Ilustračná situácia znázorňuje volanie zo škodlivého dokumentu v MS Word.
- Napr. pomocou makra sa otvorí powerpointová prezentácia vložená priamo vo Worde a taktiež príkazový riadok

Zhrnutie

- Subjekt – procesy, vlákna vykonávané v istom používateľskom kontexte (napr. calc.exe)
- Objekt – pasívna entita prístupu – objekt na FS, tlačiareň, registry, AD
- Identifikácia – používateľské meno, login name
- Autentifikácia – spravidla používateľské heslo
- Autorizácia – udelenie prístupu prihlásiť sa na daný stroj, zobraziť danú zložku, kľúč v registroch a pod.
- Audit – zápis udalostí do logu – Event log – GUI nástroj na prezeranie udalostí
- SAM – Security Account Manager – databáza lokálnych kont
- LSA – Local Security Authority – služba zodpovedná za autentifikáciu, autorizáciu, vytvára prístupový token
- Referenčný monitor

Prihlasovací proces do OS Windows

- V SAM – Security Account Manager sú uložené **hešované hodnoty hesiel**, navyše databáza hašovaných hesiel je **zašifrovaná**
  - Predstavuje bezpečnostné riziko ak sa útočník dokáže dostať do databázy hešovaných hesiel
  - **Prostredníctvom pozmenenia databázy** je možné odstrániť heslo do OS (vybrané Linuxové distribúcie či iné Boot-USB-Tools toto umožňujú bez hlbšej znalosti používateľa)

- **Každý používateľ** má na lokálnom stroji svoj **profil,** ktorý sa štandardne nikam inam neukladá, nesynchronizuje. Výnimky nateraz vynechajme.
  - %homedrive%/%users%/%username% , napr. C:\Users\fero\Desktop je plocha používateľa

- Ako posledný krok načítavania OS sa spustí proces winlogon.exe
- Winlogon.exe volá msgina.dll (dynamická knižnica prihlasovacej obrazovky), ktorá zistí zadané údaje
- Winlogon odovzdá údaje službe LSA (Local Security Authority), ktorá podľa konfigurácie zistí či sa budú údaje overovať voči lokálnej databáze alebo na doménovom kontrolóri

- **Príklad rozlíšenia druhu konta pri prihlásení**:

username vs username@domena.local vs domena\username .\username

Lokálne doménové doménové lokálne

- **Pri lokálnom prihlásení sa kontroluje heslo v SAM databáze OS**

- **Pri doménovom prihlásení sa v prípade dostupnosti doménového radiča kontroluje na ňom, v prípade nedostupnosti v nakešovaných prihláseniach v registroch lokálneho stroja**

- Pri úspechu SAM vráti LSA: SID užívateľa, SID všetkých skupín kam používateľ patrí
- LSA vytvorí prístupový token a zapíše prihlásenie do logu (v závislosti od nastavení)

Doménový radič (DC, ADDC)

- Virtuálny (alebo fyzický) stroj s nainštalovaným operačným systémom MS Windows Server (2016, 2019, 2022) a konfigurovanou rolou **active directory domain services**

- Po inštalácií servera tento nie je radičom domény, stáva sa ním až po nakonfigurovaní služieb domény

- Server môže slúžiť ako jediný, resp. hlavný radič domény, tzv. Primary Domain Controller alebo ako ďalší, doplnkový radič domény

- Server môže slúžiť aj ako Read Only Domain Controller, na ktorom nie sú uložené žiadne heslá používateľov – slúži na zrýchlenie prihlásení napr. na vysunutých pracoviskách – **bezpečnostné aspekty**, nakoľko tam nie je cache hesiel pre všetkých

- Použitím viacerých ADDC je možné zaistiť:
  - Plánovanie kapacít (500 používateľov spoliehajúcich sa na jeden radič nie je vhodné)
  - Redundancia
  - Dostupnosť

Administrácia bezpečnosti v OS – prednastavené používateľské kontá

- OS podporuje manažment bezpečnosti prostredníctvom prednastavených kont
  - **Preddefinované kontá** – sú inštalované OS (Administrator, Guest)
  - **Vstavané kontá** – sú inštalované OS, aplikáciou alebo službami
  - **Implicitné kontá** – sú vytvorené implicitne, keď sa pristupuje k sieťovým zdrojom

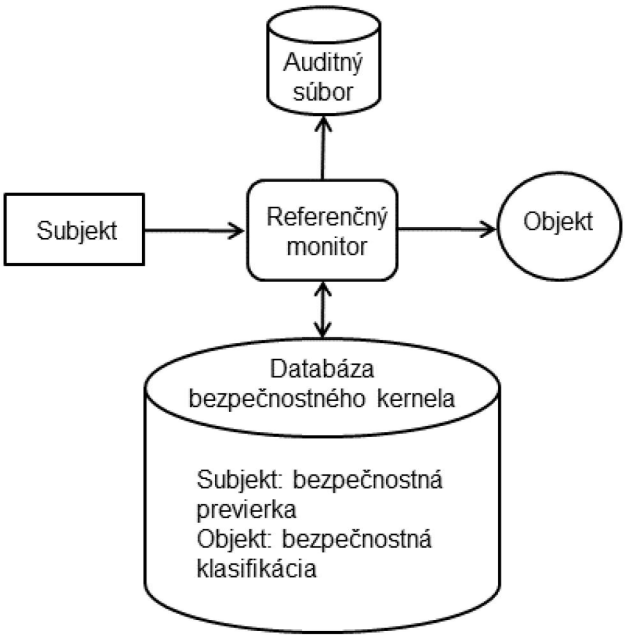
- Prednastavení používatelia a skupiny vytvorené OS môžu byť modifikovaní, ale nie zrušení.
- Prihlásenie do OS je možné cez lokálne alebo doménové konto (alebo Microsoft online účet pre domácnosti, čo však v tejto prednáške zanedbávame)
- Napr. konto **LocalSystem** je vstavané konto na vykonávanie systémových procesov. K tomuto kontu sa môžu prihlásiť iba určité procesy. Nemá profil, pracovnú plochu, ...
- **Preddefinované kontá** Administrator a Guest sú inštalované lokálne.
- Konto **Administrátor**
  - nemôže byť zrušené, môže byť deaktivované
  - má úplný prístup k súborom, adresárom, službám a ostatným zariadeniam
  - ak aj k súboru alebo adresáru pôvodne prístup nastavený nemá, vie si ho nastaviť
  - v doméne je člen skupín Administrators, Domain Admins, Domain Users, Enterprise Admins, Schema Admins a Group Policy Creator Owners
  - v doméne je konto lokálneho administrátora primárne použité pri prvotnej inštalácii systému. Po inštalácii môže byť aktuálny administrátor členom Administrators group
  - Konto **Guest** – spravidla sa nepoužíva, dočasný prístup pre hostí, riziko

Administrácia bezpečnosti v OS – prednastavené používateľské kontá

- **Vstavané skupiny** majú preddefinované používateľské práva a poskytujú ďalšiu úroveň možnosti pri prideľovaní prístupových práv používateľom.
  - Používateľ získa štandardné prístupové práva tým, že sa stane členom takejto vstavanej skupiny
  - Typickým príkladom vstavaných skupín sú Administrators, Backup Operators, User alebo Guest
- Veľa preddefinovaných skupín je inštalovaných v doménach Active Directory. Navyše existujú **implicitné skupiny**, ktoré tiež môžu byť využité na efektívnu definíciu prístupových práv
  - **Everyone** – obsahuje všetkých lokálnych a vzdialených používateľov vrátane Guest, táto skupina môže byť využitá pri udeľovaní alebo odmietnutí prístupových práv všetkým používateľom
  - **Users / Domain Users –** bežní používatelia, každý novovytvorený doménový používateľ je členom Domain Users
  - **Administrators / Domain Admins** – kontá s administrátorskými oprávneniami - univerzálne
  - **System** – je operačný systém
  - **Creator Owner** – je tvorcom alebo vlastníkom súboru alebo iného zdroja

Referenčný monitor - prakticky

- Subjekt
  - Aktívna entita v procese prístupu – žiada o prístup
- Objekt
  - Pasívna entita, ku ktorej sa pristupuje (objekt prístupu)



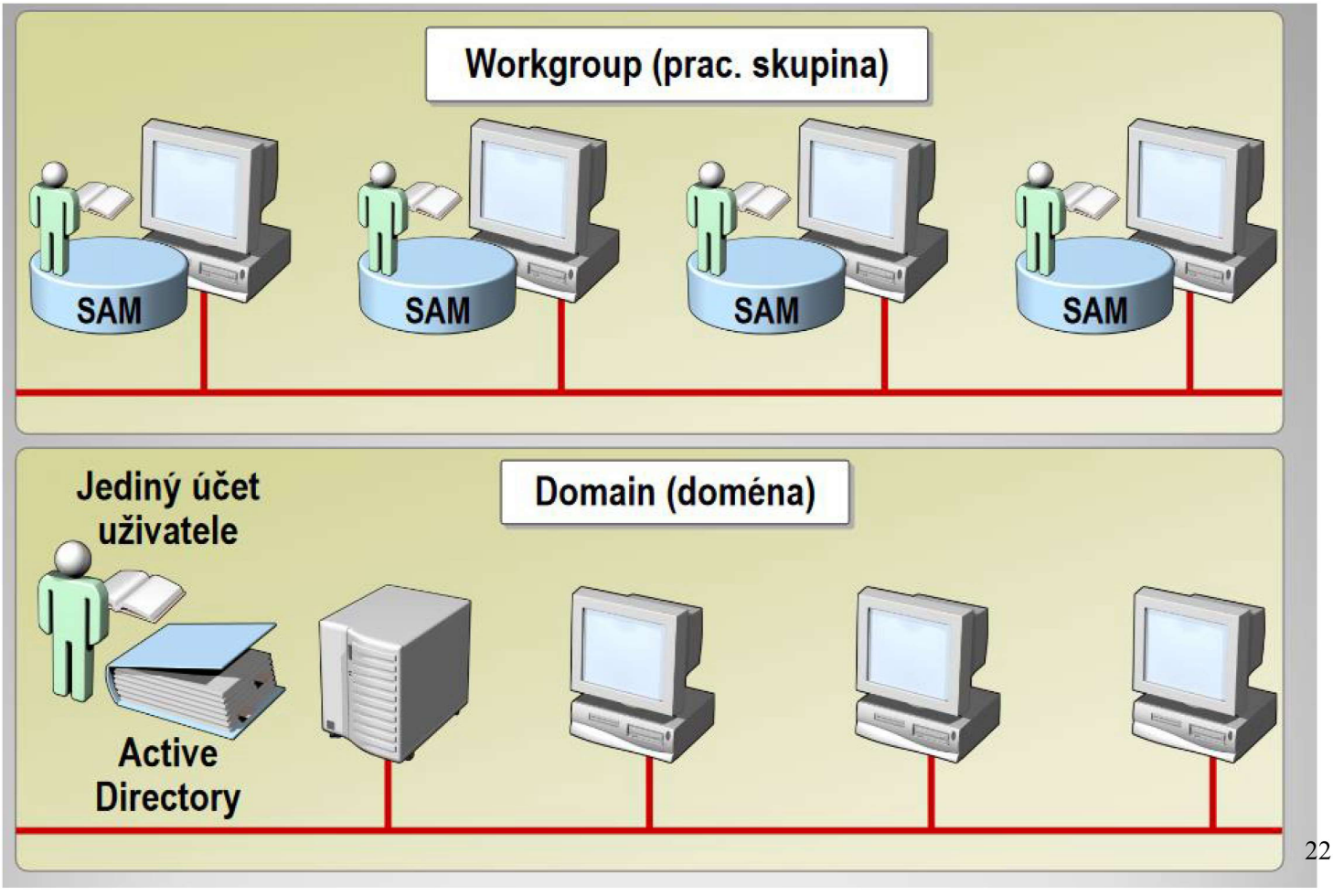
Doména – Active Directory (AD)

- Predstavme si situáciu, kedy administrátor potrebuje reagovať a centrálne ošetriť novoobjavenú zraniteľnosť na všetkých počítačoch fakulty.
- **Samostojace počítače** (samostatné pracovné stanice) s OS Windows sú zvyčajne spravované lokálne svojimi používateľmi, príp. lokálnymi administrátormi – bežný prípad – notebooky v domácnosti
- Vo väčšej organizácii je tento prístup nereálny – nie je možné lokálne spravovať desiatky až stovky pracovných staníc a serverov. Preto je dôležité používanie štruktúrovanejšieho prístupu k **prevádzkovým** a **bezpečnostným** vlastnostiam operačného systému.
- Directory – hierarchická databáza obsahujúca informácie o používateľoch a systémových zdrojoch vrátane identity (RFC 4510-4519), protokol LDAP

Doména – Active Directory (AD)

- Active Directory je implementácia adresárových služieb LDAP firmou Microsoft na použitie v systéme Microsoft Windows, AD beží ako súčasť systému Win Server
- Doména je súbor strojov zdieľajúcich spoločnú databázu používateľských kont a bezpečnostnú politiku
- Umožňuje administrátorom nastavovať politiku, inštalovať programy na mnoho počítačov alebo aplikovať kritické aktualizácie v celej organizačnej štruktúre
- Active Directory svoje informácie a nastavenia ukladá v centrálnej organizovanej databáze (adresári, databáza NTDS.dit)
- Domény môžu vytvárať hierarchiu (predstavme si AD stuba.sk, subdomény FIIT a pridružené domény ucebne.fiit.stuba.sk a zamestnanci.fiit.stuba.sk)
- Používatelia nepotrebujú kontá na individuálnych strojoch v rámci domény

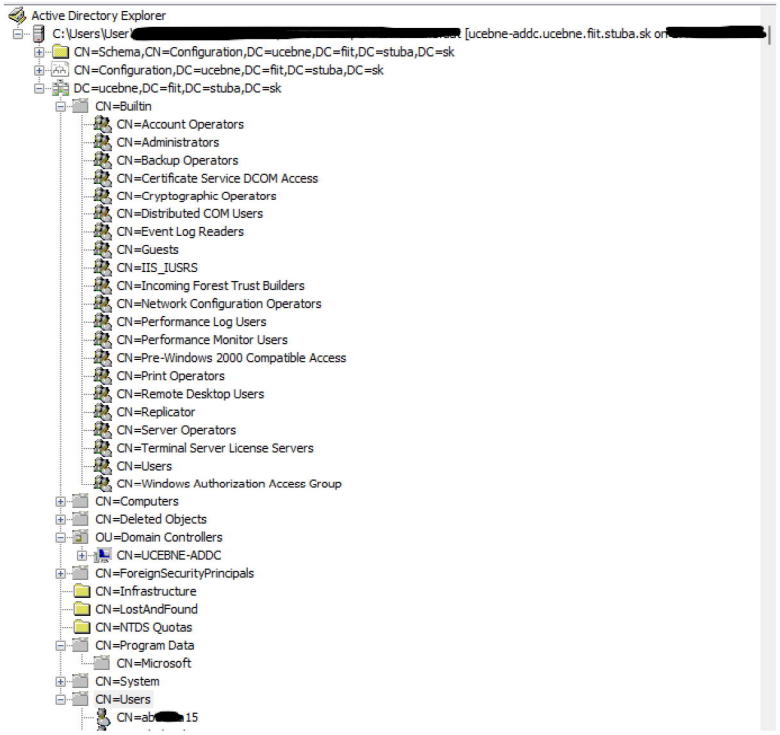
Prihlasovací proces do OS Windows



Active Directory

- Adresárová služba **organizuje objekty v rámci Active Directory**
  - Active Directory môže byť zobrazený ako strom typových objektov
  - Kontajnery (containers) sú predvolené objekty, ktoré obsahujú ďalšie objekty
  - Vedome vytvorené kontajnery sa v terminológií AD nazývajú Organizačné jednotky (OUs)
  - Každý objektový typ má špecifické vlastnosti a jedinečné **GUID** (Globally Unique Identifier)

Obr: Pohľad na štruktúru domény Ucebne.FIIT.stuba.sk



Administrácia bezpečnosti v OS – používateľské konto

- Bezpečnostne relevantné informácie o používateľoch sú uložené **SAM** do databázy používateľských účtov.
- Používateľské účty sú editované pomocou utility *User Manager for Domains*. V používateľskom účte môžu byť definované tieto polia:

Username – jedinečné meno použité pre prihlásenie (*pekna)*

Full name – meno používateľa vlastniaceho konto (účet) *(Viera Pekná)*

Expiration date – prednastavená hodnota je bez exspirácie *(1.1.2023)*

Passsword dates – čas poslednej zmeny hesla, čas exspirácie hesla, čas odkedy by malo byť heslo zmenené

Logon hours and workstations – je možné stanoviť kedy a z ktorej pracovnej stanice sa môže používateľ prihlásiť

User profile path ; logon script name – profil stanovuje prostredie pracovnej stanice používateľa (programové skupiny, sieťové spojenia, farby obrazovky, atď).
Logon script je batch súbor (vykonateľný súbor), ktorý sa automaticky vykoná pri prihlásení používateľa

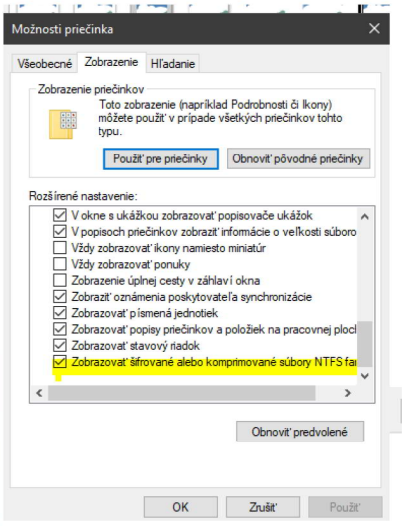
Home directory – je možné špecifikovať domáci adresár používateľa, \\ucebne-files\%username%

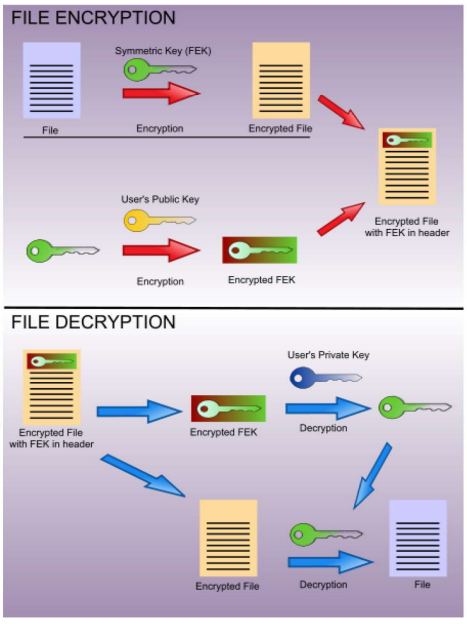
Local and global groups – skupiny, ktorých členom je používateľ.

Bezpečnostné súčasti OS Windwos

Dôvernosť - EFS – šifrovanie súborov NTFS

- Chráni údaje v pokoji a čiastočne údaje pri práci s OS
- Možnosť zašifrovať obsah konkrétneho priečinka
- Napr. zašifrovanie profilu používateľa tak, že ani administrátor nebude mať možnosť zobraziť jeho obsah
- Založené na princípe asymetrickej kryptografie
- Šifrovacie kľúče sú uložené na lokálnom stroji, nutné ich zálohovať
- V prípade poruchy PC a pokusu o čítanie údajov z iného PC toto bez obnovenia privátnym kľúčom nebude možné





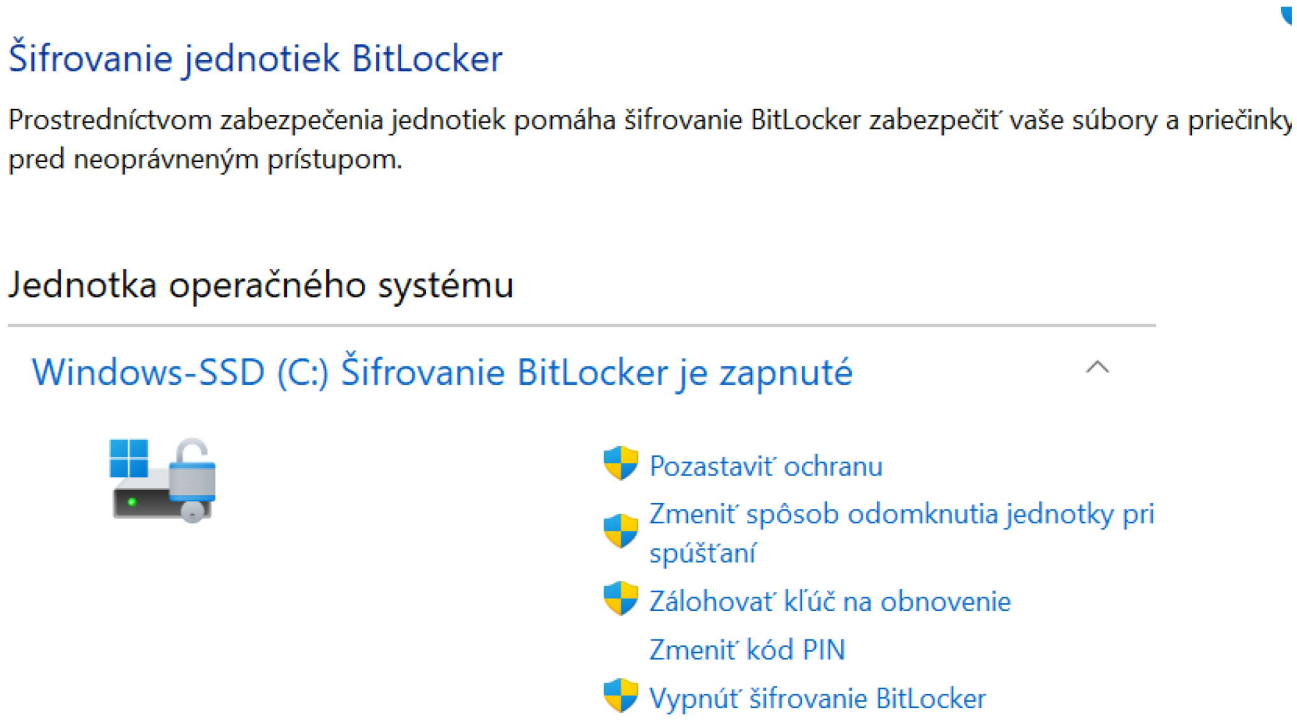
Dôvernosť – Šifrovanie BitLocker

- Chráni údaje v pokoji – bezpečnostné opatrenie proti krádeži – útočník ukradne „iba“ notebook, nie údaje

- Celý pevný disk je zašifrovaný a nepoužiteľný v inom PC (výnimkou je proces obnovy)
- Jedná sa o symetrické šifrovanie pevného disku, pričom šifrovací kľúč sa spravidla ukladá na TPM čip prítomný v počítači a na odomknutie používateľ zadáva PIN kód, resp. používa sa ďalší faktor autentifikácie ešte pred samotným štartom operačného systému.

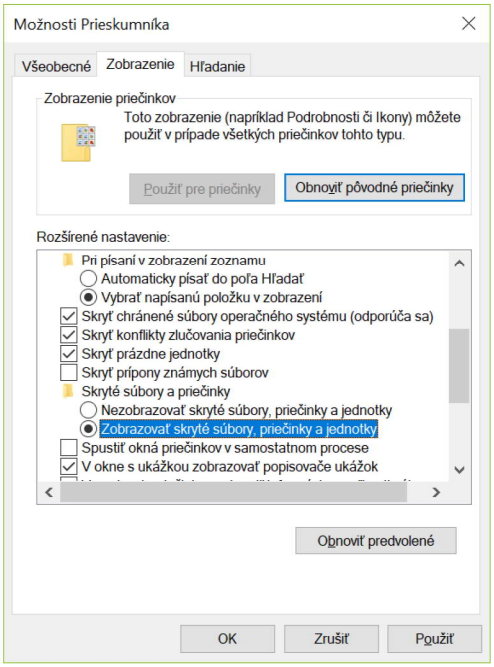
- Zároveň sa pri ustanovení šifrovania vygenerujú záložné kódy, ktoré je potrebné odložiť na iné médium alebo vytlačiť.

- Pri zapnutí PC sa disk rozšifruje:
  - Automaticky – pomocou TPM čipu, najmenej bezpečná možnosť
  - Pomocou zadania PIN kódu – pred zapnutím a načítaním OS sa používateľ vyzve na zadanie číselného kódu
  - Pomocou USB tokenu – používateľ sa vyzve na vloženie USB nosiča so špeciálnym súborom



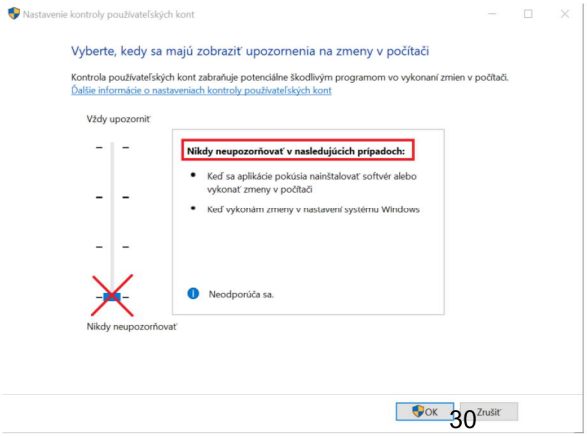
Skryté súbory v OS

- OS používa súbory, ktoré nemusia byť viditeľné pre používateľa
  - Systémové súbory – ich odstránením, pozmenením môžeme znefunkčniť profil používateľa, inštaláciu Windows
  - Skryté súbory – vizuálne ochránime – security by obscurity, na prvý pohľad nie je priečinok či súbor vidieť



UAC

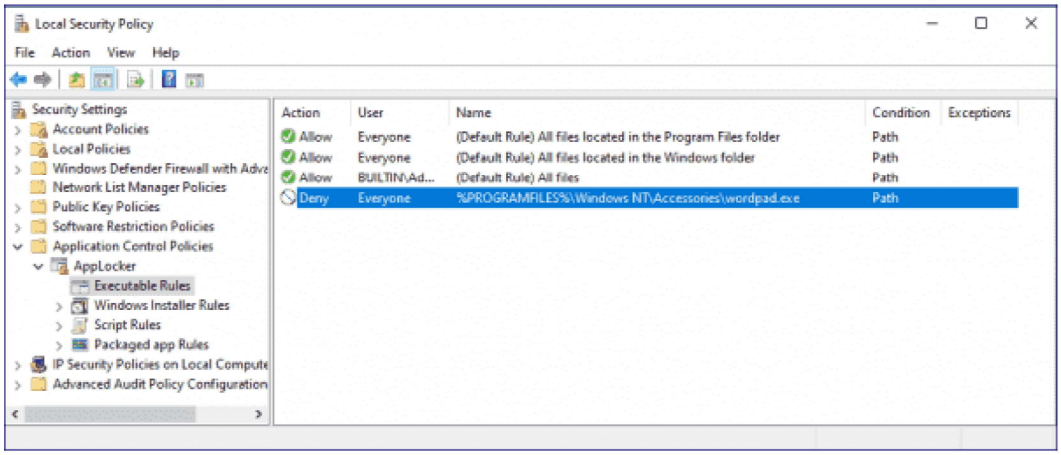
- V OS Windows sú predvolene implementované funkcionality ochrany používateľských kont, User Access Control (UAC)
- Kontrola sa vyvolá pri vykonaním bezpečnostne významných akcií, napr. inštalácií programu, úpravy systémových nastavení a pod.
- V štandardnom nastavení takúto kontrolu môže vyvolať aj bežný používateľ (Domain User) ak sa pokúša vykonať akciu, na ktorú je oprávnený iba administrátor.
- V minulosti takáto funkcionalita nebola v OS implementovaná – Windows XP
- Vyvolaná kontrola v predvolenom nastavení spočíva v stmavení pracovnej plochy a zobrazením modálneho okna v strede obrazovky, na ktorom používateľ musí vyslovene potvrdiť alebo zamietnuť zamýšľanú akciu.
- Je potrebné nastaviť UAC na maximálnu úroveň



Aplikačný whitelisting (po novom „allow list“) Applocker

- Bežný používateľ môže vykonať rozličné príkazy a spustiť utility, ktoré predstavujú bezpečnostné riziko
- Jednou zo schopností používateľa je spustiť akýkoľvek program (neberieme do úvahy AV)
- Aj program v kontexte bežného používateľa môže napáchať veľa škôd:
  - Pozmenenie konfigurácie prehliadačov
  - Pozmenenie nastavení MS Office, Outlook
  - Odoslanie obsahu priečinka „Dokumenty“, „Pracovná plocha“ útočníkovi
  - Zapojenie sa do skupiny pre distribuovaný DDoS útok
  - ... (vymyslite si vlastné...)
- MS Windows Enterprise a Education – umožňuje spustiť iba schválené aplikácie – prostredníctvom funkcionality skupinových politík – „feature“ **AppLocker**

Aplikačný whitelisting - Princíp fungovania

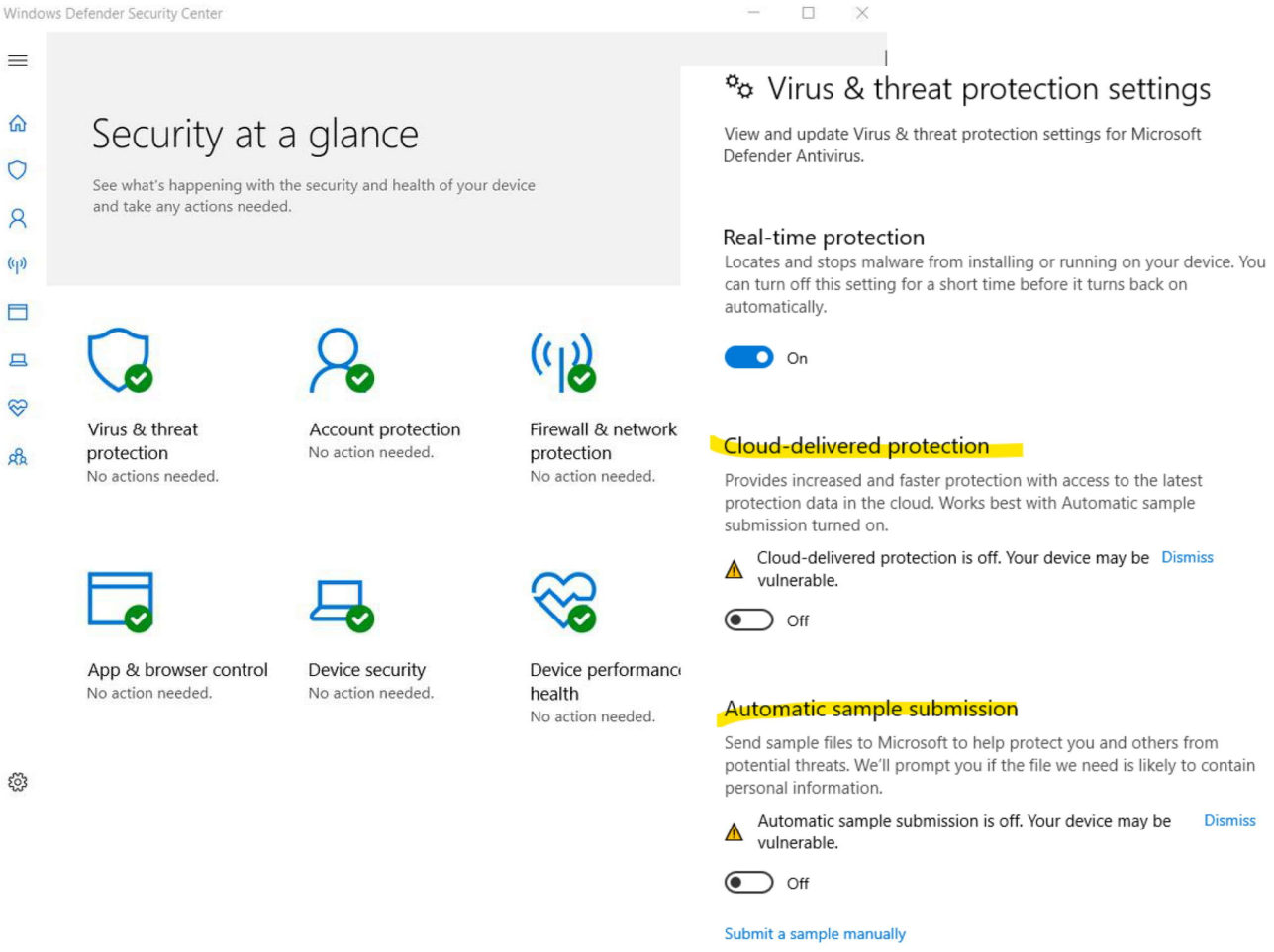


Allow	Everyone	Signed by CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US	Publisher	No

- Povolenie spúšťania aplikácií na základe:
  - Umiestnenia – cesty v súborovom systéme (C:\Windows*)
  - Hešu aplikácie – EXE
  - Podpísania certifikátom – napr. od Microsoftu
- Bezpečnostné riziko – nesprávna konfigurácia, medzery v konfigurácií – napr. Microsoft – je všetko dôveryhodné?
- Riešenie? Sprísnená konfigurácia alebo nástroje tretích strán?

Ochrana proti škodlivému kódu

- Windows 10 a Windows 11 obsahuje predvolený antimalvérový nástroj Windows Defender
- Jedná sa o základný antimalvérový program, poskytuje ochranu v reálnom čase, kontrolu súborového systému na pozadí
- Chýbajú však pokročilé nástroje konkurenčných nástrojov – napr. Bezpečný prehliadač pre online platby, **neobsahuje vlastný firewall** (na rozdiel od niektorých komerčných produktov)
- V predvolenej konfigurácií obsahuje odosielanie informácií do cloudu
- Pre využitie v podnikovom prostredí vyžaduje dodatočné nastavenia
- Pre širokú verejnosť je predvolené nastavenie postačujúce a výhodné, keďže nemusia kupovať ďalší softvér (Defender je už súčasťou ceny OS Windows)



Máme ďalšie možnosti?

- Väčšina sa spolieha na základnú ochranu
- Existujú rozšírené možnosti – možnosť konfigurácie cez GUI (Windows Professional, Enterprise, Education)
- V prípade verzie home – powershell skript

https://github.com/atlantsecurity/windows-hardening-scripts/blob/main/windows-11-hardening-script

:: Stop some of the most common SMB based lateral movement techniques dead in their tracks

powershell.exe Set-MpPreference -AttackSurfaceReductionRules_Ids D1E49AAC-8F56-4280-B9BA-993A6D -AttackSurfaceReductionRules_Actions Enabled

:: Block Office applications from creating child processes

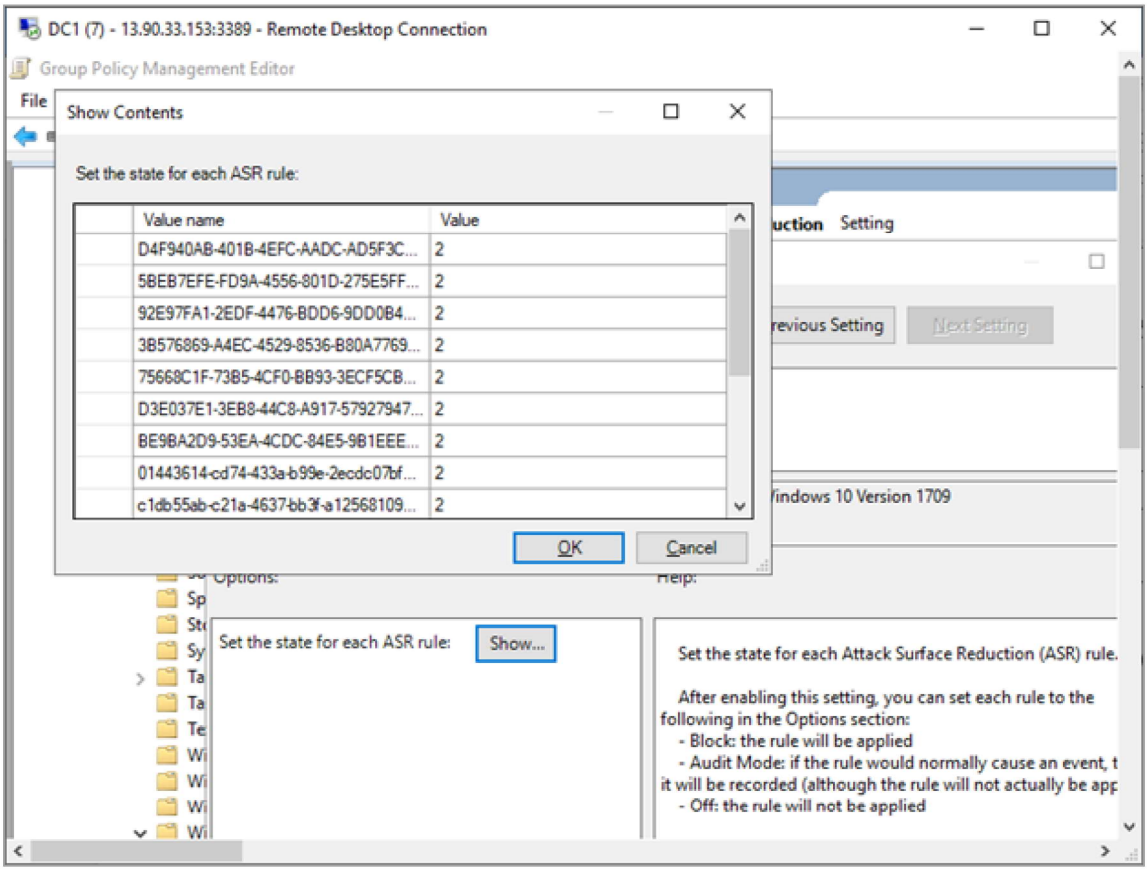
powershell.exe Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EFC-AADC-AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

:: Block Office applications from injecting code into other processes

powershell.exe Add-MpPreference -AttackSurfaceReductionRules_Ids 75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84 -AttackSurfaceReductionRules_Actions enable

:: Block Win32 API calls from Office macro

powershell.exe Add-MpPreference -AttackSurfaceReductionRules_Ids 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B -AttackSurfaceReductionRules_Actions enable



Sieťová bezpečnosť - Windows Firewall

- Predposledná línia obrany koncového uzla (pracovnej stanice či servera)
- Štandardne sú všetky prichádzajúce spojenia blokované a všetky odchádzajúce povolené
- Pre dosiahnutie zabezpečenia je nutné pravidlá skontrolovať a sprísniť (nie všetko čo je predvolene povolené je skutočne potrebné)
- **V súčasnosti tvorí najväčšie riziko povolená odchádzajúca komunikácia**
  - Útočník sa môže snažiť pripojiť sa na Command and Control Server
  - Existujú príkazy a nástroje v OS Windows, ktoré vedia na pozadí stiahnuť súbor, poslať súbor útočníkovi a pod. (napr. pomocou FTP protokolu)
  - Podniková bezpečnostná brána (firewall) chráni iba počas pripojenia do podnikovej siete, nechráni však v prípade
    - Pokusu o útoky na uzly v tej istej podsieti – tam komunikácia prebieha pomocou switchu (MAC adresy) a nie pomocou IP adries
    - Práce na inej sieti, napr. z domu, z verejnej WiFi – bez pripojenia na VPN
    - Pripojenia na VPN sieť, kde nie je vynútený režim plného tunelovania (namiesto full tunel sa využíva split tunneling)
    - Zlej konfigurácie podnikového FW (pochopiteľne)
- Firewall podporuje tri profily – režimy práce
  - Pripojenie do domácej siete, doménovej siete a verejnej siete
    - Možnosť škálovania pravidiel, napr. prichádzajúci ICMP ping povolím len z domény

Sieťová bezpečnosť - Windows Firewall v praxi

- Nepotrebné pravidlá sú zakázané
- V príslušnom sieťovom segmente sú iba ADDC, príp. iba jediný ADDC
- Na HW firewalle je povolená iba potrebná komunikácia z iných segmentov smerom na ADDC
  - Používatelia nemajú dôvod pristupovať na ADDC cez vzdialenú pracovnú plochu
  - Používatelia potrebujú využívať služby domény, autentizovať sa, prezerať zdieľané priečinky, ...
- Na HW firewalle je zakázaná komunikácia smerom do internetu a do iných zón (odchádzajúce spojenia)
  - Na ADDC nie je potrebný internet, súbory si administrátor stiahne na svojej pracovnej stanici
  - Je potrebné však povoliť aktualizácie Windows, aktualizácie antimalvérového riešenia a pod.

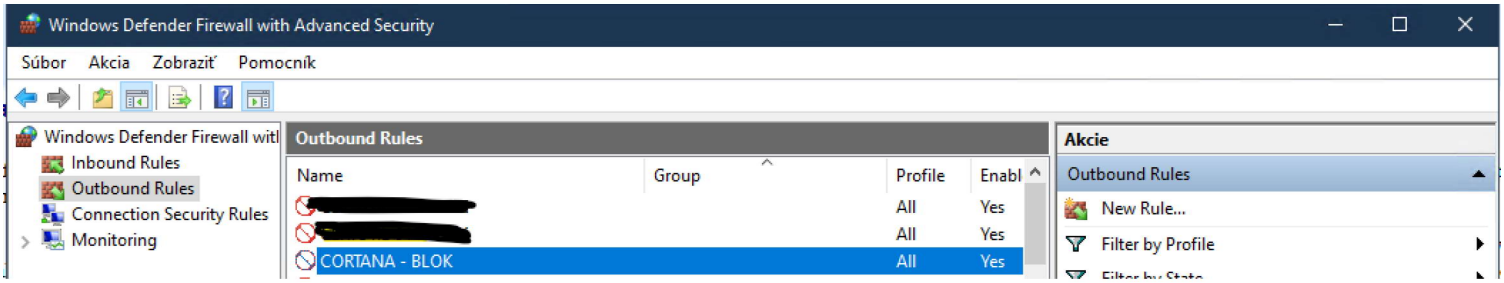
- Primárny ADDC **slúži ako NTP server** pre všetky ostatné servery a pracovné stanice v doméne, časové odlišnosti viac ako 5 min. spôsobia nemožnosť prihlásiť sa do domény

Najčastejšie nedostatky sieťovej bezpečnosti v podmienkach MS Windows

- Je možné pod právami administrátora pozmeniť konfiguráciu Firewallu, aj bez vedomia používateľa (napr. inštalátor – prehliadač Chrome)
- V domácnostiach, menších spoločnostiach nie je sieť segmentovaná – ktokoľvek sa v rámci LAN môže pokúšať prekonať opatrenia na úrovni FW
- Neznalosť administrátorov, nekompetentnosť – firewall býva úplne vypnutý, všetko je povolené (týka sa aj predradených FW)
- Pseudosegmentácia nie je segmentácia, všetko v spoločnej LAN
- Nedostatočná segmentácia a nastavenia FW pre doménové radiče

Príklad – Windows Firewall

- Zákaz odchádzajúcej komunikácie z aplikácie – cloudová služba Cortana
- V doménovom prostredí pravidlá Firewallu spravuje centrálne bezpečnostný správca, používateľ ich nemá možnosť prekonať



Príklad – Windows Firewall

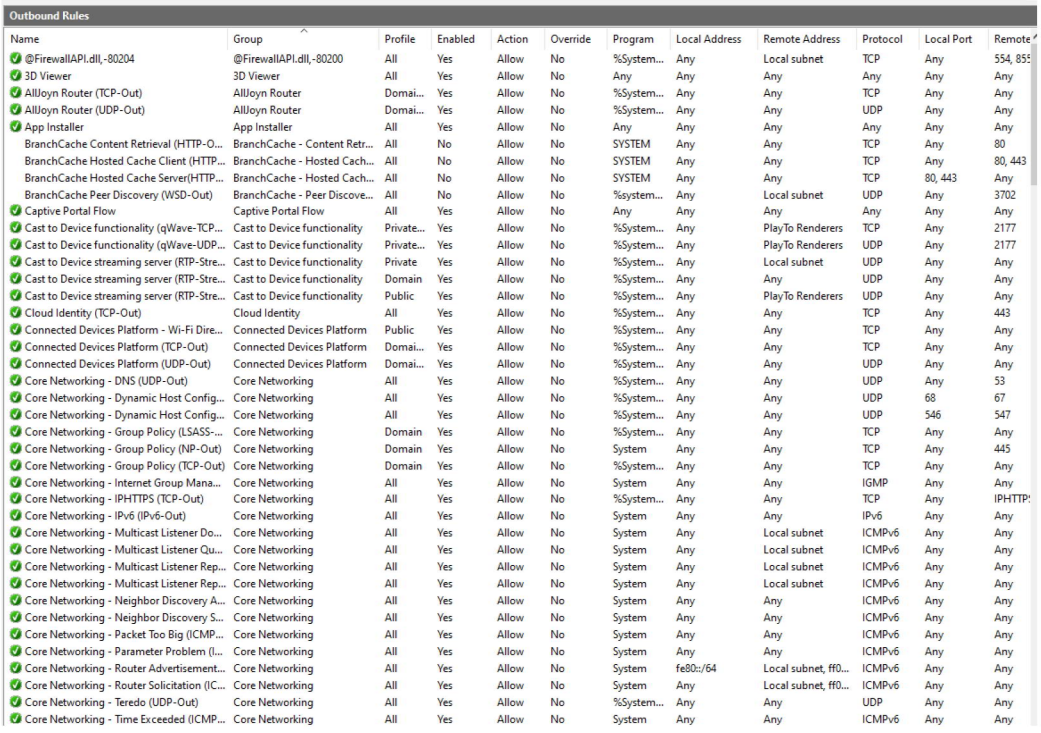
- Predvolené nastavenia Windows Firewall umožňujú využívať rozličné prichádzajúce Cloudové služby
- Predvolené nastavenia Windows Firewall umožňujú odchádzajúce spojenia aplikáciám

- [Protokol mDNS: https://techcommunity.microsoft.com/t5/networking-blog/mdns-in-the-enterprise/ba-p/3275777](https://techcommunity.microsoft.com/t5/networking-blog/mdns-in-the-enterprise/ba-p/3275777)

- mDNS – blokovať – inak by sa dal spraviť útok „poisoning“
- Blokovať port 5353, nastaviť v Chrome a Edge

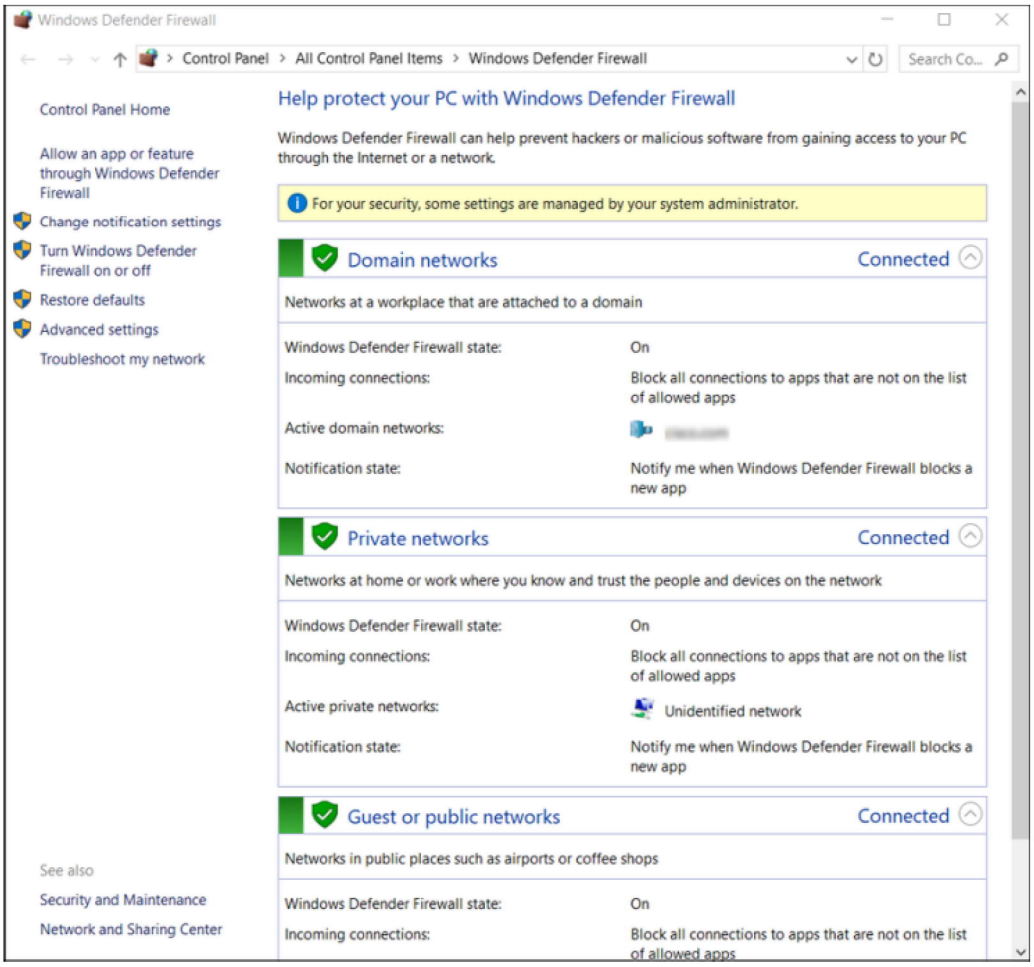
Predvolené pravidlá FW - výber

File and Printer Sharing over SMBDirect (i...	File and Printer Sharing over...	All	No	Allow	No	System	Any	Any	TCP	5445	Any
Google Chrome (mDNS-In)	Google Chrome	All	Yes	Allow	No	C:\Progr...	Any	Any	UDP	5353	Any
Groove Music	Groove Music	Domai...	No	Allow	No	Any	Any	Any	Any	Any	Any
Xbox Game Bar	Xbox Game Bar	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any



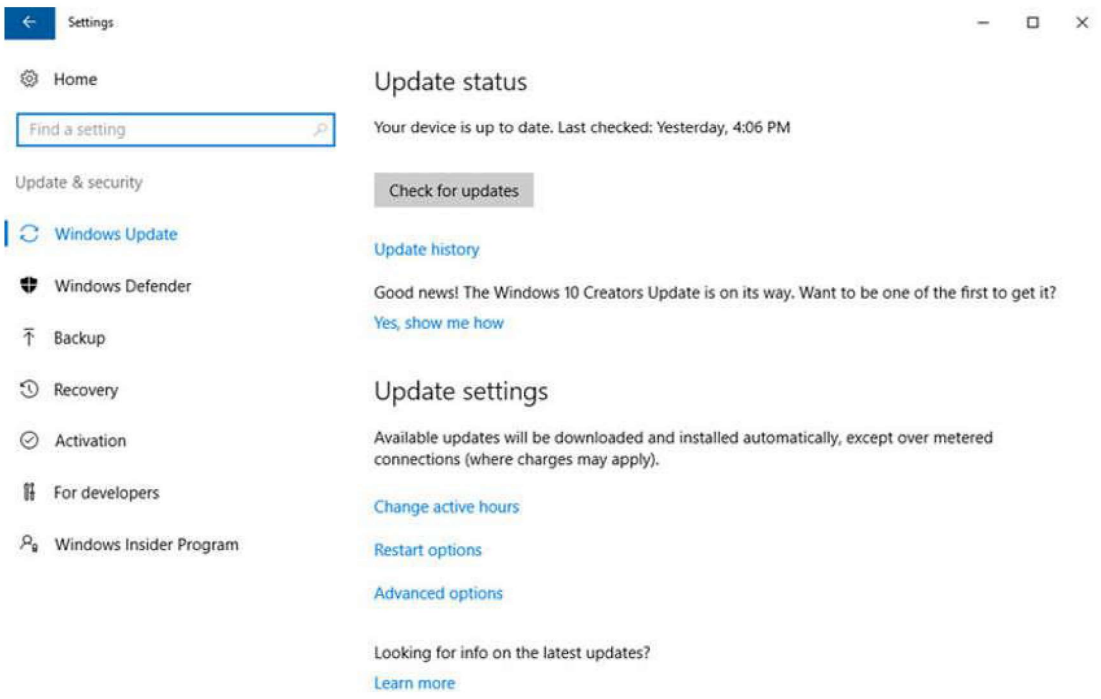
Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote
@FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	All	Yes	Allow	No	%System...	Any	Local subnet	TCP	Any	554, 855
3D Viewer	3D Viewer	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any
App Installer	App Installer	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any	TCP	Any	80
BranchCache Hosted Cache Client (HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	Any	80, 443
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	80, 443	Any
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allow	No	%system...	Any	Local subnet	UDP	Any	3702
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	Any	2177
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	Any	2177
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP	Any	Any
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	Any	Any
Cloud Identity (TCP-Out)	Cloud Identity	All	Yes	Allow	No	%System...	Any	Any	TCP	Any	443
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	Any	53
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68	67
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546	547
Core Networking - Group Policy (LSASS-...	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System	Any	Any	TCP	Any	445
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP	Any	Any
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	TCP	Any	IPHTTP
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6	Any	Any
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Parameter Problem (I...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow	No	System	fe80::/64	Local subnet, ff0...	ICMPv6	Any	Any
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet, ff0...	ICMPv6	Any	Any
Core Networking - Teredo (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any



Riadenie technických zraniteľností – Windows Update, WSUS

- V základnom, predvolenom nastavení sú zapnuté automatické aktualizácie OS
- Používateľ má možnosť odkladu o niekoľko dní
- Odklad nových funkcií
- Nastavené obdobia po ktorých aplikujeme vydanú aktualizáciu
- Na produkčné prostredia nesmieme aplikovať ihneď, musí byť overená časom (alebo otestovaná)
- Možnosť použitia Windows Server Update Services na manažment OS Aktualizácií klientskym PC – neefektívne v prípade notebookov
- Standalone PC – zrušiť možnosť sťahovania updateov z iných PC



Prepojenie na cloudové služby

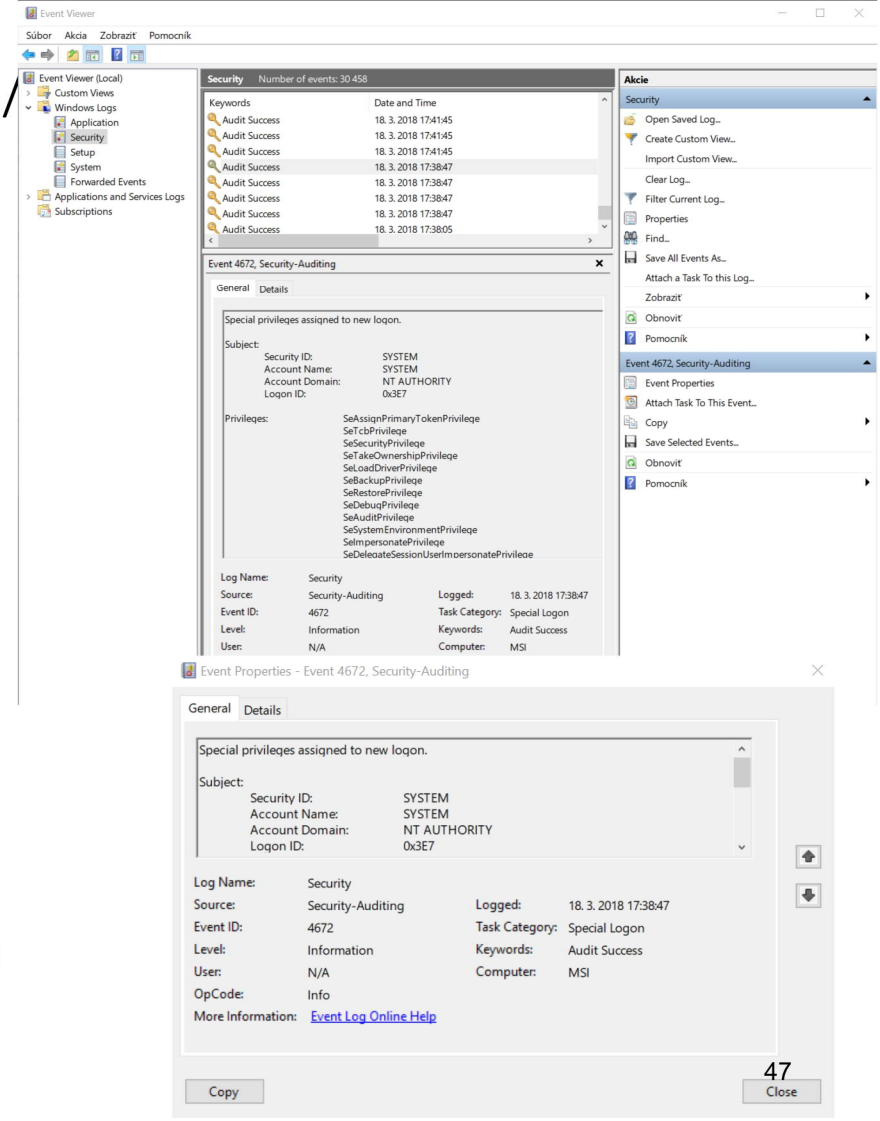
- V súčasnosti podniky upúšťajú od vlastnej infraštruktúry konzervatívnych služieb (napr. mailový server, GIT server a pod.) ale namiesto nich používajú cloudové služby

- OS Windows umožňuje plnohodnotne využívať cloudové služby Microsoft (Office) 365

- Azure Active Directory – „doména v cloude“, lokálne AD je synchronizované online, používatelia využívajú rovnaké prihlasovacie údaje na prístup k emailu, MS Teams, OneDrive, ...
- Bezpečnostné riziko **– heslá používateľov sú uložené v cloude**, možnosť nastaviť spôsob prihlásenia (federácia – máme napr. na Gsuite AIS údaje...)
  - V prípade bezpečnostného incidentu a prelomenia hesla do cloudu môže byť kompromitovaná lokálna infraštruktúra spoločnosti (ADDC)
- **Politika ochrany osobných údajov Microsoftu** – GDPR, Európsky hospodársky priestor
- Intune – nástroj na manažment pracovných staníc a serverov bez využitia lokálneho doménového radiča a skupinových politík

Bezpečnostný monitoring - Event Log / Viewer

- OS zaznamenáva vybrané bezpečnostne významné udalosti do auditného záznamu – Windows Log
- GUI na zobrazenie – Event Viewer
- Možnosť filtrovania, vytváranie vlastných pohľadov a pod.
- Možnosť prispôsobenia, čo sa má zaznamenávať
- V praxi používaný na diagnostiku, **pre účely bezpečnostného monitoringu sú logy presmerované a parsované v SIEM systéme, Syslog...**
- Log je možné zmazať, ale je tam o tom stopa
- Nie je možné prepísať iba konkrétne udalosti v logu



Záver

- Akokoľvek bezpečnostne výborne nastavený OS (hardening), šikovný administrátor a financie **nechránia** pred elementárnymi chybami používateľov

- Na fotografií vytvorenej autorom je prihlasovacie heslo k PC v obchodnom dome

Ďalšie zdroje pre samoštúdium

- Metodika pre systematické zabezpečenie ITVS

https://www.csirt.gov.sk/wp-content/uploads/2021/08/MetodikaZabezpeceniaIKT_v2.1.pdf

- Hardening príručky Australia Cyber Defense

https://www.cyber.gov.au/acsc/government/system-hardening-guidance

- NIST / Stig štandardy

https://ncp.nist.gov/checklist/629

- Materiály na stránkach csirt, NBÚ, SK-Cert, NÚKIB (CZ)

https://www.csirt.gov.sk/

- Windows Server Administrator Fundamentals, študijný materiál na certifikačné skúšky

https://docentinrete.files.wordpress.com/2012/05/manuale-2008-98-365-windowsserver.pdf