

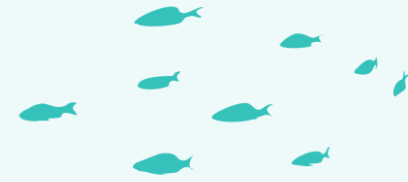
Jak se bezpečnost změnila, ale hesla zůstala v plaintextu



David Buřinský

System Engineer, System Security

david.burinsky@alef.com



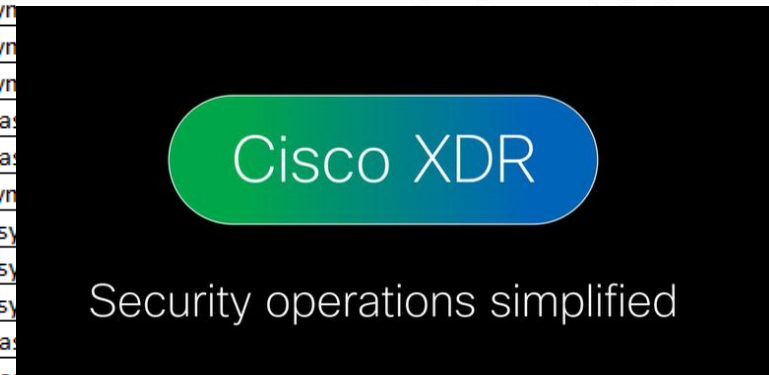
Vývoj bezpečnosti

Bezpečnostní principy

- Windows 11
 - Credential guard
 - TPM čip
- MFA
- XDR řešení
- Šifrování
- GDPR, ISO, NIS2
- Zero Trust

Algorithm	Type	Status	Key Size	Notes
RC4	Symmetric	Deprecated	128 bits	Weak due to biases in keystream
3DES	Symmetric	Deprecated	168 bits	Weak due to meet-in-the-middle attack
IDEA	Symmetric	Deprecated	128 bits	Not widely used
MD5	Hash	Deprecated	128 bits	Weak due to collision attacks
SHA-1	Hash	Deprecated	160 bits	Weak due to collision attacks
DES	Symmetric	Deprecated	56 bits	Weak due to small key size
RSA	Asymmetric	Active	1024, 2048, 4096 bits	Standard for digital signatures and encryption
ECC	Asymmetric	Active	160, 224, 256 bits	More efficient than RSA for the same security level
ElGamal	Asymmetric	Active	1024, 2048, 4096 bits	Used in PGP and other protocols
SHA-256	Hash	Active	256 bits	Standard for digital signatures and hashing
SHA-3	Hash	Active	256 bits	More secure than SHA-2
Diffie-Hellman	Key Exchange	Active	1024, 2048, 4096 bits	Used for secure key exchange
AES	Symmetric	Active	128, 192, 256 bits	Standard for encryption and decryption
Blowfish	Symmetric	Active	64, 128, 160 bits	Fast and secure
Twofish	Symmetric	Active	128, 192, 256 bits	Successor to Blowfish, considered secure
ChaCha20	Symmetric	Active	256 bits	High performance; used in modern protocols like TLS 1.3

Zero Trust Principle



Verify explicitly

Use least privileged access



**HESLO V
ČITELNÉ PODOBĚ**

RDP

**CREDENTIAL
GUARD**

Vzdálený přístup

Teorie

- **Remote Desktop Protocol**
 - Klient-server vzdálené ovládání počítače
 - mstsc.exe
- **Mimikatz**
 - Benjamin Delpy
 - Silný nástroj pro extrakci uživatelských údajů z Windows systémů
 - Eskalace privilegií
 - Penetrační testování

```
mimikatz 2.2.0 x64 ( x + v
PS C:\tools\mimikatz_trunk\x64> .\mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # ts::mstsc
!!! Warning: false positives can be listed !!!

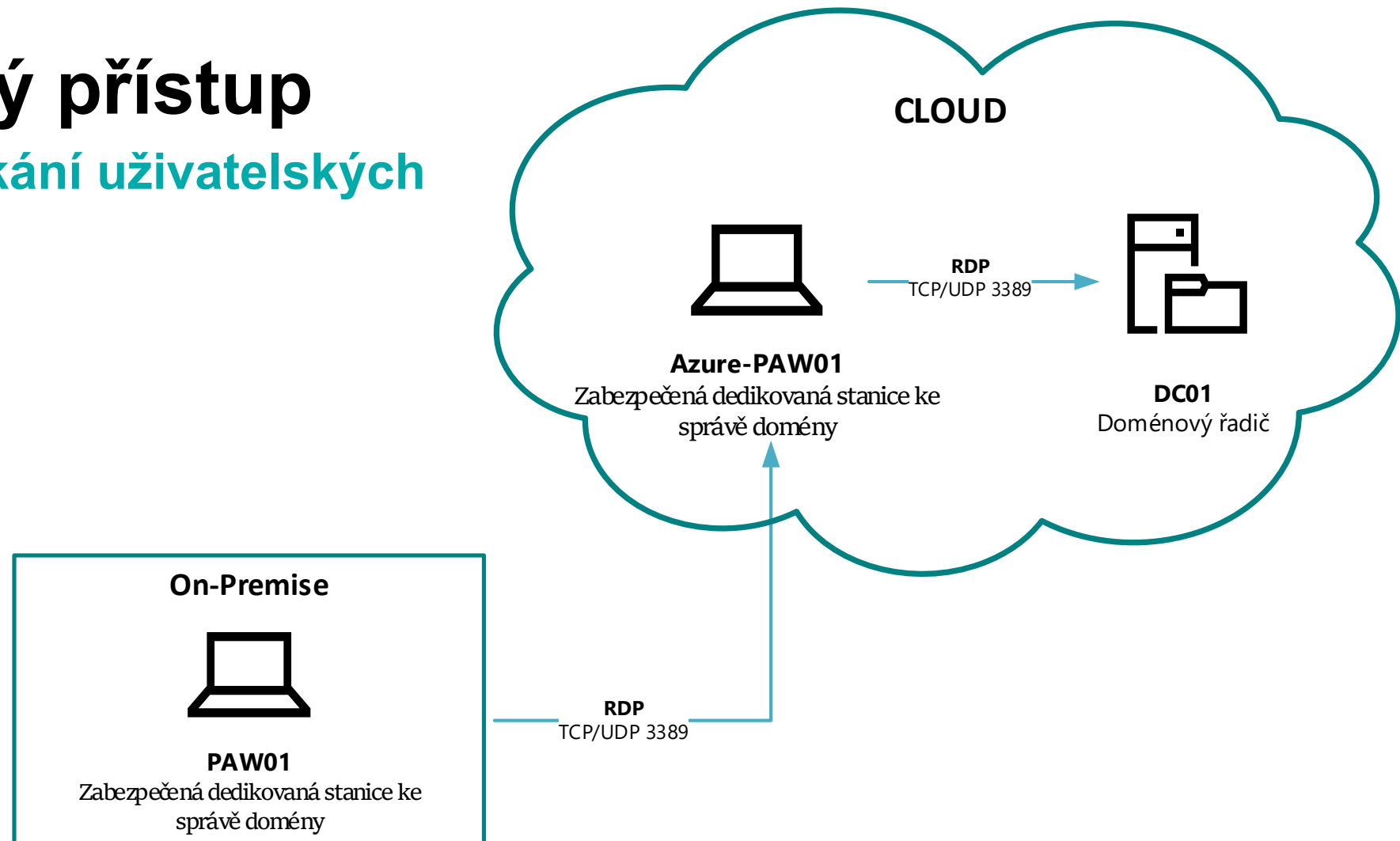
| PID 8608      mstsc.exe (module @ 0x00000000004DF7E0)

ServerName      [wstring] '20.56.75.30'
ServerFqdn      [wstring] ''
UserSpecifiedServerName [wstring] '20.56.75.30'
UserName        [wstring] 'david_da'
Domain          [wstring] 'ALEFDEMO'
Password        [protect] 'SecretPassword112233'
SmartCardReaderName [wstring] ''
PasswordContainsSCardPin [bool] FALSE
ServerNameUsedForAuthentication [wstring] '20.56.75.30'
RDmiUsername    [wstring] 'alefdemo.local\david_da'

mimikatz #
```

Vzdálený přístup

DEMO – získání uživatelských údajů



Vzdálený přístup

DEMO – ochrana před hesly v čitelné podobě



Mstsc.exe





Recycle Bin



Google Chrome



Microsoft Edge

```
Windows PowerShell × + | - □ ×
PS C:\tools\mimikatz_trunk\x64> |
```



Search



Vzdálený přístup a heslo v čitelné podobě

Mitigace

- ~~Windows 11~~
 - ~~Credential guard~~
 - ~~TPM čip~~
- MFA
- ~~XDR řešení~~
- ~~Šifrování~~
- ~~GDPR, ISO, NIS2~~
- Zero Trust

```
PS C:\tools\mimikatz_trunk\x64> .\mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # ts::mstsc
!!! Warning: false positives can be listed !!!

| PID 2628      mstsc.exe (module @ 0x000000000037F8A0)

ServerName      [wstring] 'dc02.alefdemo.safe'
ServerFqdn      [wstring] ''
UserSpecifiedServerName [wstring] 'dc02.alefdemo.safe'
UserName        [wstring] 'T0-dburinsky'
Domain          [wstring] 'ALEFDEMO'
Password        [protect] '123456'
SmartCardReaderName [wstring] ''
PasswordContainsSCardPin [bool] TRUE
ServerNameUsedForAuthentication [wstring] 'dc02.alefdemo.safe'
RDmiUsername    [wstring] 'ALEFDEMO\t0-dburinsky'
```

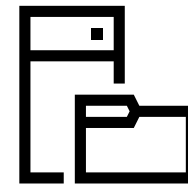

Vzdálený přístup a heslo v čitelné podobě

Mitigace

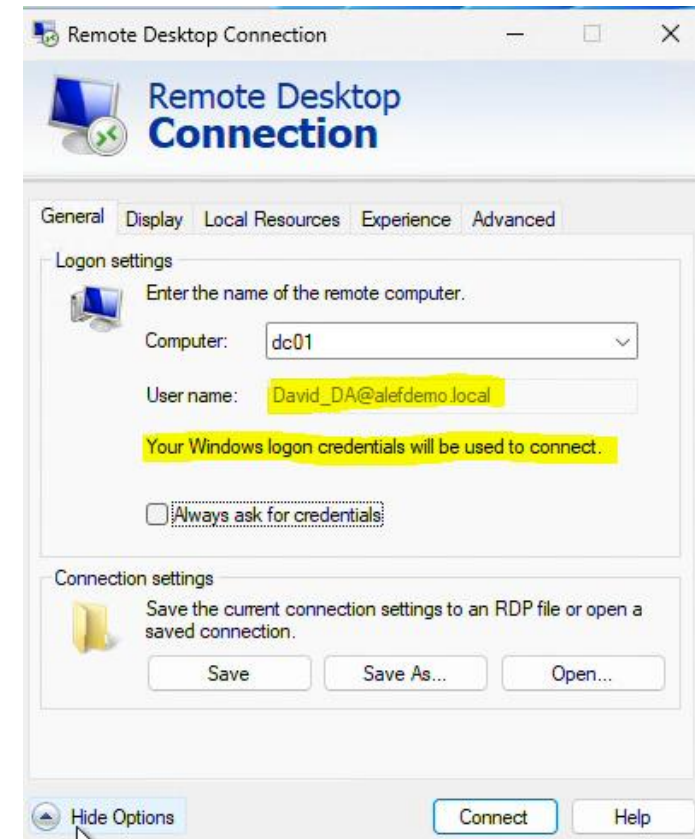
- **Restricted Admin Mode**
 - Dostupný výhradně pro členy skupiny **Administrators**.
 - **Nedochází k delegaci uživatelských údajů na cílový server.**
 - Povolení na straně serveru / možné vynucení na straně klienta.



Klient



Server



Administrative Templates\System\Credential Guard

Restrict delegation of credentials to remote servers

Restrict delegation of credentials to remote servers

Previous Setting Next Setting

Not Configured Comment:

Enabled

Name	Type	Data
(Default)	REG_SZ	(value not set)
auditbasedirectories	REG_DWORD	0x00000000 (0)
auditbaseobjects	REG_DWORD	0x00000000 (0)
Authentication Packages	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20 00 00
crashonauditfail	REG_DWORD	0x00000000 (0)
disabledomaincreds	REG_DWORD	0x00000000 (0)
DisableRestrictedAdmin	REG_DWORD	0x00000000 (0)
everyoneincludesanonymous	REG_DWORD	0x00000000 (0)
forceguest	REG_DWORD	0x00000000 (0)
fullprivilegeauditing	REG_BINARY	00
LimitBlankPasswordUse	REG_DWORD	0x00000001 (1)
Imcompatibilitylevel	REG_DWORD	0x00000005 (5)
LsaPid	REG_DWORD	0x0000027c (636)
NoLmHash	REG_DWORD	0x00000001 (1)

Require Remote Credential Guard: Participating applications must use Remote Credential Guard to connect to remote hosts.

OK Cancel Apply

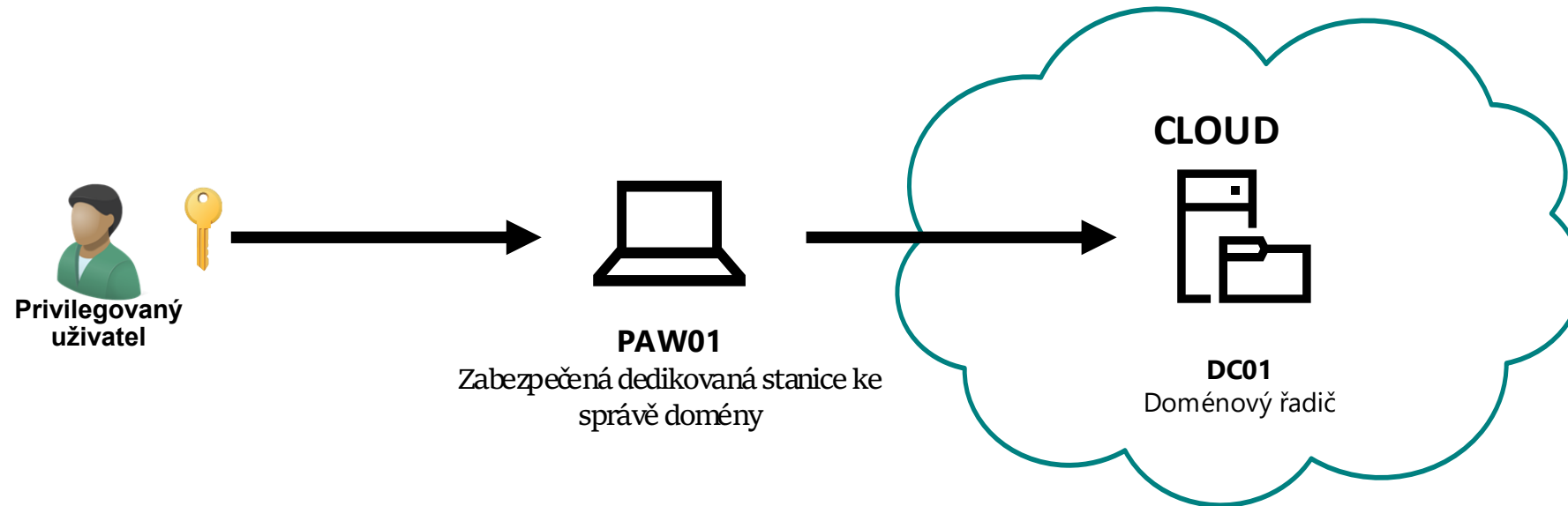
Vzdálený přístup a heslo v čitelné podobě

Mitigace

- **Restricted Admin Mode**
 - Dostupný výhradně pro členy skupiny **Administrators**.
 - **Nedochází k delegaci uživatelských údajů na cílový server.**
 - Povolení na straně serveru / možné vynucení na straně klienta.
- **Privileged Access Workstation**
 - **Dedikované** počítače pro správu infrastruktury.
 - Maximální koncentrace na **vyloučení** potenciálních **vektorů infiltrace**.
 - **Bezpečný bod kontaktu** s infrastrukturou.

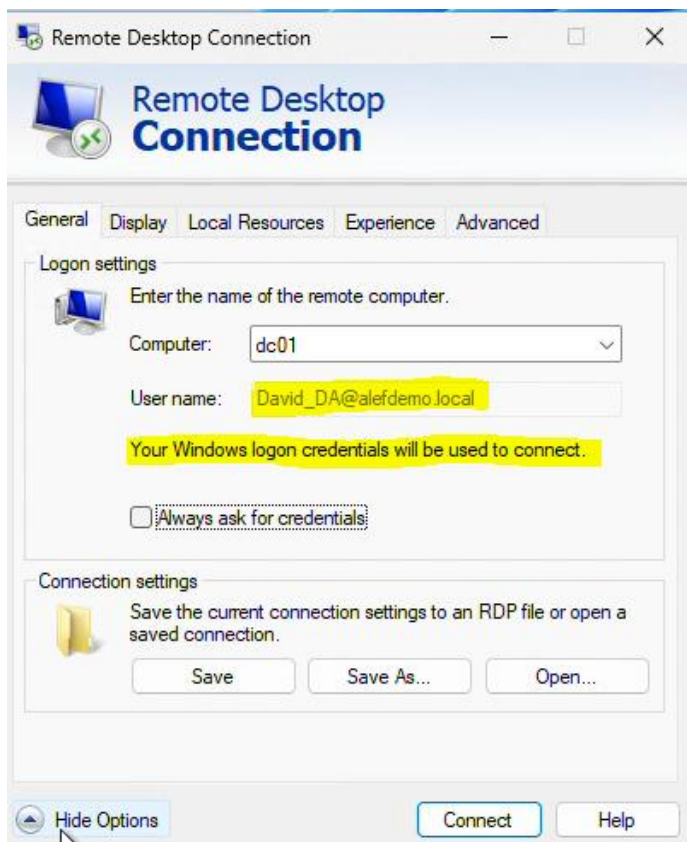
Vzdálený přístup

Mitigace – Restricted Admin Mode



Vzdálený přístup a heslo v čitelné podobě

Mitigace



```
mimikatz # ts::mstsc
!!! Warning: false positives can be listed !!!

| PID 5756      mstsc.exe (module @ 0x00000000010DF8F0)

ServerName      [wstring] 'dc01'
ServerFqdn      [wstring] ''
UserSpecifiedServerName [wstring] 'dc01'
UserName        [wstring] 'David_DA'
Domain          [wstring] 'ALEFDEMO'
Password      [protect]                 
SmartCardReaderName [wstring] ''
PasswordContainsSCardPin [bool] FALSE
ServerNameUsedForAuthentication [wstring] 'dc01'
RDmiUsername    [wstring] 'ALEFDEMO\david_da'

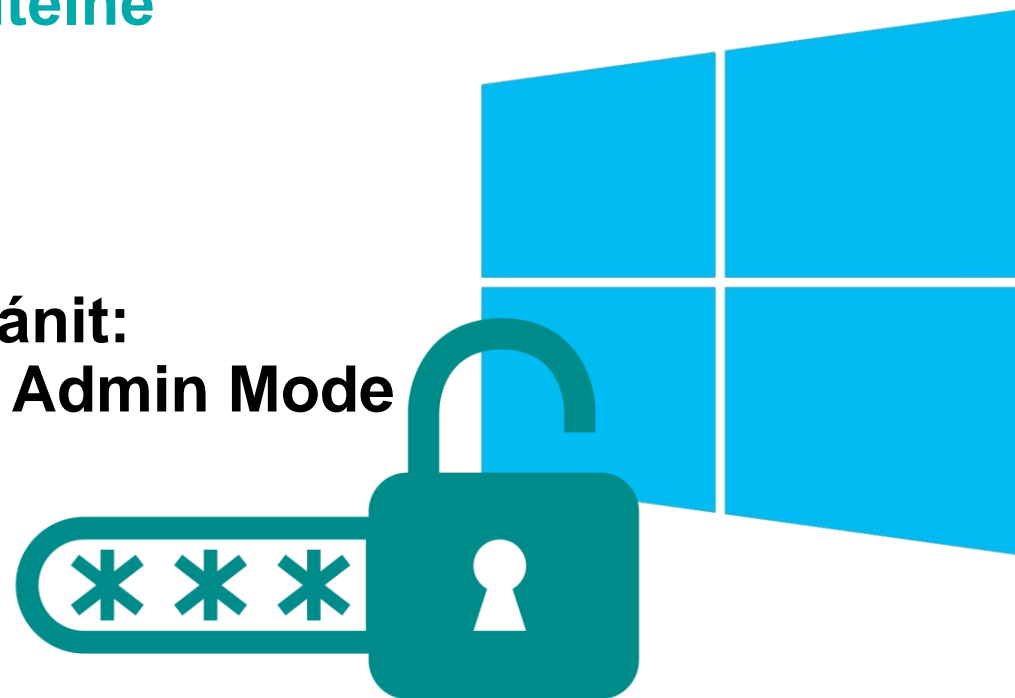
mimikatz #
```

Vzdálený přístup

DEMO – ochrana před hesly v čitelné podobě



Jak se chránit:
Restricted Admin Mode



Recycl
Bin
Micro.
Edge
Googl
Chrom

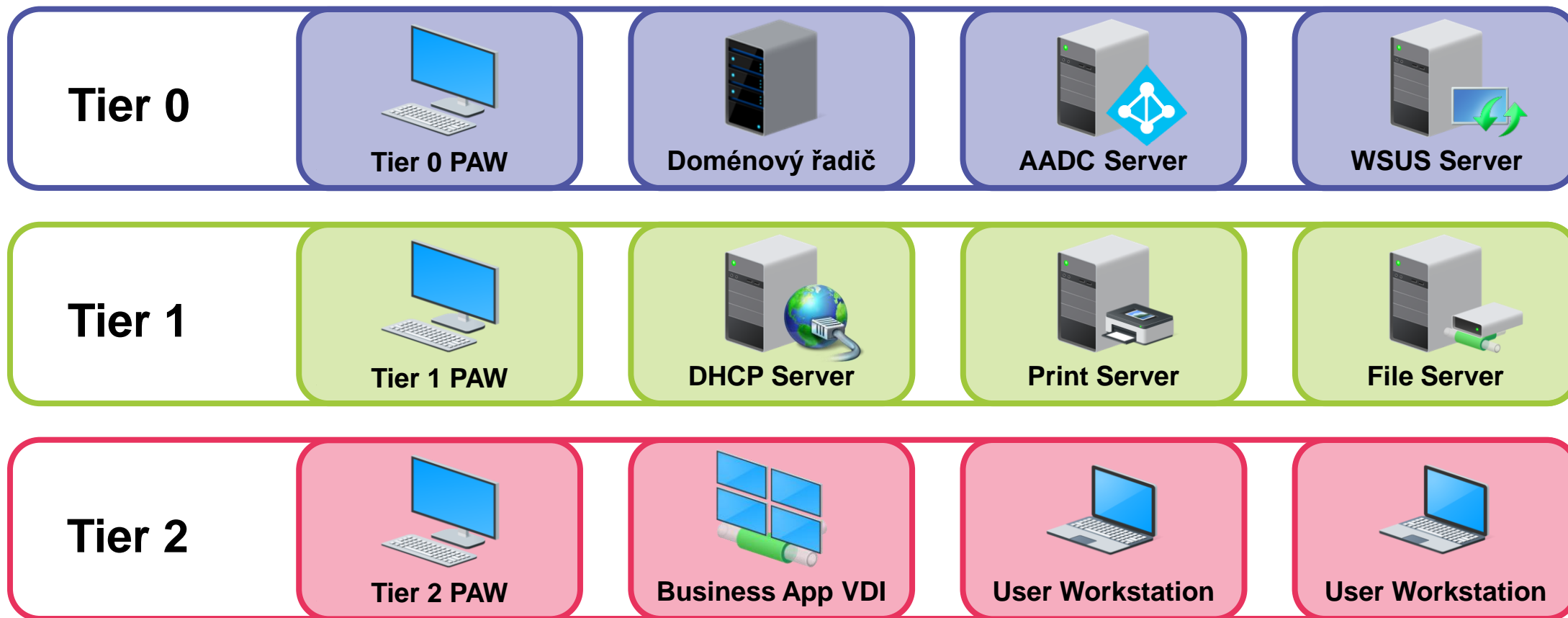
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> _
```

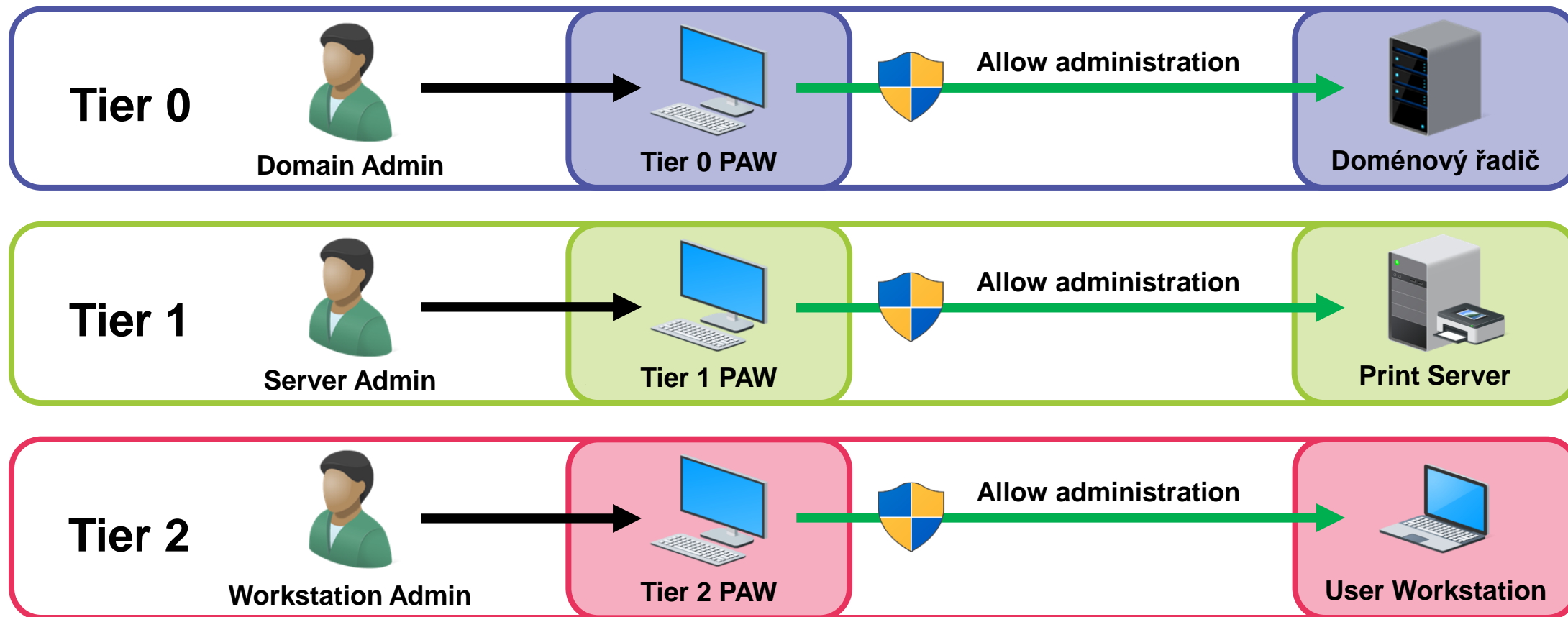
Mitigace

Koncept Tiering – On Premise



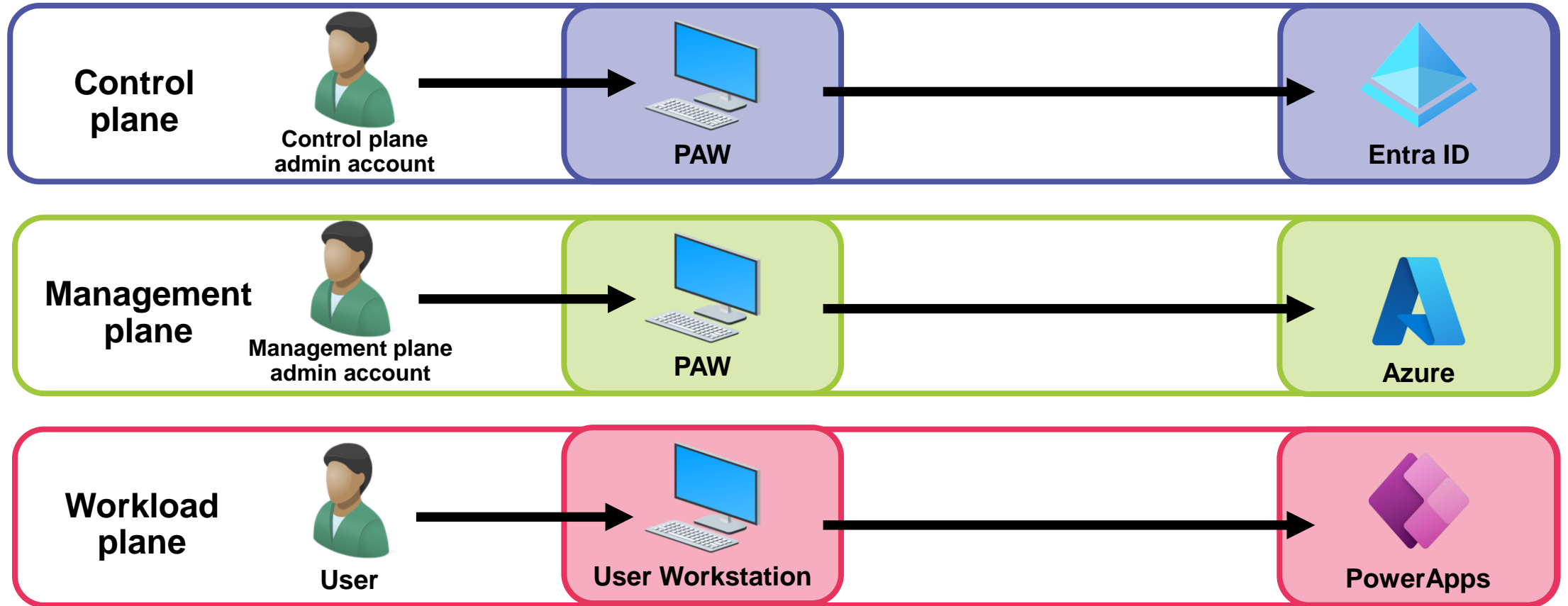
Mitigace

Koncept Tiering – On Premise



Mitigace

Konzept Tiering – Entra



Mitigace

Privileged Access Management

- Automatická změna hesel privilegovaných účtů
- Zabezpečení přístupu k privilegovaným účtům
- Automatizace bezpečnostních přístupů
- Detailní audit používání těchto účtů



Recycle Bin



Microsoft Edge

Remote Desktop Connection

General Display Local Resources Experience Advanced

Logon settings



Enter the name of the remote computer.

Computer: User name:

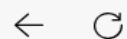
Select mimikatz 2.2.0 x64 (oe.eo)

```
| PID 3012      mstsc.exe (module @ 0x0000000000B8FAE0)

ServerName      [wstring] '10.15.16.160'
ServerFqdn      [wstring] ''
UserSpecifiedServerName [wstring] '10.15.16.160'
UserName        [wstring] 'dee7f06de68b87b6e65d54abc74684a01e2e6d31772e9c63b2e73a00cfab8bf1'
Domain          [wstring] ''
Password        [protect]
SmartCardReaderName [wstring] ''
PasswordContainsSCardPin [bool] FALSE
ServerNameUsedForAuthentication [wstring] '10.15.16.160'
RDmiUsername    [wstring] ''

mimikatz #
```

BeyondInsight: Password Safe

Not secure | <https://10.15.16.160/webconsole/#!/ps/portal?t...>

MENU

BeyondInsight



Password Safe

Quick Navigation



> Requests

Accounts

Requests

Approvals



RDP file downloaded successfully.

Dismiss

4 items

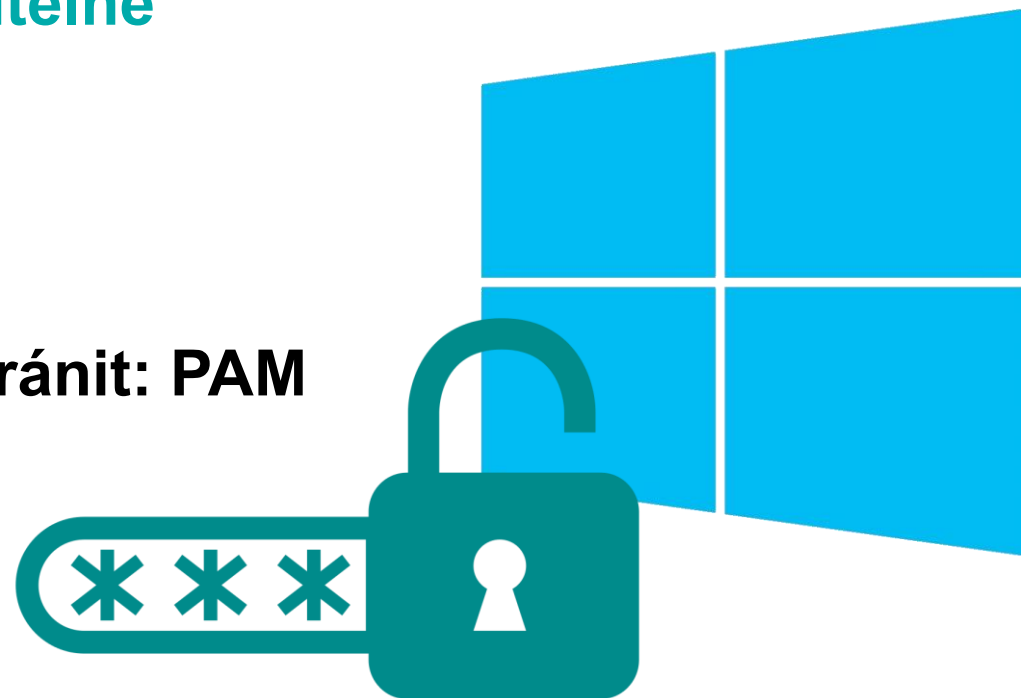


Vzdálený přístup

DEMO – ochrana před hesly v čitelné podobě



Jak se chránit: PAM





PLEASE LOG IN

Username

This field is required.

Password

Log in to

[Forgot Password?](#)

[Use SAML Authentication](#)

If you are having trouble logging in, or have forgotten your username or password, please contact your Administrator.

Závěr

- Vzdálená správa má svá rizika i ve velmi dobře zabezpečených infrastrukturách
- Implementace doporučených opatření je klíčová
 - Restricted admin
 - Tiering model
 - Privileged access workstation

Děkuji za pozornost



David Buřínský
Systems Engineer

David.burinsky@alef.com
www.alef.com

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

