Bezpečnostní incidenty v Microsoft 365

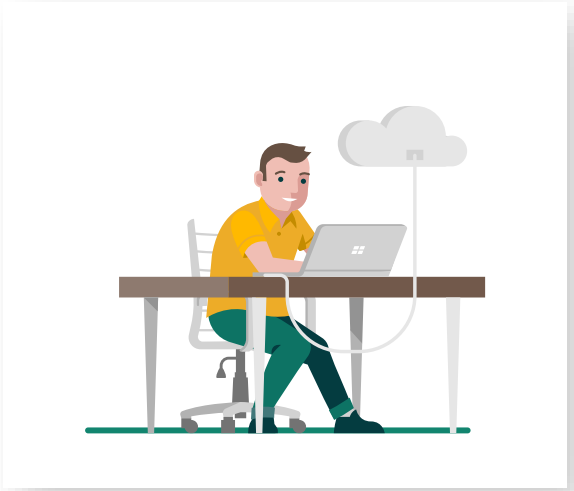
Petr Vlk

KPCS

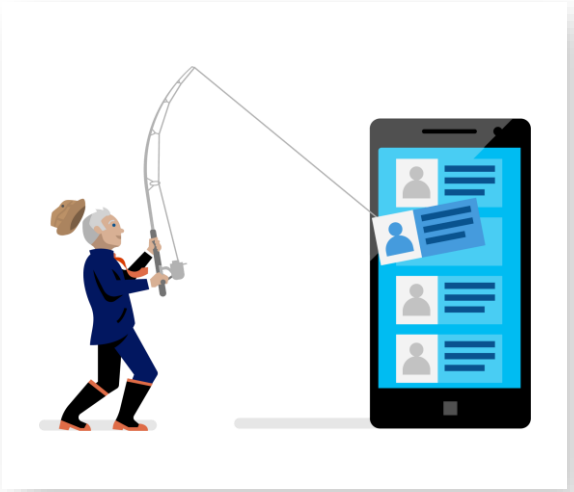

WE'RE ALL
GONNA
DIE

Moderní pracoviště začíná zabezpečením

Spolupráce



Vzdálený přístup



Aktuální hrozby

Může se to stát i vám…

Nemocnice Benešov
prosinec 2019

OKD
prosinec 2019

Fakultní nemocnice Brno
březen 2020

Psychiatrická nemocnice Kosmonosy
březen 2020

Může se to stát i vám…

Městský úřad Prahy 3
duben 2020

Povodí Vltavy
duben 2020

eD system
červen 2020

subreg
září 2020

Může se to stát i vám…

Garmin
srpen 2020

Software AG
říjen 2020

Canon
srpen 2020

Xerox
červenec 2020

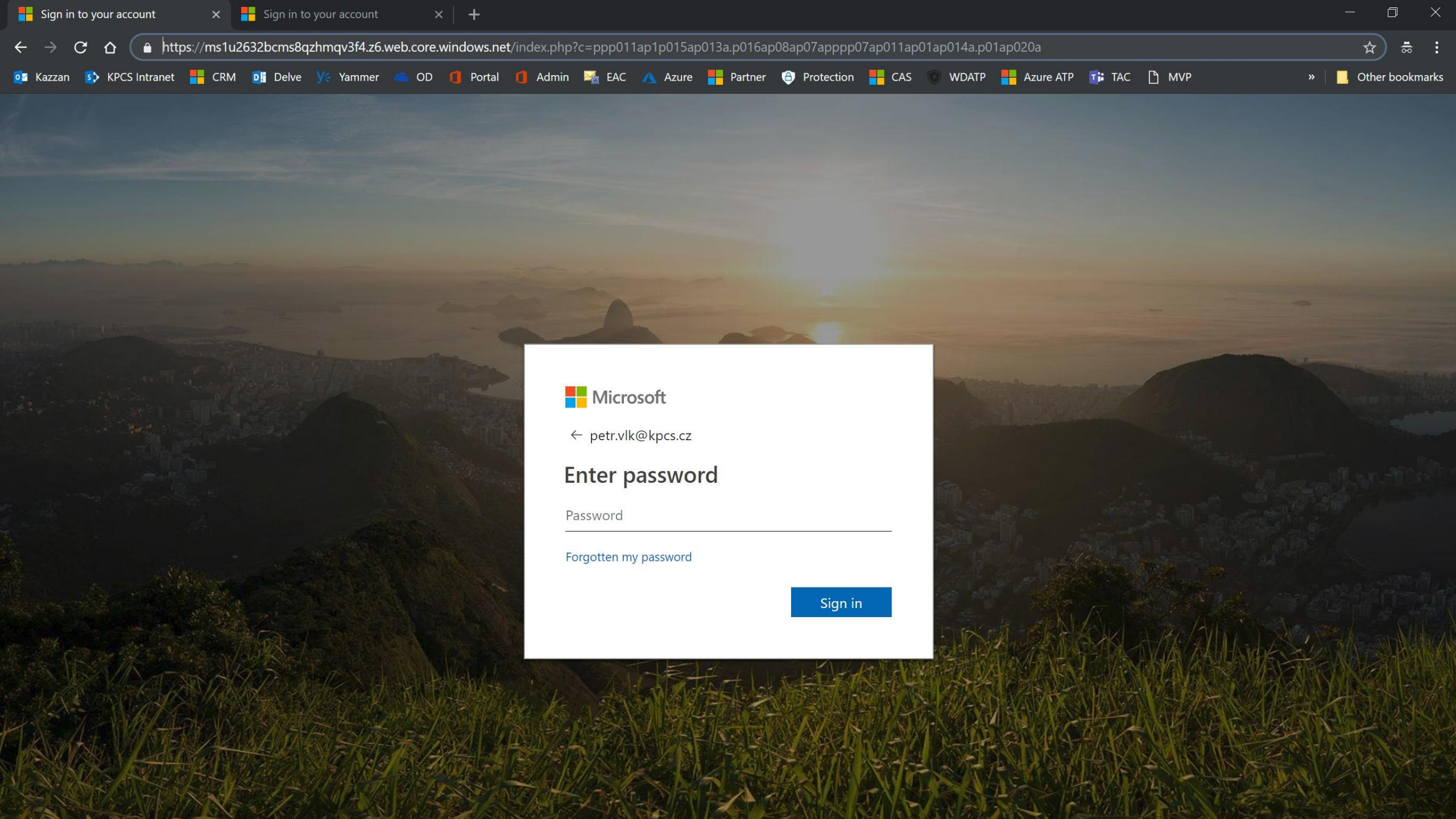
Může se to stát i vám…

Okta
březen 2022

Microsoft
březen 2022

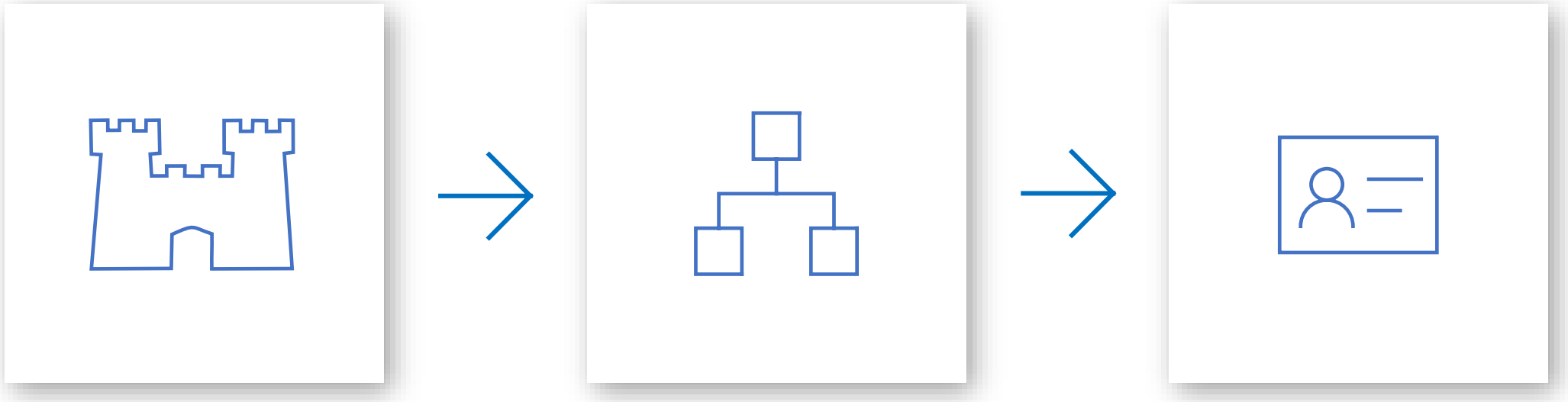
Cisco
srpen 2022

Ředitelství silnic a dálnic
květen 2022


Sign in to your account
Sign in to your account
https://ms1u2632bcms8qzhmqv3f4.z6.web.core.windows.net/index.php?c=ppp011ap1p015ap013a.p016ap08ap07apppp07ap011ap01ap014a.p01ap020a
Kazzan
KPCS Intranet
CRM
Delve
Yammer
OD
Portal
Admin
EAC
Azure
Partner
Protection
CAS
WDATP
Azure ATP
TAC
MVP
Other bookmarks
Microsoft
petr.vlk@kpcs.cz
Enter password
Password
Forgotten my password
Sign in

Správně nastavené a spravované Microsoft 365

Evoluce bezpečnostního perimetru



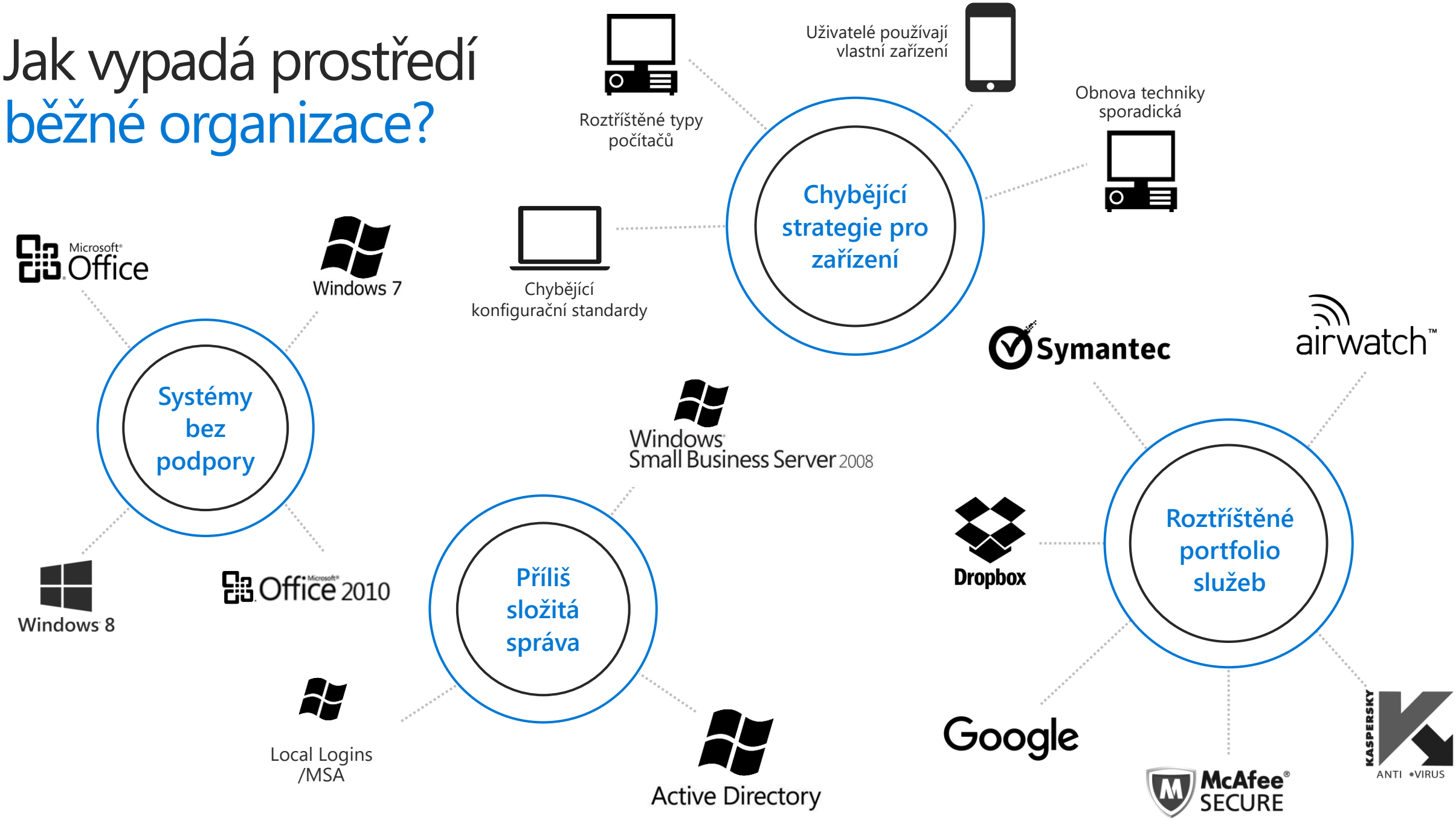
Kancelář

Síť

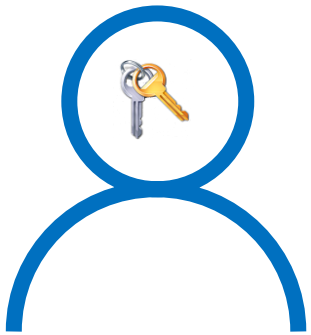
Identita

Různá rizika a vektory útoku vyžadují různé metody obrany a protiútoku

Jak vypadá prostředí běžné organizace?



Kde číhá nebezpečí



Znáte kontext svého prostředí?

- Licence Microsoft 365?
- Active Directory? Azure Active Directory?
- Azure AD Connect? AD FS?
- Exchange Online? Exchange Server? Hybrid?
- Windows 10? Windows 7? Windows XP?
- System Center Configuration Manager?
- Office? Office 365? Office Mobile?
- Aplikace? Konfigurace? Síť? VPN?
- BYOD? MFA? MDM? Antivirus? Antimalware?

Neblahé následky

Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

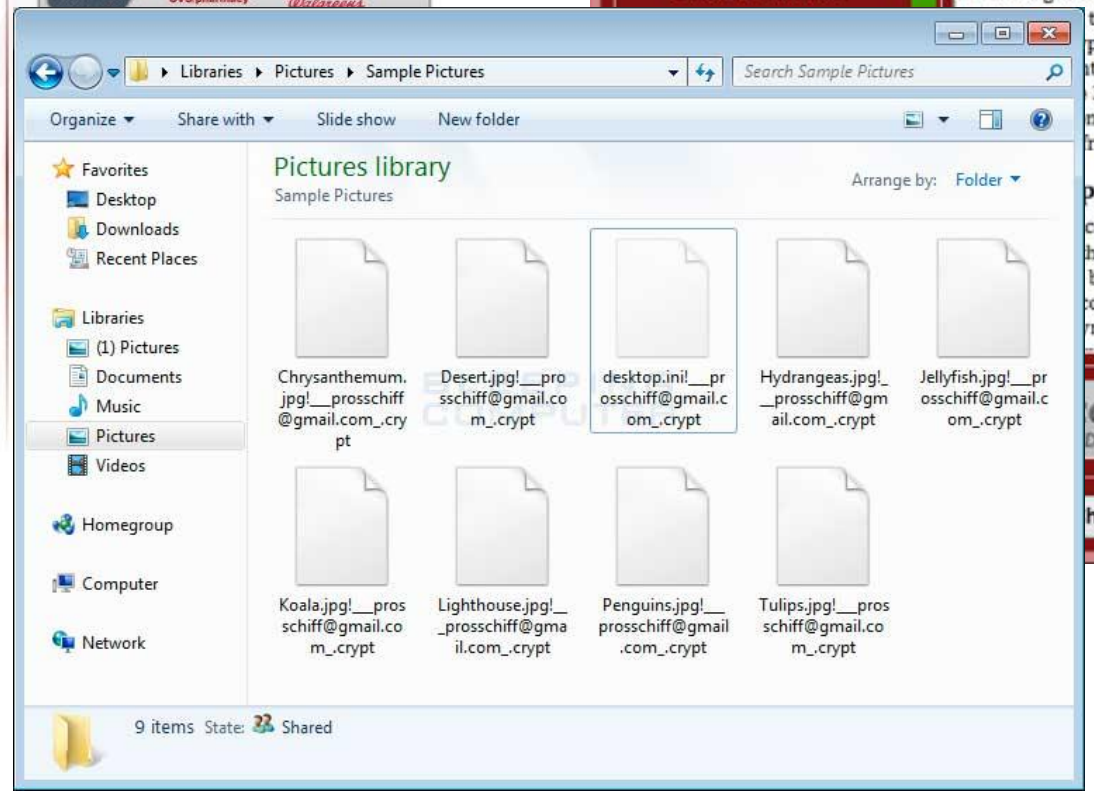
Technical details:
Involved IP address:
Involved host name:
Source or intermediary sites:

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

Permanent lock on

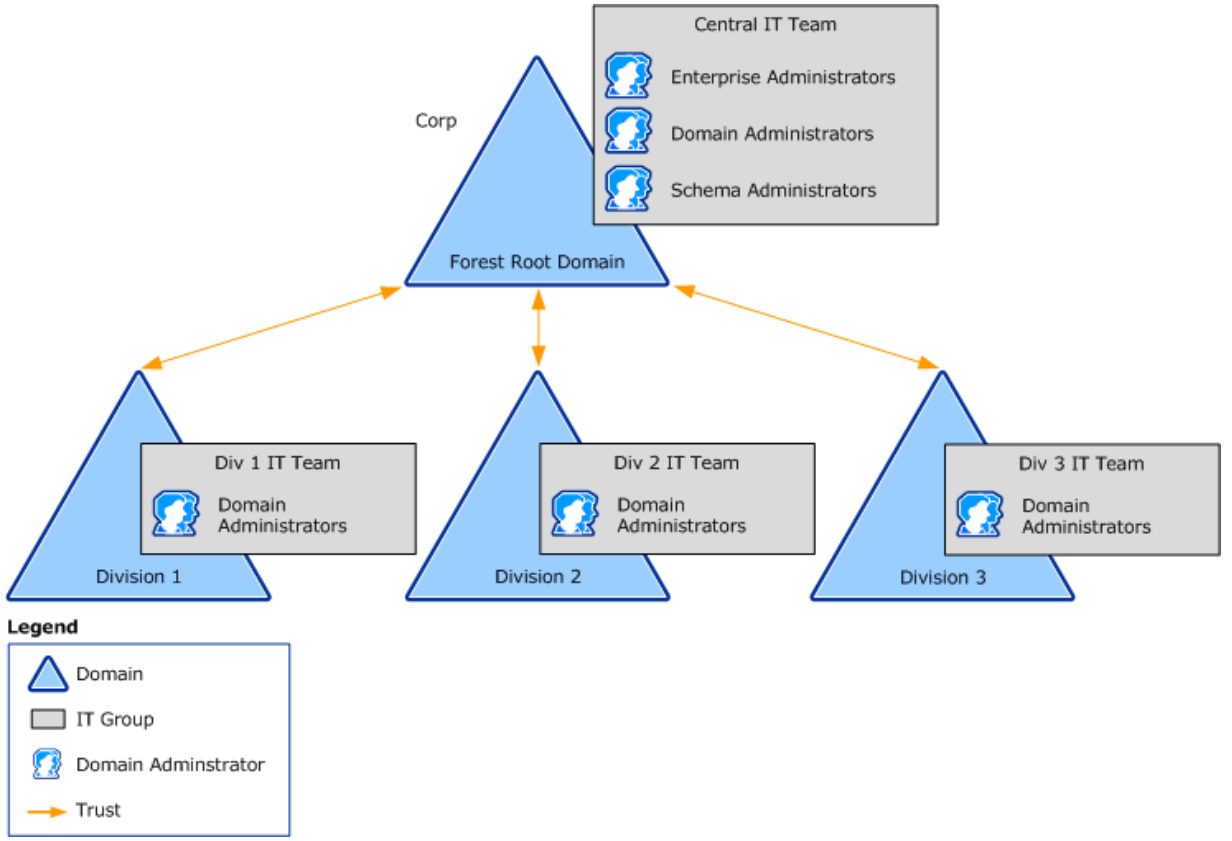


ACTIVE DIRECTORY

AD: UNDERSTAND AND PROTECT AT ALL COST

Active Directory

- Saw something outside ADUC?
- Windows Server without patches
- Without Password quality
- Without Password protection
- NTLM everywhere
- Object Permissions
- Everybody is Local Administrator
- Tiering without PAW

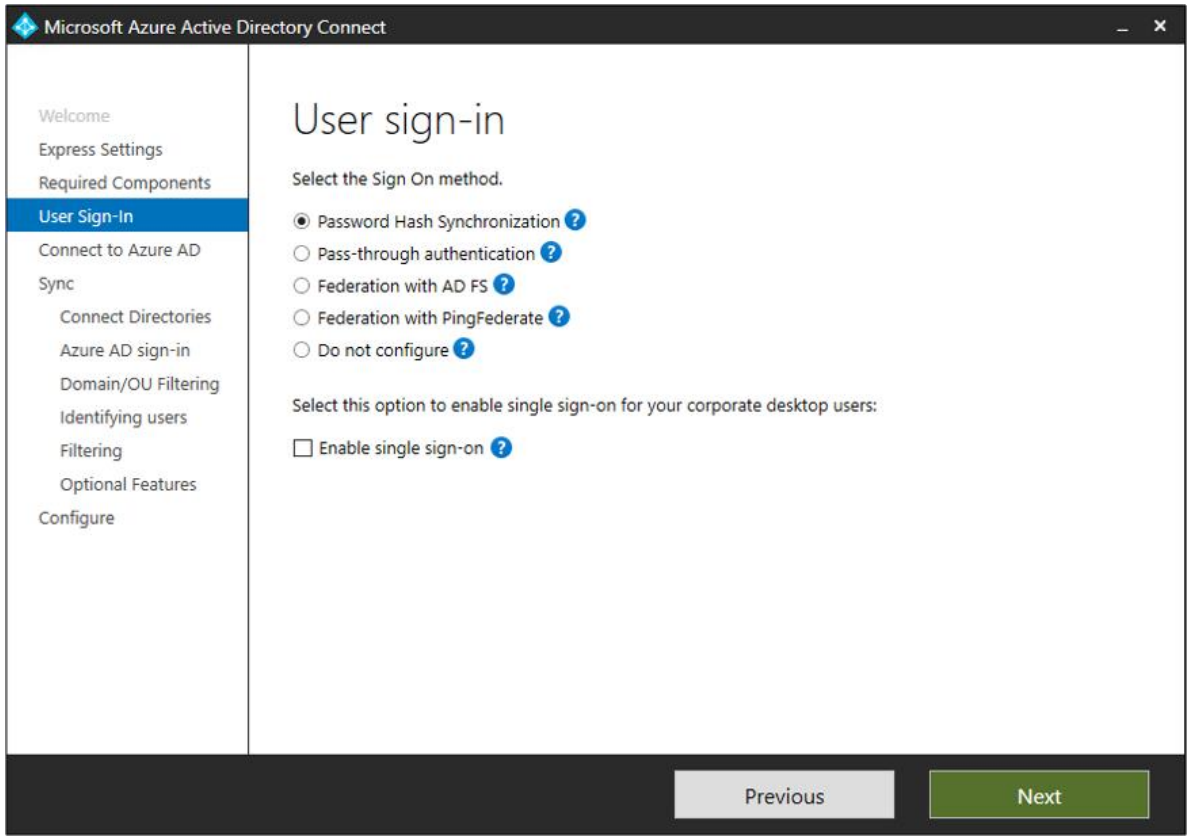


AZURE ACTIVE DIRECTORY CONNECT

AAD CONNECT: PATCH AND SETUP CORRECTLY

Azure Active Directory Connect

- Simple Password
- Global Administrator Credentials
- Setup without MFA
- Everybody is Local Administrator
- Password Secrets
- Database behind
- Permissions inside Active Directory
- Vulnerable Versions

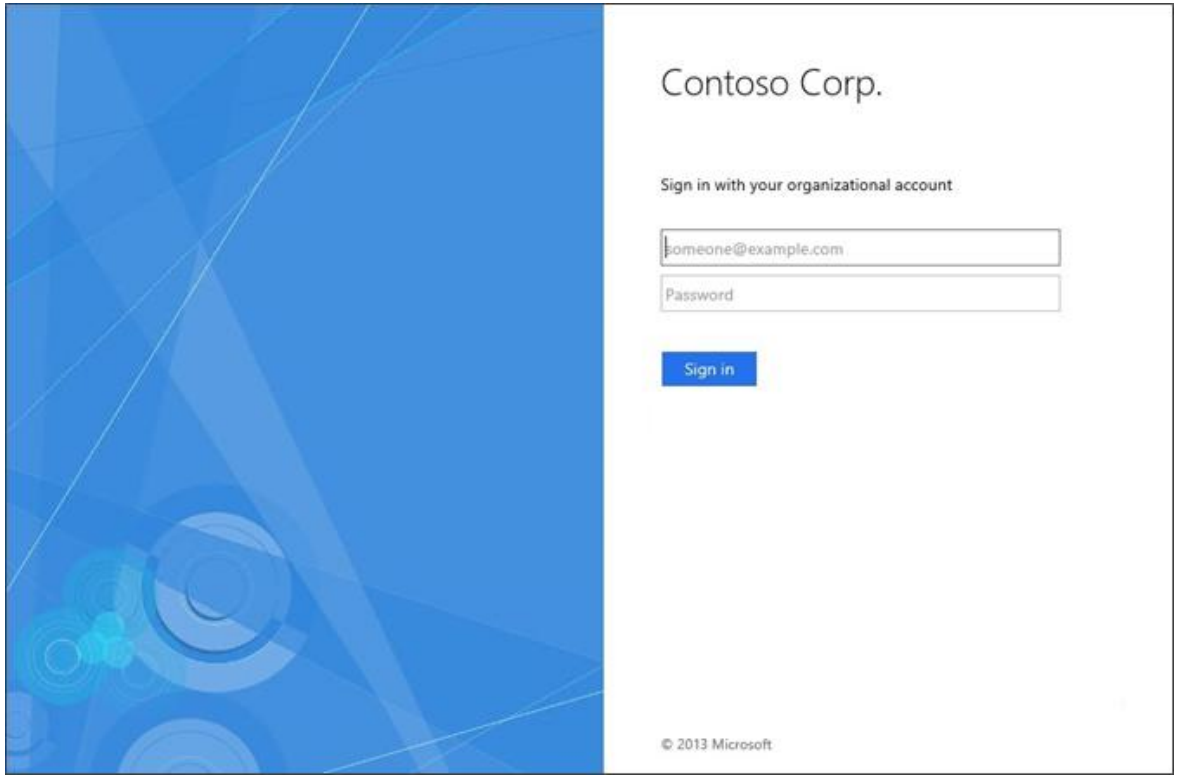


ACTIVE DIRECTORY FEDERATION SERVICES (AD FS)

AD FS: THROW AWAY IF YOU CAN

Active Directory Federation Services

- Only Password Authentication
- No Branding
- No Updates
- Everybody is Local Administrator
- Database behind
- SAML Attacks
  - SolarWinds / Golden SAML
- Federation Attacks
  - No Extranet / Smart Lockout

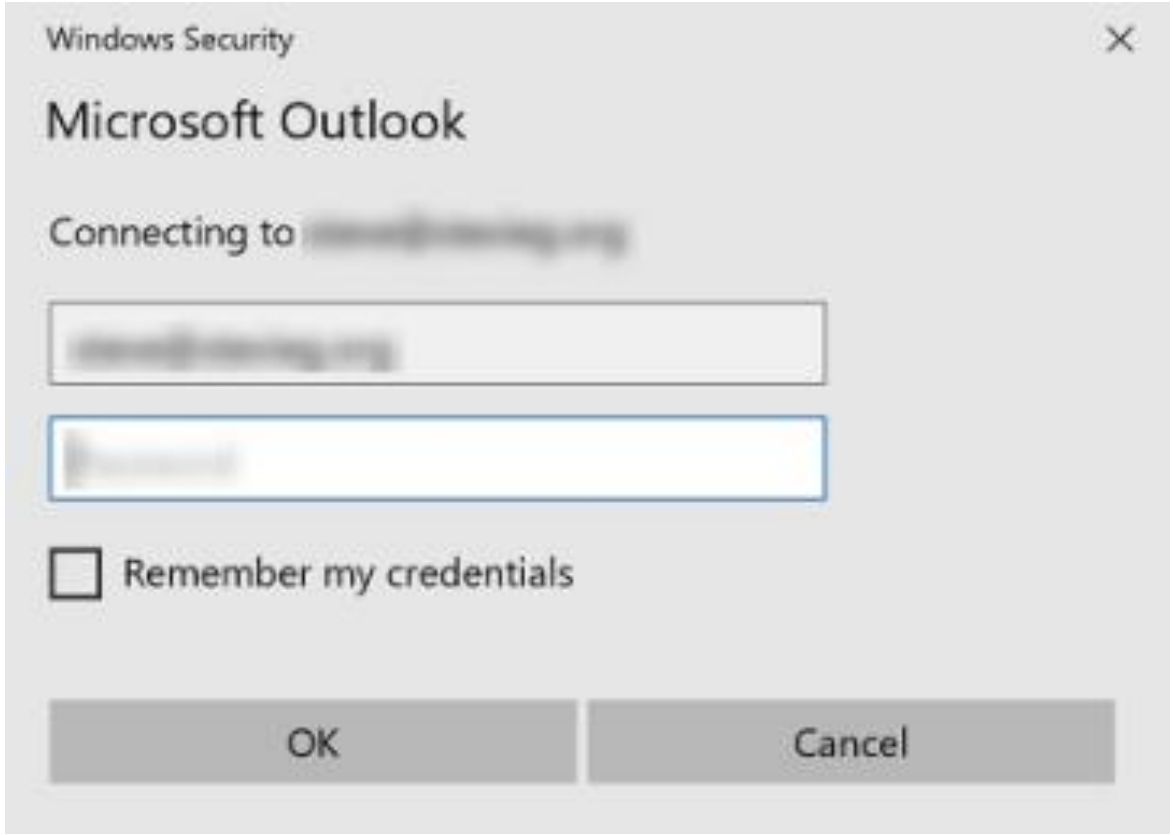


EXCHANGE HYBRID

EXCHANGE: CONSIDER, PATCH, PATCH AND PATCH

Exchange Hybrid

- Legacy Authentication
- Password Authentication
- Published directly to Internet
- Not regularly patched
  - Windows Server
  - .NET
  - Exchange
    - ProxyShell
    - ProxyLogon



POWERSHELL

PS: DO NOT BE TOO LAZY

PowerShell

- Service Accounts with Global Administrator permissions
- Service Accounts with simple password
- Administrators without MFA
- Credentials stored in plain text

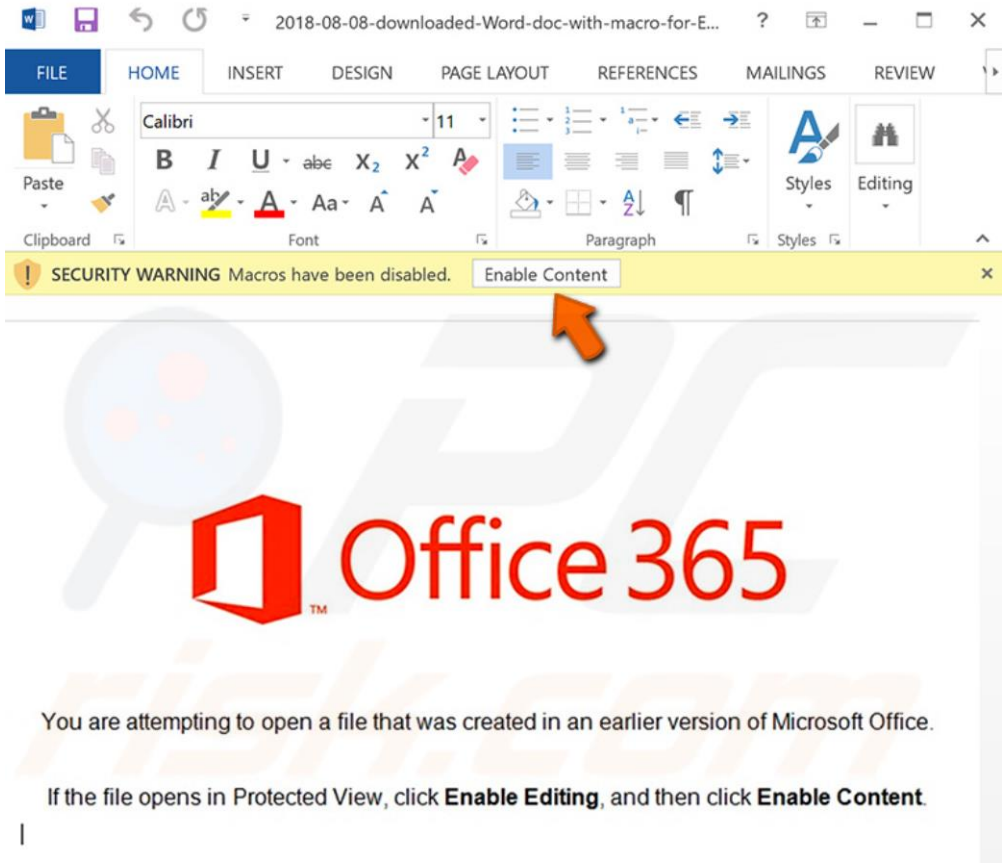
OFFICE

WHO NEED MACROS?

Office

- Missing Updates
- Legacy Components
- Macros from Internet

- Adobe Reader
  - Missing Updates
  - Scripting Allowed

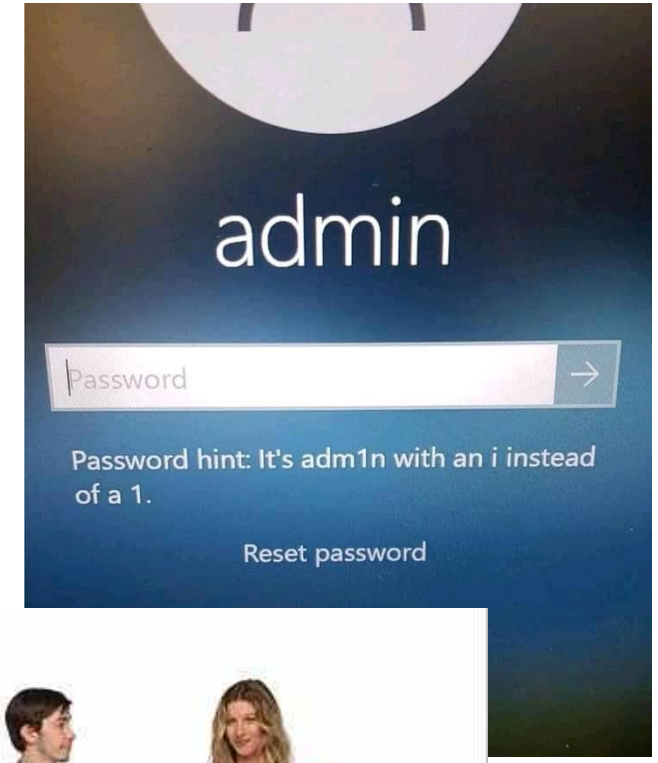


WINDOWS

BUT YOU RUN ON MAC NOW?

Windows

- User as Local Administrator
- Missing Updates
  - MECM / WSUS
- Unsupported Versions
- AV Signatures & AV Platform
- No Tamper Protection
- Autorun / ISO / HTA / HTML
- Tamper Protection / Cloud Protection
- I am Mac or waiting for next Android

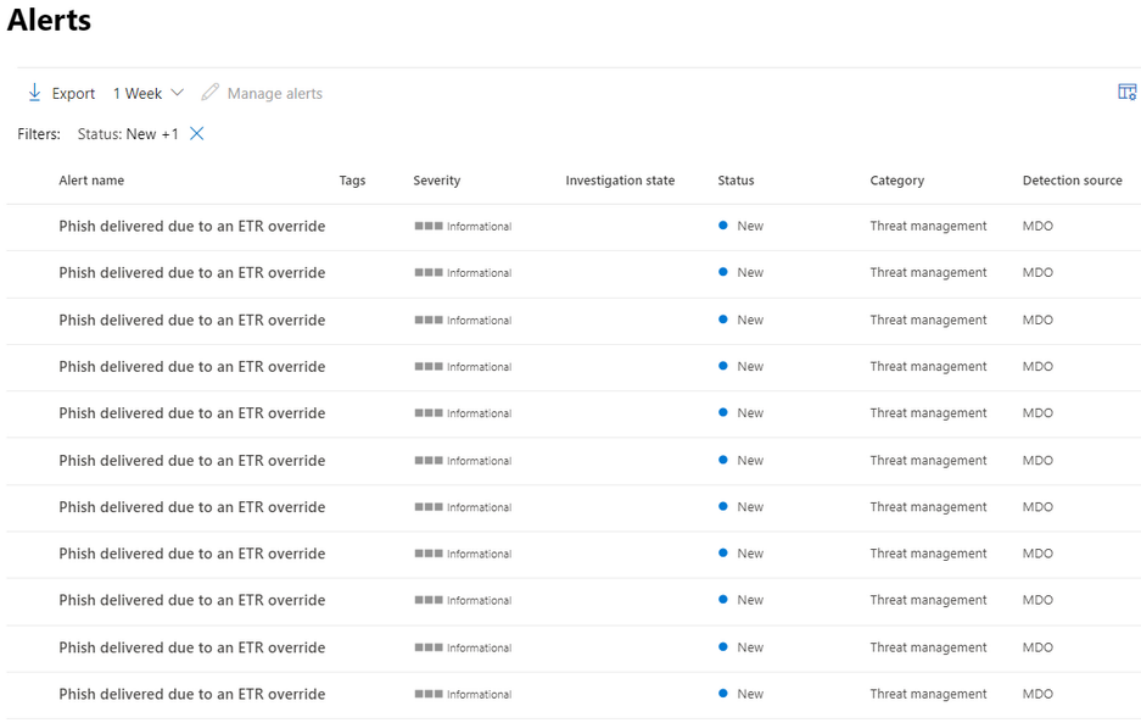


MICROSOFT 365

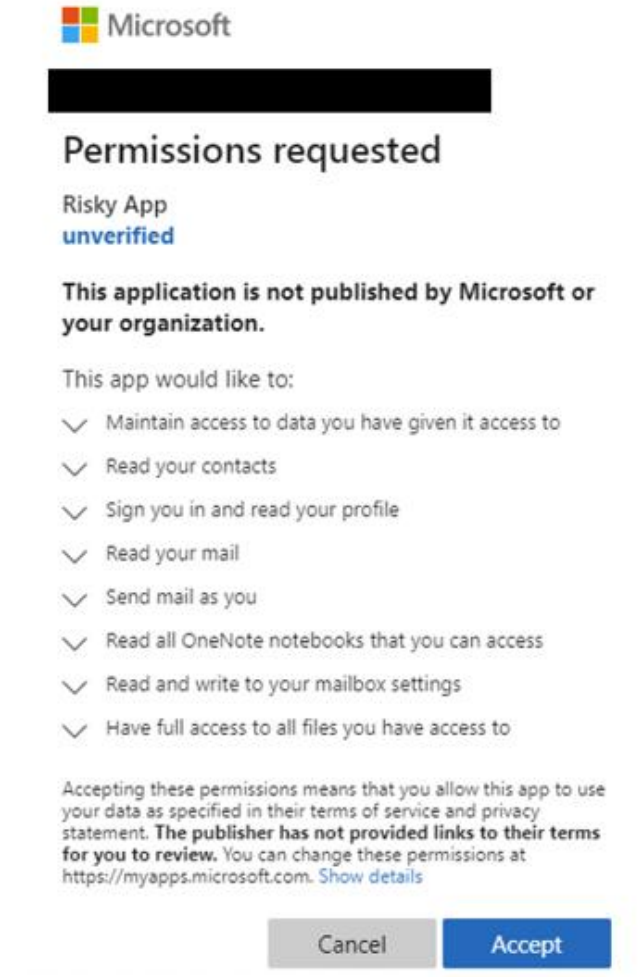
DO YOU SEE THIS CONSOLE?

Microsoft 365

- Legacy Auth Everywhere
- Without SPF / DKIM / DMARC protection
- Compromised ≠ Password Change
- OAuth Consent
- SPN Enterprise Apps
- Audit Log versus Standard
- Password Expiration
- Guests
- Delegated Admin Rights
- AntiPhishing Policy
- Transport Rules
- Content Attachment Filter

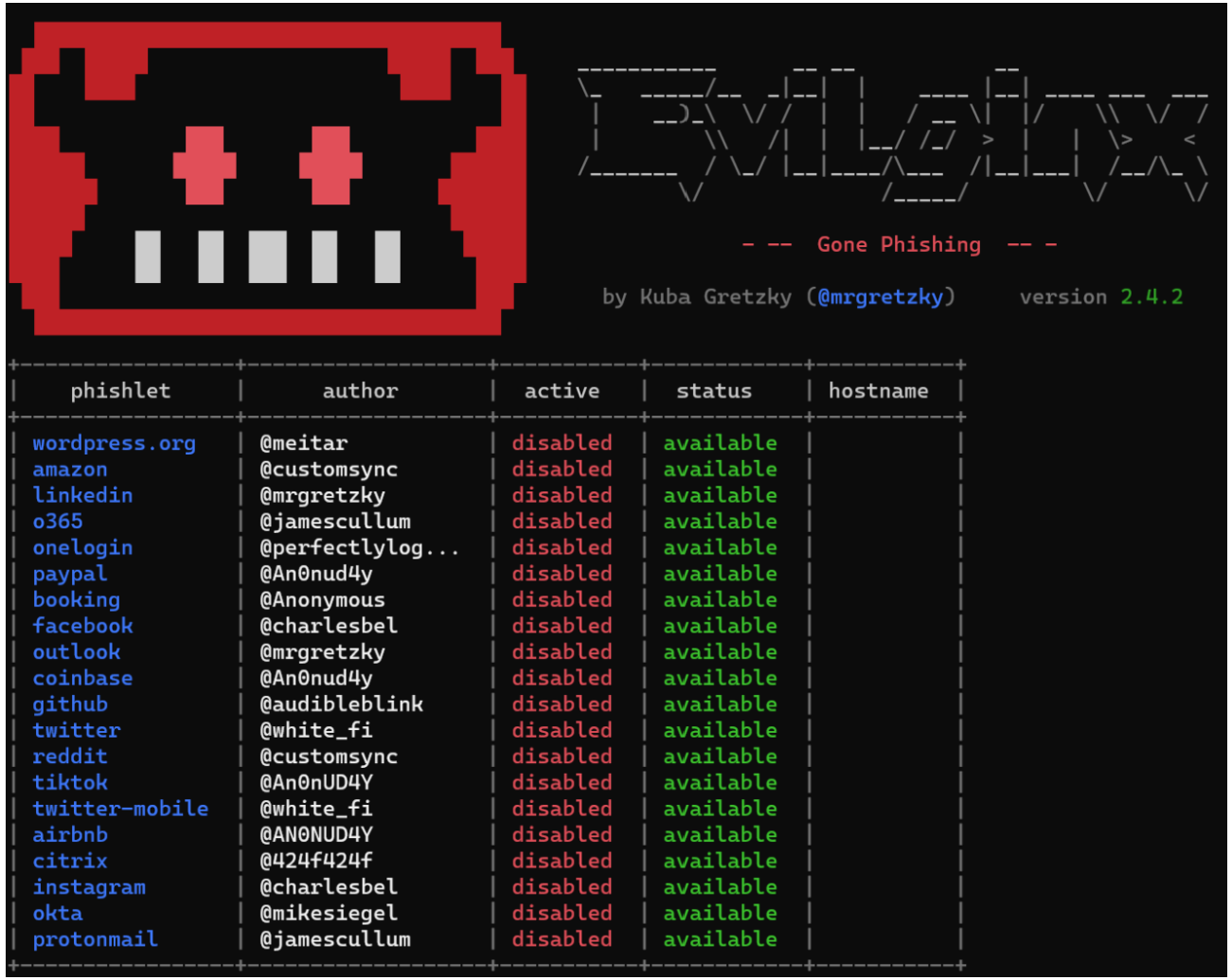


Application Consent Grants



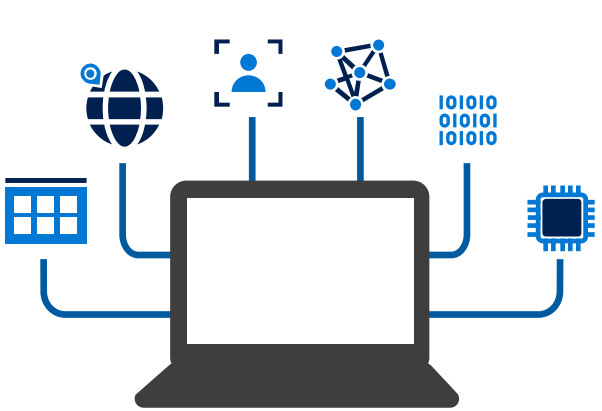
Phishing Kits = MFA no more?

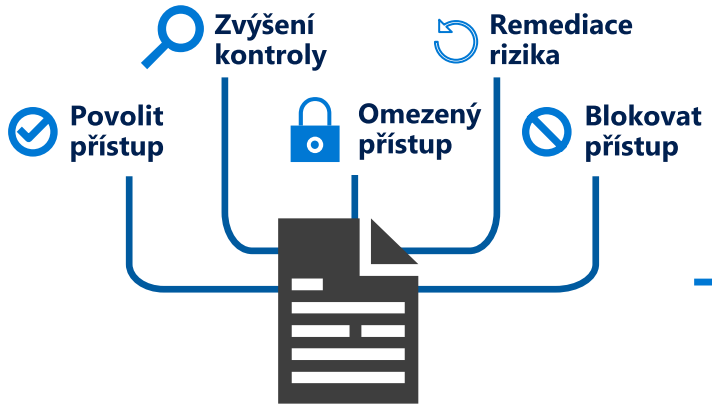
- Modlishka
- Muraena/Necrobrowser
- Evilginx2



Zero Trust

Nikdy nevěřte. Vždy ověřte.





Signál

pro informované rozhodnutí

Rozhodnutí

na základě politiky

Vynucení

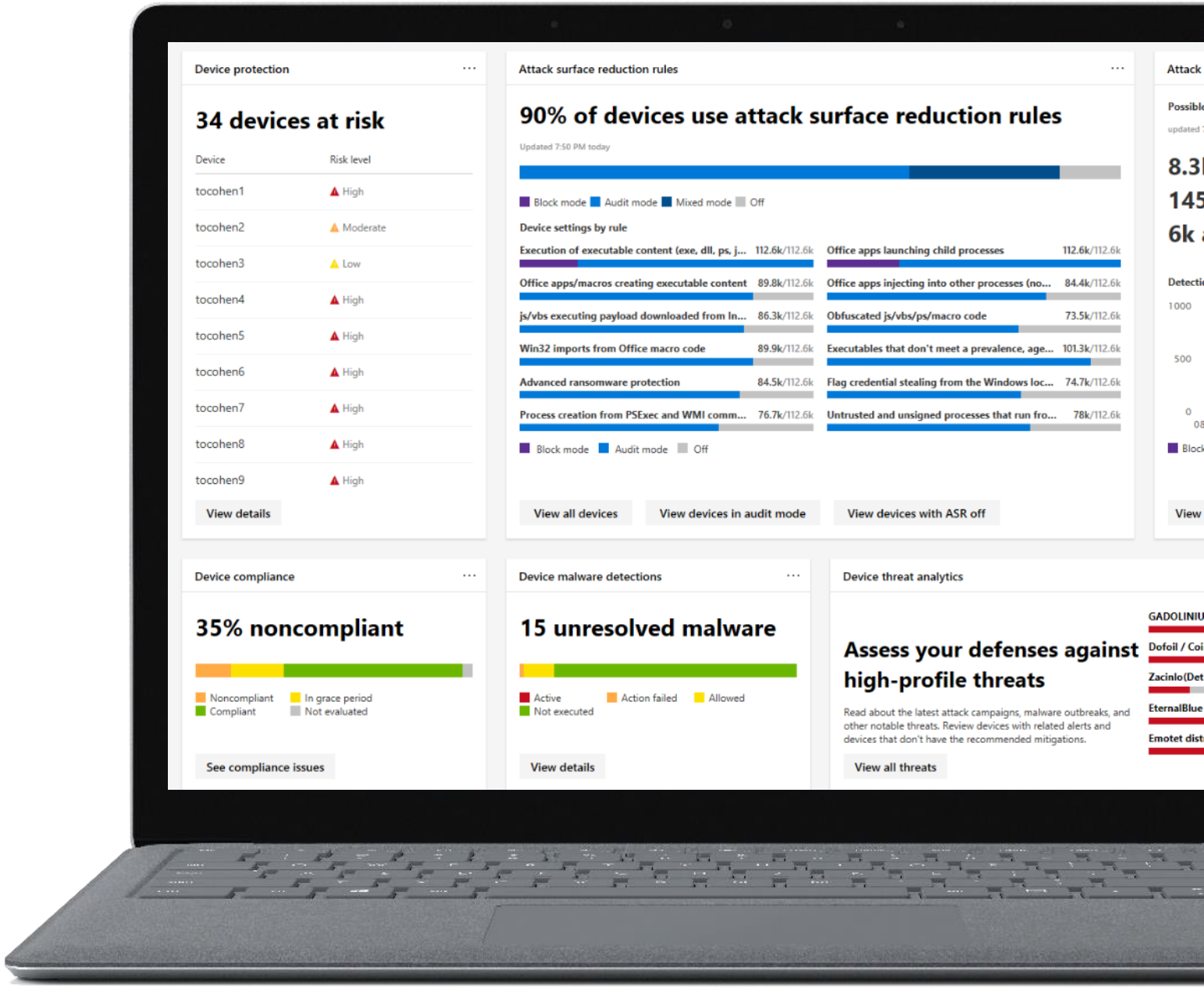
politik napříč systémy

Kybernetická bezpečnost

Identita, SSO s MFA

Aktualizace a nastavení

Správa mobilních zařízení

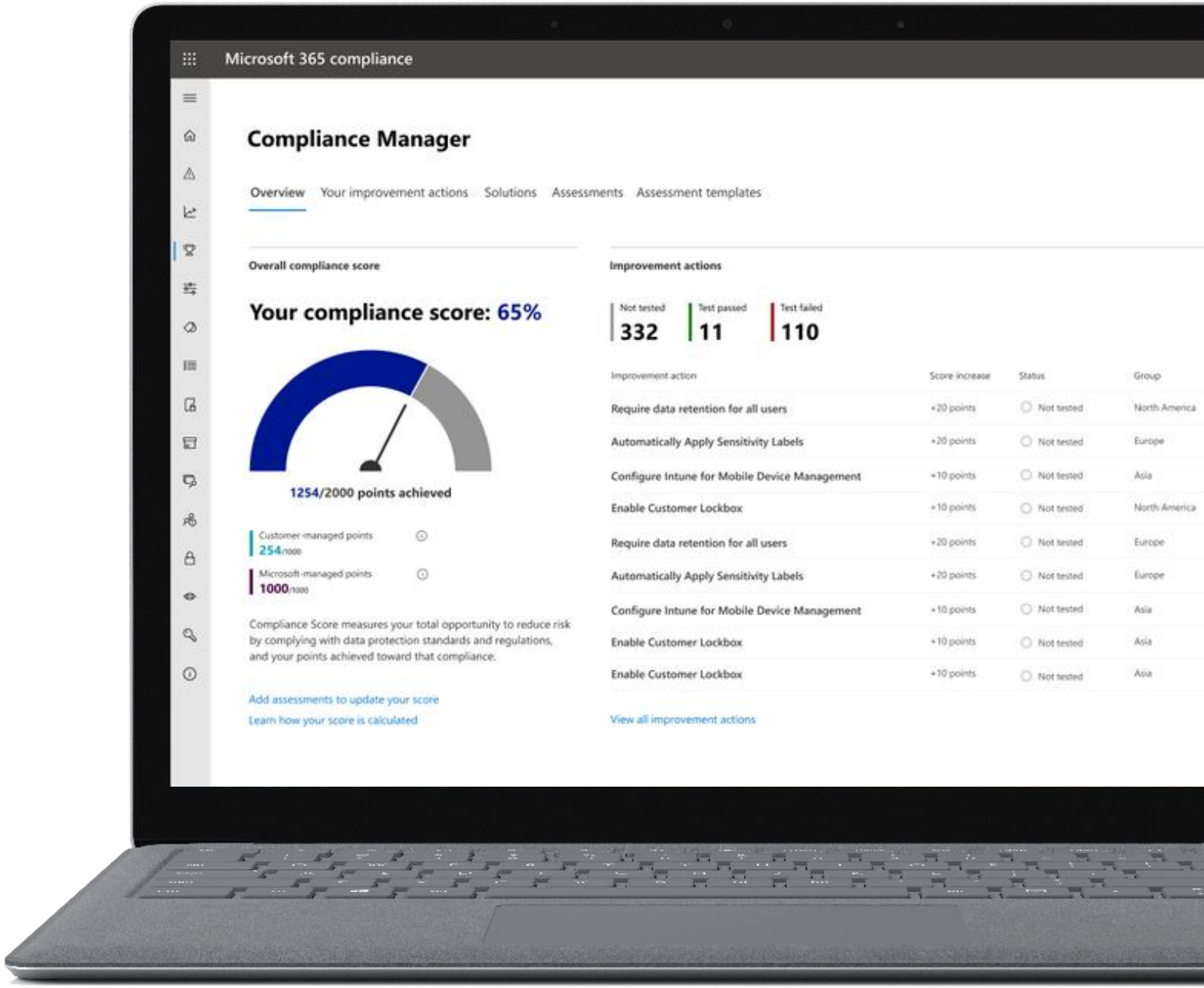


Hodnocení bezpečnosti

Certifikace a předpisy

Regulatorní předpisy

Informační bezpečnost

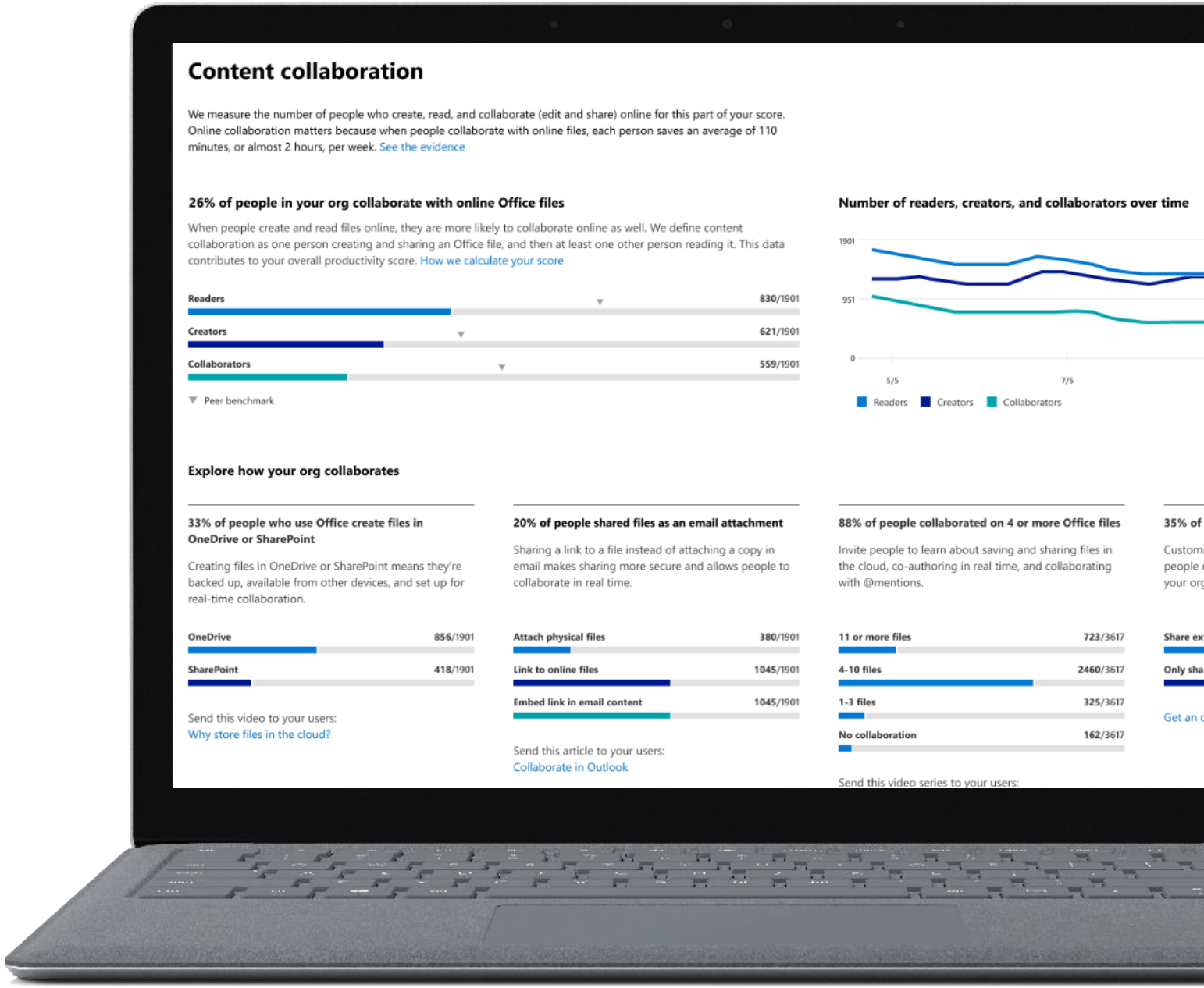


Hodnocení produktivity

Využití technologií

Adopce technologií

Technologie výhodou



Microsoft Defender
for Business

Elevate your security

- Threat & Vulnerability Management
- Attack Surface Reduction
- Next Generation Protection
- Endpoint Detection & Response
- Auto Investigation & Remediation

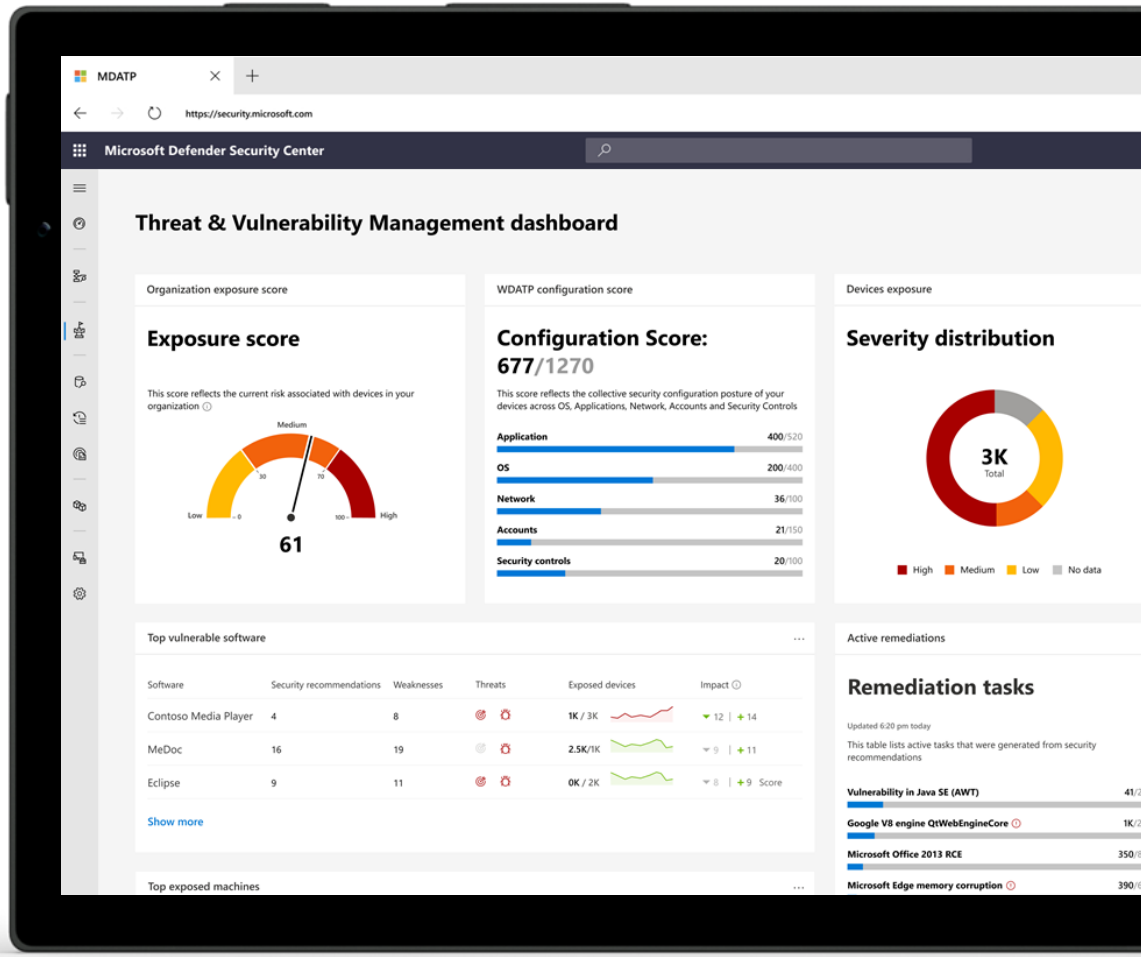
Simplified Onboarding and Administration

APIs and Integration

Threat & Vulnerability Management

A risk-based approach to mature your vulnerability management program

- Continuous real-time discovery
- Context-aware prioritization
- Built-in end-to-end remediation process



Home
Incidents & alerts
Hunting
Action center
Threat analytics
Secure score
Learning hub

Endpoints
Search
Device inventory
Vulnerability management
Dashboard
Recommendations
Remediation
Software inventory
Weaknesses
Event timeline
Partners and APIs
Evaluation & tutorials
Configuration management

Email & collaboration
Investigations

Selected device groups (3/3)

Security recommendations

Search security recommendations

Choose columns | Export | 30 items per page | 1-30 of 411

Security recommendation	OS platform	Weaknesses	Related component	Threats	Exposed devices	Stat...	Remediation type	Remediation activities	Impact	Ta
Update Rarlab Winrar to version 6.0.0.0	Windows	4	Rarlab Winrar		9 / 13	Active	Software update	0	20.30	
Update Microsoft .net Framework	Windows	10	Microsoft .net Fra...		9 / 26	Active	Software update	0	13.68	
Block JavaScript or VBScript from launching downl	Windows	1	Security controls (...		20 / 20	Active	Configuration chan...	0	13.55 + 9.(	
Block untrusted and unsigned processes that run f	Windows	1	Security controls (...		20 / 20	Active	Configuration chan...	0	13.55 + 9.(	
Update Adobe Acrobat Reader Dc	Windows	564	Adobe Acrobat R...		8 / 9	Active	Software update	2	13.02	
Block persistence through WMI event subscription	Windows	1	Security controls (...		18 / 18	Active	Configuration chan...	0	12.19 + 9.(	
Update Microsoft Windows 10 (OS and built-in ...	Windows	1083	Microsoft Windo...		6 / 16	Active	Software update	0	12.19	
Update Videolan Vlc Media Player	Windows	9	Videolan Vlc Med...		13 / 13	Active	Software update	1	10.87	
Uninstall Adobe Flash Player	Windows	21	Adobe Flash Player		6 / 9	Active	Software uninstall	0	10.45	
Update Mozilla Firefox to version 85.0.2.0	Windows	73	Mozilla Firefox		4 / 4	Active	Software update	0	8.85	
Update Python	Windows	28	Python		7 / 7	Active	Software update	0	8.15	
Block Office communication application from crea	Windows	1	Security controls (...		20 / 20	Active	Configuration chan...	0		


KPCS