Exchange Online
a OOP zabezpečení e-mailu

Petr Vlk


WE'RE ALL
GONNA
DIE

TLP: WHITE

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

PŘÍLOHA K Č.J. 8477/2021-NÚKIB-E/350 • BRNO • 11. ŘÍJNA 2021

VERZE DOKUMENTU: 1.0

OCHRANNÉ OPATŘENÍ K ZABEZPEČENÍ E-MAILŮ ZE DNE 11. 10. 2021

TLP: WHITE

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

PŘÍLOHA K Č.J. 8477/2021-NÚKIB-E/350 • BRNO • 11. ŘÍJNA 2021

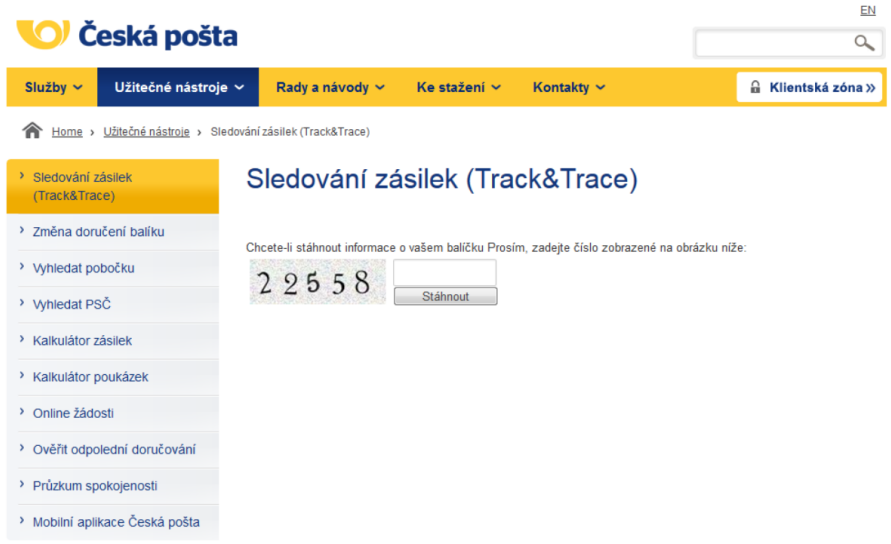
VERZE DOKUMENTU: 1.0

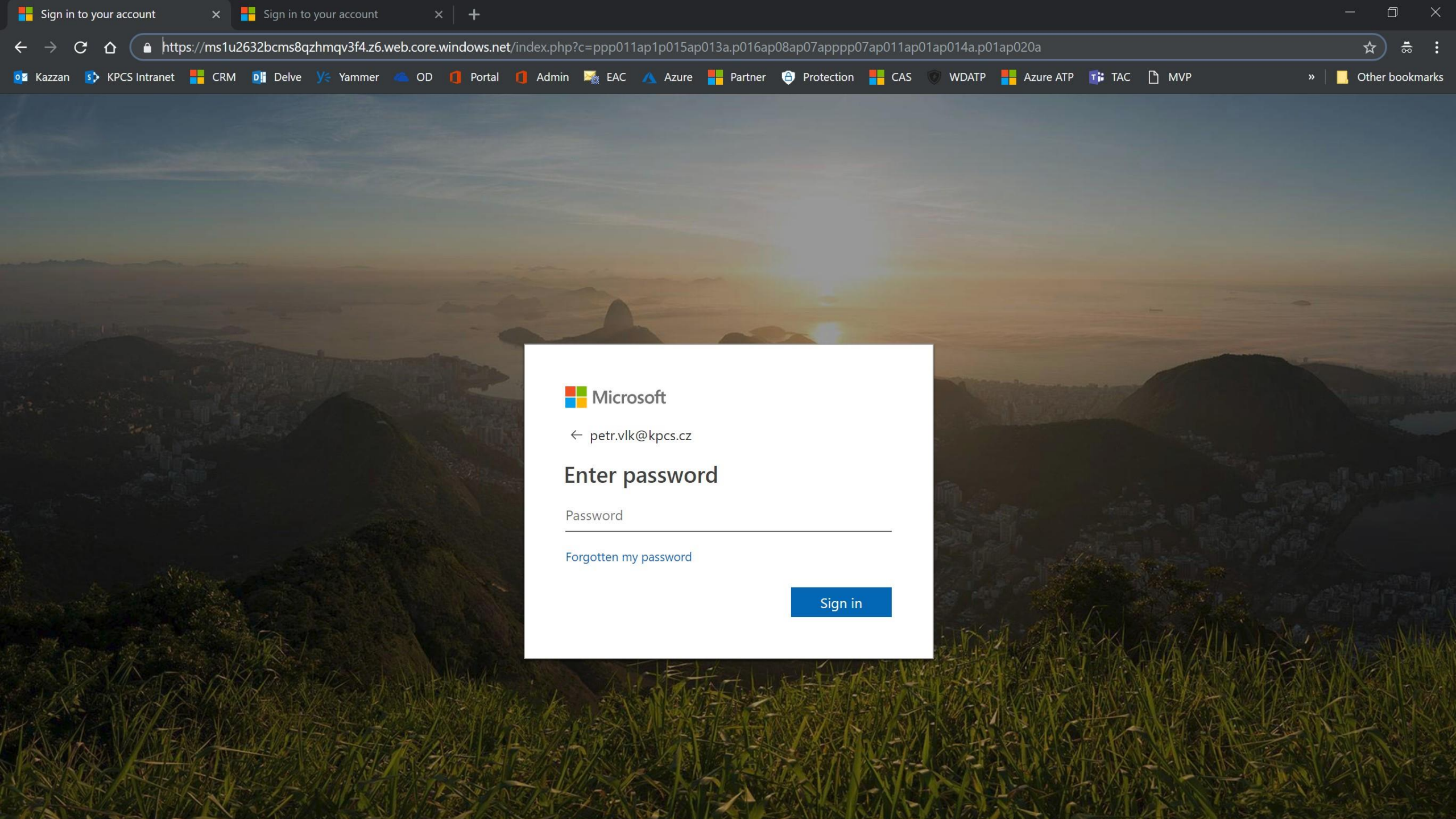
METODIKA K ZAVEDENÍ ZPŮSOBŮ ZVÝŠENÍ OCHRANY DLE OCHRANNÉHO OPATŘENÍ ZE DNE 11. 10. 2021

Aplikovatelnost

- GDPR
  - Ochrana osobních údajů a jejich zpracování
- Zákon o kybernetické bezpečnost
  - Kritické infrastruktury, významné informační systémy, předsednictví EU
- NIS2
  - Důležité segmenty průmyslu a obchodu
- Ostatní organizace
  - Víte, s kým si píší uživatelé?
  - Přece všichni dbáme na bezpečnost, že?

Phishing: Jedině na vzestupu




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

Co na to uživatel?

Úspěšných útoků přibývá

- Nemocnice Benešov - 2019
- Nemocnice Brno - 2019
- Městský úřad Prahy 3 - 2020
- Povodí Vltavy - 2020
- eD System – 2021
- SolarWinds 2021
- Microsoft - 2022
- Cisco - 2022
- Ředitelství silnic a dálnic - 2022

NÚKIB

- Národní úřad pro kybernetickou a informační bezpečnost
- Zákon o kybernetické bezpečnosti
  - Zákon č. 181/2014 Sb.
  - Pojmy, úřady, odpovědnosti, procesy
- Vyhláška o kybernetické bezpečnosti
  - Vyhláška č. 82/2018 Sb.
  - Organizační a technická opatření, bezpečnostní politiky a dokumentace
    - Bezpečnost komunikačních sítí, Kryptografické prostředky, …
  - Kybernetické incidenty
- 11. října 2021 vydává ochranné opatření k zabezpečení e-mailů
  - Metodický pokyn, termíny implementace, technologie, požadavky

Čas na paniku?

- 1. leden 2023
  - 109 dnů
  - 3 měsíce a 19 dnů
  - co nevidět
  - dřív, než si myslíme
  - kvartál a kus
  - většinu si lze ověřit z veřejného internetu

Co s tím?

- Nyní zachovejte klid.
- Teď začněte panikařit.

- Možnosti řešení?
  - Ignorace (ono to vyšumí)
  - Slova, věty a výjimky (směrnice)
  - Překotné nastavení (hned teď)
  - Zdrženlivé nastavení (1. ledna 2023)
  - Skutečné nastavení (s auditem)

OOP

- „Občanům a soukromým společnostem nehrozí žádné omezení běžné komunikace s úřady.“
- „Dobrovolné zavedení technologií a postupů popsaných v opatření každopádně doporučujeme také organizacím, které nespadají pod zákon o kybernetické bezpečnosti. Používáním doporučených technologií mohou zásadním způsobem zvýšit zabezpečení své elektronické pošty.“

- Kolik incidentů o nedoručené poště řešíte dnes?

OOP

- „Zavedení způsobů zvýšení ochrany nemůže omezit doručování e-mailových zpráv ze strany veřejnosti, případně interně v rámci organizace. V případě řádné implementace ochranného opatření tak povinným osobám nehrozí žádné omezení odesílání a doručování elektronické pošty, ať už interně nebo externě.“

- Kolik z toho díky špatné implementaci SPF, DKIM a DMARC?

E-mail

- Co je to vlastně e-mail?
  - MX? (Hosting?)
  - Poštovní server? (Exchange?)
  - Klient? (Outlook?)
  - Přenos internetem? (cloud?)
  - Přenos datovou sítí? (LAN?)
  - Služba pro rozesílání e-mailů? (SendGrid, MailChimp, SmartEmailing, …)
  - DMS? (SharePoint)
  - Datová schránka? (Spisová služba?)
  - Váš fajn notifikační skript? (PowerShell Send-MailMessage?)

Exchange jako Exchange

- Exchange Online
  - Závisí na MSFT

- Exchange Server
  - Závisí na IT
  - Závisí na Windows Server
  - Závisí na .NET komponentách
  - Závisí na publikační službě (AD FS, WAP, WAF, Load Balancer, FW…)
  - Nemá podporu pro celou sadu technologií

Přenos zpráv

- STARTTLS
- TLS v1.2 a novější
- TLS v1.0 a v1.1 jen v odůvodněných případech
- SSL v3 a starší jsou zakázány
- Kryptografické prostředky dle doporučení úřadu
  - https://docs.microsoft.com/en-us/microsoft-365/compliance/technical-reference-details-about-encryption?view=o365-worldwide

Cipher suite name	Key exchange algorithm/strength	Forward secrecy	Cipher/strength
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH/192	Yes	AES/256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH/128	Yes	AES/128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH/192	Yes	AES/256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH/128	Yes	AES/128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH/192	Yes	AES/256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH/128	Yes	AES/128
TLS_RSA_WITH_AES_256_GCM_SHA384	RSA/112	No	AES/256
TLS_RSA_WITH_AES_128_GCM_SHA256	RSA/112	No	AES/256

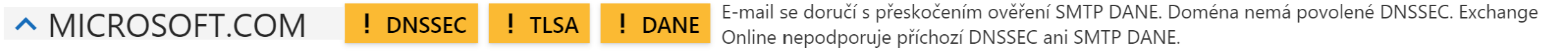
Přenos zpráv

- Validní certifikát od veřejně uznávané certifikační autority
- Název domény odpovídá certifikátu

Attribute	Value
Certificate authority root issuer	DigiCert CA - 1
Certificate name	mail.protection.outlook.com
Organization	Microsoft Corporation
Organization unit	www.digicert.com
Certificate key strength	2048

Přenos zpráv

- *DNS záznamy domény chráněné pomocí DNSSEC*
  - *Domain Name System Security Extensions*
- *TLSA záznamy publikované v souladu s DANE*
  - *TLS Authentication*
  - *DNS-Based Authentication of Named Entities*
- MTA-STS jako volitelné rozšíření
  - MTA Strict Transport Security



Poštovní klienti

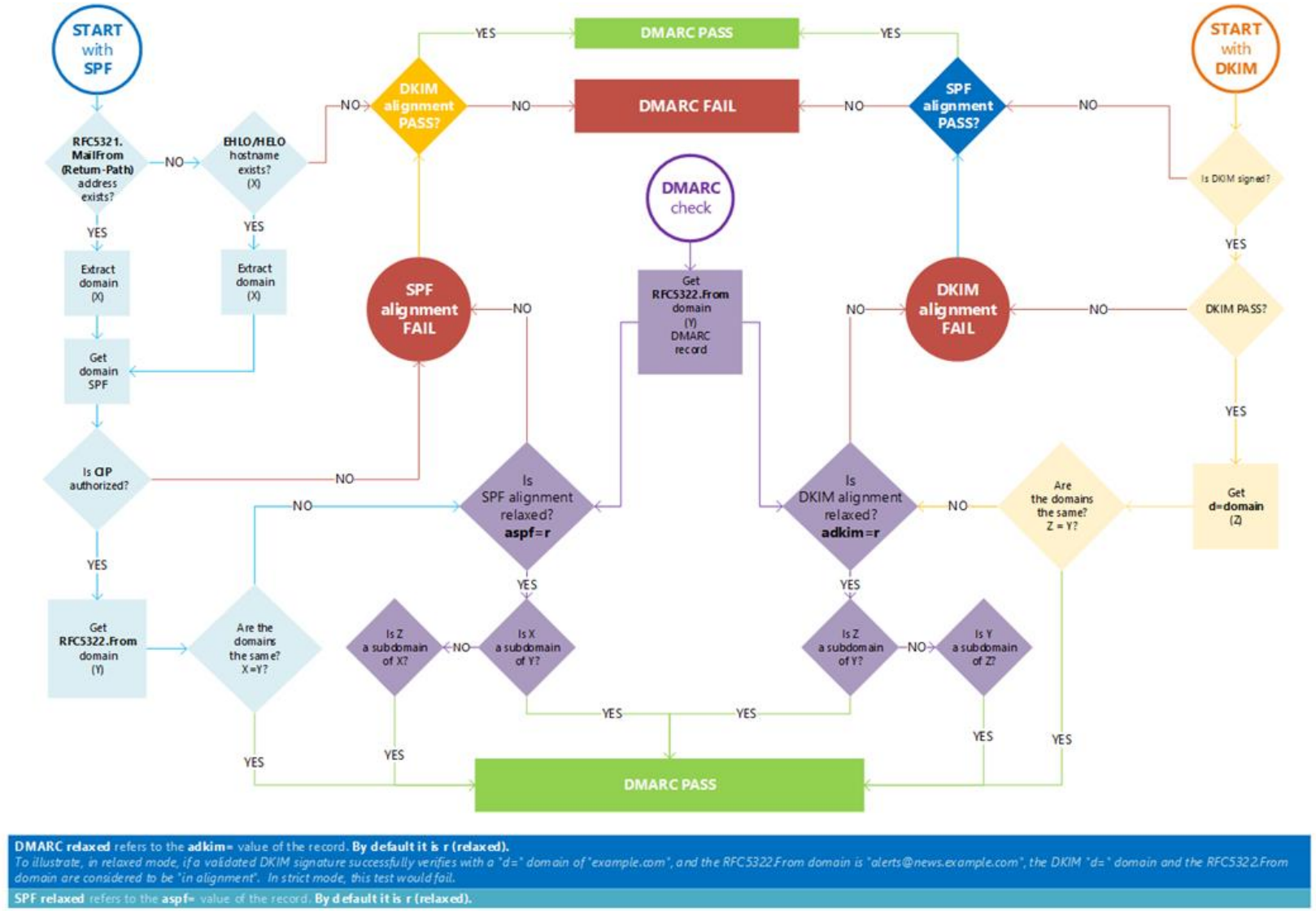
- SMTPS
- IMAPS
- POP3S
- HTTPS
- HSTS

- Outlook
- OWA

Bezpečnost komunikace

- SPF
  - Sender Policy Framework
  - Soft Fail / Hard Fail
- DKIM
  - DomainKeys Identified Mail
  - Hlavičky From and Subject
- DMARC
  - Domain-based Message Authentication, Reporting and Conformance
  - Quarantine / Reject
  - Sampling Rate 100

Je to vlastně jednoduché…



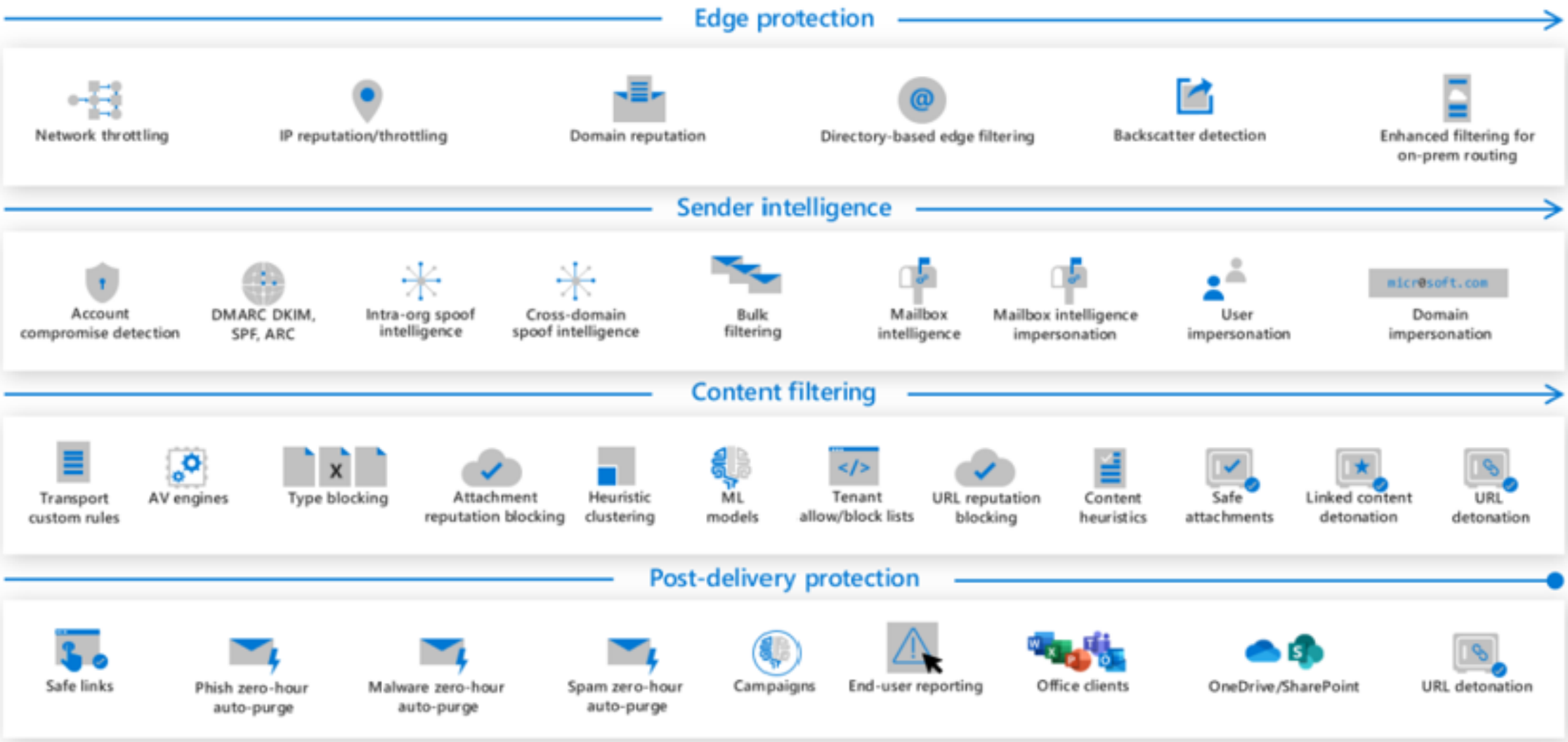
DMARC relaxed refers to the **adkim=** value of the record. **By default it is r (relaxed).**
To illustrate, in relaxed mode, if a validated DKIM signature successfully verifies with a "d=" domain of "example.com", and the RFC5322.From domain is "alerts@news.example.com", the DKIM "d=" domain and the RFC5322.From domain are considered to be "in alignment". In strict mode, this test would fail.

SPF relaxed refers to the **aspf=** value of the record. **By default it is r (relaxed).**

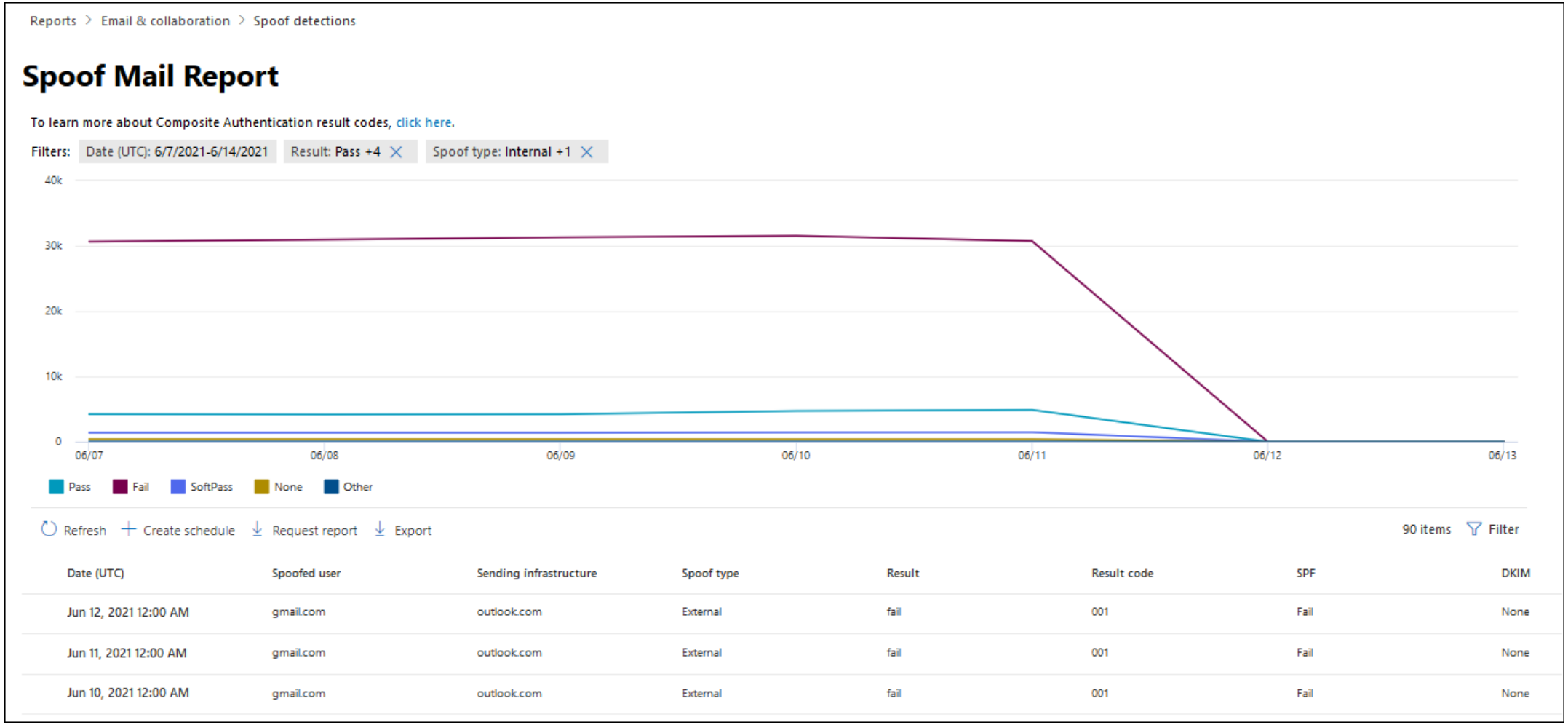
Microsoft záchranou

- Technologie
  - Exchange Online (Protection)
  - Defender for Office 365
  - Exchange Server
- Příručka pro správce

Defender for Office 365



AntiPhishing

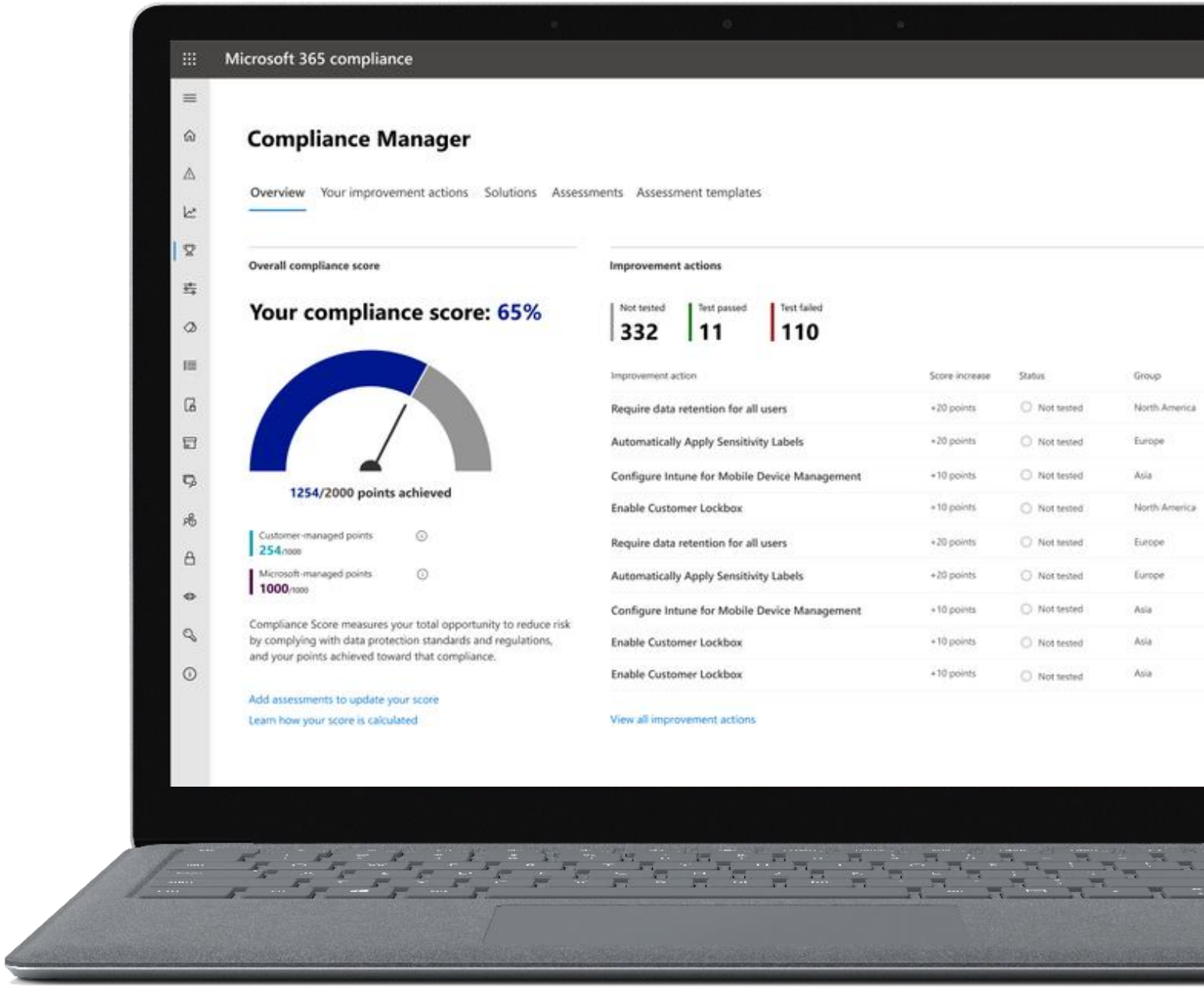


Evidence souladu

Compliance Manager

Secure Score

Audit Reports

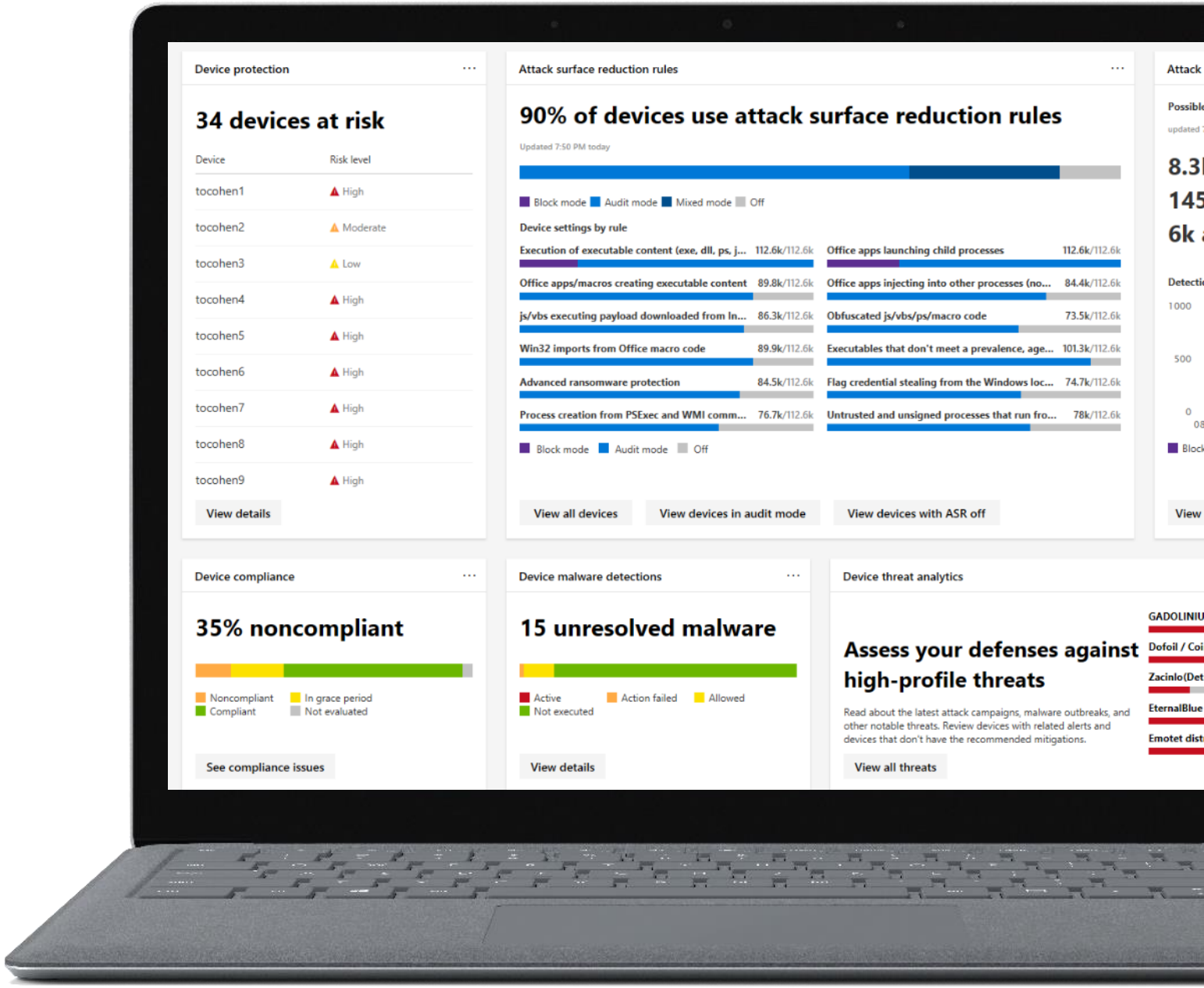


Nejen na papíře

Security Center

Exchange Online (Protection)

Defender for Office 365



Zdroje

- Email authentication in Microsoft 365 - Office 365 | Microsoft Docs
- Set up SPF to help prevent spoofing - Office 365 | Microsoft Docs
- How to use DKIM for email in your custom domain - Office 365 | Microsoft Docs
- Use DMARC to validate email, setup steps - Office 365 | Microsoft Docs
- Valimail | Welcome to Authenticate
- My Email Communications Security Assessment (MECSA) (europa.eu)
- MX Lookup Tool - Check your DNS MX Records online - MxToolbox


KPCS