

Exchange Online a OOP zabezpečení e-mailu



Petr Vlk



KPCS



WE'RE ALL
GONNA
DIE

Národní úřad
pro kybernetickou
a informační bezpečnost

TLP: **WHITE**

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**

Národní úřad
pro kybernetickou
a informační bezpečnost

TLP: **WHITE**

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



Vítejte u zákazníka

Drive jste své údaje aktualizovali, a proto musíte dokončit proces aktualizace tak, abyste měli přístup ke všem službám a můžeme chránit vaše data **Aktualizujte svůj účet**

Prejeme Vám pekný den

Jirí Tutsch / Manažer kontaktního centra
Air Bank a.s. / clen skupiny PPF

Air Bank a.s. / Evropská 2690/17 / 160 00 Praha 6 / IC 29045371
Společnost zapsaná u rejstříkového soudu v Praze, spisová značka B 16013

http://www.jetdrop.co.uk/bio/tema/Sk... Přihlášení SERVIS 24 | Česká...
Soubor Úpravy Zobrazit Oblíbené položky Nástroje Nápověda

SERVIS 24
INTERNETBANKING

Hledat v Internetbankingu a na webu Flo + Nový produkt Nastavení Odtáhnout

Nástěnka Poslat peníze Přehledy Platební karty Šablony Informace o účtu

Ověření vašich osobních údajů

Každoroční aktualizace vašich osobních údajů

Čas příjmu dočasného kódu pomocí SMS závisí na vaší síti. Za více než 3 minuty :

2:17

Chcete-li dokončit žádost o opětovné zapnutí, zadejte prosím váš referenční kód obdrženy pomocí SMS :

Potvrdit

ČESKÁ spořitelna
Bezpečnost | Kontakty | O službě | Pro nevidomé | Demo | Více informací
2016 © Česká spořitelna, a. s. - všechna práva vyhrazena.

Česká pošta

Služby Užitečné nástroje Rady a návody Ke stažení Kontakty Klientská zóna

Home Užitečné nástroje Sledování zásilek (Track&Trace)

Sledování zásilek (Track&Trace)

Chcete-li stáhnout informace o vašem balíčku Prosím, zadejte číslo zobrazené na obrázku níže:

22558 Stáhnout

- Sledování zásilek (Track&Trace)
- Změna doručení balíku
- Vyhledat pobočku
- Vyhledat PSČ
- Kalkulátor zásilek
- Kalkulátor poukázek
- Online žádosti
- Ověřit odpolední doručování
- Průzkum spokojenosti
- Mobilní aplikace Česká pošta



← petr.vlk@kpcs.cz

Enter password

Password

[Forgotten my password](#)

Sign in

Co na to uživatel?

 MINISTERSTVO PRÁCE
A SOCIÁLNÍCH VĚCÍ

Příspěvek na bydlení k dispozici pro vás

Dobrý den.
Jsme rádi, že jste s námi. Na těchto stránkách vám poskytneme veškeré informace a podporu, kterou potřebujete k získání dávek na bydlení. Vzhledem k současné netežké situaci pro mnohé z nás jsme se rozhodli pro zásadní změny v oblasti benefitů na bydlení.

Jedním z výsledků je nejjednodušší forma pobírání dávek za pár minut bez opuštění domova. Všichni dosavadní příjemci dávek na bydlení navíc mohou v novém online prostředí provádět pravidelné platby.

Cílem ministerstva sociálních věcí a zdravotnictví je co nejvíce usnadnit vám pobírání dávek a omezit zbytečnost na minimum.



Po přepočtu máte příspěvek na bydlení
6.084 Kč měsíčně.

 MINISTERSTVO PRÁCE
A SOCIÁLNÍCH VĚCÍ

[Působnost MPSV](#) - [Státní sociální podpora](#) - [Jednorázový příspěvek na dítě](#)

Jednorázový příspěvek 5000 Kč na dítě

Jednorázový příspěvek na pomoc rodinám s dětmi přichází na začátku školního roku.

Tato stránka vám poskytne veškeré informace o tom, jak o příspěvek požádat a komu je určen.

Inflaci a růst životních nákladů v současné situaci asi pociťuje každý. Jednou z nejzranitelnějších skupin jsou právě domácnosti, ve kterých žijí děti.

Naším cílem je pomoci co největšímu počtu z nich, proto rodinám se středními a nízkými příjmy vyplatíme jednorázový příspěvek 5 000 Kč na každé dítě.



1,1 milionu domácností má nárok na
jednorázový příspěvek 5000 Kč na dítě

 MINISTERSTVO PRÁCE
A SOCIÁLNÍCH VĚCÍ

Ministry - Media and public - Press releases of the ... - Year 2022

- Fake domains imitate the website of the Ministry of Labour and Social Affairs. It's phishing, the site is already blocked

Press Releases 2022

Filter by month
Select from the list...

Fake domains imitate the website of the Ministry of Labour and Social Affairs. It's phishing, the site is already blocked

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

- 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 popsanych v opatření každopádně doporučujeme také organizacím, které nespádají 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

^ MICROSOFT.COM

! DNSSEC

! TLSA

! DANE

E-mail se doručí s přeskočením ověření SMTP DANE. Doména nemá povolené DNSSEC. Exchange Online nepodporuje příchozí DNSSEC ani SMTP DANE.

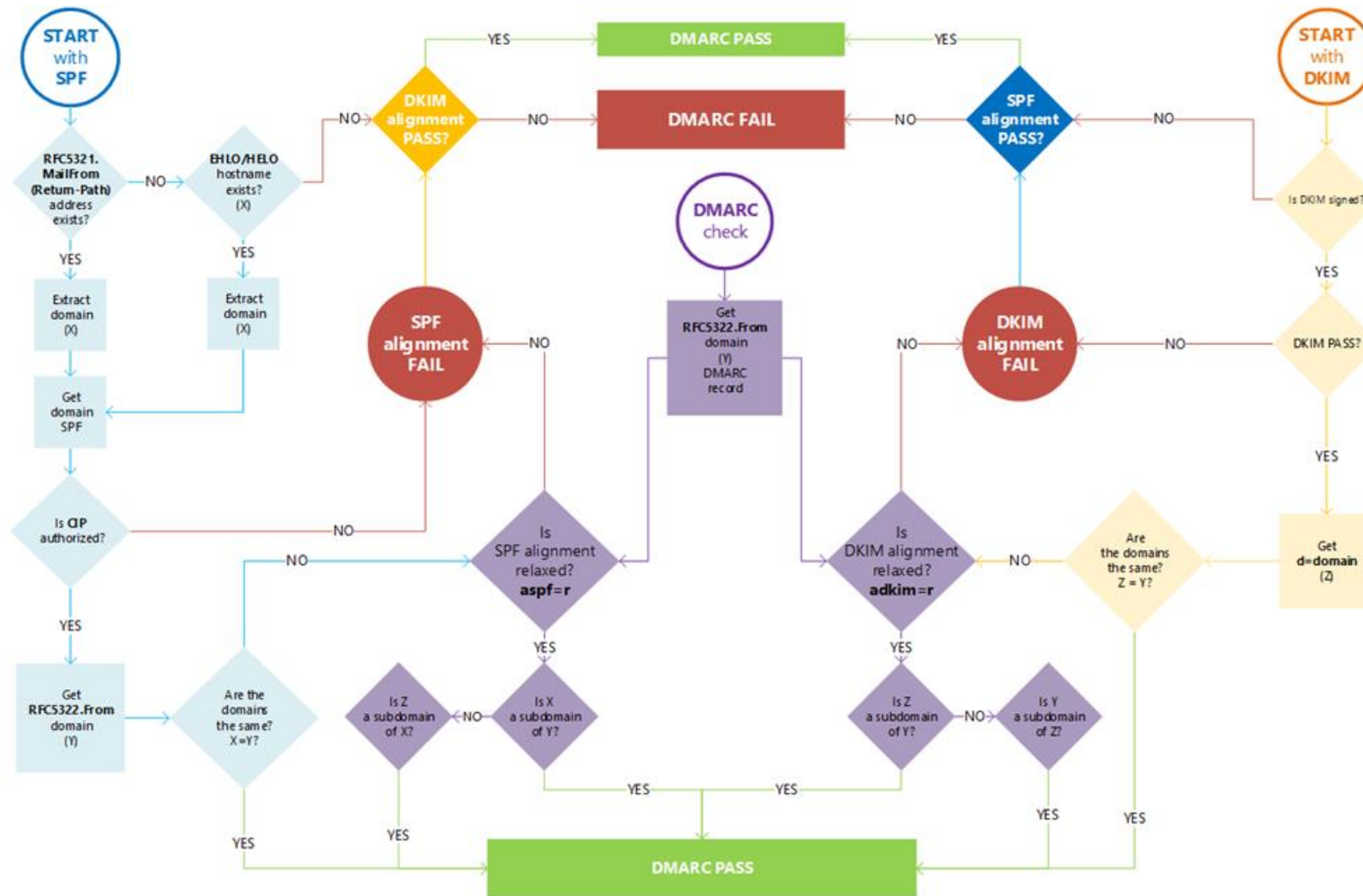
Poštovní klienti

- 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



Technické doporučení
pro Exchange Online a
Exchange Server na
základě ochranného
opatření NÚKIB

Datum: 31.10.2021

Verze 1.1

Připravili:

Jaroslav Zikmund

Senior Customer Engineer

jaroslav.zikmund@microsoft.com

Dalibor Kačmář

National Technology Officer

dalibor.kacmar@microsoft.com

Defender for Office 365

Edge protection



Sender intelligence



Content filtering



Post-delivery protection



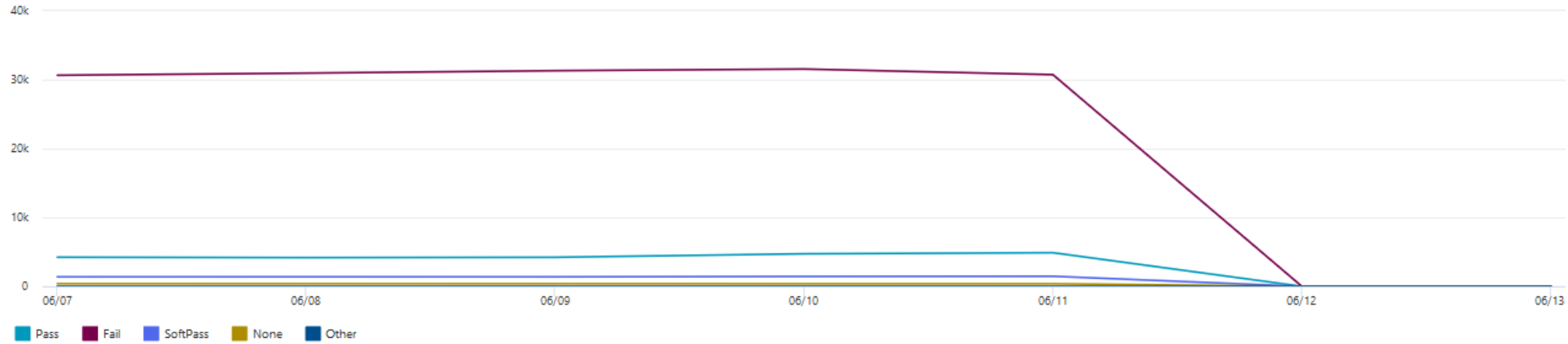
AntiPhishing

Reports > Email & collaboration > Spoof detections

Spoof Mail Report

To learn more about Composite Authentication result codes, [click here](#).

Filters: Date (UTC): 6/7/2021-6/14/2021 Result: Pass +4 Spoof type: Internal +1



Refresh + Create schedule ↓ Request report ↓ Export

90 items Filter

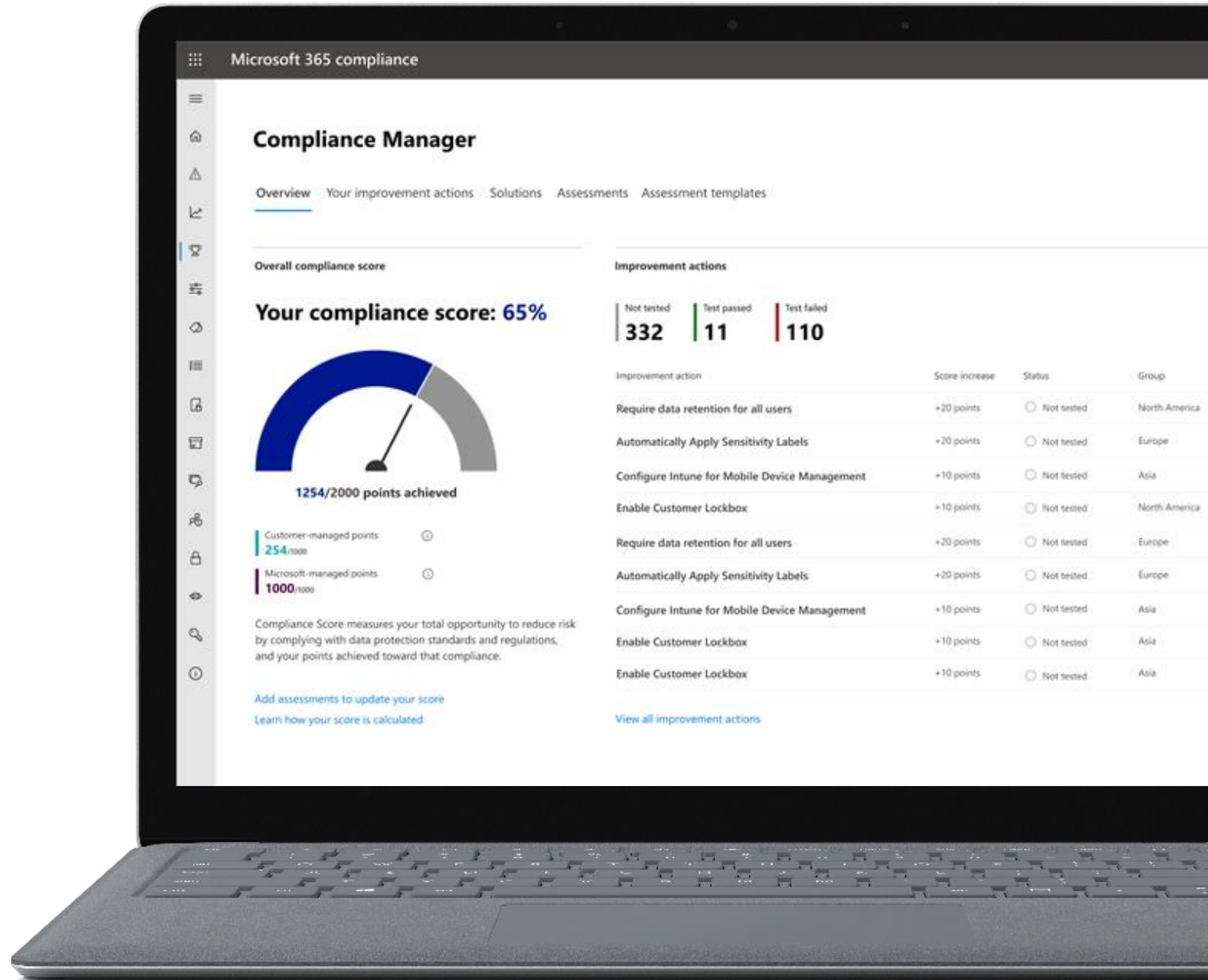
Date (UTC)	Spoofed user	Sending infrastructure	Spoof type	Result	Result code	SPF	DKIM
Jun 12, 2021 12:00 AM	gmail.com	outlook.com	External	fail	001	Fail	None
Jun 11, 2021 12:00 AM	gmail.com	outlook.com	External	fail	001	Fail	None
Jun 10, 2021 12:00 AM	gmail.com	outlook.com	External	fail	001	Fail	None

Evidence souladu

Compliance Manager

Secure Score

Audit Reports

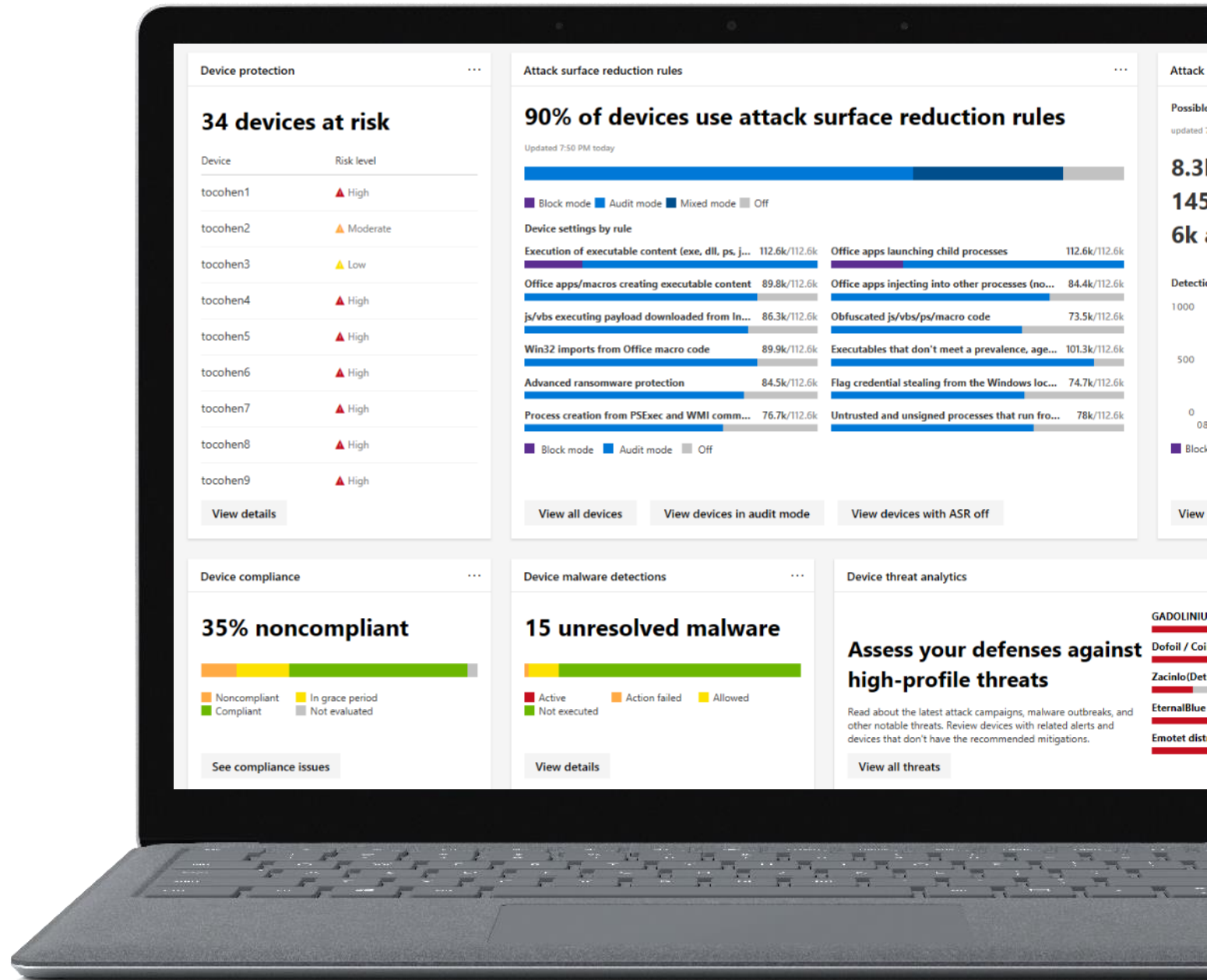


Nejen na papíře

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