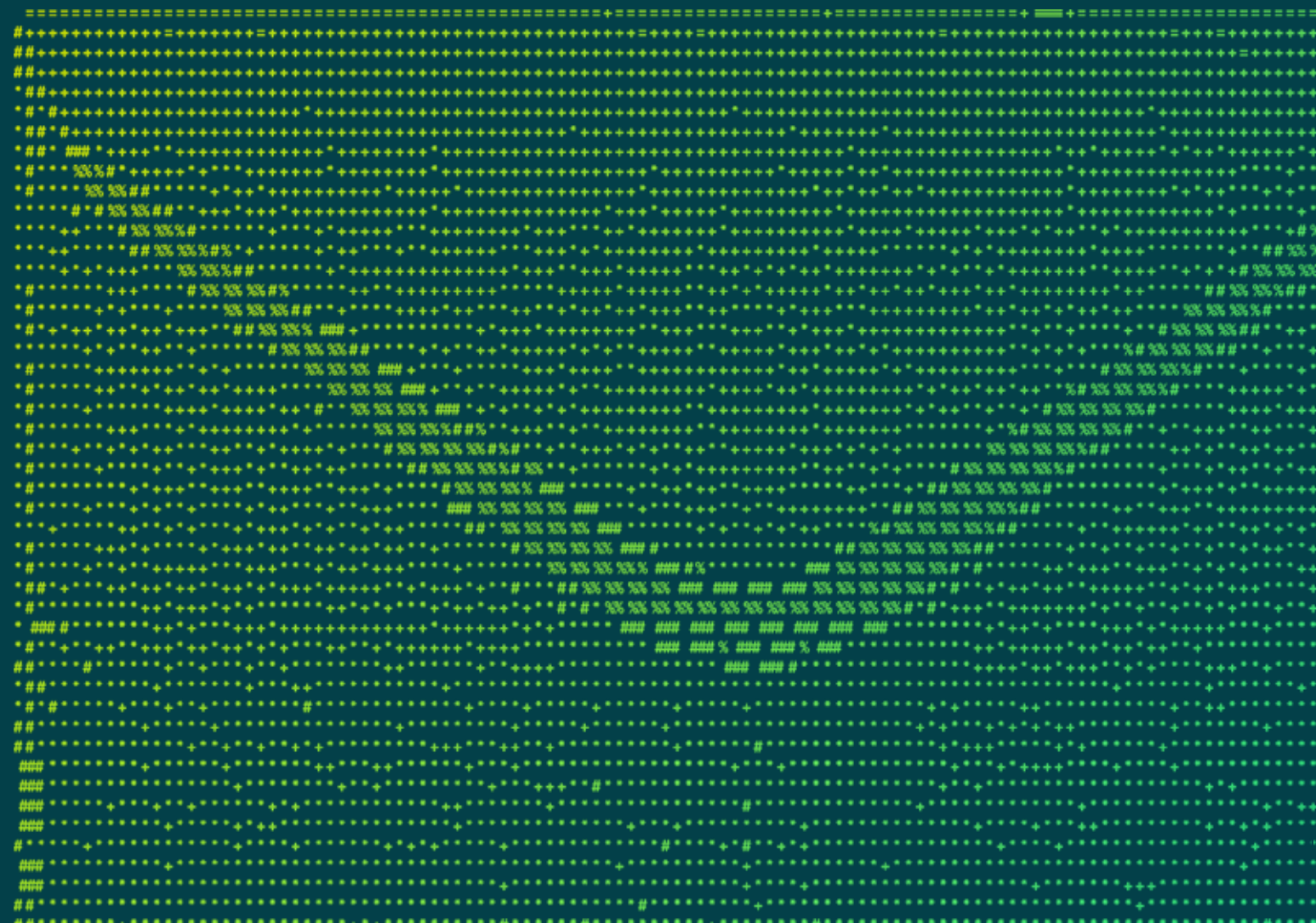
Exchange Online – „epic fails“

SEPPMAIL

Erfahrungen als europäischer Mail-Service-Provider



Roman Stadlmair
Country Manager Austria

+43 676 43 16 002
roman.stadlmair@seppmail.com
seppmail.com







MVP
Microsoft®
Most Valuable Professional

Standorte SEPPMAIL.cloud



VBSpam Q4/2023 Bericht

https://www.virusbulletin.com/virusbulletin/2023/12/vbspam-comparative-review/

Hosted solutions	Anti-malware	IPv6	DKIM	SPF	DMARC	Multiple MX-records	Multiple locations
Mimecast	Mimecast		√	√	√	√	√
N-able Mail Assure	N-able Mail Assure	√	√	√	√		
N-able SpamExperts	SpamExperts	√	√	√	√		
Net At Work NoSpamProxy	32Guards & NoSpamProxy		√	√	√	√	√
SEPPmail.cloud Filter	SEPPmail	√	√	√	√	√	√
Zoho Mail	Zoho		√	√	√	√	√

Aktueller VB-SPAM Report









Kleines 1x1 des E-Mail-Empfanges

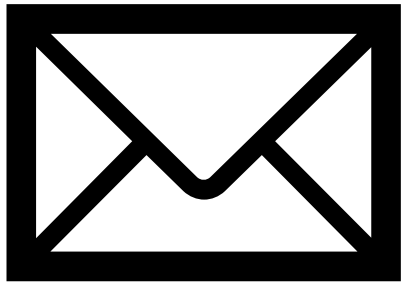
SPF, DKIM und DMARC erklärt

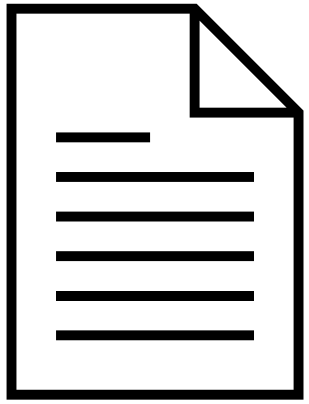


Das Drama beginnt mit …

Envelope FROM
(MAIL FROM)

Für den Empfänger nicht sichtbar
Bounce Adresse
SPF-relevant

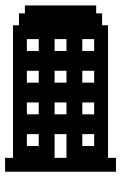




Header FROM

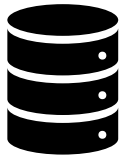
Sichtbar für Empfänger
Durch DKIM signiert
Bounce Adresse
SPF-relevant

SPF: Sender Policy Framework

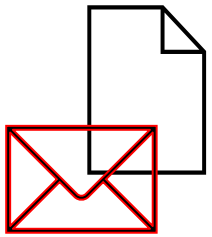


MAIL FROM: gutefirma.at

DNS



v=spf1 include:spf.gutefirma-at.seppmail.cloud -all





MAIL FROM: angreifer.at

v=spf1 ipv4:203.0.113.113 -all

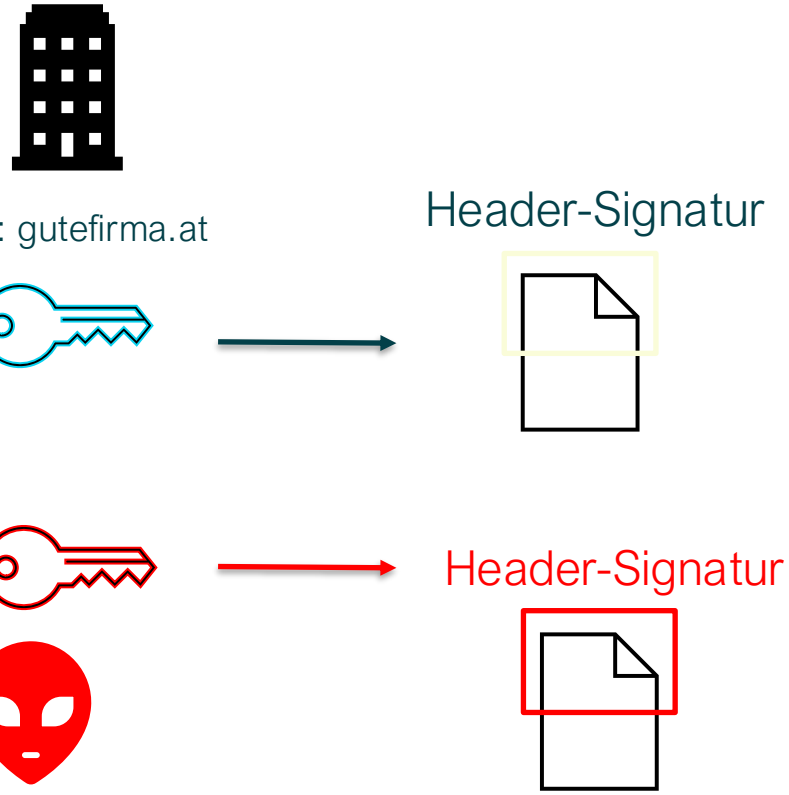
2 Probleme:
1. Spoofing mittels MAIL FROM HEADER
(Weil jeder so einen Eintrag erstellen kann)

2. Weiterleitungen bringen SPF-Fehler

DKIM: Domain Keys Ident. Mail

Lösung des Mail-Weiterleiten Problems

Sendender Server signiert den Header einer E-Mail,
Empfänger kann mittels Public-Key Signatur prüfen





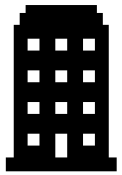
Problem:

Spoofing mittels signiertem HEADER FROM

Domain-based Mess. Auth, Report & Conformance

Mail FROM / MAIL Header Lösung

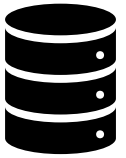
Sendender Server bestimmt wie mit FROM / MAIL FROM / DKIM Fehlern umgegangen wird.



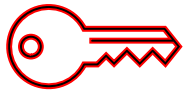
gutefirma.at

Wie sollen Empfänger mit Fälschungen umgehen ?

DNS



_dmarc.gutefirma.at {v=DMARC; p=reject; pct=100}





MAIL FROM: angreifer.at

Lösung
DMARC führt SPF und DKIM zusammen.
- FROM und MAIL FROM müssen gleich sein
- FROM Header <-> DKIM Public Key

eine der beiden muss erfüllt sein.

Landromarc

Wie man mit Exchange Online E-Mails weißwaschen kann.

https://www.engagesecurity.nz/blog/laundromarc

(3. Dezember 2025)

Es begann 2018 …

https://techcommunity.microsoft.com/blog/exchange/sender-rewriting-scheme-srs-coming-to-office-365/607932

EXCHANGE TEAM BLOG 3 MIN READ

Sender Rewriting Scheme (SRS) coming to Office 365

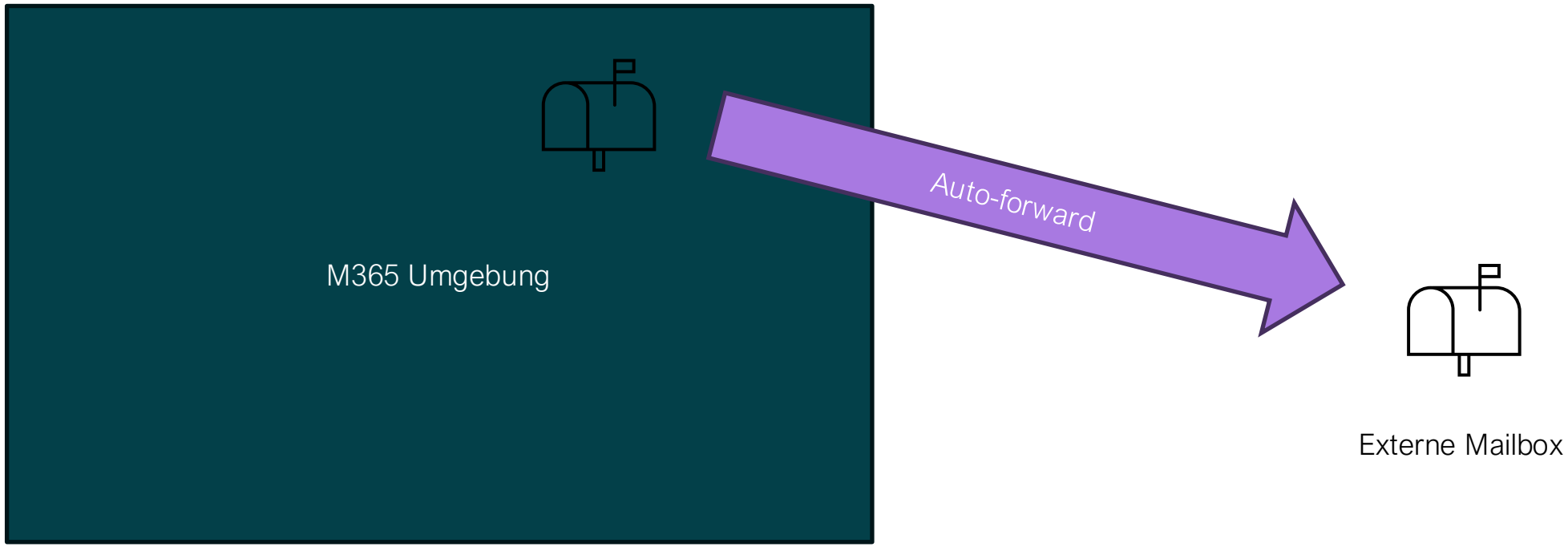


The_Exchange_Team Platinum Contributor

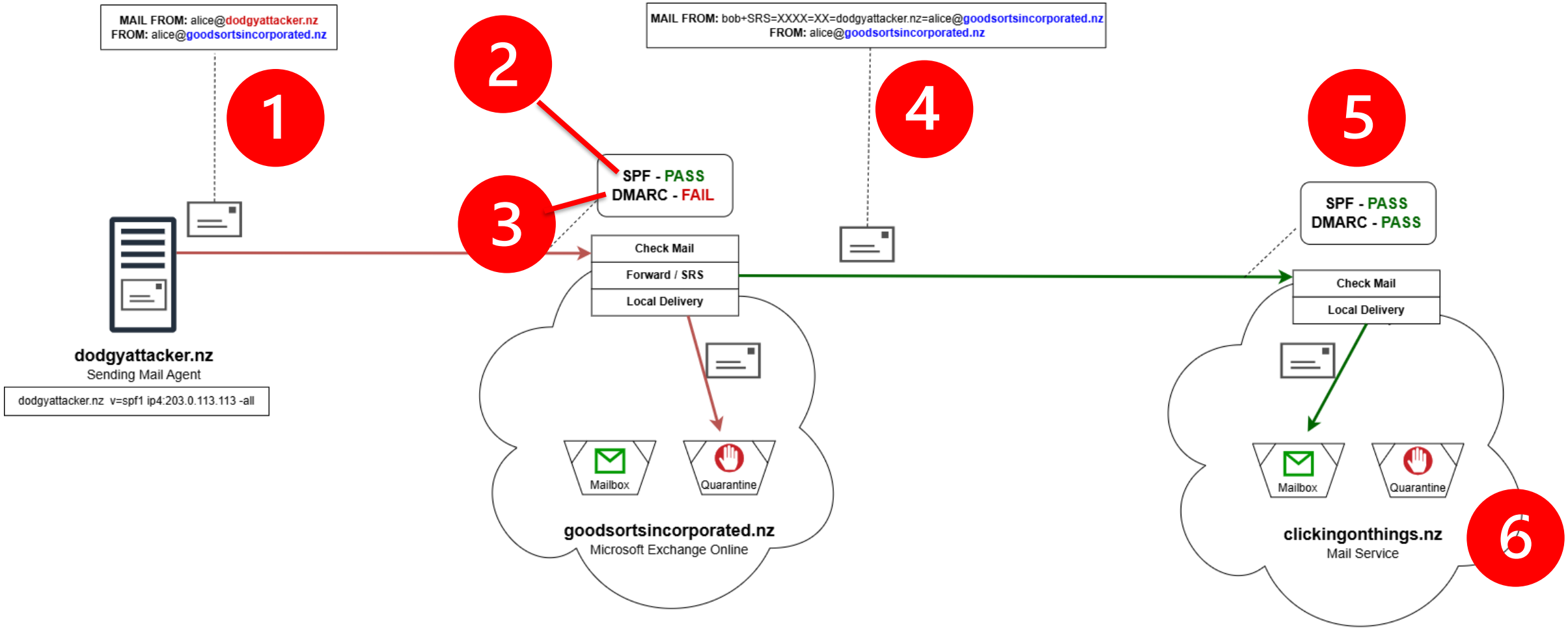
Jun 15, 2018

The introduction of email authentication mechanisms like SPF, DKIM, and DMARC have improved email security and spoofing prevention. However, some scenarios have been disrupted by these authentication mechanisms, namely auto-forwarding and relaying. Here in Office 365, we are committed to ensuring the security of our customers and the general integrity of the email ecosystem that we are a part of. From July 16th, we will begin rolling out Sender Rewriting Scheme (SRS) functionality to solve the problem of auto-forwarding being incompatible with SPF. The SRS feature will rewrite the *P1 From* address (also known as the *Envelope From* address) for all applicable messages being sent externally from Office 365. The *From* header (also known as *Display From* address or *P2 From* address) which is displayed by email clients will remain unchanged. This change will improve

Einfach mal E-Mail weiterleiten



Microsoft Sender Rewriting Scheme



Es war bekannt …

https://www.linkedin.com/pulse/spoofing-vulnerability-exchange-online-raffaele-colavecchi-hfcof

Spoofing mail flow

Spoofing vulnerability in Exchange Online



Raffaele Colavecchi
Microsoft MVP (M365: Exchange, Teams) | MCT | DMARC Warlock | Modern Work Architect @Penta

19. Februar 2024

This post is a detailed fact and analysis of a probable Exchange Online security problem present on 01/26/2024 and personally experienced. We will highlight the behavior of an incoming spoofing email in our Microsoft 365 tenant and its redirection to another mailbox managed by another Microsoft 365 tenant of one of our partners. We will inevitably get into the technical intricacies of the SPF, DKIM, DMARC and ARC protocols ending with some general pointers.

Gegenmaßnahmen

Mail-Forwarding generell unterbinden.

MX-Record weg von Microsoft

Infotech

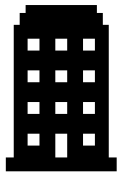
SEPPMAIL.cloud

DKIM WTF ?

Wie man DKIM so falsch wie möglich einsetzen kann

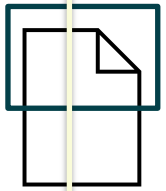
Automatisches Domain Keys Identified Mail by Exchange Online

contoso.at ➔ Kein DKIM Key konfiguriert



contosoat.onmicrosoft.com

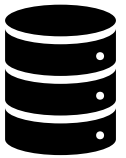
Header-Signatur



Empfänger

Lookup ➔ FAIL

DNS



~~Public Key~~

Problem:
E-Mails sind DKIM signiert, DNS Lookup schlägt fehl

Das Problem

Hi @Roman,

Thanks for sharing the details.
As per my initial analysis, yes, the public keys are not available for the domain([redacted].onmicrosoft.com) for both the selectors 1 and 2 .(odd scenario)
Since we see private keys in email headers, I can confirm that DKIM is enabled for the domain '[redacted].onmicrosoft.com' but it is not working due to underlying issues with public keys.

There are 2 ways to solve this.

1) Tenant can either disable and enable the DKIM config (or) if that doesn't work, they can try key rotation if available. (I cannot tell what's their scenario at present since I don't have access to their tenant)
2) If they wanted to report this as a issue to engineering , they can file a support ticket .

Thanks.

Gegenmaßnahmen

Nicht von onmicrosoft.com senden

*.onmicrosoft.com

nicht als Tenant Default domain konfigurieren

MX-Record weg von Microsoft

Infotech

SEPPMAIL.cloud

Weitere Probleme zum Nachlesen

Alias-Rewriting

Man sendet an nv.nn@contoso.at und bekommt eine antwort von vn.nn@fabrikam.at

DMARC Spoofing durch senden an Gruppe

https://www.linkedin.com/posts/alexshakhov_dmarc-cybersecurity-emailsecurity-activity-7404110369557975040-vDgN?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAAQIKgBHEhbz6whySXqojjCMv7IuFqit_U



False positives in Quarantäne

https://admin.cloud.microsoft/?source=applauncher#/servicehealth/history/:/alerts/EX1227432

Ignorieren von SPF, DKIM, DMARC

https://techcommunity.microsoft.com/blog/exchange/introducing-more-control-over-direct-send-in-exchange-online/440879

Die Allzweck-Gegenmaßnahme



MX weg von Microsoft !

Danke!

SEPPMAIL

https://www.seppmail.com/at

