Eigene Domains vor E-Mail-Spoofing schützen

Thomas Fauser, DMARC24

ISACA Chapter Meeting 22.12.2022

DMARC24
Security & Deliverability

Warum E-Mail-Spoofing?

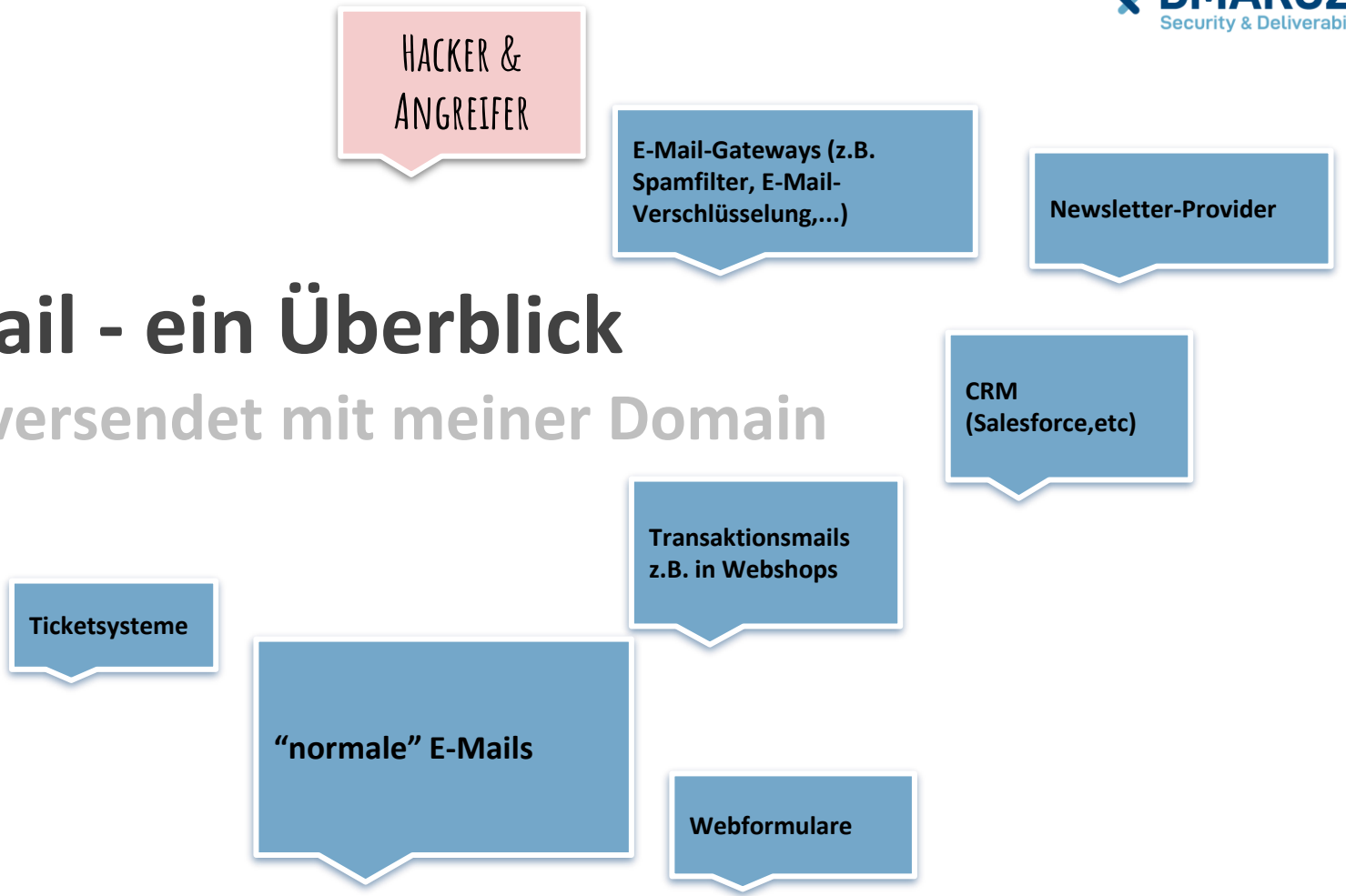
Wie ich zum Thema E-Mail-Spoofing kam

- Unternehmensdomain wurde gespooft
- Spamfilter erkannte es nicht zuverlässig
- Anforderungen von Kunden aus dem Ausland
- Intensives Spoofing bei nicht für E-Mails genutzten Domains entdeckt
- Security Awareness für Nutzer wird etwas einfacher

DMARC24
Security & Deliverability

E-Mail - ein Überblick

Wer versendet mit meiner Domain



DNS (Domain Name System)

Bekannte Funktion:

- Domain in IP-Adresse umwandeln

Zusätzlich:

- MX-Einträge zeigen, welcher Server E-Mails empfängt
- TXT-Einträge für weitere zentrale Informationen
  Durch Domaineigentümer gepflegt

DMARC24
Security & Deliverability

SPF (Sender Policy Framework)

- Definiert, wer im Namen einer Domain versenden darf
- Ein öffentlicher TXT-Eintrag im DNS der Domain
- Aufbau (Beispiel)

  `v=spf1 a include:_spf.google.com -all`

- Bezieht sich auf “Return Path” (versteckter Absender)
- Übersteht Weiterleitungen nicht

DMARC24
Security & Deliverability

DKIM (DomainKeys Identified Mail)

- Empfänger können prüfen ob E-Mail manipuliert wurde und ob der Absender den privaten Schlüssel kennt.
- Der Mailserver kennt (und generiert meist) den privaten Schlüssel
- Öffentlicher Teil des Schlüssels ist im DNS der Domain einzutragen
- Übersteht automatische Weiterleitungen

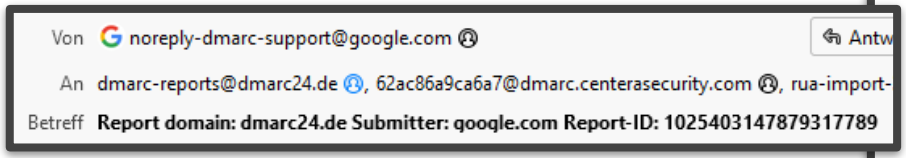
DMARC (Domain-based Message Authentication, Reporting and Conformance)

Der Abgleich mit dem sichtbaren Absender

- Gleicht “Return-Path” (SPF) mit sichtbarem Absender ab
- Gleicht “DKIM”-Domain mit sichtbarem Absender ab
- Definiert „Was tun mit E-Mails, die in beiden Checks durchfallen?“
- Definiert „Wer soll über Ergebnisse der Checks informiert werden?“
- Ein öffentlicher TXT-Eintrag im DNS der Domain
- Aufbau:

  v=DMARC1; p=reject; rua=mailto:dmarc@example.com;

DMARC-Report

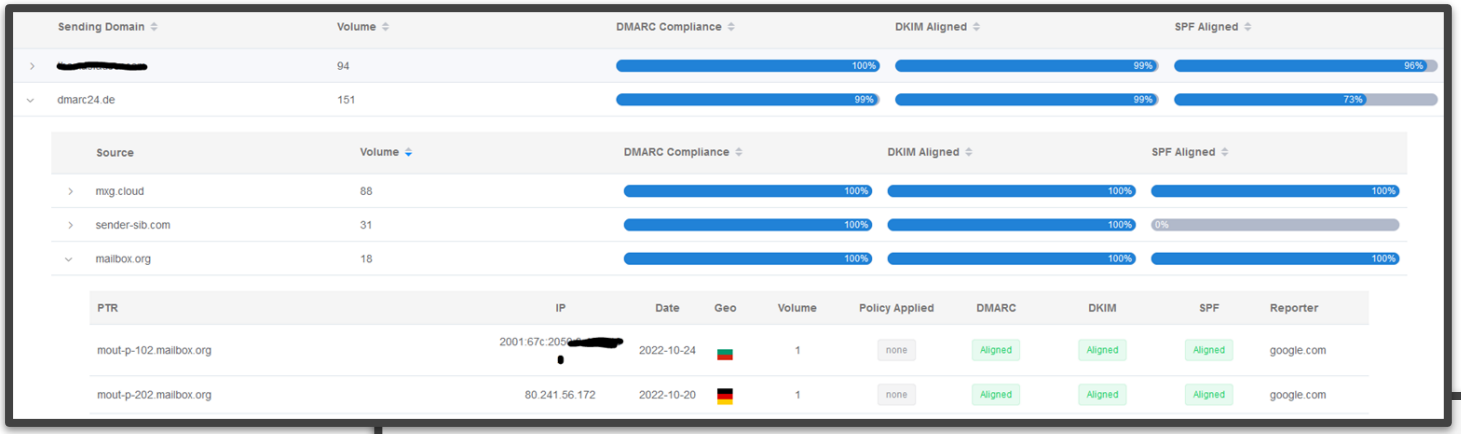



```
<?xml version="1.0" encoding="UTF-8"?>
<feedback>
  <report_metadata>
    <org_name>google.com</org_name>
    <email>noreply-dmarc-support@google.com</email>
    <extra_contact_info>https://support.google.com/a/answer/2466580</extra_contact_info>
    <report_id>1025403147879317789</report_id>
    <date_range>
      <begin>1666915200</begin>
      <end>1667001599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>dmarc24.de</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>reject</p>
    <sp>reject</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>81.201.155.152</source_ip>
      <count>1</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>dmarc24.de</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>dmarc24.de</domain>
        <result>pass</result>
        <selector>dmarc24-de-001</selector>
      </dkim>
      <spf>
        <domain>dmarc24.de</domain>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
</feedback>
```


Bei aggregierten Reports kaum bzw. keine personenbezogene Daten

Forensische Reports kaum verbreitet und selten angefordert.

DMARC-Reports

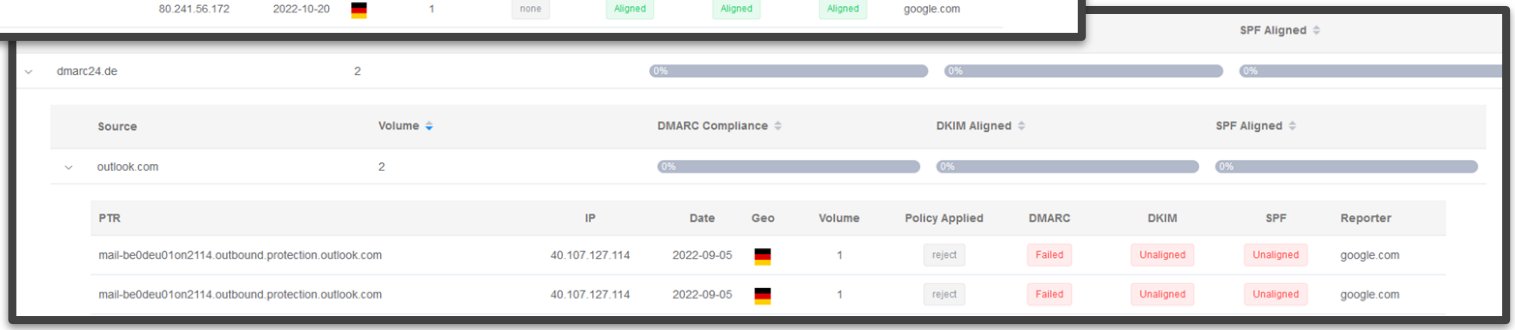


Sending Domain	Volume	DMARC Compliance	DKIM Aligned	SPF Aligned
[redacted]	94	100%	99%	96%
dmarc24.de	151	99%	99%	73%

Source	Volume	DMARC Compliance	DKIM Aligned	SPF Aligned
mxg.cloud	88	100%	100%	100%
sender-sib.com	31	100%	100%	0%
mailbox.org	18	100%	100%	100%

PTR	IP	Date	Geo	Volume	Policy Applied	DMARC	DKIM	SPF	Reporter
mout-p-102.mailbox.org	2001:67c:205[redacted]	2022-10-24		1	none	Aligned	Aligned	Aligned	google.com
mout-p-202.mailbox.org	80.241.56.172	2022-10-20		1	none	Aligned	Aligned	Aligned	google.com

DMARC Check bestanden



SPF Aligned
dmarc24.de 2 — 0% / 0% / 0%

Source	Volume	DMARC Compliance	DKIM Aligned	SPF Aligned
outlook.com	2	0%	0%	0%

PTR	IP	Date	Geo	Volume	Policy Applied	DMARC	DKIM	SPF	Reporter
mail-be0deu01on2114.outbound.protection.outlook.com	40.107.127.114	2022-09-05		1	reject	Failed	Unaligned	Unaligned	google.com
mail-be0deu01on2114.outbound.protection.outlook.com	40.107.127.114	2022-09-05		1	reject	Failed	Unaligned	Unaligned	google.com

DMARC Check durchgefallen

DMARC24
Security & Deliverability

Geo Compliance

February 01, 2022 - April 01, 2022

BIMI (Brand Indicator for Message Identification)

Voraussetzungen

- Registrierte Marke
- Validierung durch Zertifizierungsstelle
- DMARC (quarantine / reject)
- Hosting des Logos
- Support durch Mailprovider und Mailclient Empfänger

DMARC24
Security & Deliverability

Typische Implementierungsfehler

- SPF: Mehr als 1 SPF-Eintrag pro Domain-Ebene vorhanden
- SPF: Es fehlen Systeme im SPF-Eintrag (z. B. Webserver)
- SPF: Mehr als 10 DNS-Namen im SPF-Eintrag
- DKIM: Öffentlicher Schlüssel nicht in DNS eingetragen
- DKIM: Verzicht auf DKIM, weil Mailprovider kein DKIM unterstützt (z.B. IONOS)
- DMARC aktiv, aber DKIM und SPF für andere Domain ausgestellt
- DMARC aktiv, aber kein DKIM konfiguriert und Subdomain ohne SPF
- DMARC: Unentdeckte Konfigfehler ohne Auswertung der Reports

DMARC24
Security & Deliverability

Grenzen von DMARC

- Der Spamfilter oder Mailserver eines Empfängers ignoriert die Vorgaben aus der DMARC-Policy
- Wenn Angreifer ähnlich aussehende oder komplett andere Domainnamen nutzen, greifen die Sicherheitseinstellungen der Originaldomain nicht.
- Nur die E-Mail-Adresse des Absenders wird geprüft. Nicht der Absendername (der auch eine E-Mail-Adresse enthalten könnte).
- Wie alle Sicherheitsmaßnahmen sind auch SPF, DKIM und DMARC keine unüberwindbare Hürde für sehr professionelle Hacker

Anforderung gängiger Standards

- IT-Grundschutz als Standardmaßnahme
- PCI DSS 4.0 (Verarbeitung von Kreditkarten)
- Maßnahmenkatalog Ransomware des BSI
- In den Niederlanden und anderen Ländern für Behörden Pflicht

July 27, 2018 | News

All Dutch governments must implement a strict policy for DMARC and SPF by the end of 2019

Recently, a new target image agreement, made by the Standardization Forum in the Netherlands, has been approved! All Dutch governments must implement a strict policy for DMARC and SPF by the end of 2019. On 18 April 2018, OBDO agreed with this new target agreement on the advice of Standardization Forum.

The new appointment follows on a previously successful government-wide agreement and contains several goals that digital authorities in the Netherlands must meet to improve the security of the communication channel. The goals also protect the email channel of the government. An important part of these goals is the rollout of DMARC on all government domains before the end of 2019. Governments are called upon to work towards a DMARC reject policy type where a policy type result of quarantine also still satisfies.

Quelle: https://www.dmarcanalyzer.com/governments-must-implement-strict-institutions-dmarc-spf-end-2019/

DMARC/DKIM-Support bei Mailservern	DKIM für eigene Domains konfigurierbar	Respektiert DMARC-Policies	Versendet DMARC-Reports	Anzeige BIMI-Logos
MS Exchange Online 365	Ja	Ja, weitgehend	Geplant	Nein
Exchange Server (OnPremise)	Nachrüstbar	?	Nein	Nein
Google Mail / Workspace	Ja	Ja	Ja	Ja
E-Mail-Security-Gateways	Üblicherweise	Üblicherweise	Teilweise	-

Hinweis: Möglichkeiten wenn kein DKIM angeboten wird:

- **Versand über E-Mail-Security-Gateways oder spezielle SMTP-Server**
- **Nachrüstung über Plugins etc.**
- **Nutzung von SPF ohne DKIM**

Angaben ohne Gewähr.
Stand: 22.12.2022

DMARC24
Security & Deliverability

Warum DMARC nutzen?

- Schutz vor E-Mail-Spoofing (nur mit „Quaratine“ oder „Reject“-Policy)
- Höhere Reputation bei Spamfiltern und damit höhere Zustellbarkeit valider E-Mails in den Posteingang statt in den Spamordner
- Transparenz für die IT (wer versendet im Namen meiner Domains?)
- Pflicht oder Empfehlung in Standards und Regelwerken
- Stand der Technik

Referent

Thomas Fauser

- Inhaber von DMARC24
  - Spezialist für den Schutz vor E-Mail-Spoofing
  - Implementierung von DMARC bis zur wirkungsvollen „reject“-Policy
  - Software für das Monitoring von DMARC-Reports
  - Optimierung der Zustellbarkeit von validen E-Mails

- Seit 2015: Informationssicherheitsbeauftragter
- Bis 2015: IT-Systemadministrator mit Schwerpunkt Mailserver

DMARC24
Security & Deliverability
Thomas Fauser
Stachelbeerweg 9
69469 Weinheim
+49 6201 / 2717 555
tf@dmarc24.de
https://dmarc24.de

DMARC24
Security & Deliverability

Fragen?