Technische Hochschule Nürnberg

Aktueller Handlungsbedarf bei der E-Mail-Sicherheit

Prof. Dr. Ronald Petrlic

Zur Person

2015 2020 2024

Professor für IT-Sicherheit @TH Nürnberg
Lehre: von Informationssicherheits-Management bis Kryptographie
Forschung: Self-Sovereign Identity, Technischer Datenschutz, E-Mail-Sicherheit

Gründung
Petrlic Consulting GmbH
Beratung zu Datenschutz
und IT-Sicherheit, Gutachten,.
www.datensicherheit.digital

Referent @LfDI Baden-Württemberg
Leiter des Technik-Referats
Kontrolle der Einhaltung des Datenschutzes durch Unternehmen und Behörden im Ländle
Verantwortlich für 1. DSGVO-Bußgeld in D.

Studium und Promotion Informatik & PostDoc in Rechtsinformatik

Aktuelle Entwicklungen

E-Mail-Sicherheit

- **E-Mail seit Jahren als Einfallstor Nummer 1 für Phishing, Trojaner,…**
  - Angriffs-Fälle der letzten Jahre: es beginnt meist mit einer E-Mail (laut Proofpoint in 90 % der Fälle!!!)

- **Eines der Probleme: Spoofing!**
  - E-Mail kommt von vermeintlich vertrauenswürdigem Sender
  - Aber: Jeder kann E-Mails im Namen von beliebigen Sendern versenden! (sofern kein Spoofing-Schutz)
    - Pro Tag werden 3,1 Milliarden Domain-Spoofing-E-Mails verschickt (laut Proofpoint)
    - Woran erkennen Sie „gespoofte“ E-Mails?

Quelle Proofpoint: https://www.proofpoint.com/de/threat-reference/email-spoofing

Gesetzliche Grundlagen

- Notwendigkeit zur Umsetzung von Spoofing-Schutz ergibt sich u.A. aus Gesetzen

- **DSGVO**: Artikel 32 (Sicherheit der Verarbeitung)
  - Die vorgestellten Verfahren sind Stand der Technik

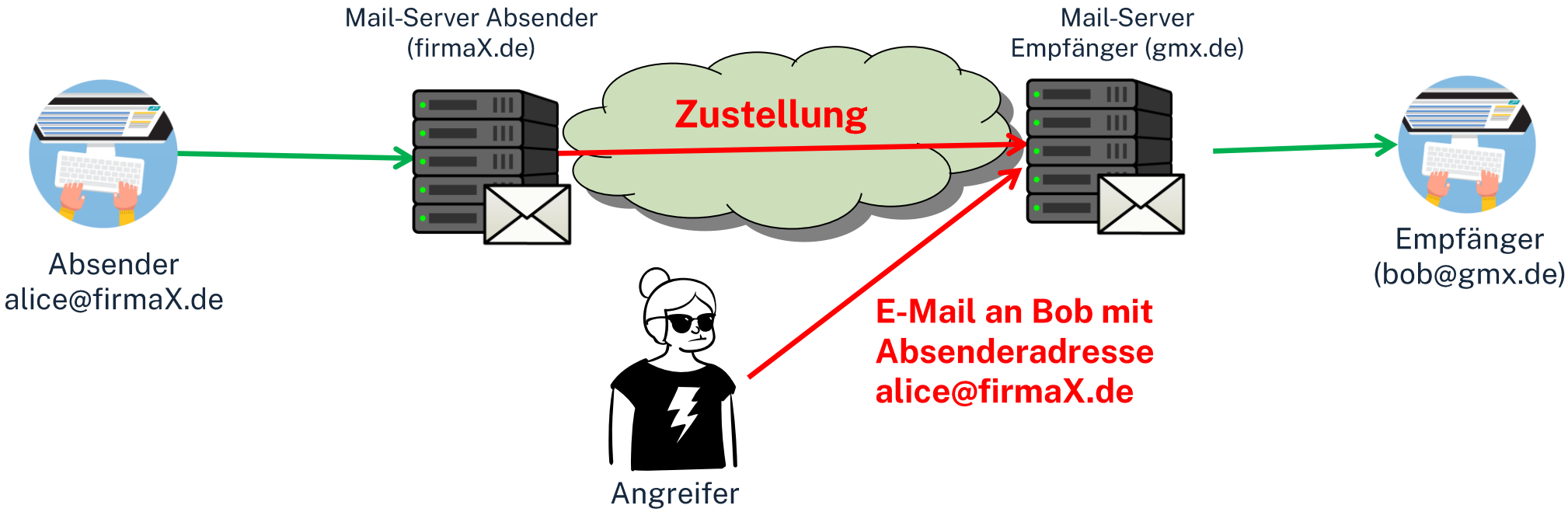
- **NIS 2**: In Erwägungsgründen konkrete Hinweise
  - EG 54: Ransomware-Angriffe per E-Mail
  - EG 89: Bewusstsein für Cyber-Bedrohungen und speziell Phishing soll geschärft werden

- **PCI**: Finanzdienstleister müssen Schutz-Maßnahmen in Bezug auf Phishing bis Ende März 2025 umsetzen
  - Explizite Empfehlung für die hier vorgestellten Schutzmaßnahmen

- Cybersicherheitsversicherungen fordern ebenfalls Umsetzung von Spoofing-Schutz

Spoofing aus technischer Perspektive

Angreifer versendet E-Mails im Namen von Alice (bzw. ihrer Organisation)



- Der Empfänger-Mail-Server (hier: GMX) kann nicht feststellen, dass die E-Mail nicht von Alice (bzw. firmaX) stammt
  - Sofern firmaX keine Maßnahmen ergriffen hat!
- Bob kann es ebenfalls nicht feststellen

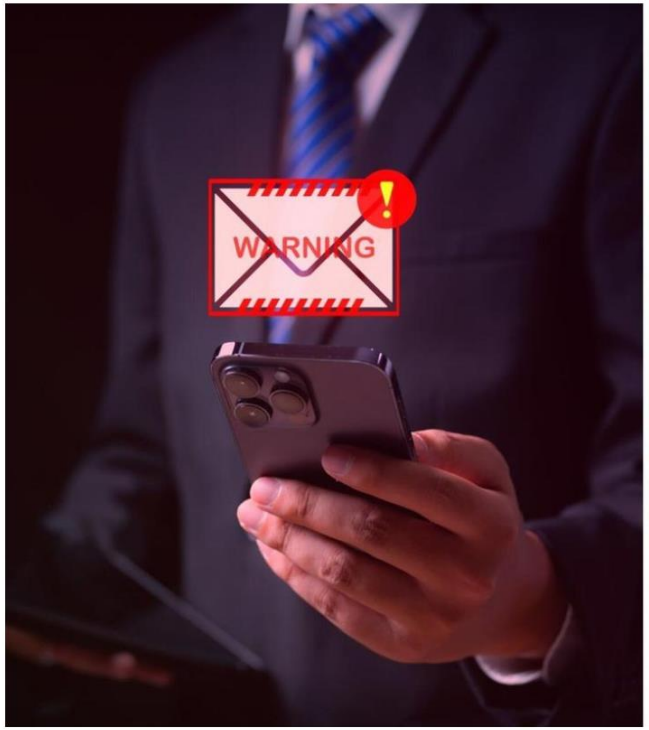
Aktueller Fall

Rechnungen im Namen der Stadt Nürnberg (November 2024)

Stadt Nürnberg warnt

Betrügerische Rechnungen: Gefälschte E-Mails der Stadt Nürnberg im Umlauf - so erkennen Sie sie

Von **Erik Thieme** 3.11.2024, 15:12 Uhr



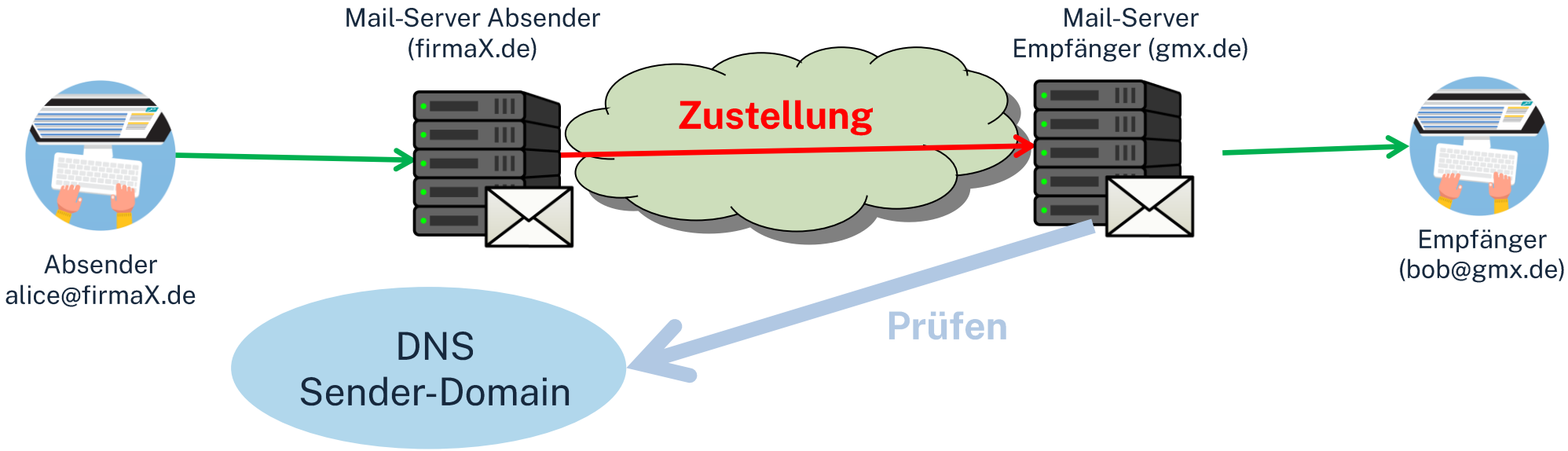
© IMAGO / Pond5 Images / Ardan Fuessmann

Die Stadt warnt vor betrügerischen E-Mails, die aktuell im Namen der Stadt Nürnberg verschickt werden.

Quellen:
https://www.nordbayern.de/franken/betrugerische-rechnungen-gefalschte-e-mails-der-stadt-nurnberg-im-umlauf-so-erkennen-sie-sie-1.14469201
https://www.nuernberg.de/internet/stadtportal/aktuell_92167.html

Spoofing-Schutz aus technischer Perspektive

Spoofing-Schutz auf E-Mail-Ebene bieten SPF / DKIM / DMARC



- **SPF**: Mail-Server des Empfängers prüft (über DNS), ob Mail von legitimen Absender-Mail-Server stammt
- **DKIM**: Absender-Mail-Server signiert ausgehende E-Mails
  - Empfänger-Mail-Server prüft Integrität & Authentizität eingehender E-Mails (öffentlicher Schlüssel liegt im DNS)
- **DMARC**: Verantwortlicher auf Sender-Seite legt im DNS fest, wie der Empfänger-Mail-Server mit Problemen bei SPF/DKIM-Prüfung umgehen soll

Spoofing-Schutz aus technischer Perspektive

Spoofing-Schutz auf E-Mail-Ebene bieten SPF / DKIM / DMARC

- Haben sich Verantwortliche in der Praxis mit den Verfahren bereits beschäftigt?
  - Die Verfahren sind 20 Jahre alt…
  - Aber: jetzt müssen sie angewendet werden!

- Aber wo ist das Problem? Wer schreibt das vor?
  - Die Aufsichtsbehörden prüfen eh nicht…
  - Also: zurücklehnen und nichts tun!

  - Aber Achtung…

Wer prüft die Umsetzung?

Die großen Mailprovider!!!

- Seit 01.02.2024:
  - „**Großversender**“ (die mehr als 5.000 Mails pro Tag an Google / Yahoo senden) **müssen SPF und DKIM umsetzen**
    - Außerdem: DMARC-Eintrag setzen
    - Bei weniger Mails: SPF **oder** DKIM nötig

  - Die **Detail-Vorgaben sind noch nicht besonders streng → das wird sich bald ändern…**
    - Und: **es wird irgendwann auch nicht mehr nur Großversender treffen!**

  - Schon jetzt: Berichte darüber, dass E-Mails nicht mehr zugestellt werden

2023: Google sperrte Heise-Verlag

Google nahm keine Mails mehr von Heise entgegen

Google stufte ct.de als Spamschleuder ein

Im Juli erklärte Google ct.de zum Spammer und verweigerte die E-Mail-Annahme. Die Probleme der stark zentralisierten Mail-Infrastruktur werden dadurch deutlich.

528

(Bild: Shutter z/Shutterstock.com)

12.08.2023, 06:30 Uhr Lesezeit: 3 Min. | c't Magazin

Von Jan Mahn

- Quelle: https://www.heise.de/news/Google-stufte-ct-de-als-Spamschleuder-ein-9241222.html

2023: Google sperrte Heise-Verlag

Google nahm keine Mails mehr von Heise entgegen

- Sperrung von 19. Juni bis 17. Juli!

- „härteste Strafe für eine Mail […], weil sie dann nicht einmal im Spamordner des Empfängers zu finden ist.“

- „Problematisch ist das, weil Google-Server nicht nur die kostenlosen Accounts für Gmail versorgen. Viele Unternehmen lassen ihre Mails mit eigener Domain mittlerweile von Google verwalten.“
  - In 10 Tagen: 4.272 Mails von Heise an Google (7.168 an Microsoft)

- „Domain ct.de ist nicht die erste, die schlagartig und ohne Erklärung in Googles Gunst gesunken ist. Immer wieder erhalten wir Mails von Administratoren eher kleiner Mailserver, die Ähnliches berichten“

Wie sieht es in der Praxis aus?

Beispiel Banken

- **Im Banking-Bereich ist das Thema Phishing ein großes Problem!**

- **Wir haben 1.249 deutsche Banken/Kreditinstitute-Mail-Server geprüft**
  - **Nur 17 % nutzen DMARC „richtig“** (42 % haben es immerhin schon eingerichtet)
  - Als DMARC Report Analyzing Provider wird häufig *Proofpoint* genutzt
    - Achtung: Metadaten der gesamten E-Mail-Kommunikation (welche Domain kommuniziert mit welcher Domain) geht damit in die USA!

- Und was machen die Banken?
  - Sie sagen ihren Kunden, sie sollen doch aufpassen und nicht auf gefälschte Mails reinfallen…

- Payment Card Industry (PCI) empfiehlt Nutzung von DMARC für Banken bis 31.03.2025

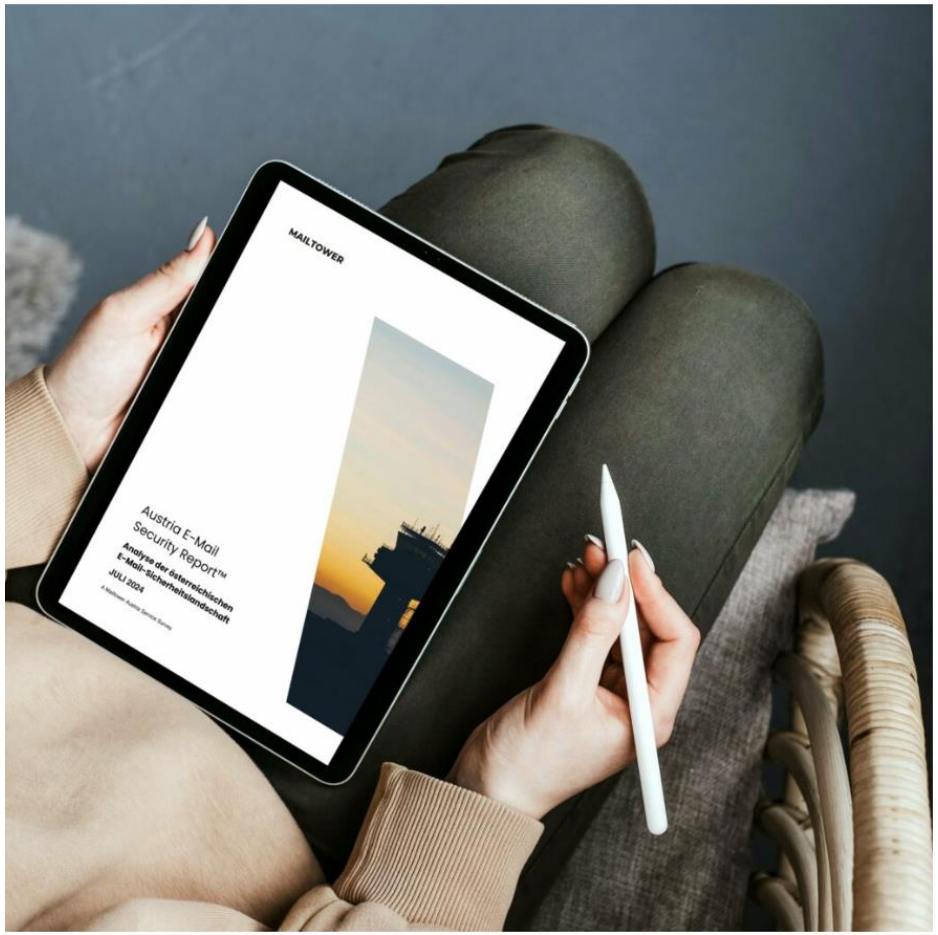
Wie sieht es in Österreich aus?

Wir haben österreichische Unternehmens-Mailserver getestet

- Insgesamt 87.017 aktive Unternehmens-Domains

- Ergebnis:
  - SPF bei 81,2 % im Einsatz („hardfail“-Konfiguration bei 52 %)
  - 32,91 % nutzen DMARC
    - Aber: „Richtige“ DMARC-Einstellung („reject“) nur bei 6 %

- Detaillierter Bericht unter blog.mailtower.app



Wie sieht es in Deutschland aus?

Natürlich schlechter als in Österreich ☺

- Insgesamt 150.000 Unternehmens-Domains untersucht

- Ergebnis:
  - SPF bei 46,10 % im Einsatz („hardfail“-Konfiguration bei 37 %)
  - 9,54 % nutzen DMARC
    - Aber: „Richtige“ DMARC-Einstellung („reject“) nur bei 3 %

- Brevo.com kommt am häufigsten als DMARC Reporting Provider vor…
  - … aber das ist doch ein E-Mail-Marketing-Dienst?

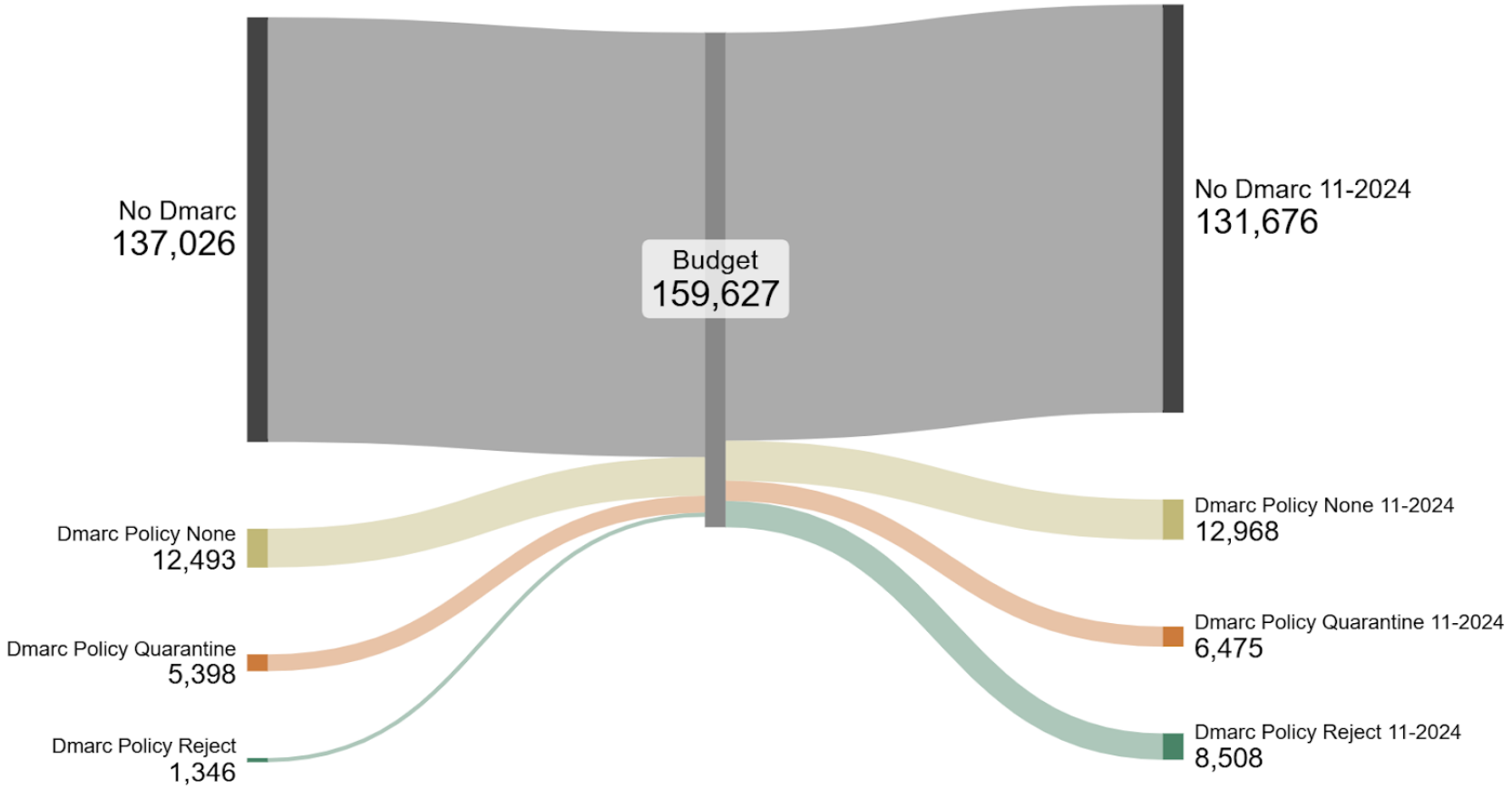
Untersuchung Deutschland Forts.

DMARC

	June 2024			November 2024			
	Good	Bad	Bad %	Good	Bad	Bad %	Change
Security	486	4052	89,30%	728	3797	83,90%	5,40%
Dentist	1543	12169	88,80%	2473	11688	82,50%	6,20%
Nursery School	312	2772	89,90%	487	2711	84,80%	5,10%
Primary Care Physician	423	3066	87,90%	591	2905	83,10%	4,80%
Facility Management	281	2428	89,60%	430	2299	84,20%	5,40%
Driving School	614	6707	91,60%	1103	7234	86,80%	4,80%
Tax Consultant	419	4578	91,60%	658	4390	87,00%	4,60%
Photographer	1466	10627	87,90%	2011	9844	83,00%	4,80%
Attorney	431	5053	92,10%	714	4887	87,30%	4,90%
Paediatrician	124	1107	89,90%	229	1140	83,30%	6,70%
Pharmarcy	4256	15699	78,70%	5422	15073	73,50%	5,10%
Law Firm	114	1183	91,20%	181	1147	86,40%	4,80%
Insurance Company	674	8361	92,50%	983	8155	89,20%	3,30%
Holidy Apartment	1201	14256	92,20%	1800	14134	88,70%	3,50%
Caretaker	196	1938	90,80%	276	1858	87,10%	3,80%
Restaurant	833	10706	92,80%	1193	10617	89,90%	2,90%
Carpenter	488	4770	90,70%	860	4612	84,30%	6,40%
Sparkasse	472	1032	68,60%	494	1022	67,40%	1,20%
Car Dealer	608	6001	90,80%	1065	6120	85,20%	5,60%
Psychotherapiest	852	5433	86,40%	1066	4950	82,30%	4,20%
Municipality	437	4768	91,60%	651	4390	87,10%	4,50%

Untersuchung Deutschland Forts.

DMARC



Zurück zum Fall der Stadt Nürnberg

Könnten E-Mails mit der richtigen Adresse in Umlauf gebracht worden sein?

- Praxis-Test:
  - Prüfen die Konfiguration des Mail-Servers der Stadt Nürnberg:
    - https://mailtower.app/de/

- Könnten die Betrüger also E-Mails im Namen der Stadt versenden? Ja! (wie in Live-Demo gesehen)
- „Die Stadt fordert ihre Bürger deshalb auf, wachsam zu sein und geht aktiv gegen die Betrugsversuche vor.“
  → die Stadt müsste die Spoofing-Schutz-Verfahren implementieren…

Was ist zu tun?

„Einfach“ einrichten!

- SPF + DKIM aktivieren & DMARC-Eintrag auf „reject“ setzen
  - Je nach Konstellation: Admin / Dienstleister / Mail-Provider unterstützt dabei

- Aufwand ist gering: TXT-Einträge im DNS setzen…
  - Beispielkonfiguration für datensicherheit.digital:
    - SPF: v=spf1 ip4:185.231.124.0/26 –all
    - DMARC: v=DMARC1; p=reject; rua=mailto:dmarc@rua.mailtower.app;

- In größeren Unternehmen können unterschiedliche Systeme E-Mails versenden (bzw. Weiterleitungen existieren)
  - Dies muss entsprechend berücksichtigt und hinterlegt werden: Aufstellen eines Umsetzungsplans!

Was ist zu tun?

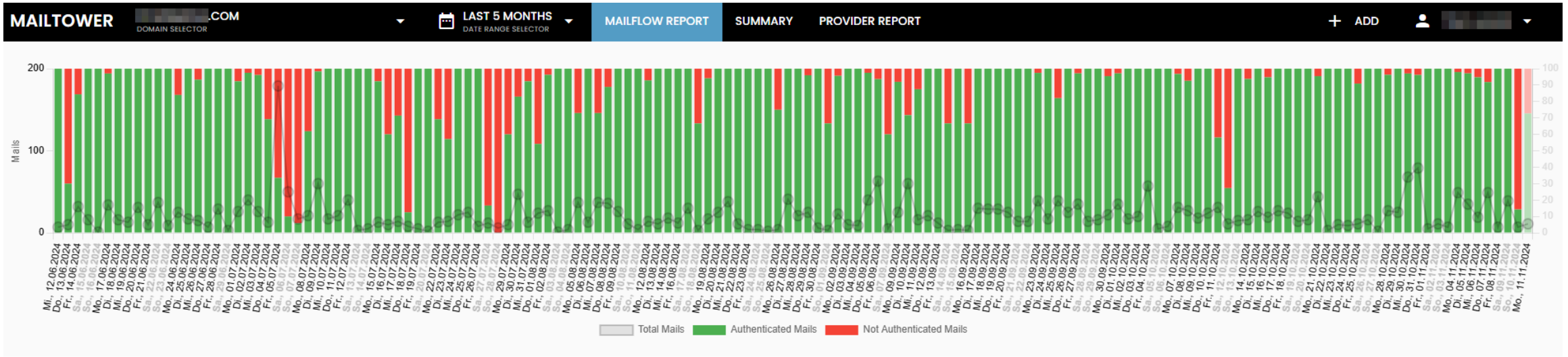
„Einfach“ einrichten!

- Empfehlung: **DMARC Report Analyzer** nutzen
  - Damit erhält man täglichen Report, der Aufschluss über Probleme und Angriffe liefert
    - Probleme können frühzeitig erkannt und behoben werden
    - Angreifer können erkannt und gemeldet werden

- Beispiel: Mailtower.app
  - Anbieter aus Österreich

Beispiel Report Analyzer

Mailtower.app

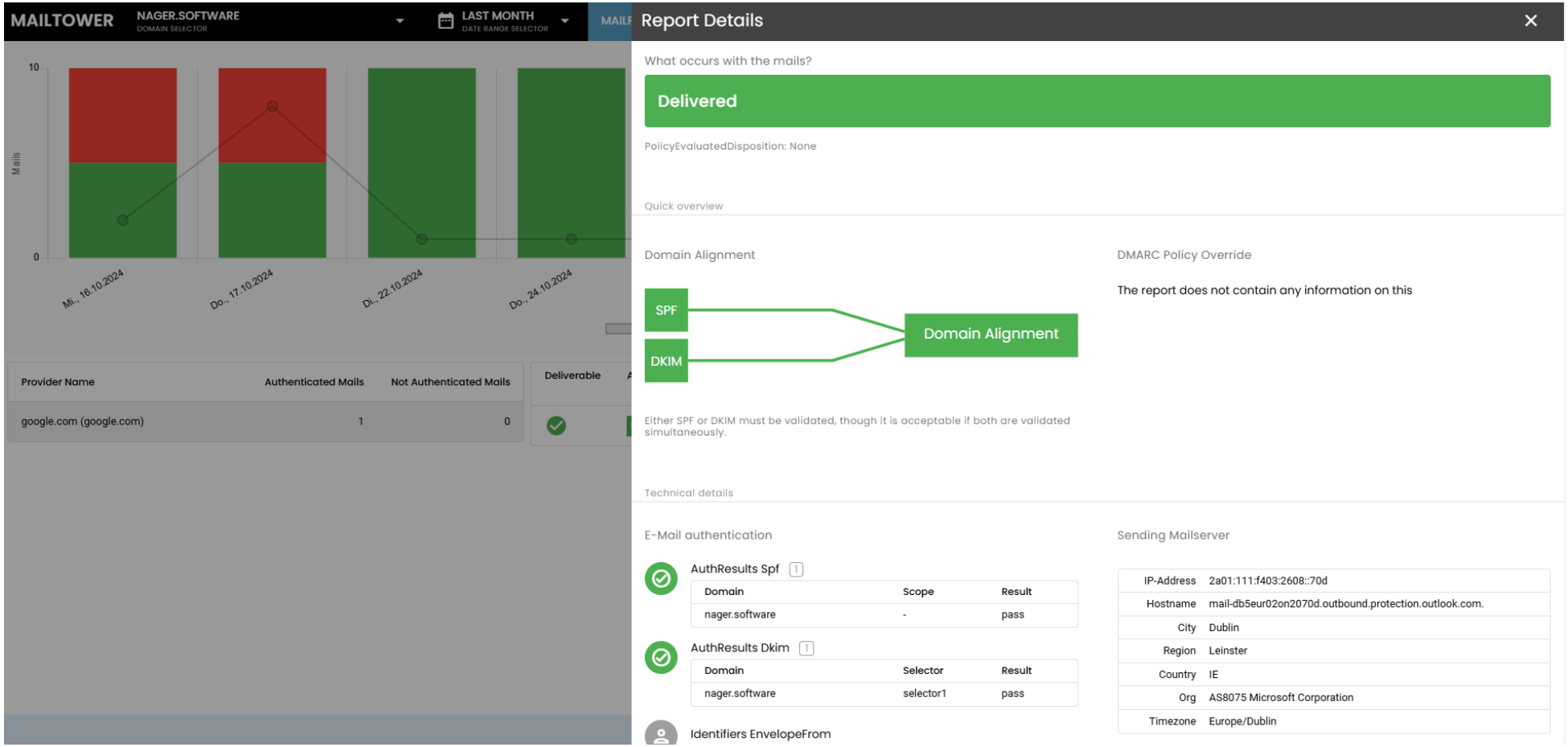


Provider Name	Authenticated Mails	Not Authenticated Mails
google.com (google.com)	7	3
GMX (gmx.net)	1	0

Deliverable	Alignment	E-Mail Volume	Envelope From Domain RFC5321.MailFrom	Header From Domain RFC5322.From	Receiver Domain RFC5321.MailTo	Actions
⊖	SPF DKIM	2		[redacted]		ⓘ
⊖	SPF DKIM	1		[redacted]		ⓘ
✓	SPF DKIM	2		[redacted]		ⓘ
✓	SPF DKIM	2		[redacted]		ⓘ
✓	SPF DKIM	1		[redacted]		ⓘ
✓	SPF DKIM	1		[redacted]		ⓘ
✓	SPF DKIM	1		[redacted]		ⓘ

Beispiel Report Analyzer

Mailtower.app



Fazit und Ausblick

- Stand der Technik entwickelt sich nur sehr langsam…
  - 20 Jahre von ersten RFCs bis zur Durchsetzung in der Praxis

- **SPF/DKIM & DMARC sind nun Stand der Technik**
  - große Schutzwirkung für eigene Organisation **und** für Empfänger!

- Umsetzung einfach und kostengünstig!!

- Im Hinblick auf E-Rechnung: Schutz vor Fake-Rechnungen im Namen des eigenen Unternehmens
  - Mindert Reputationsschäden

Vermeiden von Benachrichtigungen…

Bösartige Mail kam von richtiger Absenderadresse

Email Impersonation Alert

FT

Franklin Templeton Impersonation Alert <noreply@franklintempleton.com>

To ronald@

Reply | Reply All | Forward | •••

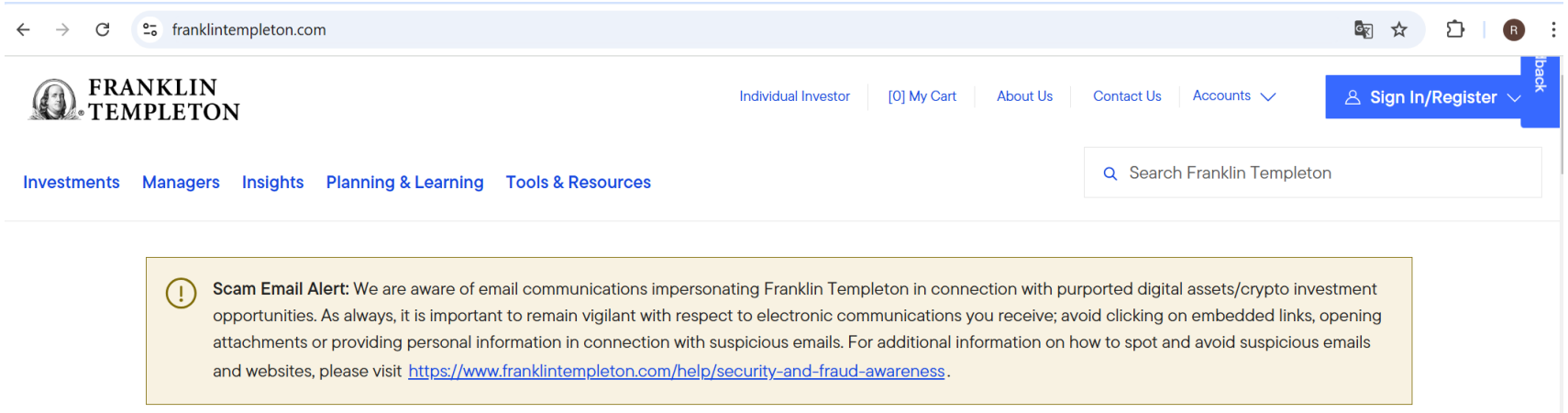
Do 17.10.2024 20:07

Follow up.

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

We recently learned that you may have received emails last week from "OpenSea Marketplace," "OpenSeaTeam," and/or "LayerZero Contact" using the email address "<noreply@franklintempleton.com>" in connection with purported digital assets/crypto investment opportunities. **These were not legitimate emails from Franklin Templeton. You should ignore or delete the emails.**

As always, it is important to remain vigilant with respect to electronic communications you receive. Avoid clicking on embedded links, opening attachments, or providing personal information in connection with suspicious emails. For additional information on how to spot and avoid suspicious emails and websites, please visit www.franklintempleton.com/help/security-and-fraud-awareness.



Diskussion

- Führen „Big Tech“-Unternehmen besseres „Enforcement“ von technischem Datenschutz durch als Aufsichtsbehörden?
  - Ist das gut, wenn diese Firmen bestimmen, wer (zukünftig) E-Mails versenden darf?

- Muss ggbfs. eine Benachrichtigung über eine Datenpanne nach Art. 33 DSGVO durchgeführt werden, wenn man als Verantwortlicher davon Kenntnis erlangt, dass in eigenem Namen gefährliche E-Mails von Dritten versendet werden (die bei einigen Betroffenen schon zu Schaden geführt haben)?
  - Und wenn die Schutzmaßnahmen eben nicht umgesetzt wurden…

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?