DMARC24
Security & Deliverability

VGSD
Mitglied

Wie du weniger SPAM erhältst und deine eigenen E-Mails nicht als SPAM eingestuft werden

VGSD Experten-Talk am 7. Mai 2024 mit Thomas Fauser, DMARC24

Unsere Themen & Ziele

- Praktische Tipps, damit das E-Mail-Thema weniger nervt
- Verständnis für technische Grundlagen rund um Spam-Mails
- Zeit für Fragen

Warum lohnt es sich als Unternehmer, sich damit zu beschäftigen?

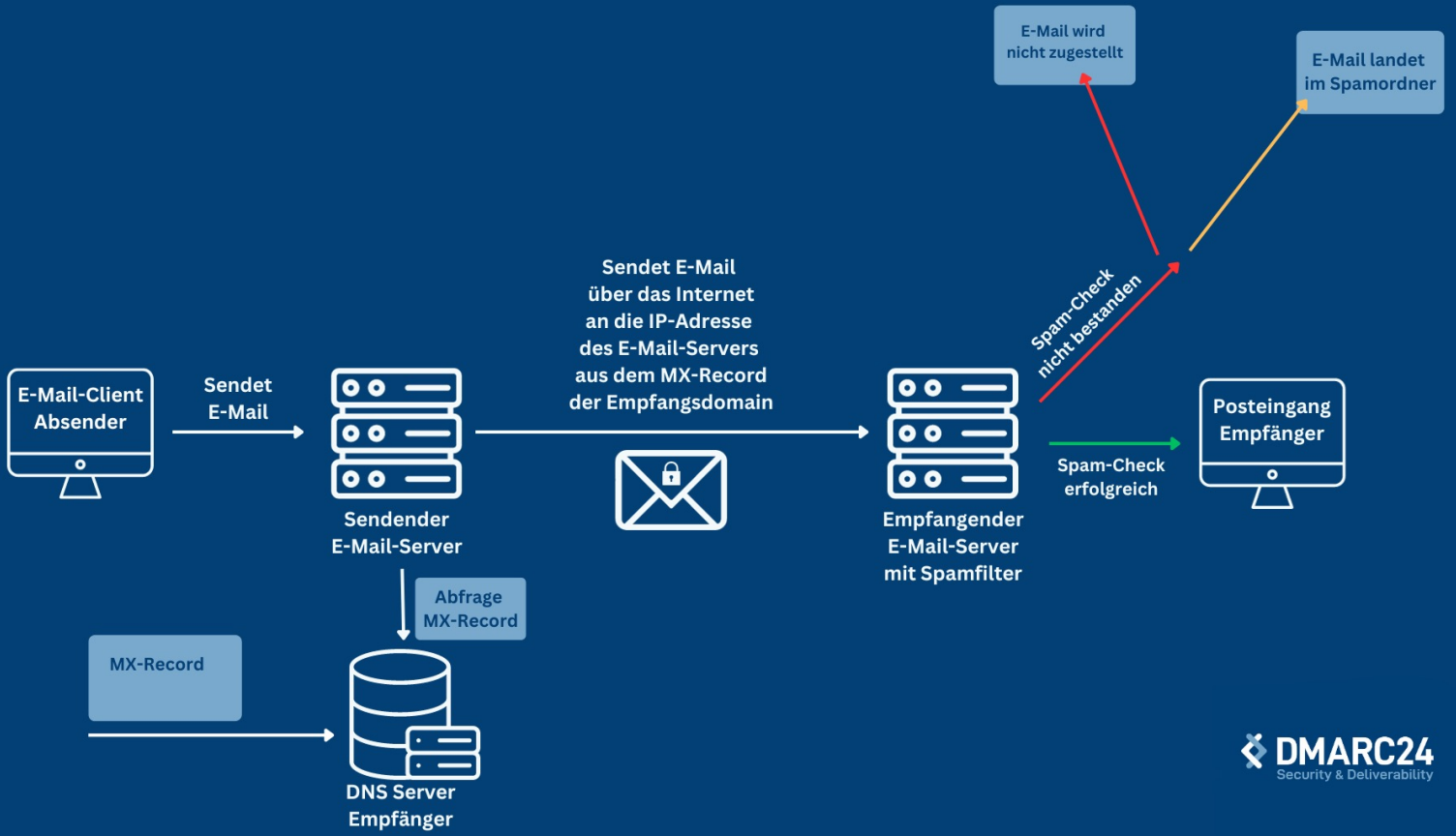
- Die Anforderungen an Versender von E-Mails steigen
- Die Bedeutung von E-Mails im täglichen Geschäftsverkehr ist weiterhin hoch

DMARC24
Security & Deliverability

Eintreffenden Spam vermeiden

So läuft ein E-Mail-Versand ab

DMARC24
Security & Deliverability



DMARC24
Security & Deliverability

DMARC24
Security & Deliverability

Frage 1: Kriterien Spamfilter

Nach welchen Kriterien trifft ein Spamfilter seine Entscheidungen und wie lernt er hinzu?

DMARC24
Security & Deliverability

Wie funktioniert ein Spamfilter?

- Regeln bei Google & Microsoft ungefähr so bekannt wie bei SEO / Suchmaschine. Tiefe Details bleiben aus Sicherheitsgründen verborgen.
- Typische Faktoren für die Bewertung
  - Reputation IPs und Domains
  - Abgleich Blocklisten
  - Benutzerinteraktion (wie viele öffnen, klicken, antworten…)
  - Spamwörter
  - Prozentzahl Spambeschwerden
  - Authentifizierung / DMARC-Policy
  - Abgleich Absender / Reply-To etc.
  - Malware
  - Ungewöhnliches Verhalten (z.B. plötzlich viele E-Mails in kurzer Zeit)

X-Spam-Status: Yes, score=8.295 tagged_above=2 required=6.31 tests=[DEAR_SOMETHING=1.973, DKIM_SIGNED=0.1, DKIM_VALID=-0.1, DKIM_VALID_AU=-0.1, DKIM_VALID_EF=-0.1, FREEMAIL_FROM=0.001, FREEMAIL_REPLY=1, HS_RSPAMD_14=4, HTML_MESSAGE=0.001, MISSING_HEADERS=1.021, SPF_HELO_PASS=-0.001, SPF_PASS=-0.001, SUBJ_ALL_CAPS=0.5, URIBL_BLOCKED=0.001] autolearn=no autolearn_force=no

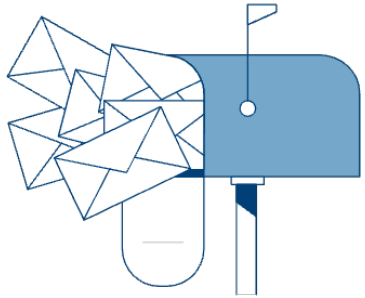
DMARC24
Security & Deliverability

Frage 2: Spam reduzieren

Welche Techniken stehen mir zur Verfügung, damit weniger SPAM in meinem Posteingang landet?

Frage 2: Spam reduzieren

1. **Spamfilter trainieren** (Spammails als Spam markieren statt löschen)
2. **Spamfilter-Einstellungen optimieren** (falls entsprechende Optionen vorhanden sind)
    1. Empfindlichkeit erhöhen
    2. Zusatzpakete kaufen
    3. Rspamd statt nur Spamassassin nutzen
    4. Unerwünschte Absender auf Blockliste hinzufügen
3. **E-Mail-Anbieter wechseln** (z.B. statt den E-Mail-Service des Webseiten-Hosters zu nutzen zu E-Mail-Anbietern wechseln, die sich auf E-Mails spezialisiert haben)
4. Ein **E-Mail-Security-Gateway** nutzen, das alle E-Mails zuerst erhält und nur „saubere“ E-Mails weiterleitet
5. E-Mail-Adresse nicht so im Internet veröffentlichen, dass sie einfach automatisiert gelesen werden kann.
6. Nicht darauf antworten



DMARC24
Security & Deliverability

Ausgehenden Spam vermeiden

DMARC24
Security & Deliverability

Frage 3: Zuverlässig versenden

Was kann ich tun, damit meine eigenen E-Mails und Newsletter nicht als SPAM eingestuft werden?

DMARC24
Security & Deliverability

Frage 3: Zuverlässig versenden

- E-Mail-Authentifizierung (SPF, DKIM & DMARC) sauber einrichten. Details folgen bei Frage 4.
- Domains und IP-Adressen „aufwärmen“, um gute Reputation aufzubauen
- Sparsam mit Links umgehen, insb. wenn sie auf viele verschiedene Seiten zeigen. Nur gültige Links nutzen.

Bei Newslettern oder Werbe-Mails zusätzlich:

- Double-Opt-In nutzen
- Keine gekauften „Listen“ oder alte Listen nutzen, um E-Mails und Newsletter zu versenden
- Inaktive Kontakte, die nicht mehr interagieren, aus Liste entfernen
- Absenderadresse auf Kontaktliste oder Whitelist setzen lassen

DMARC24
Security & Deliverability

Frage 4: E-Mail-Authentifizierung

Mein Newslettertool hat mich auf die neuen Anforderungen von Google und Yahoo hingewiesen. In der Mail standen Begriffe wie DKIM und DMARC. Was ist das und was ist für mich konkret zu tun?

Warum neue Anforderungen?

- E-Mail-Absenderadressen sind leicht fälschbar
- Jede Domain hat ebenso wie jede IP-Adresse bei Spamfiltern eine Reputation
- Durch E-Mails mit gefälschter Absenderadresse lassen sich auch die Reputation von fremden Domains beeinflussen
- Spamversender konnten die gute Reputation einer anderen Domain unberechtigt nutzen, damit ihre E-Mails zuverlässiger zugestellt werden
- Große E-Mail-Anbieter wollen nachvollziehen können, ob E-Mails wirklich von dem Absender oder einem seiner Dienstleister kommt – oder den Absender nur vortäuscht.
- Somit kann die Reputation einer Domain besser und zuverlässiger bewertet werden.

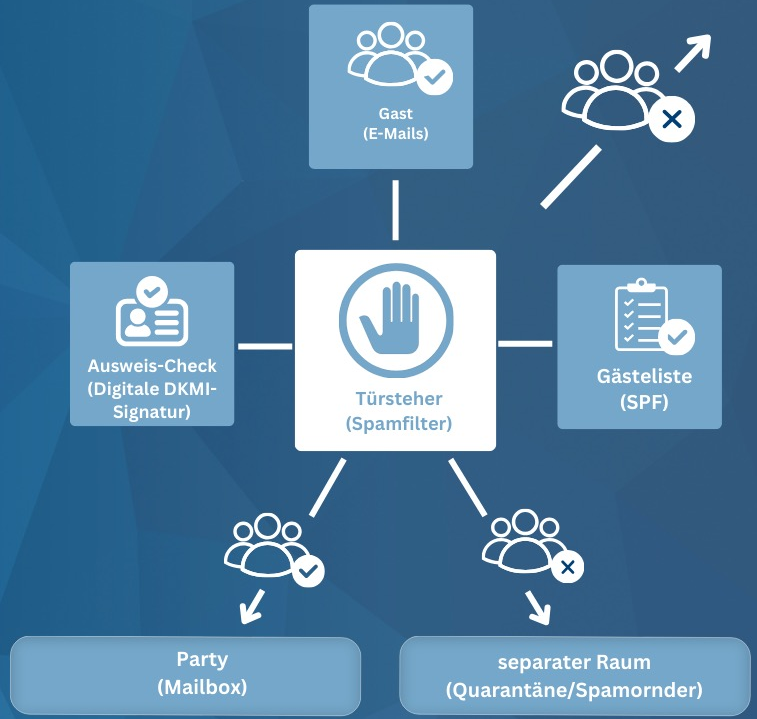
DMARC24
Security & Deliverability

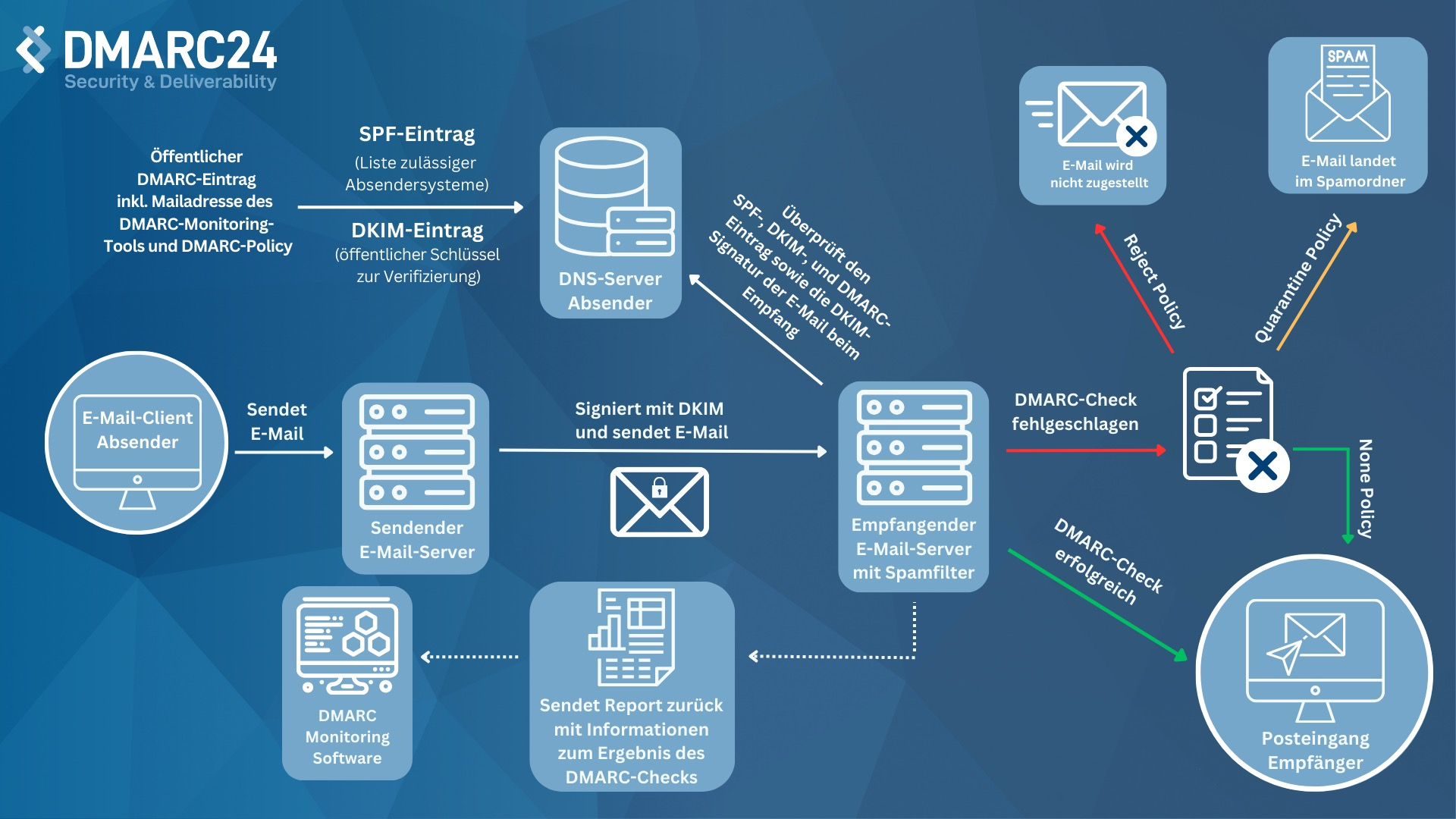
Bedeutung der Fachbegriffe SPF, DKIM und DMARC

ABKÜRZUNGEN	STEHT FÜR	BEDEUTUNG	EINFACHE ERKLRÄUNG	GRAFIK/ ESELSBRÜCKE	BEISPIEL- EINTRAG
SPF	SENDER POLICY FRAMEWORK	Überprüft, ob E-Mails von autorisierten Servern gesendet werden.	Gästeliste. Nur die Systeme, die im SPF-Eintrag (der Gästeliste) aufgeführt sind, werden eingelassen.		v=spf1 a include:_spf.google.com -all
DKIM	DOMAINKEYS IDENTIFIED MAIL	Verwendet digitale Signaturen, um E-Mail-Authentizität und -integrität zu validieren.	Fälschungssichere Ausweis mit Foto / Briefsiegel		v=DKIM1; k=rsa; p=MIIIBIjydke....
DMARC	DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING, AND CONFORMANCE	Erweitert SPF und DKIM, definiert Umgang mit Authentifizierungsfehlern und liefert Berichte.	Gastgeber, der festlegt, was geprüft wird, wie mit ungebetenen Gästen (E-Mails) umgegangen wird (ablehnen, unter Beobachtung stellen oder soll der Gastgeber nur informiert werden)		v=DMARC1; p=none; rua=mailto:email@example.com

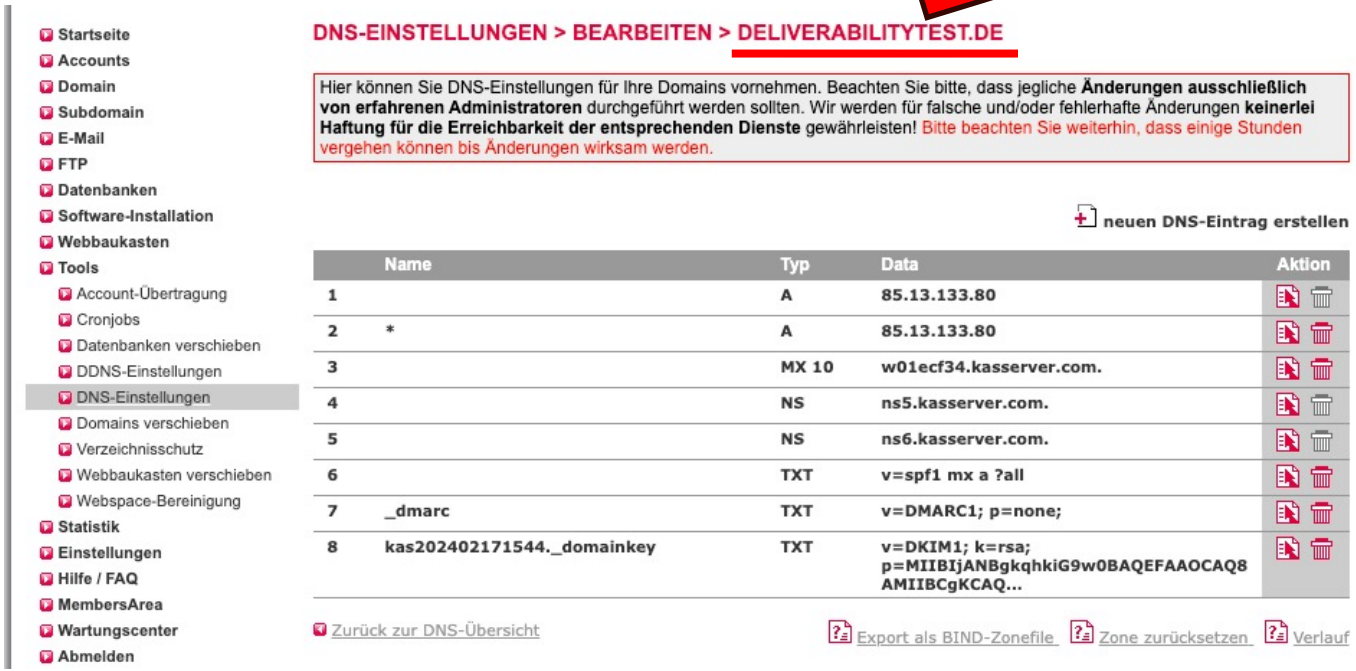
Analogie: Spamfilter als Türsteher

DMARC24
Security & Deliverability




DMARC24
Security & Deliverability
Öffentlicher DMARC-Eintrag inkl. Mailadresse des DMARC-Monitoring-Tools und DMARC-Policy
SPF-Eintrag
(Liste zulässiger Absendersysteme)
DKIM-Eintrag
(öffentlicher Schlüssel zur Verifizierung)
DNS-Server Absender
Überprüft den SPF-, DKIM-, und DMARC-Eintrag sowie die DKIM-Signatur der E-Mail beim Empfang
E-Mail wird nicht zugestellt
SPAM
E-Mail landet im Spamordner
Reject Policy
Quarantine Policy
E-Mail-Client Absender
Sendet E-Mail
Sendender E-Mail-Server
Signiert mit DKIM und sendet E-Mail
Empfangender E-Mail-Server mit Spamfilter
DMARC-Check fehlgeschlagen
None Policy
DMARC-Check erfolgreich
Posteingang Empfänger
DMARC Monitoring Software
Sendet Report zurück mit Informationen zum Ergebnis des DMARC-Checks

DNS-Einstellungen



Webseite

Mailserver (Empfang)

Zentral hinterlegte Informationen zur E-Mail-Sicherheit

Hinweise zur Implementierung

- Nur einen SPF-Eintrag pro Domain-Ebene anlegen
- DKIM-Schlüssel können beliebig viele hinterlegt werden. Einen für jeden Dienst/Server, der E-Mails im Namen der Domain versendet
- Tipp: Ein **DMARC-Monitoring-Tool** nutzen, um zu prüfen, ob alle Systeme/Dienste korrekt eingerichtet sind. Ist etwas unvollständig konfiguriert, kann es es zu Zustellbarkeitsproblemen kommen (= E-Mails landen im Spam oder werden abgewiesen)

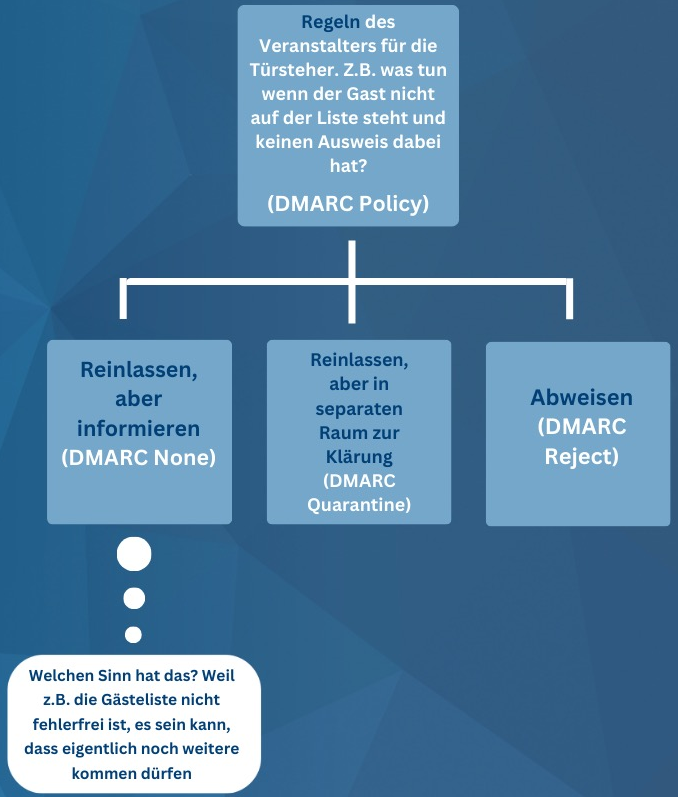
DMARC24
Security & Deliverability

Frage 5: Domain absichern

Wie kann ich verhindern, dass SPAM im Namen meiner eigenen E-Mail-Adresse versendet wird?

Analogie: Türsteher-Anweisung / DMARC-Richtlinie

DMARC24
Security & Deliverability



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

Frage 6: Mailaccount schützen

Wie reduziere ich das Risiko, dass mein E-Mail-Account gehackt wird?

DMARC24
Security & Deliverability

Frage 6: Mailaccount schützen

- Eigenes Passwort für jeden Online-Zugang
- Passkey statt Passwort
- Hardware-Token statt Passwort (z.B. YubiKey)
- 2FA aktivieren. Hinweis: Teilweise ist der Zugriff dennoch ohne 2FA möglich
- Vorsicht bei Phishing-E-Mails. Webmail-Login möglichst nur über Bookmarks aufrufen, nicht über Klicks in Links.
- Vorsicht dabei, die Passwörter zu E-Mail-Dienst Onlinediensten anzuvertrauen. Ggf. separate Accounts und Zugangsdaten zum Versand von E-Mails aus Tools heraus nehmen.
- Falls doch reingefallen: Sofort Passwort ändern. Teils wird nicht sofort zugegriffen.

DMARC24
Security & Deliverability

Dankeschön

So geht‘s weiter:

Kostenloser Kurzcheck auf meiner Webseite: www.dmarc24.de

Bei weiteren Fragen gerne auch per E-Mail oder telefonisch kontaktieren

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