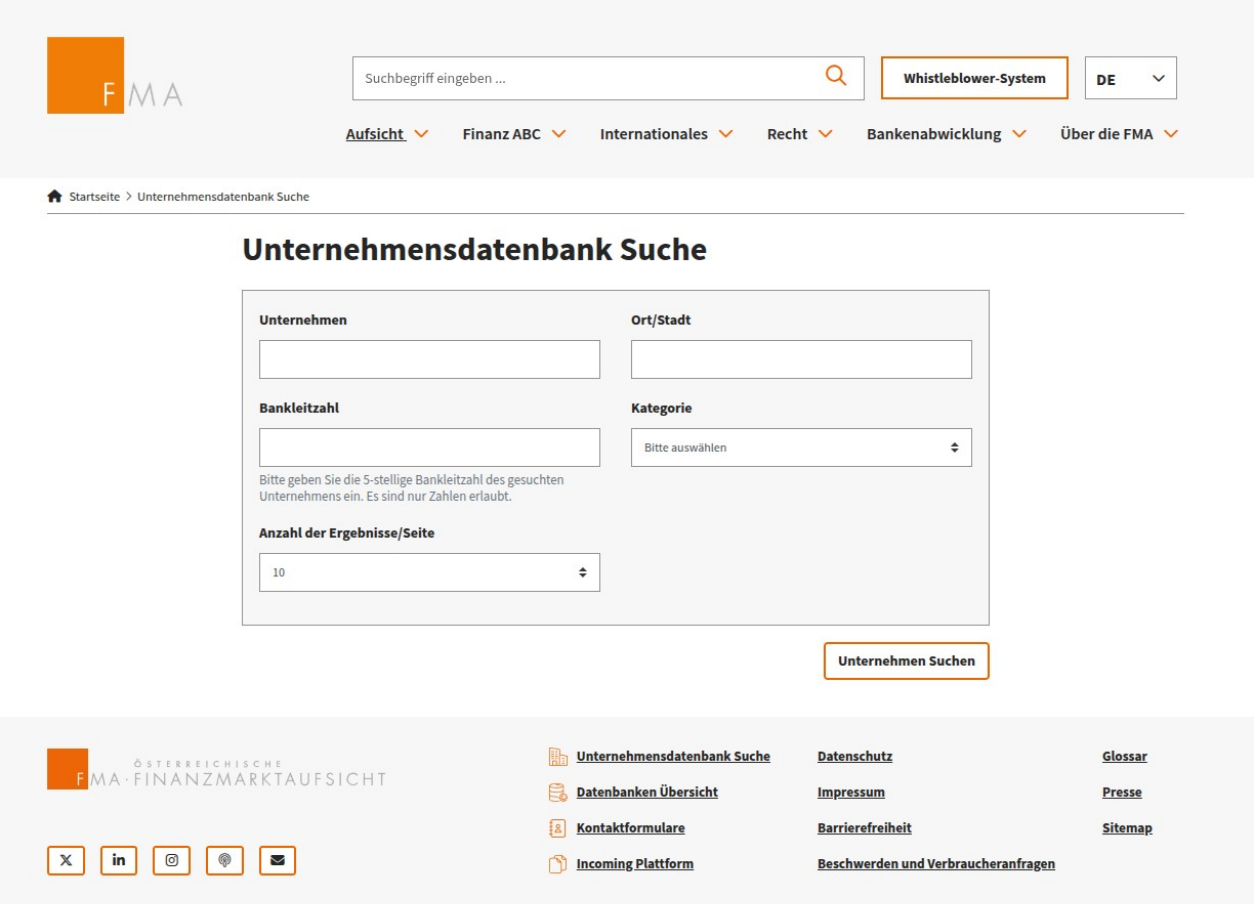
Passive Exposure-Analyse Organisationen in einem DORA-relevanten Umfeld in Österreich

Angriffsflächen-Indikatoren aus Certificate Transparency und DNS Mail Security Posture

Zusammenfassung

Ich untersuche in dieser Arbeit die externe Angriffsfläche einer Auswahl österreichischer, Organisationen in einem DORA-relevanten Umfeld auf Basis ausschließlich öffentlich zugänglicher Metadaten.

Die Auswahl leite ich aus dem **FMA-Portal zur Unternehmensdatenbank-Suche** ab und schränke sie in einem privaten Forschungsprojekt auf Bundesländer in Österreich ein.



Aus den Ergebnissen werden nur Einträge berücksichtigt, bei denen eine Website angegeben war und daraus eine Domain eindeutig extrahiert werden konnte. So entsteht die untersuchte Stichprobe von **195 Domains**.

Die Datenerhebung erfolgt passiv über Certificate Transparency zur Beobachtung von Hostnamen und Subdomains sowie über DNS zur Bewertung der E-Mail-Domänenhärtung (MX, SPF, DMARC; DKIM nur heuristisch).

Auf dieser Grundlage berechne ich einen DORA Exposure **Index (0-100)**, der Subdomain-Exposure-Signale und Mail-Posture-Risiken zu einer priorisierbaren Gesamtsicht kombiniert.

DKIM bewerte ich nur als Hinweis, weil valide DKIM-Abfragen typischerweise selector-abhängig sind. Ohne aktiven Kontext (z. B. bekannte Selector-Namen je Provider oder Mail-Flow-Analyse) sind reine DNS-Checks für DKIM nur eingeschränkt belastbar.

Diese Ergebnisse sind als Indikatoren zu verstehen. Bei einer aktiven technischen Evaluierung (z. B. Fingerprinting, Härtungstests, autorisierte Scans) ist es realistisch, dass die Lage in der Praxis tendenziell **ungünstiger ausfällt**, weil zusätzliche, in CT/DNS nicht sichtbare Expositionen (weitere Endpunkte, Fehlkonfigurationen, Legacy-Services, Schatten-IT) erfasst würden.

Abbildungsverzeichnis

Die folgenden Abbildungen werden im Dokument verwendet:

1. Motivation und Zielsetzung

1.1 Warum dieses Thema?

DORA adressiert operative Resilienz und verlangt ein risikobasiertes Management von IKT-Risiken und externen Angriffsflächen. In der Praxis entstehen viele Initial-Access-Szenarien an wiederkehrenden Punkten wie Remote Access, Identity/SSO, Admin-Portalen, Webmail sowie exponierten Dev/Test- oder Monitoring-Umgebungen. Parallel ist die Kommunikationsdomäne (E-Mail) ein zentraler Angriffskanal für Spoofing, Impersonation und Social Engineering.

SPF, DMARC und DKIM sind daher als Baseline-Härtung relevant.

1.2 Forschungsfrage?

Welche passiv beobachtbaren, externen Exposure-Signale lassen sich in einer FMA-abgeleiteten Domainmenge erkennen, und wie lässt sich daraus ein reproduzierbarer Index ableiten, der priorisierbare Angriffsflächen als Indikation liefert?

1.3 Scope und Abgrenzung

Die Untersuchung ist rein passiv.

Es werden keine aktiven Scans, keine Exploitversuche und keine Interaktionen mit Zielsystemen außerhalb der notwendigen CT- und DNS-Abfragen durchgeführt.

Einzelne Unternehmen oder Domains werden nicht veröffentlicht, es werden ausschließlich zusammengefasste Werte dargestellt. Die Arbeit liefert Indikatoren, keine Nachweise für Verwundbarkeit oder Kompromittierung.

Diese Untersuchung wurde bewusst so konzipiert, dass sie im Rahmen einer rein passiven, **OSINT-basierten Analyse** bleibt. Ziel war es, ausschließlich öffentlich verfügbare **Metadaten auszuwerten**, ohne in Systeme einzudringen, Sicherheitsvorkehrungen zu überwinden oder Dateninhalte abzufangen.

Durchgeführte Handlung:

- **Durchgeführt:**
    - Auswertung von **Certificate-Transparency-Logs** als öffentliche Protokolle über ausgestellte Zertifikate.
    - **DNS-Abfragen** (MX/TXT) zur Bewertung von SPF/DMARC/MX-Posture als reine Konfigurations- und Metadatenanalyse.
- **Nicht durchgeführt:**
    - Kein Aufruf der Websites zur Inhaltsanalyse, kein Crawling, kein Directory Brute Forcing.
    - Kein Portscan, kein Service-Fingerprinting, kein Exploit-Test, kein Bruteforce, keine Login-Versuche.
    - Keine Identifikation einzelner Organisationen im Ergebnis; nur aggregierte Daten.

2. Zielauswahl und Datenbasis

2.1 Herkunft der Zielmenge

Dieses Projekt ist ein privates Research-Vorhaben. Die Ausgangsbasis ist das öffentliche Portal der FMA zur Unternehmensdatenbank-Suche(https://www.fma.gv.at/unternehmensdatenbank-suche/).

Die Abfrage wurde auf Bundesländer in **Österreich** eingeschränkt. Aus den Suchergebnissen wurden nur Datensätze übernommen, bei denen eine Website angegeben war. Daraus wurden eindeutige Domains extrahiert, bereinigt und als Stichprobe verwendet.

Stichprobe: **195 Domains** (Anzahl der Einträge mit angeführter Website und verwertbarer Domain).

2.2 Datenquellen (passiv)

Certificate Transparency liefert Zertifikatsmetadaten, aus denen Hostnamen und Subdomains abgeleitet werden können. DNS liefert MX-Records und TXT-Records, die zur Bewertung von SPF und DMARC genutzt werden. DKIM wird nur heuristisch bewertet, weil Selector-abhängige Abfragen ohne aktiven Kontext nur eingeschränkt belastbar sind.

3. Methodik

3.1 Bewertungslogik

Ich kombiniere zwei Signale, Subdomain-Exposure aus CT und Mail Security Posture aus DNS. Beide fließen in einen **DORA Exposure Index (0-100)** ein.

3.2 Subdomain-Kategorisierung

Subdomains werden anhand des linken Labels (Prefix) in Kategorien gemappt. Die Kategorien orientieren sich an **typischen Entry Points** aus realen Angriffsketten, insbesondere Remote Access, Identity/SSO, Admin/Management, Mail/Webmail, Backup/DR sowie sekundären, aber häufig problematischen Bereichen wie Dev/Test/Staging, Monitoring und Repo/CI.

3.3 Freshness-Weighting

CT-Signale können historisch sein. Deshalb gewichte ich Treffer anhand von last_seen:

- **fresh <= 90 Tage: 1.0**
- **stale <= 365 Tage: 0.6**
- **old > 365 Tage: 0.2**
- **unknown: 0.6**

3.4 Mail Security Posture

SPF, DMARC und MX werden nach Severity (GREEN/YELLOW/RED) bewertet. DMARC gilt als RED, wenn kein DMARC vorhanden ist oder p=none gesetzt ist. SPF gilt als RED bei fehlendem SPF, allow-all oder stark auffälligen Heuristiken. MX gilt als RED bei 0 MX oder Status != ok. DKIM wird nur als heuristischer Indikator behandelt.

Eine DMARC-Policy mit p=none ist nicht „falsch“, sondern häufig ein **Einführungs- bzw. Monitoring-Zustand**. Für diese Arbeit werte ich **p=none dennoch als RED**, weil ohne Enforcement (quarantine/reject) Spoofing/Impersonation in der Praxis deutlich weniger effektiv eingedämmt wird.

3.5 Scoring und Banding (Ampellogik)

Der Index setzt sich aus zwei Teilen zusammen. Ein Teil beschreibt die Sichtbarkeit von Subdomains in Certificate-Transparency-Logs (mit Gewichtung nach Aktualität und Fokus auf kritische Entry-Point-Kategorien). Der zweite Teil bewertet die E-Mail-Härtung über DNS (MX, SPF, DMARC; DKIM nur heuristisch). Die Kurzformel kann als Abbildung ergänzt werden.

Limitationen des Index

Der DORA Exposure Index ist ein heuristischer Priorisierungswert, abgeleitet aus passiven CT- und DNS-Signalen. CT-Einträge sind ein Proxy für Zertifikatsnutzung und Namensräume, belegen jedoch keine aktuelle Erreichbarkeit oder Aktivität eines Dienstes.

Gewichte und Schwellenwerte (GREEN/YELLOW/RED) sind operativ gesetzt und nicht empirisch gegen **Ground Truth** (z. B. autorisierte Scans/Incidents) validiert.

Außerdem kann ein Bias entstehen, große Organisationen mit vielen Subdomains und Zertifikaten erhalten selbstverständlich höhere Exposure-Signale. Der Index ist daher als

reproduzierbarer Hinweis zur Priorisierung zu verstehen und nicht als Nachweis einer Verwundbarkeit oder als Compliance-Bewertung.

Um die Ergebnisse vergleichbar zu machen, habe ich für jede Domain einen **DORA Exposure Index** zwischen **0 und 100** berechnet. In diesen Score fließen zwei Dinge ein:

1. **Subdomain-Exposure:** Welche extern sichtbaren Subdomains und typische Einstiegspunkte (z. B. Login, VPN, Admin, Webmail, Dev/Test) tauchen in den Daten auf und wie „aktuell“ sind diese Signale.
2. **Mail-Sicherheitslage:** Wie gut die Domain im Bereich E-Mail abgesichert ist (MX, SPF, DMARC; DKIM nur als Hinweis).

Am Ende ordne ich jede Domain einer von drei Stufen zu, damit man schnell erkennt, wo Priorität entsteht:

- **GREEN (< 30 Punkte):** eher niedrige Exposition bzw. wenig kritische Signale
- **YELLOW (30 bis 59 Punkte):** mittlere Exposition, einzelne kritische Hinweise oder mehrere moderate
- **RED (ab 60 Punkten):** erhöhte Exposition, mehrere kritische Signale oder klare Häufungen

Diese Ampel ist kein Beweis für eine Schwachstelle, sondern eine **Priorisierung**, wo sich eine genauere (autorisierte) Prüfung am ehesten lohnt.

3.6 Limitationen

Diese Untersuchung ist bewusst konservativ und basiert ausschließlich auf passiven Metadaten (CT und DNS).
Daraus ergeben sich Grenzen; **(1) Certificate Transparency** beweist keine aktuelle Erreichbarkeit oder aktive Dienste, sondern nur, dass ein Hostname zu einem Zeitpunkt zertifiziert wurde. **(2) DNS** zeigt Konfiguration, aber nicht die tatsächliche Wirksamkeit in der Praxis (z. B. DMARC-Alignment, Forwarding-Effekte, Provider-Setups). **(3) Subdomain-Listen** aus CT können historische Artefakte enthalten (Migrationen, Alt-Systeme, automatische Zertifikatserneuerungen). **(4) Der Index** priorisiert, er ersetzt keine autorisierte technische Prüfung (Reachability, Auth-Flow, Härtung, Patchstand, etc.).

3.7 Ethik & Rechtlicher Rahmen

Dieses Projekt ist als **privates Research-Vorhaben** angelegt und folgt dem Grundsatz „**so wenig Interaktion wie möglich**“.
Ich habe keine Ziel-Websites aufgerufen, keine Requests gegen Applikations-Endpunkte gesendet und keine aktiven Scans durchgeführt. Die Datenerhebung beschränkt sich auf Certificate-Transparency-Logs und DNS-Abfragen (MX/TXT), also auf öffentlich verfügbare Metadaten.

Hintergrund dieser Entscheidung ist auch der **österreichische Rechtsrahmen** Unautorisierte Zugriffe bzw. das Überwinden von Zugriffsbeschränkungen können strafrechtlich relevant sein. Die gewählte Methodik reduziert dieses Risiko, weil sie ohne Eindringen, ohne Ausnutzung und ohne Dienstinteraktion auskommt. Die Arbeit veröffentlicht keine Einzeldomains oder Unternehmensnamen, sondern ausschließlich aggregierte Daten.

4. Ergebnisse

4.1 DORA Exposure Band (Index-basiert)

Siehe **Abbildung 1** und **Abbildung 2**.

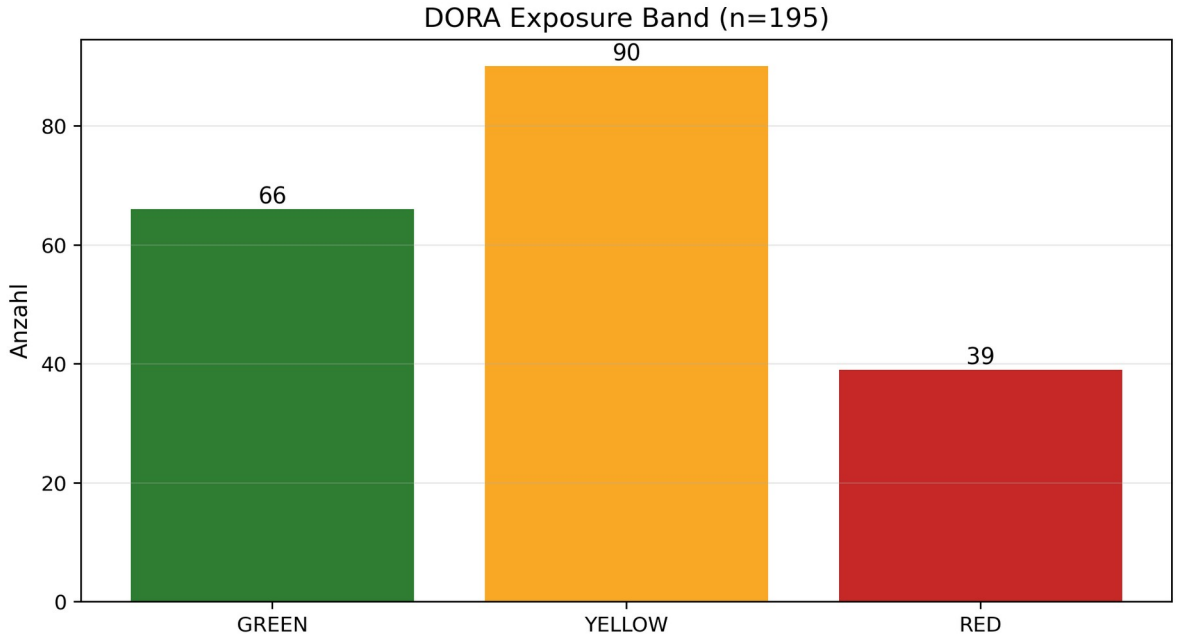


Abbildung 1: Verteilung der Domains nach DORA Exposure Band (GREEN/YELLOW/RED).

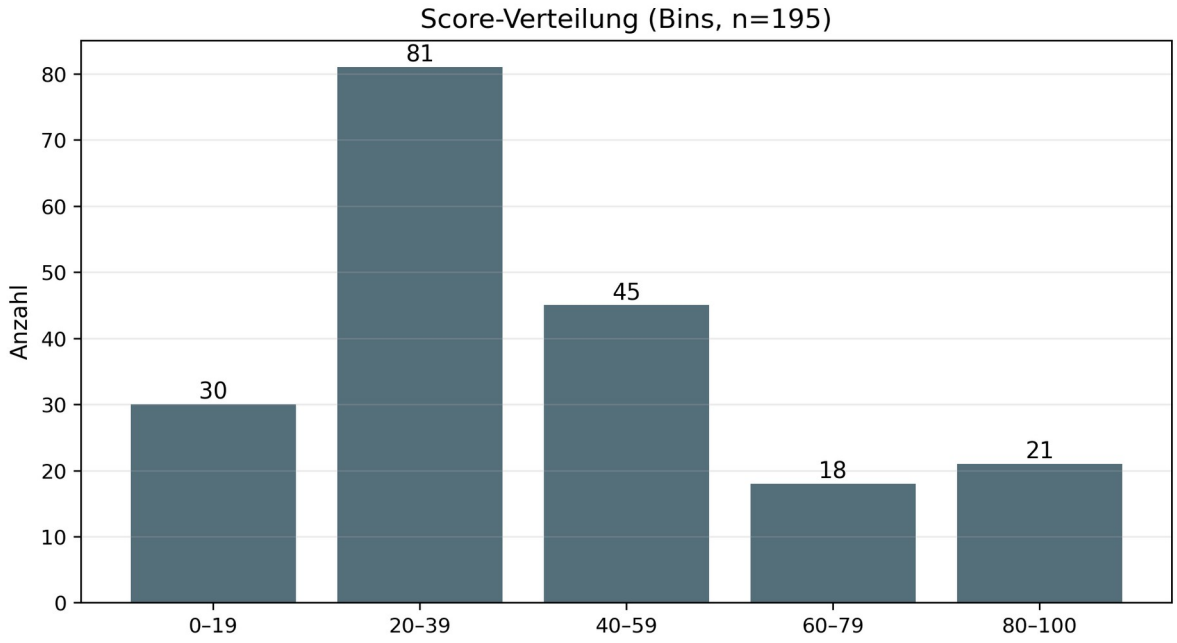


Abbildung 2: Score-Verteilung (Bins) des DORA Exposure Index.

In der Stichprobe von **195 Domains** ergibt sich folgende Verteilung:

- **GREEN:** 66 Domains (**33,8 %**)
- **YELLOW:** 90 Domains (**46,2 %**)
- **RED:** 39 Domains (**20,0 %**)

Zusätzlich hilft ein Blick auf die Score-Gruppen, um zu sehen, wie stark die Werte streuen:

- **0–19 Punkte:** 30 Domains
- **20–39 Punkte:** 81 Domains
- **40–59 Punkte:** 45 Domains
- **60–79 Punkte:** 18 Domains
- **80–100 Punkte:** 21 Domains

Der größte Teil liegt im mittleren Bereich. Gleichzeitig ist der Anteil im roten Bereich nicht klein, etwa jede **fünfte Domain** zeigt eine **erhöhte Exposition**.

Das passt dazu, dass in der Auswertung die extern sichtbaren Subdomain-Signale stärker in den Gesamtscore einfließen. Genau diese Entry Points sind in der Praxis oft die Stellen, an denen Angriffe ansetzen.

4.2 Subdomain-Exposure (Entry-Point-Fokus)

Siehe **Abbildung 3** und **Abbildung 4**.

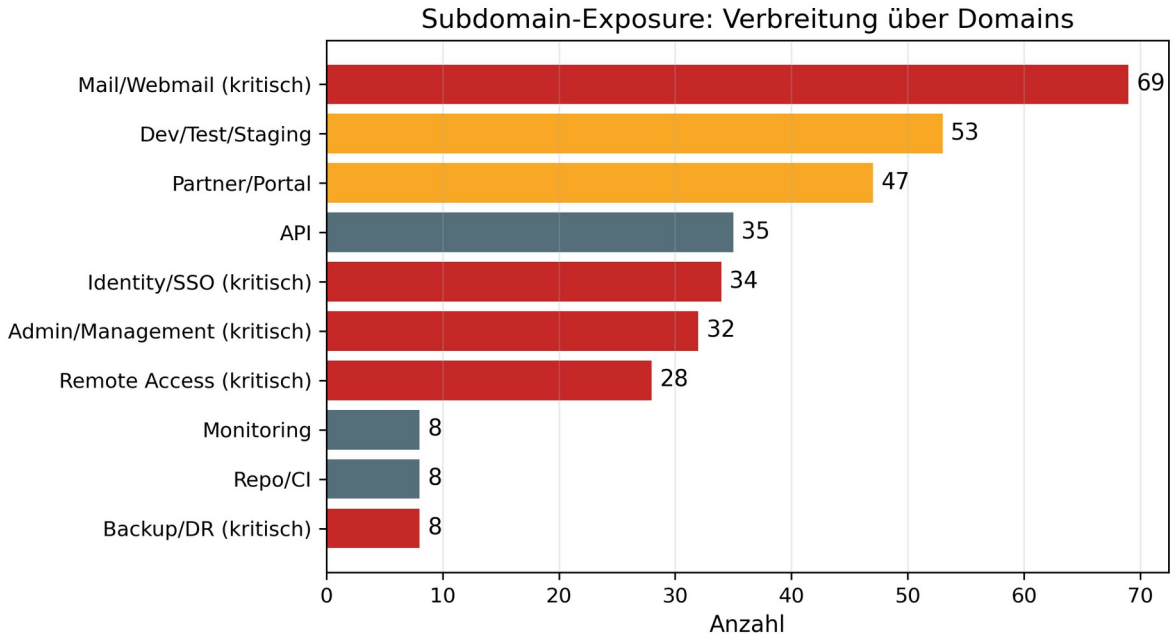


Abbildung 3: Verbreitung relevanter Subdomain-Kategorien (Anzahl Domains).

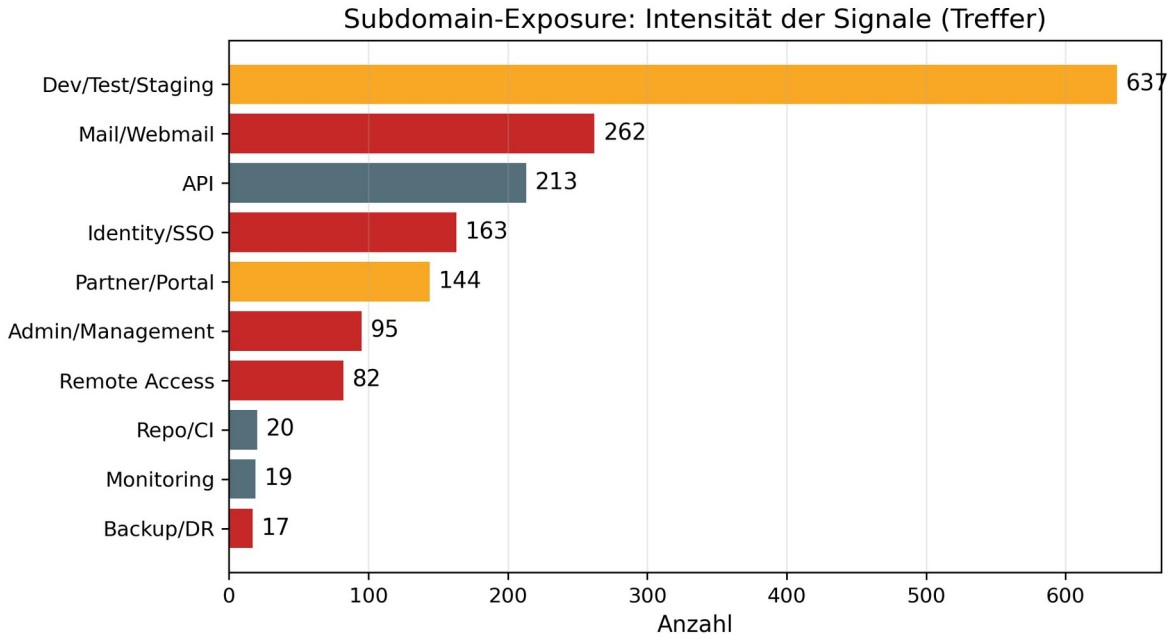


Abbildung 4: Intensität der Subdomain-Signale (Summe der Treffer je Kategorie).

Bevor ich die Zahlen einordne, kurz zur Begrifflichkeit:
Eine Domain ist zum Beispiel `faydin.blog` Ein **FQDN** (Fully Qualified Domain Name) ist der vollständig ausgeschriebene Hostname, also inklusive Subdomain, z. B. `vpn.faydin.blog` oder `login.faydin.blog` Genau solche FQDNs tauchen in Certificate-Transparency-Logs(CT) auf, wenn dafür TLS-Zertifikate ausgestellt wurden.

Das heißt nicht automatisch, dass der Dienst heute noch online ist, aber es ist ein guter Hinweis darauf, welche externen Einstiegspunkte es gab oder gibt.

In der Stichprobe sind die Subdomain-Signale breit verteilt. Für die Auswertung sind zwei Perspektiven wichtig:

1. **Wie viele Domains** haben mindestens einen Hinweis auf eine Kategorie (Verbreitung).
2. **Wie oft** taucht diese Kategorie insgesamt auf (Intensität).

Verbreitung über Domains (mindestens ein Signal in der Kategorie)

- **Mail/Webmail (kritisch): 69 Domains**
  Typisch sind Webmail-Oberflächen oder Mail-Gateways, also direkte Einstiegspunkte rund um E-Mail und Postfächer.
- **Dev/Test/Staging: 53 Domains**
  Test- und Entwicklungsumgebungen, die oft schwächer gehärtet sind oder unbeabsichtigt öffentlich sichtbar werden.
- **Partner/Portal: 47 Domains**
  Externe Portale für Kunden oder Partner, häufig Login-basiert und daher ein klassischer Angriffsvektor.
- **API: 35 Domains**
  Schnittstellenendpunkte, die Anwendungen und Dienste verbinden; sicherheitsrelevant wegen Authentisierung, Tokens und Datenzugriff.
- **Identity/SSO (kritisch): 34 Domains**
  Login- und SSO-Portale, die als zentraler „Schlüssel“ zu vielen Systemen dienen können.
- **Admin/Management (kritisch): 32 Domains**
  Verwaltungsoberflächen, Konsolen oder Panels mit hoher Auswirkung, falls kompromittiert.

- **Remote Access (kritisch): 28 Domains**
  VPN, Gateway oder Remote-Zugänge, die häufig als Initial-Access-Punkt angegriffen werden.
- **Monitoring: 8 Domains**
  Überwachungs- und Dashboard-Systeme, die zwar „nur“ Monitoring sind, aber oft sensible Betriebsinfos enthalten.
- **Repo/CI: 8 Domains**
  Code- und Build-Systeme, kritisch wegen Secrets und möglicher Supply-Chain-Risiken.
- **Backup/DR (kritisch): 8 Domains**
  Backup, Disaster-Recovery oder Virtualisierungs-Oberflächen, besonders kritisch im Kontext Ransomware.

Intensität der Signale (Summe der Treffer)

- **Dev/Test/Staging: 637 Treffer**
- **Mail/Webmail: 262 Treffer**
- **API: 213 Treffer**
- **Identity/SSO: 163 Treffer**
- **Partner/Portal: 144 Treffer**
- **Admin/Management: 95 Treffer**
- **Remote Access: 82 Treffer**
- **Repo/CI: 20 Treffer**
- **Monitoring: 19 Treffer**
- **Backup/DR: 17 Treffer**

Einordnung

Dev/Test ist in der Stichprobe besonders dominant. Das ist aus Angreifersicht relevant, weil Testumgebungen in der Praxis oft weniger strikt isoliert sind, manchmal veraltete Komponenten enthalten und gelegentlich **„vergessene“ Deployments** entstehen.

Zusätzlich sieht man in einem relevanten Anteil der Domains kritische Kategorien wie Mail/Webmail, Identity/SSO, Admin/Management und Remote Access. Diese Kategorien sind typische Einstiegspunkte in realen Angriffsketten und beeinflussen daher Priorisierung und Risikobild deutlich.

4.3 Freshness der kritischen Kategorien bzw. Wie aktuell sind die Hinweise?

Siehe **Abbildung 5**.

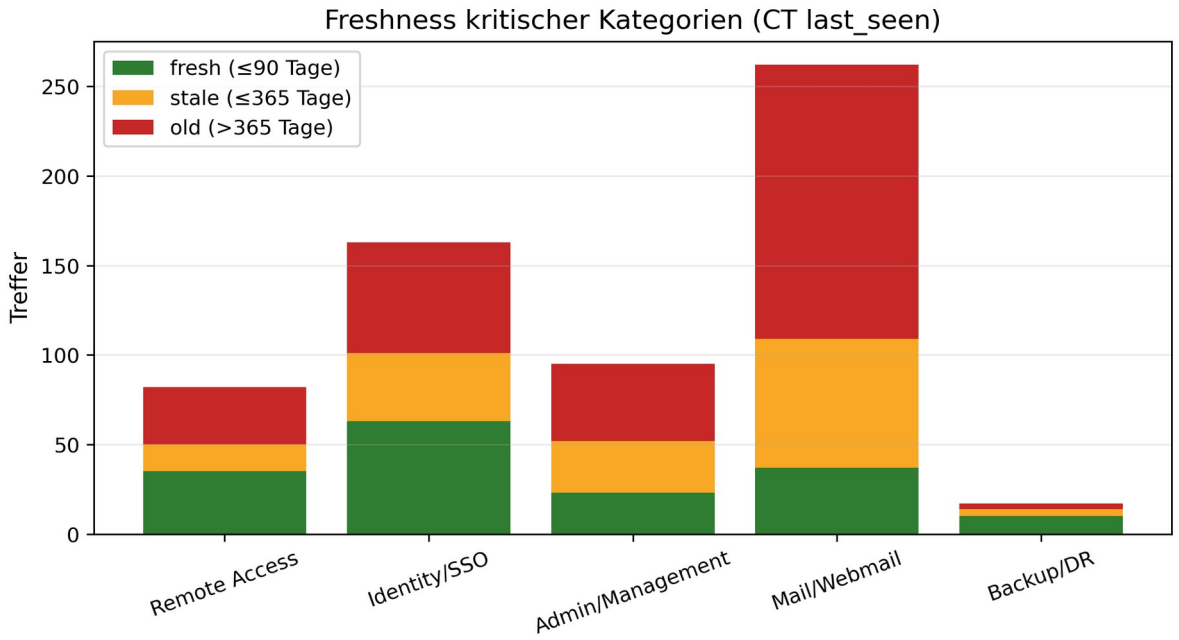


Abbildung 5: Freshness (last_seen) für kritische Kategorien: fresh/stale/old.

Certificate-Transparency-Daten zeigen, dass ein Hostname zu einem bestimmten Zeitpunkt ein TLS-Zertifikat hatte.

Sie sagen aber **nicht** sicher, ob der Dienst **heute noch aktiv ist**. Zusätzlich ist wichtig zu verstehen, dass Zertifikate eine Laufzeit haben.

In der Praxis sind Zertifikate oft für einen gewissen Zeitraum gültig und werden regelmäßig erneuert. Dadurch kann ein Hostname auch dann als „fresh“ erscheinen, wenn er weiterhin betrieben wird, aber es kann umgekehrt auch „fresh“ Signale geben, die nur aus einer automatisierten Erneuerung resultieren, ohne dass sich der Dienst selbst verändert hat.

Freshness ist daher ein guter Priorisierungshinweis, aber kein Beweis für aktuelle Erreichbarkeit.

Um alte Einträge nicht zu übergewichten, bewerte ich die Signale nach ihrer „Freshness“, also danach, wann sie zuletzt in CT beobachtet wurden:

- **fresh:** zuletzt innerhalb der letzten 90 Tage gesehen
- **stale:** zuletzt innerhalb der letzten 365 Tage gesehen
- **old:** zuletzt vor mehr als 365 Tagen gesehen

Zeitbezug für kritische Kategorien (Trefferverteilung)

- **Remote Access:** 82 Treffer (fresh 35, stale 15, old 32)
- **Identity/SSO:** 163 Treffer (fresh 63, stale 38, old 62)
- **Admin/Management:** 95 Treffer (fresh 23, stale 29, old 43)
- **Mail/Webmail:** 262 Treffer (fresh 37, stale 72, old 153)
- **Backup/DR:** 17 Treffer (fresh 10, stale 4, old 3)

Einordnung

Mehrere kritische Kategorien haben einen spürbaren Anteil an fresh-Signalen. Das ist relevant, weil es nahelegt, dass diese Einstiegspunkte zumindest in jüngerer Zeit sichtbar waren.

Dadurch steigt die Priorität für eine autorisierte interne Nachprüfung, zum Beispiel ob diese Endpunkte heute **noch erreichbar sind(Cyber-Hygiene)** und wie sie abgesichert sind.

Gleichzeitig gilt weiterhin, CT ist ein Metadaten-Signal. Ein „fresh“-Eintrag beweist nicht, dass ein Dienst aktuell aktiv ist, und ein „old“-Eintrag bedeutet nicht automatisch, dass er verschwunden ist. Die Freshness-Klassifizierung hilft vor allem dabei, die Reihenfolge für weiterführende Prüfungen sinnvoll zu setzen.

4.4 Mail Security Posture (DNS)

Siehe **Abbildung 6**.

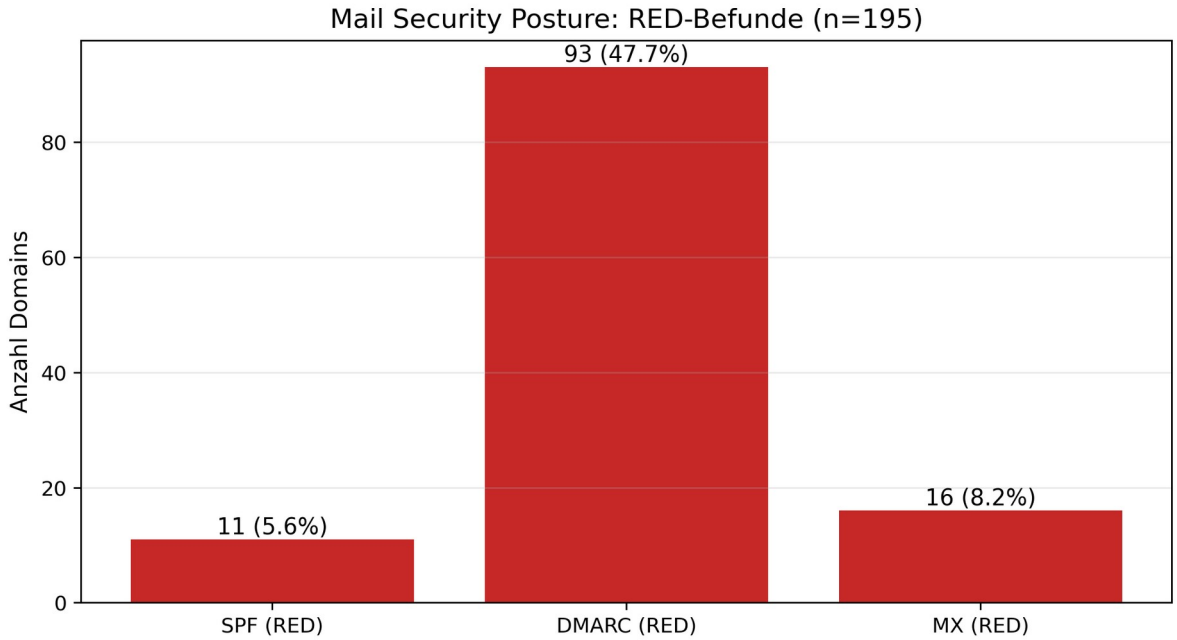


Abbildung 6: RED-Befunde in SPF/DMARC/MX (Anzahl und Anteil).

Faktencheck (Domain=195):

- **SPF RED: 11 (5,6%)**
- **DMARC RED: 93 (47,7%)**
- **MX RED: 16**

Der größte Einzelbefund ist DMARC RED, also fehlendes DMARC oder p=none. Das ist ein starker Indikator für Spoofing- und Impersonation-Risiken. SPF ist häufiger solide, aber ohne DMARC-Durchsetzung bleibt Spoofing in der Praxis oft weiterhin möglich oder zumindest schwerer kontrollierbar.

4.5 MX-Cloud- und Cloud Provider-Anteile (Heuristik)

Einordnung aus DORA-Perspektive, eine starke Konzentration auf wenige große, teils außerhalb der EU ansässige Anbieter ist nicht per se „falsch“, kann aber Abhängigkeits- und Konzentrationsrisiken erhöhen.

Genau hier setzt DORA an, Finanzunternehmen sollen ICT-Drittparteirisiken aktiv steuern, Abhängigkeiten dokumentieren und für kritische Funktionen **Exit-Strategien** und Vertragsklauseln sauber regeln.

Meine Daten zeigen keine Compliance-Bewertung, sie liefern aber ein Signal, wo sich Abhängigkeiten statistisch häufen könnten.

Siehe **Abbildung 7** und **Abbildung 8**.

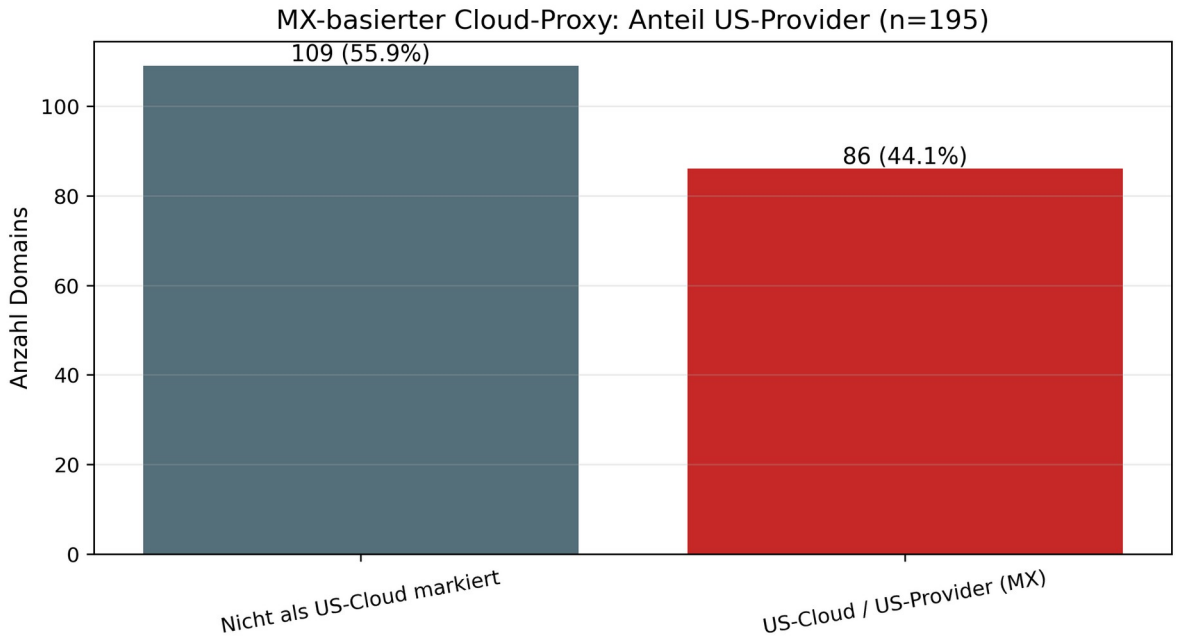


Abbildung 7: Anteil Domains mit US-Cloud/US-Provider-MX (Heuristik, n=195).

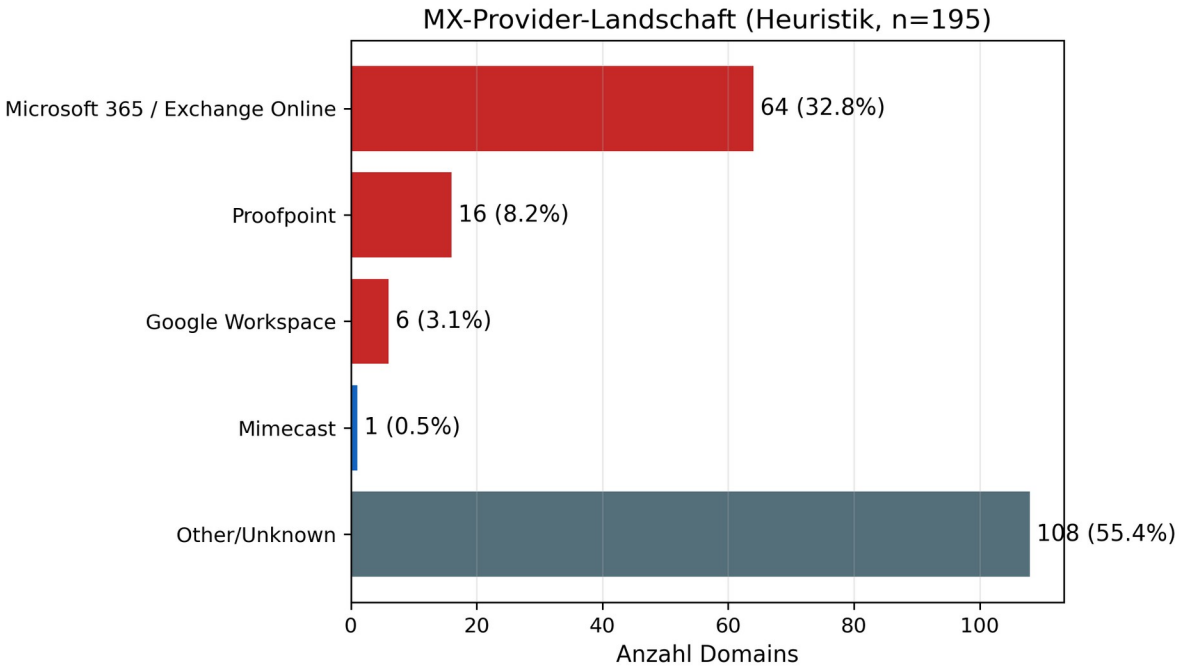


Abbildung 8: Verteilung der MX-Provider (Heuristik aus MX-Hostnamen, n=195).

Wichtig: Das ist eine Heuristik auf Basis der MX-Strings. „Other/Unknown“ heißt nicht automatisch „on-prem“, sondern nur, dass der Provider aus den MX-Namen nicht eindeutig klassifizierbar war.

Zusätzlich zur Mail-Härtung lässt sich aus den MX-Hostnamen eine grobe Einordnung ableiten, ob eine Domain ihren E-Mail-Verkehr über große **Cloud-/Managed-Provider abwickelt**. In meiner Stichprobe sind 86 von 195 Domains (**44.1%**) als **US-Cloud/US-Provider** markiert; 109 Domains (55.9%) sind in dieser Heuristik nicht als US-Cloud markiert.

4.6 Hinweis zur erwartbaren Abweichung bei aktiver Evaluierung

Diese Untersuchung ist absichtlich passiv und konservativ. Bei einer **aktiven Evaluierung** unter autorisiertem Rahmen ist es wahrscheinlich, dass zusätzliche Exposition sichtbar wird, etwa nicht zertifikatsgebundene Dienste, alternative Hostnames, Schatten-IT, Legacy-Endpunkte, falsch konfigurierte Reverse Proxies oder öffentlich erreichbare Managementports.

Dadurch würden Kennzahlen zu kritischen Entry Points und risikorelevanten Konfigurationen typischerweise **eher negativer ausfallen** als in einer reinen CT/DNS-Perspektive.

5. Schlussfolgerung

Die Auswertung zeigt, dass Subdomain-Exposure ein zentraler Treiber des Gesamtrisikos in der Stichprobe ist.

Insbesondere die Sichtbarkeit von Mail/Webmail, Identity/SSO, Admin/Management und Remote-Access-Subdomains liefert starke Priorisierungssignale.

Parallel fällt ein hoher Anteil an Domains ohne durchsetzende DMARC-Policy auf. Aus diesen Indikatoren lässt sich eine belastbare, reproduzierbare Prioritätenliste ableiten, die DORA-orientierte Maßnahmen zur Reduktion externer Angriffsflächen und zur Härtung der Kommunikationsdomäne unterstützt.

Meine Erfahrungen zeigen, dass Penetrationstests in Österreich in vielen Fällen nicht konsequent **nach etablierten Methodiken** und **Standards** (u.a OWASP WSTG, OSSTMM..) durchgeführt werden. Stattdessen werden Tests häufig primär über einen Zeitrahmen („x Personentage“) definiert, ohne klar festzulegen, welche Prüfpunkte, Controls und Abdeckungen damit verbindlich erreicht werden sollen. Dies dient in vielen Fällen zur erfüllung der ISO 27001 Norm.

Dadurch sind die Ergebnisse oft schwer vergleichbar und der langfristige Mehrwert sinkt, weil wesentliche Bereiche je nach Ansatz **unterschiedlich** oder **gar nicht geprüft** werden.

Meine Empfehlung ist daher eine **unabhängige Stelle**, die externe Angriffsfläche dieser Unternehmen laufend beobachtet, Veränderungen erkennt, Risiken bewertet und konkrete Handlungsempfehlungen zurückspielt.

Das könnte entweder über CERT.at als zentrale nationale Funktion erfolgen oder als eigenes Monitoring-Team bei der FMA umgesetzt werden, um Monitoring und Risikobewertung dauerhaft und nachvollziehbar zu verankern.

Lizenz & Nutzung

Über den Autor

Profil: https://www.faydin.blog

Ich bin Ferat Aydin, Penetration Tester, Security Architect und Security Researcher.

Ich arbeite gerne pragmatisch und nachvollziehbar, mit Fokus auf echte Angriffspfade statt theoretische Checklisten. In meiner Arbeit orientiere ich mich an Standards wie OWASP WSTG und ASVS sowie an PTES und lege Wert auf reproduzierbare Ergebnisse und klare Prioritäten, die in der Praxis umsetzbar sind.

Neben klassischen Pentests beschäftige ich mich auch mit der Analyse von Angriffsmethoden und Vorgehensweisen von Ransomware-Gruppen. Besonders interessieren mich dabei Initial Access, laterale Bewegung und die typischen Muster, die man in realen Kampagnen immer wieder sieht. Dieses Wissen nutze ich, um externe Angriffsflächen nicht nur zu messen, sondern auch realistisch einzuordnen.