

SPF, DKIM, DMARC für Exchange Online

Es gibt zwei Sorten von Organisationen: die einen haben SPF, DKIM und DMARC sauber eingerichtet, die anderen haben es noch nicht gemerkt. Der Unterschied fällt lange nicht auf, denn E-Mail ist ein erstaunlich gutmütiges Protokoll. Es liefert auch dann noch aus, wenn die Absenderangabe frei erfunden ist. Genau darauf baut jeder halbwegs ambitionierte Angriff auf: Eine Mail, die scheinbar von der eigenen Geschäftsführung kommt, ist im Zweifel überzeugender als jede technisch ausgefeilte Schadsoftware.

Die drei Mechanismen sind keine neue Erfindung. Sie sind älter als die meisten Cloud-Dienste, die sie heute benutzen, und sie sind in Exchange Online mit überschaubarem Aufwand einzurichten. Trotzdem scheitert die Einführung in der Praxis regelmäßig — nicht an der Technik, sondern daran, dass niemand mehr weiß, welche Systeme eigentlich alle im Namen der Firmendomäne Post verschicken. Das Multifunktionsgerät im zweiten Stock ist da nur der Anfang.

Es gibt inzwischen auch handfeste wirtschaftliche Gründe. Seit dem 5. Mai 2025 verlangt Microsoft von Absendern, die mehr als 5.000 Nachrichten pro Tag an outlook.com, hotmail.com oder live.com zustellen, funktionierendes SPF, funktionierendes DKIM und einen DMARC-Eintrag mit mindestens `p=none`, ausgerichtet auf mindestens einen der beiden Mechanismen. Google und Yahoo haben mit ähnlichen Anforderungen bereits im Februar 2024 vorgelegt. Wer nicht liefert, landet erst im Junk-Ordner und dann gar nicht mehr. E-Mail-Authentifizierung ist damit vom Sicherheitsthema zum Zustellbarkeitsthema geworden, und das interessiert erfahrungsgemäß deutlich mehr Menschen im Haus.

Dieser Beitrag gehört zum Handlungsfeld C der Serie [Microsoft 365 Security](#). Er beschreibt die drei Mechanismen so, dass du sie erklären kannst, zeigt die konkrete Einrichtung in Exchange Online und im DNS, führt durch den Weg von none über quarantine nach reject — und benennt die Fallen, in die man auf diesem Weg zuverlässig tritt.

FAKTEN · Was hier vorausgesetzt wird

Du hast Zugriff auf das DNS deiner Domänen und auf den Microsoft Defender Portal beziehungsweise Exchange Online PowerShell. Ohne DNS-Zugriff kannst du nichts davon umsetzen — und wenn der DNS-Zugriff beim Neffen des Geschäftsführers liegt, ist das der erste Punkt auf deiner Liste.

- › SPF und DMARC werden ausschließlich im DNS gepflegt, nicht in Microsoft 365.
- › DKIM wird in Microsoft 365 aktiviert, braucht aber zwei CNAME-Einträge im DNS.
- › Nichts davon kostet Lizenzgebühren. Es kostet Sorgfalt.

Die drei Mechanismen, ohne Zaubertricks

Bevor wir Einträge schreiben: Die drei Verfahren lösen drei verschiedene Probleme, und sie tun das unabhängig voneinander. Wer sie als eine große Sache begreift, wird beim ersten Fehlerfall unglücklich, weil er nicht weiß, an welcher Schraube er drehen muss.

SPF: Wer darf für diese Domäne senden?

Sender Policy Framework ist eine Türsteherliste im DNS. Du hinterlegst als TXT-Eintrag, welche IP-Adressen und welche Dienste Post für deine Domäne einliefern dürfen. Das empfangende System schaut nach, ob die IP-Adresse, von der die Verbindung kommt, in dieser Liste steht.

Der entscheidende und meistübersehene Punkt: SPF prüft die Domäne im MAIL-FROM des SMTP-Dialogs, also den Umschlagabsender — nicht die Adresse, die dein Gegenüber im Mailprogramm sieht. Diese beiden Angaben dürfen völlig verschieden sein, und bei Newsletter-Diensten sind sie es fast immer. SPF allein hindert also niemanden daran, eine Mail zu bauen, die im Posteingang aussieht, als käme sie von deinem Vorstand.

DKIM: Ist die Nachricht unterwegs verändert worden?

DomainKeys Identified Mail signiert ausgehende Nachrichten kryptografisch. Der private Schlüssel liegt beim Absendersystem, in unserem Fall bei Microsoft. Der zugehörige öffentliche Schlüssel steht im DNS und wird über einen sogenannten Selektor adressiert. Der Empfänger rechnet nach, ob Signatur, Kopfzeilen und Rumpf zusammenpassen.

DKIM hat zwei angenehme Eigenschaften: Es überlebt eine Weiterleitung, solange niemand die Nachricht verändert, und es sagt etwas über die Unversehrtheit aus. Es hat aber dieselbe Schwäche wie SPF: Die signierende Domäne im d=-Feld muss nicht die Domäne sein, die im sichtbaren Absender steht. Ein Angreifer kann eine Mail sauber mit seiner eigenen Domäne signieren und trotzdem deinen Firmennamen ins Von-Feld schreiben.

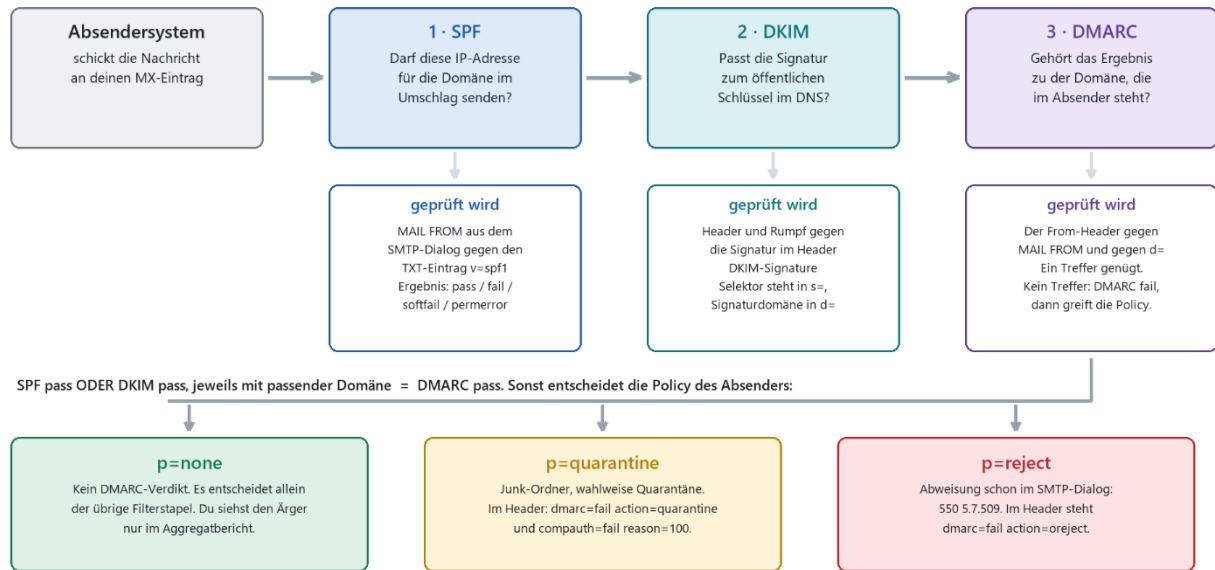
DMARC: Gehört das eigentlich zusammen?

Hier schließt sich die Lücke. DMARC nimmt die Ergebnisse von SPF und DKIM und stellt die entscheidende Zusatzfrage: Passt die geprüfte Domäne zu der Domäne, die im From-Header steht? Dieser Abgleich heißt Alignment. Besteht mindestens einer der beiden Wege — SPF mit passender Domäne oder DKIM mit passender Domäne —, dann besteht die Nachricht DMARC. Fallen beide durch, greift die Policy, die du im DNS veröffentlicht hast: none, quarantine oder reject.

Standardmäßig gilt das Alignment als relaxed, das heißt: die organisatorische Domäne muss übereinstimmen, Subdomänen sind erlaubt. Mit aspf=s beziehungsweise adkim=s kannst du auf strict umstellen, dann muss der vollqualifizierte Name exakt passen. In den meisten Umgebungen ist strict der schnellste Weg, sich selbst ins Knie zu schießen — bleib bei relaxed, bis du einen sehr guten Grund hast.

Der Weg einer Mail durch die Prüfung

Was Exchange Online Protection der Reihe nach fragt — und was am Ende passiert



Die Reihenfolge ist fest. DMARC erfindet keine eigene Prüfung, es bewertet nur die beiden davor.

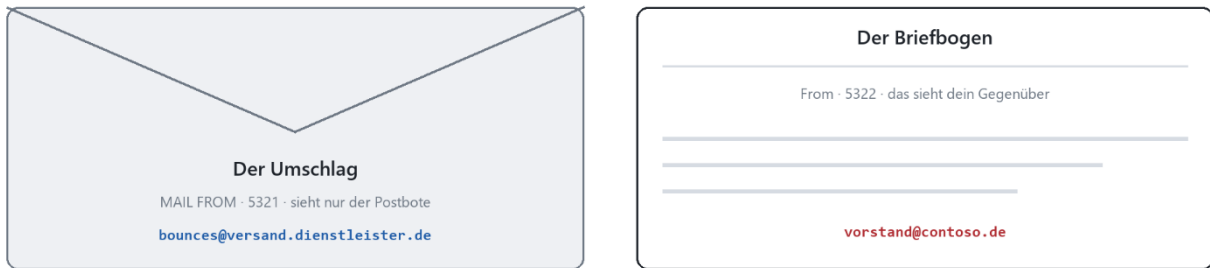
Skizze 1: Der Weg einer Mail durch die drei Prüfungen. DMARC erfindet keine eigene Prüfung, es bewertet nur, ob die Ergebnisse der beiden davor zum sichtbaren Absender gehören.

Mechanismus	Prüft	Bezieht sich auf	Blinder Fleck
SPF	Ist die einliefernde IP-Adresse berechtigt?	MAIL FROM (Umschlag, 5321)	Sagt nichts über den sichtbaren Absender; bricht bei Weiterleitungen
DKIM	Ist die Signatur gültig und die Nachricht unverändert?	d=-Wert in der DKIM-Signature	Jeder darf gültig signieren, auch der Angreifer mit seiner eigenen Domäne
DMARC	Passt SPF oder DKIM zur Absenderdomäne?	From-Header (sichtbar, 5322)	Wirkt nur, wenn SPF und DKIM darunter tatsächlich funktionieren

Tabelle 1: Was die drei Mechanismen jeweils leisten — und was nicht.

Zwei Absender, und nur einer ist sichtbar

Warum SPF und DKIM bestehen können und DMARC trotzdem durchfällt



SPF prüft links. Der Mensch liest rechts. DMARC ist die Instanz, die beide Seiten vergleicht.

From-Header	MAIL FROM bzw. DKIM d=	relaxed (Standard)	strict (aspf=s / adkim=s)
user@contoso.de	contoso.de	passt	passt
user@contoso.de	bounces.contoso.de	passt	passt nicht
user@marketing.contoso.de	contoso.de	passt	passt nicht
user@contoso.de	contoso.onmicrosoft.com	passt nicht	passt nicht
user@contoso.de	versand.dienstleister.de	passt nicht	passt nicht

Der vierte Fall ist der Klassiker: Die Mail ist sauber signiert — nur eben von der onmicrosoft.com-Domäne, und die passt nicht zum sichtbaren Absender.

Skizze 2: Umschlag und Briefbogen tragen unterschiedliche Absender. SPF liest den Umschlag, dein Gegenüber liest den Briefbogen — DMARC vergleicht beide.

WICHTIG · Der häufigste Denkfehler

„Wir haben SPF, damit sind wir geschützt.“ SPF ohne DMARC schützt niemanden vor gefälschten Absendern, weil SPF eine Adresse prüft, die kein Mensch je zu sehen bekommt. Umgekehrt gilt: DMARC ohne funktionierendes SPF und DKIM ist ein Versprechen ohne Deckung. Die drei ergeben nur gemeinsam einen Sinn.

Einrichtung in Exchange Online und im DNS

Die Reihenfolge ist nicht beliebig. Erst SPF, dann DKIM, dann DMARC mit p=none. Wer mit DMARC anfängt, veröffentlicht eine Regel für eine Prüfung, die es noch gar nicht gibt.

Schritt 1: Der SPF-Eintrag

SPF ist ein einzelner TXT-Eintrag auf dem Domänennamen selbst, nicht auf einem Unterknoten. Für eine Domäne, die ausschließlich über Exchange Online versendet, sieht er so aus:

```
Name: contoso.de (bzw. @ oder leer, je nach DNS-Oberfläche)
Typ: TXT
Wert: v=spf1 include:spf.protection.outlook.com -all
```

Kommen weitere Quellen hinzu — ein Exchange Server aus dem Hybridbetrieb, ein Fachverfahren im eigenen Rechenzentrum —, ergänzt du sie vor dem abschließenden -all:

```
v=spf1 ip4:203.0.113.10 include:spf.protection.outlook.com -all
```

Zum Abschluss empfiehlt Microsoft ausdrücklich `-all`, den harten Fehlschlag, und nicht das weichere `~all`. Der Grund ist subtil: DMARC behandelt zwar beide als SPF-Fehlschlag, aber bei `~all` wird die DMARC-Policy praktisch wirkungslos, wenn die Nachricht zusätzlich keine DKIM-Signatur trägt. Wer `~all` stehen lässt, verschenkt einen Teil der Wirkung, die er sich gerade mühsam aufgebaut hat. Für Sonderwolken gelten andere Ziele: in GCC High und im DoD-Umfeld `spf.protection.office365.us`, bei 21Vianet `spf.protection.partner.outlook.cn`.

WARNUNG · Ein Eintrag pro Domäne. Genau einer.

Zwei TXT-Einträge, die beide mit `v=spf1` beginnen, ergeben keine Vereinigungsmenge, sondern einen `permerror`. Das empfangende System kann nicht entscheiden, welcher gilt, und bewertet die Prüfung als dauerhaft fehlerhaft. Das passiert typischerweise, wenn ein Dienstleister „mal eben“ seinen eigenen Eintrag hinzufügt, statt den bestehenden zu erweitern.

- › Vor jeder Änderung den bestehenden Eintrag abfragen und dokumentieren.
- › Jede Subdomäne, die versendet, braucht ihren eigenen SPF-Eintrag. `contoso.de` deckt `marketing.contoso.de` nicht ab.
- › Time to live nicht unter 3600 Sekunden setzen, sonst drohen Zeitüberschreitungen bei der Auflösung.

Schritt 2: DKIM in Exchange Online aktivieren

Für die anfängliche `onmicrosoft.com`-Domäne musst du nichts tun: Microsoft signiert ausgehende Nachrichten aus dieser Domäne automatisch. Für deine eigenen Domänen ist das nicht der Fall, und genau das ist der Punkt, an dem DMARC später scheitert — die Signatur ist da, sie trägt nur die falsche Domäne.

Der Weg im Portal führt über <https://security.microsoft.com> zu E-Mail und Zusammenarbeit, Richtlinien und Regeln, Bedrohungsrichtlinien, Einstellungen für die E-Mail-Authentifizierung, Registerkarte DKIM. Dort schaltest du die Domäne ein. Der erste Versuch schlägt absichtlich fehl und liefert dir die beiden CNAME-Werte, die du im DNS anlegen musst. Bequemer geht es in PowerShell:

```
Connect-ExchangeOnline

# Bestand sichten
Get-DkimSigningConfig | Format-List Name,Enabled,Status,Selector1CNAME,Selector2CNAME

# Konfiguration anlegen, aber noch nicht scharfschalten
New-DkimSigningConfig -DomainName contoso.de -Enabled $false -KeySize 2048

# CNAME-Werte abholen und im DNS anlegen
Get-DkimSigningConfig -Identity contoso.de | Format-List Selector1CNAME,Selector2CNAME

# Nachdem die CNAMEs auflösen: einschalten
Set-DkimSigningConfig -Identity contoso.de -Enabled $true
```

Zwei Schlüsselpaare werden erzeugt, aber nur eines ist aktiv. Das zweite wartet auf die nächste Rotation. Deshalb brauchst du zwei CNAME-Einträge, nicht einen. Der Aufbau folgt einem festen Muster; die exakten Werte holst du dir immer aus deinem eigenen Tenant, weil ein tenantspezifisches Zeichen darin vorkommt:

```
Name: selector1._domainkey.contoso.de
```

```

Typ: CNAME
Wert: selector1-contoso-de._domainkey.contoso.n-v1.dkim.mail.microsoft

Name: selector2._domainkey.contoso.de
Typ: CNAME
Wert: selector2-contoso-de._domainkey.contoso.n-v1.dkim.mail.microsoft

```

TIPP · Tippfehler sind hier die Regel, nicht die Ausnahme

Diese Werte bestehen aus Bindestrichen, Punkten und Unterstrichen in wechselnder Reihenfolge. Kopieren, nicht abtippen. Wenn Set-DkimSigningConfig mit einem Fehler abbricht, steht der erwartete Wert in der Fehlermeldung — vergleiche ihn zeichenweise mit dem, was tatsächlich im DNS steht.

- › Es kann einige Minuten dauern, bis Microsoft die neuen CNAME-Einträge sieht. Ungeduld hilft nicht.
- › Ältere Tenants nutzen noch das Format ohne Partitionszeichen, das auf onmicrosoft.com endet. Beide Formate können für denselben Selektor nicht nebeneinander bestehen.

Schritt 3: Der DMARC-Eintrag

DMARC ist wieder ein TXT-Eintrag, diesmal auf dem Unterknoten `_dmarc`. Für den Start gilt kompromisslos `p=none` — du willst zunächst nur zuhören:

```

Name: _dmarc.contoso.de
Typ: TXT
Wert: v=DMARC1; p=none; pct=100; rua=mailto:dmarc@contoso.de

```

Die rua-Adresse ist der eigentliche Wert dieser Phase. Dorthin schicken empfangende Systeme einmal täglich einen XML-Aggregatbericht: welche IP-Adressen unter deiner Domäne versendet haben, wie viele Nachrichten das waren, ob SPF und DKIM bestanden haben und ob sie ausgerichtet waren. Lege dafür ein geteiltes Postfach oder eine Microsoft-365-Gruppe an, niemals ein persönliches Postfach. Das Volumen ist beachtlich, und die Person geht irgendwann in Urlaub.

Ein zweiter Bericht, der ruf-Bericht, liefert Einzelfälle nahezu in Echtzeit. Microsoft 365 versendet solche Berichte grundsätzlich nicht, andere Anbieter unterstützen sie nur zurückhaltend, und sie können personenbezogene Inhalte enthalten. Fang ohne ruf an.

Zweck	Typ	Name	Wert	Anmerkung
SPF	TXT	contoso.de	v=spf1 include:spf.protection.outlook.com -all	Nur einmal pro Domäne. Weitere Quellen vor -all ergänzen.
DKIM 1	CNAME	selector1._domainkey	selector1-contoso-de._domainkey.<tenant>.<x>-v1.dkim.mail.microsoft	Exakten Wert per Get-DkimSigningConfig abholen.
DKIM 2	CNAME	selector2._domainkey	selector2-contoso-de._domainkey.<tenant>.<x>-v1.dkim.mail.microsoft	Reserve für die Rotation. Muss trotzdem existieren.
DMARC Start	TXT	_dmarc	v=DMARC1; p=none; pct=100; rua=mailto:dmarc@contoso.de	Beobachtungsphase. Ändert nichts an der

				Zustellung.
DMARC Ziel	TXT	_dmarc	v=DMARC1; p=reject; pct=100; rua=mailto:dmarc@contoso.de	Erst nach mehreren ruhigen Wochen Aggregatberichte.
Subdomäne	TXT	marketing.contoso.de	v=spf1 include:servers.dienstleister.de -all	Eigener SPF-Eintrag; DMARC erbt vom Hauptnamen.
Geparkte Domäne	TXT	contoso.net	v=spf1 -all	Domäne versendet nicht. Kein DKIM-Eintrag anlegen.
Geparkte Domäne	TXT	_dmarc.contoso.net	v=DMARC1; p=reject;	Gilt auch für die onmicrosoft.com-Domäne, wenn sie nicht versendet.

Tabelle 2: DNS-Einträge als Vorlage. Ersetze contoso.de durch deine Domäne und hole dir die DKIM-Werte aus dem eigenen Tenant.

FAKTEN · Geparkte Domänen sind kein Randthema

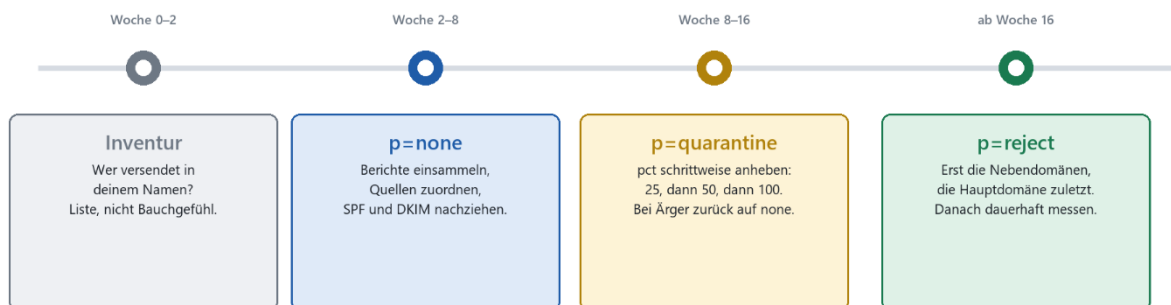
Jede Domäne, die du registriert hast und nicht für E-Mail nutzt, ist eine Einladung. Angreifer lieben die Schreibweisen-Variante, die die Marketingabteilung vor sechs Jahren vorsorglich gekauft hat. Für diese Domänen gilt: SPF auf v=spf1 -all, DMARC auf p=reject, und ausdrücklich keine DKIM-Einträge — denn ein fehlender öffentlicher Schlüssel im DNS macht jede gefälschte Signatur wertlos.

Von none über quarantine nach reject

Der Weg zur durchsetzungsfähigen Policy ist keine technische Aufgabe, sondern eine Ermittlungsarbeit. Du erhebst über Wochen, wer alles in deinem Namen Post verschickt, sortierst die legitimen Quellen ein und drehst erst dann an der Policy. Alles andere endet in einem Freitagnachmittag, an dem der Vertrieb anruft.

Von none nach reject, ohne Scherbenhaufen

Ein realistischer Fahrplan für eine mittelgroße Umgebung



Die eine Regel, die den Unterschied macht

Jede Stufe bleibt so lange stehen, bis die Aggregatberichte über mehrere Wochen keine unbekannten legitimen Quellen mehr zeigen.
Wer von none direkt auf reject springt, erfährt am Montagmorgen vom Vertrieb, welche Systeme er vergessen hat.

Die Wochenangaben sind Erfahrungswerte. Entscheidend ist nicht der Kalender, sondern der Bericht.

Skizze 3: Ein realistischer Fahrplan. Die Wochenangaben sind Erfahrungswerte — verbindlich ist nicht der Kalender, sondern das, was die Aggregatberichte zeigen.

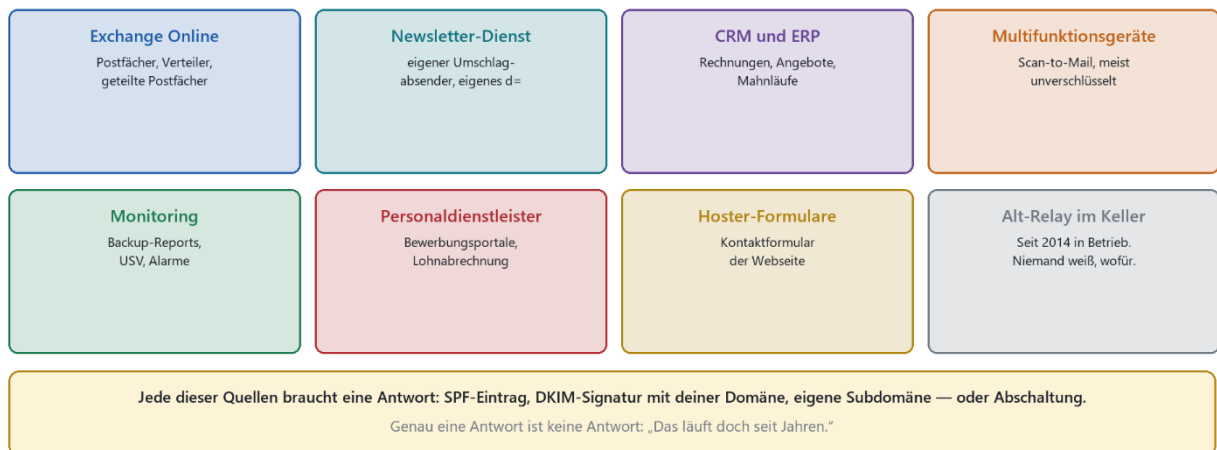
Phase 1: Zuhören mit $p=\text{none}$

In dieser Phase ändert sich für die Zustellung nichts. Genau das ist der Zweck. Du sammelst Aggregatberichte ein und beantwortest für jede auftauchende Quelle drei Fragen: Kenne ich sie? Ist sie legitim? Und falls ja, besteht sie SPF oder DKIM mit passender Domäne?

Die rohen XML-Berichte sind lesbar, aber unangenehm. Ab einer gewissen Größe lohnt sich ein Auswertungsdienst; Microsoft führt im MISA-Katalog unter microsoft.com/misapartnercatalog Anbieter, die sich in diesem Umfeld bewegen. Für kleinere Umgebungen genügt ein Skript, das die XML-Anhänge entpackt und in eine Tabelle schreibt. Wichtig ist nicht die Werkzeugklasse, sondern dass jemand die Berichte tatsächlich ansieht.

Wer verschickt eigentlich Post in deinem Namen?

Die Quellen, die in jeder zweiten Umgebung erst der DMARC-Bericht ans Licht bringt



Die Liste entsteht nicht am Whiteboard, sondern aus den Aggregatberichten der $p=\text{none}$ -Phase.

Skizze 4: Die Absenderinventur. Diese Liste entsteht nicht im Workshop, sondern aus den Aggregatberichten — und sie ist in aller Regel länger als erwartet.

Phase 2: Vorsichtig durchsetzen mit $p=\text{quarantine}$

Wenn die Berichte über mehrere Wochen keine unbekannten legitimen Quellen mehr zeigen, stellst du auf quarantine um. Der pct-Wert ist dabei dein Sicherheitsnetz: Mit pct=25 wendet ein empfangendes System die Policy nur auf ein Viertel der durchgefallenen Nachrichten an. Wenn nichts passiert, gehst du auf 50, dann auf 100. Was in der Quarantäne oder im Junk-Ordner landet, hängt vom Empfänger ab — du steuerst nur die Empfehlung.

Phase 3: Ernst machen mit $p=\text{reject}$

Am Ende steht $p=\text{reject}$ mit pct=100. Fang mit den Nebendomänen und Subdomänen an, die wenig Volumen haben, und nimm die Hauptdomäne zuletzt. Ein nützlicher Nebeneffekt: Subdomänen erben die DMARC-Einstellung des übergeordneten Namens automatisch, auch solche, die es gar nicht gibt. Wenn am Ende alle Subdomänen dieselbe Einstellung tragen wie der

Hauptname, kannst du ihre eigenen _dmarc-Einträge wieder entfernen und dich auf den übergeordneten verlassen.

Phase	DMARC-Wert	Typische Dauer	Weiter, wenn ...
Inventur	noch kein Eintrag	1–2 Wochen	Eine schriftliche Liste aller bekannten Versandwege existiert.
Beobachten	p=none; pct=100; rua=...	4–8 Wochen	Über zwei Wochen taucht keine unbekannte legitime Quelle mehr auf.
Anteilig	p=quarantine; pct=25	1–2 Wochen	Keine Beschwerden, keine legitimen Nachrichten im Junk-Ordner.
Ausweiten	p=quarantine; pct=100	3–6 Wochen	Die Berichte zeigen nur noch Fehlschläge, die du erklären kannst.
Durchsetzen	p=reject; pct=100	dauerhaft	Nebendomänen laufen sauber; Hauptdomäne zuletzt umstellen.

Tabelle 3: Phasenplan mit Abbruchkriterium. Die Stufe bleibt stehen, solange das Kriterium nicht erfüllt ist.

WARNUNG · Der Rückweg muss vorbereitet sein

Bevor du auf quarantine oder reject gehst, sollte die Rückstellung ein Vorgang von zwei Minuten sein: Wer darf den DNS-Eintrag ändern, wie lange ist die TTL, und wer entscheidet am Wochenende? Eine TTL von 24 Stunden auf dem _dmarc-Eintrag macht aus einem Fehler einen Arbeitstag Ausfall. Setze sie für die Umstellungsphase auf eine Stunde.

Eine Randnotiz mit Wirkung nach außen: Sobald deine eigene Domäne p=reject oder p=quarantine veröffentlicht, leitet Microsoft ausgehende Nachrichten aus deinem Tenant, die beim Empfänger an DMARC scheitern, über den Hochrisiko-Zustellpool. Dagegen gibt es keinen Schalter. Das ist ein weiteres Argument dafür, die Ausrichtung wirklich sauber hinzubekommen und nicht nur formal — und es passt zum Bild, das auch die [Tenant-Härtung: die 20 wichtigsten Schrauben](#) zeichnet: Die Einstellungen wirken selten isoliert.

Die Fallen, in die alle treten

Newsletter-Dienste und andere Fremdotsender

Das klassische Muster: Der Newsletter-Anbieter verschickt mit einem eigenen Umschlagabsender wie bounces@versand.anbieter.de und signiert mit d=anbieter.de. Beide Prüfungen bestehen — und DMARC fällt trotzdem durch, weil im From-Header deine Domäne steht und keine der beiden geprüften Domänen dazu passt. Im Authentication-Results-Header siehst du dann die verwirrende Kombination spf=pass, dkim=pass, dmarc=fail.

Es gibt genau zwei saubere Lösungen. Entweder der Dienst signiert mit deiner Domäne, dann brauchst du dort ein eigenes DKIM-Schlüsselpaar und einen weiteren CNAME oder TXT-Eintrag im DNS. Oder der Dienst lässt sich den Umschlagabsender auf eine Subdomäne von dir umbiegen, dann greift die SPF-Ausrichtung. Anbieter, die weder das eine noch das andere anbieten, haben in einer Umgebung mit p=reject nichts verloren.

Microsoft empfiehlt für alle Versanddienste, die nicht unter deiner direkten Kontrolle stehen, ohnehin eine eigene Subdomäne: `marketing.contoso.de` statt `contoso.de`. Das schützt die Reputation deines Hauptnamens und verschafft dir nebenbei ein eigenes Lookup-Budget.

Drucker, Scanner und Fachanwendungen

Das Multifunktionsgerät, das seit 2016 Scans per Mail verschickt, ist der Grund, warum viele DMARC-Projekte in Phase eins einschlafen. Diese Geräte kennen meist weder moderne Authentifizierung noch TLS in einer Version, die Exchange Online akzeptiert. Sie liefern über einen internen Relay ein, der dann unter deiner Domäne weiterversendet — oder sie versenden direkt, mit einer IP-Adresse, die in keinem SPF-Eintrag steht.

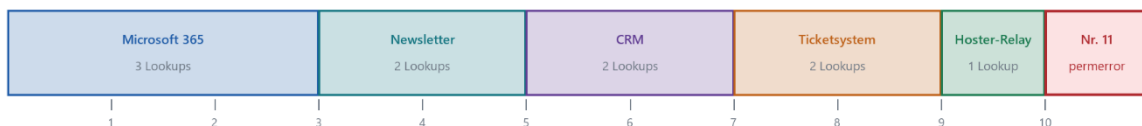
Für Exchange Online gibt es dafür drei Wege: authentifizierte SMTP-Übermittlung mit einem eigenen Postfach, ein Connector mit IP-Beschränkung, oder direkte Zustellung nur an interne Empfänger. Der erste Weg ist der beste, kollidiert aber gern mit der Abschaltung veralteter Anmeldeverfahren — siehe [Legacy Authentication endgültig abschalten](#). Plane beide Vorhaben gemeinsam, sonst reparierst du zweimal dieselbe Baustelle.

Das SPF-Lookup-Limit

SPF darf höchstens zehn DNS-Auflösungen verursachen. Wird diese Grenze überschritten, gibt es keinen halben Erfolg: Der gesamte Eintrag fällt auf `permerror`, und für DMARC ist das ein Fehlschlag. Das Tückische daran ist, dass du die Grenze nicht durch Zählen der Zeilen erkennst. Jedes `include` verweist auf einen fremden Eintrag, der seinerseits weitere `includes` enthalten kann. Ein einziger Anbieter, der seine Infrastruktur umbaut, kann deinen Eintrag über Nacht kippen.

Das Lookup-Budget: zehn und keins mehr

Warum ein gepflegter SPF-Eintrag irgendwann von selbst kaputtgeht



Alles ab dem elften Lookup wird nicht etwa ignoriert — der gesamte SPF-Eintrag fällt auf `permerror`. Für DMARC ist das ein glattes Fail.

zählt mit

```
include:
  a
  mx
exists
redirect=
```

zählt nicht mit

```
ip4:
ip6:
all
(auch als CIDR-Bereich)
```

Drei Auswege, in dieser Reihenfolge

1. Fremddienste auf eine eigene Subdomäne umziehen — jede Subdomäne hat ihr eigenes Budget von zehn.
2. Anbieter mit stabilen, dokumentierten IP-Bereichen als `ip4:` eintragen statt als `include:`.
3. Dienste konsolidieren. Drei Newsletter-Werkzeuge braucht kein Mensch.

Die Zahlen im Balken sind ein typisches Beispiel. Verschachtelte `include`-Einträge kosten mehr, als die Zeile vermuten lässt — nachmessen statt schätzen.

Skizze 5: Das Lookup-Budget. Ab dem elften Nachschlagen fällt nicht nur der letzte Eintrag durch, sondern die gesamte SPF-Prüfung.

Element	Zählt	Bemerkung
---------	-------	-----------

include:	ja	Mindestens eine Auflösung, oft mehr durch Verschachtelung
a	ja	Auch in der Form a:name.example
mx	ja	Teuer, weil jeder MX-Eintrag weiterverfolgt wird
exists	ja	Selten genutzt, aber genauso teuer
redirect=	ja	Verweist auf einen komplett anderen Eintrag
ip4: und ip6:	nein	Auch als CIDR-Bereich kostenlos
all	nein	Die Abschlussregel selbst zählt nicht

Tabelle 4: Was auf das Limit von zehn Auflösungen zählt.

TIPP · Flatten ja, aber nicht bei Microsoft

SPF-Flattening ersetzt include-Einträge durch die dahinter liegenden IP-Adressen und spart Auflösungen. Das ist für Anbieter mit stabilen, dokumentierten Adressbereichen vertretbar — dokumentiere, was du wann ersetzt hast, und prüfe es mindestens vierteljährlich nach. Bei include:spf.protection.outlook.com verbietet sich das: Die Versandinfrastruktur von Microsoft 365 wechselt ihre Adressen zu häufig.

Weiterleitungen, Verteilerlisten und ARC

Eine automatisch weitergeleitete Nachricht verliert ihre SPF-Ausrichtung zwangsläufig, weil der weiterleitende Server nun die neue Quelle ist. DKIM überlebt, solange niemand die Nachricht verändert — was Verteilerlisten mit ihrer Vorliebe für Fußzeilen und Betreffpräfixe zuverlässig zunichtemachen.

Für den eingehenden Fall bietet Microsoft 365 dafür Authenticated Received Chain an. Wenn ein Sicherheit Gateway oder ein Archivdienst vor deinem Tenant sitzt und Nachrichten verändert, trägst du dessen Signaturdomäne als vertrauenswürdigen ARC-Siegler ein. Wichtig: Es ist die Domäne des Anbieters aus dem d=Feld des ARC-Seal-Headers, nicht deine eigene.

```
Get-ArcConfig
```

```
# Achtung: der Parameter ersetzt die bestehende Liste vollstaendig
Set-ArcConfig -Identity Default -ArcTrustedSealers "gateway-anbieter.de", "archiv-anbieter.de"
```

Ob es gewirkt hat, siehst du im Header: arc=pass zusammen mit oda=1 im ARC-Authentication-Results, und compauth=pass reason=130 im Authentication-Results. Der Wert 130 ist die Bestätigung, dass das ARC-Ergebnis einen DMARC-Fehlschlag überstimmt hat. ARC hebt allerdings nur Authentifizierungsfehler auf, keine Spam-Bewertung — wenn die Nachricht wegen ihres Inhalts im Junk-Ordner landet, hilft es nicht.

WICHTIG · Gateway davor? Dann fehlen dir die Berichte

Microsoft 365 versendet DMARC-Aggregatberichte nur für Domänen, deren MX-Eintrag direkt auf Microsoft 365 zeigt. Steht ein fremdes Gateway oder eine lokale Umgebung davor, bekommen die Absender von dir keine Berichte. Für die eingehende Bewertung solltest du in diesem Fall die erweiterte Filterung für Connectors aktivieren, damit Exchange Online die ursprüngliche Quelle statt der IP-Adresse des Gateways bewertet.

Die eigene onmicrosoft.com-Domäne

Sie wird gern übersehen, weil sie „ja nur intern“ ist. Wenn du sie nicht für den Versand nutzt, gehört auch auf sie ein _dmarc-Eintrag mit p=reject. Nutzt du sie doch, brauchst du einen eigenen — angelegt wird er über das Microsoft 365 Admin Center unter Domänen, weil du die DNS-Zone selbst nicht bearbeiten kannst. Der SPF-Eintrag dieser Domäne liegt bei Microsoft und ist unveränderlich.

Prüfwerkzeuge und der laufende Betrieb

Den Nachrichtenkopf lesen

Das wichtigste Werkzeug kostet nichts und liegt in jeder Mail. Der Authentication-Results-Header fasst alle drei Prüfungen zusammen. Ein typischer Problemfall sieht so aus:

```
Authentication-Results: spf=pass (sender IP is 198.51.100.10)
smtp.mailfrom=bounces.anbieter.de; dkim=pass (signature was verified)
header.d=anbieter.de; dmarc=fail action=oreject
header.from=contoso.de; compauth=fail reason=100
```

Der Leseweg ist immer derselbe: header.from ist der sichtbare Absender. Passt smtp.mailfrom dazu? Passt header.d dazu? Wenn beides nein lautet, ist die Ausrichtung das Problem und nicht die Authentifizierung. In Outlook findest du den Kopf über Datei, Eigenschaften, Internetkopffzeilen; Microsoft stellt für die Auswertung zusätzlich einen Message Header Analyzer bereit.

Wert	Bedeutung	Was du tust
dmarc=fail action=none	Absender hat p=none veröffentlicht	Nichts erzwungen; der übrige Filterstapel entscheidet
dmarc=fail action=quarantine	Absender hat p=quarantine	Nachricht im Junk-Ordner oder in der Quarantäne
dmarc=fail action=oreject	Absender hat p=reject, Abweisung im SMTP-Dialog	Absender erhält 550 5.7.509
dmarc=bestguesspass	Kein DMARC-Eintrag der Absenderdomäne	Microsoft rät wohlwollend; die Gegenseite sollte nachbessern
dmarc=permerror	Syntaxfehler oder mehrere _dmarc-Einträge	Eintrag prüfen; nur ein _dmarc-TXT-Eintrag ist erlaubt
compauth=fail reason=100	DMARC ist ausdrücklich fehlgeschlagen	Ausrichtung an der Quelle reparieren
compauth=pass reason=130	Ein vertrauenswürdiger ARC-Siegler hat übersteuert	Erwünscht, wenn ein Gateway davorsteht

Tabelle 5: Header-Werte und was sie dir sagen.

Abfragen aus der PowerShell

Für die tägliche Arbeit reichen ein paar Zeilen. Die DNS-Auflösungen prüfst du direkt auf dem Arbeitsplatz, die Tenant-Einstellungen in Exchange Online PowerShell:

```
# Was steht wirklich im DNS?
Resolve-DnsName -Name contoso.de -Type TXT | Select-Object -ExpandProperty Strings
Resolve-DnsName -Name _dmarc.contoso.de -Type TXT | Select-Object -ExpandProperty Strings
Resolve-DnsName -Name selector1._domainkey.contoso.de -Type CNAME
```

```
# DKIM-Status und Rotationsdaten aller Domänen
Get-DkimSigningConfig | Format-List Name,Enabled,Status,Selector1KeySize,
    KeyCreationTime,RotateOnDate,SelectorBeforeRotateOnDate,SelectorAfterRotateOnDate

# Wie geht der Tenant mit fremden DMARC-Policies um?
Get-AntiPhishPolicy | Format-List Name,HonorDmarcPolicy,DmarcQuarantineAction,DmarcRejectAction
```

Schlüsselrotation nicht vergessen

DKIM-Schlüssel gehören turnusmäßig gewechselt, aus denselben Gründen wie Kennwörter. Für eigene Domänen erledigt das ein Aufruf, für die onmicrosoft.com-Domäne gibt es derzeit keine automatische Rotation. Wichtig ist der Zeitverzug: Nach dem Anstoßen dauert es vier Tage beziehungsweise 96 Stunden, bis der neue private Schlüssel tatsächlich signiert. Bis dahin gilt der alte, und eine zweite Rotation ist in dieser Zeit nicht möglich.

```
# Rotation anstoßen, dabei gleich auf 2048 Bit gehen
Rotate-DkimSigningConfig -Identity contoso.de -KeySize 2048
```

Ein Detail, über das viele stolpern: Wenn du dabei die Schlüssellänge von 1024 auf 2048 Bit anhebst, betrifft das zunächst nur den Selektor, der als Nächstes aktiv wird. Erst bei der zweiten Rotation zieht auch der andere nach. Wer wirklich überall 2048 Bit haben will, muss zweimal rotieren — mit dem entsprechenden Abstand dazwischen.

Die eingehende Seite

Bisher ging es um Nachrichten, die dein Haus verlassen. Die Gegenrichtung steuerst du in den Antiphishing-Richtlinien: Die Einstellung, die die DMARC-Policy des Absenders berücksichtigt, entscheidet, ob Exchange Online ein fremdes p=reject tatsächlich durchsetzt. Sie gehört eingeschaltet, und die zugehörigen Aktionen gehören bewusst gewählt. Das ist derselbe Regelsatz, in dem auch der Identitätsschutz und die Nachahmungserkennung sitzen — mehr dazu in [Defender for Office 365: Safe Links und Safe Attachments](#).

Und weil kein Mechanismus vollständig ist: Auch mit einwandfreiem DMARC kommen Nachrichten durch, die von einer echten, korrekt authentifizierten Domäne stammen — der eines kompromittierten Lieferanten zum Beispiel. Dafür brauchst du weiterhin geschulte Menschen und einen geübten Ablauf, siehe [Phishing-Vorfall: die ersten 60 Minuten](#) und [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#).

TIPP • Zwei Kennzahlen fürs Berichtswesen

Wenn die Geschäftsführung wissen will, ob sich der Aufwand gelohnt hat, taugen zwei Zahlen aus den Aggregatberichten: der Anteil des eigenen Mailvolumens, der DMARC besteht (Ziel: über 99 Prozent), und die Zahl der Nachrichten, die unter deiner Domäne von fremden Systemen verschickt und abgewiesen wurden. Die zweite Zahl ist das Argument, das hängen bleibt.

Häufige Fragen

Reicht nicht einfach p=reject von Anfang an?

Technisch ja, betrieblich nein. Du weißt vor der Beobachtungsphase schlicht nicht, welche Systeme in deinem Namen versenden. Die einzige Ausnahme sind Domänen, die nachweislich gar keine Post verschicken: geparkte Domänen und Schreibvarianten. Dort ist p=reject vom ersten Tag an richtig.

Was passiert, wenn ich gar nichts tue?

Kurzfristig nichts Sichtbares. Mittelfristig sinkt deine Zustellrate bei den großen Freemail-Anbietern, weil deren Anforderungen seit 2024 und 2025 gelten. Und im Ernstfall hast du keine Handhabe gegen jemanden, der unter deinem Namen Rechnungen mit geänderter Bankverbindung verschickt.

Wir haben mehrere Domänen. Muss ich das alles einzeln machen?

SPF und DKIM ja, jede Domäne und jede versendende Subdomäne braucht eigene Einträge. Bei DMARC nicht: Subdomänen erben den Eintrag der übergeordneten Domäne, auch nicht existierende. Du kannst die Vererbung mit einem eigenen _dmarc-Eintrag auf der Subdomäne unterbrechen, wenn du dort vorübergehend eine mildere Policy brauchst.

Mein Newsletter-Anbieter sagt, SPF genüge. Stimmt das?

Für die reine Zustellung vielleicht, für DMARC nicht. Frag konkret nach zwei Dingen: Kann der Dienst mit deiner Domäne DKIM-signieren, also mit d=deinedomaene.de? Und lässt sich der Umschlagabsender auf eine Subdomäne von dir setzen? Kommt zweimal nein, ist der Dienst für eine Umgebung mit p=reject ungeeignet.

Warum steht in meinem Header dkim=none, obwohl DKIM aktiv ist?

Drei häufige Ursachen: Die CNAME-Einträge lösen nicht auf, die Signierung wurde für die Domäne nie mit Set-DkimSigningConfig eingeschaltet, oder die Nachricht stammt gar nicht aus Exchange Online, sondern von einem Fremdsystem, das unter deiner Domäne versendet. Get-DkimSigningConfig beantwortet die ersten beiden Fragen in zehn Sekunden.

Wie lange dauert die Einführung realistisch?

Die technische Einrichtung von SPF, DKIM und einem p=none-DMARC-Eintrag ist an einem Vormittag erledigt. Der Weg bis p=reject dauert in einer mittelständischen Umgebung typischerweise drei bis sechs Monate — und die Zeit geht fast vollständig für die Klärung der Fremdotsender drauf, nicht für DNS-Einträge.

Brauche ich einen kostenpflichtigen DMARC-Auswertungsdienst?

Bei wenigen Domänen und überschaubarem Volumen nicht zwingend; ein Skript, das die XML-Anhänge auswertet, reicht. Ab etwa einem Dutzend Domänen oder wenn mehrere Personen mitlesen sollen, rechnet sich ein Dienst schnell. Microsoft listet Anbieter im MISA-Katalog.

Was ist mit interner Post zwischen unseren eigenen Postfächern?

Die läuft innerhalb von Exchange Online und wird von diesen Prüfungen nicht abgewiesen. Das ist gleichzeitig eine Warnung: Ein kompromittiertes internes Postfach umgeht die gesamte Absenderprüfung, weil es der legitime Absender ist. Dagegen hilft kein DNS-Eintrag, sondern Erkennung und ein geübter Ablauf.

Fazit

SPF, DKIM und DMARC sind zusammen die günstigste Sicherheitsmaßnahme, die du in Microsoft 365 umsetzen kannst. Es fällt keine Lizenz an, es ist keine Software zu betreiben, und der technische Aufwand liegt bei wenigen Stunden. Bezahlt wird in einer anderen Währung: in Sorgfalt und in der Bereitschaft, über Wochen Berichte zu lesen, statt einmal einen Schalter umzulegen.

Die drei Regeln, die den Unterschied machen, sind unspektakulär. Erstens: Fang bei p=none an und lass die Stufe stehen, bis die Berichte ruhig sind. Zweitens: Kläre jede Fremdquelle einzeln — DKIM mit deiner Domäne oder eigene Subdomäne, ein drittes Modell gibt es nicht. Drittens: Behandle geparkte Domänen mit derselben Ernsthaftigkeit wie die Hauptdomäne, denn Angreifer tun das auch.

Wer das einmal sauber aufgesetzt hat, hat nebenbei etwas Wertvolleres gewonnen als drei DNS-Einträge: eine belastbare Liste aller Systeme, die im Namen des Hauses nach außen kommunizieren. Diese Liste ist die Grundlage für so ziemlich jede weitere Sicherheitsmaßnahme — und für die Nachweise, die etwa [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) von dir verlangt. Wenn du dabei Unterstützung brauchst, ist die [Microsoft-365-Security-Beratung](#) der passende Einstieg; für Teams, die es selbst in die Hand nehmen wollen, gibt es die [Schulung Microsoft 365 Security](#).

Weiterlesen in dieser Serie

- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — der Rahmen, in den diese Einträge gehören
- › [Defender for Office 365: Safe Links und Safe Attachments](#) — die Filterschicht hinter der Absenderprüfung
- › [Legacy Authentication endgültig abschalten](#) — betrifft dieselben Geräte und Fachverfahren
- › [Phishing-Vorfall: die ersten 60 Minuten](#) — wenn doch etwas durchkommt
- › [Secure Score: sinnvoll nutzen statt Punktejagd](#) — wo diese Maßnahmen einzahlen
- › [Security-Reporting für die Geschäftsführung](#) — die zwei Kennzahlen aus den Aggregatberichten
- › [Alert Policies und Benachrichtigungen richtig aufsetzen](#) — damit die Berichte nicht unbemerkt versanden