Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: IT FÜR UNTERNEHMEN

Upgrade für die E-Mail-Sicherheit

Handlungsempfehlungen für moderne E-Mail-Infrastrukturen in Unternehmen

Eine digitale Außenkommunikation für Unternehmen ist kaum ohne das Medium „E-Mail“ vorstellbar. Die zu Grunde liegende Technik stammt aus den 80er-Jahren und bietet in ihrer Grundform große Angriffsflächen. Mit der fortschreitenden Digitalisierung und der damit verbundenen Innovationskraft, haben sich starke Sicherheitsstandards rund um die E-Mail etabliert, die den wachsenden Bedrohungen etwas entgegensetzen.

Durch die Nutzung dieser Standards sollen verschiedene Sicherheitsaspekte erreicht werden:

- Empfangende von E-Mails sollen sich darauf verlassen können, dass eine E-Mail tatsächlich von dem Absender stammt, der als Absender im E-Mail-Programm angezeigt wird. Die Manipulation dieser Absenderdaten („Spoofing“) ist eine leider häufig erfolgreich genutzte Angriffsmethode.
- Absendende und Empfangende einer E-Mail sollen sich sicher sein können, dass der Inhalt der E-Mail auf dem Weg vom Absendenden zum Empfangenden nicht verändert wurde.
- Absendende und Empfangende einer E-Mail sollen darauf vertrauen können, dass der Inhalt der E-Mail auf dem Weg durch das Internet nicht von Dritten mitgelesen wurde.

Dieses Dokument richtet sich vor allem an Unternehmen, die Ihren E-Mail-Dienst nicht oder nur teilweise selbst betreiben. Die hier genannten Empfehlungen sind das Ergebnis der fortlaufenden Beobachtung der in der Praxis verfügbaren Sicherheitsstandards im Bereich „E-Mail“ sowie den Erfahrungen aus dem Monitoring der Verbreitung und der Praxisrelevanz eben dieser Standards.

Falls in Ihrem Unternehmen kein eigenes Personal für die IT-Administration beschäftigt ist, bitten Sie Ihren IT-Dienstleister um die Umsetzung der im Folgenden genannten Maßnahmen.

Motivation

Für die Authentifizierung von E-Mail-Servern haben sich weltweit die Standards SPF, DKIM und DMARC durchgesetzt. Die Umsetzung dieser Standards stärkt den Schutz vor Angriffen, bei denen die Identität vertrauenswürdiger Sender-Domains vorgegaukelt wird (z. B. Spoofing und Phishing). Die Standards sind in der Praxis bereits verbreitet, jedoch werden bei der Umsetzung oft leicht zu korrigierende Fehler gemacht.

DANE mit DNSSEC und MTA-STS heben die E-Mail-Sicherheit durch die Absicherung des Transports auf ein höheres Niveau. Mit Hilfe von DNS-Einträgen wird allen Kommunikationspartnern signalisiert, dass eine Verschlüsselung des Transports aller E-Mails angeboten und erwartet wird. Damit können sich Unternehmen effektiv und effizient vor dem unberechtigten Mitlesen und der Manipulation ihrer E-Mails (sog. Person-in-the-Middle Angriffe) schützen. Erfreulicherweise sind entsprechende Implementierungen bereits an vielen Stellen verfügbar und nutzbar. So bieten Microsoft 365 (mit Exchange Online) und Google Workspace (mit Gmail) die Möglichkeit mit wenigen Konfigurationsschritten von diesen Sicherheitsstandards zu profitieren. Einzelne Anbieter, wie mailbox.org, implementieren diese Standards sogar ohne weiteres Zutun ihrer Kundschaft.

Empfehlung 1: Vermeidung häufiger Fehler bei SPF, DKIM und DMARC

Viele E-Mail-Dienste setzen bereits SPF, DKIM und DMARC zur Authentifizierung ihrer E-Mails um. Die Standards helfen dabei, die Identität eines sendenden E-Mail-Servers und die von ihm versendeten E-Mails an eine Internet-Domain zu binden. Da die empfangenden E-Mail-Server bei der Interpretation der Standards in der Regel fehlertolerant sind, bleiben einfach zu korrigierende Fehler oft unentdeckt. Dass solche Fehlertoleranzen den praktischen Nutzen von Sicherheitsstandards schwächen können, wurde z. B. im Jahr 2024 durch die Veröffentlichungen zum sogenannten SMTP Smuggling[1] deutlich.

Im Folgenden werden häufige Konfigurationsfehler bei der Umsetzung von SPF, DKIM und DMARC beschrieben, sowie Beispiele und Tipps gegeben, wie diese Fehler vermieden bzw. korrigiert werden können.

Tippfehler:

Eine häufige Ursache für fehlerhafte DNS-Einträge sind Tippfehler. Davon können sowohl die Werte im DNS betroffen sein (z. B. Leerzeichen in IP-Adressen) als auch die dazugehörigen Tags (z. B. „inlcude“ anstelle von „include“). Durch solche Tippfehler können einzelne Angaben im Eintrag oder der gesamte Eintrag ungültig werden. Ob diese Fehler ignoriert oder vielleicht sogar mit einem negativen Ergebnis quittiert werden hängt von der Fehlertoleranz des Empfangssystems ab.

Problematisch	**Korrekt**
v=spf1 inlcude:example.com ip4:96.7.128. 175	v=spf1 include:example.com ip4:96.7.128.175

DNS-Einträge in Anführungszeichen:

Jede der drei Technologien SPF, DKIM und DMARC erfordert das Anlegen eines entsprechenden DNS-Eintrags. Da diese von DNS-Tools (z. B. von „dig“) häufig in Anführungszeichen ausgegeben werden, um den Start und das Ende der Zeichenkette eindeutig zu markieren, ist eine häufige Fehlannahme, dass diese Einträge mit Anführungszeichen im DNS angelegt werden müssen. Tatsächlich fordern alle drei Standards, dass die DNS-Einträge unmittelbar mit dem Identifizierungsmerkmal des jeweiligen Standards beginnen, also v=spf1, v=DKIM1 und v=DMARC1.

Problematisch	**Korrekt**
"v=DMARC1;p=quarantine"	v=DMARC1;p=quarantine

[1] Quelle: https://smtpsmuggling.com/

Mehrfacheinträge:

Sowohl SPF, DKIM als auch DMARC dürfen jeweils nur mit einem einzigen Eintrag im DNS einer Domain auftauchen. Nicht selten werden zusätzliche SPF-Einträge eingepflegt, da dies für die Zusammenarbeit mit externen Dienstleistern notwendig erscheint und z. B. in den dort hinterlegten Anleitungen suggeriert wird. Die korrekte Vorgehensweise ist es in einem solchen Fall jedoch nicht mehrere Einträge zu führen, sondern die notwendigen Angaben in einem Eintrag zusammen zu führen. Existieren für eine der Technologien mehrere Einträge, ist nicht sichergestellt, dass alle Einträge beim Empfangssystem berücksichtigt werden.

Problematisch	Korrekt
v=spf1 ip4:96.7.128.175 v=spf1 ip4:96.7.128.198	v=spf1 ip4:96.7.128.175 ip4:96.7.128.198

Ungültige Versions-Bezeichnungen:

Die Versionierung der zu Grunde liegenden Standards findet, wie weiter oben bereits angedeutet, durch einen eindeutigen Wert zur Identifizierung (v=spf1, v=DKIM1 und v=DMARC1) statt. Anders lautende Angaben in dem Version-Tag, wie z. B. v=DKIMv1 und DKIMv=1, sind nicht von den Standards abgedeckt und werden im Zweifelsfall nicht vom Empfangssystem berücksichtigt oder sogar falsch interpretiert.

Problematisch	Korrekt
v=spfv1 ip4:96.7.128.175	v=spf1 ip4:96.7.128.175

Verwaiste DNS-Einträge:

Im Laufe der Zeit können sich bei komplexen E-Mail-Infrastrukturen die DNS-Einträge beteiligter Systeme (z. B. E-Mail-Server denen mittels SPF eine Sendeberechtigung erteilt wurde) anhäufen. Um Fehler und Sicherheitsrisiken zu vermeiden, sollten nicht mehr benötigte Einträge umgehend entfernt werden oder zumindest einer regelmäßigen Überprüfung unterzogen werden.

Fehlerhafte Syntax:

Anforderungen an die Syntax der Standards werden oft unbewusst missachtet. Ein Beispiel hierfür ist die fehlende Trennung der verschiedenen Tags durch Semikolons bei DKIM und DMARC. Auch das Vermischen von Einträgen, etwa bei SPF- und DMARC-Einträgen, kann eine Fehlerursache sein. Alle Einträge sollten daraufhin überprüft werden, ob sie die Anforderungen des jeweiligen Standards erfüllen.

Empfehlung 2: Nutzung von DANE und DNSSEC (am Beispiel Microsoft Exchange Online)

Microsoft setzt mit seiner Exchange Online Plattform den vom BSI empfohlenen Standard DANE mit DNSSEC um. Der Standard DANE basiert vereinfacht zusammengefasst darauf, dass ein Fingerabdruck des für die TLS-Verschlüsselung verwendeten Schlüsselmaterials geschützt durch DNSSEC in einem DNS-Eintrag des empfangenden E-Mail-Servers hinterlegt wird. Hierdurch signalisiert der Mail-Server, dass er nur verschlüsselte Verbindungen akzeptiert und ist somit vor Downgrade-Angriffen geschützt. Darüber hinaus wird das Schlüsselmaterial beim Aufbau der TLS-Verbindung verglichen, was die Verbindung gegen Person-in-the-Middle-Angriffe absichert. Zum Zeitpunkt der Erstellung dieser Empfehlung betreibt Microsoft zwei parallele Infrastrukturen für die Nutzenden von Exchange Online. Nur die modernere der beiden Infrastrukturen unterstützt DANE mit DNSSEC.

Warum DANE mit DNSSEC? DANE nutzt DNSSEC als Sicherheitsanker. Die Kombination von DANE und DNSSEC ist somit, eine entsprechende Validierung durch den Client vorausgesetzt, vor Angriffen mittels DNS Cache Poisoning, z.B. in einem öffentlichen WLAN, geschützt.

Microsoft stellt einen Leitfaden[2] zur Verfügung, der die Migration einer Unternehmens-Domain von der klassischen auf die moderne DANE-Infrastruktur erläutert. Dabei bedarf es für Bestandskunden grundsätzlich nur weniger Handgriffe, die im Folgenden skizziert werden. Eine wichtige Voraussetzung für die erfolgreiche Umsetzung ist jedoch, dass die Unternehmens-Domain mit DNSSEC abgesichert ist. Leider bieten noch nicht alle Domain-Registrierungsstellen DNSSEC für ihre Kunden an. Daher sollte vorab geprüft werden, ob diese Sicherheitsfunktion bei der DNS-Registrierungsstelle oder bei dem Web-Hoster aktiviert oder zumindest erworben werden kann.

Wichtig: Die E-Mail-Konfiguration eines Unternehmens kann beliebig komplex ausgestaltet sein. Wir empfehlen daher ein Vorgehen nach dem oben genannten Leitfaden oder bei Bedarf die Einbeziehung eines Dienstleisters, um Ausfälle im E-Mail-Dienst zu vermeiden.

Anpassung der DNS-Einträge

In einem ersten Schritt muss ein neuer MX-Record für die Unternehmens-Domain erstellt werden. Dazu ist es notwendig, mit der PowerShell[3] eine Verbindung zu Exchange Online herzustellen. Nach erfolgreicher Verbindung muss dann das folgende Kommando ausgeführt werden, wobei „example.com“ durch die tatsächliche Unternehmens-Domain ersetzt werden muss:

```
Enable-DnssecForVerifiedDomain -DomainName example.com
```

Das Kommando liefert nach einer kurzen Zeit den Namen des neuen MX-Records zurück, z. B. „example-com.o-v1.mx.microsoft“. Während die bisherigen MX-Records mit dem Suffix „*.mail.protection.outlook.com“ enden, so endet der moderne DANE-Endpunkt mit dem Suffix „*.mx.microsoft“, also mit der Top-Level-Domain von Microsoft.

Der neue MX-Record muss nun bei der Registrierungsstelle, die die Domäne hostet, temporär zum bestehenden MX-Record hinzugefügt werden. Im Anschluss sollte mit dem Inbound-SMTP-Test[4] des Remote Connectivity Analyzer überprüft werden, ob sowohl der bestehende als auch der neue MX (Mail Exchanger) erreichbar und somit funktionsfähig ist. Wenn der Test hier keine Fehler berichtet, kann der alte (auf „*.outlook.com“-endende) MX-Record bei der Registrierungsstelle gelöscht werden. Um Unterbrechungen des E-Mail-Dienstes zu verhindern, sollte vor dem Löschen die im DNS konfigurierte Gültigkeitsdauer berücksichtigt werden. Abschließend sollte mit dem DANE-Validation-Test[5] (Option: „DNSSEC-Prüfung“) des Remote Connectivity Analyzer überprüft werden, ob die Unternehmens-Domain inkl. des neuen MX-Records mit DNSSEC abgesichert ist. Falls der Test hier Fehler berichtet, sollte die Registrierungsstelle kontaktiert und ggf. die DNSSEC-Konfiguration überprüft werden.

Aktivierung von DANE

DANE für ausgehende E-Mails wurde bereits vor einigen Jahren von Microsoft umgesetzt, wobei dafür kein individueller Eingriff des Kunden notwendig war. Anders sieht es bei der Aktivierung von DANE für eingehende E-Mails aus. Dazu ist es notwendig, ebenfalls mit der PowerShell[6] eine Verbindung zu Exchange Online herzustellen. Nach erfolgreicher Verbindung muss dann das folgende Kommando ausgeführt werden, wobei „example.com“ durch die tatsächliche Unternehmens-Domain ersetzt wird:

```
Enable-SmtpDaneInbound -DomainName example.com
```

---

[2] Quelle: https://learn.microsoft.com/de-de/purview/how-smtp-dane-works
[3] Quelle: https://learn.microsoft.com/de-de/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps
[4] Quelle: https://testconnectivity.microsoft.com/tests/O365InboundSmtp/input
[5] Quelle: https://testconnectivity.microsoft.com/tests/O365DaneValidation/input
[6] Quelle: https://learn.microsoft.com/de-de/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps

Das Kommando erstellt (im Hintergrund und nach einer kurzen Zeit) sogenannte TLSA-Einträge für den neuen MX-Record. Nach einer Wartezeit von ca. 30 Minuten sollte im Anschluss mit dem DANE-Validation-Test[7] (Option: "DANE-Prüfung") des Remote Connectivity Analyzer überprüft werden, ob die Unternehmens-Domain ab sofort eingehende und mit DANE-abgesicherte E-Mails akzeptiert. Wenn der Test hier keine Fehler berichtet, ist die Unternehmens-Domain mit DNSSEC und der E-Mail-Dienst mit DANE erfolgreich abgesichert.

Exkurs: DNSSEC beim Domain-Registrar oder Web-Hoster aktivieren

Die Aktivierung von DNSSEC schützt eine Domain vor der Manipulation der im DNS hinterlegten Einträge.

Dies ist ein wirksamer Schutz vor sogenannten Spoofing-Angriffen, bei denen DNS-Abfragen (z. B. mit Hilfe von DNS Cache Poisoning) auf einen anderen Server umgeleitet werden können, und es stärkt generell all diejenigen Technologien, die das DNS nutzen. Für die Nutzung von DANE ist DNSSEC eine zwingende Voraussetzung, da es den notwendigen Sicherheitsanker bietet. Für einen durchgängigen Schutz muss DNSSEC auf der Internet-Domain die für den E-Mail-Versand genutzt wird aktiviert sein. Die Aktivierung von DNSSEC geschieht zumeist bei dem für die Domain beauftragten Registrar oder ist Bestandteil eines Paket-Angebotes bei einem Web-Hoster.

Um ein durchgängiges Sicherheitsniveau zu implementieren genügt es nicht, wenn die für den E-Mail-Empfang und -Versand eingekaufte Infrastruktur eines Anbieters DNSSEC unterstützt. Auch die eigenen DNS-Einträge der Domain müssen mittels DNSSEC geschützt sein. Bisher ist die Anzahl an Registraren und Web-Hostern, die DNSSEC unterstützen, noch überschaubar – z. B. United Internet (mit IONOS und United-Domains), netcup oder INWX unterstützten dies. Falls der Registrar noch kein DNSSEC unterstützt, kann ein separater Dienstleister für das DNS-Management genutzt werden.

Empfehlung 3: Nutzung von MTA-STS (am Beispiel Google Workspace mit Gmail)

Auf der Plattform Workspace mit Gmail von Google wird der Standard MTA-STS umgesetzt. Dieser beruht vereinfacht dargestellt darauf, dass in einem DNS-Eintrag des E-Mail-Servers auf eine via HTTPS abrufbare Policy verwiesen wird. Hauptbestandteile der Policy sind der Betriebsmodus, welcher festlegt, wie die Policy anzuwenden ist, und eine Liste der zum Empfang befugten E-Mail-Server (sog. MX-Server). Die Verifikation der Identität der MX-Server findet ausschließlich über die dabei eingesetzten Zertifikate statt. Die Zertifikate und die angewandte Policy schützen die anschließend aufgebaute TLS-Verschlüsselung vor Downgrade- und Person-in-the-Middle-Angriffen. Auch von Google (siehe DANE und DNSSEC am Beispiel Microsoft Exchange Online) werden zwei parallele Infrastrukturen im E-Mail-Bereich betrieben. Beide Infrastrukturen nutzen MTA-STS, jedoch zeichnet sich die modernere der beiden Infrastrukturen durch aktuellere Vorgaben beim Aufbau der verschlüsselten Verbindung aus.

Warum MTA-STS? Anders als DANE nutzt MTA-STS digitale Zertifikate als Sicherheitsanker und benötigt dementsprechend kein DNSSEC. Zertifikate unbekannter Herkunft werden häufig nach dem TOFU-Prinzip (Trust On First Use) akzeptiert. Gelingt es einem Angreifenden in den ersten Verbindungsaufbau einzugreifen kann die weitere Kommunikation mitgelesen und manipuliert werden. Darüber hinaus können die für MTA-STS genutzten DNS-Einträge (ohne DNSSEC) anfällig für DNS Cache Poisoning sein.

Google stellt ebenfalls einen Leitfaden[8] zur Verfügung, der die Aktivierung von MTA-STS erläutert. Dabei bedarf es für Bestandskunden grundsätzlich nur weniger Handgriffe, die im Folgenden skizziert werden. Im Gegensatz zu DANE ist es für MTA-STS nicht notwendig, dass die Unternehmens-Domain mit DNSSEC abgesichert ist.

[7] Quelle: https://testconnectivity.microsoft.com/tests/O365DaneValidation/input
[8] Quelle: https://support.google.com/a/answer/9261504

Wichtig: Die E-Mail-Konfiguration eines Unternehmens kann beliebig komplex ausgestaltet sein. Wir empfehlen daher ein Vorgehen nach dem oben genannten Leitfaden oder bei Bedarf die Einbeziehung eines Dienstleisters, um Ausfälle im E-Mail-Dienst zu vermeiden.

Anpassung der DNS-Einträge

In einem ersten Schritt müssen für die Unternehmens-Domain zwei neue DNS-Einträge (Subdomains) bei der Registrierungsstelle, die die Domäne hostet, hinzugefügt werden, wobei „example.com“ durch die tatsächliche Unternehmens-Domain ersetzt werden muss:

Host	Typ	Value
_smtp._tls	TXT	v=TLSRPTv1; rua=mailto:tlsrpt@example.com
_mta-sts	TXT	v=STSv1; id=20250313120000

Der erste DNS-Eintrag, nämlich „_smtp._tls.example.com“, aktiviert das sogenannte TLS-Reporting. Dadurch werden Berichte über Verbindungen zu externen E-Mail-Servern an die dort hinterlegte E-Mail-Adressen gesendet, in diesem Fall an „tlsrpt@example.com“. Der zweite DNS-Eintrag, nämlich „_mta-sts._tls.example.com“, aktiviert das Sicherheitsmerkmal MTA-STS. Die „id“ entspricht der konfigurierten MTA-STS-Richtlinie, die im Folgenden erläutert wird. Eine bewährte Verfahrensweise ist beispielsweise, für die ID das aktuelle Datum + Uhrzeit zu verwenden. Im Anschluss sollte mit der Admin-Konsole[9] überprüft werden, ob MTA-STS und TLS-Reporting korrekt eingerichtet wurden.

Erstellung und Veröffentlichung einer MTA-STS-Richtlinie

Im zweiten Schritt muss eine Richtliniendatei namens „mta-sts.txt“ erstellt werden. Dabei handelt es sich um eine Text-Datei mit Schlüssel-Wert-Paaren, wobei sich jedes Paar in einer separaten Zeile befinden muss:

```
version: STSv1
mode: enforce
mx: smtp.google.com
mx: aspmx.l.google.com
mx: *.aspmx.l.google.com
max_age: 86400
```

Der Schlüssel „version“ gibt die Protokollversion und der Schlüssel „mode“ den Richtlinienmodus für MTA-STS an. Während die Protokollversion fix auf „STSv1“ konfiguriert sein muss, erlaubt der Richtlinienmodus verschiedene Optionen[10], z. B. „testing“ und „enforce“, die insbesondere während der Migration auf MTA-STS hilfreich sind. Die Werte der Schlüssel „mx“ definieren, welche MX-Server E-Mails an die Unternehmens-Domain akzeptieren, in diesem Fall die Mail Exchanger (MXe) von Google. Abschließend definiert „max_age“ die maximale Gültigkeitsdauer der Richtlinie in Sekunden.

Die Richtliniendatei muss abschließend auf einem Webserver veröffentlicht werden, sodass externe E-Mail-Server die MTA-STS-Richtlinie abrufen und interpretieren können. Dazu ist es notwendig, für die Unternehmens-Domain eine Subdomain namens „mta-sts“ hinzuzufügen. Anschließend muss auf dieser Subdomain ein Verzeichnis mit der Bezeichnung „.well-known“ angelegt und die erstellte Richtliniendatei „mta-sts.txt“ in diesem Verzeichnis abgelegt werden, sodass sie beispielhaft über die folgende URL abgerufen werden kann:

[9] Quelle: https://support.google.com/a/answer/9276419?ref_topic=9261406
[10] Quelle: https://support.google.com/a/answer/9276511?ref_topic=9261406

https://mta-sts.example.com/.well-known/mta-sts.txt

Zum Abschluss ist es empfehlenswert, noch einmal mit der Admin-Konsole[11] zu überprüfen, ob MTA-STS und TLS-Reporting korrekt konfiguriert wurden. Wenn der Test keine Fehler berichtet, ist die Unternehmens-Domain mit MTA-STS und TLS-Reporting abgesichert.

Fazit

Die für den Betrieb von E-Mail-Diensten empfohlenen Sicherheitsstandards sind durch entsprechende Angebote von Dienstleistern und die Verfügbarkeit der Implementierungen schon jetzt für eine breite Maße verfügbar. Häufig lässt sich mit einem überschaubaren Aufwand die Umsetzung dieser Sicherheitsstandards deutlich verbessern. Die Empfehlungen in diesem Dokument können ein guter Startpunkt sein, um die Sicherheit des eigenen E-Mail-Dienstes bzw. des E-Mail-Dienstes der eigenen Domain zukunftssicherer zu gestalten und von den angebotenen Sicherheitsstandards zu profitieren. Weitergehende Informationen sowie Best Practices sind in den Technischen Richtlinien BSI TR-03108 Sicherer E-Mail-Transport[12] und BSI TR-03182 E-Mail-Authentifizierung[13] zusammengestellt.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.

[11] Quelle: https://support.google.com/a/answer/9276419?ref_topic=9261406
[12] Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03108/tr03108_node.html
[13] Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03182/TR-03182_node.html