DIE EINRICHTUNG VON DMARC IN IHREM UNTERNEHMEN

Jedes Unternehmen, das die Ausstellung eines VMC-Zertifikats (Verified Mark Certificate) beantragt, muss zunächst die Konformität mit dem DMARC-Standard (Domain-based Message Authentication, Reporting and Conformance) nachweisen. Dieser Leitfaden führt Sie durch die korrekte Implementierung von DMARC in Ihrem Unternehmen.

digicert®

digicert®

WAS IST DMARC?

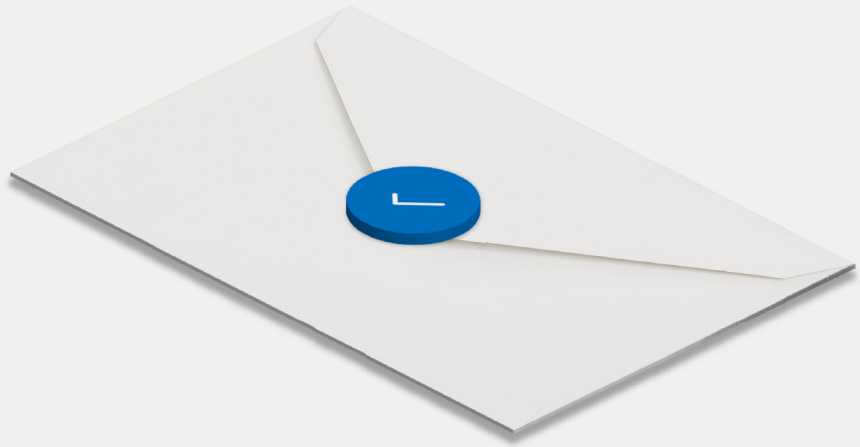
DMARC ist eine Richtlinie und ein Reporting-Protokoll zur E-Mail-Authentifizierung und zum Schutz von Business-Domains vor Betrugsversuchen wie Identitätsfälschung und Phishing.

Das Wichtigste in Kürze:

- DMARC ist ein im DNS gespeicherter TXT-Eintrag, über den Mailserver die Echtheit eingehender Nachrichten überprüfen können.
- Dadurch werden bestehende Methoden zur Authentifizierung eingehender E-Mails ergänzt und der Mailserver kann die Übereinstimmung mit vorhandenen Informationen über den Absender prüfen.
- Unternehmen haben drei Möglichkeiten, auf „abweichende" E-Mails zu reagieren:

- „p = none" (keine Aktion)
- „p = quarantine"
- „p = reject"

- Damit DMARC ordnungsgemäß funktioniert, müssen zunächst die Protokolle SPF (Sender Policy Framework) und DKIM (DomainKeys Identified Mail) eingerichtet werden.
- Der DMARC-Eintrag eines Unternehmens kann mit Internet-Tools wie diesem von valimail.com/digicert überprüft werden.



DIE BESSERE E-MAIL-AUTHENTIFIZIERUNG BEGINNT MIT DMARC

Durch DMARC soll ein Netzwerk aus Ein- und Ausgangsservern entstehen, das die Praxis der E-Mail-Authentifizierung durch Absender verbessert und Empfängern die Möglichkeit bietet, nicht authentifizierte Nachrichten abzulehnen.

digicert®

VORTEILE VON DMARC

Durch die Implementierung von DMARC profitiert Ihr Unternehmen von vier wesentlichen Vorteilen:

1. Sicherheit

Sie schützen E-Mail-Empfänger vor Spam, Betrugsversuchen und Phishing durch Missbrauch Ihrer E-Mail-Domain.

2. Transparenz

Sie erhalten ausführliche Berichte darüber, wer (oder was) Ihre Domain für den Versand von E-Mails nutzt.

3. Zustellbarkeit

Sie verbessern die Zustellbarkeit um 5–10 % und verhindern, dass Ihre E-Mails als Spam eingestuft werden.

4. Schutz der Marke

Sie schützen Ihre Marke vor Angriffen durch Identitätsfälschung.

der Kunden sind skeptisch gegenüber Marken, die sie aus gefälschten E-Mails kennen.

digicert®

SO RICHTEN SIE SPF EIN:

1. Erfassen Sie alle IP-Adressen, die für den Versand von E-Mails über Ihre Domain verwendet werden, einschließlich:
    - Webserver
    - Mailserver vor Ort
    - Mailserver des Internetanbieters
    - etwaige Mailserver von Drittanbietern
2. Tragen Sie alle sendenden und nicht sendenden Domains in eine Liste ein.
3. Erstellen Sie für jede Domain mit einem Texteditor wie Notepad++, Vim, Nano, usw. einen SPF-Eintrag im .txt Format.

    Beispiel 1: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 ip4:x.x.x.x -all
    Beispiel 2: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 include:thirdparty.com -all

4. Veröffentlichen Sie den SPF-Eintrag auf dem DNS-Server.

    Wenn Sie Ihren DNS-Server selbst verwalten, fügen Sie den entsprechenden Eintrag einfach dort ein. Wenn Ihr DNS-Server extern betreut wird, bitten Sie Ihren Serveradministrator, den Eintrag hinzuzufügen.

5. Prüfen Sie den neuen SPF-Eintrag auf dem DNS-Server mit einem Online-Tool.

WAS IST SPF?

Schutz vor unbefugtem E-Mail-Versand

SPF ist die erste Umsetzung des Konzepts der domainbasierten E-Mail-Authentifizierung. Der Standard verhindert Spoofing durch die automatische Freischaltung von IP-Adressen mit der Berechtigung zum Versand von E-Mails über eine Domain. Wenn ein Mailserver mit einer IP-Adresse, die nicht auf der Liste steht, E-Mails über die betreffende Domain versendet, schlägt die SPF-Authentifizierung fehl.

digicert®

SO RICHTEN SIE DKIM EIN:

1. Legen Sie einen DKIM-Selektor fest.

Idealerweise ist das eine einfache, benutzerdefinierte Zeichenfolge, die zur Identifizierung des öffentlichen DKIM-Schlüssels an den Domainnamen angehängt wird (z. B. „standard“).

Beispiel: “standard._domain.example.com” = host name

2. Generieren Sie für Ihre Domain einen öffentlichen und den zugehörigen privaten Schlüssel.

- Unter Windows: mit PUTTYGen
- Unter Linux und Mac: mit ssh-keygen

3. Erstellen und veröffentlichen Sie einen neuen TXT-Eintrag.

Erstellen Sie einen neuen Eintrag in der DNS-Konsole mit dem öffentlichen Schlüssel, den Sie gerade generiert haben.

Beispiel: v=DKIM1; p=IhrÖffentlicherSchlüssel

WAS IST DKIM?

Schutz für E-Mails vor Manipulation während der Übertragung

DKIM ist ein Standard zur E-Mail-Authentifizierung durch asymmetrisch verschlüsselte Signaturen.

DKIM dient der Überprüfung, ob eine E-Mail tatsächlich von der Domain mit dem zugehörigen Schlüssel stammt, und ob diese E-Mail während der Übertragung modifiziert wurde.

digicert®

DMARC-ÜBERWACHUNGSMODUS EINRICHTEN

1. Vergewissern Sie sich, das SPF und DKIM korrekt konfiguriert wurden.

2. Erstellen Sie einen DNS-Eintrag.

   Das Namensschema für den DMARC-Eintrag im Textformat lautet „_dmarc.ihre_domain.com“.

   Beispiel: v=DMARC1;p=none; rua=mailto:dmarcreports@ihre_domain.com

   Falls Sie den DNS-Server Ihrer Domain selbst verwalten, erstellen Sie analog zum SPF- und DKIM-Eintrag einen „p=none“ DMARC-Eintrag (Überwachungsmodus).

   Wenn Ihr DNS-Server extern betreut wird, bitten Sie Ihren DNS-Anbieter, den DMARC-Eintrag zu erstellen.

3. Prüfen Sie Ihren DMARC-Eintrag mit einem Online-Tool.

   Hinweis: Die Replikation dauert in der Regel 24–48 Stunden.
   Tool zur Prüfung von DMARC-Einträgen

WAS IST DER DMARC-ÜBERWACHUNGSMODUS?

Transparenz beim E-Mail-Versand über Ihre Domain

Im DMARC-Berichtsmodus erhalten Domain-Inhaber Einblick in den E-Mail-Traffic der jeweiligen Domain.

In den Berichten sind Nachrichten aufgeführt, die die DMARC-Prüfung nicht bestanden haben und bei voller Durchsetzung der Richtlinie entweder isoliert oder abgelehnt worden wären. Darüber hinaus enthalten die DMARC-Berichte Informationen über alle Systeme und Dienste, die E-Mails aus der überwachten Domain versenden.

HINWEIS: Im Überwachungsmodus wird die Richtlinie nicht durchgesetzt. Nachrichten werden auch dann normal zugestellt, wenn die Authentifizierung fehlschlägt. Das ermöglicht eine störungsfreie Implementierung des DMARC-Standards.

digicert®

HÄUFIGE TAGS IN DMARC .TXT EINTRÄGEN

TAG	OBLIGATORISCH	ZWECK
V	OBLIGATORISCH	PROTOKOLLVERSION
P	OBLIGATORISCH	POLITIKVERSION
PCT	OPTIONAL	PROZENTANTEIL DER GEFILTERTEN NACHRICHTEN
RUA	OPTIONAL	EMPFÄNGERADRESSE FÜR SAMMELBERICHTE
SP	OPTIONAL	RICHTLINIE FÜR SUBDOMAINS

digicert®

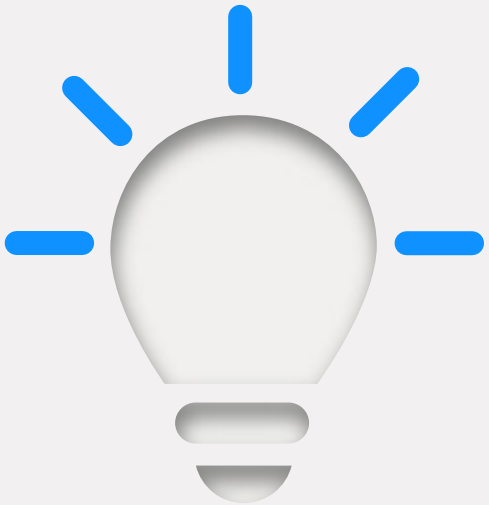
WAS STEHT IM DMARC-BERICHT?

Der Domain-Inhaber kann dem Bericht entnehmen, wie viele betrügerische E-Mails über die eigene Domain gesendet werden, woher sie stammen und ob sie mit der Anweisung „quarantine“ oder „reject“ gestoppt werden können.

Die empfängerseitigen Berichte sind XML-Dateien mit folgenden Feldern:

- Die Zahl der Nachrichten von der jeweiligen IP-Adresse
- Die Verarbeitung der Nachrichten gemäß der implementierten DMARC-Richtlinie
- Die Ergebnisse der SPF-Prüfung
- Die Ergebnisse der DKIM-Prüfung

Der XML-Bericht ist zwar lesbar, aber nicht besonders nutzerfreundlich. Für die Anzeige und Verarbeitung von DMARC-Berichten eignen sich Tools wie das von Valimail oder von anderen Anbietern.



VIER MÖGLICHKEITEN ZUR NUTZUNG VON DMARC-BERICHTEN

Solider Überblick vor der Durchsetzung der Richtlinie

1. Finden Sie heraus, welche E-Mails als unzulässig ausgewiesen werden.

2. Suchen Sie nach E-Mails, die sich nach der DMARC-Prüfung als eindeutige False-Positives herausstellen. Solche Nachrichten werden nach der endgültigen Durchsetzung der Richtlinie entweder abgelehnt oder isoliert.

3. Kontaktieren Sie die Verantwortlichen zwecks Klärung der Rechtmäßigkeit von E-Mails, die als unzulässig eingestuft wurden.

4. Aktualisieren Sie ggf. Ihren SPF-Eintrag und setzen Sie die vermeintlich unzulässigen IP-Adressen auf die Zulassungsliste.

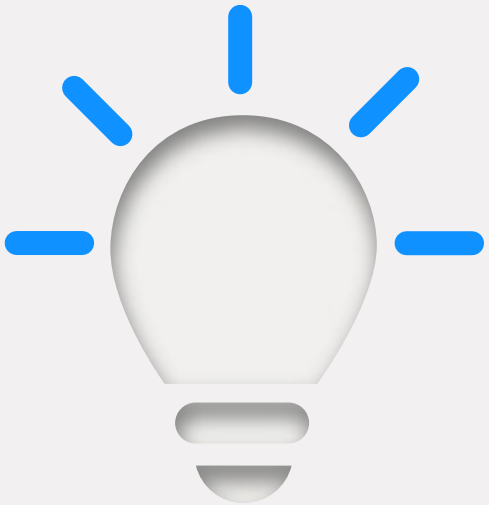
digicert®

DMARC-BERICHTE SCHAFFEN ORDNUNG VOR DER AKTIVIERUNG DER RICHTLINIENDURCHSETZUNG

Die Analyse von DMARC-Berichten kann viel Zeit in Anspruch nehmen. Wenn jedoch Absender übersehen oder falsch eingestuft werden, führt die Umstellung der DMARC-Richtlinie auf „quarantine“ oder „reject“ dazu, dass legitime E-Mails nicht zugestellt werden. Die Lösung solcher Probleme ist potenziell sehr zeitintensiv.

Vor der Durchsetzung der DMARC-Richtlinie sollten Sie deshalb die folgenden Schritte durchführen:

- Bestandsaufnahme aller Versand-Domains laut DMARC-Bericht und durch Rücksprache mit Stakeholdern
- Bestimmung der Verantwortlichen für einzelne Dienste und Versand-Domains
- Einstufung der Dienste in die Kategorien „autorisiert“, „nicht autorisiert“ und „schädlich“
- Zusammenarbeit mit Stakeholdern zwecks Identifizierung etwaiger weiterer Versand-Domains, die im DMARC-Bericht nicht aufgeführt sind
- Rücksprache mit Stakeholdern bezüglich aller neu identifizierten Versand-Domains
- Erweiterung des SPF-Eintrags um neue legitime IP-Adressen



EMPFEHLUNGEN FÜR DIE KOMMUNIKATION VOR DER DMARC-DURCHSETZUNG

Fünf Tipps zur Verbesserung der Akzeptanz

- Dokumentation und Erstellung einer Implementierungsrichtlinie für Stakeholder
- Bei Unterstützungsbedarf: Kontaktaufnahme mit DMARC-Experten wie Valimail
- Umgehende Bekanntgabe neuer Erkenntnisse aus DMARC-Berichten
- Anfangsphase der DMARC-Implementierung als internes Projekt abwickeln
- Einbindung von Führungskräften als wichtige Projektsponsoren

WIE LANGE SOLLTE DMARC IM ÜBERWACHUNGSMODUS LAUFEN?

Der Zeitaufwand richtet sich nach der Unternehmensgröße, wobei Großunternehmen in der Regel mehr Zeit veranschlagen müssen. Rechnen Sie mit mehreren Wochen bzw. Monaten.

Sobald Sie sicher sind, dass die Bestandsaufnahme abgeschlossen ist, alle autorisierten Versand-Domains bekannt und Ihre Mitarbeiter ausreichend informiert sind, können Sie die Quarantäne aktivieren.

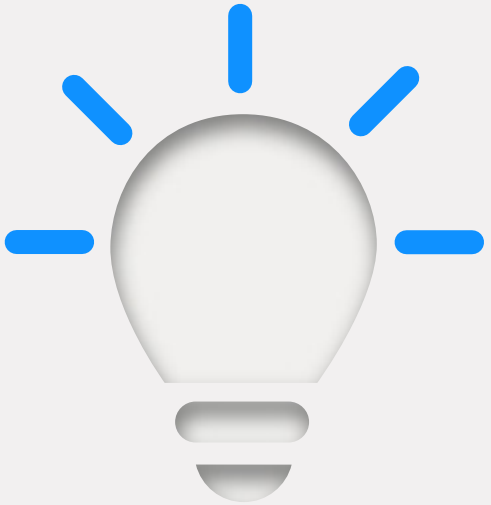
Bei aktivem Quarantänemodus werden alle nicht authentifizierten E-Mails isoliert. Das bedeutet in der Regel, dass die Nachrichten im Spam-Ordner landen.

SO STELLEN SIE DMARC AUF QUARANTÄNE UM

1. Loggen Sie sich auf Ihrem DNS-Server ein und suchen Sie nach dem DMARC-Eintrag.
2. Öffnen Sie den DMARC-Eintrag der jeweiligen Domain und ändern Sie die Richtlinie von „p=none“ zu „p=quarantine“.
   Beispiel: v=DMARC;p=quarantine;pct=10;rua=mailto:dmarcreports@ihre_domain.com
3. Fügen Sie das Tag „pct“ hinzu (Prozentanteil der gefilterten Nachrichten). Wir empfehlen, mit 10 % zu beginnen.
4. Wenn Sie sicher sind, dass alles ordnungsgemäß funktioniert, können Sie diesen Wert schrittweise auf 100 % erhöhen („pct=100“).

   HINWEIS: Für BIMI und VMC ist die Einstellung „pct=100“ erforderlich; das Tag „p“ kann jedoch wahlweise auf „quarantine“ oder „reject“ eingestellt sein.

digicert®



SO FUNKTIONIERT DIE E-MAIL-FILTERUNG:

- Wenn die Richtlinie nicht auf „p=none“ eingestellt ist, wird sie auf den unter „pct“ ausgewiesenen Anteil der Nachrichten angewendet.
- Für die restlichen E-Mails gilt die jeweils weniger strenge Regel. Beispielsweise werden bei den Einstellungen „p=quarantine“ und „pct=10“ 10 % der nicht authentifizierten E-Mails unter Quarantäne gestellt und die restlichen 90 % normal zugestellt.

digicert®

BEI „PCT=100“ KÖNNEN SIE DIE STRENGSTE EINSTELLUNG „P=REJECT“ AKTIVIEREN.

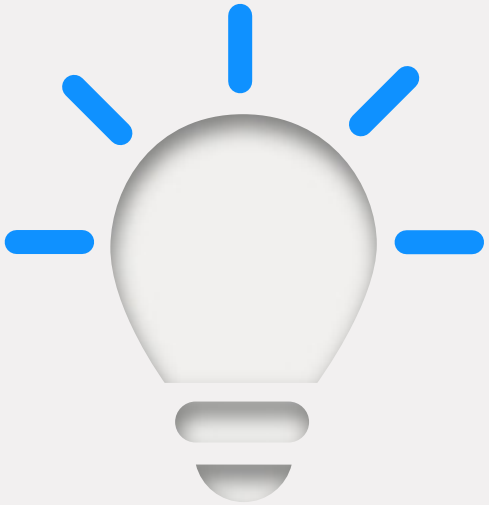
digicert®

SO STELLEN SIE DMARC AUF ABLEHNEN UM

1. Öffnen Sie den DMARC-Eintrag in der DNS-Konsole.
2. Ändern Sie die Einstellung „p=quarantine“ zu „p=reject“.
   Beispiel: v=DMARC;p=reject;pct=100;rua=mailto:dmarcreports @ ihre_domain.com
3. Speichern Sie die Änderung.

TIPP: Besonders jetzt sollten Sie den E-Mail-Verkehr im Auge behalten und sicherstellen, dass keine legitimen E-Mails abgelehnt und gelöscht werden.

Haben Sie noch weitere Fragen? Senden Sie uns noch heute eine E-Mail an contactus@digicert.com oder besuchen Sie uns unter https://www.digicert.com/de/tls-ssl/verified-mark-certificates/?



WAS BEWIRKT DIE EINSTELLUNG „P=REJECT“?

Alle E-Mails, die als nicht autorisiert eingestuft werden und die DMARC-Prüfung nicht bestehen, werden abgelehnt und gelöscht. Der Empfänger kann keine Kopie der Nachricht abrufen und wird auch nicht über ihre Löschung informiert.