digicert®

VERIFIED MARK CERTIFICATES (VMC-ZERTIFIKATE)

Mit einem Gütesiegel werten Sie Ihr E-Mail-Marketing auf – und weisen Ihre Identität nach

Wir alle versenden täglich E-Mails. Diese Kommunikationsform ist daher zum einen ausgesprochen nützlich, zum anderen aber anfällig für Angriffe – insbesondere solche, bei denen eine falsche Identität vorgetäuscht wird, wie beim Phishing. 96 % aller Phishing-Attacken nehmen ihren Anfang mit einer E-Mail, und 75 % aller globalen Unternehmen wurden 2020 zur Zielscheibe.

Woran liegt das? Zum großen Teil daran, dass Unternehmen den Empfängern keine gute Möglichkeit bieten, die Unternehmensidentität sofort und direkt zu überprüfen. Ebenso fehlt eine zuverlässige Methode, schädlichen Inhalt im Gewand einer harmlosen E-Mail schnell zu erkennen und zu isolieren.

Jedenfalls war das so, bevor es Verified Mark Certificates (VMC-Zertifikate) gab. Diese ermöglichen nämlich – zusammen mit den Standards BIMI und DMARC – eine sofort sichtbare Präsentation der eigenen Marke und umfassen strikte Vorkehrungen, die Kunden und Unternehmen gleichermaßen vor Phishing- und ähnlichen identitätsbezogenen Angriffen schützen.

Wie funktionieren verifizierte E-Mails?

Durchsetzung von DMARC + BIMI + VMC = E-Mail mit geprüftem Logo

Was sind VMC-Zertifikate?

Mit den innovativen VMCs (Verified Mark Certificates) können Unternehmen im Postfach des Empfängers neben dem Feld „Absender“ ein zertifiziertes Logo anzeigen lassen, und das noch bevor die Nachricht geöffnet wird. Beim Erwerb eines VMC-Zertifikats überprüft DigiCert gründlich die Identität des Käufers und ggf. den Markenschutz des Logos.

Siehe Liste der offiziellen Markeninformationsstellen für VMC-Zertifikate

Was ist DMARC?

„Domain-based Message Authentication, Reporting and Conformance“ (DMARC) ist ein Standard für die Authentifizierung von E-Mails und basiert auf den Protokollen SPF und DKIM. DMARC überprüft den Domainnamen des Absenders mithilfe öffentlicher Richtlinien zum Umgang des Empfängers mit fehlgeschlagenen Authentifizierungsversuchen und übermittelt Empfängerdaten an den Absender. Dies verbessert die Transparenz und schützt die Domain zusätzlich vor betrügerischen Phishing- und Spoofing-Angriffen.

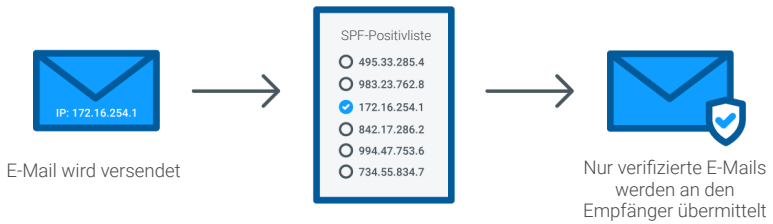
Laden Sie sich unsere Schritt-für-Schritt-Anleitung zu DMARC herunter.

Was ist BIMI?

„Brand Indicators for Message Identification“ (BIMI) ist eine E-Mail-Spezifikation, die in bestimmten E-Mail-Clients die Anzeige von Markenlogos ermöglicht, um die Umsetzung des DMARC-Standards zu erleichtern.

Wie arbeiten DMARC und BIMI zusammen?

Ihr E-Mail-Client überprüft die DMARC-Spezifikation Ihres Unternehmens, indem er sie mit Ihrem BIMI-Eintrag und dem VMC-basierten Logo abgleicht. Ist alles in Ordnung, sehen E-Mail-Empfänger künftig Ihr Logo und wissen so, dass die Nachricht wirklich von Ihnen kommt. Außerdem steigert das Logo die Kundenbindung und den Wiedererkennungswert Ihrer Marke.



E-Mail wird versendet

IP-Adresse des Absenders wird mit der SPF-Positivliste abgeglichen

E-Mail-Signatur des Absenders wird mittels DKIM verifiziert

Nur verifizierte E-Mails werden an den Empfänger übermittelt

Vorteile für die IT

Mehr Transparenz, Sicherheit und Kontrolle mit DMARC

- Verbesserte Sicherheit dank Durchsetzung des DMARC-Standards
- Verringertes Risiko von Phishing-Angriffen auf Ihr Unternehmen und Ihre Marke
- Besserer Überblick und mehr Kontrolle über von Ihrer Domain gesendete und empfangene E-Mails
- Sie sehen klar und deutlich, wie oft und mit welchen Methoden Ihre Marke zur Zielscheibe von Angriffen wird.
- Verifizierte E-Mails werden zuverlässig zugestellt und lassen sich leicht identifizieren.

Vorteile im Marketing

Mehr Sichtbarkeit im Posteingang

- Um über 10 % bessere Kundenbindung[1]
- Jede versendete E-Mail erhöht den Wiedererkennungswert Ihrer Marke.
- Ihre Marke kann sich mit DMARC und hoher E-Mail-Sicherheit profilieren.
- Ihr Markenauftritt ist authentisch, geprüft und einprägsam.
- Ihre E-Mails heben sich visuell von der Masse der Marketingnachrichten ab und sind damit noch effektiver.

Vorteile für Kunden

Weniger Phishing. Mehr Vertrauen.

Je mehr Unternehmen DMARC implementieren, umso weniger Phishing-E-Mails landen im Posteingang ihrer Kunden. Das bedeutet weniger Risiko, weniger Ärger und insgesamt mehr Komfort für den Nutzer.

Validierungsanforderungen

Die Validierungsschritte, die Unternehmen für ein VMC-Zertifikat durchlaufen müssen, ähneln denen bei SSL-Zertifikaten mit EV (Extended Validation). Dazu gehören u. a. die Identitätsprüfung des Bewerbers sowie eine persönliche Bestätigung durch einen Notar oder Rechtsanwalt. Darüber hinaus führt das Validierungsteam von DigiCert einen Videocall durch, bei dem sich der Bewerber vor der Kamera mit einem offiziellen Dokument ausweisen muss. Zu guter Letzt muss DigiCert überprüfen, ob Ihr Logo offiziell und rechtskräftig markengeschützt und korrekt formatiert ist.

So formatieren Sie Ihr Logo korrekt als SVG-Datei

Erwerb eines VMC-Zertifikats

VMC-Zertifikate sind in CertCentral erhältlich.

Hinweis: Um den Kauf abzuschließen, benötigen Sie ein aktives Konto.

Jetzt kaufen

Installation

1. Nachdem Sie Ihr SVG-Logo an DigiCert übermittelt haben, erhalten Sie eine Datei mit einer PEM-verschlüsselten Zertifikatskette.

2. Beides – also das Logo und die Zertifikatskette – muss auf einen öffentlich zugänglichen Server geladen werden und den Zugriff per HTTPS erlauben (HTTP allein reicht nicht aus).

3. Anschließend müssen Sie die korrekte URL und den Dateispeicherort in Ihrem BIMI-Eintrag hinterlegen.

Häufig gestellte Fragen

Wie viele VMCs benötige ich?

Dies hängt in der Regel von der Anzahl der Logos ab, die Ihr Unternehmen verwendet. Weitere Informationen dazu finden Sie in unserem Blogbeitrag.

Kann ich statt eines Logos auch eine Wortmarke verwenden?

Ja. Eine Wortmarke anstelle eines Logos ist möglich, allerdings muss diese bei einer teilnehmenden Markenschutzbehörde registriert sein.

Woher weiß ich, ob mein Unternehmen DMARC-konform ist?

Hier können Sie überprüfen, ob Sie die DMARC-Anforderungen erfüllen.

Wie kann ich überprüfen, ob meine Marke geschützt ist, und wie erlange ich Markenschutz?

Ihr Logo muss bei einer anerkannten Markenschutzbehörde registriert sein.

Wie Sie Ihre Marke schützen lassen, erfahren Sie in unserem Blogbeitrag.

Welche E-Mail-Clients unterstützen VMC-Zertifikate?

Gmail, Yahoo, FastMail, Verizon und andere.

Da es VMC-Zertifikate noch nicht sehr lange gibt, kommen stetig weitere E-Mail-Clients hinzu, die VMCs unterstützen. Eine aktuelle Liste finden Sie auf unserer Website.

Was passiert, wenn ich nach dem Kauf eines VMC-Zertifikats die Durchsetzung des DMARC-Standards aussetze?

Ihr Zertifikat ist dann weiterhin gültig, aber Ihr Logo wird nicht mehr angezeigt. Soll das Logo weiterhin neben der Absenderadresse erscheinen, müssen Sie DMARC aktiv durchsetzen, wie in Ihrem BIMI-Eintrag angegeben.

Wie oft muss ich das Zertifikat erneuern und neu validieren lassen?

Kunden müssen ihr Zertifikat jedes Jahr erneuern. Hat ein Unternehmen einmal den Validierungsprozess durchlaufen, ist keine weitere notarielle Beurkundung erforderlich. Die Validierung muss jedoch alle 398 Tage wiederholt werden, ähnlich wie bei den weit verbreiteten TLS/SSL-Zertifikaten mit EV. Endgültig abgeschlossen ist der Vorgang, wenn das erneuerte Zertifikat in CertCentral hinterlegt wurde.

Wir sind zwar ein offiziell registriertes Unternehmen, aber unser Logo ist nicht markenrechtlich geschützt. Können wir trotzdem ein VMC-Zertifikat verwenden?

Nein, das ist zurzeit leider noch nicht möglich. Angezeigt werden nur Logos, die rechtmäßig als Marke eingetragen wurden.

Sie haben weitere Fragen?

Weitere Informationen und Kontaktmöglichkeiten finden Sie unter https://www.digicert.com/de/tls-ssl/verified-mark-certificates/