DMARC ADVISOR

WIE SIE PHISHING UND E-MAIL-MISSBRAUCH DURCH DIE IMPLEMENTIERUNG VON DMARC VERHINDERN KÖNNEN

WHITEPAPER

Introduction

Phishing ist die vielleicht am häufigsten genutzte Art von Cyberangriffen. Vertrauliche Informationen wie Passwörter, Kreditkartennummern oder andere persönliche Daten werden über Phishing-E-Mails gestohlen. Für Einzelpersonen kann der Schaden verheerend, für Unternehmen aber manchmal sogar existenzbedrohend sein.

Laut einer Studie des Verizon Data Breach Investigation Report aus dem Jahr 2021 hatten 36 % aller Datenschutzverletzungen mit Phishing zu tun. Darüber hinaus kam bei 85 % aller Sicherheitsverstöße durch Social Engineering als Hauptmethode Phishing zum Einsatz.

Die Anti-Phishing Working Group beobachtete im 4. Quartal 2022 insgesamt 1.350.037 Phishing-Angriffe. Dies ist ein leichter Anstieg gegenüber dem dritten Rekordquartal, in dem die APWG insgesamt 1.270.883 Phishing-Angriffe registrierte.

Phishing-Angriffe kommen diesen Studien zufolge immer noch sehr häufig vor und ihre Zahl scheint nicht abzunehmen. Bei DMARC Advisor helfen wir den größten Unternehmen in Europa, ihre Domains vor Phishing-Angriffen zu schützen. Wie aus dem Titel hervorgeht, tun wir dies durch die Implementierung von DMARC. DMARC basiert auf zwei anderen offenen Standards, die in Form von Internet-Regeln E-Mail-Servern vorschreiben, wie sie mit autorisierten und nicht autorisierten E-Mail-Flüssen umgehen sollen. Diese offenen Standards sind SPF, DKIM und DMARC.

> ***36% of all data breaches involved phishing***

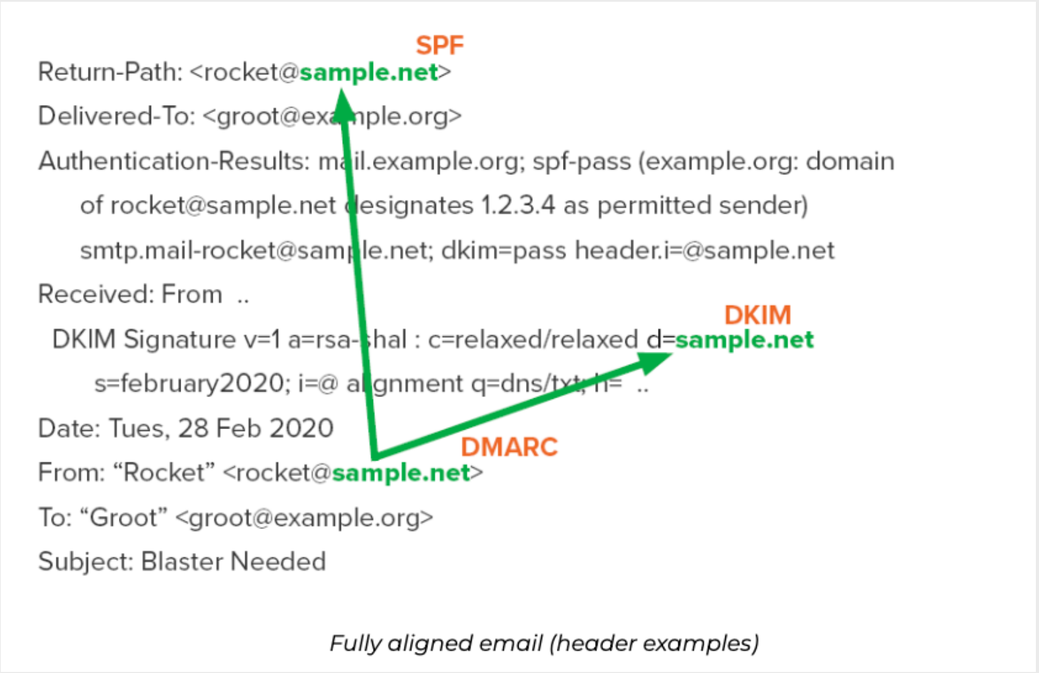
1) Whitepaper - Wie man Phishing mit DMARC verhindert

Was sind SPF, DKIM und DMARC?

SPF, DKIM und DMARC sind offene Standards, die von jeder Person kostenlos im Internet implementiert werden können. Das Bild auf der rechten Seite gibt einen schnellen Überblick darüber, wo die einzelnen Authentifizierungsmethoden in einer E-Mail zu finden sind.

Die „From“-Domain, auch als DMARC-Domain bekannt, wird in einer E-Mail angezeigt. Diese ist für jeden als „Absender“ zu erkennen. Genau diese Domain wird in Phishing-Kampagnen verwendet. Auch wenn SPF und DKIM eine Validierungsprüfung bestehen können, bedeutet das nicht, dass die DMARC-Authentifizierung erfolgreich ist. Die DMARC-Domain muss mit den SPF- und DKIM-Domains abgeglichen werden, um vor Phishing oder E-Mail-Missbrauch geschützt zu sein.

Überprüfen Sie mit dem Domain Check von DMARC Advisor, ob Ihre Domain geschützt ist. Völlig kostenlos und ohne Haken.



Fully aligned email (header examples)

DMARC ADVISOR

SPF | Sender Policy Framework

„Der Postbote“

SPF steht für Sender Policy Framework und ermöglicht es dem Inhaber einer Domain, festzulegen, welche E-Mail-Server berechtigt sind, E-Mails im Namen dieser Domain zu versenden.

Am einfachsten lässt sich SPF so erklären, dass Sie ein Paket an Ihren Freund schicken und DHL mit der Zustellung des Pakets beauftragt haben. Jeder andere Postdienst ist nicht zugelassen.

DKIM | DomainKeys Identified Mail

„Das Siegel“

DKIM steht für DomainKeys Identified Mail und funktioniert durch Hinzufügen einer digitalen Signatur zum Header einer E-Mail-Nachricht.

Am einfachsten lässt sich DKIM so erklären, dass Sie an das von Ihnen versandte Paket ein Siegel anbringen, das bei der Ankunft intakt sein sollte. Wenn das Siegel gebrochen ist, wissen Sie, dass der Inhalt manipuliert werden kann.

DMARC | Domain-based Messaging Authentication Reporting and Conformance

DMARC steht für Domain-based Messaging Authentication Reporting and Conformance und ist ein offener Standard, der auf SPF und DKIM aufbaut. Mit DMARC kann ein Domain-Inhaber festlegen, wie seine E-Mails behandelt werden sollen, wenn sie SPF- oder DKIM-Prüfungen nicht bestehen. Der Domain-Inhaber kann wählen, ob die E-Mail abgelehnt, als Spam markiert oder wie gewohnt zugestellt werden soll.

Ohne DMARC kann der Domain-Inhaber nicht sehen, wer oder was E-Mails im Namen seiner Domain versendet. DMARC liefert auch Rückmeldungen darüber, wie ihre E-Mails von anderen E-Mail-Servern behandelt werden.

Die drei DMARC-Richtlinien

DMARC ermöglicht Domain-Inhabern die Wahl einer Richtlinie, die dem empfangenden E-Mail-Server mitteilt, was mit einer E-Mail geschehen soll, wenn diese die DMARC-Authentifizierungsprüfung nicht besteht.

DMARC bietet folgende drei Richtlinien zur Auswahl:

- **p=none**: überwacht E-Mail-Flüsse. Es werden keine weiteren Maßnahmen ergriffen.
- **p=quarantine**: behandelt E-Mails, die die DMARC-Authentifizerungsprüfung nicht bestehen, als Spam und sendet sie an den Spam-Ordner.
- **p=reject**: blockiert E-Mails, die die DMARC-Authentifizierungsprüfung nicht bestehen. Die E-Mails kommen dann einfach nicht im Posteingang an. P=reject sollte immer das Ziel bei der Implementierung von DMARC sein.

Zu beachten ist, dass eine Änderung der DMARC-Richtlinie negative Auswirkungen auf Ihren E-Mail-Verkehr haben kann, wenn Sie Ihre Domains in der p=none-Phase nicht korrekt überwacht haben. Eine Domain kann nur einmal alle drei Monate für den Versand eines Newsletters genutzt werden. Es dauert somit drei Monate, um alle Daten aus dieser Domain zu erhalten. Nehmen Sie sich also Zeit für die Überwachung und treffen Sie keine übereilten Entscheidungen.

Erste Schritte mit DMARC

Für den Einstieg sind einige nicht sehr komplizierte Schritte auszuführen.

1 - Ermitteln Sie zunächst, welche Domains Sie haben. Darunter fallen sendende und nicht sendende Domains. Auch Unterdomänen.

2 - Erstellen Sie eine E-Mail-Authentifizierungsrichtlinie für jede Domain (hoffentlich haben Sie diese bereits eingerichtet). Dies sind die bereits erwähnten SPF- und DKIM-Domains.

3 - Veröffentlichen Sie eine DMARC-Richtlinie im DNS-Eintrag Ihrer Domain. Dadurch wissen andere E-Mail-Server, dass Sie DMARC verwenden und wie sie mit fehlgeschlagenen Authentifizierungsprüfungen umgehen sollen.

4 - Prüfen Sie Ihre DMARC-Berichte dahingehend, wie Ihr E-Mail-Verkehr von anderen E-Mail-Servern behandelt wird. Sie können nun alle Probleme oder Schwachstellen im Zusammenhang mit Ihren Domains ermitteln.

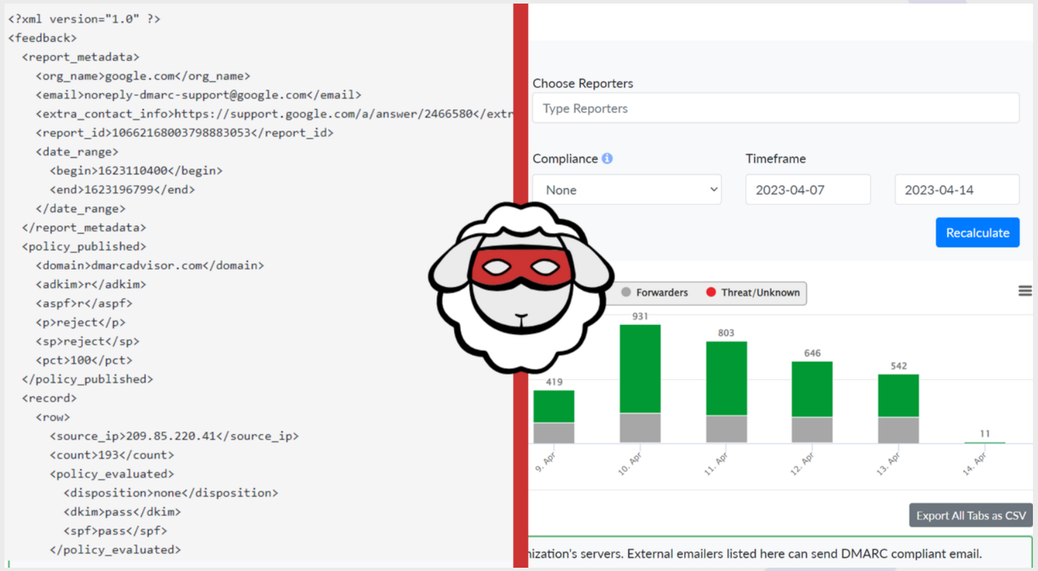
Der einzige Nachteil ist, dass diese als XML-Dateien erstellten DMARC-Berichte wie auf dem Bild rechts aussehen.

Dieser XML-Bericht bezieht sich nur auf eine einzige Domain und einen einzigen Absender. Wenn Sie also viele E-Mails von vielen Domains aus versenden, erhalten Sie mehr als genug Berichte. Die Analyse dieser Berichte kann zeitaufwändig sein und ist oft schwer richtig zu interpretieren.

```
<?xml version="1.0" ?>
<feedback>
  <report_metadata>
    <org_name>google.com</org_name>
    <email>noreply-dmarc-support@google.com</email>
    <extra_contact_info>https://support.google.com/a/answer/2466580</extra_contact_info>
    <report_id>10662168003798883053</report_id>
    <date_range>
      <begin>1623110400</begin>
      <end>1623196799</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>dmarcadvisor.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>reject</p>
    <sp>reject</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>209.85.220.41</source_ip>
      <count>193</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim>
        <spf>pass</spf>
      </policy_evaluated>
```

Raw DMARC XML data

Lesbare XML-basierte DMARC-Berichte



DMARC Advisor stellt seit 2013 lesbare DMARC-Daten bereit und liefert nach wie vor die detailliertesten Berichte der Branche.

Wir wissen, dass die Untersuchung von DMARC-Daten eine Herausforderung sein kann. Deshalb haben wir den Detail Viewer entwickelt – ein leistungsstarkes Tool, das die Navigation erleichtert. Sie können die Daten-Timeline problemlos durchsuchen und die Ergebnisse nach bestimmten Suchparametern wie Datumsangaben, Domains und Datenanbietern filtern.

Mit Hilfe der besonders nützlichen Filteroption können Sie sehen, was passiert wäre, wenn eine DMARC-Richtlinie in Kraft gewesen wäre. Mit diesen Informationen sind Sie Sicherheitsverstößen immer einen Schritt voraus und Sie können Maßnahmen zur Verbesserung Ihrer E-Mail-Sicherheit auf den Weg bringen.

Im Detail Viewer werden die DMARC-Daten in vier übergeordnete Registerkarten gruppiert: DMARC-fähig, Nicht-konform, Weiterleitung und Bedrohung/Unbekannt. Jede Registerkarte enthält detaillierte Informationen über die DMARC-Konformität und hebt jede Infrastruktur hervor, die möglicherweise genauer zu untersuchen ist. Sie können sogar jede Kategorie aufschlüsseln, um weitere Details anzuzeigen und die Quellen der E-Mails Ihrer Domain ermitteln.

Auf unserer Plattform können Sie zudem Daten von mehreren Anbietern über bestimmte Zeiträume hinweg kombinieren. So erhalten Sie einen umfassenden Überblick über die E-Mail-Sicherheit Ihrer Domain und können Ihre DMARC-Daten stressfrei auswerten. Bei DMARC Advisor setzen wir alles daran, Ihnen schnell und einfach die benötigten Einblicke zu verschaffen, und der Detail Viewer hilft uns dabei.

ÜBER DMARC ADVISOR

DMARC Advisor wurde 2013 von echten Internet-Veteranen gegründet. Wir waren der erste europäische DMARC-Anbieter. Heute sind wir auch die Nummer 1 unter den DMARC-Anbietern in Europa. Unsere Gründer gründeten auch einen der ersten E-Mail-Diensteanbieter in den Niederlanden und versendeten bereits DMARC-konforme E-Mails, bevor DMARC überhaupt erfunden wurde. Auf ihre Initiative hin, Wurde DMARC ein verbindlicher Standard für Regierungen in den Niederlanden, was auch zu einer Initiative für sichere E-Mails auf europäischer Ebene führte.

DMARC Advisor hat es sich zur Aufgabe gemacht, Menschen zu inspirieren, offene Standards als solide Grundlage zu implementieren, um das Internet sicherer zu machen. Mit mehr als 20 Jahren Erfahrung im Bereich E-Mail-Zustellbarkeit und -Sicherheit und mehr als 10 Jahren Erfahrung in der Unterstützung von Unternehmen bei der Implementierung von DMARC ist DMARC Advisor zweifellos der neue Standard für die Implementierung von DMARC!

www.dmarcadvisor.com

sales@dmarcadvisor.com

dmarc-advisor