Leistungsbeschreibung

DMARC Manager

DMARC Manager (das „Produkt“) ist eine Software as a Service (SaaS), die dem Kunden oder einem Dritten im Auftrag des Kunden hilft, Kundendomains vor Identitätsdiebstahl und Phishing-Angriffen zu schützen und die Einhaltung der Domain-basierten Nachrichtenauthentifizierung, Berichterstattung und Konformität (DMARC) zu gewährleisten. DMARC Manager bietet dem Kunden Werkzeuge zur Überwachung, Analyse und Durchsetzung von E-Mail-Authentifizierungsprotokollen wie dem Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM), sodass der Kunde die Kontrolle über die E-Mail-Zustellung behält und den Ruf seiner Organisation schützt.

1. Definitionen

Wann immer die folgenden Begriffe in diesem Dokument oder im Zusammenhang mit dessen Leistung verwendet werden, sei es in Singular- oder Pluralform, haben sie zwischen den Parteien die nachstehend definierten Bedeutungen:

Kunde(n): Der Endkunde von Hornetsecurity, der ein gültiges Abonnement zur Nutzung des DMARC Managers abgeschlossen hat.

Benutzer: Der Endnutzer des DMARC Managers, der diesen unter der Aufsicht und Verantwortung des Kunden verwendet.

2. DMARC Manager bietet den Kunden die folgende Funktionalität:
   a. Domain-Onboarding
      i. Alle im Control Panel verfügbaren Kundendomains können dem DMARC Manager hinzugefügt werden. Zunächst müssen die von Hornetsecurity bereitgestellten DNS-Einträge für jede Domain in den DNS-Einstellungen des kundenspezifischen DNS-Anbieters hinzugefügt werden. Nach erfolgreicher Konfiguration im Control Panel kann der DMARC Manager genutzt werden.
   b. Dashboard
      i. Das Dashboard bietet eine Übersicht über den E-Mail-Authentifizierungsstatus des Kunden, einschließlich Kennzahlen zur DMARC-Konformität, dem Prozentsatz authentifizierter E-Mails und potenziellen Sicherheitsbedrohungen.
      ii. Es stehen Visualisierungstools wie Diagramme zur Verfügung, um Trends in Bezug auf erfolgreiche und fehlgeschlagene DMARC-Authentifizierungen sowie die Herkunftsländer der Absender über verschiedene Zeiträume zu erkennen.
   c. E-Mail-Absender
      i. Eine Übersicht über Analysen, Konfigurationen und Warnungen für Quellen, von denen E-Mails über die jeweilige Domain gesendet werden. Dies zentralisiert die Verwaltung der DMARC-Einstellungen und der E-Mail-Sicherheit.

ii. Der Kunde erhält detaillierte Informationen über das Volumen der konformen und nicht konformen DMARC-E-Mails für jede Domain.

iii. Übersicht über alle identifizierten und verifizierten E-Mail-Quellen mit Details zum E-Mail-Volumen, dem Authentifizierungsstatus (ob E-Mails die DMARC-Prüfungen bestanden haben oder nicht) und der Kategorisierung der Quellen (z. B. autorisiert oder nicht autorisiert)

d. Domain-Konfiguration

i. DMARC Manager überprüft, dass ausgehende E-Mails, die von einer verwalteten Domain gesendet werden, die SPF- und DKIM-Validierungen bestehen. Dadurch wird sichergestellt, dass die Nachrichten authentifiziert sind und der Absender legitim ist.

ii. DMARC Manager überprüft, dass E-Mails von einer der im SPF-Eintrag aufgeführten autorisierten IP-Adressen gesendet werden, die vom Kunden oder einem Dritten im Auftrag des Kunden angegeben wurden.

e. Der Kunde kann DKIM-Schlüssel für seine Domains generieren.

i. DMARC Manager stellt sicher, dass ausgehende E-Mails von den vom Kunden oder einem Dritten im Auftrag des Kunden konfigurierten Domains mit dem DKIM-Schlüssel signiert werden.

ii. Eingehende E-Mails werden analysiert, um DKIM-Signaturen zu überprüfen.

f. DMARC Manager ermöglicht die Konfiguration und Durchsetzung von DMARC-Richtlinien, um festzulegen, wie E-Mail-Empfänger mit nicht DMARC konformen E-Mails umgehen.

i. Die vom Kunden gewählte DMARC-Richtlinie behandelt E-Mails, die die DMARC-Authentifizierung nicht bestehen. Diese Richtlinien werden pro Domain konfiguriert und legen fest, ob E-Mails abgelehnt, unter Quarantäne gestellt oder nicht angewendet werden sollen.

ii. Spezifische Richtlinien für Subdomains der Hauptdomain können vom Kunden oder einem Dritten im Auftrag des Kunden konfiguriert werden. Falls nicht explizit festgelegt, übernehmen Subdomains die Haupt-Richtlinie der Domain.

iii. Der Prozentsatz der E-Mails, die der entsprechenden DMARC-Richtlinie unterliegen, kann gesteuert werden.

iv. Zusammenfassende Berichte über den Authentifizierungsstatus der von der Domain gesendeten E-Mails sowie die Empfänger der Berichte können aktiviert werden.

g. Brand Indicators for Message Identification (BIMI) fügt E-Mails, die die DMARC-Authentifizierungsprüfungen bestehen, ein verifiziertes Markenlogo hinzu, das den Empfängern visuell anzeigt, dass die E-Mail legitim vom Kunden und der jeweiligen Marke stammt.

i. Die Nutzung von BIMI erfordert rechtliche Vorbereitungen durch den Kunden, die unabhängig von den Dienstleistungen von Hornetsecurity erfolgen. Das skalierbare Vektorgrafik-Logo (SVG), die Bestellung eines Verified Mark Certificates (VCM) und die Markenüberprüfung müssen vom Kunden beschafft werden.

ii. DMARC Manager stellt den BIMI-Eintrag bereit, der in den DNS-Einstellungen des kundenspezifischen DNS-Anbieters hinzugefügt werden muss.

h. Simple Mail Transfer Protocol - Transport Layer Security (SMTP-TLS) stellt sicher, dass E-Mails mithilfe von Verschlüsselung sicher zwischen Servern übertragen werden.

i. DMARC Manager stellt Berichte über den Erfolg und das Scheitern von TLS-Verbindungen bereit, die für die E-Mail-Übertragung zwischen Servern verwendet werden.

ii. Die Berichte enthalten Informationen wie die Identität der sendenden und empfangenden Server, Zeitstempel der Interaktionen, Arten von aufgetretenen TLS-Fehlern (falls vorhanden) und ob auf unsichere Verbindungen zurückgegriffen wurde.

i. Fehlerbericht

i. Der Fehlerbericht enthält umfassende Informationen zu einzelnen E-Mail-Vorfällen, die die DMARC-Prüfung nicht bestanden haben, einschließlich der Identität des Absenders, der Ursprungs-IP-Adresse, der E-Mail-Header-Informationen und der genauen Gründe für das Fehlschlagen der DMARC-Prüfung.

ii. Der Kunde ist dafür verantwortlich, alle erforderlichen Genehmigungen der Benutzer einzuholen und alle anwendbaren Datenschutzgesetze bei der Implementierung des Fehlerberichts einzuhalten.

iii. Der Grund für das Fehlschlagen der DMARC-Prüfung kann vom Kunden pro Domain konfiguriert werden.

iv. Der Empfänger des Fehlerberichts kann pro Domain festgelegt werden.

j. Warnmeldungen

i. DMARC Manager stellt detaillierte Informationen und Warnmeldungen zur DMARC-Überwachung und zu möglichen Problemen bereit.

ii. Die Berichte heben Quellen hervor, die E-Mails im Namen der Domain des Kunden versenden.

iii. Die Warnmeldungen benachrichtigen Kunden über potenzielle Bedrohungen oder die unbefugte Verwendung der Domain. Für eine Warnmeldung können verschiedene Empfänger hinzugefügt werden.

3. Pflichten des Kunden

a. Der Kunde ist verpflichtet, den Dienst gemäß der in diesem Dokument beschriebenen Fair-Use-Richtlinie zu nutzen und diese einzuhalten.

4. Einschränkungen und Anforderungen

a. Hornetsecurity bietet Support für autorisierte Benutzer, soweit es die Systeme von Hornetsecurity betrifft.

b. Support für Kundensysteme ist ausdrücklich von den Leistungen, die Hornetsecurity für den Kunden und die Benutzer erbringt, ausgeschlossen.

5. Haftungsausschlüsse

a. Der Kunde kann das Produkt sowohl direkt als auch indirekt konfigurieren und dabei Drittanbieterelemente integrieren. Für die Zwecke dieser Leistungsbeschreibung bezeichnet „Drittanbieterelement(e)" jedes Element, jede Information, jedes Skript, jeden Schlüssel und jede Richtlinie, die nicht von Hornetsecurity bereitgestellt werden. In einem solchen Fall kann Hornetsecurity

nicht für Schäden haftbar gemacht werden, die aus einer Konfiguration des Kunden entstehen, die nicht den Anforderungen von Hornetsecurity entspricht, oder durch jegliche Drittanbieterelemente verursacht werden.

b. Darüber hinaus kann Hornetsecurity keine Daten (Metadaten oder andere) lesen oder schreiben, wenn der Quellinhalt beschädigt ist, Fehler enthält oder anderweitig unlesbar ist, oder wenn wir durch Microsoft oder eine andere Partei, auf die wir uns zur Bereitstellung der Dienste stützen, daran gehindert werden.

c. Das Produkt und die Dienste werden im Ist-Zustand bereitgestellt. Hornetsecurity schließt ausdrücklich jegliche Zusicherungen, Bedingungen und Gewährleistungen jeglicher Art aus, ob ausdrücklich, stillschweigend, gesetzlich oder anderweitig, einschließlich, aber nicht beschränkt auf Gewährleistungen der Nichtverletzung, der Marktgängigkeit und der Eignung für einen bestimmten Zweck. Hornetsecurity garantiert nicht, dass der Zugang zum Produkt und/oder zu den Diensten, die über das Internet und verschiedene Telekommunikationsnetzwerke bereitgestellt werden, von denen alle außerhalb unserer Kontrolle liegen, fehlerfrei, ununterbrochen, zeitgerecht, sicher oder frei von Viren oder anderer Schadsoftware ist, dass sie Ihre Qualitäts- und Leistungsanforderungen erfüllen oder dass Fehler innerhalb einer vereinbarten Frist gemäß einer Service-Level-Vereinbarung behoben werden.

6. Fair Use-Richtlinie

a. Die für die Nutzung des DMARC Managers erforderliche Bandbreite, der Speicherplatz, die Infrastruktur und die Ressourcen, die Hornetsecurity in diesem Zusammenhang bereitstellt, werden zwischen allen Kunden von Hornetsecurity geteilt. Infolgedessen hat Hornetsecurity das Recht, Maßnahmen zu ergreifen, um sicherzustellen, dass alle Kunden die Lösungen in einer angemessenen und fairen Weise nutzen, damit eine solche Nutzung die normale Serviceleistung für andere Kunden nicht beeinträchtigt oder verhindert.

b. Hornetsecurity hat beschlossen, keine vordefinierten Benchmarks festzulegen, die eine übermäßige oder unangemessene Nutzung bestimmen, da Hornetsecurity nach eigenem Ermessen entscheiden kann, die normalen Servicelevels beizubehalten, indem Ressourcen, die für andere Benutzer reserviert sind und in diesem Moment nicht genutzt werden, umverteilt werden, oder Ressourcen anderweitig skaliert werden. Der Kunde versteht, dass, wenn Hornetsecurity beschließt, seine Fair-Use-Richtlinie nicht aktiv durchzusetzen, dies nicht als Verzicht auf das Recht von Hornetsecurity ausgelegt wird, dies zu tun, noch dem Kunden das Recht eingeräumt wird, die Dienste von Hornetsecurity weiterhin zu nutzen.

c. Um von den Diensten von Hornetsecurity zu profitieren, muss der Kunde abrechenbare Einheiten erwerben. Die Anzahl der erforderlichen abrechenbaren Einheiten hängt von einer Reihe von Kriterien ab, wie der Größe der Organisation des Kunden, der Anzahl der Benutzer usw.

d. Unabhängig von der Anzahl der erworbenen abrechenbaren Einheiten muss der Kunde die Dienste von Hornetsecurity sinnvoll nutzen, insbesondere in einer Weise, die nicht erfordert, dass Hornetsecurity unverhältnismäßig viele Ressourcen zuweist. Zur Bestimmung dieses Sachverhalts wird Hornetsecurity die Ressourcennutzung des Kunden (z. B. Speicheranforderungen, Anzahl der parallelen Verbindungen) mit der eines durchschnittlichen Kunden vergleichen. Hornetsecurity bestimmt den durchschnittlichen Kunden, indem die 5 % der höchsten Kunden und die 5 % der niedrigsten Kunden bei den jeweiligen Ressourcen außer Acht gelassen und der Wert zwischen allen aktiven Kunden von Hornetsecurity gemittelt wird.

e. Spezifische Merkmale der Branche, in der der Kunde tätig ist, werden bei der Feststellung, ob die Nutzung als angemessen angesehen wird, nicht berücksichtigt.

f. Wenn Hornetsecurity nach vernünftigem Ermessen und in gutem Glauben der Ansicht ist, dass die Nutzung der Hornetsecurity-Lösungen durch den Kunden nicht angemessen ist oder gegen diese Richtlinie verstößt, kann Hornetsecurity nach eigenem Ermessen eine der folgenden Maßnahmen ergreifen:

g. Dem Kunden die weitere Nutzung der Hornetsecurity-Lösungen erlauben, jedoch unter der Bedingung der Zahlung zusätzlicher Gebühren und der Einhaltung aller Bedingungen, die Hornetsecurity unter den gegebenen Umständen für angemessen hält.

h. Den Kunden darüber informieren, dass sein Konto innerhalb eines von Hornetsecurity festgelegten angemessenen Zeitraums gekündigt wird. In dieser Zeit werden alle Dienste und/oder Vorgänge ausgesetzt.

i. Wenn Hornetsecurity sein Recht zur Kündigung des Kontos des Kunden wie oben erwähnt ausübt:

j. Alle Daten (Metadaten oder andere) werden am Ende des von Hornetsecurity in der diesbezüglichen Benachrichtigung festgelegten Zeitraums gelöscht, ungeachtet entgegenstehender Bestimmungen in den Allgemeinen Geschäftsbedingungen.

k. Der Kunde erhält eine Rückerstattung der im Voraus gezahlten Gebühren für die verbleibenden Tage seiner Abonnementlaufzeit.