CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

DKIM-INTEGRATION UND -IMPLEMENTIERUNG

Inhalt

DOKUMENTENKONTROLLE UND -PRÜFUNG

Dokumentenkontrolle	
Autor	
Eigentümer	
Datum der Erstellung	
Zuletzt überarbeitet von	
Datum der letzten Überarbeitung	

.

VERSIONSKONTROLLE

Version	Datum der Genehmigung	Genehmigt durch	Beschreibung der Änderung

Einführung: die Notwendigkeit der DKIM-Implementierung

E-Mail ist einer der am häufigsten genutzten Kommunikationskanäle in Unternehmen und spielt eine entscheidende Rolle bei Geschäftsprozessen. Die Bequemlichkeit und Zugänglichkeit von E-Mails machen sie jedoch auch zu einem beliebten Ziel für Cyberkriminelle. Phishing, Spoofing und andere Formen des E-Mail-Betrugs stellen eine ernsthafte Bedrohung für die Sicherheit und Zuverlässigkeit des E-Mail-Verkehrs dar.
Um diese Risiken zu mindern und die Glaubwürdigkeit der E-Mail-Kommunikation zu gewährleisten, müssen Unternehmen unbedingt starke E-Mail-Authentifizierungsmechanismen einsetzen. Eine der wirksamsten Methoden hierfür ist **DomainKeys Identified Mail (DKIM)**. DKIM bietet eine leistungsfähige Möglichkeit, die Integrität und Authentizität ausgehender E-Mails zu gewährleisten und sowohl den Absender als auch den Empfänger zu schützen.

1. Warum DKIM?

1.1 STÄRKUNG DES VERTRAUENS IN DIE E-MAIL-KOMMUNIKATION

Mit DKIM lässt sich nachweisen, dass eine E-Mail tatsächlich von dem angegebenen Absender stammt. Dies erhöht das Vertrauen in E-Mails, die von Ihrer Domäne aus gesendet werden, was für die Kommunikation mit Kunden, Partnern und internen Stakeholdern unerlässlich ist.

1.2 SCHUTZ VOR E-MAIL-SPOOFING

Spoofing ist eine Technik, bei der Angreifer eine gefälschte E-Mail-Adresse verwenden, um Vertrauen aufzubauen und die Opfer zu täuschen. DKIM macht es Angreifern schwerer, legitime Domänennamen zu missbrauchen, da die Authentizität von E-Mails kryptografisch überprüft werden kann.

1.3 VERBESSERUNG DER ZUSTELLBARKEIT VON E-MAILS

Internet Service Provider (ISP) und E-Mail-Anbieter wie Gmail, Outlook und Yahoo! verwenden DKIM, um festzustellen, ob eine E-Mail als legitim anzusehen ist. E-Mails ohne DKIM-Signatur werden unter Umständen als verdächtig eingestuft und landen im Spam-Ordner, auch wenn sie legitim sind. DKIM trägt daher zu einer höheren Zustellungsrate bei.

1.4 TEIL EINER UMFASSENDEREN E-MAIL-SICHERHEITSSTRATEGIE

DKIM arbeitet nahtlos mit anderen E-Mail-Authentifizierungsmechanismen wie **SPF (Sender Policy Framework)** und **DMARC (Domain-based Message Authentication, Reporting, and Conformance)** zusammen. Gemeinsam bilden diese Technologien ein integriertes System zur Bekämpfung von E-Mail-Betrug und zur Verringerung des Risikos von Datenlecks.

1.5 KONFORMITÄT UND RECHTLICHE ANFORDERUNGEN

In Bereichen wie Finanzdienstleistungen, Gesundheitswesen und Behörden gibt es immer strengere Anforderungen an den Datenschutz und die Betrugsbekämpfung. Die Implementierung von DKIM kann dazu beitragen, Standards und Vorschriften wie die **DSGVO (Datenschutz-Grundverordnung) zu** erfüllen.

1.6 SCHUTZ DES RUFS DES UNTERNEHMENS

Eine kompromittierte E-Mail-Infrastruktur kann dem Ruf eines Unternehmens schweren Schaden zufügen. DKIM hilft zu verhindern, dass Ihr Domänenname für böswillige Zwecke, wie z. B. den Versand von Phishing-E-Mails, verwendet wird.

2. Schlussfolgerung

Angesichts der zunehmenden Häufigkeit und Komplexität von E-Mail-Bedrohungen ist die Implementierung von DKIM kein Luxus, sondern eine Notwendigkeit. DKIM bietet eine kostengünstige Lösung, um die Zuverlässigkeit von E-Mails zu gewährleisten, E-Mail-Betrug zu verhindern und die allgemeine Sicherheit Ihres Unternehmens zu verbessern. In diesem Beitrag wird erläutert, wie DKIM technisch funktioniert, welche Vorteile die Implementierung bietet und welche Schritte erforderlich sind, um diese Technologie in Ihrem Unternehmen erfolgreich einzuführen. Durch eine sorgfältige Implementierung und regelmäßige Überwachung können Sie die E-Mail-Sicherheit erheblich verbessern. In Kombination mit SPF und DMARC bildet DKIM eine robuste Verteidigung gegen E-Mail-Missbrauch.

3. DKIM: Technische Erläuterung und Umsetzung

3.1. WAS IST DKIM?

DKIM (DomainKeys Identified Mail) ist ein E-Mail-Überprüfungsmechanismus, der sicherstellt, dass eine E-Mail während der Übertragung nicht verändert wurde. Er funktioniert durch Hinzufügen einer digitalen Signatur zu einer E-Mail, die vom empfangenden Mailserver überprüft werden kann.

- **Wesentliche Merkmale**:
  - Überprüfung des Absenders.
  - Sicherstellung der Integrität von E-Mail-Inhalten.
  - Verhinderung der Manipulation von E-Mails während der Übertragung.

3.2. WIE FUNKTIONIERT DKIM?

3.2.1 SCHLÜSSELBEGRIFFE

1. **Digitale Unterschrift**:
   - Der sendende Server erzeugt eine kryptografische Signatur mit einem privaten Schlüssel.
   - Diese Signatur wird in den DKIM-Header der E-Mail aufgenommen.
2. **Öffentlicher Schlüssel im DNS**:
   - Der öffentliche Schlüssel, der mit dem privaten Schlüssel verbunden ist, wird in einem DNS-TXT-Eintrag veröffentlicht.
   - Die Empfangsserver verwenden diesen öffentlichen Schlüssel, um die Signatur zu v.alidieren.
   - DNSSEC sorgt dafür, dass der DNS-Lookup auch kryptografisch authentifiziert wird
3. **Selektor**:
   - Eine eindeutige Kennung, die angibt, welcher Schlüssel für die Signatur verwendet wurde. Dies ermöglicht die Verwaltung mehrerer Schlüssel.

3.2.2 TECHNISCHE FUNKTIONSWEISE VON DKIM

1. **Erzeugung von Unterschriften**:
   - Der sendende Mailserver wählt bestimmte Teile der E-Mail aus, die signiert werden sollen, z. B.:
     - Kopfzeilen: 'From', 'To', 'Subject'.
     - Der Text der E-Mail.
   - Ein Hash-Algorithmus (z. B. SHA-256) wird verwendet, um einen Hash der ausgewählten Teile zu erstellen.
   - Dieser Hash wird mit dem privaten Schlüssel verschlüsselt und ergibt die DKIM-Signatur.

2. **Hinzufügen des DKIM-Headers**:
   - Die Signatur wird der E-Mail als neue Kopfzeile hinzugefügt. Ein typischer DKIM-Header sieht wie folgt aus:

     ```
     DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=example.com; s=selector1;
     h=from:to:subject:date; bh=base64_body_hash;
     b=base64_signatur
     ```

     - **v=1**: DKIM-Version.

        - **a=rsa-sha256**: Signaturalgorithmus.
        - **d=example.com**: Die Domäne des Absenders.
        - **s=selector1**: Selektor für den öffentlichen Schlüssel im DNS.
        - **h=from:to:subject:date**: Beim Signieren verwendete Kopfzeilen.
        - **bh=base64_body_hash**: Hash des Textes der E-Mail.
        - **b=base64_signature**: Die digitale Signatur.
3. **Validierung durch den Empfangsserver**:
    - Der Empfangsserver ruft den öffentlichen Schlüssel der Domäne über DNS ab.
    - Der Server verwendet diesen öffentlichen Schlüssel, um:
        - Den Body-Hash neu zu berechnen.
        - Die Signatur zu entschlüsseln.
        - Die Werte zu vergleichen, um zu prüfen, ob die E-Mail unverändert ist.

4. Vorteile von DKIM

- **Integritätsprüfung**: DKIM garantiert, dass der Inhalt einer E-Mail während der Übertragung nicht verändert wurde.
- **Bessere Spam-Filterung**: Viele E-Mail-Anbieter geben verifizierten E-Mails eine höhere Punktzahl, was die Zustellung verbessert.
- **Schutz der Domain-Reputation**: Verringert die Wahrscheinlichkeit des Missbrauchs von Domains beim Phishing.

5. Schritte zur Implementierung von DKIM

5.1 OFFICE 365

https://learn.microsoft.com/en-us/defender-office-365/email-authentication-dkim-configure

5.2 GCP

https://support.google.com/a/answer/174124?hl=en

6. Bewährte Praktiken für DKIM

1. **Verwenden Sie eine starke Kryptographie**:
   - Verwenden Sie mindestens RSA-2048-Bit-Schlüssel, um Quantencomputer-resistente Sicherheit zu gewährleisten.
2. **Rotieren Sie die Schlüssel regelmäßig**:
   - Planen Sie eine jährliche Rotation der DKIM-Schlüssel, um das Risiko zu minimieren.
3. **Verwalten Sie Selektoren sorgfältig**:
   - Verwenden Sie eindeutige Selektoren für verschiedene Umgebungen (z. B. prod1, test1), um die Verwaltung zu erleichtern.
4. **Kombinieren Sie mit SPF und DMARC**:
   - DKIM allein bietet keinen vollständigen Schutz gegen Spoofing. Kombinieren Sie es mit SPF und DMARC für umfassende E-Mail-Sicherheit.
5. **Prüfen Sie auf Fehlkonfigurationen**:
   - Abgelaufene oder unsachgemäß konfigurierte DKIM-Einträge können E-Mails blockieren. Testen Sie regelmäßig mit Überwachungstools (https://nl.internet.nl/).

7. Mögliche Fehler und Lösungen

Problem: "Keine DKIM-Signatur gefunden"

- **Ursache**: Der Mailserver ist nicht korrekt für das Signieren von E-Mails konfiguriert.
- **Lösung**: Überprüfen Sie die Konfiguration und stellen Sie sicher, dass der richtige private Schlüssel verwendet wird.

Problem: "DKIM-Validierung fehlgeschlagen"

- **Ursache**: Der öffentliche Schlüssel im DNS stimmt nicht mit dem privaten Schlüssel überein.
- **Lösung**: Veröffentlichen Sie den richtigen öffentlichen Schlüssel im DNS-TXT-Eintrag.

Haftungsausschluss