CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

DKIM INTEGRATIE & IMPLEMENTATIE.

Inhoud

Document control and review 2

Version control 3

Inleiding: De noodzaak van DKIM-implementatie 4

1 Waarom DKIM? 4

1.1 Vertrouwen in e-mailcommunicatie vergroten 4

1.2 Bescherming tegen e-mailspoofing 4

1.3 Verbetering van de e-mailafleverbaarheid 4

1.4 Onderdeel van een bredere e-mailbeveiligingsstrategie 4

1.5 Compliance en wettelijke vereisten 4

1.6 Bescherming van de bedrijfsreputatie 4

2. Conclusie 5

3. DKIM: Technische Uitleg en Implementatie 5

3.1. Wat is DKIM? 5

3.2. Hoe werkt DKIM? 5

3.2.1 Belangrijke concepten 5

3.2.2 Technische werking van DKIM 5

4. Voordelen van DKIM 6

5. Stappen voor implementatie van DKIM 6

5.1 Office 365 6

5.2 GCP 6

6. Best Practices voor DKIM 7

7. Mogelijke fouten en oplossingen 7

DOCUMENT CONTROL AND REVIEW

Document Control	
Author	
Owner	
Date created	
Last revised by	
Last revision date	

.

VERSION CONTROL

Version	Date of approval	Approved by	Description of change

Inleiding: De noodzaak van DKIM-implementatie

E-mail is een van de meest gebruikte communicatiekanalen binnen organisaties en speelt een cruciale rol in bedrijfsprocessen. Het gemak en de toegankelijkheid van e-mail maken het echter ook tot een populair doelwit voor cybercriminelen. Phishing, spoofing en andere vormen van e-mailfraude vormen een ernstige bedreiging voor de veiligheid en betrouwbaarheid van e-mailverkeer.
Om deze risico's te mitigeren en de geloofwaardigheid van e-mailcommunicatie te waarborgen, is het noodzakelijk dat organisaties sterke e-mailauthenticatiemechanismen implementeren. Een van de meest effectieve methoden hiervoor is **DomainKeys Identified Mail (DKIM)**. DKIM biedt een krachtige manier om de integriteit en authenticiteit van uitgaande e-mails te garanderen, met als doel zowel de verzender als de ontvanger te beschermen.

1 Waarom DKIM?

1.1 VERTROUWEN IN E-MAILCOMMUNICATIE VERGROTEN

DKIM helpt bij het vaststellen dat een e-mail daadwerkelijk afkomstig is van de geclaimde verzender. Dit verhoogt het vertrouwen in e-mails die vanuit uw domein worden verzonden, wat essentieel is voor communicatie met klanten, partners en interne stakeholders.

1.2 BESCHERMING TEGEN E-MAILSPOOFING

Spoofing is een techniek waarbij aanvallers een vals e-mailadres gebruiken om vertrouwen te wekken en slachtoffers te misleiden. DKIM maakt het moeilijker voor aanvallers om legitieme domeinnamen te misbruiken, doordat de authenticiteit van e-mails cryptografisch kan worden gevalideerd.

1.3 VERBETERING VAN DE E-MAILAFLEVERBAARHEID

Internet Service Providers (ISP's) en e-mailproviders zoals Gmail, Outlook en Yahoo! gebruiken DKIM om te bepalen of een e-mail als legitiem moet worden beschouwd. E-mails zonder DKIM-handtekening kunnen als verdacht worden gemarkeerd en in de spamfolder terechtkomen, zelfs als ze legitiem zijn. DKIM draagt daarom bij aan een hogere afleveringsratio.

1.4 ONDERDEEL VAN EEN BREDERE E-MAILBEVEILIGINGSSTRATEGIE

DKIM werkt naadloos samen met andere e-mailauthenticatiemechanismen zoals **SPF (Sender Policy Framework)** en **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**. Samen vormen deze technologieën een geïntegreerd systeem om e-mailfraude te bestrijden en het risico op gegevenslekken te verkleinen.

1.5 COMPLIANCE EN WETTELIJKE VEREISTEN

In sectoren zoals financiële dienstverlening, gezondheidszorg en overheid worden steeds strengere eisen gesteld aan gegevensbescherming en het voorkomen van fraude. Het implementeren van DKIM kan bijdragen aan het voldoen aan normen en regelgeving, zoals de **AVG (Algemene Verordening Gegevensbescherming)**.

1.6 BESCHERMING VAN DE BEDRIJFSREPUTATIE

Een gecompromitteerde e-mailinfrastructuur kan ernstige schade toebrengen aan de reputatie van een organisatie. DKIM helpt voorkomen dat uw domeinnaam wordt gebruikt voor kwaadaardige doeleinden, zoals het verzenden van phishingmails.

2. Conclusie

Gezien de toenemende frequentie en complexiteit van e-mail gerelateerde dreigingen is het implementeren van DKIM geen luxe, maar een noodzaak. DKIM biedt een kosteneffectieve oplossing om de betrouwbaarheid van e-mails te waarborgen, e-mailfraude te voorkomen en de algehele veiligheid van uw organisatie te verbeteren. In dit document zullen we dieper ingaan op de technische werking van DKIM, de voordelen van implementatie en de stappen die nodig zijn om deze technologie succesvol te implementeren binnen uw organisatie. Door het zorgvuldig te implementeren en regelmatig te monitoren, kun je e-mailbeveiliging aanzienlijk verbeteren. In combinatie met SPF en DMARC creëert DKIM een robuuste verdediging tegen e-mailmisbruik

3. DKIM: Technische Uitleg en Implementatie

3.1. WAT IS DKIM?

DKIM (DomainKeys Identified Mail) is een e-mailverificatiemechanisme dat ervoor zorgt dat een e-mail niet is gewijzigd tijdens transport. Het werkt door een digitale handtekening aan een e-mail toe te voegen, die kan worden gevalideerd door de ontvangende mailserver.

- **Belangrijkste functies**:
  - Verificatie van de afzender.
  - Waarborging van de integriteit van de e-mailinhoud.
  - Preventie van e-mailmanipulatie tijdens transport.

3.2. HOE WERKT DKIM?

3.2.1 BELANGRIJKE CONCEPTEN

1. **Digitale handtekening**:
   - De verzendende server genereert een cryptografische handtekening met een private sleutel.
   - Deze handtekening wordt opgenomen in de DKIM-header van de e-mail.
2. **Publieke sleutel in DNS**:
   - De publieke sleutel die bij de private sleutel hoort, wordt gepubliceerd in een DNS TXT-record.
   - Ontvangende servers gebruiken deze publieke sleutel om de handtekening te valideren.
   - DNSSEC zorgt ervoor dat ook de DNS lookup cryptografisch geauthentiseerd wordt
3. **Selector**:
   - Een unieke identifier die aangeeft welke sleutel gebruikt is voor de handtekening. Dit maakt het mogelijk om meerdere sleutels te beheren.

3.2.2 TECHNISCHE WERKING VAN DKIM

1. **Genereren van de handtekening**:
   - De verzendende mailserver selecteert specifieke delen van de e-mail om te ondertekenen, zoals:
     - Headers: "From", "To", "Subject".
     - De body van de e-mail.
   - Met een hashing-algoritme (bijvoorbeeld SHA-256) wordt een hash van de geselecteerde delen gemaakt.
   - Deze hash wordt versleuteld met de private sleutel, wat de DKIM-handtekening oplevert.

2. **Toevoegen van de DKIM-header**:
   - De handtekening wordt toegevoegd aan de e-mail als een nieuwe header. Een typische DKIM-header ziet er als volgt uit:

     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_signature

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

        - **a=rsa-sha256**: Algoritme voor de handtekening.
        - **d=example.com**: Het domein van de verzender.
        - **s=selector1**: Selector voor de publieke sleutel in DNS.
        - **h=from:to:subject:date**: Headers die zijn gebruikt bij het ondertekenen.
        - **bh=base64_body_hash**: Hash van de body van de e-mail.
        - **b=base64_signature**: De digitale handtekening.

3. **Validatie door de ontvangende server**:
    - De ontvangende server haalt de publieke sleutel van het domein op via DNS.
    - De server gebruikt deze publieke sleutel om:
        - De body-hash opnieuw te berekenen.
        - De handtekening te decoderen.
        - De waarden te vergelijken om te controleren of de e-mail ongewijzigd is.

4. Voordelen van DKIM

- **Integriteitscontrole**: DKIM garandeert dat de inhoud van een e-mail niet is gewijzigd tijdens transport.
- **Betere spamfiltering**: Veel e-mailproviders geven hogere scores aan geverifieerde e-mails, wat de aflevering verbetert.
- **Bescherming van domeinreputatie**: Verkleint de kans op misbruik van het domein bij phishing.

5. Stappen voor implementatie van 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. Best Practices voor DKIM

1. **Gebruik sterke cryptografie**:
   - Gebruik minimaal RSA 2048-bit sleutels om quantumcomputing-resistente beveiliging te bieden.
2. **Roteer sleutels regelmatig**:
   - Plan jaarlijkse rotatie van DKIM-sleutels om risico's te minimaliseren.
3. **Beheer selectors zorgvuldig**:
   - Gebruik unieke selectors voor verschillende omgevingen (bijvoorbeeld prod1, test1) om beheer te vergemakkelijken.
4. **Combineer met SPF en DMARC**:
   - DKIM alleen beschermt niet volledig tegen spoofing. Combineer het met SPF en DMARC voor uitgebreide e-mailbeveiliging.
5. **Controleer op misconfiguraties**:
   - Verlopen of onjuist geconfigureerde DKIM-records kunnen e-mails blokkeren. Test regelmatig met monitoringtools.(https://nl.internet.nl/)

7. Mogelijke fouten en oplossingen

Probleem: "No DKIM signature found"

- **Oorzaak**: De mailserver is niet correct geconfigureerd om e-mails te ondertekenen.
- **Oplossing**: Controleer de configuratie en zorg dat de juiste private sleutel wordt gebruikt.

Probleem: "DKIM validation failed"

- **Oorzaak**: De publieke sleutel in DNS komt niet overeen met de private sleutel.
- **Oplossing**: Publiceer de correcte publieke sleutel in het DNS TXT-record.

Disclaimer