Whitepaper

E-mail security

SPF, DKIM & DMARC

Leusden, 7 oktober 2021

Versie 1.0

Leusderend 38, 3832 RC LEUSDEN info@access42.nl www.access42.nl

Inhoudsopgave

1. SPF, DKIM & DMARC

Zorg dat u goed beveiligd bent op het gebied van e-mail security.

Steeds meer aanvallen komen binnen via een email. Om die reden is het van groot belang dat uw e-mail security op orde is. Om beter te begrijpen hoe deze aanvallen kunnen worden tegengegaan, moet men eerst de aanvallen zelf begrijpen, dus laten we eens kijken naar de meest voorkomende email bedreigingen die er momenteel zijn. De volgende aanvallen worden onderstaand beschreven:

- Phishing
- Spear-Phishing
- Email spoofing

1.1 Phishing

Phishing is de poging om gevoelige informatie te verkrijgen, zoals gebruikersnamen, wachtwoorden en creditcard kaartgegevens, vaak met kwade bedoelingen, door zich voor te doen als een betrouwbare entiteit in een digitale omgeving. De berichten lijken afkomstig te zijn van gewone websites, veilingsites, banken, online betalingsverwerkers of IT-beheerders en kunnen links bevatten naar websites die met malware besmet zijn en/of de ontvanger vragen persoonlijke informatie vrij te geven.

1.2 Spear-Phishing

Spear-Phishing is een meer geavanceerde techniek van phishing. Het algeheel lijkt veel op de normale phishing methode. Echter wordt er bij spear-phishing vaak een specifiek doelwit uitgekozen. De email wordt vervolgens helemaal gecreëerd om die ene persoon te overtuigen dat het legitiem is. Emotie wordt hierin vaak toegepast zoals urgente betaling, wijzig snel je wachtwoord. Er wordt vanuit de aanvaller een gevoel gecreëerd dat de gebruiker snel moet handelen. Zodat de gebruiker geen boete krijgt i.v.m. een te late betaling of geen toegang meer heeft tot.

1.3 Email spoofing

Spoofing van e-mail is een techniek die bij spam- en phishingaanvallen wordt gebruikt om gebruikers wijs te maken dat een bericht afkomstig is van een persoon of entiteit die zij kennen of kunnen vertrouwen. Bij spoofingaanvallen vervalst de afzender de e-mailheaders, zodat clientsoftware het frauduleuze afzenderadres weergeeft, dat de meeste gebruikers voor waar aannemen. Tenzij zij de header nader inspecteren, zien

gebruikers de vervalste afzender in een bericht. Als het een naam is die ze herkennen, is de kans groter dat ze die vertrouwen. Dus klikken ze op schadelijke koppelingen, openen ze malwarebijlagen, verzenden ze gevoelige gegevens en maken ze zelfs bedrijfsgelden over.

Microsoft: 91 procent van de cyberaanvallen begint met een e-mail (Security.nl, 2020)

2. Voorkomen van e-mail aanvallen

Om email aanvallen te voorkomen kan een organisatie gebruik maken van de drie protocollen:

- SPF
- DKIM
- DMARC

2.1 SPF

Sender Policy Framework (SPF) beveiligt uw DNS servers en beperkt wie e-mails van uw domein kan versturen. SPF kan domain spoofing voorkomen. Het stelt uw mailserver in staat te bepalen wanneer een bericht afkomstig is van het domein dat hij gebruikt. SPF heeft drie belangrijke elementen: een beleidskader, zoals de naam al aangeeft, een verificatiemethode en gespecialiseerde headers in de e-mail zelf die deze informatie overbrengen. SPF werd voor het eerst voorgesteld in IETF-standaard 4408 in 2006, en werd recentelijk bijgewerkt tot standaard 7208 in 2014. De record tags die bij SPF gebruikt kunnen worden zijn hier (https://mxtoolbox.com/dmarc/spf/spf-record-tags) te vinden.

Een SPF-beleid voor het domein ‘example.nl’ kan er als volgt uitzien:

```
example.nl. TXT "v=spf1 mx a:mail.example.nl/28 ~all"
```

Het beleid in dit voorbeeld geeft aan:

- **V:** de versie van het protocol.
- **mx:** de inkomende mailservers mogen ook e-mail versturen.
- **~all:** alle andere mailservers mogen geen e-mail versturen namens deze domeinnaam.
- **a:mail.example.nl/28:** de mailservers die binnen dit bereik vallen zijn geautoriseerd voor het versturen van e-mail.

2.2 DKIM

DomainKeys Identified Mail (DKIM) zorgt ervoor dat de inhoud van uw e-mails vertrouwd blijft en dat er niet mee geknoeid is of dat de inhoud niet in gevaar komt. De standaard werd voor het eerst voorgesteld in 2007 en is verschillende keren bijgewerkt, voor het laatst met de IETF standaard 8301 afgelopen januari. Zowel SPF als DKIM zijn in 2014 bijgewerkt met de IETF-standaard 7372. De record tags die bij DKIM gebruikt kunnen worden zijn hier (https://blog.mxtoolbox.com/2020/11/28/dkim-signature-tags-a-primer/) te vinden.

2.3 DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC) koppelt de eerste twee protocollen aan elkaar met een consistente reeks beleidslijnen. Het koppelt ook de domeinnaam van de afzender aan wat er in de From: header staat. Het werd in 2015 voorgesteld als een IETF-standaard 7489. DMARC bestaat uit een TXT-record dat toegevoegd wordt aan de desbetreffende DNS-zone. Hierin staat het volgende:

Tag	Description
Version (v)	De v tag is verplicht en staat voor de versie van het protocol. Een voorbeeld is v=DMARC1
Policy (p)	wat de ontvanger moet doen met email die niet voldoet aan DKIM- of SPF-beleid (none, quarantine of reject)
Percentage (pct)	Een optioneel percentage [pct] dat aangeeft op welk deel van de e-mailstroom het DMARC-beleid toegepast moet worden.
RUA Report Email Address(s) (rua):	Het e-mailadres [rua] waarnaar de ontvangende mailproviders de rapportages kunnen sturen.
RUF Report Email Address(s) (ruf):	Het e-mailadres [ruf] waarnaar de ontvangende mailproviders de inhoud van vervalste e-mails kunnen sturen.

3. Advies Access42

Het advies van Access42 is om elke domeinnaam van uw organisatie te voorzien van een e-mailauthenticatie met behulp van SPF, DKIM en DMARC. Daarnaast adviseert Access42 om al het uitgaande e-mailverkeer te ondertekenen met behulp van DKIM.

In de eerste fase **(plan)** wordt een overzicht gecreëerd van de domeinnamen, e-mailstromen en soorten e-mail. Dit overzicht omvat zowel domeinnamen waarvandaan e-mail wordt verstuurd als domeinnamen waarvandaan nooit wordt gemaild. Veel van deze informatie zal binnen de organisatie aanwezig zijn. Een DMARC-implementatie, zelfs zonder SPF en DKIM, kan gebruikt worden om ontbrekende informatie in kaart te brengen. De verzamelde informatie wordt geanalyseerd op basis van de gestelde emailauthenticatiedoelen, zoals het voorkomen van ongeautoriseerde e-mailstromen.

In de tweede fase **(do)** worden de maatregelen geïmplementeerd. Het kan hierbij gaan om nieuwe implementaties of het doorvoeren van benodigde wijzigingen in configuraties. In de derde fase **(check)** zal de implementatie, configuratie en gebruik van de e-mailauthenticatiemiddelen gemonitord moeten worden om effectief te zijn. Let onder andere op misbruik van een domeinnaam, problemen met geautoriseerde verzenders en aanpassingen aan mailservers. De rapportages die door DMARC gegenereerd worden, kunnen hierbij van waarde zijn. Continu worden problemen en bijbehorende maatregelen geïdentificeerd. De vierde en laatste fase **(act)** is van belang om te zorgen dat de maatregelen die in de vorige stap op een continue basis worden geïdentificeerd ook worden toegepast.

3.1 Technisch stappenplan

1. Maak een DMARC-record aan voor elke domeinnaam. Gebruik de eerste periode (bijvoorbeeld: twee weken) als policy de waarde ‘none’ en specificeer een e-mailadres waar mailservers de rapportages aan kunnen sturen.
2. Gebruik de rapportages om e-mailstromen die niet voldoen aan het SPF- en DKIM-beleid te verhelpen en ‘identifier alignment’-problemen te corrigeren. Dit is ook een gelegenheid om e-mail te herkennen die wel SPF-controles doorkomt, maar niet voldoet aan het DKIM-beleid. Deze e-mails zullen ongetwijfeld problemen opleveren bij forwarding.
3. Controleer of het SPF-beleid al is toegevoegd aan een domeinnaam door het TXT-record in de DNS op te zoeken. Publiceer een SPF-beleid als een TXT-record in de DNS-zone van de desbetreffende domeinnaam. Maak gebruik van een softfail-policy om false positives te voorkomen. Zorg daarnaast dat voor alle domeinnamen waarvandaan in het geheel geen mail wordt verstuurd, een SPF-beleid is opgenomen met waarde ' v=spf1 –all’ om misbruik ervan zoveel mogelijk tegen te gaan.

4. Genereer publieke en private sleutels (van minstens 2048 bit RSA). Voeg de publieke sleutel toe als een TXT-record aan de DNS-zone van de desbetreffende domeinnaam. Zorg dat de Signing identity (d=) exact overeenkomt met de From: header-domeinnaam, vergelijkbaar met strikte alignment in DMARC. Gebruik een apart sleutelpaar en een aparte selector per organisatie en genereer regelmatig (bijvoorbeeld twee keer per jaar) een nieuw sleutelpaar om de DKIM-handtekening mee te maken.
5. Stap na de eerste periode over naar een striktere policy. Zijn voor een bepaalde domeinnaam alle mailservers opgenomen in het SPF-beleid en wordt al het e-mailverkeer ondertekend met DKIM, publiceer dan een policy ‘quarantine’ met een kleine waarde voor ‘pct’. Debug false positives (wegens gemiste mailstromen) en schroef de waarde van ‘pct’ langzaam op. Staat ‘pct’ op een waarde van 100 zonder nadelige effecten, publiceer dan een policy ‘reject’ met een kleine waarde voor ‘pct’. Herhaal de debugging en pas de waarde aan. Het doel is om uiteindelijk zoveel mogelijk mailstromen te laten authenticeren door ze ‘reject’ als beleid mee te geven.