Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Bescherm domeinen tegen phishing

Beperk e-mailspoofing met SPF, DKIM en DMARC

Handreiking | versie 2.0 | 20 december 2023

Voorkom e-mailspoofing en phishing door je domeinen te beschermen met e-mailauthenticatie. Met phishing worden valse e-mails gestuurd met misleidende inhoud, om zo de ontvanger te verleiden malafide software te downloaden of informatie prijs te geven. Aanvallers beschikken over diverse technieken om de kans op een succes te vergroten. Het vervalsen van domeinnamen ('spoofing') is daar een voorbeeld van. Spoofing bemoeilijkt voor de ontvanger het herkennen van phishingmails, doordat de e-mails in kwestie lijken te komen van het e-mailadres van een betrouwbare organisatie. Organisaties die hun domeinnamen niet beschermen tegen e-mailspoofing, kunnen als gevolg van misbruik schade veroorzaken bij ontvangers en daar ook zelf reputatieschade door oplopen. Bovendien kan de afleveringszekerheid van e-mail in gevaar komen. Ontvangende mailservers laten e-mails zonder mailauthenticatie namelijk steeds vakers niet meer aankomen in de mailboxen van ontvangers.

Het NCSC adviseert om iedere domeinnaam van je organisatie te beschermen door e-mailauthenticatie met behulp van SPF, DKIM en DMARC. Voor overheden geldt een verplichte toepassing van SPF, DKIM en DMARC omdat deze zijn opgenomen in de 'pas toe of leg uit'-lijst. Voor alle overige organisaties geldt een dringend advies deze standaarden te implementeren.

Doelgroep

E-mail beheerders, DNS-beheerders, security officers.

Samenwerkingspartners

Aan deze handreiking hebben bijgedragen: de Belastingdienst, UWV en Forum Standaardisatie.

Achtergrond

Phishing via e-mail wordt nog steeds veelvuldig gebruikt door aanvallers om toegang te krijgen tot gegevens of netwerken.[1] Aanvallers kunnen kiezen uit diverse mogelijkheden en trucs om gebruikers van e-mail te misleiden. Phishing is er in vele vormen en gedaanten, waarbij diverse beïnvloedingstechnieken worden ingezet om ontvangers te misleiden. Te denken valt aan zeer gerichte aanvallen van statelijke actoren waarbij gebruik wordt gemaakt van voorkennis ('spearphishing'), of meer generieke aanvallen met een financieel oogmerk gericht op bedrijven ('business e-mail compromise'). Welke vorm het ook betreft, phishing buit de menselijke factor in de verdedigingsketen uit; de schakel waar de kans op succes hoog is.

Een van de aanvalstechnieken die kunnen worden ingezet om de kans op succes bij phishing te vergroten is 'spoofing'. Bij spoofing wordt misbruik gemaakt van de wijze waarop het e-mailprotocol is opgebouwd. Zonder implementatie van e-mailauthenticatie - met SPF, DKIM en DMARC - wordt de afzenddomeinnaam niet geverifieerd, waardoor aanvallers e-mails kunnen opstellen waarbij het lijkt alsof het van een betrouwbare

[1] Zie het IOCTA rapport uit 2023: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf

organisatie afkomstig is. Als een gebruiker een gespoofde e-mail ontvangt, lijkt deze bijvoorbeeld verzonden van info@example.nl terwijl deze in werkelijkheid van een malafide partij afkomstig is.

Phishing e-mails die met behulp van spoofing worden vervalst, zijn hierdoor erg lastig voor de ontvangende partij om te herkennen. Bovendien heeft dit een zeer nadelig effect op de organisatie die eigenaar is van de misbruikte domeinnaam. Mogelijk bestempelen e-mailproviders de organisatie als verzender van phishingmail, waardoor ook legitieme berichten niet meer kunnen worden ontvangen. Daarnaast is het slecht voor het imago en kan er reputatieschade ontstaan.

Het NCSC adviseert om elke domeinnaam van je organisatie te beschermen met e-mailauthenticatie op basis van SPF, DKIM en DMARC. Het NCSC adviseert ook om SPF, DKIM en DMARC te gebruiken om inkomende e-mail te filteren op phishingmail. Deze handreiking gaat daar niet over. Op andere plaatsen is daarover meer informatie te vinden.[2]

Voor overheidsorganisaties is het gebruik van SPF, DKIM en DMARC verplicht. Forum Standaardisatie voert periodieke metingen uit om te controleren of overheidsorganisaties aan de verplichting voldoen.[3] Voor alle andere organisaties geldt een dringend advies. De implementatie van e-mailauthenticatie is een 'good practice' die al door veel organisaties wordt toegepast.[4]

Naast mailserverbeheerders hebben ook verzenders van bulkmail de taak om authentieke e-mail herkenbaar te maken. Daarover gaat de NCSC-handreiking 'Goede bulkmail lijkt niet op phishingmail'.

Diverse aanvalstechnieken

Spoofing is slechts één van de mogelijkheden die aanvallers inzetten om de kans op succes bij phishing te vergroten. Aanvallers kunnen ook domeinnamen opkopen die lijken op die van de betrouwbare organisatie ('typosquatting') via SMS valse berichten sturen ('smishing'') of middels QR-codes gebruikers proberen te misleiden malafide websites te bezoeken. Het is van belang te realiseren dat naast e-mailauthenticatie met SPF, DKIM en DMARC gebruikers van e-mail worden getraind in het herkennen van diverse phishingtechnieken en ook weten waar zij phishing kunnen melden.

Bescherm domeinen tegen spoofing

Het effectief beschermen tegen phishing vraagt om een meervoudige aanpak waarbij oog is voor de mens, de techniek en de organisatie. In deze handreiking richten we ons primair op het beschermen tegen e-mail spoofing met behulp van e-mailauthenticatie. Dat kan met SPF, DKIM en DMARC. Hieronder lichten we deze onderdelen toe.

SPF

Het Sender Policy Framework (SPF) is een techniek waarmee een domeinnaamhouder kan aangeven welke mailservers e-mail

[2] Meer info zie: https://www.m3aawg.org/sites/default/files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf

[3] Meer info zie: https://www.forumstandaardisatie.nl/metingen/informatieveiligheidstandaarden

[4] U kunt zelf controleren of u al over e-mailauthenticatie beschikt door de e-mailtest te doen op https://www.internet.nl/

namens deze domeinnaam mogen versturen.[5] Ontvangende mailservers kunnen met behulp van SPF controleren of een e-mail is verzonden door een geautoriseerde mailserver.

In een SPF policy geef je aan welke mailservers e-mail mogen versturen namens een domeinnaam. De policy wordt als TXT-record toegevoegd aan de desbetreffende DNS-zone.

Een SPF policy voor het domein 'example.nl' kan er als volgt uitzien:

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

De policy in dit voorbeeld geeft aan:

- *v=spf1:* de huidige versie van SPF.
- *mx*: de inkomende mailservers mogen ook e-mail versturen.
- *a:mail.example.nl*: de mailserver met deze naam is geautoriseerd voor het versturen van e-mail. Hier kunnen ook IPv4 en IPv6 adressen in worden opgenomen.
- *~all*: Hier zijn meerdere opties mogelijk. Een hardfail wordt aangegeven met minteken (-). In dit geval worden niet geautoriseerde mails afgewezen. Een softfail wordt aangegeven met het kringelteken (~). Niet geautoriseerde mails kunnen als verdacht worden aangemerkt. Voor verzendende domeinen heeft het gebruik van ~all (softfail) meestal de voorkeur. De reden hiervoor is dat wanneer de SPF-authenticatie faalt met een SPF hardfail, een ontvangende mailserver de verbinding al kan blokkeren zonder de DKIM-handtekening en het DMARC-beleid te evalueren. Dit kan leiden tot ten onrechte geblokkeerde mails.

Een ontvangende mailserver die op basis van SPF e-mail controleert, stuurt een DNS-query om te zien of de domeinnaam van het afzenderadres over een SPF-beleid beschikt. Als dit het geval is, wordt bepaald of de verzendende mailserver is opgenomen in het SPF-beleid. Als de mailserver in het beleid voorkomt, concludeert de mailserver dat de e-mail authentiek is.

Met SPF kan inkomende e-mail worden gefilterd op spam- en phishingmail. SPF biedt echter op zichzelf nog niet een effectieve bescherming tegen e-mailspoofing.[6] DMARC neemt dit nadeel weg. SPF kan bovendien niet overweg met e-mailforwarding. DKIM is hiervoor een noodzakelijke aanvulling.

Klopt de afzender?

Met SPF kan een domeinnaamhouder aangeven welke mailservers e-mail namens een domeinnaam mogen verzenden. SPF is een belangrijke stap in het beschermen tegen e-mailspoofing. Het biedt echter nog geen volledige bescherming. SPF moet in combinatie met DKIM en DMARC worden gebruikt wil het e-mailspoofing effectief bestrijden.

DKIM

Domain Keys Identified Mail (DKIM) is een techniek waarmee een domeinnaamhouder kan aangeven met welke sleutel e-mails namens deze domeinnaam ondertekend dient

[5] Zie voor technische specificaties: https://datatracker.ietf.org/doc/html/rfc7208

[6] SPF maakt gebruik van het voor de gebruiker doorgaans onzichtbare '5321.From header' veld. Het afzenderadres dat getoond wordt aan de gebruiker ('5322.From header') wordt niet gebruikt bij authenticatie door SPF, maar wel door DMARC.

te zijn.[7] Verzendende mailservers ondertekenen alle uitgaande e-mail namens deze domeinnaam met deze sleutel. Ontvangende mailservers kunnen met behulp van DKIM controleren of de e-mail door een geautoriseerde partij is verzonden.

DKIM wordt voor uitgaande e-mail ingesteld door het toevoegen van een TXT-record aan de desbetreffende DNS-zone. Het daadwerkelijk ondertekenen van de e-mail gebeurt door software op de mailserver.

De verzendende mailserver voegt het veld "DKIM-Signature" toe aan de header van een e-mail. Dit veld bevat een digitale handtekening op de inhoud van de e-mail (zowel op de headers als de body).

De ontvangende mailserver gebruikt de domeinnaam van de afzender (d) en een selector (s) uit de DKIM-Signature om een DNS-query te sturen. Het selector-veld maakt het mogelijk om verschillende keys te gebruiken voor eenzelfde domeinnaam. Als antwoord ontvangt de mailserver de publieke sleutel van de afzender, waarmee de handtekening gecontroleerd wordt. Als de controle slaagt betekent het dat de e-mail daadwerkelijk afkomstig is van de desbetreffende domeinnaam en niet aangepast is gedurende het transport. Daarnaast is het goed te overwegen om – als u bijvoorbeeld andere partijen namens uw domein laat mailen of gebruik maakt van nieuwsbrieven – dit via subdomeinen in te regelen (nieuwsbrief.example.nl) en daar eigen DKIM keys voor te maken.

Handtekeningen met DKIM

Met DKIM worden uitgaande e-mails ondertekend met een digitale handtekening (signature). De ontvanger van de ondertekende mail controleert de handtekening waarmee de authenticiteit en integriteit van de mail kan worden gecontroleerd.

Net als SPF biedt DKIM-ontvangers een extra mogelijkheid om inkomende e-mail te filteren. Een mogelijk nadeel is dat de DKIM-handtekening beschadigd kan raken wanneer het bericht tijdens verzending wordt aangepast (denk aan mailinglijsten). Een effectieve bestrijding van e-mailspoofing vergt naast SPF en DKIM ook DMARC omdat een aanvaller de handtekening eenvoudigweg kan verwijderen.

DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC) is een techniek waarmee een domeinnaamhouder beleid kan publiceren voor de afhandeling van e-mail die niet aan het SPF- of DKIM-beleid voldoet.[8] Het is daarmee een essentiële stap in het bestrijden van e-mailspoofing. Zonder DMARC weet de ontvangende mailserver immers niet wat er gebeuren moet met een e-mail die niet voldoet aan de SPF of DKIM-regels. DMARC heeft de volgende functionaliteiten:

- *Terugkoppeling*. Ontvangende mailservers sturen een rapport (XML-bestand) naar de verzendende organisatie terug wanneer dat nodig is (afhankelijk van de instellingen in DMARC). De verzendende organisatie kan daarmee inzicht verkrijgen in de e-mails die verzonden worden namens hun domeinnamen. Dit inzicht kunnen zij gebruiken om mailstromen te

[7] Zie voor technische specificaties: https://datatracker.ietf.org/doc/html/rfc6376

[8] Zie voor technische specificaties: https://datatracker.ietf.org/doc/html/rfc7489

identificeren en de werking van SPF en DKIM te verbeteren.
- *Policy.* Een DMARC-beleid instrueert ontvangende mailservers bij het afhandelen van e-mail die niet voldoet aan het SPF- en DKIM-beleid van de verzendende domeinnaam. Mogelijke instructies zijn 'reject' (weggooien), 'quarantine' (markeren als spam) en 'none' (accepteren).

In ons voorbeeld van 'example.nl' kan DMARC er als volgt uit zien:

v=DMARC1; p=reject; rua=mailto:dmarc-authfail.example.nl; aspf=s; pct=100;

DMARC bestaat uit een TXT-record (_dmarc.example.nl) dat toegevoegd wordt aan de DNS-zone. Hierin staat het volgende:

- *v =DMARC1:* De huidige versie van DMARC.
- *p*: wat de ontvangende mailserver moet doen met email die niet voldoet aan DKIM- of SPF-beleid (*none, quarantine* of *reject*). Aanbevolen is om reject als beleid toe te passen.
- *pct:* Het percentage dat aangeeft op welk deel van de e-mailstroom het DMARC-beleid toegepast moet worden. Dit is vooral bedoeld om te testen als u bijvoorbeeld van p=none naar p=quarantine of p=reject wilt opschuiven. Als 'pct' is weggelaten, staat deze standaard op pct=100.
- *rua:* Het e-mailadres waarnaar de ontvangende mailproviders de DMARC rapportages kunnen sturen.
- *aspf=s:* De mate van alignment. De ontvangende mailserver controleert of het getoonde afzenderadres overeenkomt met het domein opgegeven onder SPF (aspf) en DKIM (adkim). De waarde 'strict' ('s') zorgt voor een exacte vergelijking, terwijl de mailserver bij 'relaxed' ('r') controleert of het afzendadres binnen hetzelfde domein valt. Dit kan worden aangegeven door aspf of adkim toe te voegen met de r=relaxed en s=strict. Standaard staat de waarde op relaxed.

Beleid met DMARC

Met DMARC wordt vastgesteld wat een ontvanger van e-mail moet doen met e-mails die wel of niet voldoen aan de SPF en DKIM regels. Het vormt hiermee het sluitstuk van effectieve bescherming tegen e-mailspoofing.

DMARC is ontworpen om in combinatie met SPF en DKIM gebruikt te worden. Wanneer een e-mail niet voldoet aan het SPF- of het DKIM-beleid, zal de e-mail als niet-authentiek worden aangemerkt. Juiste configuratie hiervan is belangrijk omdat de volgende situaties problemen kunnen geven:

- Domeinnamen waarvandaan e-mails worden gestuurd aan mailinglijsten. De beheerder van een mailinglijst kan deze zo instellen dat deze geen problemen oplevert met SPF, DKIM en DMARC.[9]
- Automatisch doorgestuurde e-mails. Deze voldoen niet aan het SPF-beleid van de verzendende domeinnaam. Als de e-mail niet met DKIM ondertekend is, zal de e-mail als niet authentiek worden aangemerkt.

Handelingsperspectief

Phishing is nog steeds een van de meest toegepaste methoden om initiële toegang tot netwerken of informatie te verkrijgen. Aanvallers spelen met behulp van beïnvloedingstechnieken in op de mens als schakel van de veiligheidsketen. Een veelgebruikte methode is om je klanten, contacten of leveranciers te bereiken met e-mailspoofing. Maak het aanvallers lastiger door SPF, DKIM en DMARC te implementeren op al

[9] Zie voor meer info deze pagina: DMARC.org

je domeinnamen, inclusief de domeinen waar geen e-mail vanaf wordt verzonden.

Houd er rekening mee dat het niet mogelijk is om volledig te voorkomen dat phishingmails uw klanten bereiken. Zorg er daarom voor dat je jouw klanten en partners goed uitlegt hoe je met hen communiceert en wat zij kunnen doen als zij toch phishing e-mail uit naam van jouw organisatie ontvangen. Een good practice is om het aantal domeinen waar u e-mail mee verzendt zo beperkt als mogelijk te houden. Stimuleer daarnaast het melden van phishing vanuit je domeinnamen en richt dit in zodat slachtoffers dat eenvoudig kunnen doen. Het snel acteren op een phishing aanval of een poging daartoe is immers van groot belang om verdere schade te voorkomen.

Implementatiestrategie

1 ***Voorbereiding*** Creëer overzicht van alle domeinnamen, e-mailstromen en soorten e-mail. Dit overzicht omvat zowel domeinnamen waarvandaan e-mail wordt verstuurd als domeinnamen waarvandaan niet wordt gemaild. Een DMARC-implementatie, zelfs zonder SPF en DKIM, kan gebruikt worden om ontbrekende informatie in kaart te brengen. Analyseer de verzamelde informatie op basis van de gestelde e-mailauthenticatiedoelen, zoals het voorkomen van ongeautoriseerde e-mailstromen. Hieruit volgt een identificatie van problemen en bijbehorende maatregelen om deze problemen te verhelpen.

Technische richtlijnen:

- Maak een DMARC-record aan voor elke domeinnaam. Gebruik de eerste periode (bijvoorbeeld: een maand) als policy de waarde 'none' en specificeer een e-mailadres waar mailservers de rapportages aan kunnen sturen.
- 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. Om de analyse te vergemakkelijken kunnen tools gebruikt worden.

2 ***Uitvoering*** Implementeer de maatregelen. Het kan hierbij gaan om nieuwe implementaties of het doorvoeren van benodigde wijzigingen in configuraties. E-mailbeheer en DNS-beheer zijn hiervoor verantwoordelijk.

Technische richtlijnen:

- *(Algemeen)* Gebruik voor inactieve domeinnamen of domeinnamen waarvandaan geen mail wordt verstuurd geen DKIM, maar wel DMARC en SPF. Configureer deze domeinen met SPF en DMARC ook als deze niet gebruikt worden zodat ook van deze domeinen geen e-mailspoofing mogelijk is.
- *(SPF)* 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 valse positieven 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' (hardfail) om misbruik ervan zoveel mogelijk tegen te gaan. Het is van belang om voor ieder subdomein een apart SPF record aan te maken. Dit is om te voorkomen dat kwaadwillenden vanaf bijvoorbeeld (niet bestaande) (sub)domeinen alsnog gespoofde e-mails kunnen versturen. Let er bovendien op dat bij het verwijzen naar een externe maildienst in de SPF (een zogenaamde 'include:'), het van belang is dat deze dienst controleert of de afzender een geauthentiseerde domeinnaam gebruikt, zodat het uitgesloten wordt dat medeklanten namens elkaars domeinnamen kunnen mailen (reject_sender_login_mismatch).[10]
- *(DKIM)* 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.[11]
- *(DMARC)* Zorg dat de 'identifiers' op elkaar afgestemd zijn, zodat de 'Identifier Alignment'-controle van DMARC succesvol zal zijn. Dit zijn de velden die gebruikt worden ter authenticatie. De RCF5322.From domeinnaam en de SPF- en DKIM-domeinnamen moeten overeenkomen. De 'Strict'-modus vereist een exacte overeenkomst, de 'Relaxed'-modus een overeenkomst op basis van domeinnaam.
- *(DMARC)* 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.

3 ***Controleren*** De implementatie, configuratie en gebruik van de e-mailauthenticatiemiddelen zal 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. Testen kan bijvoorbeeld met behulp van de tool https://www.internet.nl

4 ***Bijsturen*** De maatregelen die in de vorige stap op een continue basis worden geïdentificeerd moeten uiteraard ook worden toegepast.

[10] Zie voor een uitleg van deze kwetsbaarheid: https://doi.org/10.48550/arXiv.2312.07284

[11] Meer informatie is te vinden op: https://www.m3aawg.org/sites/default/files/m3aawg-dkim-key-rotation-bp-2019-03.pdf

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

December 2023