Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Bescherm domeinnamen tegen phishing

Beperk e-mailspoofing met SPF, DKIM en DMARC

Factsheet FS-2015-06
versie 1.0 | 28 oktober 2015

Het NCSC adviseert e-mailauthenticatie in te zetten om phishing namens uw domeinnamen tegen te gaan. Phishing is een vorm van internetfraude waarbij gevoelige gegevens buit worden gemaakt door middel van een vervalst bericht, meestal per e-mail. Veelal vervalsen of 'spoofen' aanvallers een domeinnaam, zodat de phishingmail afkomstig lijkt van het e-mailadres van een betrouwbare organisatie. Dit bemoeilijkt het herkennen van phishingmail, waardoor de kans groter is dat een gebruiker gevoelige gegevens prijsgeeft. Voor de gedupeerde organisatie kan er reputatieschade optreden.

Het NCSC adviseert om elke domeinnaam van uw organisatie te voorzien van e-mailauthenticatie met behulp van SPF, DKIM en DMARC. Daarnaast adviseert het NCSC om alle uitgaande e-mail van uw organisatie met behulp van DKIM te ondertekenen.

Doelgroep
E-mailbeheerders, DNS-beheerders en security officers

Aan deze factsheet hebben bijgedragen:
- Belastingdienst
- Forum Standaardisatie
- Measuremail
- NLnet Labs
- SNS Bank N.V.
- UWV

Achtergrond

Het huidige e-mailsysteem bevat de mogelijkheid om e-mails te versturen namens andere e-mailadressen. Dit heet 'e-mailspoofing' en is uit te voeren zonder diepgaande technische kennis. Zonder extra maatregelen is er geen enkele zekerheid of een e-mail wel echt afkomstig is van de organisatie namens welke hij verstuurd wordt.

Een manier om 'e-mailspoofing' tegen te gaan, is het valideren van de identiteit van de afzender door de ontvangende persoon of organisatie. Dit wordt e-mailauthenticatie genoemd. In de loop der jaren zijn er diverse technieken ontwikkeld die dit mogelijk maken.

SPF, DKIM en DMARC zijn technieken voor e-mailauthenticatie die gebruikmaken van DNS (Domain Name System). Ze werken op domeinnaamniveau. Omdat ze op dit niveau werken, kan e-mailauthenticatie uitgevoerd worden door mailservers. Individuele gebruikers worden daardoor ontlast.

PGP en S/MIME zijn technieken voor e-mailauthenticatie op gebruikerniveau. Eindgebruikers kunnen daarmee zelf e-mail digitaal ondertekenen en handtekeningen controleren. Het werken met deze technieken is voor veel eindgebruikers te complex. Deze factsheet gaat niet verder op deze technieken in.

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

Wat is het probleem?

Phishing is een vorm van social engineering waarbij mensen verleid worden tot het overhandigen van gevoelige gegevens. De meestgebruikte phishingmethode is het versturen van vervalste e-mails die afkomstig lijken van betrouwbare organisaties. Veelal bevatten de e-mails een link naar een nagemaakte internetpagina. Daarop wordt een besmet bestand aangeboden of wordt de ontvanger gevraagd persoonlijke gegevens in te vullen. Op deze manier verschaffen kwaadwillenden zich toegang, bijvoorbeeld tot bankrekeningen of bedrijfsnetwerken.

Om de e-mails zo echt mogelijk te laten lijken, wordt het afzendadres door phishers vervalst. Daarbij gebruiken zij een domeinnaam van een betrouwbare organisatie. Een phishingmail

lijkt dan bijvoorbeeld verzonden door info@ncsc.nl, terwijl deze in werkelijkheid door een malafide partij verzonden is.

Vervalsen van e-mailadressen maakt het lastiger voor gebruikers om phishingmail te herkennen. Het verhoogt daarmee de kans op succes van een phishingaanval. Ook heeft het een 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 e-mails geweerd worden. Daarnaast is het slecht voor het imago en kan er reputatieschade ontstaan.

Wat adviseert het NCSC?

Het NCSC adviseert om elke domeinnaam van uw organisatie te voorzien van e-mailauthenticatie met behulp van SPF, DKIM en DMARC. Daarnaast adviseert het NCSC om alle uitgaande e-mail van uw organisatie met behulp van DKIM te ondertekenen.

Het NCSC adviseert ook om SPF, DKIM en DMARC te gebruiken om inkomende e-mail te filteren op phishingmail. Deze factsheet gaat daar niet over. Op andere plaatsen is daarover meer informatie te vinden.[1]

Forum Standaardisatie heeft DKIM en SPF opgenomen op de 'pas toe of leg uit'-lijst met open standaarden voor de overheid.[2] DMARC is ook getoetst en wordt naar verwachting in 2016 toegevoegd aan de 'pas toe of leg uit'-lijst als deze de status van standaard binnen standaardisatie-organisatie IETF verkrijgt.[3]

Het handelingsperspectief op de laatste pagina beschrijft een managementproces waarmee organisaties e-mailauthenticatie kunnen implementeren. De technische richtlijnen beschrijven de best practices voor de implementatie van de individuele technieken. De rest van deze factsheet is een beknopte beschrijving van SPF, DKIM en DMARC.

Beschrijving van SPF, DKIM en DMARC

Met behulp van SPF en DKIM geeft een domeinnaamhouder in zijn DNS-zone aan hoe legitieme e-mail vanaf zijn domeinnaam te herkennen is. Met behulp van DMARC geeft hij in zijn DNS-zone aan wat er zou moeten gebeuren met e-mail vanaf zijn domeinnaam die niet voldoet aan het gepubliceerde SPF- en DKIM-beleid.

Wat is SPF?

Sender Policy Framework (SPF) is een techniek waarmee een domeinnaamhouder kan aangeven welke mailservers e-mail namens deze domeinnaam mogen versturen. Ontvangende mailservers kunnen met behulp van SPF controleren of een e-mail is verzonden door een geautoriseerde mailserver.

Techniek In een SPF-beleid geeft een organisatie aan welke mailservers e-mail mogen versturen namens een domeinnaam. Dit beleid wordt als TXT-record toegevoegd aan de desbetreffende DNS-zone.

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:

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

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.

Voordelen

- De implementatie van SPF voor uitgaande e-mail vergt relatief weinig middelen.
- SPF biedt ontvangers een aanvullend gereedschap om inkomende e-mail te filteren op spam- en phishingmail. Voor de organisatie die SPF heeft ingesteld voor haar domeinnamen, heeft dit als voordeel dat reputatieschade wordt voorkomen.

Nadelen

- Op zichzelf is SPF geen effectief middel tegen e-mailspoofing. Het afzenderadres dat getoond wordt aan de gebruiker ('5322.From header') wordt niet gebruikt bij de authenticatie. Het onzichtbare '5321.From header' wel. Het gebruik van SPF samen met DMARC neemt dit nadeel weg.
- SPF kan niet overweg met e-mailforwarding, het doorsturen van e-mail. Dit komt omdat de e-mail opnieuw wordt verzonden door de mailserver die forwarding doet. DKIM, dat wel overweg kan met forwarding, is daarom vaak een noodzakelijke aanvulling.
- SPF biedt minder zekerheid wanneer meerdere organisaties dezelfde mailservers gebruiken. Is dit een probleem, dan kan dit worden opgelost door verschillende IP-adressen voor verschillende domeinnamen in te stellen op de mailserver.

Wat is DKIM?

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

[1] Meer info: 'Anti-Phishing Best Practices for ISP's and Mailbox Providers' (2015, M3AAWG). URL: https://www.m3aawg.org/sites/default/files/M3AAWG_AWPG_Anti_Phishing_Best_Practices-2015-06.pdf

[2] Bron: https://www.forumstandaardisatie.nl/actueel/item/titel/veiliger-maken-van-e-mail-krijgt-vaste-plaats-op-agenda-nederlandse-overheid/

[3] De huidige status van DMARC op de pas-toe-of-leg-uit-lijst staat op https://lijsten.forumstandaardisatie.nl/open-standaard/dmarc.

namens deze domeinnaam ondertekend dienen te zijn. 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.

Techniek 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 speciale 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-server 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 dat dat de e-mail daadwerkelijk afkomstig is van de desbetreffende domeinnaam en niet aangepast is gedurende het transport.

Voordelen

- Net als SPF biedt DKIM ontvangers een extra mogelijkheid om inkomende e-mail te filteren. Voor de organisatie die DKIM gebruikt bij uitgaande e-mail is dit gunstig voor de reputatie en merknaam.

Nadelen

- De toepassing van DKIM vergt meer middelen dan de toepassing van SPF. Om DKIM toe te passen moet er aanvullende software geïnstalleerd worden op de mailserver.
- De DKIM-handtekening kan beschadigd raken wanneer het bericht tijdens verzending wordt aangepast, bijvoorbeeld door het gebruik van mailinglists.
- Op zichzelf is DKIM geen effectieve methode tegen e-mailspoofing, omdat een aanvaller de handtekening eenvoudigweg kan verwijderen. Een mailserver weet niet wat te doen met e-mail waarbij een DKIM-handtekening ontbreekt. Het gebruik van DKIM samen met DMARC neemt dit nadeel weg.

Wat is 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.

Het biedt de volgende functionaliteit:

- *Terugkoppeling*. Ontvangende organisaties sturen een rapport (XML-bestand) naar de verzendende organisatie terug. 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 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).
- *Afzenderadres*. Een e-mail heeft in feite twee afzenderadressen, waarvan één onzichtbaar voor de gebruiker. SPF controleert enkel het onzichtbare veld, niet het afzenderadres dat getoond wordt aan de gebruiker. DMARC controleert ook of het getoonde afzendadres niet afwijkt. Dit is een belangrijke functionaliteit voor het tegengaan van e-mailspoofing.

Techniek DMARC bestaat uit een TXT-record dat toegevoegd wordt aan de desbetreffende DNS-zone. Hierin staat het volgende:

- Beleid [p]: wat de ontvanger moet doen met email die niet voldoet aan DKIM- of SPF-beleid (none, quarantine of reject).
- Een optioneel percentage [pct] dat aangeeft op welk deel van de e-mailstroom het DMARC-beleid toegepast moet worden.
- Het e-mailadres [rua] waarnaar de ontvangende mailproviders de rapportages kunnen sturen.
- Het e-mailadres [ruf] waarnaar de ontvangende mailproviders de inhoud van vervalste e-mails kunnen sturen.
- De mate van alignment. De ontvangende mailserver controleert of het getoonde afzenderadres overeenkomt met het domein opgegeven onder SPF en DKIM. De waarde 'strict' zorgt voor een exacte vergelijking, terwijl de mailserver bij 'relaxed' controleert of het afzendadres binnen hetzelfde domein valt.

Voordelen

- De functionaliteiten van DMARC stellen organisaties in staat om de gebruikte e-mailauthenticatie te verbeteren. Voor de domeineigenaar heeft dit als voordeel dat e-mailspoofing tegengegaan wordt en voor ontvangers biedt dit meer mogelijkheden voor het herkennen van phishingmail.
- Zonder DMARC zijn SPF en DKIM niet effectief in het tegengaan van e-mailspoofing. De vergelijkbare techniek ADSP[4] maakt DKIM effectiever, maar mist de functionaliteit voor terugkoppeling die DMARC biedt. Ook wordt het door weinig e-mailproviders ondersteund.

Nadelen DMARC is ontworpen om het in combinatie met SPF en DKIM in gebruik te nemen. Wanneer een e-mail zowel niet voldoet aan het SPF- als het DKIM-beleid, zal deze als niet-authentiek worden aangemerkt. De volgende situaties leveren daarom problemen op:

- Domeinnamen waarvandaan e-mails worden gestuurd aan mailinglists. Er wordt gewerkt aan oplossingen voor dit probleem.[5] De beheerder van een mailinglist kan zijn mailinglist

[4] Meer info: https://en.wikipedia.org/wiki/Author_Domain_Signing_Practices
[5] Meer info: https://dmarc.org/wiki/FAQ#I_operate_a_mailing_list_and_I_want_to_interoperate_with_DMARC.2C_what_should_I_do.3F

zo instellen dat deze geen problemen oplevert met DMARC, DKIM en SPF. Hij kan hiervoor bijvoorbeeld het afzenderadres van doorgestuurde e-mails aanpassen. Organisaties kunnen contact opnemen met beheerders van mailinglists om hen hierop te wijzen, of de mailinglist in kwestie 'whitelisten' door de mailserver ervan op te nemen in het SPF-beleid van de verzendende domeinnaam.

- E-mails die automatisch worden doorgestuurd. 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.
- In het algemeen: berichten waarbij de DKIM-handtekening niet langer klopt (bijvoorbeeld vanwege wijzigingen onderweg) en de controle van het SPF-beleid niet slaagt.

Handelingsperspectief:

1 ***Plan*** In de eerste fase 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 e-mailauthenticatiedoelen, zoals het voorkomen van ongeautoriseerde e-mailstromen. Hieruit volgt een identificatie van problemen en bijbehorende maatregelen om deze problemen te verhelpen. Marketing is samen met IT en Security/Risk Management verantwoordelijk voor de metrieken/doelstellingen. E-mailbeheer is verantwoordelijk voor het (technische) plan van aanpak. Relatiebeheer brengt de relevante derde partijen in kaart en zorgt voor een correcte contractuele afstemming (SLA's) van de benodigde activiteiten.[6]

Technische richtlijnen:

- 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.
- 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 ***Do*** In deze fase worden de maatregelen geïmplementeerd. Het kan hierbij gaan om nieuwe implementaties of het doorvoeren van benodigde wijzigingen in configuraties. E-mailbeheer en DNS-beheer zijn hiervoor verantwoordelijk.[6]

Technische richtlijnen:

- *(Algemeen)* Gebruik voor inactieve domeinnamen geen DKIM, maar wel DMARC en SPF.
- *(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 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.
- *(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.[7]
- *(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 domain en 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 ***Check*** 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. De afdelingen Security en Forensics zijn hiervoor belangrijke partijen.[7]

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

[6] Meer informatie over rollen en verantwoordelijkheden en de benodigde policies zie: http://www.bits.org/publications/security/BITSEmailAuthenticationFeb2013.pdf
[7] Meer informatie: https://www.m3aawg.org/sites/default/files/document/M3AAWG_Key_Implementation_BP-2012-11.pdf

Uitgave van **Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl | T 070-751 55 55
Publicatienr: FS-2015-06 1.0 | Aan deze informatie kunnen geen rechten worden ontleend.