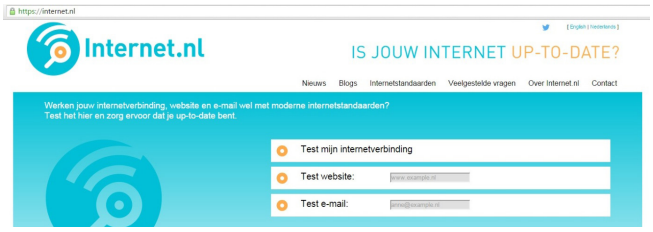
INFORMATIE
BEVEILIGINGS
DIENST

E-MAILAUTHENTICATIE: VOORKOM DAT ANDEREN E-MAILBERICHTEN VERSTUREN NAMENS UW GEMEENTELIJKE E-MAILDOMEIN

Volgens het Cybersecuritybeeld Nederland 2015 van het Nationaal Cyber Security Centrum (NCSC) is phishing een zeer grote bedreiging en is naast bewustzijn ook de bredere invoering van e-mailauthenticatie noodzakelijk. Met e-mailauthenticatie kan een gemeente haar domeinnaam beschermen tegen betrouwbaar lijkende phishing e-mailberichten waarin bijvoorbeeld bijlagen of links naar malware of valse inlogpagina's zitten. Het zorgt ervoor dat derden niet zomaar de gemeentelijke domeinnaam als afzenderadres kunnen misbruiken. Dit wordt 'afzenderadres-vervalsing' of 'e-mail spoofing' genoemd en is uit te voeren zonder diepgaande technische kennis. E-mailauthenticatie voorkomt dit en zorgt er bovendien voor dat spam nauwkeuriger wordt herkend. Het werkt op basis van de open standaarden SPF, DKIM en DMARC. Verschillende gemeenten passen deze standaarden al succesvol toe. Deze standaarden zijn ook relevant voor domeinnamen waarvan niet gemaild wordt.

Voor het uitwisselen van e-mailberichten wordt gebruik gemaakt van een relatief simpel, tekst gebaseerd protocol, dat geen betrouwbare voorzieningen bevat om na te gaan of de afzender echt is wie hij beweert te zijn. Zonder extra maatregelen is er op dit moment geen enkele zekerheid of een e-mailbericht wel echt afkomstig is van de organisatie namens welke het e-mailbericht verstuurd wordt. Een belangrijke manier om 'e-mail spoofing' tegen te gaan, is het valideren van de identiteit van de afzender door de ontvangende persoon of organisatie. Dit wordt e-mailauthenticatie genoemd. De verzendende organisatie zorgt voor echtheidskenmerken die de ontvangende organisatie geautomatiseerd kan controleren. Voor de eindgebruiker vindt dit allemaal transparant plaats en hij hoeft hier niets nieuws voor in te stellen of te valideren, maar is wel beter beschermd.



Figuur 1. website van internet.nl

Op de website Internet.nl (zie figuur 1) kunt u eenvoudig controleren of uw gemeentelijke e-maildomein gebruik maakt van de e-mailauthenticatiestandaarden SPF, DKIM en DMARC, zodat ontvangers echtheidskenmerken en bijbehorende aanwijzingen kunnen gebruiken om te controleren of een e-mailbericht vervalst is en hoe hiermee om te gaan.

E-MAILAUTHENTICATIE ZORGT ERVOOR DAT DERDEN NIET ZOMAAR DE GEMEENTELIJKE DOMEINNAAM ALS AFZENDERADRES KUNNEN MISBRUIKEN.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Deze factsheet legt uit hoe u phishing, spam en virussen die via e-mailberichten verspreid worden kunt terugdringen door gebruik te maken van e-mailauthenticatie. In deze factsheet wordt achtereenvolgens aandacht besteed aan de beveiligingsvoordelen van e-mailauthenticatie voor gemeenten, de achterliggende e-mailauthenticatie-standaarden SPF, DKIM en DMARC, hoe uw gemeente gebruik kan maken van e-mailauthenticatie en tenslotte het IBD advies. Voor meer uitgebreide en technische achtergrondinformatie wordt verwezen naar de uitgebreide versie van deze factsheet op de website van de IBD.

Wat levert e-mailauthenticatie mijn gemeente op?

Verhogen vertrouwen in gemeentelijke domeinnaam
Veelal vervalsen of 'spoofen' aanvallers een domeinnaam, zodat de phishing en spam e-mailberichten afkomstig lijken van het e-mailadres van een betrouwbare organisatie. Met e-mailauthenticatie wordt een betrouwbare e-mailcommunicatie tussen gemeenten en burgers, bedrijven, (keten)partners en (semi)overheidsorganisaties bevorderd en beschermt de gemeente zichzelf tegen e-mailberichten van ongeauthentiseerde afzenders. Dit geldt voor alle domeinnamen, waarvan de gemeente de houder is.

Concreet betekent dit dat e-mailauthenticatie ervoor zorgt dat uw gemeente:

- De kans vermindert dat derden uw e-mailadressen misbruiken voor het versturen van spam en/of phishing e-mailberichten.
- De afleveringszekerheid van e-mailberichten vergroot, zodat de e-mailberichten in de inbox van de ontvanger worden afgeleverd in plaats van de spambox.
- Minder vatbaar wordt voor oplichting en/of ransomware verspreid via vervalste e-mailadressen.

Voldoen aan wet- en regelgeving
De SPF en DKIM-standaarden zijn sinds 2013 opgenomen op de lijst met verplichte open standaarden voor de gehele publieke sector ('pas-toe-of-leg-uit-lijst') van het Forum Standaardisatie. Dit betekent dat overheden en semi-overheden SPF en DKIM dienen toe te passen en alleen in geval van zwaarwegende redenen daarvan mogen afwijken. DMARC is ook getoetst en wordt naar verwachting in 2016 toegevoegd aan de 'pas-toe-of-leg-uit'-lijst. Tevens adviseert het NCSC e-mailauthenticatie met behulp van SPF, DKIM en DMARC in te zetten om spam en phishing namens uw domeinnamen tegen te gaan.

Wat zijn de e-mailauthenticatie-standaarden SPF, DKIM en DMARC?

SPF, DKIM en DMARC worden meestal gezamenlijk ingezet om te controleren dat de afzender, het e-mailadres en –server, van een e-mailbericht inderdaad kloppen, en dat de inhoud van het e-mailbericht onderweg niet is gewijzigd. Alle drie de internetstandaarden maken gebruik van het DNS-systeem om hun informatie te publiceren.

Voor alle drie de e-mailauthenticatiestandaarden geldt dat zowel de verzendende als ontvangende organisatie, van e-mailberichten, implementatie- en beheeractiviteiten dienen uit te voeren om volledig gebruik te kunnen maken van de geboden bescherming door deze e-mailauthenticatiestandaarden. De verzendende organisatie, gemeenten, dienen de basis te leggen voor de SPF-, DKIM- en/of DMARC-standaard door deze te implementeren. Voor gemeenten betekent dit concreet dat ze hun DNS-systeem dienen te voorzien van de correcte SPF, DKIM en/of DMARC DNS-records.
De ontvangende organisaties dienen hun inkomende/ontvangende e-mailservers zo te configureren dat deze automatisch controleren of het ontvangen e-mailbericht legitiem is of niet. Hiervoor dient de inkomende/ontvangende e-mailserver te controleren of de gegevens van het ontvangen e-mailbericht overeenkomen met de instellingen van de SPF, DKIM en/of DMARC DNS-record die de verzendende organisatie heeft geconfigureerd.
Voor de eindgebruiker vindt dit allemaal transparant plaats en hij hoeft hier niets nieuws voor in te stellen of te valideren, maar is wel beter beschermd. *Opmerking*: Het toevoegen van een SPF-, DKIM- en/of DMARC-record aan het DNS-systeem kent een korte doorlooptijd. Niet alle gemeenten beheren hun eigen DNS-systeem en dienen daarom hiervoor een wijzigingsverzoek in te dienen bij hun provider die daar in een enkel geval een klein bedrag voor in rekening bracht brengt.

Hoe maakt u uw e-mailbericht betrouwbaarder?

Hiervoor dient de gemeente gebruik te maken van alle drie de e-mailauthenticatiestandaarden. Zowel SPF, DKIM en DMARC zijn bepalend voor het te bereiken beveiligingsniveau. De factsheet 'bescherm domeinnamen tegen phishing' van het NCSC kan gebruikt worden bij het configureren van het SPF, DKIM en DMARC-protocol. Opmerking: Vraag voor configureren van de e-mailauthenticatiestandaarden, indien noodzakelijk, ondersteuning aan uw leverancier of hostingpartij. Het Bureau Forum Standaardisatie (BFS) kan u ook adviseren over het gebruik van deze e-mailauthenticatiestandaarden.

Pas DNSSEC toe
Volgens de e-mailauthenticatiestandaarden is het niet noodzakelijk om daarbij ook DNSSEC te gebruiken maar dat willen we hier toch van harte aanraden. DNSSEC beschermd de integriteit van de DNS-informatie, dus ook de SPF-, DKIM- en DMARC-records, en zorgt ervoor dat het DNS-antwoord authentiek is en afkomstig van de juiste bron[1].

1 Zie ook de factsheet 'DNSSEC: Voorkom domeinnaamfraude' van de IBD.

Blokkeer niet gebruikte domeinnamen
Blokkeer geparkeerde domeinnamen (parked domain)[2] en domeinnamen die niet worden gebruikt voor het versturen van e-mailberichten. Voor het blokkeren van deze domeinnamen kan gebruik gemaakt worden van zowel SPF, DKIM en DMARC[3].

Volg stappenplan

Het volgende stappenplan kan gevolgd worden om tot het gewenste beveiligingsniveau te komen:

1. Configureer DMARC-record
Gemeenten dienen een DMARC-record toe te voegen aan hun DNS-systeem met parameter 'p=none' om de uitgaande e-mailstromen per gemeentelijk domein te kunnen onderzoeken. Configureer het DMARC-record zodanig dat de terugkoppelingen (DMARC-rapportages) van de e-mailproviders verzameld wordt worden ten behoeve van de analyse. Voor het analyseren van de DMARC-rapportages van de e-mailproviders, bijvoorbeeld voor het identificeren van de e-mailstromen, is specifieke kennis en tooling nodig zodat deze (eenvoudig) geïnterpreteerd kunnen worden.

2. Identificeer domeinnamen, e-mailstromen en soorten e-mailberichten
In deze stap dient een overzicht te worden gecreëerd van de domeinnamen, e-mailstromen en soorten e-mailberichten. Om een zo compleet mogelijk beeld te vormen van de e-mailstromen dient de terugkoppeling van de e-mailproviders gedurende een periode van 6 tot 8 weken gelogd en geanalyseerd te worden. Veel van deze informatie zal binnen de gemeente aanwezig zijn. Denk hierbij aan de volgende e-mailstromen: Ketenpartners; Leveranciers; Kantoormail; Afsprakenmodules van klantcontactcentra (KCC) en Nieuwsbrieven.

3. Identificeer legitieme e-mailstromen
Identificeer per domein welke e-mailstromen legitiem zijn ten behoeve van opname in het SPF-record. Deze configuratie zal goed gemonitord dienen te worden om mogelijke problemen snel te detecteren en op te lossen.

4. Inventariseer mailappliance
Inventariseer welke mailappliance wordt gebruikt door de gemeente ten behoeve van het inschatten van de impact voor DKIM implementatie. De toepassing van DKIM vergt meer middelen dan de toepassing van SPF. Om DKIM toe te passen dient er vaak aanvullende software geïnstalleerd worden op de e-mailserver.

5. Monitor e-mailautenticatiemiddelen
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 e-mailservers.

6. Test regelmatig de e-maildomeinen
Voor het testen van de e-maildomeinen kan gebruik worden gemaakt van de verschillende hulpmiddelen die hieronder worden benoemd.

7. Optioneel: Kies een kundige implementatiebegeleider of geef opdracht aan uw hostingpartij.

Stel eisen aan uw leverancier
Op het moment dat u gebruik maakt van een leverancier voor het afhandelen van e-mailberichten is het advies om onderstaande eisen aan uw leverancier te stellen:

- De leverancier definieert en valideert de SPF-, DKIM- en DMARC-records van het gemeentelijke domein.
- De leverancier zorgt ervoor dat de partijen, die e-mailberichten ontvangen van de gemeente, kunnen valideren dat deze e-mailberichten inderdaad van de gemeente afkomstig zijn.

Hulpmiddelen

Hulpmiddelen waarmee de DMARC configuratie kan worden gecontroleerd zijn onder andere:

- E-mail zelftest via Internet.nl
- E-mail zelftest via phishingscorecard.com

2 Een domeinnaam wordt vaak geparkeerd om de domeinnaam alvast te reserveren voor bijvoorbeeld een website die nog ontwikkeld dient te worden.
3 Zie voor meer achtergrondinformatie: https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bp-2015-12.pdf

Advies IBD met betrekking tot SPF, DKIM en DMARC

De IBD geeft het advies om:

- Ervoor te zorgen dat de gemeente beschikt over de benodigde kennis en tooling voor het identificeren van de e-mailstromen vanuit de terugkoppelingen van de e-mailproviders. Als de gemeente niet over de benodigde kennis en/of tooling beschikt, kan de gemeente kiezen voor een kundige externe implementatiebegeleider of opdracht geven aan uw hostingpartij.
- Voor het configureren van SPF, DKIM en DMARC de factsheet 'bescherm domeinnamen tegen phishing' van het NCSC te volgen.
- Voor zowel SPF als DMARC de eerste periode het beleid zo te configureren dat in eerste instantie de ontvangen e-mailberichten altijd worden geaccepteerd. Op het moment dat inzicht is in de legitieme e-mailstromen kan na verloop van tijd het beleid worden aangescherpt naar accepteren maar als spam markeren. Uiteindelijk kan het beleid nog verder worden aangescherpt naar NIET accepteren, door voor het betreffende domein het DMARC-beleid in te stellen op 'p=reject' op het moment dat er sprake is van afwijkingen.
- DNSSEC te gebruiken en voor meer achtergrondinformatie van DNSSEC de factsheet 'DNSSEC: Voorkom domeinnaamfraude' van de IBD te lezen.
- geparkeerde domeinnamen en domeinnamen die niet worden gebruikt voor het versturen van e-mailberichten te blokkeren. Voor het blokkeren van deze domeinnamen kan gebruik gemaakt worden van zowel SPF, DKIM en DMARC.
- Ervoor te zorgen dat de DMARC-rapportages, in verband met privacyaspecten, binnen de Europese Economische Ruimte (EER) worden opgeslagen en bewaard.
- Als tijdens de analyse van de terugkoppeling van de e-mailproviders blijkt dat er e-mailstromen worden geïdentificeerd die buiten de EER worden gehost, neem dan de huidige werkwijze onder de loep en neem mogelijke privacyrisico's weg.13
- Als tijdens de analyse van de terugkoppeling (DMARC-rapportages) van de e-mailproviders blijkt dat misbruik heeft plaatsgevonden, bijvoorbeeld het versturen van spam of phishing e-mailberichten, meldt dan dit misbruik zowel bij de IBD als bij de politie.

MEER INFORMATIE

MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE ANDERE FACTSHEETS VAN DE IBD EN OP DE WEBSITE WWW.IBDGEMEENTEN.NL. HIER KUNNEN GEMEENTEN BOVENDIEN VIA DE COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN. DE HELPDESK VAN DE IBD IS TE BEREIKEN TIJDENS KANTOORUREN VAN 9:00 TOT 17:00 UUR OP HET NUMMER 070 373 8011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL. TIJDENS DEZE KANTOORUREN REAGEERT DE IBD BINNEN 30 MINUTEN OP EEN INCIDENTMELDING. BUITEN KANTOORUREN IS DE IBD OP HETZELFDE NUMMER BEREIKBAAR VOOR SPOEDEISENDE MELDINGEN EN ZAL DE IBD BINNEN 60 MINUTEN REAGEREN OP EEN TELEFONISCHE OPROEP.