Opdrachtomschrijving implementatie strikte DMARC policy aan gemeenschappelijke ICT-dienstverleners

Inleiding

Uit de meest recente Meting Informatieveiligheidstandaarden blijkt dat de anti-spoofing e-mailstandaard DMARC is op slechts 49% van de overheidsdomeinen voldoende strikt is geconfigureerd. Binnen het Rijk gaat het om 53% van de domeinen waarbij DMARC voldoende strikt zijn geconfigureerd.

De informatieveiligheidstandaarden staan al enkele jaren op de 'pas toe of leg uit'-lijst en zijn daarmee conform de Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten verplicht.

Aanvullend zijn er overheidsbreed adoptieafspraken gemaakt om de adoptie te versnellen: https://www.forumstandaardisatie.nl/thema/meting-informatieveiligheidstandaarden-en-adoptieafspraken

Daarnaast zijn de informatieveiligheidstandaarden verankerd in de Baseline Informatiebeveiliging Overheid (BIO) via maatregel 13.2.3.1. De BIO vervangt de BIR: https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html#d17e150

We zien dat gemeenschappelijke IT-dienstverleners (shared service centers) een versnellend effect kunnen hebben op de adoptie van informatieveiligheidstandaarden. Zo is bij het Rijk een meetbare verbetering in de toepassing van webstandaarden zichtbaar, namelijk van 76% naar 90% in een half jaar tijd, doordat CIO BZK aan SSC-ICT opdracht heeft gegeven een significant aantal webdomeinen in samenhang te laten voldoen aan de informatieveiligheidstandaarden. Om deze reden zien wij een kans om ook in de adoptie van mailstandaarden verschil te maken door aan de gemeenschappelijke IT-dienstverleners opdracht te geven om hun klanten proactief te helpen om domeinnamen te beschermen tegen phishing met een strikte DMARC-policy.

Nut van een strikte DMARC policy

Naast dat toepassing van informatieveiligheidstandaarden hoort bij goed huisvaderschap, kan een strikte DMARC policy een kwantitatieve besparing opleveren. Via DMARC kan worden ingesteld wat de mailserver moet doen als die een verdachte e-mail ontvangt. Zo zag KPN na activering van actieve DMARC policy naast minder gespoofde e-mails ook een reductie in het aantal helpsdesk calls. PostNL zag het aantal phishing-gerelateerde vragen bij hun klantenservice met 54% dalen nadat zij hun DMARC policy hadden ingesteld op 'reject'.

Met actieve DMARC policies kan spoofing van overheidsdomeinen goed worden aangepakt. In onze metingen zien we echter dat slechts 53% van e-maildomeinen binnen het Rijk actieve DMARC policies heeft ingesteld (quarantaine of reject). Gespoofde mails verzonden namens domeinen zonder deze DMARC policies komen dus nog steeds aan.

Rol van gemeenschappelijke ICT-dienstverleners

De overheid heeft een verantwoordelijkheid voor de domeinen waarvoor zij kantoormail beheerd, wat het lastiger maakt is dat er vaak ook andere mailstromen zijn (nieuwsbrieven, facturen, etc.). Klanten hebben in de meeste gevallen zelf niet de kennis om DKIM, SPF en DMARC goed te laten configureren voor haar maildomeinen en mailstromen. SSC's kunnen aan de hand van DMARC-rapportages de legitieme mailstromen in kaart brengen en er met de klant voor zorgen dat deze netjes SPF en DKIM doen. Zodra dat is gedaan kan er een actieve DMARC policy worden ingesteld waarmee mailspoofing en mailphishing actief wordt bestreden.

Gemeenschappelijks dienstverleners moeten hier centraal de lead in nemen, en proactief aan de slag gaat om de DMARC instellingen voor (en mét) haar klanten veilig in te stellen. Dit kan door opdracht te geven om onderstaand stappenplan uit te voeren voor alle maildomeinen die in beheer zijn bij de shared service organisaties.

Stappen om tot een strikte DMARC policy te komen

Middels onderstaand stappenplan kan een ICT-dienstverlener klanten helpen van een passieve DMARC policy naar een veilige DMARC policy te komen om spoofing te voorkomen. Maak tevens gebruik van de adviezen van het NCSC en de IBD, en eventueel de how-to van Platform Internetstandaarden:

- https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-bescherm-domeinnamen-tegen-phishing
- https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2016/06/20160602_Factsheet_emailauthenticatie_v1.01.pdf
- https://github.com/internetstandards/toolbox-wiki/blob/master/DMARC-how-to.md

1. SPF, DKIM en DMARC (none) records instellen voor zover dat nog niet was gedaan

Overheidsorganisaties dienen een DMARC-record toe te voegen aan hun DNS-systeem met parameter 'p=none' om de uitgaande e-mailstromen per domein te kunnen onderzoeken. Configureer het DMARC-record zodanig dat de terugkoppelingen (DMARC-rapportages) van de e-mailproviders verzameld wordt ten behoeve van de analyse. Opmerking: 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.

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.
- (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.

2. Analyse van de DMARC rapportages om (legitieme) mailstromen te identificeren

In deze stap dient een overzicht te worden gecreëerd van de domeinnamen, e-mailstromen en soorten e-mailberichten. Dit overzicht omvat zowel domeinnamen waarvandaan e-mailberichten worden verstuurd als domeinnamen waarvandaan nooit e-mailberichten worden verstuurd. 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.

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.

3. In samenspraak met de klant verbeteren van het SPF record, en implementeren van DKIM bij verzendende mailservers, voor het klantdomein ten behoeve van legitieme mailstromen

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.

DKIM dient geïmplementeerd te worden bij alle mailservers die namens het domein mail verzenden. 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.

4. DMARC policies naar quarantaine, en actief blijven monitoren of legitieme mailstromen als spam worden aangemerkt (zo ja, zie 3)

Op het moment dat inzicht is in de legitieme e-mailstromen kan na verloop van tijd het beleid worden aangescherpt van accepteren (p=none) naar als spam markeren (p=quarantaine).

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.

5. Bij voldoende zekerheid dat legitieme mail niet als spam wordt aangemerkt DMARC policy naar reject

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.

6. Bij voortduring blijven monitoren van de DMARC rapportages

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.

Domeinen zonder e-mail

Wanneer je voor een domeinnaam geen e-mail wil gebruiken, gebruik dan de volgende instellingen:

- Plaats een zogenaamd “null MX” record in de DNS zone.
- Plaats een “SPF -all” record in de DNS zone.
- Plaats een “DMARC p=reject” record in de DNS Zone.
- Plaats geen DKIM record.

Nadere informatie

https://www.forumstandaardisatie.nl/standaard/dmarc