FS-20160315.06C

Rapportage DMARC/SPF/DKIM impactanalyse t.b.v. Forum Standaardisatie

Inleiding

Tijdens het Nationaal Beraad werd voorgesteld adoptieafspraken te maken over de internet-beveiligings-standaarden welke al via pas-toe-of-leg-uit, worden voorgeschreven bij aanbestedingen.

In de Regieraad Interconnectiviteit is gesproken over versnelde adoptie van pas-toe-of-leg-uit-normen TLS, DMARC en DNSSEC. Na de Regieraad hebben VNG, IBD en Logius/Bureau Forum Standaardisatie (BFS) gesproken over de wenselijkheid van adoptie hiervan voor het gemeentelijke domein.

Gemeenten onderschrijven dat een betrouwbare GDI van belang is voor het vertrouwen van burgers en bedrijven in de (elektronische) overheid. Daarmee onderschrijven zij ook het belang van de standaarden TLS, DMARC en DNSSEC. Met het voorstel om te komen tot versnelde adoptie van deze standaarden door plaatsing op de pas-toe-of-leg-uit-lijst konden gemeenten echter niet zonder meer instemmen.

De VNG geeft in het Nationaal Beraad aan dat gemeenten in oktober 2013 (BALV) massaal hebben ingestemd met de resolutie “informatieveiligheid, randvoorwaarde voor de professionele gemeente”, waar de minister van BZK ruimte aan gemeenten heeft gegeven voor invulling van het begrip Verplichtende Zelfregulering. In deze resolutie is opgenomen dat gemeenten de BIG als basisnormenkader aannemen. Voor de prioritering van implementatie van de BIG hebben gemeenten daarbij aangegeven ieder een eigen tempo aan te zullen houden, gebaseerd op lokale afwegingen.

De VNG kan daar niet zonder meer andere afspraken over maken. In de BIG zijn bewust géén specifieke standaarden als TLS, DMARC en DNSSEC genoemd. Het uitgangspunt vanuit VNG/IBD is dat gemeenten de ruimte moeten hebben om conform hun eigen risico inschatting de voor hen juiste maatregelen te kiezen. Kortom de gemeenten kunnen mogelijk niet mee op de gewenste versnelling van de adoptie van de genoemde standaarden.

Door het uitvoeren van een impactanalyse willen betrokken partijen uitzoeken welke impact de implementatie van deze standaarden voor gemeenten heeft, of die, zoals in de Regieraad1 is gesteld beperkt is, en of dat voor alle gemeenten geldt: de uitgangssituatie en de bekendheid met deze standaarden verschilt per gemeente en per standaard.

BFS heeft de IBD gevraagd een impactanalyse uit te voeren. Hiervoor zal het volgende worden opgeleverd c.q. uitgevoerd:

1. Beknopte impactanalyse DNSSEC;
2. Beknopte impactanalyse voor TLS, waarbij de NCSC configuratie leidend is;
3. Impactanalyse/Verkenning van de complexiteit bij gemeenten met als resultaat een plan van aanpak om te komen tot een uitrolstrategie voor SPF/DKIM en DMARC.

Deze rapportage betreft uitsluitend punt 3 van de totale opdracht.

Beschrijving onderzoek

In de opdracht wordt gesproken over drie standaarden die alle drie met e-mail authenticatie te maken hebben:

1. SPF
   Dit staat voor Sender Policy Framework. Het is een protocol dat tot doel heeft te helpen spam te verminderen door vast te stellen of de verzender van een mailbericht gerechtigd is om een bericht te verzenden namens de afzender van het bericht. Binnen het SPF protocol wordt aan het Domain Name System (DNS)-record een extra informatieveld van een domein toegevoegd. In dit record wordt vermeld welke mailservers namens dit domein mail mogen verzenden. Staat een mailserver niet in deze opsomming en verzendt deze toch mail met het betreffende domein als afzender, dan wordt de mail als onrechtmatig beschouwd.

2. DKIM
   Dit staat voor DomainKeys Identified Mail . Het is een techniek waarbij een organisatie verantwoordelijkheid kan nemen voor een bericht dat per e-mail wordt verzonden. DKIM zelf is geen technologie tegen spam, maar biedt een basis voor authenticatie, waarmee bijvoorbeeld reputatieservices opgezet kunnen worden. Deze reputatieservices op hun beurt kunnen dan gebruikt worden door anti-spamfilters.

3. DMARC
   Domain-based Message Authentication (DMARC) is een techniek die vraagt naar de identiteit van de verzender van e-mail. DMARC is een standaard waarin staat aangegeven hoe de ontvanger van e-mail aan de hand van bovengenoemde SPF en DKIM-mechanismen de herkomst van e-mail kan verifiëren. De verzender geeft met DMARC aan dat de e-mails zijn beschermd door SPF en/of DKIM en vertelt de ontvanger wat deze moet doen als het niet door de SPF/DKIM-test komt. Deze policy wordt in het publieke DNS gepubliceerd en is voor iedereen beschikbaar.

Door deze drie standaarden in samenhang in te richten kun je als gemeente voorkomen dat burgers en bedrijven spam- of phishing berichten krijgen vanuit gemeentelijke domeinnamen en er voor zorgen dat je inzicht hebt in pogingen om gemeentelijke domeinnamen te misbruiken voor spam of phishing. Uiteindelijk versterkt dit het vertrouwen in de gemeente als digitale dienstverlener.

Een typische implementatie van e-mail authenticatie omvat globaal de volgende stappen:

1. 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. Dit kan door in de DNS een DMARC-record aan te maken voor elke domeinnaam. Gebruik de eerste periode als policy de waarde ‘none’ en specificeer een e-mailadres waar mailservers de rapportages aan kunnen sturen. Door dit te doen ontstaat inzicht in mailstromen namens de gemeentelijke

domeinnamen door de DMARC terugkoppelingen van grote mailproviders te analyseren. Om de analyse te vergemakkelijken kunnen tools gebruikt worden.

2. Als er inzicht is in de legitieme mailstromen per domeinnaam kan het SPF beleid worden gepubliceerd als een TXT-record in de DNS-zone van de desbetreffende domeinnamen. Ook kan DKIM worden ingericht door het genereren van publieke en private sleutels en het toevoegen van de publieke sleutels aan de DNS-zone van de desbetreffende domeinnamen.
3. Nu dit gebeurt is kan met DMARC naar een striktere policy worden overgegaan. Dit kan via een overgangsfase. Publiceer daarvoor eerst een policy 'quarantine' om uiteindelijk zoveel mogelijk mailstromen te laten authentiseren door ze in het DMARC record 'reject' als beleid mee te geven.
4. Na de implementatie zullen configuratie en gebruik van de e-mailauthenticatiemiddelen gemonitord moeten worden om effectief te zijn. Hierbij dient onder andere gelet te worden op misbruik van een domeinnaam, problemen met geautoriseerde verzenders en aanpassingen aan mailservers

Omdat het inrichten van DKIM en SPF vooral een technische aangelegenheid is waar maar een beperkte hoeveelheid werk in zit lag de nadruk bij de impactanalyse op DMARC. Om de analyse representatief te laten zijn is er voor gekozen om met 30 gemeenten een praktijkcasus te doen. Deze casus bestond uit de volgende stappen:

- Het enthousiasmeren van gemeenten om deel te nemen aan de impactanalyse
- Het organiseren van een informatiebijeenkomst met deelnemende gemeenten
- Deelnemende gemeenten een DMARC record te laten toevoegen aan hun DNS met parameter p=none om de uitgaande e-mailstromen per domein te kunnen onderzoeken. Verder werden de DMARC records zodanig geconfigureerd dat de terugkoppelingen van de mailproviders centraal verzameld werden t.b.v. analyse door de IBD
- Het gedurende 8 weken verzamelen van de terugkoppelingen van alle deelnemende gemeenten
- Samen met deelnemende gemeenten per domein identificeren welke mailstromen legitiem zijn t.b.v. opname in het SPF-record
- Per gemeente inventariseren welke mailappliance wordt gebruikt t.b.v. het schatten van de impact voor DKIM implementatie

De totale praktijkcasus heeft een doorlooptijd gekend van vier maanden.

Bevindingen

- DMARC leeft nog niet echt bij de meeste gemeenten. Uitleg over nut en noodzaak en kennisoverdracht heeft dus tijd nodig.
- Bij veel gemeenten is enige terughoudendheid merkbaar bij het implementeren van een correct SPF record. De angst is toch aanwezig dat er mailstromen zijn die hier hinder van kunnen ondervinden.
- Het toevoegen van een DMARC record aan de DNS is op zich weinig werk met een korte doorlooptijd. Niet alle gemeenten beheren hun eigen DNS en moeten dan een ticket hiervoor aanmaken bij hun provider die daar in een enkel geval een klein bedrag voor in rekening bracht.

- Voor het identificeren van de mailstromen vanuit de terugkoppelingen van de mailproviders is kennis en tooling nodig.
- Vaak gebruiken leveranciers van klantcontactcentra en afsprakensoftware een externe hostingpartij waardoor het uitzoeken of een mailstroom legitiem is veel tijd kost.
- Gemeenten maken veel gebruik van dezelfde leveranciers voor mail en hebben de kantoormail uitbesteed aan externe hostingpartijen.
- Per gemeente zijn gemiddeld 4 a 5 verschillende mailstromen onderscheiden
- De belangrijkste mailstromen die we bij de praktijkcasus zijn tegengekomen zijn kantoormail, afsprakenmodules van klantcontactcentra en diverse nieuwsbrieven.
- Er zijn vrijwel geen mailstromen geconstateerd vanuit de grote gemeentelijke backofficeapplicaties.
- Er zijn diverse mailstromen geïdentificeerd die buiten de Europese Economische Ruimte worden gehost.
- Inhoudelijke terugkoppelingen vanuit mailproviders(zgn. forensics) zouden een privacy risico kunnen opleveren.
- Bij het analyseren van de gezamenlijke terugkoppelingen van alle domeinen is geconstateerd dat bij vrijwel alle onderzochte domeinen misbruik heeft plaatsgevonden. De domeinnamen werden gebruikt voor het versturen van spam. Onduidelijk is of de betreffende domeinnamen ook zichtbaar zijn voor ontvangers van de mail. Van het misbruik is melding gemaakt bij NCSC en politie.

Aanbevelingen

- Onderzoek de mogelijkheid om DMARC-terugkoppelingen van alle gemeenten of misschien wel alle overheidsorganisaties centraal te verzamelen t.b.v. constatering van misbruik op grote schaal.
- Maak voor gemeenten de resultaten beschikbaar van door andere gemeenten al geïdentificeerde mailstromen, bijvoorbeeld m.b.v. tooling.
- Formuleer een ondersteuningsaanpak vanuit de IBD voor gemeenten.
- Informeer de betrokken leveranciers van klantcontactcentra, hostingpartijen, providers e.d. over de nieuwe standaard zodat ze zich klaar kunnen maken voor vragen van gemeenten.
- Maak duidelijke factsheets, gericht op gemeenten.
- Adviseer gemeenten over de ontwikkeling of aanschaf van tooling waarmee ze de terugkoppelingen van mailproviders gemakkelijk kunnen interpreteren.