E-mailauthenticatie

Naar aanleiding van de publicatie "De Overheid als betrouwbare afzender (Architectuurraad Manifestgroep 11 maart 2014)" en een presentatie daarover is het idee ontstaan dat het CIP met een 'advies aan het netwerk' komt over e-mailauthenticatie: hoe weet je zeker wie de email heeft verstuurd; is het echt of nep?

De realisatie van e-mailauthenticatie spitst zich met name toe op (technische) protocollen waarmee verzonden e-mails kunnen worden voorzien van een verifieerbaar 'echtheidskenmerk' dat door de ontvanger kan worden nagetrokken. Op grond hiervan kan een redelijk niveau van zekerheid worden gegeven c.q. aangenomen omtrent de identiteit van de afzender. Dit is met name een wapen tegen phishing mails 'uit naam' van uw organisatie en kan onzekerheid over de gewenst/ongewenst status bij de ontvanger wegnemen. Met name mail uit grotere zendingen wordt door veel spamfilters gemakkelijk voor spam aangezien, ongeacht de inhoud.

Zeker wanneer een organisatie aan burgers e-mails verstuurt waaraan consequenties kunnen zitten voor de ontvanger, is het van belang dat de afzender geverifieerd kan worden. Het is daarom niet vreemd dat er bij de overheid al implementatieprojecten zijn gestart, en de vraag of uitvoerders namens de Rijksoverheid dit ook moeten willen is eigenlijk al niet meer aan de orde. Relevant is natuurlijk ook dat maatregelen voor e-mailauthenticatie zijn aanbevolen (dwz: pas toe of leg uit) door het Standaardisatieforum (www.forumstandaardisatie.nl).

Domeinverificatie, want daar hebben we het over, is niet gelijk aan een persoonlijke 'elektronische handtekening' onder een mailbericht: die verifieert de afzender als afzender. De e-mailauthenticatie waar we het hier over hebben verifieert het verzendende domein - dus geen individuele afzenders c.q. medewerkers van de organisatie.

Daarvoor is een aantal technische voorzieningen beschikbaar, die organisaties moeten implementeren. De ontvanger hoeft er niets van te merken, want hij is (vooralsnog) niet verplicht om de afzender te verifiëren. Maar als een organisatie de juiste maatregelen heeft getroffen dan kán een ontvanger dat wel als hij dat nodig vindt.
Banken doen het allang. UWV (bijvoorbeeld) werkt eraan. Het zal groeien en standaard gaan worden. De trend is er, maar vanwege niet verplichte afname aan ontvangerskant kan brede toepassing zoals het bedoeld is nog wel even duren.

De technische voorzieningen met de prozaïsche namen DNSSEC, SPF, DKIM en DMARC werken met elkaar samen om de gewenste zekerheden te verschaffen. Voor wie het allemaal weten wil: zij worden op heldere wijze en in relatie tot elkaar beschreven in de bijlage "E-mailsecurity als onderdeel van ICT-Beveiligingsrichtlijnen voor webapplicaties".

Naast dat ontvangers er in principe niet mee lastig gevallen worden, is het van belang om te weten met welke inspanningen en kosten een organisatie moet rekenen om deze voorzieningen operationeel te krijgen en te houden.

Voor het toepassen als verzender en kunnen verifiëren als ontvanger hebben beide kanten moderne maar geen ongebruikelijke of bijzonder (e-mail- en netwerk) software nodig. Voor bedrijven en organisaties met professionele leveranciers lijkt dat eerder geregeld dan voor particulieren, maar ook

daar begint het te komen: voor een e-mailprogramma als het populaire Thunderbird is een toevoeging te downloaden die verificatie van met DKIM gecertificeerde mails eenvoudig mogelijk maakt.

Voor organisaties betekent implementatie mogelijk wat aanschafkosten of upgrades van de mailsofware; niet exorbitant. De genoemde protocollen moeten natuurlijk geïnstalleerd, getest, ingeregeld ('getuned') en beheerd worden. Dit speelt vooral aan de verzenderskant en is een beperkte eenmalige inspanning voor implementatie, waarna beheer normaalgesproken niet veel extra werk met zich meeneemt. Zoals bij moderne spamfilters zal er in het begin wat meer, later minder werk zijn aan het finetunen en inrichten van eventuele uitzonderingen.

Individuele verzenders binnen de organisatie hebben er geen enkele last van, DKIM certificering werkt 'automatisch' op de achtergrond. En zoals al gezegd: voor de ontvanger is het een keuze er iets mee te doen, dat wordt (technisch) niet afgedwongen.

Voor de verzendende organisatie zijn er wel twee opletpunten. Een beetje jargon is hier helaas onvermijdelijk:

- DNSSEC vereist doorgaans wat meer inspanning omdat het een wat lastigere implementatie is en meer onderhoud vergt naarmate de organisatie (de netwerkomgeving) complexer is. Strikt genomen heeft het weinig van doen met de overige maatregelen voor e-mailauthenticatie, maar er ontstaat als het ware een gat in de voorziening als geen gebruik wordt gemaakt van beveiligde DNS. DNSSEC is overigens al enkele jaren een absolute aanrader, ook los van e-mailauthenticatie.
- Verzenders *buiten* het DKIM-domein van een organisatie, die zich willen voordoen als de verzender zelf - communicatiebureaus voor mailings bijvoorbeeld - moeten handmatig ingeregeld worden. Nu is het nog voldoende als ze worden bijgezet in het SPF register, voor DKIM is dat onvoldoende, daarvoor moeten ontvangers (!) een uitzondering regelen of aan de verzendende kant moet een list worden bedacht, bijvoorbeeld een extra (DKIM)domein voor externe verzenders. In de meeste gevallen zal dat laatste dus het geval moeten zijn.

Kortom:

- Het inrichten van voorzieningen voor e-mailauthenticatie is voor overheidsgerelateerde organisaties op weg naar 2017 geen open vraagstuk. Het hoeft niet op stel en sprong te gebeuren (er valt niets om) maar de wenselijkheid of, zo u wilt, de businesscase is er wel. En anders is er altijd nog het Standaardisatieplatform. Uitgerekend in Nederland is phishing een relatief groot probleem (in de top 3 van de wereld).
- Dit gaat gepaard met overzichtelijke en relatief beperkte kosten en implementatietrajecten - wel is er een relatie met de complexiteit van de organisatie. Voor organisaties die met andere verzenders namens de organisatie werken, zitten er ook nog wat lastigere aanpassings-activiteiten aan, afhankelijk van keuzes daarin mogelijk ook voor ontvangende partijen.
- Wie in 2017 compliant wil zijn aan de lijst van het Standaardisatieforum doet er goed aan nu reeds aan de implementatie te beginnen.

CIP/Ruud de Bruijn
28 mei 2014

Deze CIP-publicatie valt in de cat. 2 "becommentarieerde praktijk". Voor informatie hierover zie http://www.cip-overheid.nl/wp-content/uploads/2014/04/De-totstandkoming-en-status-van-CIP-publicaties-v1_2.pdf

BIJLAGE: E-mail security als onderdeel van ICT-Beveiligingsrichtlijnen voor webapplicaties

Auteurs:
Martijn Groeneweg
http://nl.linkedin.com/in/martijngroeneweg
martijn.groeneweg@mailmerk.com
Mailmerk, www.mailmerk.nl
+31651284506

Alwin de Bruin
http://nl.linkedin.com/in/alwindebruin
alwin.debruin@measuremail.com
Measuremail, www.measuremail.com
+31614169837

Publicatiedatum: 17 mei 2014

Kaderstelling

- De ICT-Beveiligingsrichtlijnen voor webapplicaties richten zich op webapplicaties en bijbehorende infrastructuur, de koppeling met internet, de opslag van de gegevens en de netwerkservices.
- Vanuit webapplicaties kan op diverse manieren e-mail worden verstuurd. Enkele voorbeelden (niet limitatief) zijn:
  i. Kantoormail vanuit een webmail omgeving
  ii. Bevestigingsmail vanuit een contactformulier op een website
  iii. Update status mail vanuit een e-loket
  iv. Nieuwsbrief vanuit een webapplicatie
  v. Bevestigingslink per mail bij registratie van een gebruiker
- Deze richtlijnen e-mail security zijn gericht op alle e-mail stromen die namens een (organisatie) domein worden verstuurd.

Proces en techniek

- Zorg ervoor dat geen onnodige procesinformatie in de headers van mail berichten meegestuurd wordt. Daarbij valt te denken aan IP adressen van interne systemen, systeemnamen, gebruikersnamen waaronder processen draaien, et cetera.
- Zorg ervoor dat de betreffende web applicatie niet misbruikt kan worden voor het verzenden van berichten naar willekeurige bestemmingen.
- Wanneer gebruik wordt gemaakt van webmail, maak dan gebruik van een goede en sterke wachtwoord 'policy'. Zorg ervoor dat enkel vanuit geauthentiseerde sessies berichten mogen worden verstuurd. Gebruik uitsluitend versleutelde verbindingen wanneer gebruikers van de webmail applicatie inloggegevens moeten invullen.
- Zorg ervoor dat de authenticiteit van de domeinnaam, die wordt gebruikt in e-mail adressen, te verifiëren is. Dit kan door registratie van SPF [SPF] records in DNS en door gebruik te maken van DKIM [DKIM]. Het is sterk aan te bevelen beide technieken te gebruiken.
- Voor zowel SPF als DKIM is het van belang per te gebruiken domeinnaam alle legitieme e-mail stromen in kaart te brengen. Het gebruik van e-mail in de context van web applicaties is niet los te zien is van het gebruik van e-mail elders binnen uw organisatie.

- Om misbruik van uw domeinnaam zoveel mogelijk tegen te gaan wordt sterk aanbevolen om gebruik te maken van de DMARC techniek.

Richtlijnen SPF

i. Vermeld alle IP adressen, waarvandaan legitieme e-mail kan worden gestuurd namens een domein, in het DNS SPF record voor dat betreffende domein.
ii. Gebruik DNS resource records van het type TXT voor de registratie van de SPF gegevens. Het gebruik van DNS resource record van het type SPF wordt in de komende versie van de standaard uitgefaseerd; enkel TXT records zijn dan nog toegestaan [SPFbis].
iii. Voor alle domeinnamen, waarvandaan in het geheel geen mail wordt gestuurd, moet een SPF record opgenomen met policy '-all' om misbruik ervan zoveel mogelijk tegen te gaan.

Richtlijnen DKIM

i. Kies zorgvuldig de domeinnaam die u wilt gebruiken voor gebruik in de DKIM handtekening.
ii. Genereer een sleutelpaar en bewaar de zgn. 'private key' in overeenstemming met de richtlijnen … Publiceer de zgn. 'public key' in DNS.
iii. Gebruik een apart sleutelpaar per organisatie. De organisatie maakt zelf het sleutelpaar aan. De private key blijft binnen organisatie. Wanneer u gebruik maakt van een 'Third Party' voor het DKIM signen van uw mail, zorg er dan voor dat er afspraken zijn met deze partij omtrent de vertrouwelijkheid van de private key.
iv. Genereer en gebruik regelmatig een nieuw public-key/private key sleutelpaar om de DKIM handtekening mee te genereren, tenminste jaarlijks.
v. Gebruik een sleutelpaar van 1024 bits. 512 bits is onveilig en wordt door Gmail niet meer geaccepteerd. 2048 bits is te lang voor sommige DNS servers en vergt meer server resources.
vi. Gebruik een vast format voor de Selector bijvoorbeeld het format 2013.xxxx waar xxxx een uniek kenmerk is voor de organisatie.
vii. Gebruik als Algoritme rsa-sha256 zoals aanbevolen in RFC 6376.
viii. Gebruik relaxed header canonicalisatie en simple body canonicalisatie zoals aanbevolen door dkimcore.org
ix. Om misbruik van uw domeinnaam tegen te gaan en zichtbaar te maken, wordt aanbevolen de richtlijnen in [DMARC] te hanteren. Zorg er daarbij voor dat de domeinnaam in het voor gebruikers zichtbare afzender adres (het RFC5322.From: adres, zie [RFC5598]) in 'alignment' is met zowel (zie voor meer informatie par. 4.2 van [DMARC]):
    1. de DKIM-signature domeinnaam als met:
    2. het zgn. 'envelope' afzenderadres (RFC5321.MailFrom).

Richtlijnen DMARC

- DMARC record op basis (organizational) domein. Let op dat dit ook van toepassing kan zijn op willekeurige subdomeinen.
- Basis domein (organizational domein) van envelope sender moet overeenkomen met basis domein van From: header domein (Relaxed alignment envelope sender).
- Zorg dat de Signing identity (d=) exact overeen komt met From: header domein. Vergelijkbaar met stricte alignment in DMARC en vereist door Microsoft Hotmail.
- Zowel SPF als DKIM implementeren op alle mailstromen. Anders geen quarantine of reject toepassen.
- Start met “none” policy. Naar “reject” policy indien alle e-mail stromen SPF- en DKIM compliant zijn.
- Harde eis voor stricte DKIM aligment in DMARC record, zodra wordt overgestapt op “reject”. Wel zachte eis voor SPF (relaxed) in verband met false positives bij forwarding.
- Monitor eventueel misbruik van de betreffende domeinnaam door derden, middels een juiste instelling van de rapportagemogelijkheden die DMARC biedt. Neem onmiddellijk actie wanneer blijkt dat derden misbruik maken van uw domeinnaam in mail adressen.

NB Zoals reeds aangegeven bij de kaderstelling is het essentieel om bij de hier genoemde punten niet enkel te kijken naar het gebruik van e-mail sec binnen webapplicaties, maar ook alle andere e-mail stromen binnen uw organisatie aan de Richtlijnen e-mail security te laten voldoen.

Best Current Practice

Let op: wanneer u aan de slag gaat met SPF, DKIM en DMARC, maak dan gebruik van de volgende tips en aanbevelingen om kosten in de toekomst te vermijden.

SPF:
Gebruik daar waar mogelijk de zogeheten ‘hard fail policy’ door toepassing van “-all”. Een SPF failure mag op zichzelf tot reject leiden door ontvangende e-mail server. Let op het risico op false positives bij forwarding.

DKIM:
Zorg dat de Signing identity (d=) exact overeen komt met From: header domein. Vergelijkbaar met stricte alignment in DMARC en vereist door Microsoft Hotmail.

DMARC:
Basis domein (organizational domein) van envelope sender moet overeenkomen met basis domein van From: header domein (Relaxed alignment envelope sender).

Referenties

[DMARC] DMARC draft specificatie, M. Kucherawy, 30 maart 2012, zie
http://www.dmarc.org/draft-dmarc-base-00-02.txt

[RFC5598] Internet Mail Architecture, D. Crocker, juli 2009, zie
http://tools.ietf.org/html/rfc5598

[SPF] Sender Policy Framework for Authorizing Use of Domains in E-Mail, Version 1, M. Wong et al, april 2006, zie http://tools.ietf.org/html/rfc4408

[SPFbis] Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, S. Kitterman, januari 2013, zie
http://tools.ietf.org/html/draft-ietf-spfbis-4408bis-09

[DKIM] DomainKeys Identified Mail (DKIM) Signatures, D. Crocker et al, september 2011, zie http://tools.ietf.org/html/rfc6376.