Intentieverklaring Veilige E-mail Coalitie

Nederland is koploper in de online wereld. Miljoenen Nederlanders verzenden en ontvangen dagelijks samen tientallen miljoenen e-mailberichten.

Onveilige e-mail zorgt helaas dagelijks voor misbruik en schade. Bedrijven, particulieren en overheden moeten erop kunnen vertrouwen dat hun e-mail veilig is. Dat betekent dat er passende beveiligingsmaatregelen moeten worden genomen. Willen die maatregelen ook echt effectief en efficiënt zijn, dan is het gebruik van de juiste standaarden in de gehele keten van verzenders en ontvangers cruciaal.

Met de Veilige E-mail Coalitie nemen bedrijfsleven en overheid het gezamenlijke initiatief tot brede invoering van e-mailbeveiliging en up-to-date standaarden. Bij dat laatste gaat het om, DMARC+DKIM+SPF tegen phishing en STARTTLS+DNSSEC+DANE tegen afluisteren. Door het open karakter van deze standaarden zijn die voor alle organisaties beschikbaar.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ontplooit in dit verband initiatieven om, in eerste instantie voor de rijksoverheid, maar vervolgens ook voor de overheid als geheel, de invoering van passende beveiligingsmaatregelen verplicht te stellen. De standaarden die de bedrijven en overheid hanteren voor beveiligd e-mailverkeer zijn getoetst en aangewezen door het publiek-private Forum Standaardisatie, op initiatief van het ministerie van Economische Zaken. Het Platform Internetstandaarden, een samenwerkingsverband van de Nederlandse internetcommunity en overheid, promoot de standaarden sinds bijna twee jaar onder andere met de testwebsite Internet.nl.

De ondertekenaars vormen een coalitie om het vertrouwen in en de veiligheid van e-mail te vergroten. Zij doen wat in hun vermogen ligt om de genoemde beveiligingsmaatregelen binnen hun organisaties in te voeren. Zij werken daarbij intensief samen aan een invoeringsplan en delen kennis en ervaring.

De initiatiefnemers vormen hiermee een coalitie die zich sterk maakt voor veilig e-mailverkeer en toenemend vertrouwen van de gebruikers, en zij roepen andere organisaties op dit voorbeeld te volgen.

Den Haag, 2 februari 2017

Initiatiefnemers Veilige E-mail Coalitie

Met support van Platform Internetstandaarden

Achtergrond van Veilige E-mail Coalitie

E-mail is het meest gangbare digitale communicatiemiddel

Miljoenen Nederlanders verzenden en ontvangen dagelijks samen tientallen miljoenen e-mailberichten. Bedrijven, particulieren en overheden moeten daarom kunnen vertrouwen op veilige e-mail. Veilige e-mail is echter niet vanzelfsprekend.

Voor criminelen is e-mail een aantrekkelijk doelwit

E-mail via onbeveiligde verbindingen kan gemakkelijk worden onderschept. Nederlandse bedrijven en particulieren lopen daardoor het risico dat bedrijfsinformatie of persoonsgegevens in verkeerde handen terecht komen. Een ander risico vormen vervalste e-mails die criminelen sturen uit naam van bijvoorbeeld ondernemingen of banken (phishing), en die soms zeer persoonlijk gericht zijn (spear phising). Dit kan ernstige zakelijke en persoonlijke schade veroorzaken (financieel, reputatie). Het Nationaal Cyber Security Centrum (NCSC) bestempelt het afluisteren van e-mail en e-mail-phishing al een aantal jaren als groot risico in zijn jaarlijkse Cyber Security Beeld.

Up-to-date standaarden maken e-mail aanmerkelijk veiliger

E-mail wordt aanmerkelijk veiliger door invoering van de gestandaardiseerde echtheidskenmerken DMARC+DKIM+SPF (bij verzending) en de controle daarop (bij ontvangst). De standaarden STARTTLS+DNSSEC+DANE zorgen voor versleuteling van de communicatie tussen de e-mailsystemen van providers, waardoor e-mail niet zomaar kan worden afgeluisterd. Het is noodzakelijk deze up-to-date standaarden voor e-mail-beveiliging breed in te voeren, want het werkt alleen als alle betrokken partijen deze standaarden doorvoeren; leveranciers van e-mailsystemen, e-mail-providers en organisaties die zelf veel e-mailen.

De coalitie wil de invoering van veilige standaarden versnellen

De initiatiefnemers van de Veilige E-mail Coalitie zijn aanbieders en beheerders van e-mail-faciliteiten. Zij staan klaar om veilige standaarden in te voeren in hun systemen of zijn daar al mee bezig. De e-mailbeveiligingsstandaarden die de coalitiepartners invoeren zijn DMARC+DKIM+SPF (tegen phishing) en STARTTLS+DNSSEC+DANE (tegen afluisteren). De coalitiepartners werken samen en delen 'best practices' voor een goede en snelle invoering in het belang van de eigen organisatie en van hun relaties.

Toelichting standaarden

1. Standaarden ter preventie van phishing

DKIM
Met DKIM wordt de elk uitgaand e-mailbericht van een digitale handtekening voorzien. Zo wordt voorkomen dat kwaadwillenden een bericht namens een ander kunnen verzenden (spoofing) of de inhoud van een bericht onderweg kunnen veranderen.

SPF
SPF voorkomt dat e-mailberichten van ongeautoriseerde computersystemen geaccepteerd worden. Het werkt via een online gepubliceerde lijst waarmee ontvangende systemen de geldigheid van de verzender controleren voor zij een bericht aannemen.

DMARC
DMARC is een aanvulling op DKIM en SPF en geeft aanwijzing hoe om te gaan met inkomende berichten waarvan de DKIM- of SPF-controle niet in orde blijkt te zijn. Berichten worden weggegooid of apart gezet en die informatie wordt gedeeld met de beheerder van het afzenddomein.

2. Standaarden ter preventie van afluisteren

STARTTLS
De verbinding tussen de mailservers kan met TLS worden versleuteld door gebruik te maken van het protocol STARTTLS. Beide mailservers moeten STARTTLS ondersteunen om de versleuteling te laten werken. Versleuteling met STARTTLS beschermt goed tegen afluisteren door een passieve aanvaller die afluistert zonder het berichtenverkeer te manipuleren.

DNSSEC+DANE
Als een verzendende mailserver DNSSEC-validatie toepast, dan kan deze betrouwbaar een met DNSSEC ondertekende domeinnaam van de ontvangende mailserver opvragen. DANE is een techniek die voortbouwt op DNSSEC. Als beide zijden van de verbinding DANE toepassen, kan versleuteling met STARTTLS worden afgedwongen. Het kan voorkomen dat een actieve aanvaller, die tracht het berichtenverkeer te manipuleren, de mailverbinding tussen mailservers afluistert.

Contactgegevens

Platform Internetstandaarden
p/a ECP
Overgoo 13
Postbus 262
2260 AG Leidschendam
WWW: https://www.internet.nl/

Contactpersoon
Gerben Klein Baltink, voorzitter Platform Internetstandaarden
Email: gerben@internet.nl

Ondertekening

Organisatie	Naam vertegenwoordiger	Handtekening
PostNL	Marcel Krom CIO	
KPN	Jaya Baloo CISO	
Betaalvereniging Nederland	Marco Doeland Head of Risk Management	
DDMA	Monique Rutten Adjunct directeur	
Thuiswinkel.org	Roland van Kortenhof Manager Operations en ICT	
VNO-NCW & MKB-Nederland	Erik te Brake, Manager Regelgeving, Marktwerking en Consumentenbeleid	
Stichting Zeker-Online	Bianca Smit Directeur	
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Hans Wanders Rijks-CIO	
XS4ALL	Jan-Pieter Cornet Postmaster	

Organisatie	Naam vertegenwoordiger	Handtekening
Stichting DINL	Michiel Steltman Directeur	
Nederland ICT	Lotte de Bruijn Directeur NL-ICT	
Fraudehelpdesk	Fleur van Eck Directeur	
Dutch Datacenter Association	Stijn Grove Directeur	
Belastingdienst	Sjef Klomp Security Officer	
Platform Internetstandaarden	Gerben Klein Baltink Voorzitter	