Forum Standaardisatie

Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.forumstandaardisatie.nl

notitie

Aan:	Forum Standaardisatie		
Van:	Bureau Forum Standaardisatie		
Datum:	13 september 2017	**Versie**	1.0
Betreft:	Overzicht reactie openbare consultatieronde functioneel toepassingsgebieden internet veiligheidstandaarden		
Bijlagen:	1. Reactie Networking4all		

1. Reactie Networking4all

Van: Sebastian Broekhoven
Verzonden: dinsdag 29 augustus 2017 8:37
Aan: Forum standaardisatie
Onderwerp: Consultatieprocedure functioneel toepassingsgebieden internet veiligheidstandaarden

Beste,

Bij deze wil ik graag reageren op de openbare consultatie.
https://www.forumstandaardisatie.nl/content/openbare-consultatie-functioneel-toepassingsgebieden-internet-veiligheidstandaarden

Vraag 1:
Nee

Vraag 2:
Ja, het lijkt mij handig dat er vanuit NCSC een aanbeveling moet komen voor een goed SPF record. Het opstellen van een SPF record met hierin bijvoorbeeld een +all of een ptr: optie helpt niet mee aan de veiligheid. Dus niet alleen het toepassen, maar ook het "goed" toepassen van de standaarden is van belang. Echter heeft SPF nog wel meer nadelen. Zoals het gebruik van aliassen/forwarders op email adressen.

Vraag 3:
Ja. DKIM toepassen is goed. Echter moet er ook op gelet worden dat de implementatie goed is. Als de mail binnen komt bij een van de mx-server en DKIM is daar goed, moet de inhoud van de mail onderweg naar de mailbox van de ontvanger niet meer aangepast worden. Want daar gaat DKIM op stuk. Op bijvoorbeeld een server met een virusscanner welke in de body van het bericht plaatst: "E-mail is op virussen gescand door Merk X". Deze informatie kan ook in de header van de e-mail.

Vraag 4:
Het gebruik van DMARC is zeker aan te raden. Wel zal in de toekomst zeker ook gekeken moeten worden naar het ARC-protocol wat problemen met DMARC corrigeert. Het ARC protocol is echter nog jong, het is geboren in 2016. Google gebruikt het al en andere partijen hebben ook aangekondigd dit te implementeren. Ook al is DMARC geen IETF standaard, het is een project van het Trusted Domain Project welke betrouwbaar is. Hou wel weer rekening met de valkuilen van DMARC. Omdat DKIM en SPF beide genoeg valkuilen hebben, is het nodig deze te verduidelijken.

Tot nu toe is het advies, gebruik DMARC tot de eerste "hop" waar de mail binnen komt en DMARC gecontroleerd word, gebruik verder daar achter het ARC-protocol.

Dus: DMARC, zeker gebruiken. Kijk echter ook verder naar ARC.

Vraag 5:
Ja, als het duidelijker kan mag het duidelijker. Echter HTTPS / HSTS is natuurlijk altijd iets tussen de client (browser) en de webserver (dmv headers) met de website en applicatie er op.

Vraag 6:
Nee, niet helemaal.
TLS gebruiken tussen applicaties is goed. Het is een standaard welke tussen 2 totaal verschillende applicaties goed kan werken. Het gebruik van IPsec is leuk, maar als dat betekend dat de applicatie niet-versleuteld mag communiceren met een andere applicatie lijkt mij dat niet goed.

DNS over TLS staat nog te veel in de kinderschoenen. Net als bij DNSSEC is dit ook grotendeels afhankelijk van de resolvers bij de instellingen en access providers.

Vraag 7:
Ja, DNSSEC moet gebruikt blijven worden. Wel zijn er nog te veel afhankelijkheden waardoor niet iedereen vanzelfsprekend gebruik maakt van DNSSEC.

Vraag 8:
Ja, standaarden als SPF, DKIM, DMARC, HTTPS+HSTS, TLS en DNSSEC zijn in theorie voor iedereen goed in te zetten. Ook zal dit wel gestimuleerd moeten worden vanuit de overheid. Niet alleen waarom, maar ook de richtlijnen voor het goed gebruiken van deze standaarden.

Andere aankomende standaarden zoals ARC zouden op iets van een roadmap moeten komen. Zo misschien ook de combinatie SMTP/TLS/DANE

Kind regards | Met vriendelijke groet,

Sebastian Broekhoven
Product Manager Security

Networking4all B.V.