edustandaard

Concept Verslag werkgroep Uniforme Beveiligingsvoorschriften (mei 2020)

Maandag 18 mei 2020, 13:00 – 15:00. Locatie: online.

Aanwezig: Arnold Greving (DUO), Dirk Linden (Kennisnet, voorzitter), Jaap Mooij (Kennisnet), Joost van Dijk (Surfnet), Jordy van den Elshout (Kennisnet, verslag), Rimmer Hylkema (ThiemeMeulenhoff) en Robert Klein (Kennisnet)

Afwezig: Olav Loite (VDOD), Marten Bakker (The Learning Network)

Agenda

1. Opening
   a. Verslag voorgaande bijeenkomst vaststellen
   b. Actielijst doornemen
2. TLS-voorschriften
   a. Integraal doornemen, waarbij we inzoomen op:
      i. Technische mogelijkheden voor certificaatcontrole
      ii. Duidelijkheid in samenhang
      iii. Bijlage I: Afspraken over uitfaseren (H2M)
   b. Vervolg
      i. ROSA-scan, afstemming andere werkgroepen en agenderen voor Architectuurraad 2 juli 2020
3. Veilig en betrouwbare e-mail (SPF, DKIM en DMARC)
   a. Afspraken maken o.b.v. huidige informatie en materialen
4. Andere beveiligingsstandaarden
   a. Wet Digitale Overheid (zie bijlage)
5. Afsluiting
   a. Volgende bijeenkomst

1. Opening

Het overleg start ongeveer 30 min later, aangezien een deelnemer problemen heeft met het geluid en verbinding met een alternatief ook niet voor iedereen werkt. De voorzitter stelt voor om het verslag van het voorgaande overleg door te lopen, waarbij we expliciet stilstaan bij de acties.

Jordy laat weten dat Olav en Marten niet aanwezig kunnen zijn. Beide zijn gevraagd om op- of aanmerkingen te maken op de voorschriften. Van Olaf hebben we een reactie gehad. Die heeft geen opmerkingen en is akkoord met de huidige versie.

a. Verslag voorgaande bijeenkomst(en)

Het verslag is doorgenomen en er zijn geen opmerkingen. Het verslag Maart 2020 is daarmee vastgesteld.

b. Actielijst

De meeste acties zijn afgerond en zijn verwerkt in de laatste versie van de voorschriften. Deze worden besproken tijdens het integraal doornemen van de voorschriften, aangezien daar de focus op ligt.

Actie #10 m.b.t. de 'technische mogelijkheden voor het controleren van certificaten' heeft door omstandigheden vertraging opgelopen. Wel is de uitkomst tot nu toe verwerkt in de voorschriften en wordt daar verder besproken.

2. Uniforme Beveiligingsvoorschriften

De voorzitter stelt voor dat we de voorschriften integraal doornemen. Het is belangrijk dat we het eens zijn over hetgeen wat nu vastgesteld is, aangezien we een volgende fase ingaan van de voorschriften.

a. Integraal doornemen

Alle openstaande punten zijn verwerkt in de laatste versie van de UBV. Deze versie is voorafgaand toe gestuurd, met het verzoek deze integraal door te nemen. Tijdens dit agendapunt bespreken we de laatste op- en aanmerkingen. Daarbij zoomen we tevens in op de laatste wijzigingen, die in het document gemarkeerd zijn.

De afspraak rondom het gebruik van poort 443 is daarbij nogmaals besproken. Voor bestaande verbindingen kan een alternatieve poort gebruikt worden. Dat is de uitzondering. Een serviceregister voor het poortnummer hoeft er niet te komen, want kan in de standaardnotatie voor URL meegenomen worden die je tussen partijen hebt afgesproken. Het feit blijft wel dat - met name door de breed beschikbare optie SNI - alternatieve poortnummers niet meer nodig zijn en bijdraagt aan een veilige situatie en een efficiënt beheer. Nieuwe verbindingen zouden dan ook poort 443 moeten gebruiken.

<u>Afspraak</u>
De afspraak - over poort 443 zoals deze nu geformuleerd staat - blijft staan.

Tekstvoorstel voor het onderscheid met legacy-situatie besproken en sluit beter aan op wat we met beogen met deze afspraak.

Daarnaast stilgestaan bij Hoofdstuk 5. PKI, waarin een aantal acties zijn verwerkt. Het voorbeeld van Let's Encrypt is bijgewerkt onder DV. Daarnaast is het gebruik van wildcard certificaten beperkt voor gevoelige gegevensuitwisselingen. Hier zijn geen opmerkingen op. Wel wordt de vraag gesteld of certificaten voor DV in alle gevallen gebruikt mag worden. Daar is op dit moment geen bezwaar tegen. Wel van belang dat aangegeven wordt dat dit de minimale eisen zijn. Minimaal DV.

Daarnaast is het verzoek om hulptools op te nemen in de voorschriften, zodat men eenvoudig kan controleren of de configuratie veilig is. Voorbeelden hiervan zijn internet.nl, ssllabs.com en hardenize.com. Daarnaast zijn er ook een scripts zoals testssl die voor M2M kunnen helpen als de servers niet beschikbaar zijn vanaf het internet. Wat vaak het geval is. Wel moet er rekening gehouden worden dat hulptools snel kunnen verouderen. De classificatie die bv. uit ssllabs naar voren komt, kan gekoppeld worden aan de BIV-classificatie.

<u>Actie Jordy</u>
Hoofdstuk 5. PKI bijwerken, zodat duidelijk is dat DV minimaal is. Daarnaast welke hulptools beschikbaar zijn voor het controleren de configuraties.

i. Technische mogelijkheden voor certificaatcontrole

De bijbehorende actie #10 is nog niet afgerond, echter zou dit wel het geval moeten zijn want er zitten nog wat haken en ogen aan de implementatie. Bijvoorbeeld wanneer de resources

voor OCSP niet beschikbaar zijn, heeft dit impact op de beschikbaarheid van de gegevensuitwisseling. Daarnaast is er nog geen duidelijkheid of uitspraak over hoe partijen moeten reageren op het verlopen of ingetrokken certificaten. Wel is de werkgroep het er mee eens dat het certificaat gecontroleerd moet worden.

Aangezien er nog teveel onduidelijk is, stelt de voorzitter voor om dit eerst nader uit te werken. Waarbij we het uitgangspunt nemen dat certificaat controle moet plaatsvinden. Daarbij moet duidelijk worden 'wat' de consequenties moeten zijn van enerzijds 'verlopen certificaten' en 'ingetrokken certificaten'. Vervolgens bepalen 'hoe', zoals welke technische mogelijkheden hiervoor zijn.

Afspraak
Om de voorschriften voor certificaat controle scherp te krijgen, wordt dit komende 2 á 3 weken apart opgepakt met de werkgroep via de e-mail.

Actie Allen
Jordy stuurt een verzoek rond, zodat een ieder invulling kan geven aan 'wat' de consequenties moeten zijn van certificaat controle. Arnold en Robert werken vervolgens de 'hoe', wat overigens grotendeels is gedaan i.r.t. actie #10. Dit geldt zowel voor de situatie M2M als voor de situatie voor H2M.

ii. Duidelijkheid in samenhang
De samenhang tot verschillende standaarden en uitwisseling contexten was niet voldoende scherp beschreven, dan wel gelinkt naar de juiste bronnen. Hiervoor is de tekst onder Hoofdstuk 1 bijgewerkt.

Daarnaast vraagt de voorzitter of iemand ideeën heeft bij de scoping van het document. Een (UBV) document voor alles of apart per thema, zoals nu de TLS-voorschriften. Rimmer stelt voor dat het wel handig is om per thema een apart document op te stellen. Dit als onderdeel van UBV als geheel. De voorzitter stelt dan ook het volgende voor, wat voor iedereen akkoord is:

Afspraak
Per thema één document, waarbij het eerste hoofdstuk de samenhang met UBV en andere thema's wordt toegelicht.

iii. Bijlage I: Afspraken over uitfaseren (H2M)
Zowel de inhoud als opzet besproken. Daar zijn geen op- of aanmerkingen op.

b. Vervolg

i. ROSA-scan, afstemming andere werkgroepen en agenderen voor Architectuurraad 2 juli 2020
Alle gemaakte opmerkingen worden verwerkt tot een volgende versie. Deze versie wordt voorgelegd voor een ROSA-scan. Daarnaast zal afstemming plaatsvinden met andere standaarden. Vervolgens wordt de versie voorgelegd voor de Architectuurraad van 2 juli 2020. De vraag van de voorzitter is of daar op- of aanmerkingen bij zijn. Die zijn er niet.

3. Veilig en betrouwbare e-mail (SPF, DKIM en DMARC)

a. Afspraken maken o.b.v. huidige informatie en materialen

Dit is het volgende onderwerp die we verder willen uitwerken. Rimmer heeft hier het nodig voor uitgewerkt, echter stelt hij voor om dit eerst voor te bereiden. In een zelfde vorm als de TLS-voorschriften. Een belangrijk invalshoek daarbij is de waarom, zoals vorige keer ook in de presentatie werd aangehaald. Dat sluit aan op de adviezen voor de KRO's.

Afspraak
Rimmer, Dirk en Jordy bereiden het geheel voor, door een eerste aanzet van de voorschriften voor Veilige en Betrouwbare E-mail. Hiervoor wordt een afspraak gepland.

Actie Jordy
Afspraak plannen met Rimmer, Dirk en Jordy voor een eerste aanzet van de voorschriften voor Veilig en Betrouwbare E-mail.

4. Andere beveiligingsstandaarden

Edustandaard heeft het verzoek gekregen om de WDO-beveiligingsstandaarden op te nemen binnen ROSA. In de bijlage is te zien welke standaarden dit zijn, die overigens grotendeels behandeld zijn of worden binnen onze werkgroep.

DANE heeft echter wel een grote impact, ook wanneer hier fouten in worden gemaakt. Dit wordt opgepakt onder het thema Veilig en betrouwbare e-mail, echter is het de vraag of dit voorgeschreven kan worden. Het middel niet erger is dan de kwaal. Dat wordt binnen dit thema onderzocht.

Daarnaast draagt Rimmer een ander thema aan: 'Security headers'. Aantal daarvan worden getoetst in de hulptool van internet.nl. Waarom deze geen onderdeel zijn van de WDO, is de vraag. Wel is de werkgroep het er mee eens om dit ook als thema op te pakken. Ook zou hier een hogere prioriteit aangegeven moeten worden dan DANE.

DNSSEC valt niet binnen één van de eerder genoemde thema's. Deze kan separaat opgepakt worden onder het thema 'Domeinnaambeveiliging'.

Afspraak
'Security headers' wordt als apart thema opgepakt. Deze en de WDO-beveiligingsstandaarden worden in de volgende thema's opgepakt:

Standaard	Doel standaard	Thema (status)
TLS/HTTPS Het NCSC heeft aanvullende eisen t.a.v. cijfersuites	Beveiligde verbinding	TLS (in afronding)
DNSSEC	Domeinnaambeveiliging	Domeinnaambeveiliging
SPF	Anti-phishing email	Veilig en betrouwbare e-mail (Bezig)
DKIM	Anti-phishing email	Veilig en betrouwbare e-mail (Bezig)
DMARC	Anti-phishing email	Veilig en betrouwbare e-mail (Bezig)
HTTPS, HSTS en TLS conform NCSC richtlijn	Beveiligde verbinding	TLS (in afronding)

STARTTLS en DANE. Voor gebruik van DANE gelden strikte policies	Encryptie van mailverkeer	Veilig en betrouwbare e-mail (Bezig)
SPF en DMARC	Strikte policies voor emailstandaarden	Veilig en betrouwbare e-mail (Bezig)
Security headers*		Security headers

5. Afsluiting

De voorzitter vraagt een ieder of hij nog iets anders heeft, maar dat is niet het geval. De volgende afspraak is afhankelijk van het verdere proces voor de vaststelling van de TLS-voorschriften. Om wel alvast een datum te hebben staan, is een voorstel voor na de zomervakantie gedaan: maandag 31 augustus 2020. Wanneer we eerder iets hebben te bespreken, wordt dit per e-mail besproken en of een apart overleg voor gepland.