edustandaard

Concept Verslag werkgroep Uniforme Beveiligingsvoorschriften (januari 2020)

maandag 27 januari 2020, 13:00 – 15:00

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

Afwezig: Marten Bakker (The Learning Network)

Agenda

1. Opening
    a. Verslag voorgaande bijeenkomst vaststellen
2. Uniforme Beveiligingsvoorschriften; het concept doornemen
    a. Opzet en structuur
        i. Verwijzen of expliciet opnemen van richtlijnen NCSC
    b. Inhoudelijk (M2M)
        i. Verschil tussen Serviceaanbieder en Servicegebruiker; een selectie van de minimale cipher suites toestaan voor Servicegebruikers?
        ii. OCSP-Stapling (M2M) of andere invulling voor controle van certificaten; wat is het risico wanneer de geldigheid niet gecontroleerd kan worden?
        iii. Verplichting van poort 443; tegenstrijdig met Edukoppeling; wel of niet gewenst?
        iv. Verplicht opnemen van SNI; wenselijk, maar ook haalbaar?
    c. Inhoudelijk (H2M)
        i. OCSP-Stapling (M2H); privacy versus security; keuze of voorschrijven?
        ii. HTTPS hier of elders verplicht stellen, zoals wettelijke verplichtingen?
    d. Wanneer welke certificaat
        i. PKIoverheid indien OIN verplicht en de integriteit noodzakelijk is?
        ii. Wanneer welke soort certificaat, zoals DV, OV en EV?
    e. Afspraken over (uit)fasering
        i. TLS-configuraties ‘Uit te faseren’
        ii. Versie TLS 1.3
    f. Vervolg: afstemming met Edukoppeling en andere (gelieerde) standaarden
3. Wettelijke verplichtingen
    a. Presentatie met praktijkvoorbeelden
    b. Vervolg
4. Afsluiting
    a. Andere onderwerpen?
    b. Volgende bijeenkomst

1. Opening

De voorzitter opent de vergadering en vraagt of er onderwerpen missen op agenda. Dat is niet het geval en de voorzitter stelt voor om het verslag van de vorige bijeenkomst na te lopen. Daarbij is expliciet stilgestaan bij de acties en afspraken, en of we daarover eens zijn. Waaronder die van het volgen van de TLS-voorschriften van NCSC, waar we straks in de agenda rekening mee houden.

Op basis van het verslag zijn de volgende opmerkingen gemaakt (per punt):

Afspraak over onderscheid tussen M2M en H2M
Het maken van het onderscheid wordt door de werkgroep onderschreven, echter levert de term M2C verwarring op. De voorzitter licht daarom toe dat de term H2M (human-to-machine) gehanteerd wordt i.p.v. M2C, omdat dit een meer gebruikte term is. Zo wordt dit ook in de standaardisatieraad gebruikt. In Edukoppeling wordt gesproken over S2S (system-to-system), echter zou het goed zijn om hier ook eenduidig in te zijn. Joost merkt daarbij op dat er tevens verschil kan zijn tussen frontend en backend, en H2M meestal over browserverkeer gaat. Werkgroep stelt dan ook voor om het onderscheid goed toe te lichten, ten behoeve van de leesbaarheid van de voorschriften. Daarbij houden we de scheiding van M2M en H2M aan en worden varianten daarop als voorbeeld toegelicht.

Aanvullende afspraak
We hanteren de termen M2M en H2M voor het onderscheid. Deze begrippen worden toegelicht - met voorbeelden - om onduidelijkheden te voorkomen.

Afspraak over afhandeling op separaten domeinen (FQDN)
Bij dit punt wordt een aanvulling door Arnold aangedragen, waarbij ook scheiding aangebracht zou moeten worden voor legacy situaties. Wat overigens geldt voor beide communicatiesoorten: M2M en H2M. Dat punt komt tevens terug in de afspraken die we maken. Bijvoorbeeld bij het gebruik van 'uit te faseren' configuraties voor H2M. Dat wordt ook door Olaf aangehaald en benadrukt daarbij om deze ruimte standaard niet te bieden voor M2M. Dat wordt gedeeld door de werkgroep. Kanttekening die daarbij wordt gemaakt is dat *libraries* vaak niet alle configuraties met classificatie 'goed' zullen ondersteunen. Daar zullen we rekening mee moeten houden.

Daarnaast merkt Joost op dat term domeinen verwarring kan scheppen. Daarop wordt voorgesteld om FQDN te gebruiken, waar de werkgroep het mee eens is. Dat wordt bijgewerkt in het verslag van november 2019.

Afspraak over voorschriften o.b.v. profielen
Arnold geeft aan dat dit relatie heeft met zijn eerdere aanvulling voor legacy situaties. Belangrijk daarbij is wel, dat dit technisch niet vanuit één bron (FQDN, serverconfiguratie, virtual host) moet komen. Dit, om een downgrade attack naar legacy instellingen te voorkomen.

Het voorbeeld wat gegeven wordt over de impact van TLS 1.3 - wat impact heeft op TLS Interception - schept volgens Joost verwarring. De term TLS (Terminiation) proxy spreekt meer voor zich, in de context waar we het binnen deze werkgroep over hebben. Dat wordt gedeeld door de werkgroep. Voor de duidelijkheid wordt het voorgaande verslag daarop aangepast. De voorzitter stelt tevens voor om TLS 1.3 in een volgende overleg verder te behandelen.

Op basis van de het aantal op- en aanmerkingen, stelt de voorzitter voor om het verslag nog niet vast te stellen, maar eerst de besproken opmerkingen in het verslag bij te werken. Vervolgens vaststellen per mail, is volgens de werkgroep akkoord. Arnold biedt daarbij aan om het verslag ook nog na te lopen en waar nodig aan te scherpen.

Actie Arnold
Verslag nalopen en aanscherpen waar nodig.

2. Uniforme Beveiligingsvoorschriften

a. Opzet en structuur

Voorstel van Arnold is om expliciet te verwijzen naar andere standaarden, maar wel de leesbaarheid in ogenschouw te nemen. Daarnaast stelt hij voor om aan te vullen met informatie over 'hoe' configuraties toegepast kunnen worden. Dat wordt door de werkgroep gedeeld.

Daarnaast haalt Rimmer aan dat ook we met een brede doelgroep rekening moeten houden. Hierbij zou het wenselijk zijn om op score te communiceren. Bijvoorbeeld een ondergrens van B via SSL labs. Dirk haalt daarbij het certificeringsschema aan, die daarbij kan helpen.

Aanvullend daarop benadrukt de voorzitter dat de verhouding tot verschillende afspraken ook helder moeten zijn. Met name met Edukoppeling. Daar wordt komende periode naar gekeken en helderheid verschaft in de voorschriften zelf.

b. Inhoudelijk M2M

i. **Willen we een verschil maken tussen serviceaanbieder en service-afnemer?**
De serviceaanbieder heeft te maken met verschillende service-afnemers en zou daarom alle verplichte cipher suites moeten ondersteunen. Voor een service-afnemer die aan het eind van de keten zit, is dit wellicht anders. De voorzitter vraagt hoe de werkgroep hier tegenaan kijkt.
Arnold draagt daar zijn visie bij aan en komt daarbij terug op het eerder aangedragen punt, om scheiding aan te brengen o.b.v. veiligheid en legacy (profiel). Wel belangrijk om die profielen technisch gescheiden in te richten (per FQDN), als maatregel op downgrade attacks. Dit geeft tevens inzicht in het gebruik van beide profielen. Daar is de werkgroep het mee eens. Scheiding maken tussen serviceaanbieder en service-afnemer, eventueel op basis van de aangedragen profielen (legacy/veilig).

De exacte invulling is hiermee echter nog niet vastgesteld. De voorzitter stelt voor om een voorstel hiervan op te nemen in de voorschriften en deze volgende overleg te behandelen. Jaap draagt bij een mogelijke oplossing aan: de verplichte lijst opdelen in twee profielen, aangezien daarmee hetzelfde wordt beoogd.

ii. **Willen we controle van certificaten verplichtstellen?**
Voorafgaand aan deze vraag, werd de werkgroep tevens gevraagd of certificaatcontrole nu plaatsvindt. Dat is het geval. De werkgroep is het dan ook eens met het verplichtstellen hiervan. De vraag is alleen op welke wijze, bijvoorbeeld met OCSP-stapling. Robert benadrukt wel om rekening te houden met de consequenties van deze functie. Wanneer de OCSP-resource niet beschikbaar is voor de server, moet de verbinding dan wel of niet opgezet moeten worden. Wanneer dit afgewezen wordt, heeft dit impact op de dienstverlening. Om dit te voorkomen, draagt Arnold aan om *graceperiode* van bijvoorbeeld drie dagen in te voegen. Kanttekening daarbij is dat deze logica dan wel in de software aanwezig of ingebouwd moeten zijn.

Op welke wijze dit verplicht gesteld moet worden is dus nog onduidelijk. Daarentegen is de werkgroep er in ieder geval wel over eens dat de controle moet plaatsvinden. Om een

geschikte voorschrift voor op te stellen, is het raadzaam om eerst onze achterban hierover te bevragen. Daarnaast benadrukken Joost en Arnold ook andere aspecten aan die in de praktijk gecontroleerd zouden moeten worden, zoals root- en domeinverificatie.

Afspraak
Verificatie van certificaten zou actief moeten plaatsvinden, alleen deze wijze waarop moet nog bepaald worden.

Actie Allen
Inventariseer welke opties er gebruikt worden en/of mogelijk zijn voor het controleren van certificaten. Niet alleen voor de geldigheid, maar voor ook andere aspecten zoals root- en domeinverificatie. Deze uitvraag geldt voor zowel voor M2M (incl. 2-zijdige TLS) als voor H2M communicatie.

iii. **Is het wenselijk om af te wijken van poort 443?**
In Edukoppeling is het gebruik van andere poorten toegestaan, wat overigens niet voor Digikoppeling het geval is. Vanuit de werkgroep is er geen aanleiding om te af te wijken van de standaard poort. In de basis volgen we namelijk de internationale standaard en dus poort 443 voor HTTPS. De voorzitter stelt in ieder geval voor om te achterhalen waar de uitzondering precies vandaan komt.

Actie Dirk
Navraag doen over de achtergrond van de afspraak Edukoppeling betreffende afwijking van poort 443.

iv. Willen we SNI verplichtstellen?
Rimmer stelt voor om hier ook een actie aan te koppelen en na te vragen bij onze achterban. Mogelijk dat we hier vanaf kunnen wijken in een legacy-situaties. Daarnaast vraagt Arnold zich af of het verplichtstellen nodig is, want het toepassen van SNI biedt efficiëntie. Echter benadrukt Robert dat dit niet voor iedereen geldt, zoals voor een serviceaanbieder. Die heeft met meerdere service-afnemers te maken die wel of niet SNI geconfigureerd hebben. De werkgroep is er in ieder geval over eens om dit gezien efficiëntie verplicht te stellen. Mede gezien dat SNI al lange tijd beschikbaar is in vele softwarecomponenten. Wanneer die niet het geval is, zijn de systemen mogelijk verouderd. Ondanks dat, zullen we dit controleren bij onze achterban.

Actie Allen
Navragen wat de impact is voor de achterban voor het verplicht stellen van SNI. Op basis hiervan kunnen we het verplicht stellen concretiseren.

c. Inhoudelijk H2M

i. OCSP-Stapling; wel of niet voorschrijven?
Robert licht toe dat dit een keuze is tussen security en privacy. In geval van OCSP-stapling aan, dient de server verbinding te hebben met het internet, wat het minder veilig maakt. Wanneer de optie niet geboden wordt, dan dient de client zelf het certificaat te controleren bij de certificaatuitgever. Op dat moment is het surfgedrag (welke domeinnaam bezocht wordt) van de client inzichtelijk voor de certificaatuitgever. Volgens de werkgroep zou beide niet het geval moeten zijn, dus wordt voorgesteld om een aanvullende oplossing te onderzoeken. Waarbij OCSP-stapling actief is, zonder dat dit

minder veilig wordt. De voorzitter stelt voor om de mogelijkheden hiervan te onderzoeken, alvorens dit voor te schrijven.

Actie Robert en Arnold
Onderzoeken wat de (technische)mogelijkheden zijn voor certificaatcontrole, die zowel veilig als privacy vriendelijk is.

Joost draagt daarbij de suggestie aan om deze verplichting op te nemen als een 'pas-toe-leg-uit'-voorschrift. Dat kan tevens gelden voor meerdere voorschriften, maar niet voor alle. Sommige moeten te allen tijde verplicht zijn voor de interoperabiliteit. Aanvullende suggestie van Joost daarop is om aan te geven wanneer een voorschrift voor de interoperabiliteit of security geldt. De reden van de voorschrift.

Afspraak
De rationale van de voorschriften worden expliciet opgenomen, waarmee tevens aangegeven kan worden of deze tot de categorie 'pas-toe-leg-uit' behoort.

ii. HTTPS in alle gevallen verplichtstellen?
Dit komt op meerdere plaatsen terug, zoals ook in de wettelijke verplichtingen. De voorzitter stelt voor om dit in deze voorschriften ook expliciet op te nemen. Dit is tegenwoordig ook gewoongoed. Joost benadrukt dat dit wel afhankelijk is een andere verplicht, zoals het soort certificaat. Wanneer PKIoverheid voor alle situaties verplicht is, dan kan dit hoge kosten met zich meebrengen. Maar in alle gevallen PKIoverheid verplichtstellen is niet het geval, benadrukt de voorzitter.

d. Wanneer welk certificaat?
Robert licht toe dat wanneer OIN verplicht is een PKIoverheid-certificaat nodig is. Zo is dit nu ook in het concept van de voorschriften meegenomen. In andere gevallen is er voor nu geen reden om PKIoverheid verplicht te stellen. Wel voor andere soorten, zoals een Domain Validate (DV), Organisation Validate (OV) of Extended Validate (EV) certificaat.

Daarnaast haalt Robert aan dat de toegevoegde waarde voor browsers (de groene balk) van EV-certificaten komt te vervallen. En stelt daarmee de vraag in hoeverre we daar nog eisen aan moeten stellen. Joost benadrukt dat met M2M een EV nog wel van toegevoegde waarde kan zijn, aangezien hier een uitgebreidere validatie aan zit. De werkgroep stelt voor om in ieder geval duidelijk te zijn in de verschillen. Daarnaast stel de voorzitter voor om een verbinding te maken met de BIV-classificatie.

Afspraak
De verschillen tussen DV, OV en EV worden toegelicht in de voorschriften, zodat partijen zelf de keuze kunnen maken. Daarnaast voorschrijven in welke gevallen een soort minimaal het geval moet zijn.

e. Afspraken over (uit)fasering
Gezien de tijd stelt de voorzitter voor om dit punt niet te behandelen. In het volgende overleg komen we hierop terug.

f. Vervolg
Het concept wordt bijgewerkt aan de hand van de punten die besproken zijn. Daarnaast de uitkomst van de acties die besproken zijn.

3. Wettelijke verplichtingen

a. Presentatie met praktijkvoorbeelden

Rimmer start met zijn presentatie, onder het thema veilig en betrouwbaar mailen. De aanleiding om dit binnen ThiemeMeulenhof op te pakken was o.a. phishing en signalen van medewerkers dat e-mailberichten in de SPAM van ontvangende partijen belanden. De internetstandaarden die behandeld worden zijn SPF, DKIM en DMARC. In de presentatie wordt ten eerste de doelstelling ervan behandeld: 1) Vergroten afleverbetrouwbaarheid van email, en 2) Voorkomen misbruik door derden (phishing). Vervolgens wat de genoemde internetstandaarden inhouden. Vervolgens welke tooling er beschikbaar is en hoe dit werkt en als afsluiting, welke risico's spelen bij configuratie.

SPF, DKIM en DMARC staan ook op de 'pas-toe-leg-uit'-lijst van Forum Standaardisatie. De internetstandaarden zelf hebben te weinig aandacht. Ondanks dat dit zonder aanvullende kosten is te configureren is en toegevoegde waarde heeft voor Veilig Mailen. De werkgroep is het hiermee eens.

b. Vervolg

Rimmer deelt de kennis graag met andere. De voorzitter stelt daarbij voor om dit te verwerken tot implementatierichtlijnen en voorschriften binnen deze werkgroep. Daarvoor neemt Rimmer het voortouw, aangezien dit reeds op zijn eigen planning staat. Daarbij wordt eerst gewerkt aan de praktische implementatierichtlijnen, waarop vervolgens ook de afspraken bepaald kunnen worden.

<u>Actie Rimmer</u>
De presentatie wordt verder uitgewerkt in een praktische implementatie richtlijn en deelt deze met de werkgroep.

<u>Afspraak</u>
Op basis van de praktische implementatie richtlijnen zullen voorschriften bepaald worden en opgenomen worden als Uniforme beveiligingsvoorschriften.

4. Afsluiting

De voorzitter vraagt wanneer de volgende bijeenkomst gepland kan worden. Op basis eenzelfde periode is het moment van maandag 30 maart voorgesteld. Dit schikt voor iedereen en is vervolgens direct gepland, waarbij alle deelnemers uitgenodigd zijn. Joost stelt daarvoor weer een locatie bij Surf beschikbaar.