edustandaard

Verslag werkgroep Uniforme Beveiligingsvoorschriften (oktober 2020)

Maandag 12 oktober 2020, 10:30 – 12:00. Locatie: online.

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

Afwezig: Marten Bakker (The Learning Network)

1. Opening

a. Verslag voorgaande bijeenkomst(en)

Toelichting: Het concept verslag van de voorgaande bijeenkomst is eerder toegestuurd en zonder aanvulling als concept op Edustandaard geplaatst. De gemaakte afspraken en acties worden ter bevestiging nagelopen.

De voorzitter vraagt of iemand op- of aanmerkingen heeft op het verslag. Die zijn er niet. Het verslag van de bijeenkomst september 2020 wordt daarmee vastgesteld.

b. Actielijst

Toelichting: Na de laatste bijeenkomst zijn er vier nieuwe acties op de actielijst geplaatst. Acties m.b.t. de thema's 'Security Headers' en 'veilig en betrouwbare mail' zijn reeds onderdeel van de agenda.

2. TLS-voorschriften

a. Reacties op consultatie

Toelichting: In totaal zijn twee reacties op de consultatie via Edustandaard ontvangen. Deze reacties (en andere reacties via de werkgroep) zijn bij de desbetreffende voorschriften geplaatst als commentaar in het werkdocument van UBV TLS. Gezien het beperkte commentaar, worden deze gezamenlijk besproken.

De reacties van de consultatie zijn gezamenlijk besproken, mede wat hiermee te doen. Zoals bij het onderscheid tussen H2M en M2M wat een grote impact op bestaande omgevingen met zich mee kan brengen. Deze voorschrift maakt het mogelijk om minder strenge voorschriften voor H2M toe te passen, zonder dat dit tot een minder veilige situatie leidt voor M2M. Daarmee is het voorschrift niet strikt noodzakelijk, maar wel van belang voor de veiligheid. Op basis van deze nuance wordt het voorschrift bijgewerkt. Concreet is het verzoek gedaan om duidelijker aan te geven welke voorschriften verplicht zijn en welke als best practice gehanteerd kunnen worden

Een andere opmerking gaat over de nut en noodzaak van het aanbieden van de cipher suite *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256.* Deze is minder veilig, maar kan wel noodzakelijk zijn voor de interoperabiliteit. Daarom is besloten dat hiervan afgeweken mag worden, als dit dit niet tot interoperabiliteit problemen leidt. Deze uitzondering wordt toegevoegd.

Verder verdient het voorschrift (TLS-M2M-06) voor het verplicht gebruik van een volledige FQDN een nadere onderbouwing, aangezien hier onduidelijkheid over is. Daar is de werkgroep het over eens en wordt bijgewerkt.

Actie Jordy
Tot slot staat er één reactie nog open met betrekking tot het toepassen van *self signed* certificaten voor een server. Deze is onvoldoende duidelijk om te bespreken. Daarvoor wordt contact gelegd met de indiener. Eventuele wijzigingen worden in de volgende versie meegenomen, die - zoals onder volgende agendapunt is afgesproken - vooraf wordt toegestuurd.

b. Laatste wijzigingen n.a.v. commentaar laatste bijeenkomst

Toelichting: naar aanleiding van de laatste bijeenkomst is er tweetal opmerkingen geplaatst. Dit met betrekking tot 1) de scope van de 'gegevensuitwisseling in het onderwijs' en 2) de uitzondering voor een Single Page Application. Deze zijn bijgewerkt in een nieuwe versie (zie UBV TLS 0.7.1).

De toevoeging van de alinea voor de scope is akkoord, echter wel met aanpassing op basis van hetgeen besproken. De interne gegevensuitwisseling zou niet volledig buiten scope geplaatst moeten worden als deze wel onderdeel is van de keten. Daarnaast kan er onderscheid gemaakt worden tussen voorschriften voor 'Beveiliging' en 'Interoperabiliteit'. Die laatste categorie is alleen van toepassing bij gegevensuitwisseling met derden.

De toegevoegde uitzondering, bijvoorbeeld voor Single Page Application is tevens akkoord. Deze kan toegevoegd worden onder een aparte subparagraaf (2.2.1 Wanneer onderscheid niet mogelijk is).

Afspraak
De voorzitter vraagt of na het bijwerken van de laatste opmerkingen in UBV TLS, deze aangeboden kan worden aan Architectuurraad. Voorafgaand wordt deze per e-mail bij de werkgroep voorgelegd. Daar is de werkgroep het unaniem over eens. In die versie worden ook de wijzigingen op basis van de reactie op de consultatie van de werkgroep Edukoppeling meegenomen.

Actie Jordy
Laatste opmerkingen in UBV TLS verwerken incl. overige reacties op de consultatie en deze als nieuwe versie voorleggen bij de werkgroep, zodat deze vervolgens voorgelegd kan worden bij de Architectuurraad.

3. Veilig en betrouwbare e-mail

a. Eerste concept

Toelichting: de werkgroep is gevraagd om commentaar te leveren op de eerste conceptversie UBV Veilig en Betrouwbare e-mail. Deze zijn tijdens de vorige bijeenkomst besproken. De meeste daarvan zijn bijgewerkt in een nieuwe versie en kunnen besproken worden.

De wijzigingen zijn besproken en akkoord bevonden. Daarnaast zijn de overige opmerkingen besproken. Hetgeen besproken en besloten is verwerkt als opmerking en wordt verwerkt in een volgende conceptversie. Daarmee blijft de actie voor het verwerken van het commentaar nog openstaan.

4. Andere beveiligingsstandaarden

Gezien de tijd is dit agendapunt niet behandeld. Wel heeft Arnold de informatie over ‘Security Headers’ toegestuurd, zodat een overleg met een deel van de werkgroep gepland kan worden om dit nader te bespreken.

5. Afsluiting

In afstemming met de werkgroep is een nieuw moment gepland: maandag 16 november 2020 van 13:00 tot 14:30. Uitnodiging hiervoor is verstuurd via Outlook.