edustandaard

Concept Verslag werkgroep Uniforme Beveiligingsvoorschriften (september 2020)

Maandag 21 september 2020, 13:00 – 14:30. Locatie: online.

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

Afwezig: Marten Bakker (The Learning Network), Olav Loite en Rimmer Hylkema (ThiemeMeulenhoff)

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 augustus 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.

Actielijst doorgenomen. Daar zijn geen geen opmerkingen bij.

2. TLS-voorschriften

a. Laatste wijzigingen, versie in consultatie

Toelichting: Naar aanleiding van de laatste bijeenkomst waarbij met name stil is gestaan bij certificaatcontrole, is de versie van de UBV TLS bijgewerkt in een versie 0.7. Deze versie is in consultatie gegaan (zie UBV TLS v0.7: publieke consultatie).

Arnold heeft deze versie intern bij DUO neergelegd, en daar waar geen opmerkingen bij. Joost heeft zelf nog een opmerking toegevoegd voorschrift TLS-ALG-02 (onderscheid tussen M2M en H2M). Dit onderscheid is niet altijd mogelijk, zoals bij *Single Page Application.* Bijvoorbeeld met Open Onderwijs API.

Afspraak

De toelichting bij het voorschrift TLS-ALG-02 dient bijgewerkt te worden, zodat duidelijk is wat er geldt in een situatie met een *Single Page Application.*

Daarnaast speelt de vraag in hoeverre het geheel een voorschrift (verplicht is) of een advies is voor inrichting. Dit hangt samen met de scope, waar onduidelijkheid over is. De vraag is bijvoorbeeld of het WO zich hierin kan herkennen, met de soort uitwisselingen die daar plaatsvinden.

Kijken we naar interne uitwisselingen, tussen systemen, dan zouden deze logischerwijs ook niet binnen scope vallen.

Afspraak
UBV TLS zijn voorschriften als deze binnen de scope vallen. Op dat moment geldt een '*pas toe of leg uit' principe.* Daarom is het van belang dat de scope scherp gesteld wordt van "de gegevensuitwisselingen in het onderwijs".

Actie Jordy
De scope van voorschrift UBV TLS aanscherpen, waarbij gekeken wordt naar een reeds bestaande toelichting over "de gegevensuitwisseling in het onderwijs". Daarnaast de toelichting bij TLS-ALG-02 bijwerken, zodat dit tegemoet komt aan de uitzondering van een *Single Page Application.*

3. Veilig en betrouwbare e-mail

a. Eerste concept

Toelichting: Op basis van een analyse van de standaarden en beschikbare informatie en voorbespreking met Dirk Linden, Rimmer Hylkema en Jordy van den Elshout is een eerste conceptversie uitgewerkt. Op basis daarvan is de werkgroep gevraagd om op- en aanmerkingen te plaatsen, zodat deze besproken kunnen worden.

De werkgroepleden hebben hun commentaar in het document geplaatst en zijn tijdens de bijeenkomst mondeling besproken. Wat besproken is, is tevens toegevoegd aan het commentaar in het document. Op basis daarvan wordt een nieuwe versie gemaakt.

Actie Jordy
Commentaar van de werkgroep verwerken in een nieuwe versie 'UBV Veilig en Betrouwbare e-mail'.

4. Andere beveiligingsstandaarden

a. Security Headers

Toelichting: 'Security Headers' is een apart thema, naast de WDO-beveiligingsstandaarden. Dit is belangrijk onderdeel voor de veiligheid van webdiensten. Het is ook onderdeel van de test op internet.nl, echter wordt daar een subset getest. Welke nog meer van belang zijn en op welke wijze deze toegepast moeten worden, is een vraag die open staat. Voorgaande bijeenkomst is besloten dat een ieder zich hier verder in verdiept om dit vervolgens met de werkgroep verder te verkennen.

Arnold heeft het nodige ingelezen en een PoC opgesteld, wat hij nog op papier gaat zetten. Ook Joost heeft de nodige kennis van dit onderwerp, echter vraagt hij zich af in hoeverre dit generiek op te stellen is. De voorzitter stelt voor om eerst een voorzet te maken op basis van input van Arnold en op basis daarvan verder te bespreken met de werkgroep.

Actie Arnold
Informatie op papier zetten en aanleveren bij Jordy en of Dirk. Op basis hiervan wordt een separate meeting gepland om het thema 'security Headers' te bespreken en verder uit te werken in een document.

b. Domeinnaambeveiliging

Toelichting: Tijdens de vorige bijeenkomst is besloten om hier eerst een discussiestuk voor te starten, alvorens te bepalen of dit een apart (thema)document moet zijn of opgenomen moet worden in de bestaande (thema)documenten als randvoorwaarden. In het discussiestuk Domeinnaambeveiliging is een voorzet gedaan met achtergrond incl. risico's en maatregelen.

Er zijn geen aanvullende risico's en of maatregelen te benoemen. Wel kan er rekening gehouden worden met DNS of HTTPS, wat als context meegenomen wordt. Daarnaast kan de toelichting van domeinnaam beveiliging aangescherpt worden.

Actie Jordy
Commentaar verwerken in het discussiestuk Domeinnaam beveiliging, zodat dit een volgende keer besproken kan worden.

5. Afsluiting

De voorzitter rondt gezien de tijd het overleg af. In afstemming met de werkgroep is een nieuw moment gepland, waarin alle aanwezigen kunnen: maandag 12 oktober 2020 van 10:30 tot 12:00. Uitnodiging hiervoor is direct verstuurt via Outlook.