edustandaard

Verslag werkgroep Uniforme Beveiligingsvoorschriften (Februari 2021)

Dinsdag 9 februari 2021, 10:00 – 11:30. Locatie: online.

Aanwezig: Dennis van Jeveren (DUO), Dirk Linden (Kennisnet, voorzitter), Jaap Mooij (Kennisnet), Jeroen Renard (Odin Groep), Jordy van den Elshout (Kennisnet), Marten Bakker (The Learning Network), Robert Klein (Kennisnet) en Rimmer Hylkema (ThiemeMeulenhoff)

Afwezig: Geen

1. Opening

Jeroen is voor de eerste keer aangeschoven als aanvulling op de werkgroep.

Aangezien Jeroen voor het eerst aanschuift, vindt er eerst een korte introductie van elkaar plaats. Daarnaast geeft Dirk Linden een toelicht over de achtergrond van de werkgroep en welke standaarden er (op dit moment) behandeld worden.

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 december 2020 wordt daarmee vastgesteld.

b. Actielijst

Toelichting: Tijdens de vorige bijeenkomst zijn er vier acties genoteerd en zijn ook allen afgehandeld. Dat laatste geldt ook voor een aantal andere acties. Acties met een relevante status worden mondeling toegelicht.

Actie #33: *Kijken of er een nieuwsbericht rondom één van de thema's nuttig kan zijn. Zo ja, dan zorgen dat deze geplaatst wordt op Edustandaard.*
Toelichting: Er is aandacht besteed aan UBV TLS. Hiervoor is een bericht opgesteld en op 28 januari gepubliceerd als nieuwsbericht op Edustandaard.nl: Een veilige en betrouwbare verbinding noodzakelijk voor de privacy van leerlingen

Actie #27: Verkennen mogelijkheid tot scannen van onderwijsdomeinen in het VO, PO en MBO.
Toelichting: na verkennend gesprek met Surf, tot het dashboard van internet.nl gekomen. Deze is aangevraagd en wordt op dit moment getest binnen Kennisnet. Op basis daarvan wordt gekeken of dit bruikbaar is voor de sector.

Jordy laat het dashboard inhoudelijk zien aan de werkgroep. De werkgroep ziet daar de voordelen van in: het een mooie tooling die een zinvolle bijdragen kan leveren voor implementatie van de UBV. Wel wordt door de werkgroep aangegeven dat het mooier zijn als branchepartijen zelf ook toegang krijgen tot het dashboard, gezien het belang voor het onderwijs (de publieke sector). Het voelt minder goed dat publieke partijen de branchepartijen scannen, als zij dit zelf ook zouden kunnen doen. Dirk haalt daarbij aan dat dit punt komende

standaardisatieraad aangestipt zal worden. Ook stelt Dirk voor om een aantal voorbeelden te delen met de werkgroep.

Actie Jordy
Een aantal voorbeeldrapportage uit het dashboard van internet.nl delen met de werkgroep.

2. Update n.a.v. de Architectuurraad

a. Goedkeuring UBV TLS

Toelichting: In de architectuurraad is versie 1.0 van UBV - TLS behandeld. Daarbij is het volgende besluit genomen: “De Architectuurraad adviseert de Standaardisatieraad om UBV-TLS 1.0 in beheer te nemen en toe te voegen als een soort PTOLU-afspraak in het Edustandaard-portfolio”. Zie voor meer informatie de Verslag Architectuurraad 21-1-2021

Naast de toelichting zijn er geen vragen. De voorzitter geeft daarbij aan dit een mooie mijlpaal is: het eerst vastgestelde werk van deze werkgroep.

b. Veilig en Betrouwbaar e-mailverkeer ter consultatie

Toelichting: De UBV-afspraak ‘Veilig en betrouwbaar e-mailverkeer’ is door Dirk Linden toegelicht. Daarbij is verzocht om de achterban hierover te informeren en deze afspraak te reviewen. Hier wordt een openbare consultatie voor gestart.

Naast de toelichting is besproken om de laatste wijzigingen niet op dit moment te behandelen maar tijdens de consultatie. Het moment van consultatie wordt daarmee ook gebruikt als review ronden door de werkgroepleden zelf.

Actie Jordy
Consultatie starten voor UBV Veilig en Betrouwbaar e-mailverkeer, die tevens naar de werkgroep wordt gestuurd met het verzoek deze bij de achterban neer te leggen om feedback op te halen.

Afspraak
Werkgroepleden sturen de consultatie door naar hun achterban om feedback op te halen. Daarnaast nemen alle werkgroepleden het document integraal door voor de laatste opmerkingen.

3. Andere beveiligingsstandaarden

a. Thema TLS - Impact nieuwe voorschriften NCSC v2.1

Toelichting: Het NCSC heeft - zoals vooraf aangekondigd - onlangs nieuwe voorschriften voor TLS gepubliceerd (link). De belangrijkste wijzigingen zijn: a) afwaardering TLS 1.2 van ‘Goed’ naar ‘Voldoende’, b) volgorde cipher suites niet verplicht bij ciphers ‘Goed’, en c) ondersteuning van ‘Client-initiated renegotation’ is niet langer ‘Onvoldoende’, maar ‘Voldoende’.
De wijzigingen hebben geen invloed op de voorschriften van UBV TLS zelf, maar wel op de profielen. Waar verwezen of geciteerd wordt naar NCSC, is de tekst aangepast. Ook zijn de profielen geupdate op basis van de wijzigingen van NCSC.

Jordy licht de wijzigingen mondeling toe en wat voor effect dit heeft gehad op de voorschriften zelf. Daarbij is expliciet stilgestaan bij technische impact van ‘Client-initiated renegotation’.

Robert en Dennis geven daarbij aan dat deze onveilig is bij het gebruik van TLS1.0 en TLS1.1. Op basis daarvan afgesproken om het gebruik ervan onder voorwaarden op te nemen.

Afspraak
Het gebruik van 'Client-initiated renegotation' in combinatie met TLS1.0 en TLS1.1 is niet toegestaan. Dat wordt als voorwaarden opgenomen in de bijlage van de voorschriften.

Daarnaast wordt de nieuwe versie (1.1) van UBV TLS tijdens de volgende bijeenkomst vastgesteld, zodat een ieder nog naar de wijzigingen kan kijken.

b. Thema 'Security Headers'

Toelichting: het thema 'Security Headers' heeft een verdere uitwerking gekregen. De vorm hiervan - niet de inhoud - wordt toegelicht.

Dennis en Robert presenteren het document en lichten de structuur ervan toe. Daarbij is deels ook de inhoud behandeld, als voorbeeld. Daaruit kwam al naar voren dat een aantal 'Security Headers' niet meer relevant zijn, aangezien deze *deprecated* (afgekeurd) zijn. Het huidige overzicht spreekt de meeste werkgroepen al zeer aan. Alleen het overzicht van de verschillende 'Security Headers' en hun werking en waarden ervan, is al een toegevoegde waarden voor de sector. Wat nog mist is een advies voor toepassing, wat volgt na verdere uitwerking van de 'security Headers' zelf.

Afspraak
Komende tijd wordt het document verder uitgewerkt. Tijdens de volgende bijeenkomst wordt deze inhoudelijk behandeld. Voorafgaand aan de bijeenkomst wordt het document ter review voorgelegd aan de werkgroep.

4. Afsluiting

In afstemming met de werkgroep is een nieuw moment gepland: dinsdag 16 maart van 10:00 tot 11:30. Uitnodiging hiervoor is direct verstuurd via Outlook.