

Verslag werkgroep Uniforme Beveiligingsvoorschriften (April 2021)

Dinsdag 6 april 2021, 10:30 – 12:00. Locatie: online.

Aanwezig: Dennis van Jeveren (DUO), Jaap Mooij (Kennisset, voorzitter), Jeroen Renard (Odin Groep), Jordy van den Elshout (Kennisset, verslag), Robert Klein (Kennisset) en Rimmer Hylkema (ThiemeMeulenhoff)

Afwezig: Dirk Linden (Kennisset), Marten Bakker (The Learning Network)

1. Opening

Aangezien Dirk Linden niet aanwezig kan zijn, zit Jaap Mooij deze bijeenkomst voor. Jaap begint het overleg en vraagt of er naast de opgestelde agenda, nog andere punten zijn. Die zijn er niet.

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 februari 2020](#) wordt daarmee vastgesteld.

b. Actielijst

Toelichting: tijdens de vorige bijeenkomst zijn twee acties genoteerd en zijn gedeeltelijk afgehandeld. De status van deze acties wordt kort toegelicht.

Acties worden doorgenomen. Actie omtrent de voorbeeldrapportage van het dashboard internet.nl, wordt nog toegestuurd.

2. Update (n.a.v. de Standaardisatieraad)

a. Goedkeuring UBV TLS

Toelichting: versie 1.0 van UBV - TLS is nu definitief in beheer genomen: "De Standaardisatieraad besluit tot inbeheername van UBV-TLS 1.0". Zie voor meer informatie het [Verslag Standaardisatieraad 11-2-2021](#) (agendapunt 3. UBV-TLS)

Naast de toelichting zijn er geen vragen vanuit de werkgroep. Rimmer - die aanwezig was tijdens de standaardisatieraad - licht toe wat er besproken is. Dat is terug te lezen in het bovengenoemde verslag van de Standaardisatieraad.

b. Veilig en Betrouwbaar e-mailverkeer ter consultatie

Toelichting: de consultatie - van 18 februari tot 29 maart 2021 - is afgerond. Opmerkingen konden ingediend worden via info@edustandaard.nl. De consultatie is ook onder de aandacht gebracht binnen het netwerk IBP van het PO en VO.

Er zijn weinig reacties binnen gekomen. De voorzitter staat daarom expliciet stil of er voldoende aandacht is geweest en vraagt daarvoor een aantal werkgroepleden. Rimmer en Jeroen geven

aan dat zij hier proactief aandacht aan hebben besteed en de voorschriften inhoudelijk hebben doorgenomen (met hun achterban). Daaruit zijn geen opmerkingen gekomen die behandeld moeten worden.

Verder geeft Jordy aan dat er een aantal reacties is geweest via het netwerk IBP PO/VO. Deze zijn beantwoord en heeft tevens geleid tot een opmerking in het document. De werkgroep bespreekt deze - naast de andere gemaakte opmerkingen in het document. Hetgeen besproken is verwerkt in het document en wordt nader bijgewerkt. De voorzitter vraagt of na het bijwerken, de versie vastgesteld kan worden. Daar is de werkgroep het unaniem over eens.

Afspraak

Nadat de opmerkingen zijn verwerkt in het document Veilig en Betrouwbaar e-mailverkeer, kan deze ter vaststelling aangeboden worden.

Actie Jordy

Zorgen dat de opmerkingen - door de werkgroepleden - verwerkt worden in het document en een nieuwe versie van het document wordt gemaakt, die ter vaststelling aangeboden wordt.

3. Andere beveiligingsstandaarden

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

Toelichting: naar aanleiding van de nieuwe TLS-voorschriften v2.1 van NCSC zijn de voorschriften bijgewerkt. Deze is voorgelegd aan de werkgroep ter review.

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 renegotiation' 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.

De werkgroep bespreekt de analyse en de impact op de voorschriften, per wijziging in het document. Deze zijn allen duidelijk en akkoord bevonden.

Afspraak

De bijgewerkte versie wordt als nieuwe versie (1.1) vastgesteld en kan voorgelegd worden aan de Architectuur- en Standaardisatieraad.

Actie Jordy

Zorgen dat de nieuwe versie (1.1) van UBV TLS wordt voorgelegd en gepubliceerd op de website van Edustandaard.

Tijdens het bespreken van de opmerkingen in het document, wordt tevens voorgesteld om nader stil te staan bij de toekomst van de TLS versies. Op dit moment is TLS 1.2 verplicht voor de interoperabiliteit en wordt daarnaast 1.3 aanbevolen voor extra veiligheid en toekomstvast configuraties. Dit is in lijn met de richtlijnen van het NCSC.

Afspraak

Tijdens de volgende bijeenkomst staan wordt expliciet stilgestaan bij de toekomst van de TLS versies, ter bevordering van een toekomstvaste gegevensuitwisseling in het onderwijs.

b. Thema 'Security Headers'

Toelichting: Het thema 'Security Headers' heeft een verdere uitwerking gekregen. Deze is voorafgaand aan de werkgroep gestuurd ter review. De werkgroepleden is gevraagd om feedback als opmerking in het document te plaatsen.

De opmerkingen in het document zijn gezamenlijk met de werkgroep besproken. Hetgeen besproken is genoteerd in de opmerking in het document.

Afspraak

Het document is opgesteld om inzicht te bieden in de verschillende 'Security Headers' en bevat geen verplichte voorschriften. Het document met thema 'Security Headers' wordt dan ook gepositioneerd als handreiking, niet als voorschrift.

Actie Dennis/Robert (en vervolgens Jordy)

Zorgen voor een versie waarin alle opmerkingen zijn gewerkt en die ter consultatie aangeboden kan worden. Jordy zorgt vervolgens dat deze ter consultatie wordt aangeboden middels een (nieuws)bericht.

4. Afsluiting

In afstemming met de werkgroep is een nieuw moment gepland: dinsdag 1 juni van 10:30 tot 12:00. Uitnodiging hiervoor is direct verstuurd middels een agendaverzoek (Outlook).