

Verslag werkgroep Uniforme Beveiligingsvoorschriften (november 2020)

Maandag 30 november 2020, 13:30 – 15:00. Locatie: online.

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

Afwezig: Marten Bakker (The Learning Network) en Olav Loite.

1. Opening

Voordat we met de agenda starten heeft Arnold een mededeling. Gezien zijn vertrek bij DUO kan hij vanaf 1 januari niet meer deelnemen aan de werkgroep. Joost geeft aan dat dit ook voor hem geldt, en vanaf 1 januari niet meer werkzaam is voor SURF.

Actie Dirk

Afspraak maken voor nieuwe vertegenwoordiging vanuit DUO en SURF. Zowel Joost als Arnold vragen intern na wie hun opvolger voor de werkgroep kunnen zijn.

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 oktober 2020](#) wordt daarmee vastgesteld.

b. Actielijst

Toelichting: Na de laatste bijeenkomst zijn er geen nieuwe acties op de actielijst geplaatst. Op dit moment staan er - naast de lopende thema's - geen acties open.

2. TLS-voorschriften

a. Update n.a.v. Architectuurraad

Toelichting: Tijdens de Architectuurraad van 29 oktober 2020 heeft Dirk Linden - als voorzitter van de werkgroep UBV - een update gegeven over de status van UBV TLS (Zie [Sheets Update UBV TLS](#)).

Dirk licht de update toe en geeft daarbij aan dat dit onderwerp in een groter kader speelt, de WDO-standaarden. Een vraag die speelt in de standaardisatieraad is de impact van deze voorschriften. Ook gezien de afhankelijk met andere partijen, zoals bij DANE en DNSSEC.

Microsoft heeft bijvoorbeeld eerder aangegeven DANE en DNSSEC te willen implementeren. Dit staat in een blogpost '[Support of DANE and DNSSEC in Office 365 Exchange Online](#)'. Daarin wordt gesproken dat eind van 2020 DANE actief is voor uitgaand e-mailverkeer en 2021 voor inkomend e-mailverkeer.

Om de impact van de voorschriften in te schatten, kan het nuttig zijn om een scan uit te voeren hoe de implementatie van de standaarden ervoor staat. Zoals dit ook gebeurt door de overheid voor overheidsdomeinen. En door SURF voor het HO, die een scan elk kwartaal uitvoert. Deze gegevens zijn op aggregatieniveau via SCIPR (SURF) in te zien. Het toetsen van sommige voorschriften kan via een API van Internet.nl. Dit kan ook een mogelijkheid zijn om binnen het onderwijssector de stand van zaken op te maken.

Actie Dirk/Jordy

Verkennen mogelijkheid tot scannen van onderwijsdomeinen in het VO, PO en MBO.

b. [Laatste wijzigingen n.a.v. commentaar laatste bijeenkomst](#)

Toelichting: Naar aanleiding van de vorige bijeenkomst en nog binnenkomende reacties op de consultatie, zijn er wijzigingen aangebracht. Deze worden met de werkgroep besproken, zodat op basis daarvan een nieuwe versie gemaakt en gepubliceerd kan worden. Doel hiervan is om de laatste wijzigingen te bespreken en op basis daarvan vaststellen dat dit de laatste conceptversie is. Deze kan dan voorgelegd worden als 1.0 aan de architectuur- en standaardisatieraad.

De voorzitter vraagt of iemand nog op- of aanmerkingen heeft. Die zijn er niet. Dat geldt ook voor de omschrijving van de scope die recentelijk is aangescherpt. Mochten daar toch vragen over zijn vanuit de achterban, dan kan dit zonder aanpassing van de voorschriften beantwoord worden.

Afspraak

Mocht er vragen zijn over de scope, dan kan dit toegelicht worden. Met name omdat elke situatie anders kan zijn. Daarmee is toelichting van de scope wel afdoende.

Afspraak

De huidige versie is akkoord volgens de werkgroep en kan als concept afspraak geplaatst worden op Edustandaard. Deze versie wordt aangeboden in de Architectuurraad en Standaardisatieraad, waarmee het een 1.0 kan worden. Indieners van reactie op de consultatie worden ook benaderd.

Actie Jordy

Laatste versie publiceren op Edustandaard als concept afspraak (versie 0.9) incl. communicatie richting de indieners die een reactie hebben gegeven op de consultatie.

3. Veilig en betrouwbare e-mail

a. [Laatste wijzigingen n.a.v. commentaar laatste bijeenkomst](#)

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 inhoudelijk besproken en verwerkt in een nieuwe conceptversie. Als we het hierover eens zijn, kan de aanpak hiervan toegevoegd worden. Doel hiervan is om de voorschriften vast te stellen, zodat op basis daarvan de aanpak geschreven kan worden.

Er zijn niet direct op- of aanmerkingen. Wel merkt Rimmer op dat er een volgorde in volwassenheid nodig is, wat niet direct in de voorschriften zelf naar voren komt. Dit kan wel terugkomen in de aanpak, welke nog uitgewerkt moet worden. Daar kan de aanpak van de GEU voor gebruikt worden.

De voorzitter vraagt hoe we deze voorschrift kunnen afronden. Voorstel hierin is om dit apart op te pakken als voorbereiding op de volgende bijeenkomst, die we voor dit jaar willen plannen.

Actie Jordy

Samen met Rimmer en Dirk de voorschriften nalopen en afronden, waarbij tevens gekeken wordt naar een eerste compacte versie voor de implementatieaanpak.

4. Andere beveiligingsstandaarden

a. Thema ‘Domeinnaambeveiliging’

Tijdens een vorige bijeenkomst is afgesproken om een discussiestuk te starten voor domeinnaambeveiliging (DNSSEC e.d.). Op basis hiervan kan besloten worden of dit een apart thema moet zijn, of dat dit als algemene maatregel opgenomen kan worden in andere thema's. Dit is uitgewerkt in het Discussiestuk Domeinnaambeveiliging. Doel hiervan is om deze voorschriften te bespreken en vast te stellen. Tevens besluiten waar deze voorschriften een plek moeten krijgen.

De voorschriften zijn besproken met de werkgroep. In het discussiestuk zijn de opmerkingen geplaatst. Daarnaast is het voorstel gedaan om de voorschriften op één plek te beschrijven en waar nodig te verwijzen. Wel met de kanttekening dat de thema's zelfstandig leesbaar moeten blijven.

Afspraak

Uitgangspunt moet zijn om de voorschriften op één plek te beschrijven en vanuit andere thema's te verwijzen, waarbij wel de leesbaarheid van de voorschriften in het ogenschouw gehouden wordt. Uitwerking kan beperkt blijven tot een afgerond discussiestuk.

Actie Jordy

Discussiestuk Domeinnaambeveiliging afronden incl. een voorstel hoe de voorschriften verwerkt kunnen worden in de andere thema's.

b. Thema ‘Security Headers’

Het thema ‘Security Headers’ moet nog verder uitgewerkt worden, voordat deze besproken kan worden. Doel: Informeren en evt. voortgang bespreken.

Arnold presenteert hetgeen wat hij nu heeft uitgewerkt. Daarbij stelt hij de vraag in hoeverre dit onderdeel is van de keten. Want de voorschriften hebben als snel impact op de systemen zelf. De werkgroep erkent dat. Voorgesteld wordt om dit - net als bij UBV TLS - op te pakken: algemene voorschriften en inhoudelijke voorschriften. Arnold doet hier een voorzet in, die vooraf wordt besproken met Jordy en Robert.

Afspraak

Het thema ‘Security Headers’ wordt uitgewerkt in eenzelfde format als UBV TLS, waarbij expliciet stil wordt gestaan bij de impact van elke ‘Security Header’. Op basis daarvan kunnen de voorschriften bepaald worden in afstemming met de werkgroep.

Actie Arnold

De 'Security Headers' analyseren en uitwerken, zodat op basis daarvan de voorschriften bepaald kunnen worden.

5. Afsluiting

In afstemming met de werkgroep is een nieuw moment gepland: dinsdag 15 december van 11:00 tot 12:30. Uitnodiging hiervoor is direct verstuurd via Outlook.