edustandaard

# Verslag werkgroep Uniforme Beveiligingsvoorschriften (november 2019)

maandag 11 november 2019, 13:00 - 15:00, Surfnet, Utrecht

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

Afwezig: geen

## Agenda

1. Opening, Kennismaking
2. Aanleiding werkgroep Uniforme Beveiligingsvoorschriften
    a. Aanleiding vaststellen
    b. Doelstelling: gezamenlijk komen tot set uniforme beveiligingsvoorschriften die de interoperabiliteit en efficiëntie ten goede komt.
3. Bespreekpunten TLS-voorschriften
    a. Op welke wijze de 'ICT-beveiligingsrichtlijnen voor TLS v2.0' (NCSC, 2019) hanteren als basis?
    b. De reikwijdte van de set van voorschriften, zoals beperking tot M2M-communicatie.
4. Afsluiting
    a. Vervolg
    b. Andere onderwerpen (voorraad agenda)
    c. Volgende bijeenkomst

## 1. Opening, Kennismaking

Allereerst is de tijd genomen voor kennismaking. Een aantal werkgroepleden waren reeds met elkaar bekend, andere niet. Vervolgens is de agenda vastgesteld; hierbij is geen aanvulling gewenst.

## 2. Aanleiding werkgroep Uniforme Beveiligingsvoorschriften

De voorzitter licht de aanleiding toe. Op dit moment zijn er op gebied van informatiebeveiliging verschillende afspraken in de sector (en daar buiten) waar dienstverleners mee te maken hebben. Soms conflicteren deze of zorgen voor onnodige complexiteit. Met deze werkgroep willen we daarom komen tot een set uniforme beveiligingsvoorschriften die de informatieveiligheid, interoperabiliteit en efficiënte ten goede komt. En die inpaspaar zijn in andere afspraken en standaarden die in de onderwijsketen gehanteerd worden. De werkgroepleden zijn het hiermee eens en onderschrijven dit met praktijkvoorbeelden. Met name met betrekking tot TLS, wat het eerste onderwerp is die aan de hand van het volgende agendapunt verkend wordt.

## 3. Bespreekpunten TLS-voorschriften

Aan de hand van de volgende punten worden de eerste (proces)afspraken rondom TLS-voorschriften gemaakt.

### a) Op welke wijze de 'ICT-beveiligingsrichtlijnen voor TLS v2.0' (NCSC, 2019) hanteren als basis?

De werkgroep wordt gevraagd of het wenselijk is om aan te sluiten van internationale standaarden, zoals op nationaal gebied, de ICT-beveiligingsrichtlijn voor TLS van NCSC. Arnold geeft daarbij aan dat DUO de NCSC richtlijn al gebruikt. De NCSC richtlijn laat echter nog ruimte voor keuzes en interpretatie. Zo geeft de richtlijn per cipher een kwalificatie 'Onvoldoende', 'Voldoende'en 'Goed'. Wat geen volledige duidelijkheid over welke cipher wel of niet gebruikt *mag* worden. DUO hanteert daarom ook de aanvullende interne afspraak dat ciphers met de kwalificatie 'Onvoldoende' en 'Voldoende' uitgefaseerd moeten worden. Dit punt kwam ook al naar voren in de GAP-analyse die Kennisnet heeft opgesteld. Uit verdere discussie in de werkgroep kan worden geconcludeerd dat het nodig is om aanvullende afspraken te maken over welke ciphers in de onderwijsketen gebruikt mogen worden. Welke dat zijn en welke formulering we daarbij hanteren zullen we met elkaar vast moeten stellen. GAP analyse en de afspraken van DUO kunnen daarbij tot voorbeeld dienen.

Vraag van de werkgroep is dan ook of DUO deze informatie met de werkgroep kan delen, zodat deze als input gebruikt kan worden voor uniforme voorschriften binnen deze werkgroep.

Actie (Arnold)
Met de werkgroep delen van TLS beveiligingsvoorschriften die binnen DUO worden gehanteerd, om als input te dienen voor de op te stellen Uniforme Beveiligingsvoorschriften.

Samenvattend leidt eea tot de eerste afspraken:

**Afspraak**
**Voor de Uniforme Beveiligingsvoorschriften maken we waar mogelijk gebruik van 'hoger gelegen' afspraken. Bij voorkeur internationale afspraken, indien nodig nationale afspraken en alleen als die allemaal niet voldoen aanvullende afspraken die in deze werkgroep worden gemaakt. Als we afwijken van bovenliggende afspraken, dan moet dit onderbouwd worden.**

**In geval van afspraken rondom TLS, wordt de ICT-beveiligingsrichtlijn voor TLS van NCSC gevolgd. Bij het maken van nadere afspraken wordt gerefereerd aan deze richtlijn.**

### b) De reikwijdte van de set van voorschriften, zoals beperking tot M2M-communicatie

De afspraken waarin op dit moment TLS afspraken zijn opgenomen gaan vooral over Machine to Machine (M2M) gegevensuitwisselingen. Vraag is alleen of we ons daartoe kunnen/moeten beperken. Rimmer benadrukt dat alleen afspraken maken over TLS niet afdoende is. Wanneer deze algemene (strikte) afspraken voor clientverkeer toegepast worden, heeft dit impact op de gebruiker, wat niet (voor alle dienstverleners) wenselijk is. Er zou dan ook onderscheid gemaakt moeten worden in afspraken voor Machine-to-Client (M2C) en Machine-to-Machine (M2M). Dit leidt tot de volgende afspraak:

**Afspraak**
**Bij het maken van afspraken wordt onderscheid gemaakt tussen de toepassing op M2C en M2M. Dat maakt het mogelijk om striktere regels toe te passen voor M2M, zonder dat clients (gebruikers) hier last van hebben.**

**Hieruit wordt tevens geconcludeerd dat de gewenste reikwijdte van de uniforme beveiligingsvoorschriften breder is dan alleen M2M.**

De werkgroep merkt daarnaast op dat sommige dienstverleners (nog) te maken hebben met beide soorten verkeer op één platform/domein. Dit zou niet het geval moeten zijn en leidt tot de volgende afspraak:

**Afspraak**
**Verkeer voor M2C en M2M dient op separate domeinen (FQDN) te worden afgehandeld zodat striktere regels voor M2M kunnen worden gehanteerd zonder dat dit direct impact heeft op het M2C domein.**

Naast het onderscheidt tussen M2M en M2C, wordt opgemerkt dat maatregelen risico-gebaseerd toegepast moeten worden. Het Certificeringschema IBP ROSA is ook met deze gedachte opgesteld: o.b.v. een BIV-classificatie wordt de benodigde maatregelen aangewezen. Daarbij is het mogelijk om beargumenteerd af te wijken. Daarnaast wordt aangestipt dat afspraken niet onnodig complex gemaakt moeten worden. Bijvoorbeeld de verplichting van ondertekening van berichten. Dit zou onder voorwaarden vereist moeten worden. Hier zouden ook afspraken over terug moeten komen, in lijn met profielen. Het best-effort profiel van Edukoppeling voorziet hier bijvoorbeeld ook in, waarbij tevens wordt opgemerkt dat deze niet algemeen bekend is. Op basis hiervan wordt geconcludeerd dat de afspraken (lees: maatregelen) risico-gebaseerd gemaakt moeten worden. Niet voor elke situatie zijn de zwaarste maatregelen nodig.

**Afspraak**
**Voorschriften worden afgewogen op proportionaliteit en ingedeeld op basis van profielen als oplossing voor het 'one-size-fits-all'-probleem**.

Werkgroepleden vermelden daarbij dat implementatie voor dienstverleners lastig kan zijn. Dat geldt (straks) met name voor TLS 1.3, wat een grote impact kan hebben op de infrastructuur. TLS 1.3 heeft namelijk impact op TLS (Termination) Proxy. Dienstverleners zouden hier vroegtijdig over geïnformeerd moeten worden, zodat hier rekening mee gehouden kan worden.

Daarnaast wordt uitgesproken dat het voor dienstverleners lastig kan zijn om verouderde TLS-configuraties uit te faseren. Met name voor M2C, gezien de mogelijke businessimpact die dit kan hebben. Zoals de plicht van levering. De werkgroep benadrukt daarbij wel dat het goed is om hier afspraken over vast te leggen, zodat informeren mogelijk is. Vervolgens kunnen afspraken gemaakt worden voor uitfasering. Dienstverleners kunnen op hun beurt de gebruikers infomeren, bijvoorbeeld met banners bij gebruik van verouderde TLS-verbinding. Met de juiste logging, geeft dit tevens inzicht in het gebruik van verouderde protocollen.

**Afspraak**
**De werkgroep gaat over de inhoud van de afspraken, besluiten over implementatie worden elders genomen. In de werkgroep gaan we wel de randvoorwaarden creëren om in de toekomst afspraken in– en uit te faseren. Dat doen we onder andere door specificaties van nieuwe afspraken (bijvoorbeeld TLS 1.3) tijdig beschikbaar te hebben. Om de 'oude' afspraak vervolgens nog een tijd naast de nieuwe te ondersteunen.**

De werkgroep merkt daarbij dan ook op dat dienstverleners geïnformeerd en ondersteund moeten worden, bijvoorbeeld met best-practices voor de meest gebruikte software en componenten. Dit aan de hand van praktijkervaringen die werkgroepleden of hun achterban hebben.

**Actie (Allen)**
**Best-practices verzamelen en delen met de werkgroep, zodat deze met dienstverleners gedeeld kunnen worden als ondersteuning voor implementatie van TLS-configuraties.**

Als laatste punt bespreekt de werkgroep de toevoeging van Server Name Indicator (SNI). Dit is een toevoeging op TLS en maakt het mogelijk om aan één IP-adres en poort verschillende diensten met SSL certificaten te verbinden. Dat levert verschillende voordelen op, zoals efficiëntie in beheer en onderhoud. Het verplicht opnemen van SNI wordt niet door alle werkgroepleden onderschreven en leidt dan ook tot de volgende afspraak:

**Afspraak**
**Ongeacht wat wenselijk is (wel of niet verplicht stellen van SNI), wordt de uitspraak hierover vastgelegd in de voorschriften.**

## 4. Afsluiting

De praktijkvoorbeelden en gewenste afspraken die door de leden van werkgroep zijn aangedragen, onderschrijven het belang van de werkgroep en het maken van uniforme beveiligingsvoorschriften.

### a) Vervolg

De gemaakte afspraken en actiepunten leiden tot input voor de volgende bijeenkomst. Dit wordt meegenomen in het voorstel voor de uniforme beveiligingsvoorschriften.

### b) Andere ontwerpen

De voorzitter stipt tevens tweetal ander gerelateerde onderwerpen toe, die binnen deze werkgroep behandeld kunnen worden. Het eerst onderwerp betreft de:

**Wettelijke verplichtingen (STARTTLS, DANE, DMARC e.d.)**
Tijdens de vergadering van de standaardisatieraad van april 2019 stond op de agenda dat een aantal wettelijke voorgeschreven standaarden opgenomen zouden moeten worden in ROSA. Voorstel nu is om de beveiligingsstandaarden uit de daar behandelde memo te bespreken in onze werkgroep. Deze beveiligingsstandaarden zijn voor de overheid verplicht en (deels) voor dienstverleners binnen de sector (zie ook streefbeeldafspraken Forum Standaardisatie). Een aantal werkgroepsleden laat weten dat ze deze verplichte standaarden (deels) al hebben toegepast. De voorzitter is geïnteresseerd in deze praktijkervaringen en vraagt wie daar een volgende keer meer over kan vertellen. Rimmer biedt aan om dit te doen. Deze ervaringen kunnen – net als voor TLS – verzameld en gedeeld worden als ondersteuning bij implementatie.

**Actie (Rimmer)**
**Tijdens de volgende bijeenkomst een toelichting geven over de praktijkervaring over toepassing van DMARC e.d.**

**Wanneer welk certificaat, zoals een PKIoverheid of ander soort certificaat** is een ander punt wat voorzitter aanhaalt. Mede op basis van gesprekken in andere werkgroepen van Edustandaard. Dit wordt herkend door de werkgroep en besluit dat dit ook onderdeel moet zijn van de voorschriften, bijvoorbeeld aan de hand van de beoogde profielen. Een PKI-certificaat is namelijk niet altijd benodigd of wenselijk.
**Afspraak**
**Wanneer welk certificaat, zoals een PKI of ander soort certificaat wordt vastgesteld op basis van de beoogde profielen voor TLS-voorschriften.**

### c) Volgende bijeenkomst

De voorzitter stelt voor direct een volgende bijeenkomst te plannen. Daarbij houden we rekening met ruimte voor voorbereiding. Een voorzet voor zowel de beveiligingsvoorschriften, als voor de

aanpak hoe dit vorm te geven. Op basis daarvan komt de werkgroep tot een tijdstip: maandag 27 januari 2020 van 13:00 tot 15:00. Deze is direct vastgesteld en gepland, waarbij alle deelnemers uitgenodigd zijn.