edustandaard

Concept Verslag werkgroep Uniforme Beveiligingsvoorschriften (maart 2020)

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

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

Afwezig: Olav Loite (VDOD), Joost van Dijk (Surfnet)

Agenda

1. Opening
    a. Verslag voorgaande bijeenkomst vaststellen (incl. verslag van de eerste bijeenkomst
    b. Actielijst doornemen

2. Uniforme Beveiligingsvoorschriften
    a. Opzet en structuur
        i. Profielen, zoals voor Edukoppeling; samenvoeging van voorschriften NCSC, DK en UBV voor de leesbaarheid.
    b. Inhoudelijk punten
        i. Is het wenselijk om af te wijken van poort 443?
        Toegevoegd punt aan de hand van de actielijst.
        ii. Verkenning voorschriften PKI
        iii. Authenticatie en tweezijdige TLS
    c. Afspraken over (uit)fasering
        i. TLS-configuraties 'Uit te faseren', zoals TLS1.0 en TLS1.1
        ii. Naast TLS1.2 ook TLS1.3 voor de onafhankelijkheid en toekomstvastheid
3. Veilig en betrouwbare e-mail (SPF, DKIM en DMARC)
    a. Afspraken maken o.b.v. huidige informatie en materialen
    b. Vervolg
4. Afsluiting
    a. Andere onderwerpen?
    b. Volgende bijeenkomst

1. Opening

De voorzitter stelt voor om de vergadering compact te houden, aangezien een overleg via videoconferencing de nodig aandacht vraagt. Daarnaast vraagt hij of er onderwerpen missen op agenda. Dat is niet het geval en de voorzitter stelt voor om het verslag van de vorige bijeenkomst na te lopen.

a. Verslag voorgaande bijeenkomst(en)

Daarbij licht Jordy toe dat het verslag van de eerste bijeenkomst ook is bijgewerkt, op basis van hetgeen besproken tijdens de tweede bijeenkomst. Het verslag van de tweede bijeenkomst geeft alles weer, ook welke wijzigingen zijn gemaakt op het eerste verslag. Wanneer we het eens zijn over het verslag van de tweede bijeenkomst, zijn we het ook eens over het eerste

verslag. De voorzitter vraagt of hier opmerkingen over zijn. Deze zijn er niet, waarmee de voorzitter voorstelt om de verslaglegging vast te stellen.

Verder stelt de voorzitter voor om het verslag van voorgaande keer door te lopen, met name expliciet de acties en afspraken. Waaronder het onderscheid tussen service-afnemer en serviceaanbieder. De vraag daarbij is of dit nu onderdeel is van de voorschriften. Jordy bevestigd dat dit onderdeel is van de voorschriften, onder TLS-versie en *cipher suites* voor M2M communicatie. Daarnaast zijn alle punten verwerkt of staan de agenda of actielijst, die later in het overleg worden behandeld. Voor wat betreft de verplichting van poort 443, stelt de voorzitter voor om die apart op te nemen op de agenda. Deze wordt toegevoegd onder 2b(i).

b. Actielijst

De voorzitter stelt voor om de openstaande acties na te lopen:

Actie 2: van de eerste bijeenkomst staat nog open. Dit betreft het ophalen van best-practices, echter is deze aan allen toegekend en algemeen gesteld waardoor invulling lastig is. De voorzitter vraagt of iemand hier ideeën bij heeft. Arnold stelt voor om eerst een inventarisatie te maken wat er gebruikt wordt aan technieken binnen onze sector. Bijvoorbeeld welke webservices er gebruikt worden, zoals Apache, IIS, etc. Voor die soorten kan een TLS-configuratie uitgeschreven worden die partijen helpen met de implementatie. Maar ook voor het gebruik van certificaten, dan ook kijken naar de programmeertalen, zoals Java, .NET, etc. De voorzitter onderschrijft dit en stelt voor om hier een document voor te starten, waarin dit verzameld kan worden. En dat begint dan met een opsomming aan gebruikte technieken.

Actie Jordy
Document aanmaken voor een opsomming van gebruikte technieken, om daar vervolgens de configuraties voor uit te schrijven o.b.v. UBV.

Actie 7: de voorzitter vraagt hoe we hier zinnig invulling aan kunnen geven. Daarbij geeft Arnold aan dat dit in logica opgelost moet worden, maar het is niet handig om hier verschillende soorten voorbeeldcode voor uit te schrijven. Eventueel wel stappen die in de code genomen moet worden. Jordy vraagt welke mogelijkheden daarbij gebruikt moeten worden, want zowel bij OCSP-stapling als toepassing van CRL, lopen we tegen andere problemen aan. Arnold is het daarmee eens en geeft aan dat dit nader onderzocht moet worden, en op basis daarvan keuze moeten maken. Jordy stelt daarbij wel voor om de afspraak vast te leggen dat er altijd op geldigheid van certificaten gecontroleerd moeten worden. De wijze waarop, kunnen de implementatierichtlijnen dan bij helpen. Daar is Arnold het ook mee eens en stelt tevens voor om de voorbereiding van Actie #10 (onderzoek van (technische)mogelijkheden voor certificaatcontrole) erbij te pakken. Aangezien Actie 7 en 10 veel overlap hebben, stelt Jordy voor om deze samen te voegen. Dat is akkoord.

Actie 10: Arnold presenteert een uitwerking van technische mogelijkheden voor het controleren van certificaten, die hij samen met Robert heeft voorbereid. De voorzitter geeft aan dat dit handig is om die discussie beter te kunnen voeren en stelt voor om hier een apart document van te maken. Op dat moment is de ‘wat’ en ‘hoe’ duidelijk gescheiden. Op basis hiervan wordt de actie bijgewerkt.

Actie Arnold
De voorbereiding (in de mailwisseling) verzamelen in een document 'Technische mogelijkheden voor controle certificaat' en plaatsen op de Drive van de werkgroep.

Actie 9: de voorzitter vraagt of iemand hier een terugkoppeling op heeft. Arnold geeft aan dat dit onderdeel is van de poort 443 discussie en dat er vanuit DUO geen voorkeur is voor het wel of niet verplicht stellen van SNI. Om dit punt af te ronden vraagt Jordy of we SNI nu verplicht kunnen stellen, of levert dit impact op voor de achterban? De voorzitter stelt voor om de impact vraag eventueel bij Olaf neer te leggen, echter geeft Robert aan dat deze discussie wellicht al gevoerd is bij VDOD. Dit gezien het feit dat zij reeds met OSO e.d. te maken hebben die daarmee reeds verplicht is en gebruikt wordt. De voorzitter stelt daarom voor om de verplichting van SNI voor nu vast te stellen. Arnold verwacht ook geen problemen, aangezien de meeste browsers, OS-en en webservices dit al jarenlang ondersteunen.

Afspraak
De verplichting van SNI wordt definitief gemaakt in de voorschriften. De actie is daarmee ook afgehandeld worden.

Actie 11 voor uitwerking van veilige mail staat geagendeerd en wordt daar verder behandeld.

2. Uniforme Beveiligingsvoorschriften

a. Opzet en structuur

In het voorgaande overleg is besloten om aandacht te besteden aan de leesbaarheid van de voorschriften, zonder dat teveel wordt overgenomen. In gesprek met Edukoppeling kwam echter naar voren dat dit niet praktisch is, aangezien er naar verschillende bronnen gekeken moeten worden. Daarom is hier een profiel voor opgesteld: een overzicht van alle geldende eisen met daarbij de status, bron en referentie. Jordy heeft dit informeel getoetst bij één van de werkgroepleden van Edukoppeling, waarvan de uitkomst positief is. Tegelijkertijd geeft dit profiel met alle voorschriften ook inzicht voor UBV, met name als er afspraken wijzigen. Daarnaast haalt Arnold aan dit tegemoet komt aan de update mechanisme, die we nodig hebben. Want de bovenliggende kaders hebben een lage update interval en op deze wijze kunnen nieuwe afspraken eerder gerealiseerd worden. De voorzitter stelt voor om deze nieuwe opzet te hanteren. Daar is geen tegenspraak in.

Afspraak
Profielen met de volledige voorschriften worden opgenomen als bijlage, om tegemoet te komen aan de leesbaarheid voor verschillende uitwisseling contexten.

b. Inhoudelijk punten

i. Is het wenselijk om af te wijken van poort 443?

De voorzitter heeft hiervoor overleg gehad met Gerald, aangezien hij binnen de werkgroep Edukoppeling een punt van gemaakt heeft. Dit omdat er eerder besloten is om het poortnummer vrij te laten, nu in UBV wordt teruggedraaid en impact heeft op bestaande verbindingen. De wens is namelijk om meerdere verbindingen op een server af te handelen, echter is daar SNI voor. Daarnaast wordt gevreesd dat daarmee alle verbindingen aangepast moeten worden, wat een grote impact met zich mee kan brengen. Dat begrijpt de voorzitter ook en stelt voor om deze uitgangspunten vast te houden: mogelijkheid tot meerdere sessies op één host en geen onnodige aanpassingen voor bestaande situaties. Daarom stelt de voorzitter voor om SNI verplicht te stellen voor nieuwe verbindingen. Dit wordt door Rimmer onderkent, aangezien 443 de standaard is volgens CISSP. Arnold kan deze opmerking goed begrijpen voor H2M, maar voor M2M is deze minder relevant aangezien je hier onderling

afspraken over kan maken. Maar dat is juist het probleem volgens de voorzitter, want in de praktijk levert dat problemen op. Meestal ben je in gesprek met de applicatie verantwoordelijke en niet met die van het netwerk, wat vaak ook nog eens bij verschillende partijen belegd kan zijn. Robert onderschrijft dat dit problemen zijn die hij in de praktijk tegenkomt. Om tegemoet te komen aan alle bezwaren, stelt de voorzitter voor om SNI verplicht te stellen voor nieuwe verbindingen. Op basis daarvan kijken we verder.

Afspraak
De voorschrift voor het gebruik van 443 wordt definitief gemaakt, met de uitzondering voor bestaande verbinding. Daarbij onderschrijven wat belang is om vast te houden aan 443. Ook bekijken we hoe partijen deze transitie kunnen maken voor de toekomst.

Aanvullend daarbij geeft Arnold aan dat er voor de huidige situatie wel een register moet zijn met alle verbindingen en hun afwijkende poortnummers, anders kan men elkaar niet vinden. Maar dat is juist hetgeen wat we proberen te voorkomen, aldus de voorzitter.

ii. Verkenning voorschriften PKI
Jordy licht toe dat in het voorgaande overleg besloten is dat de verschillende soorten certificaten - onder welke validatie deze is uitgegeven - te beschrijven. Op basis daarvan kunnen partijen zelf een keuze maken voor het juiste certificaat. De vraag is echter of dit voldoende is om te zorgen dat partijen de juiste certificaat hanteren.

Rimmer geeft aan dat daarnaast ook PKIoverheid gehanteerd kan worden, waarvoor extra handelingen nodig zijn. Jordy geeft aan dat dit onder *organisation validated* (OV) valt, echter wel met strengere eisen. Dat staat ook in de voorschriften beschreven. Daarnaast geldt een PKIoverheid certificaat wanneer OIN verplicht is, wat onder M2M beschreven staat. Dat staat ook toegelicht onder hoofdstuk 5. PKI van de voorschriften, echter is dit niet voor iedereen duidelijk. Jordy licht toe wat hij daarmee bedoelt. De PKIoverheid Server certificaat kent ook een *extended validated* (EV) variant, echter wordt deze voorzien van een KvK nummer i.p.v. OIN. Daarom is deze niet geschikt voor M2M-communicatie, maar wel voor een publieke site. De voorzitter stelt voor om deze verduidelijking aan te brengen in de voorschriften. Daarnaast haalt Rimmer de Let's Encrypt certificaten aan. Die vallen volgens Jordy onder de DV, aangezien daarbij voldoende is om aan te tonen dat de aanvrager beheerder is van een domein. Dit wordt bijgewerkt als voorbeeld.

Actie Jordy
Het verschil van PKIoverheid OV en EV duidelijk toelichten en voor welke situaties dit van toepassing is. Daarnaast Let's Encrypt als voorbeeld opnemen.

Verder vraagt Rimmer of *wildcard* certificaten ook een onderdeel moet zijn van voorschriften, aangezien dit risico's met zich meebrengt. Op dat moment is er geen overzicht waar certificaten gebruikt worden. Arnold onderschrijft dit en adviseert om dit niet te gebruiken vanuit een security perspectief. Robert geeft aan dat niet algemeen voorgeschreven kan worden, aangezien sommige situaties hier niet voor lenen. Niet voor M2M, maar voor H2M, zoals websites met veel verschillende domeinnamen. Op dat moment loop je tegen limieten aan van automatische DV-certificaten. Op dat moment dient op een andere wijze het overzicht gerealiseerd te worden. De voorzitter geeft aan dat we hier dan ook niet te streng in kunnen zijn, maar voor gevoelige uitwisselingen niet gewenst is. Jordy oppert daarmee om een voorschrift op te stellen o.b.v. de BIV-classificatie, zoals ook eerder voor andere voorschriften is gedaan.

Actie Jordy
Voorstel wanneer een *wildcard* certificaat toegepast mag worden en deze opnemen in een nieuwe conceptversie van de voorschriften.

Jordy vraagt aan de werkgroep of er nog andere voorschriften gewenst zijn voor het toepassen van het juiste certificaat. Bijvoorbeeld voor de toepassing van Let's Encrypt certificaten, zoals Rimmer eerder aanhaalde. Arnold ziet hier geen beveiligingsrisico's in, als dit gedegen wordt toegepast. Daarnaast haalt Robert het voordeel ervan aan: het heeft een automatisch verwerkingsmechanisme, waardoor de kans op het verlopen van certificaten juist kleiner is in tegenstelling tot handmatige certificaten. Op basis hiervan concludeert de werkgroep dat hier geen aanvullende afspraak voor nodig is.

Daarnaast vraagt Jordy aan de werkgroep of er contexten zijn waarbij gewenst is dat de gebruiker de organisatie achter een website kan controleren. Dit is bijvoorbeeld alleen mogelijk met een OV of EV certificaat, aangezien in een DV certificaat de organisatienaam niet wordt opgenomen. Volgens de werkgroep zijn deze er tot nu toe niet, met name omdat de doorsnee gebruiker hier niet op controleert.

Afspraak
Er zijn geen extra afspraken nodig om te zorgen dat partijen de juiste certificaten toepassen. De huidige toelichting onder hoofdstuk PKI zou voldoende moeten zijn.

iii. Authenticatie en tweezijdige TLS
De voorzitter licht dit punt toe. Bij tweezijdige TLS, waarbij authenticatie plaatsvindt met het certificaat is soms gewenst. Voor Edukoppeling is dit verplicht, echter zou dit voor meer contexten verplicht kunnen zijn. Jordy geeft aan dat hier nu een voorschrift voor opgenomen is: "*TLS-M2M-08: Indien een OIN verplicht en de integriteit daarvan noodzakelijk (niveau 3) is, dient de authenticatie met een certificaat van PKIoverheid plaats te vinden"*. De vraag is of dit ook onder andere condities verplicht gesteld moet worden. Robert onderschrijft dat de betrouwbaarheid afhankelijk is van de CSP, zoals PKIoverheid.

Gezien de tijd en het nog te behandelen agendapunten, stelt de voorzitter voor om een vervolg te plannen. Daar stemt de werkgroep mee in. Een vervolgafspraak wordt gepland op dinsdag 14 april.

Vervolg op dinsdag 14 april 2020 tussen 9:00 - 10:00. 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: Olav Loite (VDOD), Marten Bakker (The Learning Network)

De voorzitter opent opnieuw het overleg en stelt voor om te beginnen waar we vorige keer geëindigd zijn. Dat betreft het punt over 'Authenticatie en tweezijdige TLS'. Jordy licht toe dat hier nu een richtlijn voor is opgenomen, echter geldt deze alleen wanneer OIN verplicht is, zoals voor Edukoppeling. De vraag aan de werkgroep is of er andere situaties zijn waarin we dit verplicht willen stellen. Die is er volgens de werkgroep niet. Joost draagt daarbij aan dat - hoe het nu geformuleerd is - niet strijdig is met hoe Surf het georganiseerd heeft; zij werken niet met OIN en dus geen PKIoverheid certificaten.

De voorzitter vraagt zich echter af of deze voorschrift apart opgenomen dient te worden, aangezien deze reeds onderdeel is van het profiel Edukoppeling. Rimmer stelt voor om dit voor de transparantie wel te laten staan. De voorzitter beaamt dat het goed is voor de volledigheid, echter zou het dan logisch zijn om dit onderdeel te laten zijn van hoofdstuk PKI.

Afspraak
Voorschrift voor authenticatie met PKIoverheid geldt voor uitwisseling contexten met OIN. Vooralsnog alleen voor Edukoppeling en (nog) niet voor andere contexten. Voor de duidelijkheid wordt deze voorschrift verplaatst naar het hoofdstuk PKI.

d. Afspraken over (uit)fasering

i. TLS-configuraties 'Uit te faseren', zoals TLS1.0 en TLS1.1
De voorzitter licht het agendapunt toe. Veel partijen hebben TLS1.0 en TLS1.1 uitgefaseerd of doen dit in 2020. Microsoft heeft de voorbereiding op TLS 1.2 voor Office 365 voor juni 2020 op de planning staan. De voorzitter vraagt of dit nog een interessant thema is, aangezien browsers dit komende tijd ook uitfaseren en dus niet meer mogelijk wordt om op basis hiervan een verbinding te maken. Robert geeft aan dat de uitfasering door COVID-19 zijn uitgesteld. Daarnaast stelt Rimmer voor om hier wel iets over op te nemen, met name voor gevoelige uitwisselingen.

De voorzitter vervolgt het agendapunt. TLS1.0 en TLS1.1 is volgens de voorschriften niet (meer) toegestaan, echter voor H2M kan hier uitzondering voor gemaakt worden. De voorzitter vraagt zich echter af of voorschriften nodig zijn, aangezien de browsers zullen opleggen wat er gebruikt kan worden. Jordy geeft echter aan dat dit niet geldt voor verouderde devices die niet meer geupdate worden. Arnold geeft ook aan dat het een balans is dus veiligheid en functionaliteit: zoveel mogelijk devices accepteren. Partijen moeten daarom de tijd krijgen om nieuwe TLS-versies te implementeren. Aangezien er devices gebruikt worden met oude versies van browsers - doordat deze niet geupdate (kunnen) worden - vraagt de voorzitter of deze dan geblokkeerd moeten worden.

Robert geeft aan dat zij vanaf vorige jaar een strategie voor het uitfaseren hebben gehanteerd. Gebruikers zijn door middel van een banner op de hoogte gebracht wanneer zij met een verouderde browser verbinding maakten. Met de achterliggende gedachte om de verouderde TLS-versies uit te faseren. Inmiddels is dit ook gerealiseerd, mede gezien het feit dat de verouderde TLS-versies nog gering gebruikt werden. De voorzitter geeft aan dat het mooi zijn als we dit gelijktijdig met de sector kunnen doen en vraagt hoe andere hierin zitten. Rimmert geeft aan dat zij dit ook grotendeels hebben gedaan en de rest volgt; daar loopt nog een traject voor. Langer dan gepland, door de impact die dit kan hebben. Daar zullen andere partijen mogelijk ook last van hebben. Tijdig nieuwe TLS-versies implementeren is dan ook essentieel. Jordy geeft aan dat het dan juist goed is om dit op de lijst met uit te faseren te zetten, zodat dit ook gecommuniceerd kan worden.

De voorzitter geeft aan dat nu niet alle partijen even snel zijn met het uitfaseren en daarmee niet eenduidig overkomt naar de gebruikers die webdiensten binnen de sector benaderen. Hij stelt voor om hier gezamenlijk in op te trekken. Dus niet alleen afspreken wanneer oudere TLS-versies uitgeschakeld moeten zijn, maar ook hoe lang we dit als sector willen ondersteunen.

De voorzitter vraagt de werkgroep hoe lang we de oude versies willen toestaan of dat we dit aan het browserforum over willen laten. Arnold stelt voor om dit zelf te bepalen, aangezien

onze sector wellicht andere risicoprofielen kent. Hij stelt dan ook voor om dit risicogebaseerd te doen. De voorzitter onderschrijft dit en stelt voor om de afspraak dan ook risicogebaseerd te maken. Joost vraagt zich echter af of deze afspraak überhaupt gemaakt moet worden, aangezien de verouderde TLS-versies reeds de classificatie uitfaseren heeft in het NCSC document. Daarnaast benadrukt hij dat de browsers deze te zijner tijd niet meer zullen ondersteunen, op dat moment weten partijen dit ook. Rimmer geeft daarbij echter aan dat we moeten voorkomen dat partijen worden overvallen. We moeten ze tijdig adviseren om nieuwe TLS-versies te implementeren, zodat oudere op elk gewenst moment uitgeschakeld kunnen worden.

Rimmer benadrukt nogmaals dat de toepassing van TLS1.3 de nodige impact met zich meebrengt. Daarom stelt Arnold voor om tevens het advies op te nemen dat partijen een parallelle infrastructuur met TLS1.3 kunnen opbouwen, om daarmee een bigbang migratie te voorkomen. Bijvoorbeeld wanneer verouderde protocollen niet meer veilig zijn. Op dat moment kan alleen de legacy situatie uitgeschakeld worden, zonder dat dit impact heeft op de veilige verbindingen.

De voorzitter geeft aan dat we op dit moment voldoende hebben geïnventariseerd en stelt voor om op basis hiervan het nodige te zullen opnemen in de voorschriften, waarop gereflecteerd kan worden.

Afspraak
Op basis van de inventarisatie tijdens het agendapunt ‘TLS-configuraties ‘Uit te faseren’, zoals TLS1.0 en TLS1.1’ zullen we het nodige opnemen in de voorschriften. Op basis daarvan kan de werkgroep reflecteren.

ii. Naast TLS1.2 ook TLS1.3 voor de onafhankelijkheid en toekomstvastheid
De voorzitter geeft aan dat dit punt deels aanbod is gekomen tijdens het vorige agendapunt over uitfasering TLS1.0 en TLS1.1. De vraag is wat het advies moet zijn richting de sector wanneer zij TLS1.3 geïmplementeerd moeten hebben. Bijvoorbeeld 2021. Robert zet daar vraagtekens bij, echter geeft de voorzitter dat er nu niks over geadviseerd wordt. Iets van helderheid zou goed zijn. Rimmer geeft aan dat het ook een kwestie is van bespreken met de achterban. Volgens Rimmer zou het ook goed zijn dat de achterban voorafgaand aan de begroting op de hoogte is, zodat dit begrotingstechnisch meegenomen kan worden. Partijen zouden al moeten beginnen met analyseren van de omgeving, zodat inzichtelijk wordt wat er aangepast moet worden om TLS1.3 te activeren. Robert geeft aan dat zij reeds bezig zijn met de implementatie van TLS1.3 om inzichtelijk te maken wat hiervoor nodig is. Dit zouden andere partijen ook kunnen doen. De voorzitter stelt dan ook voor om hier aandacht aan te vestigen, dus te stimuleren om de volgende versie van TLS klaar te hebben staan. Maar geen harde datum.

Afspraak
Ketenpartijen moeten gestimuleerd worden om de nieuwe versie van TLS1.3 te implementeren, zodat inzichtelijk wordt wat voor impact dit heeft en dus begroot kan worden.

3. Veilig en betrouwbare e-mail (SPF, DKIM en DMARC)

a. Afspraken maken o.b.v. huidige informatie en materialen

Naar aanleiding van de voorgaande presentatie en nieuwe informatie en materialen, kunnen afspraken gemaakt worden. Deze kunnen als eis opgenomen worden in de voorschriften.

Rimmer vraagt zich af of deze niet beter apart opgenomen kan worden, met name voor de distributie. De voorzitter geeft aan dat dit nog niet bepaald is. Hiervoor vindt nog overleg plaats met Edustandaard. Het is in ieder geval van belang om alle afspraken vast te leggen.

b. Vervolg

Rimmer stuurt de documenten toe en wordt in het volgende overleg verder besproken.

4. Afsluiting

De voorzitter bedankt een ieder voor zijn bijdragen en stelt voor om het gezien de tijd hierbij te laten. Arnold opperde eerder om de overleggen wat korter op elkaar te laten plaatsvinden. Op basis daarvan is 18 mei voorgesteld. Dit schikt voor aanwezige. Of dit ook voor de afwezige geldt, zien we via de reactie op het agenda-verzoek.