Implementatieadvies WDO standaarden

Voor:	Standaardisatieraad
Van:	Bureau Edustandaard
Datum	sept / okt 2020

Aanleiding

Op verzoek van de KRO's heeft de Standaardisatieraad besloten om de WDO beveiligingsstandaarden te volgen. Hierbij zijn 2 verzoeken gedaan. Het eerste verzoek was om de WDO standaarden op te nemen in de ROSA. De tweede vraag was om advies te geven op welke wijze de WDO standaarden geïmplementeerd kunnen worden.

WDO standaarden in de ROSA (vraag 1)
De Standaardisatieraad heeft ingestemd met het eerste verzoek. Op basis van dit verzoek heeft de Architectuurraad een procesvoorstel gedaan voor opstellen van architectuurkaders voor de WDO standaarden waarbij de werkgroep Uniforme beveiligingsvoorschriften wordt belast met de uitvoering van dit proces. Dit voorstel is goedgekeurd door de Standaardisatieraad.
De WDO standaarden worden opgenomen in de ROSA bij de verplichte standaarden. Een standaard is verplicht als dit in de wet is opgenomen of hierover een bestuurlijke afspraak is gemaakt. Een voorbeeld van een wettelijke verplichte standaard zijn de toegankelijks richtlijnen. Scholen moeten deze volgen door Europese regelgeving. De WDO standaarden zijn verplicht voor de overheid door nationale regelgeving. De B-organen (private organen met publieke taak) vallen binnen de scope van de wet maar de B-organen worden niet landelijk aangewezen. Binnen het onderwijsdomein hebben de KRO's de bestuurlijke beslissing genomen de beveiligingsstandaarden te volgen. In de ROSA wordt de volgende toelichting gegeven

- Doel standaard
- Achtergrond van verplichting (wettelijk of bestuurlijke beslissing)
- Datum waarop standaard moet zijn ingevoerd. Bij de WDO standaarden worden de implementatiedata van de overheid overgenomen.
- Werkingsgebied, hier wordt de scope beschreven.
- Toepassingsgebied. Hier wordt aangeven welke processen worden geraakt.

Implementatie WDO standaarden (vraag 2)
Het adviesvoorstel bestaat uit 2 onderdelen:

- Een procesvoorstel dat aangeeft welk proces gevolgd kan worden bij de implementatie van de WDO standaarden.
- Een inhoudelijke paragraaf die aangeeft wat de impact is en wat er inhoudelijk moet gebeuren. Wat er moet gebeuren zal per standaard verschillen. In de inhoudelijke paragraaf wordt de standaard TLS uitgewerkt en er wordt een vooruitblik gegeven voor de mailstandaarden.

Procesvoorstel

Het voorgesteld proces is onderverdeeld in 3 fasen: voorbereiding, realisatie en evaluatie.
In de WDO zullen periodiek nieuwe standaarden worden opgenomen. Bij elke nieuwe standaard zal dit proces opnieuw doorlopen moeten worden. Implementeren van standaarden gebeurt nu ook al, dit geldt ook voor beveiligingsstandaarden. Wij beginnen dus niet op nul. Dit geldt met name voor de voorbereidingsfase. Alleen gebeurt het implementeren nu op vrijwillige basis. Er is geen zicht op wie de standaard implementeert en wie niet. En er zijn ook geen instrumenten om vast te stellen hoe het staat met de implementatie van de standaard.

Bij de uitwerking van het procesvoorstel kan gebruik worden gemaakt van de ervaring die wordt opgedaan met individuele standaarden. Gestart wordt met de standaarden TLS en de mailstandaarden. De voorbereidingsfase is al gedaan. Op basis hiervan is ook al vastgesteld dat voor de realisatie het reguliere standaardisatieproces kan worden gevolgd. Voor deze standaarden is ook gekeken op welke wijze evaluatie plaats kan vinden. Met name om ook stappen te kunnen zetten die er voor zorgen dat iedereen deze standaard gaat volgen. Waarbij gekeken is hoe gebruik gemaakt kan worden van initiatieven die al lopen. De concretisering van het proces zal iteratief plaatsvinden op basis van concrete praktijkervaringen. Waarbij ook aandacht is voor een stapgewijze professionalisering. De instrumenten die WDO gebruikt voor evaluatie zijn geschikt als eindbeeld maar voor het onderwijsdomein zijn tussenstappen nodig.

De standaarden waarbij wordt gestart (TLS en mailstandaarden) zijn relatief makkelijk omdat hiervoor veel draagvlak bestaat en er maar weinig aanpassingen nodig zijn om ze te implementeren. De bereidheid om te investeren wordt vooral bepaald door de wil om te investeren in veiligheid.

Dit geldt niet voor elke standaard. De WDO stelt bijvoorbeeld ook eisen aan toegang en schrijft voor A-organen ook een standaard voor (gebruik van eID, eHerkenning en EIDAS). Binnen het onderwijsdomein is dit in sommige gevallen verplicht maar er zijn ook veel andere vormen van toegang die vaak sectorspecifiek zijn. Architectuurkaders voor toegang voor het onderwijsdomein moeten aansluiten bij de eisen van de WDO maar er is meer voor nodig om een doorlopende leerlijn te borgen. Tijdens de voorbereidingsfase kan door de Architectuurraad vastgesteld worden waar de knelpunten zitten en welke keuzes gemaakt moeten worden. Maar voor het maken van deze keuzes is sector overschrijdende besluitvorming nodig. En voor het bepalen van de impact van de keuzes is projectsturing nodig. Voor deze complexe standaarden kan de Architectuurraad alleen geen architectuurkaders opstellen. Wel kunnen tijdens de voorbereiding werkpakketten worden gedefineerd die nodig zijn voor het opstellen van deze architectuurkaders. En per werkpakket kan ook worden aangegeven of er een meest gerede partij is die belast kan worden met dit werkpakket. Op dit werkpakket moet projectsturing uitvoeren met een bestuurlijk verantwoordelijk als opdrachtgever. Het onderdeel realisatie wordt later uitgewerkt aan de hand van een complexe standaard.

Voorbereiding

De voorbereiding wordt gedaan door de werkgroep UBV. Het doel is om de veiligheid van de informatiehuishouding te borgen. De beveiligingsstandaarden zijn een middel om dit doel te bereiken. Er moet ook gekeken worden naar de samenhang met andere standaarden en de organisatorische maatregelen. Dit heeft als consequentie dat het implementeren van beveiligingsstandaarden wordt ingebed in grotere werkpakketten die als 1 geheel worden geïmplementeerd. De volgende principes worden gehanteerd bij de voorbereiding:

Principe 1 Koppel standaarden aan doelen
De overheid stuurt op maatschappelijke waarden. De WDO standaarden kunnen gekoppeld worden aan het doel "borgen van veiligheid en continuïteit van de informatievoorziening.

Principe 2 Maak een context specifieke analyse

- Onderscheid toepassingsgebieden
  Voor elk toepassingsgebied kan het nodig zijn een andere implementatiestrategie te hanteren. Bepaal voor welke toepassingsgebieden een analyse moet worden uitgevoerd.
- Voer risico analyse uit. Voer per toepassingsgebied een risico analyse uit. Bepaal het huidige en het gewenste beveiligingsniveau.
- Bepaal de inhoudelijke randvoorwaarden
  Bepaal de randvoorwaarden voor implementatie. Kijk hierbij naar de samenhang met andere standaarden en welke aanpassingen aan processen en informatievoorziening nodig zijn om het gewenste beveiligingsniveau te bereiken. De WDO stelt bijvoorbeeld eisen aan de organisatorische maatregelen. Voor de Rijksoverheid worden deze beschreven in de BIO, binnen het onderwijsdomein wordt hiervoor het certificeringsschema IBP gebruikt. De WDO standaarden worden opgenomen in het certificeringsschema. Aansluiten op de WDO heeft als consequentie dat het certificeringsschema periodiek herzien moet worden. En het object van implementatie wordt dan een nieuwe versie van het certificeringsschema, met alle onderliggende standaarden.
- Bepaal de prioriteit voor de implementatie. Voor elk toepassingsgebied wordt bepaald welke urgentie de implementatie heeft. Dit wordt bepaald door het verschil tussen het gewenste beveiligingsniveau en het huidige beveiligingsniveau. Dit bepaalt het beveiligingsrisico, dit wordt afgezet tegen de kosten die gepaard gaan met de implementatie. Daarnaast wordt gekeken naar het verandervermogen van de organisatie. Het verandervermogen wordt mede bepaald door het totaalpakket aan veranderingen die een organisatie binnen een bepaald tijdsbestek moet realiseren.
- Bepaal stuurmogelijkheden op de implementatie
  De mate waarin gestuurd kan worden op de implementatie verschilt per toepassingsgebied en soms per organisatie. Hierbij kan gebruik worden gemaakt om een logische fasering in de implementatie aan te brengen. DUO zal als A-orgaan WDO standaarden sneller moeten implementeren en zal de betreffende standaarden in al haar uitwisselingen met ketenpartijen verplicht zal stellen. Omdat die ketenpartijen het daarmee al beschikbaar hebben, kunnen ze het makkelijker toepassen in andere uitwisselingen. De context van OSO kent een goed georganiseerde governance met sterke vertegenwoordiging vanuit het publieke domein en ook hier is de verwachting dat het snel doorvoeren van afgesproken standaarden op draagvlak kan rekenen. Een vergelijkbare redenering geldt voor uitwisselingen van het OSR (Onderwijs serviceregister) van Kennisnet, deze zal snel de nieuwe beveiligingsstandaarden adopteren en dus ook hanteren in alle uitwisselingen. Ketens waar minder regie is vanuit het publieke domein bijv. leermiddelenketens zijn afhankelijk van de mate waarop hier regie kan worden uitgevoerd
- Analyseer belemmeringen en overtuigingen die adoptie in de weg kunnen staan. Binnen een toepassingsgebied kunnen maatregelen zijn getroffen die wel de veiligheid in betreffende keten kunnen garanderen maar waarvoor andere standaarden zijn gebruikt. Dat maakt uitwisseling met andere domeinen minder voorspelbaar en hierdoor minder veilig. Er is een verschil tussen een lokaal belang en het stelselbelang.
- Maak een implementatieadvies met voorstellen voor realisatie en evaluatie

Realisatie

Op basis van het implementatie advies wordt besloten of voor de realisatie het reguliere standaardisatieproces kan worden gevolgd of dat projectsturing nodig is. Wanneer het reguliere standaardisatieproces kan worden gevolgd beperkt de overkoepelende sturing zich tot communicatie. De sectorraden zijn hiervoor eindverantwoordelijk. Op basis van het implementatie advies kunnen zij bepalen op welke wijze zij dit doen.

Wanneer projectsturing nodig is zullen de KRO's eindverantwoordelijk zijn. Voor deze situatie gelden de volgende implementatieprincipes:

Principe 3 Beleg implementatieverantwoordelijkheid
De implementatieverantwoordelijkheid kan per toepassingsgebied verschillen. Beleg de verantwoordelijkheid voor de implementatie binnen een toepassingsgebied.

Principe 4 Richt plan-do-check act cyclus in voor implementatie.
De implementatieverantwoordelijke moet sturen op de implementatie. Hiervoor moet een plan-do-check act cyclus worden ingericht.

Principe 5 Neem relevantie beveiligingsdoelen op in het I-plan voor ketenprocessen
Neem de relevante beveiligingsdoelen op in het meerjarig i-plan. Koppel aan deze doelen de werkpakketten die in het implementieadvies beschreven zijn. De globale impact is beschreven in het implementatieadvies. Voor het bepalen van de financiële consequenties zal aanvullende analyse nodig zijn. Zorg dat deze analyse wordt uitgevoerd zodat de beveilingsdoelen geprioriteerd kunnen worden ten opzichte van andere doelen. Op basis van deze afweging wordt bepaald in welk jaar de implementatie van de standaarden plaats zal vinden. De implementatieverantwoordelijke zorgt voor communicatie met alle betrokkenen en een gedragen I-plan.

Principe 6 Stuur op projecten uit I-plan
De veranderdoelstellingen uit het I-plan worden vertaald naar concrete projecten. Elke organisatie stuurt op de eigen projecten. Bij complexe verandertrajecten kunnen ketenprojecten worden gestart die enerzijds zorgen voor de coördinatie en anderzijds worden belast met het realiseren van ketenvoorzieningen. De implementatieverantwoordelijke beslist of het nodig is om ketenprojecten te starten.

Evaluatie

Het belangrijkste verschil met de huidige werkwijze is dat een afgesproken standaard geen advies is maar een verplichting. Daarom is evaluatie nodig. Voor de evaluatie gekozen worden tussen verschillende instrumenten. In deze paragraaf worden een aantal alternatieven beschreven. Bij het implementatieadvies voor een standaard wordt ook gekeken naar evaluatie. Waarbij gekeken wordt of gebruik kan worden gemaakt van initiatieven die al lopen.

Principe 7 Bepaal op welke wijze voortgang geborgd kan worden.
De daadwerkelijke implementatie vindt plaats door individuele organisaties. Wanneer een ketenproject belast wordt met de implementatie kan dit ketenproject de voortgang monitoren. Dit is echter lang niet altijd het geval. Daarom zal op stelselniveau bepaald moeten worden op welke wijze evaluatie plaats. Hierbij wordt gekeken naar de wijze waarop Rijksbreed de evaluatie georganiseerd is. De aanpak hoeft niet hetzelfde te zijn maar wel gelijkwaardig.
Hieronder zijn een aantal opties voor evaluatie. De opties zijn opgenomen in volgorde van toenemende regie. Hierbij is gekeken naar de wijze waarop evaluatie binnen de overheid wordt uitgevoerd. Waarbij is onderkend dat binnen het onderwijs nog niet wordt gestuurd op implementatie en dat het niet wenselijk is om meteen een heel strakke regie te gaan voeren. Daarom wordt onderkend dat een stapgewijze professionalisering nodig is:

- Softwarecatalogus
  Een softwarecatalogus kan inzicht bieden in de mate waaraan een leverancier aandacht besteed aan veiligheid. Het voorstel is dat te doen op basis van het certificeringsschema. Waardoor een instelling kan zien welke leveranciers zich committeren aan het certificeringsschema.
- Opnemen standaarden in de inkoopvoorwaarden
  In de inkoopvoorwaarden kan de eis worden opgenomen dat wordt aangesloten op het certificeringsschema. Op basis van de inkoopvoorwaarden kan bepaald worden of een instelling hier naar vraagt of niet.
- Motiveren afwijking in jaarverslag (comply or explain)
  In de jaarplan richtlijnen kan worden opgenomen dat als verplichte standaarden niet gevolgd worden dit in het jaarverslag gemotiveerd moet worden. Dit speelt vooral als bij nieuwe projecten verplichte standaarden niet zijn opgenomen in de inkoopvoorwaarden. Evaluatie is mogelijk door op basis van de jaarverslagen te monitoren wanneer wordt afgeweken. Hiermee wordt de verantwoordelijkheid voor de implementatie ook expliciet belegd bij een instelling. Er is een duidelijk kader dat aangeeft welke standaarden de instelling moet implementeren. Tevens is aangegeven dat de consequentie is dat de instelling middels de inkoopvoorwaarden aan de leverancier moet vragen om dit te doen. Bij gebruik van standaard inkoopvoorwaarden zoals die van SIVON hoeft de instelling geen technische kennis te hebben. Als de instelling hier bewust van afwijkt neemt ze hiervoor ook de bestuurlijke verantwoordelijkheid door dit te motiveren in het jaarverslag.
- Monitoring door meting
  Implementatie van standaarden kan niet volledig gevolg worden middels de inkoopvoorwaarden. Er is niet altijd sprake van een inkooptraject. Bijvoorbeeld omdat de standaard vraagt om beheerinstellingen op een specifieke manier te configureren. Bij sommige standaarden kan monitoring plaatsvinden door metingen. Hiermee kan een volledig beeld van de actuele situatie worden verschaft.
- Monitoring door enquête
  Middels een enquête kan instellingen worden gevraagd of ze standaarden kennen en implementeren. Nadeel hiervan is dat de respons op enquêtes laag is. En dat op schoolniveau vaak de kennis van standaarden onvoldoende is om antwoord te kunnen geven op de implementatie van specifieke standaarden. Er moeten dan meer generieke vragen worden gesteld. Of er wordt aan leveranciers gevraagd in welke mate zijn verplichte standaarden volgen.

Inhoudelijke paragraaf

De Wet Digitale Overheid stelt een aantal standaarden op gebied van informatieveiligheid verplicht. In deze paraaf wordt per standaard beschreven wat de impact is en waarmee rekening gehouden moet worden met de implementatie.

Toelichting op rol werkgroep UBV
In het voorgestelde proces is de Edustandaard werkgroep UBV verantwoordelijk voor:

- Analyse
  Bij de analyse wordt bepaald hoe de standaard aansluit op de onderwijscontext
- Opstellen kaders
  Op basis van de analyse bepaalt de werkgroep UBV waar en op welke wijze de standaard geimplementeerd moet worden
- Bepalen globale impact
  De werkgroep maakt een inschatting van de globale impact van de implementatie van de kaders

De werkgroep heeft conform deze rol een analyse gedaan op de TLS standaard en een eerste verkenning voor de mailstandaarden. Hieronder wordt een inhoudelijke duiding gegeven op de TLS standaard en wordt een vooruitblik gedaan op de mailstandaarden

Implementatieadvies TLS

Analyse
De standaard TLS is bedoeld om een beveiligd transport te bieden bij machine koppelingen
De aangewezen standaarden (HTTPS, HTST en TLS) zijn geschikt om de veiligheid te borgen maar laten ruimte voor eigen interpretatie waardoor problemen kunnen ontstaan bij de samenwerking. Voor het onderwijsdomein zijn aanvullende maatregelen nodig..

Opstellen kaders
De werkgroep UBV heeft kaders opgesteld die aangeven hoe de standaarden geïmplementeerd moeten worden. In de huidige situatie is dat een advies aan applicatie leveranciers hoe zij de standaard moeten toepassen.. Verwachting is dat op korte termijn een definitieve versie van deze standaard kan worden vastgesteld.

Een standaard op zich zelf kan er niet voor zorgen dat de veiligheid wordt geborgd. Er is een samenhangende set van organisatorische en technische standaarden die samen de veiligheid borgen. De WDO bevat hiervoor ook kaders. De werkgroep heeft hiervoor het certificeringsschema ontwikkeld. Dit schema zorgt voor de samenhang en de afzonderlijke standaarden voor de concretisering. De standaarden die in de WDO worden aangewezen zorgen er voor dat de algemene afspraken worden aangevuld met concrete maatregelen die periodiek worden herijkt. Het Certificeringsschema geeft invulling aan de 'organisatorische en technische beveiligingsmaatregelen' van de modelverwerkersovereenkomst van het Privacyconvenant

Het certificeringsschema vormt dus het kader. Periodiek komt een nieuwe versie van het certificeringsschema. Deze nieuwe versie moet geïmplementeerd worden.

Globale impact
Gebruik van het certificeringsschema is niet verplicht.. Voor leveranciers die zich hier al bij hebben aangesloten is de impact gering. Er zijn echter ook leveranciers die het certificeringsschema niet ondertekend hebben.

Implementatie van de TLS standaard zal gedeeltelijk 'vanzelf' gaan::

<u>Machine-machine koppelingen op basis van Edukoppeling</u>
Gebruik van Edukoppeling vereist dat het certificeringsschema is ondertekend en Edukoppeling zal gebruikt gaan maken van TLS. Alle gegevensuitwisselingen die gebruik maken van Edukoppelingen worden daarmee automatisch compliant met de UBV TLS afspraken.

Grote browserleveranciers gaan TLS gebruiken voor HTTPS
Organisaties die een beveiligde website beheren ontkomen er niet aan TLS te gebruiken,

De impact zit dus vooral bij uitwisselingen die geen gebruik maken van Edukoppeling en bij leveranciers die het certificeringsschema niet willen ondertekenen.

Monitoren en meten
De werkgroep UBV heeft een adviesrol. Leveranciers bepalen zelf hoe zij omgaan met het certificeringsschema. deze ook werkelijk toepassen. Er is geen certificerende instantie die bepaald of toepassingen voldoen aan de afspraken uit het Certificeringsschema. Leveranciers van toepassingen doen dit in principe via een self assesment en een pas-toe-leg-uit verklaring in de beveiligingsbijlage van de verwerkersovereenkomst. Tenminste voor toepassingen die binnen de scope van het Privacy convenant vallen. Voor toepassingen die daar buiten vallen bestaan nog geen afspraken. Er is ook geen register van toepassingen waarin wordt bijgehouden of deze compliant zijn aan de van toepassing zijn beveiligingsstandaarden en afspraken. Daardoor is het ook niet goed mogelijk om inzicht te krijgen in niveau van compliance en is het dus ook niet mogelijk om te sturen op verhogen van deze compliancy.

Momenteel wordt wel gewerkt aan instrumenten die hier ondersteunde in zouden kunnen zijn. Voor het funderend onderwijs wordt namelijk gewerkt aan een referentie architectuur, de FORA. Een tool die in dat kader wordt ontwikkeld is de zogenaamde softwarecatalogus. Idee van deze softwarecatalogus is dat toepassingen die in het funderend onderwijs worden gebruikt hierin worden geregistreerd om compliancy aan de referentie architectuur te kunnen valideren. Deze tool zou mogelijk ook ingezet kunnen worden om compliancy aan Certificeringsschema en WDO standaarden te kunnen registreren.

Opbouwen draagvlak
Er moet draagvlak worden opgebouwd om de stap te zetten van vrijblijvende adviezen naar regie op het implementeren van kaders. Hierbij kan gebruik worden gemaakt van al lopende initiatieven. Door gebruik te maken van leveranciers die op vrijwillige wijze al het certificeringsschema ondertekenen en grote schoolbesturen die al samenwerken binnen de FORA om te komen tot een software catalogus. De sectorraden kunnen hiervan gebruik maken voor bewustwording van alle instellingen dat dit belangrijk is en dat het een gemeenschappelijk belang is om hier gemeenschappelijke afspraken over te maken.

Implementatieadvies e-Mail standaarden

De WDO stelt bij gebruik van mail de standaarden SPF, DKIM, DMARC, STARTTTLS en DANE verplicht.

Analyse
De emailstandaarden SPF, DKIM & DMARC zijn het meest effectief als ze gezamenlijk worden gebruikt. Deze standaarden vergroten gezamenlijk de afleverbetrouwbaarheid van email:

- Legitieme e-mailberichten worden niet meer onterecht als SPAM wordt aangemerkt
- Beperken risico's van misbruik (e-mail)domeinnaam door derden (phishing).

Zowel bij ingaand als bij uitgaand mailverkeer is er impact:

Uitgaand verkeer
De standaarden moeten goed worden toegepast anders wordt legitieme e-mail niet meer afgeleverd

Ingaand verkeer
De ontvangende partij moet controleren, er moet filtering op ingaand verkeer worden ingesteld.

Deze standaarden zijn pas effectief als ze breed worden toegepast. Waarbij een stapgewijze implementatie nodig is om geleidelijk ervaring met de standaard op te doen. De geleidelijke invoering geldt vooral voor de ontvangende kant. Bijvoorbeeld door wel te starten met analyseren maar nog niet met filteren

Kaders
Op basis van deze analyse gaat de werkgroep UBV kaders opstellen voor veilig en betrouwbaar e-mail verkeer. Deze afspraak bevat een nadere duiding van de standaarden en best practices voor implementatie.

Implementatie
Afspraken voor ketenbreed toepassen van deze afspraken zijn er nog niet.
Geadviseerd wordt om te beginnen met het adviseren van deze standaarden maar nog niet te verplichten. De reden is dat grote mailproviders (zoals Microsoft 365) de standaard op dit moment nog niet of maar beperkt ondersteunen. Organisaties dwingen om aan deze standaard te voldoen gaat daarmee voor problemen zorgen aangezien dit zou betekenen dat ze van mailprovider moeten wisselen.

De werkgroep UBV zal deze standaarden blijven volgen om te bepalen wat het juiste moment is om over te gaan van adviseren naar verplichten. Dit wordt mede bepaald door het moment dat grote leveranciers als Microsoft overstappen.

Monitoren en meten
De website internet.nl kan gebruikt worden voor zelf assessment door onderwijs instelling of leverancier. Hiermee kan gecontroleerd worden in hoeverre aan de standaarden wordt voldaan. Wanneer ketenbreed wordt afgesproken om dit te doen en de bevindingen te delen wordt hiermee inzicht verkregen in de implementatiegraad van de standaarden.