edustandaard

Concept Notulen Werkgroep IBP (maart 2024)

14 maart 2024, 13:00 – 14:30, locatie: online

Aanwezig	Dirk Linden (Edustandaard, voorzitter), Jordy van den Elshout (Edustandaard, expert), Ernst-Jan Heuseveldt (VDOD), Esther van Wijngaarden (Match iT Support), Claudia Cobelens (OCW), Floris Pols (BOOR), Ilja Förster (Sanoma), Jeroen Renard (Heutink), José Teuwen (Kennisnet), Marc Berenschot (Universiteit Twente), Marcel de Rijke (SIVON), Martijn Bijleveld (MBO Digitaal), Paul Gillijns (MEVW), Paul Gijzen (Visma), Rick Reesen (TLN), Robin Rootseler (Vodix), Ruud Tas (ROC Mondriaan), Sandra Schreurs (TLN), Maarten de Niet (namens FORA, tijdens agendapunt 3a).

Notulen

1. Opening
    a. Ruimte voor toelichtingen en voorstellen.
    De werkgroep is lange tijd niet bijeengekomen geweest en de werkgroep heeft veel nieuwe leden.

    Besproken: iedereen heeft zich kort voorgesteld. Daarnaast is het doel en proces van de werkgroep toegelicht. Hierbij is aangegeven dat in een aparte kerngroep de verbetervoorstellen voorbereid worden, die in deze werkgroep behandeld/goedgekeurd kunnen worden.

2. Stand van zaken
    a. Algemeen
    Huidig gebruik van het Certificeringsschema (CS) IBP ROSA, voorgaande wijzigingen op hoofdlijnen, en andere ontwikkelingen (zoals ROSA scan op Surf Baseline) bespreken.
    Doel: zorgen dat iedereen dezelfde informatiepositie heeft, vooral voor de nieuwe werkgroep leden.

    Besproken: aan de hand van de presentatie (zie bijlage 20240314 Kickoff werkgroep.pdf) is toegelicht wat het CS IBP inhoudt en waar het van op toepassing is. Ook is aangehaald wat de wijzigingen zijn in de laatste versie. En dat we nu 2 jaar verder zijn na de laatste wijziging. Er is voldoende aanleiding om gezamenlijk het Toetsingskader te herzien.

    Besluit: met een kleiner gezelschap (kerngroep) het Toetsingskader herzien.

    Vragen die gesteld zijn (incl. een samenvatting van het antwoord):
    1. Hoe breed wordt het CS IBP gebruikt? Absolute aantallen zijn niet bekend, maar zien wel dat het steeds breder gebruikt worden. Naast het gebruik in Privacy convenant, wordt hier ook expliciet naar verwezen vanuit het Normenkader IBP FO. Ook wordt opgevraagd in DPIA trajecten, zoals SIVON dat nu doet.
    2. Hoe gaan we om met opmerkingen op de inhoud? En specifiek over de formulering in relatie tot invulling door cloud leveranciers. Opmerkingen kunnen altijd aangemeld worden bij info@edustandaard.nl. Uitbesteden van maatregelen staat expliciet verder op de agenda.
    3. Zoeken wij (inhoudelijk) ook verbinding met Surf Baseline? Vertegenwoordigers van de werkgroepen hebben onderling contact en hebben eerder ook afstemming gehad.

Dit blijft ook in de toekomst het geval, om inhoudelijk niet uit elkaar te lopen. Dit is ook één van de aanbevelingen uit de ROSA-scan.

b. Ontwerpgebied IBP
In 2023 is er een nieuwe versie van ROSA gepubliceerd. *Naar aanleiding hiervan zijn ook de principes voor IBP herzien en uitgewerkt in een IV-domein (*Inrichten IBP-maatregelen*) binnen de ROSA.*
Doel: informeren over de uitwerking IV-domein IBP en bespreken van eventuele vragen of aandachtspunten.

Besproken: ROSA is nader toegelicht incl. de positie van de afspraken die we in deze werkgroep maken. Op dit moment zijn hier geen vragen over.

Besluit: mochten er wel vragen zijn, dan kunnen deze in een volgende werkgroep bijeenkomst behandeld worden of achteraf ingediend worden via info@eudstandaard.nl.

c. Document Toezicht
Toezicht vindt steeds vaker plaats en gaat komende jaren toenemen. Binnen de onderwijssector lopen daar verschillende trajecten voor, zoals ook binnen Digitaal Veilig Onderwijs door SIVON. Daarnaast zijn enkele opmerkingen binnengekomen op het document Toezicht. i) Zo leidt classificatie van onafhankelijkheid (laag, midden, hoog) verwarring op; deze heeft dezelfde classificatie categorieën heeft als de BIV, waardoor de lezer hier een koppeling in maakt. Deze is er alleen niet. ii) Ook zijn de eisen voor de externe audit niet voldoende duidelijk. Registratie van een auditor kan bijvoorbeeld op meerdere niveaus.
Voorstel is om het document te herzien met een review door belanghebbenden, mede op basis van de huidige en gewenste toezicht in de sector.
Doel: voorstel bespreken en bepalen wie een actieve rol kan of moeten spelen in de review van het document Toezicht.

Besproken: naast de toelichting (zoals hierboven uiteengezet) voorgesteld om het document te herzien.

Besluit: hier is geen bezwaar tegen en wordt daarom als thema meegenomen voor herziening, wellicht – gezien de aard van dit document - met een andere samenstelling dan bij de inhoudelijke thema's.

Vraag tijdens dit agendapunt: in hoeverre sluit het CS aan op het Normenkader die in het onderwijs gebruikt wordt? Het CS is een nadere invulling van het Normenkader en zou daarmee helpen bij het invullen van het Normenkader IBP. Vanuit het Normenkader IBP FO wordt de relatie met het CS inzichtelijk gemaakt.

d. Wetgeving NIS2
Op 17 oktober 2024, of later door uitstel, treedt de Nederlandse versie van NIS2 in werking. Waarschijnlijk door middel van opvolging van de Wet beveiliging netwerk- en informatiesystemen (Wbni). In artikel 21 lid 2 (NIS2) staan maatregelen die getroffen moeten worden. Zoals over bekendmaking van kwetsbaarheden (sub f) en gebruik multifactor-authenticatie (sub j). De vraag is in hoeverre deze overeenkomen en in lijn zijn met het Toetsingskader. Wanneer dat wel het geval is, draagt dat op een effectieve wijze bij aan het conformeren aan deze wetgeving (indien een aanbieder van ict-toepassingen

hieraan moet voldoen).
Doel: bespreken en besluiten om impact van NIS2 mee te nemen in herziening van het Toetsingskader.

Besluit: geen bezwaar tegen dit voorstel en NIS2 maatregelen worden meegenomen in de herzien van het Toetsingskader.

3. Inhoudelijk
   a. Vaststellen BIV-classificatie
   De BIV hoort door de proces/data-eigenaar (de verwerkingsverantwoordelijke) vastgesteld te worden, echter wordt dit met de huidige opzet door de leverancier bepaald door het invullen van de vragenlijst. In de praktijk wordt dit ook veelal door alle schoolinstellingen (de verwerkingsverantwoordelijke) overgenomen, echter is de vraag of de BIV-classificatie in dat geval juist is. In geval van een hogere BIV door de leverancier hoeft dit geen probleem te zijn, echter bij een lagere BIV wel; de (persoons)gegevens zijn in dat geval onvoldoende beschermd conform de baseline. De verantwoordelijkheid om dit te controleren ligt bij schoolinstelling, echter is enige mate van uniformiteit gewenst. De sectorale Referentie Architectuur (zoals FORA, MORA en HORA) kunnen hier mogelijk een rol in spelen. Daarin zijn BIV-classificaties opgenomen als referentiecomponent en kan naar verwezen worden.
   Doel: Situatie en mogelijke verbeteringen bespreken. Indien mogelijk tot een besluit komen, welke uitgewerkt kan worden in het Cert. schema. Mogelijk ook een bestellingen richting andere initiatieven, zoals modelverwerkersovereenkomsten t.b.v. de blijvende verantwoordelijkheid tot controle.

   Besproken: een nadere toelichting van de referentie architectuur, zoals FORA, zodat iedereen hiervan op de hoogte is. Ook hoe de BIV dan centraal vastgesteld kan worden. Aangezien de referentie architectuur met name door publieke partijen is vastgesteld, zouden private partijen ook inspraak willen op het gebruik van een centrale BIV-classificatie. Vanuit de private partijen is het ook van belang om rekening te houden met toepassingen die niet volledig overkomen met generieke objecten uit de referentie architectuur. Opmerking is ook dat voorkomen moet worden dat dit tot nieuwe of andere discussies gaat leiden. Uit de praktijk (vanuit publieke partijen) wordt wel gezien dat classificaties soms verkeerd (lees: te laag) worden ingeschat. Ofwel een gedeeld beeld tussen private en publieke partijen.

   Besluit: in samenwerking – zowel publieke als private partijen – dit vraagstuk verkennen. Dit wordt dan als één van de (aparte) thema's opgepakt.

   b. Uitbesteden van maatregelen en de controle hierop
   Steeds vaker worden clouddiensten gebruikt waarmee ict-toepassingen in het onderwijs worden aangeboden. In dat geval worden meerdere maatregelen door de cloudprovider verzorgt, echter blijft de aanbieder/verwerker verantwoordelijk dat dit afdoende is ingevuld. Daarnaast zijn maatregelen standaard verzorgt (zoals fysieke beveiliging), of op basis van een instelling (zoals encryptie). Edustandaard heeft het signaal ontvangen dat hier meer informatie per maatregel en leverancier over gewenst is. Wellicht dat collectief hier een FAQ voor ingericht kan worden, zodat alle aanbieders hierin het onderwijs profijt van kunnen hebben.
   Doel: bespreken of een FAQ hier passend is en op welke manier dit collectief georganiseerd kan worden.

Besluit: de werkgroep staat positief tegenover dit voorstel en wordt dan ook als één van de (aparte) thema's opgepakt. Hierin wordt bepaald hoe dit vormgegeven kan worden.

4. Afsluiting

Besproken: welke thema's nu als apart behandeld kunnen worden: i) Toetsingskader, ii) Toezicht, iii) Centrale BIV-classificatie met Referentie Architectuur en iv) 'Uitbesteden van maatregelen en controle hierop'.
Besluit: voor het meewerken van de thema's wordt een poll uitgezet. Vervolgens wordt per thema een kerngroep gepland, waarvoor een datumprikker wordt uitgezet. Een volgende werkgroep bijeenkomst zal ongeveer na 2 maanden weer plaatsvinden; hier wordt i.v.m. de grootte van de werkgroep ook een datumprikker voor uitgezet.