Memo

Aan	Standaardisatieraad
Van	Dirk Linden
Datum	9 mei 2016
Onderwerp	Informatiebeveiliging binnen Edustandaard

1. Inleiding

Tijdens de standaardisatieraad van 5 november 2015 werd een presentatie gehouden over Informatiebeveiliging binnen Edustandaard. Hierin werden de verschillende initiatieven in kaart gebracht die in het onderwijs worden ontplooid om informatiebeveiliging goed te regelen. Naar aanleiding van deze presentatie kwam een aantal vragen naar boven waar deze notitie een antwoord op tracht te geven.

De eerste vraag ging over de relatie tussen informatiebeveiliging en privacy. Het zijn sterk gerelateerde thema's die soms los maar vaak ook in samenhang met elkaar moeten worden opgepakt. Hoe wordt deze samenhang geborgd?

De tweede vraag ging over afbakening van de activiteiten van edustandaard. Welke rol ligt bij edustandaard en welke rol ligt bij andere partijen?

2. Informatiebeveiliging en Privacy

Het thema privacy kwam in de presentatie van 5 november niet expliciet aan bod, toch is privacy nadrukkelijk in beeld. Dit blijkt onder ander uit het feit dat het ROSA katern 'Privacy en Beveiliging' heet. Omwille van eenduidigheid zou het overigens helpen als dit vanaf nu 'Katern IBP' wordt genoemd. In dit memo zal deze naam vast worden gebruikt.
De thema's informatiebeveiliging en privacy zijn sterk verbonden maar toch verschillend. Privacy is verankerd in de wet en het heeft dus geen zin om daar binnen het onderwijs een eigen standaard voor te ontwikkelen. De implementatie van privacy is wel iets waar ketenafspraken over kunnen worden gemaakt. Dat wordt ook gedaan binnen Edu-K, middels het privacyconvenant. Het privacyconvenant is in een publiek-private samenwerking tot stand gekomen.
Privacy geeft de noodzaak om informatiebeveiligingsmaatregelen toe te passen. Welke maatregelen worden ingezet, en met welk volwassenheidsniveau, is ook iets waar ketenafspraken over gemaakt kunnen worden. Door ondertekenen van het privacyconvenant verplichten leveranciers zich nu ook om passende maatregelen te nemen. Daarmee is het voor onderwijsinstellingen alleen niet duidelijk wanneer het goed genoeg is. En voor leveranciers is het een probleem dat klanten hun diensten op basis van verschillende normenkaders willen beoordelen. Met de Edu-K werkgroep privacy is hierover ook al gesproken. Het is de intentie om hiervoor het certificeringsschema te gebruiken wat in ontwikkeling is binnen edustandaard. Door opname in de model bewerkersovereenkomst (te weten: de bijlage Organisatorische en technische beveiligingsmaatregelen) wordt het certificeringschema dan aan het privacyconvenant verbonden.

De vertaling van privacyprincipes naar de onderwijspraktijk is ook iets waar in het kader van edustandaard afspraken over gemaakt kunnen worden. De principes zijn al opgenomen in het katern IBP, terwijl een nadere uitwerking daarvan in architectuurrichtlijnen nog moet plaatsvinden. Voorbeeld van richtlijnen die ontwikkeld kunnen worden zijn ontwikkel richtlijnen voor 'Privacy by Design'.

Voorstellen:
- Naamgeving: Katern 'Privacy en Beveiliging' wordt Katern IBP
- Edustandaard werkgroep Informatiebeveiliging wordt werkgroep IBP en krijgt als opdracht mee om architectuur principes van de principes uit het katern IBP. Principes al benoemd nu architectuurrichtlijnen.

Memo

Beknopt overzicht Privacyafspraken:

Alle afspraken in lijn met de principes uit het ROSA katern IBP.

	PO-VO	MBO [1)]	HO
Instelling	Privacyconvenant **[Edu-K]**	Framework IBP: **[Taskforce IBP]** * Compliancekader privacy (IBPDOC 2b) * Toetsingskader privacy (IBPDOC7) ** eventueel nader te bepalen toetsingskader voor leveranciers* (vgl. privacyconvenant)	Juridisch normenkader cloudservices hoger onderwijs **[Juridische commissie Surfnet]**
Afdwingbaarheid bij Leveranciers	*Model bewerkersovereenkomst* met bijlages: A) Privacybijsluiter B) Technische en organisatorisch beveiligingsmaatregelen (met daarin de verplichting zich te conformeren aan het Certificeringsschema)	*Voorlopig:* ** leermiddelen:* bewerkersovereenkomst (gebaseerd op model po/vo) ** Overig zoals MS, Google:* SURF-modelbewerkersovereenkomst	SURF-modelbewerkersovereenkomst
Aantoonbaar compliant	Verklaring ondertekening privacyconvenant (centraal register bij privacyconvenant.nl)	Individuele ondertekening bewerkersovereenkomst	Individuele ondertekening bewerkersovereenkomst
Toetsbaar	*In onderzoek:* Toetsing bewerkersovereenkomsten Interne audits o.b.v. Toetsingskader CS (in 2016)		Externe audit o.b.v. TPM verklaring

- 1): in het mbo vindt er op dit moment een inventarisatie plaats of het mogelijk en wenselijk is dat mbo-instellingen voor de aanschaf van digitale leermiddelen aansluiting zoeken bij het privacyconvenant (po/vo). Voorlopig is er een aangepaste model bewerkersovereenkomst gebaseerd op de model bewerkersovereenkomst po/vo.
- In het mbo wordt er door instelling gebruik gemaakt van het Compliancekader privacy (IBPDOC2b) en Toetsingskader privacy (IBPDOC7) dat gebaseerd is op de privacyprincipes zoals opgenomen in de ROSA katern ‘Privacy en informatiebeveiliging’.

Memo

3. De rol van Edustandaard bij informatiebeveiliging

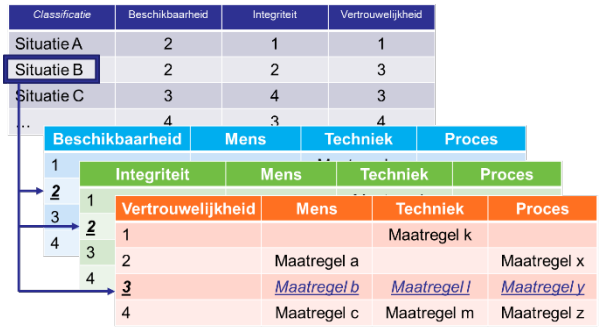
In het onderwijs zijn momenteel veel plekken waar afspraken rondom informatiebeveiliging worden gemaakt. Er is behoefte aan een overzicht om voor alle belanghebbenden helder te maken welke afspraken waar gemaakt worden.

De principes die door alle partijen worden gehanteerd zijn ondergebracht in de ROSA in het Katern IBP. De ROSA en daarmee het katern IBP worden beheerd door Edustandaard. Het belangrijkste uitgangspunt in dit katern is de, door de informatiekamer bekrachtigde, afspraak om de ISO27001/27002 standaard als basis voor alle afspraken te hanteren. Alle afspraken in onderstaand overzicht zijn dan ook gerelateerd aan deze internationale norm. De instellingsnormenkaders zijn sectorspecifiek ontwikkeld, om goed aan te sluiten bij de behoefte van de sector. De normenkaders zijn wel op elkaar afgestemd. Zo is het MBO kader afgeleid van het HO normenkader en wordt PO/VO kader afgestemd op het MBO kader.

Beknopt overzicht informatiebeveiligingsnormen onderwijssectoren
Alle afspraken in lijn met de principes uit het ROSA katern IBP

	PO-VO	MBO	HO
Instelling	In ontwikkeling – **[Kennisnet in opdracht van PO en VO-raad]**	Normenkader MBO – **[Taskforce IBP MBO]**	Normenkader Informatiebeveiliging HO 2015 - **[SURFnet]**
	X	Peer audits o.b.v. Toetsingskader MBO	Peer audits o.b.v. Toetsingskader HO
Leveranciers	Certificeringsschema bestaande uit: • Normenkader • Toetsingskader (TKI) • *Toezichtskader* (voorlopig interne audits) **[Edustandaard werkgroep IBP]**		Juridisch Normenkader Cloudservices – **[Juridische commissie Surfnet]**
	Interne audits o.b.v. Toetsingskader CS (in 2016)		Externe audit o.b.v. TPM verklaring

Het Certificeringsschema
Uit bovenstaand schema vallen de afspraken uit het certificeringschema onder verantwoordelijkheid van Edustandaard. Het schema is gebaseerd op het door ROSA voorgeschreven ISO27002 normenkader. Deze ISO normen zijn alleen nogal hoog over. Het toetsingskader van het certificeringsschema biedt daarom een vertaling naar praktische en toetsbare maatregelen. Het toetsingskader bestaat uit een instrument om voor classificatie en risicoanalyse. Dit instrument levert de zogenaamde BIV classificatie, waarmee het belang van Beschikbaarheid, Integriteit en Vertrouwelijkheid wordt uitgedrukt. Op basis van deze classificatie kunnen in het toetsingskader de betreffende maatregelen worden gevonden. Het toetsingskader bevat maatregelen waarover publieke en private partijen het eens zijn geworden dat deze de betreffende risico's voldoende afdekken. Dit geeft zowel onderwijsinstellingen als leveranciers helderheid welke maatregelen bij welke risico's geïmplementeerd moeten zijn. Het certificeringsschema wordt in eerste instantie ontwikkeld voor toepassingen in de educatieve en administratieve keten in het PO/VO, maar is generiek inzetbaar. Het maken van afspraken over implementatie van het certificeringsschema in de leermiddelenketen vindt plaats binnen Edu-K. De discussie over toezicht wordt ook daar gevoerd. Zodra daar helderheid over is en er een toezichtkader kan worden opgesteld zal dit ook onderdeel worden van het certificeringsschema.



Memo

Certificeringsschema: Wat gebeurt waar?

Prinicpes (waarom)	Afspraken (wat)	Implementatie (hoe)
ROSA	Certificeringsschema	Implementatieplan
Edustandaard	**Edustandaard**	**Edu-K**
Standaardisatieraad ▪ Bestuurlijke vaststelling door o.a. sectorraden en brancheorganisaties	**Standaardisatieraad** ▪ Bestuurlijke vaststelling door o.a. sectorraden en brancheorganisaties	**Edu-K** ▪ Vaststellen implementatiekaders ▪ Vaststellen toezicht
Architectuurraad ▪ Samenhang met architectuur ▪ Samenhang met andere processen (vb Edukoppeling, OSO)	**Werkgroep** ▪ Ontwikkeling en beheer certificeringsschema	**Tactisch overleg Continuïteit en beveiliging** ▪ Implementeren van certificeringsschema (obv risicoanalyse) ▪ Afspraken over toezicht

Informatiebeveiliging gerelateerde thema's

Naast de thema's die direct over informatiebeveiliging gaan zijn er ook thema's die er nauw aan verwant zijn. De IAA architectuur bevat afspraken en maatregelen om informatiebeveiliging en privacy in de keten te borgen.

De Edukoppeling transactiestandaard wordt gebruikt voor de communicatie tussen systemen (M2M) ten behoeve van vertrouwelijke gegevensuitwisseling. Daarmee is de koppeling tussen systemen veilig geregeld. Om te zorgen dat de gekoppelde systemen zelf ook goed zijn beveiligd wordt het certificeringsschema gebruikt.