edustandaard

Voor:	Standaardisatieraad, Edustandaard
Van:	Dirk Linden (Voorzitter Werkgroep IBP)
Datum	10-7-2017
Betreft	Vragen omtrent implementatie van het certificeringsschema

Zoals blijkt uit de diverse beoordelingen is inhoudelijk alles rondom het certificeringsschema in orde. Toch leven er in de keten nog veel vragen rondom het schema en het gebruik hiervan. Deze vragen of soms zelfs zorgen zouden aanleiding kunnen geven om CS v.2017 nog niet in beheer te nemen door Edustandaard. Als werkgroep IBP zouden we dat erg jammer vinden omdat inbeheername nu de volgende stap naar volwassenheid het schema moet vormen. De vragen rondom implementatie hebben overigens onze nadrukkelijk aandacht. In de in de vergadering van 27 juni hebben we deze uitvoerig besproken en van onze reactie voorzien. Als onderdeel van het implementatieplan binnen Edu-K, zal ook hier ook nadrukkelijk aandacht aan worden besteed. De komende weken zullen worden gebruikt om eventuele verdere vragen of zorgen rondom implementatie te inventariseren. Om een indruk te geven hierbij vast een overzicht van de vragen die ons op dit moment bekend zijn met daarbij onze reactie.

Vraag 1: *"Zijn de eisen van CS v.2017 niet te zwaar, in ieder geval voor een aantal toepassingen?"*

Reactie: CS v.2017 biedt voldoende mogelijkheden om de maatregelen goed aan te laten sluiten bij de eisen van de ICT-toepassing. Niet voor elk product gelden zware eisen. Het belangrijkste instrument voor het realiseren van dit maatwerk is het classificatiehulpmiddel van het CS v.2017. Met dit hulpmiddel worden de eisen aan Beschikbaarheid, Integriteit, Vertrouwelijkheid (BIV) van de toepassing bepaald. Op basis van deze 'BIV-classificatie' worden de benodigde maatregelen gevonden in het toetsingskader.

Vraag 2: *"Ontwikkeling van dreigingen op het gebeid van beveiliging gaat snel waardoor maatregelen snel verouderen. Voor onze toepassing hebben we een betere oplossing om hetzelfde te bereiken. Dwingt CS v.2017 ons om de 'oude' maatregel te implementeren?"*

Reactie: CS v.2017 is een 'pas toe of leg uit' standaard. Het rapportageformat van het CS v.2017 biedt voldoende ruimte voor toelichting. Het is dus altijd mogelijk om uit te leggen dat een andere oplossing is gekozen om hetzelfde te bereiken. De werkgroep IBP moedigt alle partijen aan om ideeën voor een betere invulling van maatregelen te delen. Met deze inzichten kan het toetsingskader verder worden verbeterd. Dit heeft al goed gewerkt naar aanleiding van reeds uitgevoerde pilots. In het Edu-K implementatieplan voor CS v.2017 is daar onder het kopje 'praktijkervaring' ook nadrukkelijk aandacht aan besteed. Met de standaardisatieraad en de werkgroep IBP is geregeld dat nieuwe inzichten op korte termijn in het certificeringsschema kunnen worden opgenomen.

Vraag 3: *"Is het realistisch om deze eisen op te leggen aan kleinere leveranciers. Worden kleine leveranciers niet zo buiten spel gezet?"*

Reactie: Gevoelige data zoals zorg en persoonsgegevens vragen passende maatregelen los van de omvang van de leverancier. Er is op basis van CS v.2017 een pilot gedaan bij een kleine leverancier (4 medewerkers). Deze leverancier gaf aan dat het CS hen juist had geholpen om zicht te krijgen op de nodige maatregelen. Het CS v.2017 bleek een bron van informatiebeveiligingskennis die voor hen anders veel moeite had gekost om te verkrijgen. Voldoen aan de maatregelen door kleine leveranciers is goed mogelijk doordiensten (bijv. hosting) af te nemen van leveranciers die deze maatregelen hebben geïmplementeerd. In het implementatieplan is ook rekening gehouden met beproeven van het schema door kleinere partijen. Eventueel benodigde aanpassingen kunnen nog worden doorgevoerd.

Vraag 4: *"Wij hebben al (of zijn bezig met) een ISO 27001 certificering. Waarom zouden wij dan het certificeringsschema nog nodig hebben?"*
Reactie: Dit wordt uitgebreid toegelicht in de algemene beschrijving van het CS v.2017 onder 'Hoofdstuk 2.2 Relatie tussen het certificeringsschema en andere normenkaders' Het korte antwoord is dat een organisatie die conform ISO-27001 werkt het proces document van CS v.2017 niet nodig heeft, beiden geven invulling aan een continue verbetercyclus. De maatregelen uit het CS v.2017 moeten wel worden toegepast, het is daarbij aannemelijk dat veel van de maatregelen op basis van de ISO-maatregelen al ruim voldoende zijn ingevuld. Het CS v.2017 is ook van

belang omdat een uniform rapportageformat biedt, waarmee communicatie en transparantie in de onderwijsketen worden bevorderd.

Vraag 5: *“Als het certificeringsschema is vastgesteld gaan scholen waarschijnlijk in hun aanbestedingseisen opnemen. Hoe moeten we er mee omgaan als ze daarbij te hoge eisen stellen?”*

Reactie: Het certificeringsschema biedt juist transparantie over wat onder welk niveau wordt verstaan. En welk niveau voldoende is voor welke soort gegevens of toepassing. In de praktijk verstaat iedereen nu wat anders onder ‘laag’, 'midden' of ‘hoog’. In CS v.2017 zijn hiervoor definities opgenomen voor Beschikbaarheid, Integriteit en vertrouwelijkheid. Ervaring in het hoger onderwijs leert dat het zich in de praktijk uitmiddelt, zeker omdat de classificatie reeds op de onderwijsprocessen plaatsvindt. Ervaring in het MBO laat hetzelfde zien.
Als onderdeel van het implementatieplan zal ook communicatie richting scholen worden opgenomen zodat scholen weten wat ‘voldoen aan het certificeringsschema’ inhoud en hoe zij dat op een passende wijze in hun inkooptrajecten kunnen in zetten

Vraag 6: *‘Het certificeringsschema is bedoeld voor alle leveranciers in de onderwijsketen. De communicatie loopt via de branchevertegenwoordigers. Als andere leveranciers er niet aan hoeven voldoen levert dat oneerlijke concurrentie. Hoe bereiken we andere leveranciers en zorgen dat zij er ook aan voldoen?’*

Reactie: Door er mee te beginnen en het goede voorbeeld te geven. Scholen gaan ernaar vragen en stellen daar mee de norm.