edustandaard

Memo

Voor:	Standaardisatieraad, Edustandaard
Van:	Elise Lustenhouwer, Bureau Edustandaard
Datum	22 maart 2018
Betreft	Update Certificeringsschema informatiebeveiliging en privacy ROSA 2018

1. Samenvatting

Na in beheer name in 2017 is vanuit de praktijk en de werkgroep IBP terugkoppeling gekomen ter verheldering, verbetering en ondersteuning van de implementatie van het Certificeringsschema. Ook zijn er voortschrijdende inzichten in relatie tot risicobeelden en de stand van de techniek. Deze terugkoppeling en voortschrijdende inzichten zijn gedurende het afgelopen jaar door de werkgroep IBP verwerkt in een nieuwe tussentijdse versie.

De afspraak is een gezamenlijk opgesteld ‘normenkader’, een baseline van maatregelen op het gebied van informatiebeveiliging voor organisaties die diensten – ondersteund door ict-toepassingen – leveren in de onderwijsketen. Op basis van een voorgeschreven werkwijze bepaalt een leverancier een beveiligingsniveau. Aan dit beveiligingsniveau zijn specifieke maatregelen gekoppeld die gelden als een baseline waaraan de leverancier dan moet voldoen (comply) of een beargumenteerde afwijking voor moet geven (explain).

2. Doel en doelgroep

Het doel van het Certificeringsschema is drieledig:

- Specificatie van een baseline van maatregelen op het gebied van informatiebeveiliging en privacy;
- Transparantie bieden over welke ICT-toepassingen voldoen aan deze baseline;
- Het creëren van een solide basisniveau van informatiebeveiliging voor alle geleverde ict-toepassingen in de onderwijsketen.

Als het Certificeringsschema niet geaccepteerd wordt door het veld, dan komen scholen met verschillende normenkaders waaraan organisaties die ict-diensten leveren getoetst gaan worden, wat de auditdruk vergroot. Organisaties die ict-diensten leveren worden niet expliciet getoetst op een breed gedragen normenkader in de onderwijssector. Dit leidt mogelijk tot een onvoldoende niveau van informatiebeveiliging, willekeur en geen transparantie.

Het is belangrijk om jaarlijks een update uit te brengen om voortschrijdende inzichten en actuele risico’s te kunnen verwerken in maatregelen. De goedkeuring van een nieuwe versie door de architectuur- en standaardisatieraad draagt bij aan de acceptatie in de onderwijsketen.

3. Advies van bureau Edustandaard

Het bureau geeft het volgende advies: “Goed” om de volgende redenen:

- Het betreft een update van de afspraak die reeds in beheer is genomen. Bij indiening van de afspraak vorig jaar, was het advies “Voldoende met aandachtspunten.” Deze aandachtspunten zijn inmiddels opgepakt of onderbouwd.
- Het kortcyclisch doorontwikkelen van de afspraak bevalt goed en sluit goed aan op de behoefte om gebruik te kunnen maken van de nieuwste ontwikkelingen op het gebied van privacy en beveiliging.
- Omwille van de adoptie van het Certificeringsschema is ervoor gekozen om de focus op de technische maatregelen te houden en de scope niet uit te breiden met ‘mens’ en ‘proces’. Er is daarom voor gekozen om de roadmap hierin niet te volgen.

4. Advies Architectuurraad

De update van het Certificeringsschema betreft een kleine update die op het gebied van architectuur geen wijzigingen met zich mee bracht. Om die reden is er geen nieuwe architectuurscan uitgevoerd. Bij de in beheer name vorig jaar is er een architectuurscan uitgevoerd. De punten die hieruit naar voren kwamen, zijn opgepakt of onderbouwd. Belangrijke opmerkingen hierbij zijn:

- Het certificeringsschema is geen uitwisselingsstandaard en bevindt zich daarom niet in een architectuurketen. Wel is het Certificeringsschema breed toepasbaar omdat elke ict-toepassing gecertificeerd kan worden op het gebied van beveiliging en privacy.
- Vanuit Edukoppeling wordt verwezen naar het Certificeringsschema. Met de werkgroep Edukoppeling is afstemming geweest over de nieuwe aanpassingen van het Certificeringsschema en dit levert geen problemen op voor Edukoppeling.
- Het Certificeringsschema moet gezien worden als een *baseline* voor beveiligingsmaatregelen. Er zijn altijd nog aanvullende beveiligingsmaatregelen te nemen over een ict-toepassing door een organisatie.

5. Roadmap

Het beheer van de afspraak is als volgt vormgegeven:

- De werkgroep IBP werkt met *Requests for Change* en past op basis daarvan de afspraak aan. Vanwege de snelle ontwikkelingen op het gebied van privacy en beveiliging is er behoefte om meerdere malen per jaar een nieuwe versie beschikbaar te hebben. Deze wordt op Edustandaard gepubliceerd. Eenmaal per jaar wordt de afspraak formeel aangeboden aan de Standaardisatieraad om deze formeel te bevestigen.

6. Gevraagd besluit

De leden van de Standaardisatieraad wordt gevraagd om, gelet op bovenstaande overwegingen, in te stemmen met de in beheer name van de afspraak *Certificeringsschema informatiebeveiliging en privacy ROSA*, versie 2018.