Verslag werkgroepbijeenkomst Certificeringsschema ROSA

Datum:14 april 2016
Aanwezig: Herrie Abbink (Educus), Dirk Linden (Kennisnet), Axel Eissens (Kennisnet), Twan van der Meer (Cap Gemini), Ad van Etten (DUO), Oscar ter Meer (OCW), Paul Arnold (Van Dijk), Rob van der Staaij (GEU, Thieme Meulenhoff)
Afwezig: Alf Moens (Surf), Job Vos (Kennisnet), Ludo Cuijpers (MBO)

- **Opening**
- **Introductie en voorstelronde**
- **Vaststellen agenda**
    - OK bevonden.

- **Mededelingen**
    - De overige aanwezigen zijn verhinderd door onder andere congressen: Ludo Cuijpers (MBO), Job Vos (Kennisnet) en Alf Moens (Surf). Bote Folkertsma (Studielink) lijkt niet meer bereikbaar.

- **Certificeringsschema**
    - Korte terugblik totstandkoming Certificeringsschema:
      Er was een constatering tijdens de invoering van Edukoppeling, waarbij de vraag openbleef wat er aan het einde van de verbinding nog verder moet gebeuren. Daaruit is een eerste versie van het Certificeringsschema gemaakt op basis van de Cloud Control Matrix. Sindsdien is er een behoefte geweest aan een breder schema, en vanuit ROSA aan een op ISO 27002 gebaseerd schema. ISO 27002 was alsnog te ruim om specifiek te kunnen toetsen op eisen, waardoor de opdracht was om aan een invoeringsstrategie te werken. Daar is in het afgelopen half jaar gewerkt. Er was de wens om eerder bij elkaar te komen, maar om de gang erin te houden en om een praktijktoets uit te voeren, is dat vandaag. Er wordt een 1.9 versie voorgelegd vandaag, wat betekent dat we als werkgroep alsnog bij kunnen sturen.

    - Presentatie Twan van der Meer over de ontwikkelde instrumenten (Dataclassificatie en Toetsingskader Informatiebeveiliging) en de ervaringen uit de pilot.

    - Verschillende discussiepunten komen aan bod vanuit de werkgroepleden. Antwoorden moeten gelezen worden als intentie. Besluiten zijn (nog) niet genomen.
        - ➔ Komt er ook een verankering zoals met het privacyconvenant? Ja, de intentie is om het Certificeringsschema op te nemen als eis of invulling van de IB-eis in het privacyconvenant.
        - ➔ Wie is in de sheets de business? Een niet technisch persoon die juist op de functionaliteit zit. Het gaat om bewust maken van veiligheid faciliteren dmv bewustwording.
        - ➔ Gaat dit ook voor mbo gelden? Uiteindelijk wel, maar het is onderdeel invoeringsstrategie om eerst po/vo te voorzien.

- ➔ Scholen moeten dus ook maatregelen moeten nemen. Dat wordt door iedereen onderkend. Het Certificeringsschema richt zich op leveranciers, de effecten/impact/maatregelen die naar aanleiding daarvan bij onderwijsinstellingen komen worden o.a. in Edu-K besproken.
- ➔ Beschikbaarheidseisen kunnen veranderlijk zijn in de tijd. Het proces faciliteert juist de discussie met techniek en business en daarmee kun je als resultaat een balans slaan tussen kosten/investering en de eisen (bijvoorbeeld dat je maatregelen tijdelijk inzet, of altijd de hoogste beschikbaarheid inregelt tegen hogere kosten).
- ➔ Alle aangesloten partijen zijn belangrijk, hoe kijken we daar tegenaan? Het Certificeringsschema moet overal op van toepassing zijn, maar richt zich in de toepassing op een enkele leverancier. Een oplossing of een invulling van dit vraagstuk blijft nog in het midden hangen.
- ➔ Denk na over de haalbaarheid van eisen (bijvoorbeeld in relatie tot kleine partijen en nieuwe toetreders).
    - Opmerking hierbij vanuit Cap Gemini is dat de kosten vooral gaan zitten in de beschikbaarheid, welke je kan relateren aan de eisen van klanten die je in de SLA opneemt. Op het gebied van vertrouwelijkheid zitten de kosten niet.
- ➔ Denk ook na over de specificiteit van de eisen en het waar mogelijk aansluiten op bestaande kaders/specificaties.
- ➔ Hoe ga je om met nieuwe versus bestaande systemen? Certificeringsschema moet een basis zijn voor nieuwe systemen, bestaande systemen veiliger krijgen is een kwestie van kosten/prioriteit.
- ➔ Het is belangrijk dat bedrijven naar de software (laten) kijken, dat deze wordt getoetst. Deze maatregelen staan in het toetsingskader en de werkgroepleden kijken of deze eisen inderdaad op het juiste abstractieniveau gesteld worden.

- Reactie werkgroepleden op huidige opzet:
    - ➔ Hele prettige en duidelijke kapstok.
    - ➔ Prettige ontkoppeling tussen business (doelen) en maatregelen.
    - ➔ Goed om de resultaten te zien. Prioriteren van resultaten is ook belangrijk.
    - ➔ Awareness (door bijvoorbeeld phishing campaigns) is ook belangrijk om op te nemen.

- **Bespreken notitie certificeringsschema:**
    - Gaat dit werken op deze wijze? Werkgroepleden antwoorden:
        - ➔ Het is een kwestie discipline, het moet wel gedaan worden. Kennisnet neemt dit mee naar Edu-K.
        - ➔ Onderwijsinstellingen moeten dit willen. vo-raad moeten zich er comfortabel bij voelen (en dus zelf ook actie ondernemen). Kennisnet neemt dit mee naar Edu-K.

➔ Profileer dat dit hét certificeringsschema is waar het hele onderwijs mee gaat werken.
➔ OCW onderschrijft dat creëren draagvlak noodzakelijk is.

- **Vaststellen beslissing op voorstellen**
  - Zie vervolgafspraken.

- **Samenstelling en opzet volgende werkgroepbijeenkomst**
  - Huidige samenstelling blijft.

- **Vervolgafspraken**
  - Eerst de komende zes weken samenwerken aan de inhoud
  - Volgende werkgroepbijeenkomst over zes weken
    ➔ Dan de vervolgstappen uit de notitie verder vormgeven/besluiten
  - Kennisnet doet een voorstel voor een reviewprocedure

- **Bijlagen**
  - Presentatie Certificeringsschema proces
  - Classificatietool
  - Toetsingskader Informatiebeveiliging

- **Vragen om in het achterhoofd te houden tijdens de review**
  - Zijn de eisen niet te hard/professioneel? Let wel, het moet een baseline zijn die nieuwe toetreders en kleinere bedrijven het werk niet onmogelijk maakt.
  - Dekt het beschreven proces alles af?
  - Kun je bij eisen aansluiten op bestaande initiatieven/standaarden in plaats van een té specifieke eis in het toetsingskader? Bijvoorbeeld in plaats van syntax controle -> toetsing aan de OWASP Top 10/NCSC richtlijnen voor webapplicaties/CIP richtlijnen voor secure software development.
  - Wat wordt waar geregeld/geëist? Bijvoorbeeld:
    ➔ School eist Privacyconvenant
      - Daarin staat het Certificeringsschema
    ➔ In het Certificeringsschema staat dat de leverancier aan bepaalde eisen moet voldoen.
    ➔ Hierdoor hoeft een school alleen te checken of het Certificeringsschema is getoetst, maar niet de diepte in hoeft op bijvoorbeeld softwareontwikkeling.