Verslag Edustandaard werkgroep IBP

Datum: 27 juni 2017
Aanwezig: KBb-e, VDOD, SURF, GEU, OCW, Kennisnet
Afwezig: DUO

Opening

Mededelingen

Vorige notulen

- Notulen januari 2017 worden niet besproken en stilzwijgend goedgekeurd wegens lange periode sinds die bijeenkomst

Terugkoppeling uit het veld

- Er is op basis van de terugkoppeling door Kennisnet gewerkt aan een nieuwe versie van de documentatieset ten behoeve van de indiening bij Edustandaard.
- De Edustandaard website is up-to-date gebracht. De werkgroep loopt door de gewijzigde pagina heen en noteert op- en aanmerkingen.
- Voor de vaststelling/inbeheername Edustandaard certificeringsschema wil de voorzitters graag de veelgestelde vragen/geuitte zorgen bespreken:
    - Is het certificeringsschema wel geschikt voor kleine partijen?
        - Een pilot bij een kleine leverancier heeft uitgewezen dat het juist (kleine) partijen verder kan helpen om concrete maatregelen te nemen. Een tussenoplossing die we in de praktijk tegenkomen is dat een aantal maatregelen reeds door de achterliggende leveranciers van hosting worden getroffen.
        - SURF: in het hoger onderwijs is modus gevonden waarbij kleine leveranciers met stapjes erdoorheen kunnen komen.
        - KBb-e: wij merken dat het vooral de onbekendheid ermee een rol speelt. SURF: en hoge kosten bij externe audits.
    - Zijn sommige maatregelen te streng?
        - Dit hangt samen met te zware classficaite maar regelmatige feedback en verbetering moeten dit ondervangen
    - Zijn sommige maatregelen te oud?
        - Bijvoorbeeld hot stand by ~> dit is illustratief want in de cloud heb je infrastructuur waar dit niet voor relevant is (door bijvoorbeeld automatisch schalen).
        - Ook hier helpt regelmatige feedback met liever een suggestie dan louter commentaar op de maatregel.
    - Worden maatregelen niet te hard afgedwongen?
        - Je wordt er zelf ook mee geholpen (bijv hacking en ddos oplossen)
    - Kunnen scholen (middels aanbestedingen) geen 3-3-3 eisen?
        - Een uitleg over wat ‘voldoen aan het certificeringsschema’ betekent moet transparantie bieden, waarbij het niet de bedoeling is dat unilateraal vanuit de klant een classificatie wordt gesteld.
        - Het certificeringsschema streeft transparantie na. Nu spreken we een gemeenschappelijke taal, iedereen weet bijvoorbeeld wat er nu onder integriteit midden wordt verstaan.
        - SURF: in het HO merken we dat het zich uitmiddeld, zeker ook omdat de classificatie reeds op de onderwijsprocessen plaatsvindt (zo ook al in het mbo)
    - Er zijn al normenkaders, waarom is er nu een nieuwe?
        - Dit wordt als het goed is in het algemene verhaal goed toegelicht.
    - Zijn alle partijen nu nog goed aangesloten?
        - KBb-e suggereert een communicatieplan verwijzend naar het implementatieprogramma zeker richting de GEU, VDOD, et cetera. Zo kan niemand zeggen dat ze het niet wisten.
        - De uitdaging dat niet alle partijen bij branches zijn aangesloten wordt later aangepakt.

De voorzitter vraagt of iedereen akkoord is met de indiening in de huidige vorm:

- VDOD: Akkoord, erg benieuwd naar praktijk
- GEU: Akkoord
- KBb-e: Akkoord, mits overname opmerkingen in nabije toekomst
- SURF: Akkoord, mits overname opmerkingen in nabije toekomst. Tevens erg benieuwd naar implementatie in de praktijk. Een changelog is vanaf nu erg belangrijk voor communicatie en nuttig voor hertoetsing in de toekomst.
- LC: Akkoord, met de suggestie om de namen op te nemen voor werkgroepleden om de acceptatie in het veld te ondersteunen

- Kennisnet: Akkoord
- OCW: Akkoord
- DUO: Akkoord (per mail)

Roadmap
- RFC 1 (laag/midden/hoog)
    - Goedgekeurd
    - Aanvullende discussie:
        - SURF: kunnen we een opmerking in procesdocument maken over dat het uitgangsniveau midden is? Dit wordt overgenomen in de laatste versie.
        - KBb-e/SURF: in het classificatiemiddel staat identiteitsfraude bij integriteit, maar dit hoort eigenlijk bij vertrouwelijkheid. Het voorstel is om dit te wijzigen in 'heeft financiele gevolgen of ernstige/blijvende schade'. Dit wordt overgenomen in de laatste versie.
- RFC 2 (fysieke toegang)
    - Goedgekeurd
- RFC 3 (vernietiging van apparatuur)
    - Goedgekeurd, aangevuld met een variant "vernietiging van de datadrager")
- RFC 4 (loggingsmaatregelen)
    - Goedgekeurd, met de volgende aanpassing:
        - "ter illustratie" weghalen want dubbelop

Rondvraag

Afsluiting
- De volgende vergadering:
    - Datum: 3 oktober
    - Tijd: 15:00 – 17:00
    - Locatie: Kennisnet in Zoetermeer
    - Suggesties voor agendapunten:
        - Komt er een certificeringsschema voor scholen of aanpak IBP? En hoe kunnen we dat 'harder maken'?
        - ROSA-scan

Actiepunten
- AP Kennisnet: oude notulen anonimiseren en op website Edustandaard
- AP SURF: opsturen tekstvoorstel over 'andere route HO'
- AP Kennisnet: RFC format voor op edustandaard website onderzoeken
- AP Kennisnet: indienen RFC irt richtlijnen Autoriteit Persoonsgegevens voor loggingsmaatregelen