NORA Sessie 5

29 mei 2013 in Amersfoort

Agenda en een samenvatting

Jaap van der Veen

Agenda 29-5-2013

1. Welkom
2. Presentatie Eric Brouwer en Joris Dirks over Kennismodel NORA-Wiki en hoe we onze informatie daarin kunnen plaatsen
3. Overzicht van best practices + toelichting daarop van Jule Hintzbergen (KING) over patronen
4. Vervolgafspraken opstellen 'Operationele Baseline' als verzameling best practices. Wie kan tijd vrijmaken? Wanneer starten we? PvIB en BIR-OB patronen customizen zodat ze maximaal inzetbaar zijn.
5. Hulp aan gemeenten t.a.v. patronen en best practices

Resultaten sessie 5 29-5-2013

- **Het NORA kennismodel** is nog in ontwikkeling. De ophanging van de inhoud van het katern beveiliging is ingetekend. We moeten ervaren of dit de juiste ophanging is. Voor het **ontwerpkader** denken we na over een praktische ophanging van normen en patronen. Bijvoorbeeld met groeperende thema's van beheersmaatregelen, waar de IB functies onder vallen en de patronen met hun implementatierichtlijnen. In feite zou het een combinatie van het beste uit drie werelden moeten worden: die van de het bestaande NORA dossier "Normen IT-voorzieningen", het BIR-OB en de PvIB-patronen. Actie punt: Jaap, wie denkt er mee?

- **De NORA-3 afgeleide principes** (AP) vertonen qua abstractieniveau veel overeenkomsten met de IB-functies maar de volgende IB-functies worden in het geheel niet afgedekt door de afgeleide principes: *Vastleggen Gebeurtenissen, Controle, Alarmering en Rapportering en Systeemintegriteit.* Dit wordt meegenomen in de aanpassingenronde van de principes. Verder moet gekeken worden naar de SMART- formulering van de principes zelf (zie syntax) Actiepunt: Eric Brouwer.

- **Patronen gerelateerd aan BIG**; Presentatie van Jule Hintzbergen. Plaat gepresenteerd, met generieke patronen: NORA-breed en specifieke patronen per doelgroep. Dit lijkt een haalbaar voorstel, mits de specifieke patronen niet 'normerend' worden opgelegd voor de Gemeenten.

- **Verplichtend gebruik patronen?** De vraag was of het haalbaar is om voor de Gemeenten (maar ook andere organisaties) een 'verplicht' gebruik van patronen toe te passen zoals met succes bij DWR is toegepast. Geconcludeerd werd, dat dit verplichtende model niet gaat werken , omdat de systeemlandschappen van bestaande organisaties doorgaans veel van elkaar verschillen, waarvoor meerdere varianten per specifiek patroon nodig zouden zijn. Dat geld voor gemeenten die van schaalgrootte van elkaar verschillen, maar ook voor gemeenten met een overeenkomende schaalgrootte. Niet alleen de schaagrootte bepaalt immers de implementatie maar ook de geschiedenis van de bestaande systemen. Voor DWR werkten de verplichte patronen wel omdat DWR een beperkte scope had én een relatief korte lifecycle van systemen, waardoor legacy-afhankelijkheden van minder van invloed zijn op de realisatie.

Resultaten sessie 5 29-5-2013

- **Best Practices Gemeenten**. Als gevolg van toenemende awareness voor Informatiebeveiliging bij gemeentelijke bestuurders is de vraag naar practische oplossingen voor beveiliging groot. Naar verwachting zo groot, dat dit capaciteitsproblemen kan veroorzaken bij de ondersteunende instantie. Door KING is een gedocumenteerde uitvraag lijst van benodigde best practices opgesteld (Ondersteuningsvraag Operationele Baseline) en verspreid onder de expertgroepleden met de dringende vraag om hierop te reageren. De informatie zou al voor de zomer beschikbaar moeten zijn.
- **Hulp bij best Practices vanuit de expertgroep. (status 12 juni)** **Vanuit** de expertgroep zijn inmiddels enkele hulpmiddelen binnen gekomen en een verkennend gesprek op 11-6 heeft opgeleverd dat doelstellingen en implementatierichtlijnen van het HBB (Handboek Beveiliging Belastingdienst) als vertrekpunt bruikbaar lijken voor de gemeenten. In de samenwerking KING-expertgroep wordt dit verder uitgewerkt en uitgetest. De meeste onderwerpen in de uitvraaglijst zijn namelijk op tactisch niveau en organisatieonafhankelijk beschreven in deel B of C van het HBB.
- Met Jules de afspraak gemaakt dat we samen het BYOD patroon vorm gaan geven (Actie Jaap) Wie mee wil denken is van harte welkom!

Patronen, normen en hoe verder?

- PvIB: Beschouwingsmodellen en patronen.
  - Generieke oplossing voor generiek probleem
  - Generieke oplossing voor specifiek probleem
  - Beschrijvend; overzicht maatregelen in tabel
- BIR-OB:
  - 1e generatie opzet van patronen; (vanuit DWR)
  - Implementatierichtlijnen per patroon
- NORA ontwerpkader 2013 *om uit te werken*:

  Vanuit thema's en IB-functies naar beheers-maatregelen, patronen en implementatierichtlijn per patroon. Het idee is om in Wiki-vorm deze informatie bij elkaar te brengen….. Dus geen afzonderlijk normenkader meer, maar een geïntegreerde presentatievorm. Dat geeft de gebruiker meer houvast en overzicht over wat van belang is voor z'n ontwerp. De norm staat dan bij de toepassing. De auditor kan daarmee vervolgens gerichter toetsen op *opzet-bestaan en werking*

  De normen zijn al beschikbaar, evenals een uitgebreide set van patronen, procedures en overige best practices. De uitdaging voor de komende periode is het geheel te integreren tot een handzaam ontwerpkader en te borgen als katern.

Vergelijking IB-functies NORA dossier en Afgeleide Principes van NORA 3

- Beschikbaarheid

Continuiteitsvoorzieningen: De IT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid

  - AP35: de levering van de dienst is continu gewaarborgd
  - AP 36: wanneer de levering van een dienst mislukt, wordt de uitgangssituatie hersteld (=implementatie van AP35)

- Integriteit

Geprogrammeerde controles: In toepassingsprogrammatuur worden geprogrammeerde controles opgenomen, gericht op invoer, verwerking en uitvoer

Zonering: De technische infrastructuur is in zones ingedeeld om isolatie van onderdelen hiervan mogelijk te maken

Filtering: Op het koppelvlak tussen zones zijn filterfuncties gepositioneerd voor het gecontroleerd doorlaten van gegevens; niet-toegestane gegevens worden tegengehouden.

Onweerlegbaarheid berichtenuitwisseling Bij berichtenuitwisseling wordt de onweerlegbaarheid van verzenden en ontvangst geborgd.

  - AP38 De betrokken faciliteiten zijn gescheiden in zones
  - AP 39 De betrokken systemen controleren informatieobjecten op juistheid, volledigheid en tijdigheid
  - AP 40 De berichtenuitwisseling is onweerlegbaar

- Vertrouwelijkheid

Identificatie, Authenticatie en Autorisatie: Logische toegangscontrole vindt plaats voordat IT voorzieningen kunnen worden gebruikt

  - AP 37 Dienstverlender en afnemer zijn geauthenticeerd wanneer de diens een vertrouwelijk karakter heeft
  - AP38 De betrokken faciliteiten zijn gescheiden in zones

- Controleerbaarheid

Vastleggen gebeurtenissen: Handelingen en meldingen van de IT-voorzieningen worde vastgelegd in logging

Controleren, Alarmeren, In de technische infrastructuur zijn signaleringsfuncties werkzaam ter controle op het vastgestelde inrichtingsdocument

Systeem integriteit: In de technische infrastructuur zijn functies werkzaam die de systeem integriteit ondersteunen

Conclusie: de AP's lijken op de beveiligingsfuncties en zijn onvolledig in hun bereik…

Vergelijking in tabelvorm

Vertrouwelijkheid

Beschik baarheid

Integriteit

Controleer baarheid

Betrouwbaarheid

IB-functie	Doel van de beveiligingsfunctie	Is gebaseerd op
Continuïteit voorzieningen	De IT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid	NORA AP 35 en 36
Geprogrammeerde controles	In applicaties worden geprogrammeerde controles opgenomen, gericht op invoer, verwerking en uitvoer.	NORA AP 39
Zonering	De technische infrastructuur is in zones ingedeeld om isolatie van onderdelen hiervan mogelijk te maken.	NORA AP 38
Filtering	Op het koppelvlak tussen zones zijn filterfuncties gepositioneerd voor het gecontroleerd doorlaten van gegevens; niet-toegestane gegevens worden tegengehouden	NORA AP 38
Onweerlegbaarheid gegevensuitwisseling	Bij berichtuitwisseling wordt de onweerlegbaarheid van verzending en ontvangst geborgd.	NORA AP 40
Identificatie Authenticatie Autorisatie	Logische toegangscontrole vindt plaats voordat IT-voorzieningen kunnen worden gebruikt.	NORA AP 37
Vastleggen gebeurtenissen	Handelingen in en meldingen van IT-voorzieningen in de technische infrastructuur worden vastgelegd in logging.	ontbreekt in NORA
Controle Alarmering Rapportering	In de technische infrastructuur zijn signaleringsfuncties werkzaam ter controle op vastgestelde inrichtingsdocument (configuratiedossier).	ontbreekt in NORA
Systeemintegriteit	In de technische infrastructuur zijn functies werkzaam, die de systeemintegriteit ondersteunen.	ontbreekt in NORA

SMART syntax van principes

Principle ::= (P1, P2,…,Pn) Strength (Q1, Q2, …, Qn)