

## *Verlag Adviesraad IBD d.d. 22 november 2019*

### **1 Stand van zaken Agenda Digitale Veiligheid**

In de Digitale Agenda Veiligheid 2020-2024 staan de hoofdpunten voor de komende 4 jaar vanuit de VNG vermeld: weerbaarheid en herstelvermogen van gemeenten, maar ook breder (de overheid en samenwerkingsketens). De Agenda Digitale Veiligheid is aan de orde geweest in de commissies Informatiesamenleving, Bestuur en Veiligheid en de Cie. Dienstverleningszaken. Het resultaat: het document wordt gesteund en men heeft verzocht het stuk nader uit te werken. Het concept stuk is tevens gedeeld met het ministerie van BZK en nader besproken met de G5. Ook daar heeft men positief gereageerd. Afgesproken wordt dat er een laatste kritische redactieslag plaatsvindt, waarna het document het vervolgtraject in gaat. Voor dit vervolgtraject worden diverse opties besproken, waaronder het inzetten van de Taskforce Samen Organiseren en het College van Dienstverleningszaken om het onderwerp onder de aandacht te brengen.

### **2 Stand van zaken IBD**

De afgelopen maanden zijn veel meldingen gedaan van geslaagde phishing mail acties. De IBD heeft daarom nogmaals onder de aandacht gebracht dat naast bewustwording ook een aantal technische maatregelen van belang zijn, met 2 factor authenticatie als belangrijkste maatregel.

Na recente kwetsbaarheidmeldingen is gebleken dat niet altijd adequaat wordt gereageerd op een high-high melding (hoge kans, hoge impact). De IBD heeft het eigen protocol aangepast: bij high-high meldingen die echt grote risico's met zich meebrengen wordt ook de sms-dienst ingezet. Dit moet uiteraard spaarzaam en bedachtzaam gebeuren. Het is van groot belang dat gemeenten adequaat reageren op dit soort meldingen, dit geldt zeker ook voor meldingen die gemeenten straks vanuit het KPN SOC/GGI Veilig ontvangen. Het aanleveren van een actuele ICT-foto is erg belangrijk. In een netwerkinventarisatie (waarvan binnenkort de pilot van start gaat), kan de IBD gemeenten door middel van een scan helpen dit overzicht van hard- en software actueel te houden. Ook door het NCSC is aangegeven dat zij hiermee worstelen. Als serieuze adviezen niet worden opgevolgd, moet er geëscaleerd kunnen worden. Organisaties kunnen enorm kwetsbaar zijn, als er geen actie wordt ondernomen. Het NCSC en de IBD zoeken hierin de samenwerking en gaan het proces rondom kwetsbaarheidmeldingen scherper beschrijven: wie dient op welk moment geïnformeerd te worden, welke escalatiemogelijkheden zijn er et cetera.

De IBD zat in de jury van het evenement Hack The Hague, een goed initiatief vanuit de gemeente Den Haag dat jaarlijks wordt georganiseerd.

De VNG/IBD heeft in samenwerking met het Agentschap Telecom een game over Telekwetsbaarheid in beheer genomen. Deze game gaat in op bedrijfscontinuïteit in geval van uitval van ICT en telecom. Gemeenten kunnen het spelmateriaal downloaden vanaf de website van de IBD en de game zelfstandig spelen.

#### **Regiobijeenkomsten**

De IBD organiseert twee keer per jaar een reeks regiobijeenkomsten. Een dergelijke reeks bestaat uit vier bijeenkomsten rondom privacy en gegevensbescherming en 4 bijeenkomsten rondom informatiebeveiliging. Opvallend is dat het maximaal aantal deelnemers (50) vaak al binnen een dag of een paar dagen bereikt is. Steeds vaker speelt de gastgemeente een rol in de plenaire opening, bijvoorbeeld door het welkomstwoord te verzorgen. Als voorbeeld wordt de gemeente Valkenswaard genoemd, waar de burgemeester de bijeenkomst plenair heeft geopend.

Sinds mei 2019 maakt een gemeentelijke CISO deel uit van het team van de IBD. Dit door middel van een tijdelijk dienstverband voor twee dagen per week. Deze CISO blijkt een heel erg goede ambassadeur richting de achterban en de IBD overweegt een vergelijkbaar initiatief voor privacy op te zetten.

Rondom de verkiezingen is de IBD als adviseur betrokken bij een risicoanalyse op het huidige systeem van OSV en de doorontwikkeling daarvan. De IBD is door BZK gevraagd om CISO's van gemeenten te informeren over een veilig gebruik van OSV.

Het grootste deel van gemeenten (65%) staat positief tegenover de Standaard Verwerkersovereenkomst, nog eens 22% staat er neutraal tegenover. De acceptatie van de standaard in het adoptiejaar is hoog. Via de beheergroep kunnen gemeenten en leveranciers hun opmerkingen en aanvullingen voorstellen.

Het DPIA tool staat sinds enkele maanden online en inmiddels zijn 60 DPIA's (risicoanalyse op het verwerken van persoonsgegevens in gemeentelijke processen) uitgevoerd. De kern van deze tool is dat het mogelijk is om DPIA's te delen, zodat anderen de analyse kunnen hergebruiken, dit komt de kwaliteit ten goede en is erg efficiënt.

### **3 Update Landelijk Dekkend Stelsel**

Momenteel vindt aanvullend overleg plaats tussen het NCSC en de IBD over de samenwerkingsafspraken. Deze zullen op zijn laatst in maart 2020 zijn afgerond, waarna de IBD officieel een aangewezen CERT is. Een prachtige mijlpaal, aldus voorzitter Weerwind.

### **4 Toevoegen van een ondertitel aan de naam Adviesraad IBD**

Gezamenlijk is besloten de naam Adviesraad IBD te handhaven en een ondertitel toe te voegen. Eerder is in dit kader de ondertitel '**Het gemeentelijk adviesorgaan digitale weerbaarheid**' genoemd. Alle Adviesraadleden gaan akkoord met deze ondertitel.

### **5 Positionering Adviesraad IBD irt VNG Governance**

In diverse gremia wordt gesproken over digitale veiligheid. Het is van groot belang dat wat in de Adviesraad IBD besproken wordt, goed over gebracht wordt naar deze andere overlegorganen. De linking pin constructie die er nu is, is hierbij van belang. Daarnaast zal de de IBD een halfjaarlijks verslag opleveren met daarin een terugblik en een vooruitblik. Waar nodig kan dit verslag in de diverse overleggen worden toegelicht door een lid van de Adviesraad die deelneemt aan dat specifieke overleg.

### **6 Vergaderdata in 2020**

In 2020 komt de Adviesraad IBD bijeen op:

- Woensdag 11 maart 2020;
- Woensdag 17 juni 2020;
- Woensdag 16 september 2020;
- Woensdag 11 november 2020.