INFORMATIE BEVEILIGINGS DIENST

JAAROVERZICHT 2016
ACCENTVERSCHUIVING NAAR STERKERE CERT-TAAK

Gemeenten hebben in 2016 gewerkt aan de verdere versteviging van de informatiebeveiliging en zijn verder gegroeid in hun volwassenheid op het thema. Inmiddels is het belangrijkste gedeelte van de maatregelen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) geïmplementeerd en, mede omdat de verandere omgeving dat vereist, is de tijd aangebroken om meer te werken aan het detecteren van risico's en het voorkomen van incidenten. Betere detectiemogelijkheden en de sterkere basis leiden automatisch tot meer waargenomen incidenten. De toegenomen volwassenheid bij de doelgroep en de veranderende omgeving leiden tot een accentverschuiving in de behoefte van gemeenten en daarmee de focus van de IBD van beleidsondersteuning richting incidentondersteuning, ofwel de CERT-taak.

Meldplicht datalekken
In 2016 is de meldplicht datalekken van kracht geworden. Deze meldplicht heeft geleid tot transparantie over informatiebeveiligingsincidenten voor zover die betrekking hebben op persoonsgegevens. De IBD heeft gemeenten voorafgaand aan de inwerkingtreding van deze meldplicht uitgebreid geïnformeerd over de betekenis en de uitwerking hiervan. De IBD helpdesk heeft met name in de eerste helft van het jaar veel geholpen met het beoordelen en analyseren van datalekken om te bepalen of gemeld moest worden aan de toezichthouder en / of de betrokkenen.

Kwetsbaarheden
Het aantal bekende kwetsbaarheden in ICT-componenten liep in 2016 uiteen van enkele tot wel tientallen per dag. Gemeenten worden door hun aansluiting bij de IBD gericht en op maat op de hoogte gesteld van kwetsbaarheden die op de eigen situatie van toepassing zijn. De meest opzienbarende kwetsbaarheden van 2016 waren die in het https-protocol, in Windows, in Linux en in enkele firewalls.

Incidenten
De helpdesk van de IBD heeft in 2016 376 keer ondersteuning verleend bij informatiebeveiligingsincidenten van gemeenten. Dit betreft een toename die voor het grootste deel is toe te schrijven aan betere detectiecapaciteit en inwerkingtreding van de meldplicht datalekken. De aard en omvang van de incidenten verschilt per geval. Tot halverwege het jaar was een toename in ransomwareaanvallen te zien. Een goed backup- en restorebeleid kan hierbij veel ellende voorkomen en beperkt de impact van een besmetting. De IBD voorziet gemeenten regelmatig van tips en handelingsperspectief om nieuwe besmettingen te voorkomen. Een aantal maal leidde een incident bij ketenpartners en toeleveranciers van gemeenten tot een omvangrijk datalek.

Bronnen
De IBD verkrijgt informatie over (potentiele) incidenten uit steeds meer bronnen. Bijvoorbeeld van onderzoekers en ethisch hackers onder responsible disclosure en rechtstreeks van ontwikkelaars en leveranciers. Het is hierbij van essentieel belang dat de IBD een onafhankelijke en vertrouwde partij is waar in vertrouwen een melding kan worden gedaan.

Woordvoering & Communicatie
Informatiebeveiliging wordt steeds meer een mainstream onderwerp voor lokale en landelijke media. Hacks rondom de verkiezingen in de VS en grote datalekken bij o.a. LinkedIn, Dropbox en Yahoo maar ook incidenten dichter bij de eigen organisatie maken het fenomeen zichtbaar en tastbaar. Dit heeft als gevolg dat incidenten bij gemeenten breed uitgemeten worden in de media. (Crisis)communicatie wordt een steeds belangrijker aspect van incidentmanagement in het digitale domein. In maart brachten onderzoekers een kwetsbaarheid in beveiligde https-verbindingen aan het licht waarop RTL-Nieuws websites van gemeenten onderzocht en tot de conclusie kwam dat 49 domeinen kwetsbaar waren. Er waren meer metingen van gemeentelijke domeinen, zoals het initiatief faalkaart.nl, een herhaalde meting van RTL Nieuws en de meting van de Open State Foundation. Binnenlands bestuur onderzocht gemeentelijke e-mail en concludeerde dat nog niet alle gemeenten de open standaarden van de pas-toe-of-leg-uit-lijst geïmplementeerd hadden.

DE TOEGENOMEN VOLWASSENHEID BIJ DE DOELGROEP EN DE VERANDERENDE OMGEVING LEIDEN TOT EEN ACCENTVERSCHUIVING VAN BELEID NAAR INCIDENTONDERSTEUNING.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Gemeenten streven naar snelheid, transparantie en openheid in de communicatie. De IBD draagt hieraan bij door duiding te geven aan incidenten in de gemeentelijke context. Gemeenten kunnen een beroep doen op de IBD voor advies bij communicatie en woordvoering en de IBD kan waar nodig en gewenst een toelichting verzorgen op de feiten en omstandigheden Ondersteuning bij woordvoering en communicatie blijkt voor gemeenten een waardevolle aanvulling op het eigen incidentmanagementproces.

BIG
De IBD ondersteunt gemeenten bij de implementatie van maatregelen uit de BIG, o.a. door operationele producten uit te brengen die aansluiten bij de BIG en passen bij de praktijk van gemeenten. In 2016 zijn ondersteuningsproducten uitgebracht voor de implementatie van technische standaarden zoals TLS, DNSSEC, DMARC en DKIM. Andere operationele BIG-producten gingen over veilige toepassing van Wifi, en bedrijfscontinuïteitsbeheer. Verder zijn verschillende BIG-producten bijgewerkt en in lijn gebracht met actuele ontwikkelingen.

De IBD heeft een nieuwe versie uitgebracht van de model-bewerkersovereenkomst. De nieuwe modelovereenkomst is ingrijpend gewijzigd ten opzichte van de eerdere versies. Daarbij kan het model nu gebruikt worden voor twee soorten bewerkersovereenkomsten, te weten voor de Wbp en/of voor de BRP. Verder heeft de IBD in dit kader een bijdrage geleverd aan de totstandkoming van de nieuwe Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT).

De IBD ondersteunt alle Nederlandse gemeenten bij vraagstukken op het gebied van informatiebeveiliging. De IBD is betrokken bij veel projecten en biedt advies over de veilige inrichting en uitvoering van projecten in relatie tot de BIG. De belangrijkste projecten waar de IBD aan (mee)werkt zijn: De Digitale Agenda 2020 (DA2020), Programma Borging Veilige Gegevensuitwisseling via Suwinet (BGVS),doorontwikkeling BIRBIO en Informatiebeveiliging in de Omgevingswet. Voor GEMMA heeft de IBD gezorgd voor de uitbreiding van de referentiecomponenten met de belangrijkste beveiligingsstandaarden.

Bewustwording
De factor mens blijft de belangrijkste schakel in informatiebeveiliging. Bewuste medewerkers zijn van essentieel belang om de gemeentelijke informatievoorziening te beveiligen en beveiligd te houden. Om de bewustwording verder te stimuleren heeft de IBD in 2016 een crisisoefening ontwikkeld: de IBD Crisisgame. Ook heeft de modelcampagne Safe & Sound een update gekregen en heeft de IBD het bordspel 'Spion op je pad' uitgebracht.

Kennisdeling en samenwerking
Kennisdeling blijft de sleutel tot succes. De IBD faciliteert en voedt het kennisnetwerk van Nederlandse gemeenten. Gemeenten leren van elkaar en wisselen ervaringen uit op de IBD-community en tijdens de regionale bijeenkomsten van de IBD. De IBD heeft in 2016 verder ingezet op het verstevigen van contacten om het collectief van gemeenten in verbinding te brengen met specifieke kennis en capaciteiten. Als sectoraal schakelpunt is de IBD vanzelfsprekend nauw verbonden met het Nationaal Cybersecurity Centrum (NCSC). De IBD is onderdeel van het Nationaal Respons Netwerk (NRN) waarin kennis en capaciteiten van verschillende private en publieke partijen worden gebundeld. In 2016 heeft de IBD de banden aangehaald met partijen als de nationale politie, de fraudehelpdesk, het Centraal Meldpunt Identiteitsfraude en –fouten (CMI).

Vooruitblik
In 2016 is langzaam maar zeker het accent van de dienstverlening verschoven van beleid naar incidentcoördinatie en technische ondersteuning vanuit de CERT. Deze accentverschuiving zet ook in 2017 door. Nu gemeenten de grootste slag gemaakt hebben bij de implementatie van de BIG is de tijd aangebroken om meer nadruk te leggen op het detecteren van risico's en daarmee het voorkomen van incidenten. In 2017 voert de IBD. een verkenning uit naar de maatregelen die noodzakelijk zijn om nieuwe risico's het hoofd te kunnen bieden zoals het delen van actuele dreigingsinformatie tussen gemeenten, de zogeheten Threat Intelligence (TI), en het real time monitoren door middel van een Security Information Event Managementproces (SIEM). Vanaf 2017 kunnen ook intergemeentelijke sociale diensten en belastingsamenwerkingen van gemeenten aansluiten bij de IBD. Met de aansluiting van deze nieuwe doelgroepen is een volgende stap gezet in het veiliger maken en het veilig houden van de gemeentelijke informatievoorziening. In 2017 zal de IBD bijdragen aan het opbouwen van een ondersteuningsaanbod voor gemeenten op privacyvraagstukken vanuit VNG en KING.

INFORMATIE BEVEILIGINGS DIENST

MEER INFORMATIE
MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE FACTSHEETS VAN DE IBD EN OP DE WEBSITE WWW.IBDGEMEENTEN.NL.
HIER KUNNEN GEMEENTEN BOVENDIEN VIA DE COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN. DE HELPDESK VAN DE IBD IS TE BEREIKEN TIJDENS KANTOORUREN VAN 9:00 TOT 17:00 UUR OP HET NUMMER 070 373 8011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL. TIJDENS DEZE KANTOORUREN REAGEERT DE IBD BINNEN 30 MINUTEN OP EEN INCIDENTMELDING. BUITEN KANTOORUREN IS DE IBD OP HETZELFDE NUMMER BEREIKBAAR VOOR SPOEDEISENDE MELDINGEN EN ZAL DE IBD BINNEN 60 MINUTEN REAGEREN OP EEN TELEFONISCHE OPROEP.