INFORMATIE
BEVEILIGINGS
DIENST

DE INFORMATIEBEVEILIGINGSDIENST VOOR GEMEENTEN (IBD)

De Informatiebeveiligingsdienst voor gemeenten (IBD) is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de collectieve keuze van gemeenten voor coördinatie en ondersteuning op het gebied van informatiebeveiliging via de IBD. De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen. Deze factsheet geeft een kijkje in de keuken van de dienstverlening van de IBD.

EEN INFORMATEBEVEILIGINGSDIENST, WAAROM EIGENLIJK?

We leven in een tijdperk waarin informatie in grote hoeveelheden beschikbaar is. De ontwikkelingen in de digitale wereld hebben actief bijgedragen aan de beschikbaarheid van deze informatie, die jaarlijks nog steeds toeneemt. Technologieën maken het ons steeds gemakkelijker om informatie te gebruiken en met elkaar te delen. Maar de beveiliging van de digitale informatie die we delen, blijkt niet altijd zo sluitend als we graag zouden wensen. Ondanks het verhoogde bewustzijn bij organisaties komt het onderwerp in ons land regelmatig negatief in het nieuws.

Ook de Nederlandse gemeenten staan hierbij voor een uitdaging. Gemeenten zijn, net als andere (overheids-) organisaties, uitermate kwetsbaar als het gaat om hun (digitale) dienstverlening en met name het veilig/beveiligd uitvoeren van deze dienstverlening. Zeker in een tijd waar verantwoordelijkheden zwaarder, budgettering krapper en succesvolle prioritering steeds belangrijker worden. Beveiligingsincidenten gaan over meer dan geld alleen. De overheid beheert veel persoonsgegevens. Als de overheid de digitale beveiliging hiervan niet voldoende kan borgen is het vertrouwen in de overheid in het geding. Naast de digitale veiligheid kan cybercrime uiteraard ook de fysieke veiligheid van burgers en organisaties in gevaar brengen. Denk bijvoorbeeld aan het hacken van besturingssystemen van sluizen en bruggen.

Coördinatie en bewustzijn zijn onontbeerlijk als het gaat om een fundamentele oplossing op het vlak van informatiebeveiliging.

COÖRDINATIE EN BEWUSTZIJN, DAT VRAAGT OM ACTIE!

VNG en KING hebben medio 2012 de intentie uitgesproken de IBD op te richten. Dit mede in navolging van het succesvol eerste initiatief op het vlak van informatiebeveiliging, namelijk de ondersteuning aan gemeenten in het kader van het ICT-Beveiligingsassessment DigiD. En in januari was de oprichting van de IBD een feit.

De IBD heeft drie concrete doelen. Hierbij staat kennisontwikkeling, kennisdeling en kennisvermeerdering op het vlak van informatiebeveiliging bij gemeenten centraal.

1. Het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.
2. Het leveren van integrale coördinatie en concrete ondersteuning op gemeentespecifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. Het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen.

De nadruk ligt hierbij zowel op het verhogen van het informatiebeveiligingsbewustzijn bij management- en beleidsverantwoordelijken als op het bieden van concrete ondersteuning aan gemeentelijke ICT-verantwoordelijken. Uiteraard afgestemd op de concrete behoefte bij een gemeente.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

DE IBD-DIENSTVERLENING, FASEGEWIJS UITBOUWEN

De IBD heeft sinds 2013 haar dienstverlening gefaseerd ingericht en uitgebouwd. Via de website www.IBDgemeenten.nl vindt u alle relevante informatie over informatiebeveiliging. Het IBD-dienstverleningspakket is gebaseerd op haar drie doelen en als volgt uitgewerkt:

1. Bewustzijnsopbouw

Om dit doel te bereiken, werkt de IBD nauw samen met gemeentelijke partners. In 2015 worden de afspraken uit de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' in samenhang verder gerealiseerd. Het belangrijkste uitgangspunt van de Resolutie is een vorm van Verplichtende Zelfregulering: het borgen en verankeren van informatieveiligheid in de reguliere bedrijfsvoering en het afleggen van verantwoording daarover op een transparante wijze. De IBD ontwikkelt samen met de partners concrete initiatieven en producten die gemeenten ondersteunen zich verder te ontwikkelen en te professionaliseren op informatiebeveiligingsvlak.

2. Incidentpreventie, -detectie en -coördinatie

Eén van de doelen van de IBD is het aan gemeenten leveren van concrete ondersteuning in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging. Dit doel vertaalt zich in de concrete uitwerking naar een drietal verantwoordelijkheden richting gemeenten:

1. **Incidentpreventie**
   Het doel van 'Incidentpreventie' voor gemeenten is het voorkomen van incidenten. Dit door gemeenten zo snel als mogelijk te informeren over algemene dreigingen en door informatie te verzamelen over gemeentelijke incidenten en hierover periodiek te rapporteren.

2. **Incidentdetectie**
   Het doel van 'Incidentdetectie' voor gemeenten is het tegen gaan van verdere verspreiding van mogelijke virussen, wormen, botnetten en aanvallen van buitenaf. De IBD waarschuwt die gemeenten waarvan bekend is dat deze gemeenten geïnfecteerde systemen hebben.

3. **Incidentcoördinatie**
   Het doel van 'Incidentcoördinatie' voor gemeenten is het voorkomen van incidenten. En, in geval incidenten zich toch voordoen, het beperken van de technische-, financiële- en imagoschade bij gemeenten.

Deze drie verantwoordelijkheden zijn concreet vormgegeven middels een ontwikkeld producten- en dienstenportfolio. Een portfolio dat continu aangevuld wordt met nieuwe producten en diensten. Om dit te bereiken en deze verantwoordelijkheden daadwerkelijk op te kunnen pakken, werkt de IBD nauw samen met het Nationaal Cyber Security Centrum (NCSC) en uiteraard met elke specifieke gemeente.

3. Projecten

De IBD zet zich op projectbasis (in opdracht) in voor specifieke aan informatiebeveiliging gerelateerde onderwerpen. Het ondersteunen bij de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is hiervan een voorbeeld.

DE IBD-DIENSTVERLENING EEN FEIT

Op alle drie de geschetste dienstverleningsvlakken van de IBD zijn we volop actief. Bovendien is er een IBD-Helpdesk in het leven geroepen. Hier kunt u tijdens kantooruren terecht met vragen over de IBD-dienstverlening en gerichte vragen aangaande incidentpreventie en incidentdetectie van mogelijke onvolkomenheden in uw gemeentelijke ICT-inrichting als het gaat om informatiebeveiliging. Uiteraard blijft uw gemeente zelf, eventueel in combinatie met uw ICT-leverancier(s), verantwoordelijk voor het oplossen van deze onvolkomenheden.

Bij de drie IBD-doelen staan kennisontwikkeling, kennisdeling en kennisvermeerdering op het vlak van informatiebeveiliging bij gemeenten centraal. Om dit te stimuleren heeft de IBD factsheets ontwikkeld per doel. De factsheets behorend bij een doel zijn te herkennen aan de volgende kleuren:

1 BEWUSTZIJN

2 INCIDENTEN

3 PROJECTEN

MEER INFORMATIE

MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE ANDERE 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.