Producten en diensten van de

INFORMATIE BEVEILIGINGS DIENST

voor gemeenten

Let op: nieuw telefoonnummer IBD
070 - 204 55 11

Links naar verschillende onderwerpen in deze brochure vindt u op www.informatiebeveiligingsdienst.nl/pdc

Inleiding

De Informatiebeveiligingsdienst (IBD) voor gemeenten werkt aan het verhogen en op peil houden van de informatiebeveiliging en gegevensbescherming van Nederlandse gemeenten vanuit de kracht van het collectief. De IBD is een initiatief van alle Nederlandse gemeenten. Alle gemeenten, intergemeentelijke sociale diensten en belastingsamenwerkingen kunnen aansluiten bij de IBD en gebruik maken van de diensten en producten.

Factsheets, handreikingen en documenten zijn ook voor niet-aangesloten organisaties openbaar beschikbaar op de website www.informatiebeveiligingsdienst.nl.

Als u bent aangesloten bij de IBD, kunt u gebruik maken van al onze diensten. Wij helpen u beveiligingsincidenten te voorkomen en we waarschuwen u als uw systemen kwetsbaarheden vertonen. En mocht er een incident plaatsvinden, bieden we hulp en ondersteuning om de schade zoveel mogelijk te beperken en de situatie te herstellen. Tevens kunt u bij de IBD terecht voor uw vraagstukken over privacy en gegevensbescherming.

Voor vragen op het gebied van informatiebeveiliging kunt u een e-mail sturen aan info@IBDgemeenten.nl en voor vragen op het gebied van privacy kunt u een e-mail sturen aan privacy@VNG.nl.

Voorkomen en waarschuwen

Als gemeente of samenwerkingsverband wilt u beveiligingsincidenten natuurlijk zoveel mogelijk voorkomen. De IBD helpt u hierbij. Zo kunt u bij ons bijvoorbeeld informatie krijgen over kwetsbaarheden en het tegengaan van risico's. Soms weet u zelf niet waar het gevaar zit, omdat kwetsbaarheden niet zichtbaar zijn. Elke dag worden nieuwe kwetsbaarheden ontdekt, en we weten niet alles. Daarom houdt de IBD in de gaten of er nieuwe of bekende veiligheidsproblemen zijn met door u gebruikte software, hardware of systemen.

Ook controleert de IBD op indicaties dat gemeenten getroffen kunnen zijn door malware en hacks. Hiervan ontvangt u direct bericht. Zodat u maatregelen kunt nemen om misbruik te voorkomen.

De informatie die we u geven, komt van partnerorganisaties, meldingen van leveranciers, ethische hackers en onderzoekers, gemeenten, samenwerkingsverbanden en eigen onderzoek. Door uw meldingen worden alle gemeenten veiliger.

Kwetsbaarheidswaarschuwingen

We sturen u een waarschuwing als er kwetsbaarheden bekend zijn van door u opgegeven software en hardware. De kwetsbaarheidswaarschuwing bestaat uit een beschrijving van het probleem, informatie over oplossingen of workarounds en een risicoanalyse. U ontvangt deze informatie alleen over die systemen waarvan u dat wenst of nodig heeft. In aanvulling hierop stuurt de IBD ook informatie over kenmerken van andere dreigingen (CTI).

Detectie van besmettingen

De IBD kan in samenwerking met (internationale) partners lijsten met besmette systemen controleren op aanwezigheid van gemeentelijke IP-adressen. Wij hebben hiervoor een overzicht nodig van uw externe IP-adressen. De IBD waarschuwt uw gemeente als een ICT-systeem geïnfecteerd is. Zo kunt u snel maatregelen nemen om verspreiding van mogelijke virussen, wormen, botnetten en aanvallen te beperken.

Schade beperken

Mocht het zover komen dat er toch een veiligheidsincident is, dan kan de IBD u adviseren over de mogelijke oplossingsrichting en helpen, met coördinatie en crisiswoordvoering.

Coördinatie door de IBD

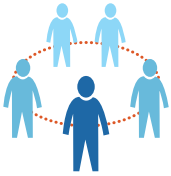
In geval van een incident kunt u de IBD benaderen voor hulp en ondersteuning. Bij een incident waarbij meerdere gemeenten betrokken zijn kan de IBD coördinerend optreden namens gemeenten. Bijvoorbeeld in de richting van andere overheden, leveranciers of ketenpartners. Hiermee beperken we de technische-, financiële- en imagoschade voor uw gemeente en andere gemeenten. Bij een incidentmelding bepalen gemeente en de IBD samen de ondersteuningsbehoefte. Waar nodig kunnen andere gemeenten bijstand verlenen door middel van het gemeentelijk responsnetwerk. De IBD kan (online) aansluiten in uw crisisteam.

Advies communicatie en woordvoering

Communicatie over informatiebeveiliging is vaak technisch en complex. De IBD ondersteunt u bij het vertalen van de situatie naar begrijpelijke taal voor gemeenteraad, bestuur, inwoners en ondernemers. We ondersteunen u, in geval van incidenten of een crisis bij gemeenten, met concrete adviezen aan de beveiligings- en privacyfunctionaris (CISO, PO en FG) en de woordvoerder van uw gemeente of meerdere gemeenten. Waar nodig kan de IBD ook namens gemeenten het woord voeren.

Contact onderhouden met leveranciers en ketenpartners

De IBD onderhoudt het contact met leveranciers en ketenpartners van gemeenten. In een landelijk dekkend stelsel houdt de IBD het contact met de rijksoverheid, provincies, waterschappen en andere sectoren. Zo kunnen we in geval van een incident snel alle benodigde partijen bereiken.



Kennis delen en kennis vermeerderen

Het delen van kennis is de sleutel tot succes. U staat er als gemeente niet alleen voor en als u een vraag heeft, dan heeft een andere gemeente daar meestal al een antwoord op gevonden. De IBD helpt u bij het leggen van de verbinding met andere gemeenten.

Advies & belangenbehartiging

Informatiebeveiligings- en privacyfunctionarissen kunnen bij de IBD terecht voor vragen over informatiebeveiliging, privacy en gegevensbescherming. Als onderdeel van de koepel van gemeenten kan de IBD, een antwoord vinden op vraagstukken die specifiek spelen voor gemeenten. De IBD onderhoudt hiervoor het contact met relevante ketenpartners, toezichthouders en leveranciers om actuele vraagstukken te bespreken.

Verhogen digitale weerbaarheid

Om de digitale weerbaarheid van gemeenten te verhogen ontwikkelde de IBD een programma met handvatten voor de meest urgente maatregelen en processen uit de BIO. In het programma VDW treft u onder andere kennisproducten, mindmaps en instructievideo's.

VNG Forum

Op het VNG Forum kunt u kennis en informatie uitwisselen met collega's van andere gemeenten. U kunt op het VNG Forum meedoen aan discussies of zelf een discussie starten.

(Online) bijeenkomsten

De IBD organiseert doorlopend (online) bijeenkomsten over informatiebeveiliging en privacy. Bij deze bijeenkomsten schuiven regelmatig experts aan van gemeenten, VNG, rijksoverheid en de Autoriteit Persoonsgegevens.

Trainen en oefenen

Oefenen is een belangrijk thema in de Agenda Digitale Veiligheid. Om te zorgen dat uw gemeente adequaat reageert tijdens een incident, ontwikkelde de VNG/IBD games en (crisis)oefeningen. Deze oefeningen kunt u in de eigen organisatie en / of met ketenpartners zoals de veiligheidsregio en de politie uitvoeren.

Bewustwording

Om het bewustzijn van informatiebeveiliging en privacy te verhogen binnen uw gemeente, kunt u gebruikmaken van de verzamelde bewustwordingscampagnes van gemeenten.

Beheer-, expert- en werkgroepen

De IBD werkt samen met gemeenten in beheer-, expert en werkgroepen. De beheergroepen gaan over het onderhoud en actualisatie van producten en diensten. De expert- en werkgroepen gaan over actuele vraagstukken en resulteren in een kennisproduct (zie ondersteuningsproducten hieronder). Contactpersonen van de IBD ontvangen via de maandmonitor een oproep om deel te nemen.

DPIA-tool en collectieve DPIA's

De IBD heeft een tool beschikbaar gesteld waarmee gemeenten een Data Protection Impact Assessment (DPIA) uit kunnen voeren. Een belangrijk uitgangspunt van de DPIA-tool is het default delen van ingevulde DPIA's met alle andere leden van de IBD-community. Dit om te stimuleren dat gemeenten van elkaar leren en niet zelf het wiel opnieuw hoeven uit te vinden Daarnaast voert de IBD samen met gemeenten ook collectieve DPIA's uit. De DPIA-tool wordt onderdeel van de Integrale Risico en Privacy Analyse Tool.

Aansluiten bij collectieven

De IBD sluit regelmatig aan bij bijeenkomsten van (regionale) CISO/FG-collectieven. Neem contact op met de IBD als u ons wilt uitnodigen.

Beleid ontwikkelen

De Baseline Informatiebeveiliging Overheid beschrijft wat u als gemeente moet doen om de informatiebeveiliging op orde te houden. Het gaat bijvoorbeeld over normen en eisen voor goed bestuur, beleid, beheer en het beperken van risico's. Daarnaast vormt de AVG het kader voor de omgang met persoonsgegevens. Op onze website vindt u handreikingen, factsheets en voorbeelddocumenten. Deze kunnen u helpen de AVG en de BIO in uw gemeente toe te passen en maatregelen en beleid specifiek te maken voor uw gemeente.

Handreikingen en factsheets

Handreikingen en factsheets beschrijven best practices op het gebied van informatiebeveiliging en privacy. Gemeenten en de IBD maken zo veel mogelijk samen producten: de IBD maakt stukken van gemeenten generiek en beschikbaar voor andere gemeenten.

Borging AVG

De IBD ontwikkelde het AVG Borgingsproduct om de AVG te vertalen naar een kwaliteitscyclus binnen de gemeente. Dit instrument geeft gemeenten concrete handvatten om een goede omgang met persoonsgegevens te waarborgen.

Standaard Verwerkersovereenkomst

De IBD beheert de standaard verwerkersovereenkomst (VWO) van Nederlandse gemeenten. Wijzigingsvoorstellen worden behandeld door de beheergroep VWO.

Advies in projecten

De IBD is op verzoek van (leden van) de VNG als adviseur betrokken bij collectieve projecten van gemeenten. De adviseurs van de IBD voeren risicoanalyses uit en zij adviseren over veiligheidsmaatregelen en het waarborgen van privacy.

Publicaties en rapportages

Dreigingsbeeld

Elke twee jaar publiceert de IBD het dreigingsbeeld informatiebeveiliging Nederlandse gemeenten. Dit dreigingsbeeld heeft als doel gemeenten weerbaarder te maken op het gebied van informatiebeveiliging door inzicht te geven in de belangrijkste risico's en dreigingen voor de gemeentelijke informatievoorziening.

Maandmonitor

De maandmonitor biedt een overzicht van relevante ontwikkelingen op het terrein van informatiebeveiliging en privacy in de gemeentelijke context. De IBD geeft in de maandmonitor algemene adviezen in lijn met de BIO en de AVG.

Geef de actuele gegevens door aan de IBD

Wij vragen u aantal zaken actueel te houden en aan ons door te geven, zodat we u goed van dienst kunnen zijn:

1. Gegevens van algemene contactpersonen bij uw gemeente of samenwerkingsverband voor de IBD. Voor het onderwerp privacy kunt u de contactgegevens van de FG of privacy officer aan ons doorgeven.

2. Gegevens van 'vertrouwde' contactpersonen bij uw gemeente of samenwerkingsverband voor de IBD. Zij mogen vertrouwelijke informatie ontvangen en aan ons sturen.

3. De externe IP-adressen van uw gemeente.

4. Informatie van alle ICT-systemen waarover u kwetsbaarheids-waarschuwingen van de IBD wilt ontvangen.

Contact met de IBD

Heeft u vragen en/of opmerkingen over informatiebeveiliging en privacy, dan kunt u contact opnemen via info@IBDgemeenten.nl, privacy@VNG.nl of 070 204 55 11.

Incident? Spoed?

Als er sprake is van een spoedeisend incident of een datalek, dan kunt u de IBD 24 uur per dag bereiken via 070 204 55 11. Buiten kantooruren krijgt u via de voicemail instructies om de piketfunctionaris te bereiken.

INFORMATIE BEVEILIGINGS DIENST

Nassaulaan 12
2514 JS Den Haag
070 204 55 11
info@IBDgemeenten.nl
privacy@VNG.nl