IBD 2022

Jaaroverzicht 2022

INFORMATIE BEVEILIGINGS DIENST

387
incidenten met een hulp-, coördinatie- of ondersteuningsvraag van gemeenten

1.250 ±
telefoongesprekken

1102
kwetsbaarheidsmeldingen IBD-CERT

62
hoge kans op misbruik en een grote potentiële schade

18
algemene waarschuwingen

2
advies- en ondersteuning in crisisteam op locatie

1
inzet van de Rapid Response Triage

1
SMS-waarschuwing buiten kantooruren over een ernstige kwetsbaarheid aan alle gemeenten

2.313
vragen en meldingen over informatiebeveiliging

467
vragen over privacy

21
medewerkers

Overzicht medewerkers
https://www.informatiebeveiligingsdienst.nl/medewerkers-van-de-ibd/

103.000
bezoekers www.informatiebeveiligingsdienst.nl

Top 3 downloads

1. Bio
2. Baselinetoets
3. Handreiking Dataclassificatietoets

4000+
gemeentelijke deelnemers op het Privacyforum

671
geplaatste reacties

210
gestelde vragen

62
bijeenkomsten online en offline

33
over privacy

29
over informatiebeveiliging

542
onderzoeken uitgevoerd in integrale risico- en privacy-analyse IRPA

3.902
analyses bezig

64
nieuwe en bijgewerkte kennisproducten

20
Maandmonitoren Informatiebeveiliging en Privacy

Incidenten en kwetsbaarheden

Voor de IBD begon 2022 met de nasleep van de **Log4J-kwetsbaarheden** die in december 2021 bekend werden. Een vervelende en riskante kwetsbaarheid, omdat het Log4J-component onderdeel is van tienduizenden hard- en softwaresystemen. De IBD bracht een document uit met de geleerde lessen over de aanpak van complexe kwetsbaarheden .

Het aantal kwetsbaarheden met een hoge kans op grote schade was met meer dan 60 wederom hoger dan in voorgaande jaren. Vooral kwetsbaarheden in het veelgebruikte Microsoft Exchange hielden gemeenten bezig, dit omdat de oplossing lang op zich liet wachten en in de tussentijd verschillende instellingen moesten worden gewijzigd. Gedurende heel 2022 ontving de IBD opvallend veel **meldingen over phishing** en **pogingen tot CEO-fraude, waarbij een crimineel zich voordoet als belangrijk persoon binnen een organisatie**. In algemene zin worden dit soort malafide mails of berichten steeds professioneler (of in elk geval minder slordig) en pogingen om **geld** of inloggegevens afhandig te maken slagen steeds vaker. In januari zijn tientallen gemeentelijke inloggegevens door een partnerorganisatie van de IBD aangetroffen op een gehackte website. Om misbruik van dergelijke gegevens te voorkomen blijft **2-factorauthenticatie een belangrijk verdedigingsmechanisme**. In februari viel Rusland Oekraïne binnen. De IBD had in 2022 geen concrete aanwijzingen dat digitale aanvallen in relatie tot die oorlog impact hadden op Nederland, maar sluit gevolgen en aanvallen in Nederland niet uit voor de toekomst. **De IBD staat hierover in nauw contact met het Nationaal Cyber Security Centrum (NCSC)**.

Werkleerbedrijf Voorne-Putten Werkt werd begin maart slachtoffer van een hack. De aanvaller verkreeg toegang tot het IT-systeem en stal een grote hoeveelheid data. De **hack bij de gemeente Buren** had een grote impact. Ook **voor dit incident zijn de lessen opgetekend** zodat andere gemeenten kunnen leren en waar nodig maatregelen kunnen nemen. In november werd ook **werkleerbedrijf Pantar slachtoffer van een hack**. Bij zowel Buren als Pantar bood de IBD op locatie advies en ondersteuning aan het management en het bestuur. Bij de overige incidenten sloot de IBD online aan bij het crisisteam.

Gelukkig had 2022 ook goed nieuws. Gedurende het jaar kreeg de IBD kant-en-klare meldingen compleet met onderzoek over incidenten, die dankzij oplettende systeembeheerders en **goede monitoring** werden gestopt voordat noemenswaardige schade optrad. Er was één melding die meteen een goede les in zich had. De organisator van een phishing-bewustwordingsactie was vergeten om dit aan de CISO te melden. Die seinde vervolgens conform protocol de IBD in.

Log4J-kwetsbaarheden
https://www.informatiebeveiligingsdienst.nl/product/kwetsbaarheden-in-log4j-lessen-voor-de-gemeenten-en-de-ibd/

Blog over CEO-fraude
https://www.informatiebeveiligingsdienst.nl/blog/blog-maak-medewerkers-bewust-van-ceo-fraude/

CEO-fraude in het nieuws
https://www.rtvdrenthe.nl/nieuws/14377616/internetcriminelen-doen-zich-voor-als-drentse-burgemeesters-geloof-me-ik-heb-nog-nooit-vastgebonden-gezeten

Hack bij gemeente Haarlemmermeer
https://www.noordhollandsdagblad.nl/cnt/dmf20221221_71077382

Handreiking 2-factor authenticatie
https://www.informatiebeveiligingsdienst.nl/product/handreiking-2-factor-authenticatie-2fa-voor-gemeenten/

Nationaal Cyber Security Centrum (NCSC)
https://www.ncsc.nl/onderwerpen/oekraine

Hack bij werkleerbedrijf VPwerkt
https://www.vpwerkt.nl/cyberaanval-op-voorne-putten-werkt-bv/

Hack bij gemeente Buren
https://www.buren.nl/nieuws/datadiefstal-gemeente-buren/7399/

Lessen van de hack bij gemeente Buren
https://www.informatiebeveiligingsdienst.nl/nieuws/lessen-uit-de-hack-en-datalek-gemeente-buren/

Hack bij werkleerbedrijf Pantar
https://pantar.nl/nieuws/hack/

Monitoring & Response
https://www.informatiebeveiligingsdienst.nl/project/monitoring-response/

CERT en doorontwikkeling

De IBD-CERT startte met een pilot om bij een grootschalig incident ter plekke ondersteuning te bieden. Naast de bestaande ondersteuning op afstand, voert de IBD onder specifieke condities, triage op locatie uit met behulp van ervaren incidentresponders. Deze dienst is één keer ingezet.

De incidentdienstverlening is uitgebreid met **advies op locatie aan de ambtelijke top, bestuurders en hun crisismanagementteam**. Dit is in de praktijk bij twee incidenten toegepast. **De IBD netwerkinventarisatie** is beschikbaar voor alle gemeenten. Daarnaast is de CERT een pilot scan-tooling gestart om de buitenkant van gemeentelijke ICT-omgeving te scannen op risico's. Het is de bedoeling om deze pilot voort te zetten in 2023.

Advies op locatie
https://www.informatiebeveiligingsdienst.nl/ondersteuning-bij-incidenten/

Netwerkinventarisatie
https://www.informatiebeveiligingsdienst.nl/project/netwerk-inventarisatie-nwi/

Producten, kennisdeling en advies

De IBD maakte maar liefst **64 nieuwe en bijgewerkte kennisproducten** op de thema's **informatiebeveiliging en privacy**.

Alle nieuwe en geactualiseerde producten komen tot stand in nauwe samenwerking tussen de IBD en contactpersonen bij gemeenten. Ook publiceerde de IBD haar nieuwe **Dreigingsbeeld** , dat mede dankzij de **uitzending in Nieuwsuur** veel aandacht kreeg.

Als Kenniscentrum voor informatiebeveiliging en Privacy van de VNG adviseerde de IBD de verschillende projectteams o.a. over **PGB 2.0**, de Wet aanpak meervoudige problematiek sociaal domein (**Wams**), **de organisatie en tooling rond verkiezingen**, **Werk en Inkomen**, **Omnichannel** en **het afsprakenstelsel voor de Landelijke Monitor Complexe Casuïstiek in de jeugdhulp.**

64
nieuwe en bijgewerkte kennisproducten

Kennisproducten
https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/

Dreigingsbeeld Informatiebeveiliging Gemeenten 2023 – 2024
https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/

Uitzending Nieuwsuur
https://www.npostart.nl/nieuwsuur/19-10-2022/VPWON_1334680

VNG: Ontwikkeling en implementatie PGB 2.0
https://vng.nl/projecten/ontwikkeling-en-implementatie-pgb-20

Wams
https://www.programmasociaaldomein.nl/actueel/nieuws/2022/07/11/wams

Organisatie verkiezingen
https://www.kiesraad.nl/

VNG: Werk, inkomen en sociale zekerheid
https://vng.nl/rubrieken/werk-inkomen-en-sociale-zekerheid

VNG: Omnichannel kanaalstrategie - dienstverlening
https://vng.nl/projecten/omnichannel-kanaalstrategie-dienstverlening

VNG: Jaarrapportage over complexe casuïstiek in de jeugdhulp
https://vng.nl/nieuws/jaarrapportage-over-complexe-casuistiek-in-de-jeugdhulp

Bedrijfscontinuïteit centraal

Om gemeenten te helpen de continuïteit van de dienstverlening en bedrijfsvoering te beheersen, is het online dossier **Business Continuity Management (BCM)** in 2022 uitgebreid. Het dossier bevat producten die helpen om BCM als onderwerp te agenderen bij gemeenten, te bepalen waar gemeenten staan met betrekking tot BCM, en bij het vormgeven van de gemeentelijke backup- en herstelstrategie.

Business Continuity Management (BCM)
https://www.informatiebeveiligingsdienst.nl/business-continuity-management-bcm/

Privacy en gegevensbescherming

Voor veel gemeentelijke privacyexperts stond 2022 vooral in het teken van de audit Wet politiegegevens (Wpg). Gemeenten kwamen in 2021 al voor deze opgave te staan, maar kregen van de Autoriteit Persoonsgegevens uitstel tot eind 2022 om de audit aan te leveren. De IBD heeft zich in 2022 ingespannen om gemeenten hier zoveel mogelijk bij te ondersteunen. Dankzij een actieve werkgroep met privacy-officers en functionarissen gegevensbescherming uit verschillende gemeenten, leverde 2022 **tien nieuwe Wpg-kennisproducten** op. Gemeenten die deze kennisproducten gebruiken, voldoen voor een groot deel aan de verplichtingen die voortvloeien uit de Wpg.

Het privacyteam werkte ook aan een **vernieuwd privacybeleid**. Met dit product kunnen gemeenten om hun privacybeleid verduidelijken aan inwoners en ketenpartners. Bijvoorbeeld door het op de website te plaatsen voor iedereen die meer wil weten over hoe de gemeente omgaat met persoonsgegevens en privacy. Het privacyteam leverde ook de **Handreiking Privacy- en cookieverklaring** en een bijgewerkte versie van het vooringevulde gemeentelijke **Register van Verwerkingen** op.

De IBD droeg bij aan de juridische 2-daagse en aan de **opleiding 'Gegevensdeling in het sociaal domein.'** Negentien trainers uit de gemeentelijke praktijk werden tijdens een speciale opleidingsdag voor deze training klaargestoomd. Zij gaven in totaal 28 keer de training aan 504 deelnemers.

Kennisproducten met betrekking tot de Wet politiegegevens
https://www.informatiebeveiligingsdienst.nl/kennisproducten-met-betrekking-tot-de-wet-politiegegevens/

Privacybeleid
https://www.informatiebeveiligingsdienst.nl/product/privacybeleid/

Handreiking Privacy- en cookieverklaring
https://www.informatiebeveiligingsdienst.nl/product/handreiking-privacy-en-cookieverklaring/

Vooringevuld verwerkingsregister gemeenten
https://www.informatiebeveiligingsdienst.nl/product/vooringevuld-verwerkingsregister-gemeenten/

Opleiding Gegevensdeling in het Sociaal Domein 2022-2023
https://www.vngconnect.nl/academie/Training/opleiding-gegevensdeling-in-het-sociaal-domein-2022-2023/f2a6da1f-f7d4-42bf-96b9-06bd3093debc

Integrale risico- en privacyanalyse tool (IRPA)

De vernieuwde integrale risico- en privacy-analyse (IRPA) tool is beschikbaar voor gemeenten en wordt inmiddels goed gebruikt. In IRPA voerden gemeenten 542 onderzoeken uit en startten zij 3.902 analyses. De tool is **samen met een aantal gemeenten** ontwikkeld en getest. Het doel is om analyses op het gebied van privacy en informatiebeveiliging gemakkelijk, professioneel en éénduidig te kunnen uitvoeren. Analyses als de **(Pre-) Data Privacy Impact Assessment (DPIA)**, het **Eenvoudig hulpmiddel voor bepalen maatregelen, BBN en schade voor betrokkenen**, de **Baseline toets BBN BIO**, **de Risicoanalyse**, **de GAP(-O-)analyse** en **De Ethische Data Assistent (DEDA)**

542
onderzoeken uitgevoerd in integrale risico- en privacy-analyse IRPA

3.902
analyses bezig

Werk- en expertgroepen
https://www.informatiebeveiligingsdienst.nl/werk-en-expertgroepen

Handreiking DPIA BIO
https://www.informatiebeveiligingsdienst.nl/product/handreiking-dpia-bio/

Eenvoudig hulpmiddel voor bepalen maatregelen, BBN en schade voor betrokkenen
https://www.informatiebeveiligingsdienst.nl/product/eenvoudig-hulpmiddel-voor-bepalen-maatregelen-bbn-en-schade-voor-betrokkenen/

Baselinetoets BBN BIO
https://www.informatiebeveiligingsdienst.nl/product/baselinetoets-bbn-bio/

Handreiking Diepgaande Risicoanalyse Methode Gemeenten
https://www.informatiebeveiligingsdienst.nl/product/handreiking-diepgaande-risicoanalyse-methode-gemeenten/

GAP-analyse uitleg BIO
https://www.informatiebeveiligingsdienst.nl/product/gap-analyse-uitleg/

IRPA-tool
https://www.informatiebeveiligingsdienst.nl/irpa-tool/

Online en offline bijeenkomsten

De IBD organiseerde 62 bijeenkomsten (fysieke en online), 29 over informatiebeveiliging en 33 over privacy. Dit bracht gemeenten met elkaar in contact om kennis te delen over onder andere Business Continuity Management, Monitoring en Response, procesautomatisering en de Wet politiegegevens. Adviseurs van de IBD spraken onder andere op bijeenkomsten van de Kiesraad, verschillende ministeries, vakverenigingen zoals de **vereniging van gemeentesecretarissen**, de **IMG/VIAG** en koepelorganisaties. Ze waren twaalf keer aanwezig bij verschillende CISO/FG-samenwerkingsverbanden en namen deel aan tien gemeentelijke cyber-crisisoefeningen die waren georganiseerd door veiligheidsregio's. Ook trad de IBD op in de **landelijke overheidsbrede cyberoefening**.

Vereniging van gemeentesecretarissen
https://www.gemeentesecretaris.nl/

Overheidsbrede cyberoefening
https://viag.nl/samenwerkingsverbanden/samenwerkingsverbanden-koepels/img-100-000

IMG/VIAG
https://viag.nl/samenwerkingsverbanden/samenwerkingsverbanden-koepels/img-100-000

Meer aandacht voor organisatiebreed risicodenken

De IBD zette in 2022 actief in op het betrekken en informeren van management en directie van gemeenten bij het organisatiebreed risicodenken. Hiervoor voerden onze adviseurs diverse gesprekken met gemeentesecretarissen, met het doel een beeld te krijgen van hun problematiek en ondersteuningsmiddelen te kunnen aanbieden. In 2023 zal in aanvulling op het **kaartje in de meterkast** extra ondersteuning voor de ambtelijke top worden ontwikkeld.

Kaartje in de meterkast voor de gemeentesecretaris
https://www.informatiebeveiligingsdienst.nl/product/kaartje-in-de-meterkast-voor-de-gemeentesecretaris/

IBD dichtbij gemeenten

In zestig één-op-één gesprekken met CISO's gingen de adviseurs van de IBD vaker dan ooit op bezoek bij gemeenten. Gemeenten bezochten ook de IBD, met name de gemeentelijke functionarissen op de CISO-, PO- en de FG-stoelen verdienen daarbij bijzondere aandacht. Ook in 2022 werkten gemeentelijke CISO's en FG's enkele dagen per week op de **IBD-locatie in Den Haag**. Zij brachten waardevolle inzichten over de bruikbaarheid en de toepasbaarheid van de adviezen, de producten en de diensten. Andersom kregen deze personen een kijkje in de keuken van de IBD.

Na evaluatie in 2022 wordt de **IBD-adviesraad** uitgebreid met meer gemeentelijke deelnemers, inclusief gemeentesecretarissen en vertegenwoordigers van gemeenschappelijke regelingen.

Routebeschrijving IBD-locatie in Den Haag
https://vng.nl/artikelen/routebeschrijving-vng-den-haag

Governance & Adviesraad IBD
https://www.informatiebeveiligingsdienst.nl/governance-ibd/

Beleidsontwikkeling en wetgeving

De IBD werkte ook in 2022 nauw samen met de beleidscollega's van het team **Agenda Digitale Veiligheid (ADV)**. Zij adviseert over beleid, lobby en vertegenwoordiging van gemeenten, o.a. in de afspraken rond de nieuwe **Nederlandse cybersecuritystrategie**, de **nieuwe Europese richtlijn voor netwerk- en informatiebeveiliging NIS2**, **het Landelijk Crisisplan Digitaal** en de doorontwikkeling en **verplichting van de BIO per 2024**.

Agenda Digitale Veiligheid 2020-2024
https://vng.nl/publicaties/agenda-digitale-veiligheid-2020-2024

Nederlandse Cybersecuritystrategie 2022-2028
https://www.ncsc.nl/onderwerpen/nederlandse-cybersecurity-strategie

RICHTLIJN (EU) 2022/2555
https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555&from=EN

Landelijk Crisisplan Digitaal (LCP)
https://www.nctv.nl/documenten/publicaties/2022/12/23/landelijk-crisisplan-digitaal

Baseline Informatiebeveiliging Overheid (BIO)
https://vng.nl/publicaties/agenda-digitale-veiligheid-2020-2024

Vooruitblik 2023

In 2023 is het 10 jaar geleden dat gemeenten de IBD oprichtten. Dat gaat gevierd worden met een of meerdere inhoudelijke bijeenkomsten.

Ook in 2023 helpt de IBD gemeenten bij het versterken van de digitale weerbaarheid en het op orde krijgen en houden van de gegevensbescherming. Daarnaast focust zij zich op de doorontwikkeling van de CERT-taken, en geeft ze prioriteit aan de positionering van CISO's, FG's en PO's. De dienstverlening op het vlak van informatiebeveiliging en privacy versterkt elkaar steeds meer en dat reflecteert op producten en gecombineerde regiobijeenkomsten. Net als in 2022, bezoeken adviseurs gemeenten om de IBD- aanpak te toetsen en de behoefte in kaart te brengen.

Voor management en directie van gemeenten is een table-top oefening ontwikkeld op basis van de ervaringen met recente incidenten bij gemeenten. Met deze crisisoefening, die op aanvraag kan worden begeleid door de IBD, beleeft het management wat er op een gemeente afkomt bij een informatiebeveiligingsincident.

Het privacyteam levert in 2023 een **vernieuwd borgingsproduct** op. Gemeenten kunnen hiermee eenvoudig en eenduidig in kaart brengen in welke mate zij voldoen aan de eisen die de AVG stelt aan het verwerken van persoonsgegevens en wat er nodig is om de bescherming van persoonsgegevens naar een hoger niveau te brengen. In werksessies kunnen gemeenten kennismaken met de nieuwe versie, die rond maart 2023 beschikbaar komt. Ook een nieuwe training voor PO's en FG's besteedt hier aandacht aan. De IBD stelt een model beschikbaar voor gemeenten waarmee zij kunnen onderzoeken in hoeverre de voordelen van het toepassen van vormen van kunstmatige intelligentie (AI) opwegen tegen mogelijke risico's.

AVG Borgingsproduct 2.0
https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-2-0/

De IBD zet zich in om de arbeidsmarktkrapte op lange termijn te verminderen, door kennisinstellingen en lokale overheid met elkaar te verbinden. Door zelf structureel stages aan te bieden, en door stageopdrachten op te halen en uit te zetten bij gemeenten, laat de IBD zien dat werken bij gemeenten interessant, relevant en uitdagend is. Zo hopen we dat een grote groep MBO-, HBO- en universitaire studenten zich op termijn zal aandienen op de arbeidsmarkt van informatiebeveiliging en privacy bij gemeenten.

De IBD is in gesprek met rekenkamers over het optimaliseren van hun informatiebeveiligings- en privacyonderzoeken en met de Vereniging van Griffiers, om te kijken naar de problematiek die speelt bij de beveiliging van ICT van raadsleden.

Onder leiding van de VNG beleidscollega's en in samenwerking met een werkgroep van gemeenten, maakt IBD begin 2023 een inschatting van de impact van de Europese NIS2 richtlijn. Gemeenten bepalen een standpunt over de toepasselijkheid van NIS2 op gemeentelijke processen.

Vragen of meldingen?

070 204 55 11
info@IBDgemeenten.nl

De IBD kan 24 uur per dag worden benaderd voor spoedeisende vragen en meldingen.