INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie

Jaaroverzicht 2019

2019 stond voor gemeenten op het gebied van informatiebeveiliging en privacy in het teken van de verdere implementatie van de Algemene Verordening Gegevensbescherming (AVG) [1] en de overgang naar het gezamenlijke normenkader voor informatiebeveiliging van alle overheidslagen, de Baseline Informatiebeveiliging Overheid (BIO) [2]. In het afgelopen jaar hielp de IBD gemeenten bij het verhogen van hun digitale weerbaarheid en het borgen van privacy in de organisatie door middel van gericht advies, ondersteuning bij incidenten en kennisdeling. In dit jaaroverzicht treft u de meest in het oog springende activiteiten en ontwikkelingen.

Het jaar in cijfers

De IBD ontving in 2019 3044 vragen en meldingen over privacy en informatiebeveiliging en de IBD CERT stuurde maar liefst 1751 kwetsbaarheidsmeldingen uit, waarvan 23 zeer ernstige, dat wil zeggen met een hoge kans op en hoge waarschijnlijkheid van misbruik. Tweemaal werd hiervoor ook een waarschuwings-sms gestuurd aan de contactpersonen, waarvan 1 op kerstavond in verband met een ernstige kwetsbaarheid in Citrix. De IBD ontving 14 onderzoekswaardige responsible disclosure [3] meldingen, de melders hebben een kleine attentie ontvangen voor de moeite en zijn vermeld in de hall of fame [4]. De website van de IBD werd 112.716 maal bezocht met gemiddeld 3 pagina's per bezoek. In totaal zijn 88.615 documenten gedownload. De meest gedownloade documenten waren de BIO (3662 unieke downloads) en de standaardverwerkersovereenkomst (2803 unieke downloads). Het websitebezoek is ten opzichte van 2018 bijna verdubbeld.

De IBD registreerde 144 informatiebeveiligingsincidenten met een hulpvraag van gemeenten [5]. Hierbij verleende de IBD op afstand assistentie in de vorm van bijvoorbeeld analyse van logbestanden, woordvoerings- en communicatieadvies en advies over aanvullende maatregelen om herhaling van incidenten te voorkomen. Eén maal is de hulp van andere gemeenten ingeroepen om een gemeente bij te staan na een incident. Deze vorm van gemeentelijke bijstand bleek zeer goed te werken en we noemen dit voortaan het gemeentelijk responsnetwerk (GRN).

De BIO: Risicomanagement centraal

Het afgelopen jaar was het overgangsjaar naar een uniform normenkader voor informatiebeveiliging samen met de rijksoverheid, de waterschappen en de provincies: de Baseline Informatiebeveiliging Overheid (BIO) [6]. Deze BIO is net als de eerdere baseline gebaseerd op de internationale ISO27001/2-standaard. Gemeenten krijgen met de BIO meer ruimte om vanuit risicomanagement de voor hen relevante maatregelen te treffen. De BIO positioneert de bestuurder en het management sterker in de sturende rol op het gebied van informatieveiligheid. Om nadere invulling te geven aan risicomanagement ontwikkelde de IBD een gemeentespecifiek ondersteuningsprogramma [7] voor de BIO in lijn met de bestaande en bekende aanpak van gemeenten. De gezamenlijke overheidsnorm is allesomvattend en gaat in op beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen). De risicogebaseerde aanpak betekent ook dat de grootste risico's als eerste dienen te worden aangepakt. In het kader van het verhogen van de digitale weerbaarheid van gemeenten biedt de IBD een prioritering van de belangrijkste maatregelen [8] en processen [9].

De IBD paste circa 70 bestaande kennisproducten aan op basis van de nieuwe norm. In het productenoverzicht op de website zijn de handreikingen en factsheets te vinden. Ook zijn in 2019 een aantal nieuwe producten geïntroduceerd waaronder de handreiking verhoging informatiebeveiligingsbewustzijn [10], de factsheet en toolkit veilige e-mail in het zorgdomein [11], de factsheet Gehackt, hoe nu verder? [12]. In vervolg op de bestaande IBD crisisgame maakte VNG Beleid een nieuwe cybergame gericht op gemeentelijke bestuurders [13].

Incidenten bij gemeenten

De IBD nam een toename waar van zogeheten CEO-fraude [14] en salarisfraude door middel van spear phishing. Hierbij wordt uit naam van een collega een verzoek gedaan voor een betaling. De criminelen gaan geraffineerd te werk en doen hun huiswerk: namen van medewerkers worden opgezocht op sociale media als LinkedIn en de verzoeken lijken legitiem. Er is altijd een soort tijdsdruk en een plausibele reden om dit tijdelijk buiten de bestaande afspraken af te handelen. De IBD adviseerde CISO's van gemeenten om te werken aan bewustwording bij de financiële afdeling om incidenten in het vervolg te voorkomen.
Doordat een medewerker van een gemeente na een phishing mail zijn inloggegevens had prijsgegeven werden uit naam van deze medewerker duizenden nieuwe phishingmails verstuurd. Dit had als gevolg dat de mailserver van de organisatie op een blacklist kwam waardoor de gehele e-mailcommunicatie meerdere weken niet beschikbaar was. Een verkeerd ingestelde firewall in combinatie met niet geüpdatete software zorgde ervoor dat criminelen bij een gemeente een cryptominer konden installeren om zo geld te verdienen. >>

De IBD zag meerdere niet geslaagde pogingen om ransomware te installeren bij gemeenten en samenwerkingsverbanden, waaronder bij de gemeente Lochem. Deze gemeente heeft de lessen van de hack [15] laten optekenen zodat andere gemeenten daarvan kunnen leren.

Privacy

Team privacy van de IBD ondersteunt gemeenten met het borgen van privacy en gegevensbescherming in de organisatie. Het borgingsdocument [16] en het voorbeeld van de jaarrapportage [17] biedt gemeenten een handzaam format om verantwoording af te leggen en hun prioritering te kunnen bepalen. De nieuwe AVG-contentbibliotheek [18] biedt een basisset aan vragen en antwoorden over privacybewustzijn en kennis over de AVG. De bibliotheek kan door gemeenten en leveranciers gebruikt worden voor bewustwordingstools en -systemen. Sinds 2019 is het voor gemeenten mogelijk om Data Protection Impact Assessments (DPIA) gestructureerd uit te voeren met behulp van de DPIA-tool op onze website [19]. De tool maakt het mogelijk om resultaten onderling te delen voor hergebruik door andere gemeenten. Inmiddels zijn zo'n 150 DPIA's gedeeld. De DPIA op het gebruik van Whatsapp-zakelijk [20] van de IBD is ook beschikbaar voor hergebruik. Samen met 11 gemeenten is een documentenset voor Privacy by Design [21] voor gemeenten uitgewerkt. Begin 2020 zal deze set worden gepubliceerd.

In de Algemene Ledenvergadering van juni 2019 [22] is de standaard verwerkersovereenkomst (VWO) [23] tot gemeentelijke standaard verklaard, volgens het principe van verplichtende zelfregulering. 2019 gold als overgangsjaar. Uit een enquête blijkt dat 98% van de gemeenten inmiddels het document als standaard heeft omarmd.

Projecten van gemeenten

De IBD is in projecten van gemeenten betrokken als adviseur over privacy, gegevensbescherming en informatiebeveiliging, waaronder o.a.: de projecten PGB 2.0 [24] Regie op Gegevens met De Blauwe Knop [25], DPIA op de Digitaal Stelsel Omgevingswet (DSO) [26] en nID [27], Common Ground: Uitvoeren DPIA op de logging binnen NLX [28], DPIA op - en samenwerking met het projectteam GGI-Veilig [29], advies over GGI-Afspraken [30] i.v.m. Cloudcomputing, review beveiligingseisen voor een aantal collectieve aanbestedingen: 14+ netnummer en GT-Print [31] en het beoordelen van beveiligingseisen voor gemeenten voor de invoering van de Wvggz [32]. Ook werkte de IBD nauw samen met het beheerteam ENSIA [33] bij de transitie naar de BIO.

Kennisdeling en -vermeerdering

In 2019 organiseerde de IBD 17 regiobijeenkomsten verspreid door het land, 8 voor privacy en 9 voor informatiebeveiliging. Zo'n 200 burgemeesters speelden onder leiding van de IBD de crisisgame[34] tijdens de jaarlijkse bijeenkomsten van het Nederlands Genootschap van Burgemeesters. Uit de nabespreking bleek dat veel burgemeesters meer contact met hun IT-afdelingen zoeken, om meer gevoel te krijgen bij de impact van een informatiebeveiligingscrisis. Het voornemen om een kop koffie te drinken met hun CISO om te kijken hoe het in de gemeente gesteld is met informatieveiligheid en te vragen waar hij of zij van wakker van ligt is daarbij een eerste start. Voor privacyofficers / FG's organiseerde de IBD in samenwerking met de VNG Academie een serie tweedaagse trainingen over adviesvaardigheden [35]. Een aantal nieuwe workshops is toegevoegd aan het portfolio, waaronder de BIO voor kleine gemeenten en de 10 geboden voor de CISO. Inmiddels zijn er 16 workshops beschikbaar voor CISO's [36] van gemeenten.

De IBD stelde in 2019 ook een aantal nieuwe instrumenten beschikbaar waar gemeenten zelf mee aan de slag kunnen. In samenwerking met Agentschap Telecom van het Ministerie van Economische Zaken en Klimaat publiceerde de IBD ook een serious game over het thema 'telekwetsbaarheid' [37]. Met steun van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ontwikkelde de IBD de Privacy Pubquiz [38], alle gemeenten, waterschappen en provincies ontvingen het pubquiz promotiepakket inclusief een zakje borrelnootjes. De IBD nam ook het initiatief om aan te sluiten bij collectieven van privacy- en informatiebeveiligingsfunctionarissen van gemeenten. De IBD heeft sinds afgelopen jaar een zogenaamde CISO-stoel, een plaats voor een gemeentelijke CISO om voor twee dagen per week mee te draaien in het team. Geert van Uijthoven van de A2-samenwerking draaide in 2019 zes maanden lang twee dagen per week met ons mee en vertelt in een blog over zijn ervaring [39]. Gemeenten kunnen via het VNG Forum AVG [40] informatie over privacy en gegevensbescherming met elkaar delen, vragen aan elkaar stellen en documenten uitwisselen. De IBD onderhoudt ook nauw contact met leveranciers van gemeenten. Zo ontvangen zij ook kwetsbaarheidswaarschuwingen en belangrijke meldingen vanuit de CERT en houden wij de leveranciers periodiek op de hoogte van de belangrijkste ontwikkelingen op het gebied van informatiebeveiliging en privacy. Ook namen we deel aan de leveranciersbijeenkomsten van VNG Realisatie en organiseerden we een eigen leveranciersbijeenkomst over de BIO en Privacy by Design.

Verhogen digitale weerbaarheid (VDW)

Het programma Verhogen Digitale Weerbaarheid [41] biedt gemeenten een stapsgewijze aanpak om de meest belangrijke en urgente processen en maatregelen in de gemeente te implementeren. Bij de implementatie van de BIO genieten deze maatregelen en processen prioriteit.

>>

Bekijk de producten in ontwikkeling op onze website:
https://www.informatiebeveiligingsdienst.nl/project/producten-in-ontwikkeling/

*** TLP-Wit**

Deze informatie wordt met u gedeeld onder TLP-Wit. Dit houdt in dat de informatie vrij verspreid mag worden, voor zover de verspreiding niet strijdig is met de wet zoals bijvoorbeeld de wet op het auteursrecht

Weten wat je hebt (configuratiebeheer), actueel houden van hard- en software (patchmanagement) en bewaken wie wat mag (gebruikers- en rechtenbeheer) in combinatie met maatregelen als twee-factorauthenticatie en een goed ingericht incidentproces voorkomt het merendeel van de incidenten. Om op het onderwerp configuratiemanagement ook concreet ondersteuning te bieden zijn in het najaar voorbereidingen getroffen voor een netwerkinventarisatie (NWI) pilot op locatie. Hiermee stellen we gemeenten in staat om geautomatiseerd een inventarisatie te maken van alle hard- en software op het interne netwerk.

Doorkijk naar 2020

De IBD zet in 2020 de ingezette lijn voort van de stapsgewijze en geprioriteerde aanpak van het verhogen van de digitale weerbaarheid van gemeenten. In 2020 start de daadwerkelijke netwerkinventarisatie op locatie bij gemeenten. Ook start de detectie en monitoring bij gemeenten in het kader van GGI Veilig. We streven ernaar om de informatiepositie bij gemeenten rondom actuele dreigingen te optimaliseren. We zullen nauw samenwerken met de SIEM/SOC voorziening van GGI Veilig.

De IBD zal gemeenten ondersteunen bij de interpretatie en de opvolging van de meldingen die hieruit voortkomen.

Samen met VNG beleid werken we aan het vergroten van het handelingsperspectief voor gemeentebestuurders en -managers. De eerste prioriteit is een succesvolle en gemeentebrede implementatie van de BIO geprioriteerd volgens het programma Verhogen Digitale Weerbaarheid. Een van de instrumenten die we hierbij onderzoeken is een volwassenheidsmodel dat antwoord geeft op de vraag: waar staat mijn gemeente na een succesvolle implementatie van de BIO en wat zijn de meest effectieve vervolgstappen in deze fase. Een ander instrument dat we verkennen is een integrale risicomanagementtool.

De CERT van de IBD werkt nauw samen met het Nationaal Cyber Security Centrum (NCSC)[42] en zal naar verwachting begin 2020 door de minister van Justitie en Veiligheid worden aangewezen als sectorale CERT als onderdeel van een landelijk dekkend stelsel. In 2020 verkennen we of en hoe we de verbinding kunnen maken met een bredere doelgroep van overheidspartijen waar gemeenten veel mee samenwerken zoals waterschappen, provincies en veiligheidsregio's. VNG heeft in 2019 gewerkt aan een ontwikkeling van de agenda digitale veiligheid, waarin onder meer de gemeentelijke weerbaarheid een gespecificeerde actielijn is. We verkennen in dit kader een mogelijke verbreding en verdieping van onze dienstverlening in nauwe samenspraak met VNG Beleid.

De IBD zal voor het thema privacy in 2020 nog steviger inzetten op de collectieve aanpak. Dit doen we met behulp van bijvoorbeeld vooringevulde verwerkersovereenkomsten of door het uitvoeren generieke DPIA's. Ook voor privacy werken we samen met gemeenten volwassenheidsniveaus uit waardoor meer grip op privacy ontstaat. Volwassenheidsniveaus worden in 2020 toegevoegd aan het borgingsproduct. Zowel online als offline stimuleren we kennisdeling tussen gemeenten. Bijvoorbeeld door complexe casuïstiek in werkgroepen te bespreken of actief opvolging te geven op discussies op het VNG AVG Forum.

In 2020 brengt de IBD wederom een dreigingsbeeld uit, dat we zullen hernoemen naar het informatiebeveiligings- en privacybeeld gemeenten.

Het team van de IBD per 1 december 2019 [43]

Jaaroverzicht

De IBD stuurt het jaaroverzicht aan de contactpersonen voor informatiebeveiiging en privacy. Indien u vragen of opmerkingen heeft, kunt u contact opnemen met de ibd via info@ibdgemeenten.nl of privacy@VNG.nl.

*** TLP-Wit**

Deze informatie wordt met u gedeeld onder TLP-Wit. Dit houdt in dat de informatie vrij verspreid mag worden, voor zover de verspreiding niet strijdig is met de wet zoals bijvoorbeeld de wet op het auteursrecht

Links in dit jaaroverzicht

1 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving
2 https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/
3 https://www.informatiebeveiligingsdienst.nl/responsible-disclosure/
4 https://www.informatiebeveiligingsdienst.nl/responsible-disclosure/2019-responsible-disclosure-hall-of-fame/
5 https://www.informatiebeveiligingsdienst.nl/ondersteuning-bij-incidenten/
6 https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/
7 https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/#IB
8 https://www.informatiebeveiligingsdienst.nl/product/vdw-module-1-mindmap-maatregelen/
9 https://www.informatiebeveiligingsdienst.nl/product/vdw-module-1-mindmap-processen/
10 https://www.informatiebeveiligingsdienst.nl/product/handreiking-verhogen-bewustzijn-informatiebeveiliging/
11 https://www.informatiebeveiligingsdienst.nl/product/factsheet-en-toolkit-veilige-e-mail-in-het-zorgdomein/
12 https://www.informatiebeveiligingsdienst.nl/product/factsheet-gehackt-hoe-nu-verder/
13 https://vng.nl/nieuws/nieuwe-cybergame-officieel-gelanceerd
14 https://www.informatiebeveiligingsdienst.nl/blog/blog-maak-medewerkers-bewust-van-ceo-fraude/
15 https://www.informatiebeveiligingsdienst.nl/product/leren-van-lochem-lessen-uit-een-informatiebeveiligingsincident/
16 https://www.informatiebeveiligingsdienst.nl/product/criteria-borging-avg-borgingsproduct-gegevensbescherming-in-de-gemeentelijke-organisatie/
17 https://www.informatiebeveiligingsdienst.nl/nieuws/voorbeeld-jaarrapportage-fg-voor-college-en-gemeenteraad-beschikbaar/
18 https://www.informatiebeveiligingsdienst.nl/product/privacy-avg-contentbibliotheek/
19 https://community.informatiebeveiligingsdienst.nl/gebruik-dpia-tool-ibd/
20 https://www.binnenlandsbestuur.nl/digitaal/nieuws/beperkt-privacyrisico-bij-gebruik-whatsapp.11823525.lynkx
21 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf
22 https://vng.nl/artikelen/agenda-en-stukken-alv-2019
23 https://www.informatiebeveiligingsdienst.nl/project/verwerkersovereenkomst-gemeenten/
24 https://www.vngrealisatie.nl/producten/ontwikkeling-en-implementatie-pgb20
25 https://www.vngrealisatie.nl/producten/blauweknop
26 https://aandeslagmetdeomgevingswet.nl/digitaal-stelsel/documenten/privacy-impact-assessment/
27 https://www.vngrealisatie.nl/producten/nid-stelsel-privacy-een-informatiemaatschappij
28 https://nlx.io/
29 https://www.vngrealisatie.nl/producten/ggi-veilig
30 https://www.vngrealisatie.nl/producten/ggi-afspraken
31 https://www.vngrealisatie.nl/Gezamenlijke-inkoop-en-beheer
32 https://www.dwangindezorg.nl/wvggz
33 https://www.vngrealisatie.nl/ensia
34 https://vng.nl/nieuws/lochemconferentie-2019-waardevol-digitaliseren-en-innoveren
35 https://www.vngacademie.nl/Training/ibd--daagse-training-advies--en-toezichtvaardigheden-voor-fgs-en-pos/ea5b66d3-1fd6-403e-9de2-1299d9855d99
36 https://www.informatiebeveiligingsdienst.nl/workshops-informatiebeveiliging/
37 https://www.informatiebeveiligingsdienst.nl/nieuws/serious-game-telekwetsbaarheid-biedt-inzicht-in-gevolgen-van-uitval-telecom/
38 https://www.informatiebeveiligingsdienst.nl/privacy-pubquiz/
39 https://www.informatiebeveiligingsdienst.nl/blog/blog-ervaringen-bij-de-ibd/
40 https://forum.vng.nl/do/login
41 https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/
42 https://www.ncsc.nl/
43 https://www.informatiebeveiligingsdienst.nl/medewerkers-van-de-ibd/