Brief aan de leden
T.a.v. het college en de raad

Datum
7 januari 2019

Ons kenmerk
TIS/U201801170
Lbr. 19/002

Telefoon
(070) 373 8393

Bijlage(n)
2

Onderwerp
Standaardverklaring Baseline Informatiebeveiliging Overheid

Samenvatting
Informatieveiligheid is een randvoorwaarde voor een professionele gemeente. We werken steeds meer samen in een vernetwerkte overheidsomgeving. Daarbij moeten we impliciet kunnen vertrouwen op een adequaat beveiligingsniveau van ketenpartners. Gemeenten, Rijk, waterschappen en provincies gaan daarom over op één uniform normenkader voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). Voor gemeenten is 2019 voorzien als voorbereidingsjaar. Op 1 januari 2020 is de BIO de officiële richtlijn op het gebied van informatiebeveiliging die alle gemeenten volgen.

Met de BIO is informatiebeveiliging meer dan voorheen een zaak van de bestuurder. Als bijlage bij deze ledenbrief ontvangt u daarom ter ondersteuning 'De 10 bestuurlijke principes voor informatiebeveiliging.

Verder zend ik u ter kennisname het onlangs verschenen Dreigingsbeeld Nederlandse Gemeenten 2019 toe. In dit dreigingsbeeld worden de belangrijkste risicofactoren rond gemeentelijke informatieveiligheid geduid. Net als voorgaand jaar zijn de belangrijkste risico's te vinden in het imago en menselijk handelen. Bestuurlijk een relevant onderwerp. Het dreigingsbeeld biedt mede in het licht van de BIO een handelingsperspectief om de belangrijkste risico's aan te pakken. Wij adviseren u dit dreigingsbeeld met uw gemeentelijke CISO te bespreken en voor uw gemeente passende acties te initiëren.

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

Aan de leden

Datum
7 januari 2019

Ons kenmerk
TIS/U201801170
Lbr. 19/002

Telefoon
(070) 373 8393

Bijlage(n)
2

Onderwerp
Standaardverklaring Baseline Informatiebeveiliging Overheid

Geacht college en gemeenteraad,

Via deze weg willen wij u graag informeren over de standaardverklaring van de Baseline Informatiebeveiliging Overheid (BIO) per 1 januari 2020.

Aanleiding

In de buitengewone algemene ledenvergadering op 30 november 2018 hebben gemeenten ingestemd met het proces van standaardverklaring. Dat maakt Samen Organiseren mogelijk. Samen Organiseren is het vliegwiel voor het verbinden en versnellen van de Gezamenlijke Gemeentelijke Uitvoering (GGU). Echt samen organiseren houdt in dat gemeenten standaarden afspreken. Daarmee worden ook kosten voor individuele gemeenten bespaard (één keer ontwikkelen, 355 maal toepassen). Voor standaarden in informatiebeleid, informatietechnologie en dienstverlening hebben gemeenten het College van Dienstverleningszaken (CvD) in het leven geroepen. De BIO is de eerste standaard waarover het CvD positief advies heeft afgegeven aan het VNG Bestuur. Het bestuur heeft hier positief op gereageerd en de BIO tot standaard verklaard per 1 januari 2020.

Aanvullend zijn daarbij ook "De 10 bestuurlijke principes voor informatiebeveiliging" tot standaard verklaard die de bestuurder ondersteunen in de aansturing van informatieveiligheid. De BIO is eveneens interbestuurlijk bekrachtigd in het Overheidsbrede overleg Digitale Overheid (OBDO).

Informatiebeveiliging meer dan voorheen zaak van bestuurder

Informatieveiligheid is een randvoorwaarde voor een professionele gemeente. We werken steeds meer samen in een vernetwerkte overheidsomgeving. Daarbij moeten we impliciet kunnen vertrouwen op een adequaat beveiligingsniveau van ketenpartners. Gemeenten, Rijk, waterschappen en provincies gaan daarom over op één uniform normenkader voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). Voor gemeenten is 2019 voorzien als voorbereidingsjaar. Op 1 januari 2020 is de BIO de officiële richtlijn op het gebied van informatiebeveiliging die alle gemeenten volgen.

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

Verandering voor gemeenten: risicomanagement centraal
De BIO betekent een verandering voor gemeenten. Ten opzichte van de huidige Baseline Informatiebeveiliging Gemeenten (BIG) worden bijna 200 maatregelen niet meer genoemd. Gemeenten krijgen zo meer ruimte om voor hen op basis van het risico relevante maatregelen te treffen. De maatregelen uit de BIG die in de BIO nog wel worden genoemd gelden als verplicht voor alle overheden. De BIO positioneert de bestuurder en het management sterker dan voorheen in de rol waarin hij of zij risico-gebaseerd stuurt op het gebied van informatieveiligheid. Zij zullen hierover op het advies van de betrokken Chief Information Security Officers afspraken moeten maken. Ter ondersteuning daarbij zijn 'De 10 bestuurlijke principes voor informatiebeveiliging' vastgesteld. Ze dienen als handvatten voor dat gesprek.

De 10 bestuurlijke principes voor informatiebeveiliging:

1. Bestuurders bevorderen een veilige cultuur
2. Informatiebeveiliging is van iedereen
3. Informatiebeveiliging is risicomanagement
4. Risicomanagement is onderdeel van de besluitvorming
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
6. Informatiebeveiliging is een proces
7. Informatiebeveiliging kost geld
8. Onzekerheid dient te worden ingecalculeerd
9. Verbetering komt voort uit leren en ervaring
10. Het bestuur controleert en evalueert

Standaardisering van informatiebeveiliging
Met de vaststelling van de Gezamenlijke Gemeentelijke Uitvoering en het Jaarprogramma 2019 kiezen we er als gemeenten voor om gezamenlijk te standaardiseren in de uitvoering van beleidsarme thema's, en een nieuwe gemeenschappelijke en generieke (sectoronafhankelijke) basisinformatievoorziening te realiseren. Standaarden kunnen in belangrijke mate bijdragen aan het realiseren van gezamenlijke uitvoeringskracht en daarmee ruimte voor maatwerk op terreinen waarop gemeenten het verschil willen maken. De BIO is de eerste standaard waarover het College van Dienstverleningszaken (CvD) positief advies heeft afgegeven aan het VNG Bestuur. Het bestuur heeft hier positief op gereageerd en de BIO daarmee verbindend verklaard voor gemeenten per 1 januari 2020. De baseline is interbestuurlijk bekrachtigd in het Overheidsbrede overleg Digitale Overheid (OBDO).

De belangrijkste reden voor de interbestuurlijke adoptie van de BIO is het samenwerken in een vernetwerkte overheidsomgeving, waarbij we impliciet moeten kunnen vertrouwen op een adequaat beveiligingsniveau van ketenpartners. Het bestaan van meerdere overheidsbaselines is bovendien niet efficiënt. De BIO zorgt voor een overheidsbrede standaardisatieslag en sluit aan bij de voor de markt geldende NEN-ISO 27002:2013 norm. Daarop zijn een tweetal aanvullingen op de standaard gekomen die op details ingaan, maar geen afbreuk doen aan de principes zoals deze in de NEN 2013 geformuleerd staan. Deze NEN 2013 is de meest recente basis. Als gemeente kunt u er daarmee op vertrouwen dat u én de andere overheidspartners met deze BIO aan de meest recente normen voldoet.

IBD ondersteunt ambtelijke organisatie
Voor de jaren 2018 en 2019 verantwoorden gemeenten zich nog over de BIG. Voor het jaar 2020 zal de verantwoording zijn aangepast aan de BIO. Voor de inrichting van informatiebeveiligingsmaatregelen kunnen gemeenten gebruik maken van de ondersteuningsproducten van de IBD. De bestaande producten worden momenteel aangepast aan de BIO en komen in het eerste halfjaar van 2019 beschikbaar. Andere ondersteuningsproducten, zoals een quickscan, worden voor de gezamenlijke overheidslagen onder regie van het Rijk ontwikkeld en door de IBD toepasbaar gemaakt voor gemeenten. Aanvullend ontwikkelt de VNG een ondersteuningsprogramma gericht op het management en het bestuur van gemeenten.

Mocht u als bestuurder op de hoogte willen zijn van de voor uw gemeente relevante dreigingen en risico's dan kan het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020 u op weg helpen. Het dreigingsbeeld laat zien dat de belangrijkste beveiligingsrisico's niet zozeer technisch van aard zijn, maar met name liggen in de eigen organisatie (waaronder het menselijk handelen) en in de samenwerking met ketenpartners. We adviseren u hierover met uw CISO in gesprek te gaan en met deze functionaris voor uw gemeente passende acties te initiëren.

Met vriendelijke groet,

Vereniging van Nederlandse Gemeenten

J. Kriens
Algemeen directeur

INFORMATIE
BEVEILIGINGS
DIENST

Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020

VNG Realisatie

Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020

INFORMATIE
BEVEILIGINGS
DIENST

De IBD heeft het *Dreigingsbeeld 2019/2020* opgesteld op basis van een analyse van incidentrapportages van gemeenten, meldingen aan de IBD en een analyse van andere bronnen, zoals het *Cybersecuritybeeld Nederland* (CBSN). Daarnaast zijn er interviews afgenomen bij gemeenten, de *Computer Emergency Responce Teams* (CERT's) van andere organisaties en enkele leveranciers van gemeentelijke ICT-diensten.

Het *Dreigingsbeeld informatiebeveiliging Nederlandse Gemeenten* verschijnt vanaf nu iedere twee jaar.

Informatiebeveiliging = risicomanagement

Het dreigingsbeeld 2019/2020 biedt een handvat om de informatiebeveiliging verder te verbeteren en daarmee de digitale weerbaarheid van uw gemeente verhogen. Het IBD geeft u inzicht in de belangrijkste bedreigingen en ontwikkelingen, en adviseert over de prioriteiten voor de komende jaren.

Informatiebeveiliging gaat verder dan ICT alleen. Beveiliging van gegevens en systemen is een zaak van uw hele organisatie. Het gaat om de mensen in uw organisatie, om de manier waarop zij met risico's omgaan. Het gaat om het inrichten van processen en procedures, om kennis en bewustzijn. En in de laatste plaats pas om techniek. Of de dreiging nu komt van een onbewuste medewerker, een criminele organisatie of een stroomstoring: de technische en organisatorische maatregelen om schade te voorkomen, te beperken en te vermijden zijn hetzelfde. Risicomanagement is de basis van een goede informatiebeveiliging.

De risico's van een slechte informatiebeveiliging zijn talrijk: privacyschendingen door een datalek, economische schade door het uitlekken van vertrouwelijke plannen, fysieke schade door storingen in systemen in de openbare ruimte. En de rijksoverheid noemt in het CSBN informatiediefstal door criminele organisaties, vertaald naar gemeenten betekent dit ondermijning van gemeentelijke processen.

Gemeentelijke bestuurders zijn verantwoordelijk voor de informatiebeveiliging van de gemeente. Zij bepalen hoeveel risico de gemeente wil lopen. De lijnmanager is verantwoordelijk voor de inrichting van processen en systemen zodat de risico's teruggebracht worden tot een acceptabel niveau.

Inwoners en ondernemers moeten erop kunnen vertrouwen dat hun gegevens veilig zijn, dat de informatie die de gemeente uitwisselt met andere overheden betrouwbaar is en dat de gemeente zorgt voor een veilige leefomgeving. Betrouwbare informatie is de belangrijkste grondstof voor een gemeente om haar werk goed te kunnen doen. Hiervoor is informatiebeveiliging een randvoorwaarde.

Risico's en prioriteiten

Risico's 2019–2020

Imagoprobleem informatiebeveiliging

Laag op de politieke agenda, weinig bewustzijn en onvoldoende budget.

› *pag. 10*

Risico's niet integraal in beeld

De risico's die wel in beeld zijn, krijgen bovenmatig veel aandacht

› *pag. 11*

Basis niet op orde

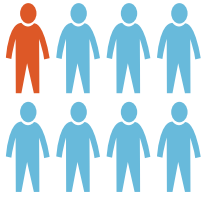
Simpele routine-aanvallen zijn vaak succesvol

› *pag. 12*

Te weinig mensen

Te veel werk, en te weinig gekwalificeerde specialisten

› *pag. 12*



Complexiteit neemt toe

Gemeenten zien kansen van innovatie, maar niet de risico's

› *pag. 13*

Prioriteiten 2019–2020

Informatiebeveiliging op de agenda

Zorg ervoor dat informatie-beveiliging aandacht krijgt.

› *pag. 16*

De basis op orde

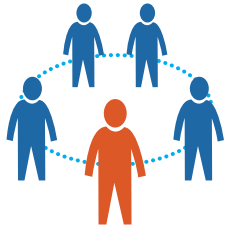
Verhoog de digitale weer-baarheid van uw gemeente.

› *pag. 17*

Versterk de menselijke schakel

Bewuste medewerkers zijn de beste beveiligings-maatregel.

› *pag. 18*



Versterk de CISO

Stel de CISO in staat om u optimaal te kunnen adviseren.

› *pag. 18*

Inzicht in nieuwe technologieën

Pas *security- & privacy-by-design*-principes toe.

› *pag. 19*

Incidenten oktober 2017–juli 2018

Soort

Beschikbaarheid

Sabotage **3**

DOS/DDOS **10**

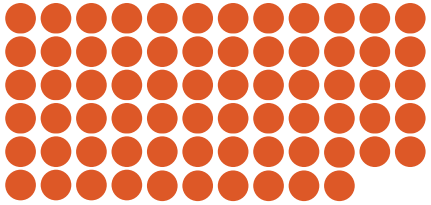
Fraude

Illegaal naamgebruik **6**

Onrechtmatig gebruik resources **8**

Informatiebeveiliging

Ongeauthenticeerde modificatie **7**



Ongeauthenticeerde toegang **70**

Malafide materiaal

Copyright **1**

Kinderporno, rascisme, oproep tot haat **2**

Spam **10**

Malware

Command & Control server **5**

Distributie **2**

Infectie **4**

Poging tot binnendringen

Inlogpoging **1**

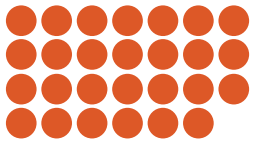
Misbruik kwetsbaarheid **8**

Succesvolle inbraak

Compromitatie van account **16**

Exploitatie kwetsbaarheid **35**

Verzamelen van informatie



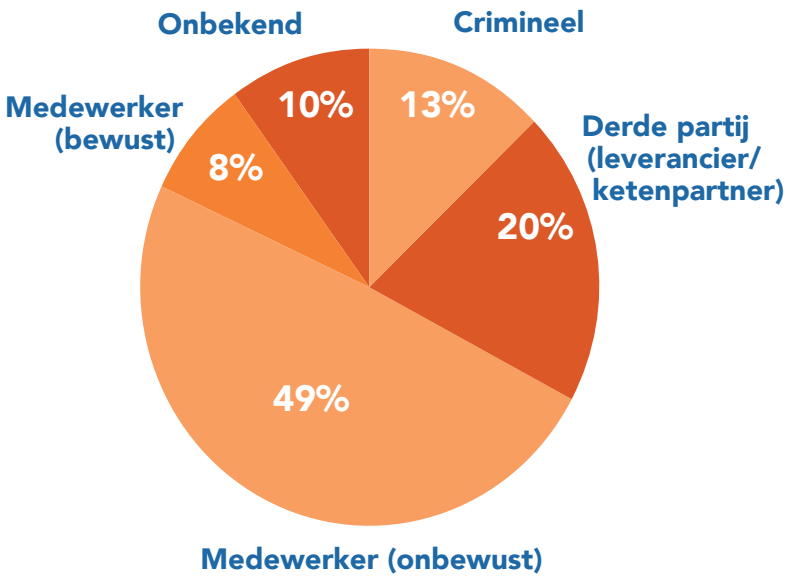
Phishing **27**

Scannen **16**

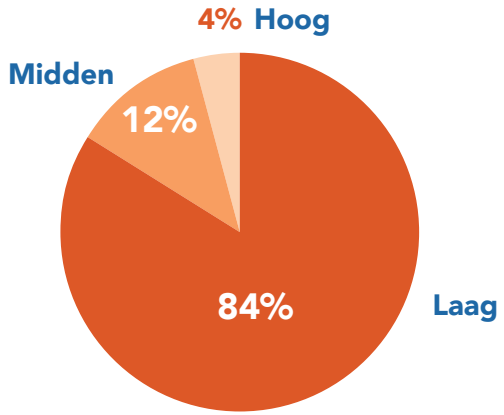
Sniffen **2**

Incidenten oktober 2017–juli 2018

Door wie



Impact



Totaal

Totaal aantal incidenten 429

Incident melden bij de IBD

De IBD telt incidenten op basis van meldingen en informatie uit incidentrapportages van gemeenten. In totaal zijn er in deze periode 429 geteld. Is er een informatiebeveiligingsincident in uw gemeente? Meld dit dan bij het IBD via www.informatiebeveiligingsdienst.nl. Zo helpt u ons een volledig beeld te krijgen, ook van de incidenten waarbij geen ondersteuning van de IBD nodig is.

Risico's

De belangrijkste risico's voor de gemeentelijke informatieveiligheid zijn:

1. Informatiebeveiliging kampt met imagoprobleem;
2. Inzicht in risico's is niet integraal;
3. Aanvallen succesvol door ontbreken basismaatregelen;
4. Te veel werk voor te weinig mensen;
5. De complexiteit neemt toe.

1. Informatiebeveiliging kampt met een imagoprobleem

De IBD analyseerde 331 recente coalitieakkoorden van gemeenten. Hieruit blijkt dat beveiliging van informatie niet op de politieke agenda's staat. Alles wat direct en zichtbaar bijdraagt aan de dienstverlening aan inwoners en ondernemers kan rekenen op veel belangstelling vanuit politiek, bestuur en management. Maar informatiebeveiliging heeft niet het imago direct bij te dragen aan dienstverlening. Het wordt gezien als bijzaak, en soms zelfs als drempel of last. Informatiebeveiliging en privacy worden vaak pas in een laat stadium betrokken, terwijl de gevolgen van incidenten juist ook voor de bedrijfsvoering van uw gemeente groot kunnen zijn. Incidenten kunnen ervoor zorgen dat een gemeente tijdelijk niet in staat is om inwoners en ondernemers van dienst te zijn.

Het gevolg van het negatieve imago is dat er vaak geen of onvoldoende budget is gereserveerd voor informatieveiligheid. En als het er is, zit het verstopt in het ICT-budget. Dit heeft als risico dat het geld naar andere prioriteiten gaat. Zonder vast budget voelen lijnmanagers de verantwoordelijkheid voor de beveiliging van hun dienst of product onvoldoende. Informatiebeveiliging komt in de verantwoording over output en financiën niet aan de orde. Lijnmanagers sturen op output en financiën, niet op het managen van risico's in de informatiebeveiliging.

2. Inzicht in risico's is nog onvoldoende integraal

Informatiebeveiliging gaat over beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen. Gemeenten geven aan dat zij in veel gevallen onvoldoende zicht hebben op risico's die dit in gevaar brengen. Risico's binnen én buiten de gemeentelijke organisatie, bijvoorbeeld bij leveranciers of in samenwerkingsverbanden.

Gemeenten zijn kwetsbaar voor cybersecurity-incidenten. Uit de interviews blijkt dat gemeenten zich het meeste zorgen maken over de bescherming van persoonsgegevens en verstoring van de ICT-systemen. Er zijn daarnaast ook processen die kwetsbaar zijn voor beïnvloeding van buitenaf. Bijvoorbeeld verkiezingen, maar ook vergunningsprocessen en processen in het domein van werk en inkomen.

Gemeenten hebben niet eenduidig vastgelegd welke systemen, informatie en processen beschermd moeten worden. Informatie over incidenten en maatregelen is wel beschikbaar, maar verspreid door de hele organisatie. Gemeenten zijn daarnaast vaak afhankelijk van externe leveranciers voor ICT-voorzieningen en de beveiliging daarvan. Ook werken gemeenten veel samen in Gemeenschappelijke Regelingen, dit maakt het naleven van een uniforme werkwijze rondom informatieveiligheid en privacy erg complex.

Onvoldoende zicht op de risico's zorgt er daarnaast voor dat de risico's die wel in beeld zijn bovenmatig veel aandacht krijgen.

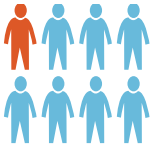
3. Aanvallers blijven succesvol door ontbreken basismaatregelen

Aanvallers hebben vaak niet meer nodig dan een niet bijgewerkt stukje software of een klik op een phishingmail om toegang te krijgen tot systemen. Gemeenten kunnen veel voorkomende incidenten voorkomen met behulp van enkele essentiële basismaatregelen. Zij hebben hier nog stappen in te zetten, met name op het gebied van basisbeveiligingsprocessen, basis ICT-processen en bewustwording.

Uit de interviews en incidentrapportages blijkt dat gemeenten nog niet weerbaar genoeg zijn. Basisprocessen zoals omgaan met incidenten, het bijwerken van hard- en software, het bijhouden van overzicht in de ICT-huishouding en het bijhouden van wijzigingen hierin (incidentmanagement, patchmanagement, configuratiemanagement en changemanagement) zijn nog niet goed genoeg op orde. Het ontbreekt vaak aan inzicht in eerdere incidenten, en de kosten van incidenten en verstoringen. Ook weet niet iedereen in de organisatie wat er voor nodig is om apparatuur en software up-to-date te houden.

Optimale digitale veiligheid is noodzakelijk voor het functioneren van de steeds intensiever gedigitaliseerde gemeente. Basismaatregelen bieden een robuuste barrière tegen digitale dreigingen.

4. Te veel werk voor te weinig mensen



Overheid en bedrijfsleven putten uit dezelfde groep informatiebeveiligingsprofessionals. Maar gemeenten kunnen de salarissen die de markt betaalt nauwelijks evenaren. Er ontstaan problemen wanneer ervaren medewerkers de organisatie verlaten en er nieuwe moeten worden aangenomen. Er zijn te weinig mensen, en er is te veel werk. Informatiebeveiligingsprofessionals bij gemeenten besteden relatief veel tijd aan verantwoording in zelfassessments en audits. Dit gaat ten koste van de tijd die zij kunnen steken in de informatiebeveiliging.

Informatiebeveiliging draait om risicomanagement. Het doen van onderzoeken maakt hier principieel deel van uit. Inherent daaraan is structureel gelegenheid nodig voor onderzoek en advies ten aanzien van digitale risico's. In de praktijk verdwijnt risicomanagement naar de achtergrond omdat de waan van de dag regeert. Men werkt incidentgedreven en is verder druk met de opvolging van audits en zelfassessments.

5. Complexiteit neemt toe

De digitale weerbaarheid van gemeenten staat onder druk door een toenemende complexiteit en connectiviteit in het ICT-landschap, nieuwe ontwikkelingen en door te weinig aandacht voor digitale veiligheid bij experimenten en innovatieve projecten.

Onderwerpen als Internet of Things (IoT), smart cities, big data, kunstmatige intelligentie (AI) en blockchain worden vaak opgepakt door domeinspecialisten. Zij zien vooral de voordelen van de nieuwe ontwikkelingen voor inwoners en ondernemers. Zaken als beheer, informatiebeveiliging en privacy worden gezien als beperkend voor de innovatie. Er is te weinig aandacht voor digitale veiligheid bij experimenten en innovatieve projecten. Hiermee ontstaat een schaduw-ICT, die los van de andere informatievoorziening bestaat. Dit vraagt om een multidisciplinaire aanpak met verschillende expertises. Dat begint bij het vaststellen van verantwoordelijkheid en eigenaarschap.

Trends en ontwikkelingen

De belangrijkste trends en ontwikkelingen voor de gemeentelijke informatieveiligheid zijn:

1. Aandacht voor privacy;
2. Baseline Informatiebeveiliging Overheid;
3. *Internet of things (IoT)*en *smart society*;
4. Kunstmatige intelligentie *(AI)*;
5. *Common Ground*.

1. Aandacht voor privacy door AVG

De invoering van de Algemene Verordening Gegevensbescherming (AVG) heeft voor een boost gezorgd in de aandacht voor de bescherming van persoonsgegevens. Een positieve ontwikkeling, want privacy is hierdoor een blijvend aandachtspunt voor gemeenten. Dit helpt de informatieveiligheid te vergroten.

2. Van BIG naar BIO

De Baseline Informatiebeveiliging Overheid (BIO) wordt het nieuwe normenkader voor alle overheden. Deze vervangt de Baseline Informatiebeveiliging Gemeenten (BIG). De huidige baselines van gemeenten, provincies, waterschappen en het rijk zijn allemaal nog gebaseerd op de NEN/ISO normen uit 2005 en lopen achter op de nieuwe normen uit 2013. Een gezamenlijk kader voorkomt dat alle overheidslagen voor zichzelf een nieuwe baseline moeten opstellen. De BIO wordt gezamenlijk beheerd, onder regie van het ministerie van Binnenlandse Zaken.

3. *Internet of things* en *smart society*

Smart society-projecten dragen bij aan het vergroten van de leefbaarheid en veiligheid binnen de gemeente. Voorheen 'domme' objecten, worden slim (*IoT*) en maken het besturen van de stad makkelijker. Bijvoorbeeld prullenbakken die zelf aangeven dat ze vol zitten, of parkeerplaatsen die zelf aangeven dat ze vrij zijn. Maar dit zet ook de informatieveiligheid verder onder druk. De IoT-apparatuur en -software die gemeenten hiervoor inzetten, zorgt voor meer risico's en kwetsbaarheden. Zeker als ook de scheiding tussen gemeentelijke ICT en IoT niet goed wordt geregeld, een verouderd cameraysteem in het gemeentelijke netwerk kan dan de entree zijn tot gegevens en systemen van de gemeente.

4. Kunstmatige intelligentie

Kunstmatige intelligentie of *artificial intelligence (AI)* biedt kansen voor gemeenten. AI kan gemeenten helpen om beter inzicht te krijgen in hun processen en gegevens, en daarmee zorgen voor een betere dienstverlening voor inwoners en ondernemers. Het is ook een beveiligingstool van de toekomst. Met AI kunnen betere veiligheidsanalyses worden gedaan van allerlei systeem- en netwerkinformatie. Hiermee hebben gemeenten sneller inzicht in mogelijke incidenten of inbraakpogingen. De technologie is echter nog erg onvolwassen en vormt daarmee een risico voor de bedrijfsvoering. Hackers kunnen dit in de toekomst gebruiken om in te breken op gemeentelijke systemen.

5. *Common Ground*

Met *Common Ground* wordt een grote stap gezet in de richting van een open, transparante overheid waarbinnen gegevens sneller en veiliger kunnen worden uitgewisseld, zowel intern als extern. *Common Ground* is een beweging waarin gemeenten werken aan een stapsgewijze modernisering van de ICT-infrastructuur. Naast aandacht voor privacy is er vanaf het begin ook veel aandacht voor informatieveiligheid.

Prioriteiten 2019/2020

Om de belangrijkste risico's te beheersen is een combinatie van technische en organisatorische maatregelen noodzakelijk. De IBD adviseert gemeenten voor 2019/2020 de volgende prioriteiten te stellen:

1. Zet informatiebeveiliging op de agenda van het college en zorg dat lijnmanagers verantwoordelijkheid kunnen nemen

Betrouwbare informatievoorziening is een randvoorwaarde voor de gemeente. Om dit te bereiken moet de top van de organisatie doordrongen zijn van het belang van informatiebeveiliging en een voorbeeldfunctie innemen. Alleen dan ontstaat er een cultuur waarbij voldoende aandacht is voor informatiebeveiliging.

Vaak denkt men dat de *Chief Information Security Officer* (CISO) verantwoordelijk is voor alle beveiligingsvraagstukken binnen de gemeente. Terwijl dit de taak is van proces-eigenaren of lijnmanagers. Lijnmanagers moeten weten wat het belang is van de processen waar zij verantwoordelijk voor zijn en daarnaast de risico's en bijbehorende beveiligingsmaatregelen kennen die verbonden zijn aan hun informatiesystemen. Hiervoor kunnen de lijnmanagers de baselinetoets uit de BIG uitvoeren en meer betrokken zijn bij strategisch risicomanagement.

Informatiebeveiliging is niet alleen een ICT-probleem. De budgetten voor informatiebeveiliging moeten inzichtelijk worden gemaakt per proces en systeem. Als de basis beheerprocessen en maatregelen op orde zijn, kan er een kosten-batenanalyse gemaakt worden van informatiebeveiliging. Blijf aandacht houden voor informatieveiligheid en privacy en zorg voor een cultuur waarin lijnmanagers worden aangesproken op het leveren van betrouwbare dienstverlening aan de burger.

Acties

- Benut de kansen van de AVG. Het onderwerp heeft nu volop de aandacht;
- Laat u periodiek bijpraten door uw CISO. Ga het gesprek aan en stuur actief op informatiebeveiliging;
- Betrek en informeer stakeholders door transparant via de *Planning & Control-cyclus* te rapporteren over informatieveiligheid;
- Richt een proces van risicomanagement in, beleg de verantwoordelijkheden en zorg dat lijnmanagers risicogestuurd hun werk kunnen doen;
- Elke lijnmanager moet zijn of haar risico's in beeld hebben en hiervoor een passend beveiligingsplan opstellen en actueel houden.

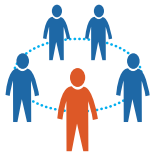
2. Breng de basis op orde

Gemeenten hebben een belangrijke rol in het leveren van betrouwbare dienstverlening. Betrouwbare informatie is de belangrijkste grondstof voor het werk van Nederlandse gemeenten, hiervoor is informatieveiligheid een randvoorwaarde. Basale beveiligingsprocessen en maatregelen zijn belangrijk om de digitale weerbaarheid van de gemeente te verhogen. De IBD helpt gemeenten bij het verhogen van de digitale weerbaarheid.

Acties

- Zorg ervoor dat de basisprocessen en maatregelen rondom beveiliging en beheer op orde zijn en beleg de processen bij de juiste verantwoordelijke;
- Laat de CISO regelmatig rapporteren over effectiviteit van deze processen aan het hogere management en het college (de bestuurlijke portefeuillehouder);
- Laat u (op tijd) adviseren door de CISO;
- Reserveer structueel budget voor informatieveiligheid;
- Deel uw beveiligingsincidenten en uw incidentrapportages met de IBD zodat de andere gemeenten hier ook van kunnen leren.

3. Versterk de menselijke schakel



De meeste incidenten worden nog steeds veroorzaakt door menselijk handelen. Dat beeld is ongewijzigd ten opzichte van het vorige Dreigingsbeeld. De medewerkers zijn zich onvoldoende bewust van de gevolgen van kleine menselijke fouten.

Het is verleidelijk om met technologie te proberen om alle gebruikergerelateerde beveiligingsincidenten terug te dringen. Maar technologie alleen is niet de oplossing. Informatiebeveiliging begint bij de bewuste medewerker.

Zorg er daarom voor dat er voldoende en regelmatige aandacht is voor bewustwording van de medewerkers. Bewuste medewerkers zijn uw belangrijkste verdedigingslinie tegen informatiebeveiligingsincidenten. Geef medewerkers de mogelijkheden om veilig te werken en zich bewust te worden van de risico's. Bestuurders moeten de medewerkers ervan doordringen dat informatiebeveiliging van iedereen is. Zij hebben een voorbeeldfunctie.

Acties

- Blijf zorgen voor bewustwording en training, herhaal deze en meet de resultaten;
- Zorg ook voor het verhogen van het kennisniveau van de technisch- en functioneel beheerders;
- Zorg ervoor dat medewerkers veilig kunnen handelen door het ter beschikking stellen van veilige tools en veilige bestandsuitwisseling.

4. Versterk de positie van de CISO

De CISO heeft een sleutelpositie binnen de gemeente om informatiebeveiliging te laten slagen. Een CISO moet zijn tijd verdelen tussen plannen, ondersteunen, controleren en bijsturen. Hiermee kan hij of zij op de juiste manier de juiste informatie beschikbaar stellen aan de de top van de gemeente. Een CISO moet de ruimte en de middelen krijgen en investeren in kennis en kunde om de gemeente weerbaarder te maken tegen huidige en toekomstige digitale dreigingen.

Acties

- Investeer in de CISO;
- Postitioneer de CISO strategisch en onafhankelijk binnen de gemeente;
- Geef de CISO de ruimte, mandaat en middelen om zijn of haar taak goed te kunnen uitvoeren.

5. Verbeter het inzicht in de risico's van nieuwe technologieën

Er komen technologische veranderingen op de gemeente af. Deze zorgen voor nieuwe kwetsbaarheden en risico's. Maak de juiste mensen verantwoordelijk voor deze ontwikkelingen en betrek vanaf het beginstadium de CISO en de verantwoordelijke lijnmanagers. Zo krijgt u vroegtijdig inzicht in kwetsbaarheden en risico's en kan hier direct op worden ingespeeld. Technologische ontwikkelingen raken de gehele gemeente.

Acties

- Nieuwe technologieën vereisen een gedegen aanpak om tijdig kwetsbaarheden en risico's te onderkennen;
- Doe in een vroeg stadium een impactanalyse (gegevensbeschermingseffectbeoordeling of DPIA);
- Pas *security- en privacy-by-design*-principes toe;
- Betrek de CISO, de FG en de verantwoordelijke lijnmanagers in een vroeg stadium;
- Gebruik audits als middel om de status van informatiebeveiliging te onderzoeken en deel de bevindingen met het MT;
- Controleer naast opzet en bestaan ook de werking van informatiebeveiligingsprocessen en stuur op resilience (veerkracht).

Colofon

Informatiebeveiligingsdienst (IBD)
Nassaulaan 12
2514 JS Den Haag
www.informatiebeveiligingsdienst.nl
info@IBDGemeenten.nl
070 373 80 11

Met dank aan
De gemeenten die hebben bijgedragen aan het vervaardigen van dit product.

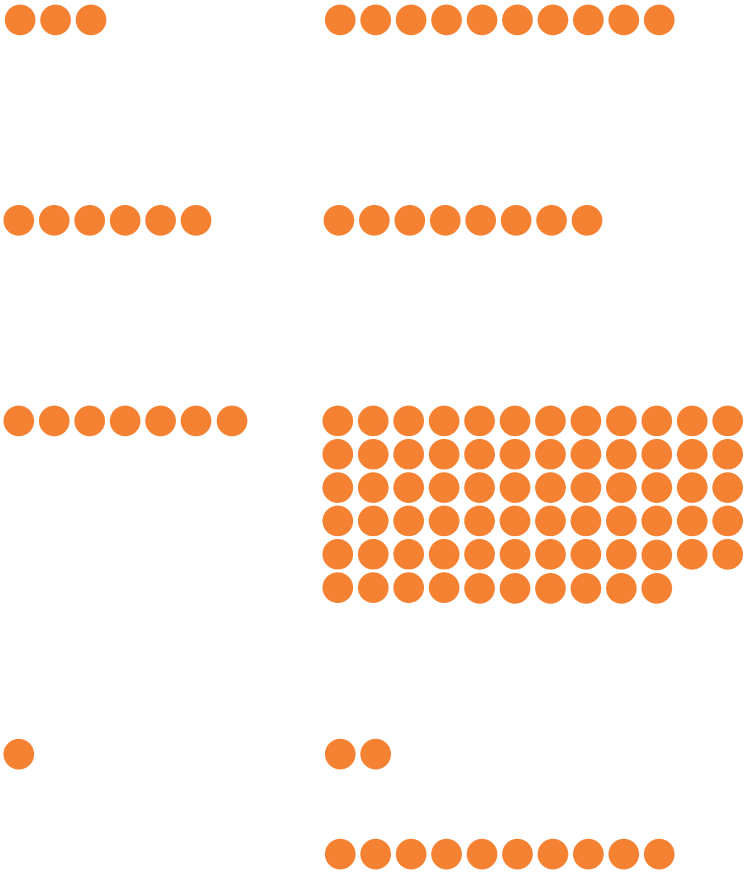
Over de IBD
De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten.
De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Ontwerp
Grafisch ontwerp en infographics: *Simpel is slim/Coform*

INFORMATIE
BEVEILIGINGS
DIENST

VNG Realisatie



INFORMATIE BEVEILIGINGS DIENST

Nassaulaan 12
2514 JS Den Haag
070 373 80 11
info@IBDGemeenten.nl