Digitale veiligheid en de gemeentelijke bestuurder

Bestuurlijke prioriteiten bij het IBD-dreigingsbeeld 2023-2024

Digitale veiligheid en de gemeentelijke bestuurder

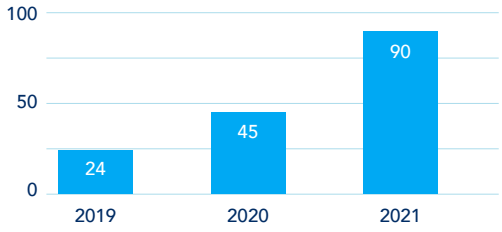
Het dreigingsbeeld vertaald in vijf bestuurlijke prioriteiten

In het dreigingsbeeld 2023-2024[1] beschrijft de Informatiebeveiligingsdienst (IBD) de grootste risico's voor gemeenten op het gebied van informatiebeveiliging en gegevensbescherming.

Het dreigingsbeeld samengevat

Actuele dreigingen

- Meer ransomware met destructievere gevolgen;
- Steeds meer en ernstigere kwetsbaarheden in software;
- Gevaren in ketens uit het zicht.



Aantal kwetsbaarheden met hoge impact

Grootste risico's

- Verstoringen in de bedrijfsvoering;
- Vertrouwelijke informatie in verkeerde handen;
- Uitval van de dienstverlening.

De 6 succesfactoren om de weerbaarheid te vergroten

- *Mensen:* investeer in bewustwording en weerbaarheid;
- *Financiën:* zorg voor structureel budget voor digitale veiligheid;
- *Techniek:* implementeer de basismaatregelen tegen ransomware;
- *Eigenaarschap:* zet informatiebeveiliging en gegevensbescherming op de bestuurlijke agenda;
- *Organisatie:* breng de ambtelijke experts in positie en zorg voor een veilige cultuur;
- *Samenwerkingsverbanden:* maak afspraken en zie erop toe.

Bestuurlijke prioriteiten bij het dreigingsbeeld

Het realiseren van de maatregelen en aanbevelingen uit het dreigingsbeeld vraagt om stevige bestuurlijke aandacht en support op de volgende vijf pijlers van gemeentelijke dienstverlening:

1. Voeren van het gesprek met de gemeenteraad;
2. Herijken van het Integraal Veiligheidsplan;
3. Borgen van de bedrijfscontinuïteit;
4. Versterken van de weerbaarheid tegen steeds professionelere cyberdreiging;
5. Pakken van de regierol richting leveranciers en samenwerkingsverbanden.

1. https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/

Bestuurlijk aan de slag

De vijf bestuurlijke prioriteiten bij het dreigingsbeeld uitgewerkt in concrete aanbevelingen

Bestuurders beseffen dat digitale veiligheid een brede maatschappelijke opgave is

Uit gesprekken tussen gemeentebestuurders en hun ambtelijke experts blijkt dat digitale veiligheid in de kern ook om de kwaliteit en de continuïteit van dienstverlening gaat.
Benadrukt wordt hoe noodzakelijk het is dat gemeenten, maar ook het Openbaar Ministerie en de politie, over voldoende structurele middelen beschikken om te operationaliseren wat er in hun beleidsplannen staat. *Tip: betrek uw lokale en regionale ketenpartners om voldoende budget en capaciteit vrij te maken in het opsporings- en vervolgingsapparaat.*
Daarbij past de notie dat gemeenten ook in hun eigen digitalisering kwetsbaar zijn voor cyberdreigingen. In de unaniem aangenomen resolutie digitale veiligheid is het thema digitale veiligheid tot chefsache verklaard[2]. Er zijn 10 bestuurlijke principes voor informatiebeveiliging uitgewerkt.[3]
Kortom: het is tijd voor daadkracht. Het realiseren van de aanbevolen maatregelen uit het dreigingsbeeld vraagt om stevige bestuurlijke aandacht op de volgende vijf pijlers van gemeentelijke dienstverlening:

Prioriteit 1: Voer het gesprek met de gemeenteraad

"Door Digitale Veiligheid op te nemen in de gemeentelijke kadernota, geef je het thema ook bestuurlijk veel meer plek. ICT is meer dan bedrijfsvoering. Het is veel meer dan ICT alleen."

Burgemeester van Dam, gemeente Hollands Kroon

Het thema Digitale Veiligheid vraagt naast prioriteit en capaciteit ook om voldoende financiële middelen voor 'het eigen huis op orde'. Informatieveiligheid is immers geen luxegoed, maar een pure noodzaak. De gemeentelijke informatievoorzieningen zijn een kwetsbaar object voor kwaadwillenden en de interne informatiebeveiligingsorganisatie vraagt om continue aandacht van de ambtelijke organisatie.

Aanbevelingen

- Raadsleden hebben 'budgetrecht' en bepalen waar de gemeentelijke inkomsten aan uitgegeven worden. Ga in gesprek met uw gemeenteraad om het bewustzijn te bevorderen en structureel budget vrij te maken voor het thema Digitale Veiligheid.

Casus Gemeente Hollands Kroon

Digitale Veiligheid in Kadernota

In de begroting van Hollands Kroon is er structureel aandacht voor digitale veiligheid. In de kadernota integrale veiligheid is cybercriminaliteit een van de onderwerpen. In de vorige kadernota beperkte dit onderwerp zich voornamelijk tot projecten om inwoners weerbaar te maken. In de nieuwe kadernota integrale veiligheid krijgt informatieveiligheid een prominente plek onder cybercriminaliteit. Daarmee krijgt de noodzaak om het eigen huis op orde te krijgen en te houden meer politiek bestuurlijke aandacht.

2. Resolutie digitale veiligheid: https://vng.nl/sites/default/files/2021-01/08_resolutie_digitale_veiligheid.pdf
3. 10 bestuurlijke principes voor informatiebeveiliging: www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/

Prioriteit 2: Herijking van het Integraal Veiligheidsplan

"Maak digitale veiligheid onderdeel van het integraal veiligheidsplan en bespreek het met de gemeenteraad. Reserveer zeker 10% van je ICT-budget voor informatiebeveiliging."

Burgemeester Backhuijs, gemeente Nieuwegein

De nieuwe beleidscyclus van het Integraal Veiligheidsplan (IVP) wordt dit jaar in nagenoeg alle gemeenten opnieuw vastgesteld. Door het thema Digitale Veiligheid op te nemen in het IVP raakt het thema zowel ambtelijk als bestuurlijk merkbaar geborgd binnen de organisatie. Hierdoor kan er voldoende capaciteit en budget beschikbaar worden gesteld om niet alleen de gemeente zelf, maar ook inwoners en ondernemers weerbaar te maken tegen digitale dreigingen. Daarnaast is het van belang om aandacht te besteden aan slachtofferschap en de meldingsbereidheid bij incidenten te vergroten.
Het thema Digitale Veiligheid wordt gezien als ''the new kid on the block" binnen het veiligheidsdomein[4]. De verregaande digitalisering van de samenleving zal zowel de criminaliteit als de veiligheidsaanpak van inhoud en vorm doen veranderen.
Het Kernbeleid Veiligheid wordt gebruikt als basis voor de op te stellen IVP's. Begin 2020 heeft de VNG als addendum op het Kernbeleid Veiligheid het focusblad Digitale Veiligheid[5] uitgebracht om aandacht te vragen voor dit nieuwe thema. Het doel van dit focusblad is dat de gemeentelijke rol op het thema Digitale Veiligheid verder kan worden vormgegeven en het handvatten biedt voor een goede verwerking van dit thema in het IVP.

Het thema Digitale Veiligheid vraagt om een integrale aanpak[6] en aandacht van de gehele organisatie en bestaat uit vier onderdelen:

1. Eigen huis op orde, aandacht voor informatiebeveiliging
2 Preparatie op cybercrises en -incidenten;
3 Cybercrime en gedigitaliseerde criminaliteit;
4 Online aangejaagde ordeverstoringen.

Aanbevelingen

- Volledige digitale veiligheid bestaat niet. Daarom is het zaak om ook aandacht te besteden aan de voorbereiding op een cybercrisis of -incident. Uit onderzoek van de WRR (2019) blijkt dat het onderdeel preparatie bij veel overheidsorganisaties nog onderbelicht is.[7] En op het moment dat crisisplannen rondom digitale veiligheid wel klaar liggen worden de mogelijke scenario's niet of nauwelijks geoefend.[8] Niet alleen de warme fase van een cyberincident of -crisis vraagt om aandacht, ook de gemeentelijke organisatie heeft behoefte aan een jaarlijkse 'brandoefening', zoals het uitvallen van de stroomvoorziening of het interne netwerk.
- Niet alleen de afdeling ICT is verantwoordelijk voor de informatiebeveiliging, dat is bij uitstek een verantwoordelijkheid van alle medewerkers binnen de gemeente. Juist daarom is het van belang ook informatiebeveiliging en privacy bewaking te borgen in het IVP.
  De uitwerking van dit onderdeel binnen het thema Digitale Veiligheid vraagt extra aandacht en een intensievere samenwerking tussen de Chief Information Security Officer (CISO) en de afdeling Openbare Orde en Veiligheid.

4. Lokaal veiligheidsbeleid in 2030: https://vng.nl/sites/default/files/2022-06/Lokaal-Veiligheidsbeleid-in-2030.pdf
5. VNG Focusblad Digitale Veiligheid: https://vng.nl/publicaties/focusblad-digitale-veiligheid
6. CCV-cyberwegenkaart: https://vng.nl/nieuws/lokale-cyberwegenkaart-geupdatet
7. Digitale ontwrichting: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting
8. Cybercrises bij gemeenten: https://www.researchgate.net/publication/348961473_Cybercrisis_bij_gemeenten_Een_verkennend_onderzoek_naar_de_voorbereidingen_ervaringen_en_uitdagingen

Prioriteit 3: Borging van de bedrijfscontinuïteit

"Elke gemeente zou de komende twee jaar verplicht moeten trainen en aan een peer-to-peer gesprek moeten deelnemen."

Burgemeester Potters, gemeente De Bilt

Veel gemeenten kampen met een gebrek aan capaciteit. Er ligt daarnaast een opgave ten aanzien van deskundigheidsbevordering, kennisdeling en de mate waarin experts tussen inhoudelijk jargon en bestuurlijke taal kunnen schakelen. Naast het versterken van ambtelijke expertise is er ook in de breedte, dus domein overstijgend, aandacht nodig voor kennisgroei en zo integraal mogelijke weerbaarheidsoefeningen.

Aanbevelingen

- Neem uw bestuurlijke rol bij prioritering en laat u regelmatig bijpraten over het onderwerp digitale veiligheid vanuit de organisatie.
- Onderbouw en benadruk hoe essentieel digitale veiligheid is voor het bedrijfscontinuïteitsmanagement (BCM) en agendeer aandacht voor deskundigheidsbevordering en integrale weerbaarheidsoefeningen.
- Stel gezamenlijk met de organisatie de (bestuurlijke) impact vast bij een incident en wees betrokken bij de maatregelen in het geval van een verstoring van de bedrijfscontinuïteit.
- Implementeer en borg de maatregelen tegen ransomware[9] en de principes bij de Baseline Informatiebeveiliging Overheid (BIO).[10]
- Hanteer een duidelijke PDCA-cyclus en risicomanagement systematiek, zodat u op basis van het dreigingsbeeld snel en risicogericht aan de slag kunt.

Casus Gemeente De Bilt

Integrale weerbaarheidsoefening

De intensieve digitale weerbaarheidsoefening die in de gemeente De Bilt werd gehouden, wijst uit dat digitale veiligheid veelomvattender is dan vooraf voorzien. Het onderwerp raakt ook de verantwoordelijkheden rond openbare orde en veiligheid en crisisbeheersing.
Eén van de eyeopeners was dat in het geval van cyberincidenten de vaste samenwerkingspartners vaak met dezelfde problemen kampen. De maatschappelijke druk en onrust is groot en maakt een crisis al snel regionaal. De gemeentelijke bedrijfscontinuïteits- en crisisplannen voorzien vaak nog niet in die reikwijdte.

Prioriteit 4: Versterken van de weerbaarheid tegen steeds professionelere cyberdreiging

Cybercriminelen slaan steeds vaker toe. Ook bij overheidsinstellingen, die in toenemende mate afhankelijk zijn van digitale systemen. De dienstverlening van gemeenten bevat immers steeds vaker gedigitaliseerde processen, waardoor ze kwetsbaar zijn voor een aanval op, of zelfs de uitval van deze systemen.
De diepgang en reikwijdte van effecten en gevolgschade van cyberincidenten nemen steeds verder toe. Denk bijvoorbeeld aan de hacks bij de gemeenten Buren en Hof van Twente waarbij de uitval van systemen enorme effecten hadden op de gemeentelijke dienstverlening. Niet alleen de kans op digitale ontwrichting neemt toe, ook de mate waarin cybercriminelen geprofessionaliseerd zijn vormt een steeds hoger dreigingsniveau.

9. VNG cyberalert: https://www.informatiebeveiligingsdienst.nl/nieuws/voorzitter-vng-wijst-burgemeesters-op-maatregelen-ransomware/
10. 10 bestuurlijke principes voor informatiebeveiliging: https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/

Aanbevelingen

- Draag er zorg voor dat de aanbevelingen uit het dreigingsbeeld worden opgevolgd en geef hieraan zichtbaar steun. Maak bijvoorbeeld gebruik van tweefactor authenticatie en pas sterke wachtwoorden toe.
- Goed voorbeeld doet goed volgen. Wees u bewust van vertrouwelijke informatie via de digitale snelweg en in de fysieke wereld. Burgemeesters en wethouders vervullen een voorbeeldfunctie, zowel intern als extern. Heb daarom aandacht voor uw publieke functie, maar ook voor uw persoonlijke digitale veiligheid. Zorg dat u altijd de meest recente updates installeert van uw apparatuur en programma's.

Casus Gemeente Smallingerland

Bewustzijn bij medewerkers activeren en versterken

In Smallingerland besteden ze wanneer nieuwe medewerkers in dienst treden in de vorm van een animatie aandacht aan digitale bewustwording. Ook doen ze gedurende het jaar regelmatig phishing tests. En schuiven ambtelijke experts, soms onaangekondigd, aan bij werkoverleggen. Smallingerland heeft een eigen escaperoom ingericht in de bunker, waarover ze beschikken. Dat is een prachtige voorziening om medewerkers via teambuilding te laten kennismaken en oefenen met digitale veiligheidsvraagstukken.

Prioriteit 5: Pakken van de regierol richting leveranciers en samenwerkingsverbanden

"Digitale veiligheid is geen IT-probleem, maar een gezamenlijk dienstverleningsprobleem"

Burgemeester Meerts, gemeente Wijk bij Duurstede

Gemeenten zijn gemiddeld in zo'n 30 samenwerkingsverbanden actief. Desondanks hebben ze vaak onvoldoende regie en grip op de gegevensuitwisseling die in zulke samenwerkingen plaatsvindt. Het sociaal domein is een gemeentelijk werkterrein waarin erg veel gevoelige gegevens uitgewisseld worden met tal van samenwerkende partijen. Hierbij is het voor de meeste gemeenten nauwelijks mogelijk om (toe)zicht op dat informatielandschap te houden.

Aanbevelingen:

- Agendeer bestuurlijk de vraag: Wat doen we zelf, wat organiseren we regionaal en wanneer schalen we landelijk op? Maak met gemeenten waarmee u intensief samenwerkt structuurafspraken waarin duidelijk is wie doorzettingsmacht heeft in geval van een cybercrisis. Op zulke momenten heeft u immers geen tijd te verliezen.
- Focus niet alleen op het contracteren van leveranciers en het vastleggen van samenwerkingsafspraken, maar besteed juist ook aandacht aan het gezamenlijk oefenen van crises, monitoren van beveiligingsgraden en het naleven van gegarandeerde terugval- en herstelscenario's.
- Bespreek met gemeenschappelijke regelingen welke governance er van ze verwacht wordt. Werk in het verlengde van de gemeentelijke nota's Verbonden partijen samen met gemeenschappelijke regelingen aan normenkaders waarop de digitale beveiligingsgraad getoetst en bewaakt kan worden.

Casus politie-eenheid/regio Rotterdam

Gecombineerde inzichten meenemen in doelgroep gerichtere aanpak via publiek-private samenwerking.

Het Jaarbeeld Cybercrime 2021 van de politie-eenheid Rotterdam laat zien dat 84% van de slachtoffers van gedigitaliseerde criminaliteit jonger is dan 57 jaar. Het laat ook zien dat de financiële schade het grootst is bij 50-plussers. De meldingsbereidheid bij slachtoffers van digitale fraude en internetoplichting is echter beperkt. Lang niet alle slachtoffers doen melding bij de gemeente of de politie. Inwoners melden misbruik echter in veel gevallen wel bij hulpverleningsorganisaties of financiële dienstverleners. In de regio Rotterdam bleek dat gesprekken met banken en slachtofferhulp veel meer cijfers en inzichten opleveren dan waarover gemeenten zelf beschikken. De politie-eenheid Rotterdam, het Openbaar Ministerie en de 25 gemeenten in de eenheid Rotterdam werken daarom in de periode tot en met 2024 samen met publieke en private partners aan een versnelde positieve ontwikkeling op het gebied van weerbaarheid en bewustzijn in het digitale domein.

Meer weten?

Maak gebruik van de ondersteuning die het programma Agenda Digitale Veiligheid van de VNG aan gemeenten biedt. Om het thema digitale veiligheid nog hoger op de bestuurlijke agenda te krijgen en te houden zet de Vereniging van Nederlandse Gemeenten (VNG) zich in om samen met het ministerie van Binnenlandse Zaken collectieve ondersteuning voor gemeenten te organiseren.

Meer informatie vindt u op: https://digitaleveiligheid.pleio.nl
Contact via: teamadv@vng.nl

Vereniging van Nederlandse Gemeenten

Nassaulaan 12
2514 JS Den Haag
+31 70 373 83 93

info@vng.nl

oktober 2022

Foto omslag: ANP / Patricia Rehe
Grafisch ontwerp: Simpel is slim

vng.nl