Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten

2023 → 2024

VNG

INFORMATIE
BEVEILIGINGS
DIENST

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 ondersteunt gemeenten bij de implementatie van de BIO 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 en hun samenwerkingsverbanden kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

INFORMATIE
BEVEILIGINGS
DIENST

VNG

Voorwoord

Het is 1 april 2022 als de telefoon gaat…

‘Michiel, wij zijn gehackt.’
‘Het is 1 april, is dit een grap?’
‘Nee, dit is geen grap,
dit is serious business.’

De nachtmerrie van iedere gemeente wordt waarheid… we zijn gehackt. De eerste dagen na de hack leek het alsof dit met name een klus was voor de medewerkers van ICT en de betrokken manager. Naar mate de dagen vorderden en het effect zichtbaar werd, 130 GB op het darkweb en 5 TB aan informatie gestolen, kwam het besef keihard binnen. Dit is een crisis en dit is iets van ons allemaal; van de hele organisatie maar ook zeker van het bestuur. Maar laten wij vooral ook niet vergeten welke effecten het heeft op de samenleving: een overheid waarvan alle informatie is gestolen… Wat doet dat met je inwoners en bedrijven? Hoe heeft dit kunnen gebeuren? Hoe gaat de gemeente om met haar informatiemanagement en ICT-beveiliging? Allemaal vragen waar je mee te maken krijgt en waarvan zowel het bestuur als ik merkte dat niet overal direct antwoord op gegeven kon worden. Persoonlijk ongemak, jazeker, maar ook een leerpunt voor ons als organisatie. Hoe betrokken zijn wij bij dit onderwerp? Kennen wij de risico’s? Voelen wij ons eigenaar?

Mijn oproep aan ons allemaal is om informatieveiligheid en informatiemanagement een onderwerp te laten zijn van zowel de organisatie- als de bestuurlijke agenda. Het zit in alles wat we doen. Als gemeente Buren zijn wij daarom transparant geweest in onze communicatie. In deze sfeer van transparantie moeten we doorlopend onze actuele risico’s onder ogen zien. Dit dreigingsbeeld helpt daarbij.

[redacted],
Gemeentesecretaris Buren

Inleiding

Inleiding

Voor u ligt het **Dreigingsbeeld Informatiebeveiliging 2023 → 2024**. De Informatiebeveiligingsdienst (IBD) wil met deze publicatie gemeenten ondersteunen bij het in beeld krijgen en managen van de risico's voor inwoners, ondernemers, de ambtelijke organisatie, de politiek en het bestuur.

Somber beeld

De lezer zou somber kunnen worden van het beeld. Veel gemeenten zetten stappen om de informatiebeveiliging op een hoger niveau te krijgen. Maar de dreiging neemt zo snel toe, dat er meer nodig is om het groeiende gat te dichten. Als gemeenten hun weerbaarheid niet verhogen zal de toenemende, steeds professionelere dreiging in combinatie met het steeds grotere 'aanvalsoppervlak', leiden tot meer incidenten: een neerwaartse spiraal.

Gemeenten kunnen het tij keren

Het goede nieuws is dat gemeenten het tij kunnen keren. De gemeentesecretaris kan hierbij een belangrijke aanjaagrol vervullen. Door regie te voeren op integraal risicomanagement. En door uit te dragen dat informatieveiligheid niet iets is van de ICT-afdeling, maar van alle mensen in de hele organisatie. In deze publicatie schetsen we de belangrijkste dreigingen en de zaken die binnen gemeenten een rol spelen. De IBD sluit dit dreigingsbeeld af met een stapsgewijs handelingsperspectief voor de gemeentesecretaris.

Over de voorbeelden

De IBD hecht eraan te vermelden dat de transparantie over de risico's bedoeld is om van te leren. Al te vaak wordt in berichtgeving over informatiebeveiliging de schuldvraag centraal gesteld. Dat proberen we in dit dreigingsbeeld te vermijden. De genoemde voorbeelden zijn vooral bedoeld om inzicht te geven en dienen als opstap om het handelingsperspectief voor gemeenten te beschrijven.

Grootste risico's voor gemeenten

De gemeentesecretaris is als schakel tussen bestuur en ambtelijke organisatie in de eerste plaats een risicomanager. Hij of zij kan worden gezien als hoeder van de continuïteit en de kwaliteit van de dienstverlening. Wat zijn op dit moment de grootste risico's op het gebied van de informatiebeveiliging en gegevensbescherming?

Uitval van dienstverlening en bedrijfsvoering

Als informatie niet beschikbaar is, leidt dat tot problemen in de dienstverlening en de bedrijfsvoering. Nagenoeg ieder proces, van uitgifte van paspoorten tot het betalen van uitkeringen, wordt uitgevoerd of ondersteund door digitale informatie- en communicatievoorzieningen. In het ergste geval moeten gemeenten dienstverleningsprocessen stilleggen.

Vertrouwelijke informatie in verkeerde handen

In principe is overheidsinformatie openbaar. Tenzij deze informatie privacygevoelig is, schade kan toebrengen aan de overheid of commercieel voor- of nadelig kan zijn voor derden. Gemeenten verwerken voor hun wettelijke taken veel vertrouwelijke informatie. Denk aan gegevens over werk en inkomen, zorg, veiligheid of commercieel interessante informatie over gebiedsontwikkeling, aanbestedingen en bedrijfsgevoelige informatie. Onterechte toegang tot deze informatie kan uiterst nadelig uitvallen voor inwoners en ondernemers. Een datalek of een overtreding van de AVG kan leiden tot hoge boetes.

Fouten in de dienstverlening

Informatiebeveiligingsincidenten kunnen leiden tot fouten in de dienstverlening. Kwaliteit en integriteit van data worden in het algemeen niet direct gezien als doel van informatiebeveiliging. Toch dient dit risico nadrukkelijk op het netvlies te staan van de directie. Want als informatie niet integer is, kan dat leiden tot vertraagde of foute beslissingen, verkeerde handelingen en verspilling van tijd en menskracht.

Hoge herstelkosten, reputatieschade en minder vertrouwen in de overheid

Informatiebeveiliging wordt vaak gezien als een (onnodige) kostenpost. De kosten voor preventieve maatregelen staan in geen verhouding tot de kosten van een incident. Die lopen al gauw op tot tonnen of miljoenen euro's. Zo'n incident heeft ook een grote impact op medewerkers. Een getroffen organisatie is vaak weken of maanden bezig om de bedrijfsprocessen en informatiebeveiliging weer op orde te krijgen en de complete gegevensregistraties opnieuw op te bouwen. Beveiligings- en privacy- incidenten schaden ook het vertrouwen van burgers in de overheid, de reputatie van de organisatie en haar bestuurders.

Actueel dreigingsbeeld

De IBD ziet dat in het bijzonder drie soorten dreigingen opvallen sinds het uitbrengen van het vorige dreigingsbeeld 2021- 2022.

- **Meer ransomware, destructievere gevolgen**
- **Steeds meer en ernstiger kwetsbaarheden in software**
- **Gevaren in ketens uit het zicht**

Meer ransomware, destructievere gevolgen

De dreiging van ransomware-aanvallen neemt toe. Aan de lopende band proberen criminelen een ingang te vinden. De (potentiële) gevolgen van een aanval worden ook steeds ernstiger: het wordt merkbaar. Het fenomeen ransomware (gijzelsoftware) komt al jaren voor. Criminelen versleutelen gegevens en persen het slachtoffer af om deze gegevens na het betalen van losgeld weer toegankelijk te maken. De IBD ontving de afgelopen twee jaar steeds meer meldingen van situaties waar gemeentelijke processen langdurig(er) verstoord zijn als gevolg van destructieve gijzelsoftware. Criminelen aarzelen niet om privacygevoelige gegevens van inwoners, bedrijven en medewerkers online te publiceren.

De gemeente Buren* werd in 2022 getroffen door een ransomwareaanval. Bij de hack zijn gegevens van de gemeente gestolen. Vervolgens is een grote hoeveelheid data gepubliceerd op het darkweb, een afzonderlijk en anoniem deel van het internet.

Ook in het buitenland zijn de afgelopen jaren veel lokale overheden getroffen door ransomware zoals Palermo (IT), Atlanta, Baltimore, Knoxville, Albany, New Orleans (VS), Luik (BE), Frankfurt (DE), Weiz (AT).

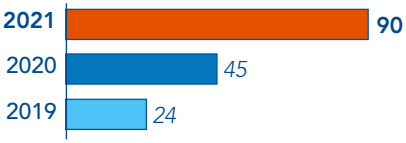
De Ierse gezondheidszorg heeft een forse prijs betaald voor de ransomwareaanval in 2021. De kosten zijn opgelopen tot net iets minder dan 52 miljoen euro. Het leeuwendeel daarvan is voor herstel van de versleutelde en daarmee gegijzelde systemen. Een relatief kleine kostenpost - van nog altijd miljoenen - is voor preventieve maatregelen**.

* *https://www.buren.nl/nieuws/datadiefstal-gemeente-buren/7399/*
** *https://www.agconnect.nl/artikel/ransomware-kost-ierse-zorg-tientallen-miljoenen-niet-aan-losgeld*

Steeds meer en ernstiger kwetsbaarheden in software

Alle hard- en software bevat kwetsbaarheden en fouten. Deze zouden kunnen worden misbruikt door kwaadwillenden. Het is daarom zaak om kwetsbaarheden tijdig te verhelpen. In 2021 heeft de IBD 1841 kwetsbaarheden gesignaleerd. De ene kwetsbaarheid is de andere niet en daarom wordt per geval een risicoschatting gemaakt op basis van kans en impact. Gevallen met een hoge kans op misbruik en ernstige gevolgen komen in de afgelopen jaren relatief steeds vaker voor. Vaak is het verhelpen van een kwetsbaarheid een kwestie van updaten, maar soms is het complexer en moeten systemen ingrijpend gewijzigd worden.

Jaar en aantal kwetsbaarheden met hoge kans op misbruik, hoge mogelijke impact:



De kwetsbaarheid in de softwarecomponent Log4j en massaal misbruik daarvan zorgde er eind 2021 voor dat tienduizenden softwarepakketten met grote spoed moesten worden aangepast of bijgewerkt. Feitelijk was deze kwetsbaarheid aanwezig bij nagenoeg iedere organisatie ter wereld met een omvangrijke ICT-omgeving – dus ook Nederlandse gemeenten. Omdat het hier ging om een bouwsteen van software was medewerking en hulp nodig van leveranciers en dienstverleners. Iedere gemeente is eind 2021 druk geweest met het aanpassen of bijwerken van software om incidenten te voorkomen. In enkele gevallen moesten systemen tijdelijk uitgeschakeld worden om misbruik te voorkomen.

Gevaren in ketens uit het zicht

Een gemeente neemt deel in gemiddeld 30 samenwerkingsverbanden en maakt gebruik van diensten van derden zoals softwareleveranciers. Omdat men bij uitbesteding vooral stuurt op de kwaliteit van de uiteindelijke dienstverlening en informatiebeveiliging en privacy gezien worden als operationele details, is daar weinig aandacht voor in de samenwerkingsafspraken. Politiek gezien is uitbesteding en/of samenwerking bedoeld om zaken tegen lagere kosten op een hoger kwaliteitsniveau te krijgen. Informatiebeveiliging is in die zin een kostenpost. Als er al concrete afspraken zijn over informatiebeveiliging en privacy dan staat controle op de naleving beperkt op de agenda. Gemeenten vertrouwen erop dat bij een samenwerkingsverband dergelijke zaken 'gewoon geregeld zijn'. Dit heeft als gevolg dat er weinig zicht is op de feitelijke risico's als taken zijn uitbesteed. Gemeenten zijn in de afgelopen twee jaar regelmatig geconfronteerd met incidenten die ontstaan zijn bij derden waarbij de gevolgen in de eigen gemeente merkbaar waren.

Werkbedrijf Senzer, een samenwerkingsverband van zeven gemeenten, werd in 2021 getroffen door een inbraak op het netwerk. De betaling van uitkeringen liep vertraging op. Systemen waren niet toegankelijk, medewerkers konden daardoor niet op een normale manier hun werk doen.

Werkleerbedrijf Voorne-Putten Werkt BV (VPW) was in 2022 slachtoffer van een cyberaanval. De aanvaller heeft zich toegang verschaft tot het IT-systeem, een grote hoeveelheid data gestolen en ontoegankelijk gemaakt voor de organisatie met afpersing als doel. VPW zou anderhalve week na de aanval migreren naar een nieuwe werkomgeving met meerfactorauthenticatie (MFA), maar was dus net te laat.

Een softwarebedrijf van vijf Limburgse gemeenten is in 2022 getroffen door ransomware. Door de aanval waren bestanden van het administratiesysteem van het sociaal domein versleuteld. Er zijn voor zover bekend geen gegevens bekend buitgemaakt.

Weerbaarheid vergroten: 6 succesfactoren

Wat kan een gemeentesecretaris doen om de organisatie weerbaarder te maken en de kans op een incident of crisis aanzienlijk te verkleinen?

Vertrekpunt zijn de AVG en de BIO (Baseline Informatiebeveiliging Overheid, het normenkader voor informatieveiligheid). Omdat gemeenten over veel gegevens beschikken, met veel applicaties en processen werken en ook samenwerken buiten de gemeentegrenzen, hebben zij hier een enorme klus aan. Gemeenten die (allereerst) de basis op orde willen brengen, kunnen een belangrijke eerste stap zetten door aan de slag te gaan met 6 succesfactoren. Het toepassen hiervan biedt geen garanties - net zomin als een alarmsysteem dat doet in de fysieke wereld. Maar het vermindert de risico's voor informatieveiligheid en gegevensbescherming aanzienlijk. De succesfactoren beïnvloeden elkaar en moeten in samenhang met elkaar worden opgepakt. De succesfactoren kennen uitdagingen en kunnen gezien worden als een ketting die zo sterk is als de zwakste schakel. Alleen techniek maakt gemeenten niet weerbaar, alleen bewustwording of veilige werkprocessen ook niet.

'Wij hadden geen indicatie dat wij zaken niet goed op orde hadden. We hebben gekozen om ons systeembeheer uit te besteden en jaarlijks werd een programma Informatiebeveiliging ontwikkeld, met audits, trainingen en beleidsontwikkeling. Wij 'scoorden' hier altijd goed op en toch is het ons overkomen. Geen signalen geeft geen enkele garantie.'

Dennis Lacroix, *gemeentesecretaris Hof van Twente*

'If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.'

Bruce Schneier

Succesfactor Financiën

Reserveer een vast percentage in het budget voor informatiebeveiliging en privacy

Gemeenten die een vast percentage in het budget reserveren voor informatiebeveiliging en privacy, hebben het voordeel dat ze een structurele, cyclische aanpak kunnen hanteren. Zij hoeven niet voor iedere activiteit te motiveren dat er in de eerste plaats budget nodig is. In de resolutie Digitale Veiligheid* is door alle leden van de VNG in 2021 een vast budget voor digitale veiligheid onderschreven. De Cyber Security Raad** hanteerde in 2017 10% van het ICT-budget als ondergrens. De dreiging is sinds 2017 alleen maar toegenomen.

De Chief Information Security Officer (CISO) en Privacy Officer (PO) kunnen de gemeentesecretaris binnen een structurele en cyclische aanpak adviseren over de verdeling van budget, vanuit inzicht in de risico's en oplossingsrichtingen. En daarmee een belangrijke rol spelen bij het plannen, uitvoeren, controleren en bijstellen van activiteiten gericht op informatiebeveiliging en privacy. Het is nuttig om informatiebeveiliging te integreren in reguliere gemeentelijke plannen. Denk hierbij aan afdelingsplannen, het Integraal Veiligheidsplan (IVP), en de risicoparagraaf in de gemeentelijke begroting.

* *https://www.informatiebeveiligingsdienst.nl/nieuws/resolutie-digitale-veiligheid-aangenomen/*
** *https://www.cybersecurityraad.nl/documenten/jaarplannen/2018/04/01/csr-meerjarenstrategie-2018-2021*

Uitdaging

Het onderwerp wordt nog vaak gezien als een kostenpost die ten koste gaat van het primaire proces: de dienstverlening aan inwoners en ondernemers. Veel gemeenten hebben de afgelopen jaren herhaaldelijk moeten bezuinigen. Informatiebeveiliging en privacy doen mee in de strijd om het geld.

Hier wringt de schoen nog eens extra: alleen door meer digitalisering is het mogelijk om het werk uit te blijven voeren en daardoor neemt de afhankelijkheid toe. Die afhankelijkheid maakt de bescherming van informatiesystemen urgenter dan ooit tevoren.

> **'We moeten keuzes maken met de personele krapte en alle urgente dossiers, waarin informatievoorziening en ondersteuning van procesflow primair is. Ik maak me zorgen over de aandacht die we in deze context besteden aan de essenties op informatiebeveiliging en of we daarmee niet de volgende crisis die veroorzaakt wordt door verwaarlozing op ons afroepen.'**
>
> **Beatrijs de Vries,** *gemeentesecretaris Coevorden*

Daarbij komt: de schade van een informatiebeveiligingsincident is niet altijd eenvoudig in kosten uit te drukken. Er lijkt bovendien sprake te zijn van een preventieparadox: als je investeert dan gebeurt er niets, dus volgt de vraag: waarom hebben wij ons geld hieraan besteed. Tegelijkertijd als je niet investeert gebeurt er ook vaak niet - direct - iets.

Het helpt ook niet dat je niet ziet dat er een digitaal raampje of deurtje openstaat. Anders dan bij een fysiek incident is er geen zichtbare component; de brand, zwaailichten en afzetlinten ontbreken. Het is daarentegen wel direct zichtbaar als er onvoldoende capaciteit is voor jeugdzorg. Maar hoe kun je jeugdzorgtaken uitvoeren als je niet meer bij de informatie kunt? Of als de dossiers op straat liggen?

Succesfactor Techniek

De basismaatregelen tegen ransomware zijn op orde

Techniek is niet onfeilbaar. Er bestaan geen waterdichte technische beveiligingsmaatregelen. Daarom is het belangrijk om hierin een gelaagdheid aan te brengen zodat als een maatregel niet afdoende blijkt, er andere maatregelen zijn die dat opvangen. De gemeente neemt daarom in samenhang noodzakelijke basisbeveiligingsmaatregelen om afdoende beschermd te zijn en borgt dat deze ook worden toegepast in relaties met externe partijen.

- De software en hardware zijn up-to-date.
- Geen meerfactorauthenticatie (MFA/2FA)? Geen toegang tot de systemen.
- De gemeente heeft door monitoring zicht op wat er op het netwerk gebeurt en laat zich hierin bijstaan door een professionele dienstverlener.
- Het netwerk is opgedeeld in verschillende zones zodat een digitale brand niet kan overslaan tussen systemen.
- De gemeente heeft back-ups en test deze regelmatig.
- De gemeente is voorbereid en geoefend op uitval van systemen en overige incidenten.

Lees hiervoor ook de oproep van VNG-voorzitter Jan van Zanen aan alle burgemeesters van Nederland.

Ledenbrief cyberalert

De gemeente Enschede maakt gebruik van een zogeheten managed monitoring & response dienst:

‘Omdat de dreigingen in aantal en complexiteit toenemen, hebben we een professionele securitypartner in de arm genomen. Zij vormen een paar extra ogen op ons netwerk. Dankzij hun monitoring & response kunnen wij bij verdachte situaties snel acteren.’

Kees Meijer, *algemeen directeur/gemeentesecretaris Enschede*

Uitdaging

Het grootste deel van de (ransomware)incidenten is terug te voeren op het ontbreken van één of meerdere van deze maatregelen. De snelheid waarmee gemeenten het been bijtrekken haalt het niet bij de snelheid waarmee de criminele tegenpartij professioneler wordt. Dat digitale open ramen en deuren worden opgemerkt blijkt uit dit voorbeeld: Een gemeente installeerde een nieuwe server en koppelde deze aan het internet. Deze bevatte nog kwetsbaarheden. Binnen een week was deze server gehackt en had een ‘onbevoegde’ toegang tot de hele gemeentelijke omgeving.

Succesfactor Eigenaarschap management

Informatiebeveiliging en gegevensbescherming staan op de managementagenda

- Agendeer in het MT wat er overblijft, nadat je je technische verdediging hebt ingericht. Dit komt neer op ‘de menselijke factor’: cultuur, bewustzijn en voorbeeldgedrag van het management.
- Maak het management verantwoordelijk voor informatiebeveiliging en gegevensbescherming. Hoe meer bewustzijn er is op besluitvormend niveau, hoe meer we bevorderen dat dit bewustzijn er is in de werkwijze van de mensen in de organisatie. Wat doen we als volgende week dinsdag de computers het niet meer doen? Hoe goed zijn wij eigenlijk weerbaar tegen datalekken en fouten in onze informatievoorziening? Welke informatie zwerft er eigenlijk rond op onze systemen? Deze vragen gaan niet over techniek maar over bedrijfscontinuïteit en over werkprocessen.
- De gemeentesecretaris voert de regie over het risicomanagement en de CISO/ privacyfunctionaris zijn de eerste adviseurs die helpen bij een veilige bedrijfsvoering en dienstverlening.
- Het MT oefent idealiter jaarlijks met uitval van systemen in de eigen organisatie. Samen met partners en leveranciers.

Succesfactor Organisatie

Positie Chief Information Officer (CISO) en een veilige cultuur

‘De CISO, PO’s en FG van Amstelveen werken al jaren intensief samen voor Amstelveen en Aalsmeer. Samen vormen ze een zichtbare drie-eenheid, waar de organisaties op positieve wijze rekening mee houden. Dit maakt het voor medewerkers laagdrempelig om incidenten, klachten of andere kwesties bij hen te melden. Mijn collega-gemeentesecretaris in Aalsmeer en ik ontvangen elke drie maanden een gezamenlijke rapportage, die ook naar de portefeuillehouder en burgemeester gaat. Zo staat het onderwerp ook op de bestuurlijke agenda.’

Bert Winthorst, *gemeentesecretaris Amstelveen.*

- De CISO en de FG zijn strategisch adviseurs voor de gemeentesecretaris, directie en bestuur. Dit komt tot uitdrukking in hun plek binnen de organisatie en in hun functiewaardering. Gelet op het concernbrede werkgebied is een plek binnen een concernstaf (of soortgelijke omgeving) de meest logische.
- Investeer in kennis en vaardigheden van CISO, PO en FG: de ontwikkelingen gaan snel en specialistische kennis is vaak noodzakelijk.
- Moedig samenwerking tussen CISO’s, PO’s en FG’s van verschillende gemeenten aan, opdat zij gebruik kunnen maken van elkaars kennis en expertise. Ook samenwerking met de CIO, de controller en audit-afdeling kan vruchten afwerpen. Maak gebruik van een ‘securitypartner’ als specialistische kennis ontbreekt of onvoldoende op peil is.
- Doe collectief wat kan. Standaardiseer waar het kan. Betrek de CISO bij deze plannen. En benut de kennis en expertise die IBD/VNG heeft over ‘samen organiseren’.
- Minstens zo belangrijk is een open en veilige cultuur, waarin medewerkers worden gestimuleerd om incidenten te melden. Waarin incidenten worden besproken. En waarbij de melder een terugkoppeling krijgt. Vanzelfsprekend is voorbeeldgedrag van de ambtelijke en bestuurlijke top hiervoor essentieel.

Uitdaging

Mede als gevolg van een gebrek aan aandacht en eigenaarschap bij de ambtelijke top zijn veel CISO's, PO's en FG's onvoldoende 'in positie'. De afstand tot het management is te groot en belangrijke informatie, bijvoorbeeld over risico's, bereikt het management niet. Ook spreken deze functionarissen en het management vaak niet 'dezelfde taal'. Omdat informatiebeveiliging ten onrechte wordt gezien als een ICT-kwestie, zitten deze belangrijke functionarissen 'verstopt' binnen ICT/I&A afdelingen.

De krapte op de arbeidsmarkt zet bovendien druk op de beschikbaarheid van voldoende IT-professionals en voldoende specialistische IT-kennis en capaciteit bij gemeenten. Inhuur van een securitypartner kan hier uitkomst bieden. Het is daarbij wel van belang inzichtelijk te hebben welke kennis en expertise nodig is. De kennis daartoe ontbreekt soms bij gemeenten.

Succesfactor Samenwerkingsverbanden

Maak afspraken en zie erop toe

De partners en leveranciers van de gemeente Hoeksche Waard moeten bij het afsluiten van contracten met een verwerkersovereenkomst op onafhankelijke wijze kunnen aantonen dat zij voldoen aan de gestelde veiligheidseisen. Dat kunnen ze doen door een accountantsverklaring te overleggen of een Third Party Memorandum (TPM). En ze moeten zich bereid verklaren mee te werken aan een controle en datalekprocedure als de gemeente dat verlangt of daartoe verplicht is*.

Als gemeente blijf je verantwoordelijk voor de data van de inwoners, ongeacht op welke wijze een proces of dienst wordt uitgevoerd. Het buiten de eigen deur plaatsen van taken ontslaat je niet van verantwoordelijkheid. Het maakt niet uit of processen en systemen bij een leverancier draaien of bij een gemeentelijk samenwerkingsverband. Maak afspraken en controleer periodiek of de afspraken op papier in de praktijk worden nagekomen. Laat het samenwerkingsverband niet alleen verantwoording afleggen over de doelen en de middelen, maar ook over informatiebeveiliging en privacy. Ook hier kunnen gemeenten gebruikmaken van de kracht van het collectief en standaardiseren wat mogelijk is.

* *https://www.gemeentehw.nl/wp-content/uploads/2022/02/RK-HW-Informatiebeveiliging-en-privacy-Eindrapport-DEF.pdf*

Succesfactor
De factor mens

Investeren in bewustwording

Een belangrijke bouwsteen van informatiebeveiliging en privacy is bewustzijn van medewerkers. Door informatiebeveiliging en gegevensbescherming te koppelen aan het werkproces zijn risico's herkenbaar voor medewerkers. Veel incidenten zijn terug te voeren op een gebrek aan digitaal bewustzijn en andersom: een verhoogd digitaal bewustzijn zorgt ervoor dat incidenten snel herkend en erkend worden. Een veilige omgang met data is onderdeel van het primaire proces en vraagt dus permanent aandacht en voorbeeldgedrag van directie en management en doorlopend trainen van alle medewerkers. Maar ook van gemeenteraad en college. De factor mens kan worden versterkt met technische maatregelen: de gemeente houdt er rekening mee dat een wachtwoord in verkeerde handen kan vallen en hanteert daarom een extra factor bij het inloggen (2FA/MFA in de vorm van een code die elke 30 seconden wijzigt). De werkgever biedt ook veilige tools die het werkproces ondersteunen, hiermee voorkom je dat gegevens op onveilige wijze gedeeld worden.

Een afdelingsmanager kreeg tijdens het werk meldingen op haar telefoon die normaal gesproken alleen bij het inloggen horen te verschijnen. "U logt in op de digitale werkomgeving, klik hier om te bevestigen". Na meermaals op annuleren te hebben gedrukt besloot ze toch maar een keer op de knop OK te klikken. Gelukkig meldde de manager dit bij ICT-beheer en zo is misbruik van haar account voorkomen.

Uitdaging

De aandacht verslapt snel en we zijn vaak goed van vertrouwen. Zowel binnen de organisatie als in samenwerking met externe partijen vraagt informatieveiligheid 'offers'. De snelste en de makkelijkste weg is niet altijd een veilige weg. Informatieveiligheid vraagt dan bijvoorbeeld om een extra handeling (bijvoorbeeld meerfactorauthenticatie). Een digitale veiligheidscultuur zou eigenlijk net zo normaal moeten zijn als het dragen van een helm op een bouwplaats, maar dat wordt niet zo ervaren.

INFORMATIE
BEVEILIGINGS
DIENST

De IBD adviseert ook de gemeentesecretaris
De IBD adviseert, faciliteert kennisdeling en ondersteunt bij incidenten. De gemeentelijke CISO, FG en PO weten de IBD doorgaans goed te vinden. De IBD kan ook de gemeentesecretaris en de burgemeester van advies voorzien, zowel op het vlak van preventie als bij incidenten. Vertrouwelijkheid is hierbij gewaarborgd.

Bronnen
De IBD baseert zich in deze publicatie op dagelijks contact met gemeentelijke CISO's, FG's en PO's. De IBD analyseert en deelt informatie met hen over dreigingen en kwetsbaarheden in software. Ze faciliteert het delen van kennis en ervaring in de dagelijkse praktijk en naar aanleiding van incidenten. De IBD heeft een groot aanbod ondersteunende producten en diensten en onderhoudt contacten met leveranciers. Bij incidenten heeft de IBD een adviserende, soms ook coördinerende rol. Indien de situatie en de gemeente daarom vraagt komt de IBD 'op locatie'. Ook baseert de IBD zich in deze publicatie op gespreksrondes over informatieveiligheid en privacy met bestuurders, directeuren en medewerkers van gemeenten.

Informatiebeveiligingsdienst (IBD)
Nassaulaan 12, 2514 JS Den Haag
www.informatiebeveiligingsdienst.nl
info@IBDGemeenten.nl
070 204 55 11

VNG

INFORMATIE
BEVEILIGINGS
DIENST