Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten

2025 → 2026

VNG

INFORMATIE
BEVEILIGINGS
DIENST

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

Over de IBD
De Informatiebeveiligingsdienst (IBD) is de sectorale CERT/CSIRT voor alle Nederlandse gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. Als schakelpunt met het Nationaal Cyber Security Centrum (NCSC) en andere CERTs binnen het Cyber Weerbaarheidsnetwerk, draagt de IBD bij aan de Baseline Informatiebeveiliging Overheid (BIO) en geeft zij regelmatig kennisproducten uit.

INFORMATIE
BEVEILIGINGS
DIENST

VNG

Inhoud

Samenvatting

Gemeenten staan in 2025-2026 voor een onverminderd complex digitaal dreigingslandschap. Ransomware, datalekken en uitval van processen door incidenten vormen de grootste bedreigingen. Dit vraagt om een proactieve aanpak om digitale veiligheid te waarborgen en vertrouwen van inwoners en ondernemers te behouden. Dit alles in het licht van financiële en personele krapte.

Huidige situatie en uitdagingen

- **Ransomware** blijft de grootste dreiging. Criminelen gebruiken kwetsbare systemen om gevoelige data te stelen en organisaties af te persen, met aanzienlijke gevolgen zoals privacyschendingen, imagoschade en financiële verliezen.
- **Incidenten bij leveranciers** leiden tot verstoringen in gemeentelijke processen. Gemeenten zijn afhankelijk van externe partijen, wat de noodzaak benadrukt van duidelijke afspraken over beveiliging.
- **Beperkte capaciteit, kennis en middelen** bemoeilijken investeringen in digitale veiligheid.

Weerbaarheid

Gemeenten moeten hun digitale weerbaarheid versterken door:

1. **Basismaatregelen** zoals toegangsbeheer met multifactorauthenticatie, netwerkscheiding, back-ups en monitoring in combinatie met bewustwording.
2. **Leveranciersmanagement** te verbeteren met expliciete eisen aan informatiebeveiliging en controle hierop.
3. **Samenwerking** en standaardisatie tussen gemeenten te intensiveren om kosten te verlagen en kennis te bundelen.

Lange termijn

De opkomst van AI biedt zowel kansen als risico's. AI kan beveiligingsprocessen efficiënter maken, maar wordt ook gebruikt door criminelen voor verfijnde aanvallen zoals deepfake-fraude. Gemeenten moeten alert blijven op technologische ontwikkelingen, zoals quantumcomputing, die toekomstige encryptie kunnen doorbreken.

Conclusie

Digitale veiligheid is geen luxe maar een noodzakelijke voorwaarde voor continuïteit en vertrouwen in gemeentelijke dienstverlening. Gemeenten moeten blijven investeren in bewustwording, technologie en samenwerking om huidige én toekomstige dreigingen effectief het hoofd te kunnen bieden.

Voorwoord

De digitale veiligheid van onze organisaties is een onderwerp dat ons allemaal raakt. Gemeenten, groot en klein, staan gezamenlijk voor uitdagingen die onze dienstverlening aan onze inwoners en het vertrouwen in de overheid kunnen beïnvloeden. Het is juist deze gedeelde verantwoordelijkheid die ons de kans biedt om samen sterker te staan.

Als voorzitter van de Vereniging van Nederlandse Gemeenten (VNG) ben ik ervan overtuigd dat samenwerking de sleutel is tot succes. Digitale dreigingen stoppen niet bij gemeentegrenzen; ze vragen om een gezamenlijke aanpak waarin gemeenten elkaar versterken. Door kennis te delen, standaarden te ontwikkelen en gezamenlijk op te trekken, kunnen we onze weerbaarheid vergroten.

Ik ben bijzonder trots op de rol die de Informatiebeveiligingsdienst (IBD) al meer dan tien jaar vervult als collectieve voorziening voor gemeenten. De IBD biedt niet alleen expertise en ondersteuning bij incidenten, maar fungeert ook als een verbindende factor in het complexe landschap van informatiebeveiliging en privacy. Dankzij deze collectieve aanpak hebben we als gemeenten een solide basis gelegd om digitale risico's proactief te beheersen.

Dit dreigingsbeeld biedt ons waardevolle inzichten in de grootste dreigingen en kansen van dit moment. Dit helpt ons om – samen met onze adviseurs – strategische keuzes te maken en onze verantwoordelijkheid als bestuurders waar te maken. Samen kunnen we ervoor zorgen dat digitale veiligheid geen obstakel is, maar een fundament voor vertrouwen en innovatie.

Sharon Dijksma
Burgemeester Utrecht
Voorzitter VNG

Inleiding

Het Dreigingsbeeld Informatiebeveiliging 2025-2026 van de IBD is voor de gemeentebestuurders en de gemeentesecretaris. Het helpt hen om inzicht te krijgen in digitale dreigingen en de impact daarvan op de gemeente. Daarnaast is het een waardevol instrument voor de gemeentelijke CISO, ISO, PO en FG om management, directie en bestuur effectief te adviseren over digitale risico's. Zo draagt het dreigingsbeeld bij aan een goed geïnformeerd gemeentelijk beleid om efficiënt, effectief, zorgvuldig en vooral ook veilig te kunnen werken.

Google geeft 1740 resultaten op de zin: "de wereld digitaliseert in rap tempo". Dat maakte deze stelling over de snelheid van digitalisering net zo afgezaagd en betekenisloos als dat ze een complete onderschatting is. "Rap tempo" doet namelijk geen recht aan de revolutionaire veranderingen van nu met grote impact op onze samenleving. In dit licht kan een bestuurder van een gemeente zich zomaar weerloos voelen tegenover het digitaliseringsgeweld om ons heen.

Informatiebeveiliging en privacybescherming lijken een onoverkomelijke hindernis voor de gemeentelijke dienstverlening en bedrijfsvoering. Gesprekken gaan veelal over gevaren, bedreigingen en risico's. En de makkelijkste manier van risicobeheersing is risicovermijding. Dat betekent dat dingen niet mogen worden gebruikt, niet mogen worden gedeeld, niet mogen worden ingezien. Daarnaast worden voor de gebruiker drempels opgeworpen bij het inloggen (zo'n vervelende extra code en een niet te onthouden wachtwoord dat elke zes weken anders moet). Dit zorgt voor weerstand.

Ten slotte, de toevoeging "cyber" aan verder tamelijk normale begrippen geeft de onderwerpen informatieveiligheid en privacy iets geheimzinnigs en mystieks. Zo lijkt het alsof deze domeinen alleen voor inhoudsdeskundige ICT-ers zijn. Dit zorgt voor onbegrip.

Deze cocktail van machteloosheid, weerstand en geheimzinnigheid maakt dat digitale veiligheid niet het lievelingsonderwerp is op de bestuurlijke agenda. We hebben niet de illusie dat we digitale veiligheid met dit dreigingsbeeld het populairste vergaderpunt maken, maar wel dat het beter begrepen wordt. En daarmee wil de IBD de interne dialoog in gemeenten stimuleren.

Welke risico's moeten we beheersen?

Gemeenten moeten zorgen dat hun systemen en gegevens:

1. **Beschikbaar zijn: werken wanneer nodig.**
2. **Integer zijn: correct, betrouwbaar, nauwkeurig en volledig.**
3. **Vertrouwelijk blijven: alleen toegankelijk voor bevoegden.**

Het is de taak van directie en management om risico's in de praktijk te beheersen, onder verantwoordelijkheid van de bestuurder.

Bij enkele gemeenten en samenwerkingsverbanden hebben digitale incidenten geleid tot miljoenen euro's schade, wekenlange uitval van dienstverlening en diefstal van gevoelige gegevens.

Beschikbaarheid, integriteit en vertrouwelijkheid: schade voor inwoners, ondernemers en medewerkers

Inwoners kunnen serieus last hebben van uitval van gemeentelijke diensten, een datalek of fouten in de gemeentelijke systemen. Denk aan uitkeringen die niet op tijd uitbetaald kunnen worden of gevoelige informatie die op straat wordt gegooid. Gemeenten moeten deze risico's meewegen bij beslissingen over de dienstverlening en de bedrijfsvoering. Naast snelheid, efficiëntie, zorgvuldigheid, betaalbaarheid en klantvriendelijkheid is (digitale) veiligheid een bepalende factor voor de kwaliteit van de gemeentelijke uitvoering. Daarbij hebben gemeenten ook een verantwoordelijkheid als werkgever. Medewerkers moeten gebruik kunnen maken van veilige systemen en de gemeente dient zorgvuldig om te gaan met de gegevens die ze over haar werknemers vastlegt.

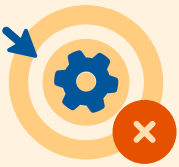
Imagoschade en financiële schade

Wanneer de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen) beschadigd worden, keldert het vertrouwen van inwoners in de overheid, bestuurders en ambtenaren. Dit geldt niet alleen voor data. Publieke dienstverleners worden ook geacht zorgvuldig om te gaan met publiek geld. Bij enkele gemeenten en samenwerkingsverbanden hebben digitale incidenten geleid tot miljoenen euro's schade, wekenlange uitval van dienstverlening en diefstal van gevoelige gegevens. Dat raakt inwoners in hun beeld van gemeenten.

Op welke scenario's moeten gemeenten zich voorbereiden

Uitval van processen door een incident in de organisatie

Een digitaal incident bij de gemeente kan diensten rond het sociaal domein, burgerzaken, uitkeringen of vergunningverlening stilleggen. Gemeenten moeten ransomware, menselijke fouten en technische storingen voorkomen door netwerksegmentatie toe te passen, actuele back-ups te maken en toegangsrechten strikt toe te passen. Het interne gemeentelijke crisisteam moet voorbereid zijn met uitgewerkte continuïteitscenario's en een duidelijk communicatieplan om de dienstverlening snel weer op gang te brengen.



Uitval van processen door een incident bij externe partijen

Gemeenten zijn voor hun werk afhankelijk van externe partijen: leveranciers, zoals softwarebedrijven en clouddiensten. Een (ver)storing bij een ICT-leverancier of een ketenpartner kan ervoor zorgen dat gemeentelijke processen stil komen te liggen. Denk aan uitval van uw zaaksysteem of een storing in DigiD. Gemeenten moeten vooraf eisen stellen aan leveranciers en die vastleggen in afspraken, bijvoorbeeld over continuïteit en beveiliging. Liefst doen gemeenten dit collectief. Denk ook aan afspraken over hoe te handelen tijdens een incident. Dan is het namelijk aan gemeenten om snel contact te leggen met de relevante leverancier(s), alternatieve procedures in te zetten en informatie over de impact te verzamelen voor (bestuurlijke) besluitvorming.

Datalek door een intern incident

Een datalek, veroorzaakt door bijvoorbeeld een verkeerd ingestelde server of een phishing-aanval, kan duizenden inwoners raken. Die komen allemaal verhaal halen bij de gemeente. Gemeenten moeten medewerkers trainen in het herkennen van risico's, toegangsrechten strikt toepassen en gegevens minimaliseren om schade te beperken. Bij een datalek moeten zij direct een inschatting maken van de risico's, melding doen conform de AVG en transparant communiceren met betrokkenen van wie de data zijn en/of raken.

Datalek door een incident bij externe partijen

Een hack bij een leverancier kan betrekking hebben op data van inwoners, ondernemers en medewerkers. Gemeenten moeten vooraf zorgen dat contracten duidelijke afspraken bevatten over onder andere bewaartermijnen van data, het gebruik van data, beveiligingsmaatregelen en audits. Denk ook aan sancties wanneer niet wordt geleverd. Bij een datalek moeten leveranciers snel acteren om de impact van het incident in kaart te brengen en de gevolgen te beperken.

Actueel dreigingslandschap 2025-2026

Dit dreigingsbeeld is opgesteld op basis van incidenten bij gemeenten, meldingen en vragen van gemeentelijke contactpersonen. Het beeld is verder gebaseerd op het cybersecuritybeeld Nederland, dreigingsbeelden van andere sectoren zoals de zorg en het onderwijs, actuele vakliteratuur en interviews met experts. Gemeenten staan anno 2025 voor een complex en veelzijdig dreigingslandschap, waarin cybercriminaliteit, geopolitieke spanningen en technologische afhankelijkheden een grote rol spelen.

Ransomware blijft de nummer één dreiging voor gemeenten.

Bovendien zijn gemeenten in de Cyberbeveiligingswet (Cbw) aangemerkt als zogeheten essentiële entiteit: vanaf 2025 hebben zij een expliciete zorgplicht voor digitale veiligheid. Hoewel stappen worden gezet om de weerbaarheid te vergroten, blijven de uitdagingen groot door beperkte middelen (bezuinigingen op het gemeentefonds en tekorten in de jeugdzorg), capaciteit en kennis. Hieronder wordt een overzicht gegeven van de belangrijkste dreigingen en de impact hiervan op gemeentelijke organisaties.

In 2023 en 2024 waren ruim 150 gemeenten een of meerdere keren betrokken bij ransomware in de leveranciersketen.

De grootste dreiging: ransomware

Ransomware blijft de nummer één dreiging voor gemeenten. Criminelen maken gebruik van zwakheden in systemen die via internet toegankelijk zijn, zoals websites, toegangsportalen, inlogschermen. Na toegang nemen zij ruim de tijd om rond te kijken wat er te halen valt, zich te nestelen, gevoelige data te stelen en te versleutelen en vervolgens slachtoffers af te persen. Tot 2020 gebeurde dit vooral door systemen of gegevens met gijzelsoftware op slot te zetten en geld te vragen voor de sleutel. Tegenwoordig persen criminelen de getroffen organisatie vooral af met dreigen om gestolen data openbaar te maken.

De impact van ransomware is aanzienlijk: diefstal en publicatie van gegevens leiden tot grove schending van privacy van inwoners, imagoschade van gemeenten, verminderd vertrouwen in de overheid als geheel en financieel verlies voor gemeenten als gevolg van reparatie- en herstelkosten. In 2023 en 2024 waren ruim 150 gemeenten een of meerdere keren betrokken bij ransomware in de leverancierskeken. Het ging hierbij onder andere om incidenten bij dienstverleners, zoals een print-servicebureau en aanbieders van clouddiensten.

Gemeenten en hun leveranciers zijn de afgelopen jaren niet per se het gerichte doelwit geweest van criminelen, maar door kwetsbare systemen en buitgemaakte inloggegevens worden gemeenten wel vaak slachtoffer van deze gelegenheidsaanvallen. Bij gemeenten gaat het dan bijvoorbeeld om de volgende gestolen gegevens: (persoons-)gegevens van inwoners en medewerkers, dossiers uit het jeugd- en zorgdomein, gegevens die te maken hebben met veiligheid en ondermijning of kopietjes van identiteitsbewijzen.

Bestuurlijke vraag: Doet u voldoende om te voorkomen dat gevoelige data gestolen worden en (hoe) bent u voorbereid als dit onverhoopt gebeurt?

Beperkte middelen bemoeilijken weerbaarheid: compliance risico's

Financiële zorgen werpen hun schaduw vooruit. Gemeenten doen er veel aan om hun digitale weerbaarheid te vergroten. Echter, structurele tekorten in budgetten, capaciteit en kennis maken het lastig om digitale veiligheid naar het gewenste niveau te brengen en te houden. De primaire taken van gemeenten krijgen vaak prioriteit boven investeringen in ICT-beveiliging, terwijl deze juist op lange termijn nodig zijn om continuïteit te waarborgen.

Dit leidt niet alleen tot mogelijk onveilige situaties, maar ook tot compliancerisico's, ofwel risico's die voortvloeien uit het niet naleven van wet- en regelgeving zoals de AVG en de Cbw.

> Bestuurlijke vraag: Maakt u, gegeven de financiële krapte, bewuste keuzes om de belangrijkste risico's te beheersen?

Financiële schade en langetermijnrisico's: e-mail als zwakste schakel

E-mail blijft de meest gebruikte en meest gangbare communicatiemethode. Bij e-mail ligt veel verantwoordelijkheid bij de eindgebruiker om zich aan de procedures te houden en zo een datalek en/of 'inbraak' te voorkomen. Een foutje is helaas zo gemaakt (persoonsgegevens verkeerd versturen of een malafide link niet herkennen). E-mail is daarom een aantrekkelijk doelwit voor cybercriminelen en een potentieel risico voor de informatiebeveiliging van organisaties.

Organisaties moeten er helaas vanuitgaan dat het niet te voorkomen is dat medewerkers misleid worden.

Criminelen gebruiken phishing graag als methode, omdat het voor hen zo makkelijk is. Op internet circuleren lijsten met miljarden e-mailadressen en in combinatie met (zakelijke) informatie die mensen vrijwillig openbaar maken via bijvoorbeeld LinkedIn. Dit is een prima visvijver voor criminelen. Ook niet-technisch onderlegde criminelen kunnen aan de slag met laagdrempelige phishingdiensten die worden aangeboden. Daarnaast maakt generatieve AI phishingcampagnes verfijnder en moeilijker te herkennen, waardoor de kans op succesvolle aanvallen toeneemt. Organisaties moeten er helaas vanuitgaan dat het niet te voorkomen is dat medewerkers misleid worden.

Criminelen maken massaal gebruikersnamen en wachtwoorden buit. Dit kan op de lange en middellange termijn weer leiden tot digitale inbraken en andere incidenten. Criminelen weten met enige inspanning ook direct geld te stelen. Factuurfraude door een malafide of fictieve tussenpersoon is een groeiend probleem, ook voor gemeenten. Hierbij onderschept een oplichter de communicatie tussen de gemeente en een leverancier. De fraudeur past een factuur aan door het rekeningnummer te vervangen door zijn eigen rekening. De gemeente ontvangt deze nagemaakte factuur, die er echt uitziet, en betaalt het bedrag aan de oplichter. Pas als de echte factuur onbetaald blijft, ontdekken gemeente en leverancier de fraude. Deze vorm van oplichting is moeilijk te herkennen, omdat alles er legitiem uitziet. Robuuste betaalprocedures bevatten daarom regels voor wijzigingen op facturen en rekeningnummers, bijvoorbeeld door deze altijd telefonisch te verifiëren bij de leverancier via een bekend nummer.

Bestuurlijke vraag: Wat doet u om schade van onvermijdelijke en geslaagde phishingaanvallen te beperken?

Een groeiend risico: incidenten bij leveranciers

Een groeiend deel van de gemeentelijke ICT wordt als dienst afgenomen. De transitie naar software-as-a-service (SaaS) brengt voordelen zoals vereenvoudigd beheer. Gemeenten profiteren van snellere implementaties en minder technische zorgen, maar ervaren tegelijkertijd een verlies aan controle en grip. Incidenten in de toeleveringsketen vormen een toenemende dreiging. Ransomware en phishing bij leveranciers leiden regelmatig tot grootschalige verstoringen en/of datalekken bij meerdere gemeenten tegelijk. Deze gebeurtenissen benadrukken het belang van duidelijke afspraken (eisen stellen) met leveranciers over beveiliging en incidentrespons. De toenemende afhankelijkheid van externe partijen voor clouddiensten of oplossingen die als dienst via internet worden aangeboden maakt gemeenten kwetsbaarder voor dit soort aanvallen.

Bestuurlijke vraag: Heeft u de ketens en afspraken met derden in beeld en (hoe) bent u in control?

Beperkte impact, maar storend: DDoS-aanvallen

DDoS (Distributed Denial of Service) is een aanval waarbij kwaadwillenden een website of online dienst (bijvoorbeeld Inlogsysteem DigiD) platleggen door deze te overspoelen met een enorme hoeveelheid nepverkeer vanaf meerdere bronnen tegelijk. DDoS-aanvallen zijn een integraal onderdeel geworden van hybride oorlogsvoering, waarbij statelijke actoren en activistische groepen betrokken zijn. Pro-Russische groeperingen voerden DDoS-aanvallen uit op Europese verkiezingswebsites en Nederlandse havens als reactie op steun aan Oekraïne. Activistische groepen richten zich vaak op symbolische doelen, zoals overheidswebsites of publieke diensten, om maximale maatschappelijke impact te bereiken. Dit is bijvoorbeeld zichtbaar in aanvallen op DigiD. Hoewel de impact bij de lokale overheid vaak beperkt blijft tot de tijdelijke onbereikbaarheid van gemeen-

telijke websites, kan dit toch hinder veroorzaken voor inwoners die afhankelijk zijn van gemeentelijke online-diensten. Gemeenten moeten daarom blijven investeren in maatregelen zoals DDoS-bescherming om deze verstoringen te minimaliseren en dit (collectief) te eisen bij de belangrijkste cloudleveranciers.

Bestuurlijke vraag: Hoe lang acht u uitval van de gemeentelijke online diensten acceptabel en passen de maatregelen bij deze risicoacceptatie?

Zwakke schakel: complexe informatievoorziening

De complexe informatievoorziening bij gemeenten vormt een structurele uitdaging voor digitale weerbaarheid. Zo vallen veel ICT-systemen buiten het zicht van gemeentelijke beheerders. Incidenten zoals die als gevolg van de Log4j-kwetsbaarheid, de NAFIN-storing en telecomstoringen illustreren hoe kwetsbaar organisaties zijn door ketenafhankelijkheden; een probleem in één schakel kan leiden tot grootschalige verstoringen van (online) diensten. Het blijkt niet altijd mogelijk om een compleet overzicht te hebben van alle afhankelijkheden. Bovendien bestaat software die als dienst wordt afgenomen vaak uit meerdere componenten en verbindingen die moeilijk inzichtelijk te maken zijn. Het versnipperde ICT-landschap van gemeenten en het gebrek aan overzicht vergroot de kans op onopgemerkte kwetsbaarheden.

Ook hierin zijn standaardisatie en samenwerking tussen gemeenten een must om schaarse capaciteit, kennis en onderhandelingskracht te bundelen.

Bestuurlijke vraag: Hoe gaat u om met het beperkte overzicht op de informatie-voorziening en ICT-huishouding? Weegt u de voor- en nadelen van versimpeling en verregaande standaardisatie?

Onvoldoende grip op gevoelige data

Alle gemeentelijke processen zijn kwetsbaar voor incidenten. De impact is het grootst in domeinen waar veel gevoelige data worden verwerkt, zoals veiligheid, jeugd en zorg en werk en inkomen. Gemeenten zetten doorlopend stappen om deze gegevens beter te beschermen door middel van dataminimalisatie, toegangsrechtenbeheer, logging en monitoring. Maar de onderwerpen data en gegevensdeling hebben naast technische maatregelen, ook bewuste keuzes nodig van het management.

Gegevensopslag en gegevensdeling vragen om een evenwicht: te veel opslaan of delen leidt net zo goed tot risico's als te weinig opslaan of delen. Onvoldoende opslaan of delen kan leiden tot gebrekkige samenwerking en inefficiënte dienstverlening, terwijl overmatige of onzorgvuldige gegevensopslag en -deling juist kan resulteren in datalekken of schendingen van de privacy. Het vinden van een balans tussen noodzakelijke en veilige opslag en uitwisseling blijft daarom een complexe uitdaging in de gemeentelijke ketensamenwerking. De gemeente moet wettelijk gezien kunnen aantonen en uitleggen dat gegevens passend zijn beschermd.

Bestuurlijke vraag: Bewaakt uw management de balans in opslag en delen van data en nemen de juiste functionarissen hun verantwoordelijkheid?

Het gevaar bestaat dat de organisatie niet meebeweegt met de ontwikkelingen en medewerkers ongereguleerd en uit het zicht zelf AI inzetten voor het eigen werk.

Kansen én risico's: opkomst van AI

De opkomst van (generatieve) AI biedt zowel kansen als bedreigingen voor gemeenten. AI kan worden ingezet om bedrijfsvoering en dienstverlening te helpen. Het kan ook beveiligingsprocessen efficiënter maken, bijvoorbeeld door geavanceerde monitoring en automatische detectie van verdachte activiteiten. Tegelijkertijd maken criminelen gebruik van AI voor nieuwe aanvalsmethoden zoals deepfake-fraude of gerichte phishingcampagnes.
Sinds de invoering van de AVG is het besef gegroeid dat we als verantwoordelijke controle moeten hebben over de wijze waarop persoonsgegevens van inwoners en medewerkers worden verwerkt. Met de opkomst van AI-toepassingen staat deze controle onder druk. Ook, of juist, wanneer de gemeente zelf terughoudend is bij het toepassen van AI. Het gevaar bestaat dat de organisatie niet meebeweegt met de ontwikkelingen en medewerkers ongereguleerd en uit het zicht zelf AI inzetten voor het eigen werk.

AI-modellen functioneren vaak als een black box: het is onduidelijk hoe zij data verwerken en waar die terechtkomen. De Europese AI Act reguleert het gebruik van AI en eist dat risico's voor mens en maatschappij worden geminimaliseerd. Gemeenten moeten kunnen aantonen dat ze AI op een zorgvuldige en transparante manier inzetten. Ook hierin is samenwerking tussen gemeenten een must om schaarse capaciteit, kennis en onderhandelingskracht te bundelen.

Bestuurlijke vraag: Benut uw organisatie in voldoende mate de voordelen van AI terwijl ze zich bewust is van de mogelijke risico's?

Sterk wisselende risico's: operationele technologie

In gemeenten vormen procesautomatisering en operationele technologie (OT) een tot nu toe onderbelicht onderdeel van de infrastructuur. Voorbeelden hiervan zijn systemen voor riolering, verkeersregelinstallaties, camerasystemen en gebouwbeheersing. Sabotage van operationele technologie is reëel, ook al hebben zich recent geen grote incidenten voorgedaan in Nederland. Tegelijkertijd is er ook een reëel risico op fysieke sabotage. Gemeenten moeten de digitale en fysieke bescherming van fysieke objecten daarom integraal beschouwen.

Dit dreigingsbeeld gaat natuurlijk over digitale dreigingen en in het algemeen zijn systemen die aan het internet hangen kwetsbaar. De risico's rond operationele technologie variëren sterk tussen gemeenten. In de meeste gevallen is beheer van dergelijke systemen uitbesteed aan leveranciers en dienstverleners. Risicobeheersing vraagt om goed opdrachtgeverschap, regelmatig bestuurlijk overleg over lokale risico's en een heldere taakverdeling. Gemeenten blijven voor diepgaande kennis en kunde afhankelijk van leveranciers en dienstverleners.

Bestuurlijke vraag: Heeft u uw operationele technologie in kaart en heeft u daarbij de afhankelijkheden en de risico's voor fysieke processen in beeld?

Langetermijn strategische risico's

Op korte termijn blijft de afhankelijkheid bestaan door het ontbreken van realistische alternatieven.

Afhankelijkheid: monoculturen & afhankelijkheid van leveranciers

De afhankelijkheid van ICT-leveranciers en met name Amerikaanse techreuzen vormt een strategisch risico voor gemeenten. Niet alleen maken gemeenten zelf veel gebruik van online diensten van bijvoorbeeld Microsoft, Oracle en Amazon, ook hun leveranciers doen dit. In het geval van Microsoft is sprake van een monocultuur en dat heeft voordelen, ook op het gebied van beveiliging. Maar nadelen zijn er ook: bij uitval van componenten van Microsoft vallen potentieel veel processen stil. Recent is ook meer aandacht voor de strategische afhankelijkheid nu handelsrelaties en bondgenootschappen onder druk staan door heffingen, regels en verschillen in waarden en politieke opvattingen.

Op korte termijn blijft de afhankelijkheid bestaan door het ontbreken van realistische alternatieven. Het vraagt samenwerking binnen de overheid, tussen publieke en private partijen en tussen lidstaten van de EU om deze alternatieven wel mogelijk te maken.

Bestuurlijke vraag: Is uw organisatie bewust van de risico's van technologische monoculturen en vendor lock-in?

Computers worden slimmer dan mensen

De ontwikkelingen rond generatieve AI gaan zo snel dat naast de eerder behandelde operationele risico's ook twee strategische risico's opdoemen: artificial general intelligence en op de langere termijn zelfs singulariteit. Artificial general intelligence verwijst naar het moment dat een AI-systeem, in tegenstelling tot nu, niet meer hoeft te worden getraind om taken uit te voeren maar dat het zichzelf taken kan aanleren. Singulariteit verwijst naar het moment waarop intelligentie van computersystemen de menselijke capaciteiten in alle aspecten overtreft. Wanneer dit punt bereikt wordt, zal de mens niet meer in staat zijn om de werking van computersystemen te doorgronden. Aangezien de computergestuurde beslissingen en acties dan snel in aantal zullen toenemen, zal de invloed op de gehele maatschappij groot zijn. Zeker gezien de ontwikkeling dat AI een steeds integraler onderdeel vormt van computersystemen. Autonome systemen, denk aan zelfrijdende voertuigen en zelfdenkende software, zorgen voor nieuwe en tot nu toe ongekende dilemma's.

Bestuurlijke vraag: Anticipeert u op risico's door geen onomkeerbare stappen te nemen bij het gebruik van AI?

Quantumcomputing

Quantumtechnologie zet de vertrouwelijkheid van gegevens onder druk. Versleutelde gegevens die nu veilig lijken, kunnen in de nabije toekomst alsnog ontsleuteld worden door quantumcomputers. Deze computers maken gebruik van de principes van de quantummechanica. Ze verschillen fundamenteel van traditionele computers en hebben het potentieel om complexe problemen veel sneller op te lossen. Door hun veel grotere rekenkracht hebben zij ook het potentieel om de huidige manier van versleutelen snel te kraken. Beveiliging van data voor de lange termijn vereist tijdige migratie naar post-quantumcryptografie en een strategische aanpak om toekomstige quantumdreigingen te mitigeren.

Bestuurlijke vraag: Is uw organisatie voorbereid op de dreiging van quantumcomputing door in elk geval zicht te hebben op welke gegevens ook op lange termijn beschermd moeten worden?

Weerbaarheid en maatregelen

Het is naast een morele en financiële verantwoordelijkheid ook een wettelijke verplichting om digitale risico's te beheersen.

Ransomware-aanvallen, geslaagde phishingpogingen en incidenten bij leveranciers tonen aan dat de gevolgen van incidenten groot kunnen zijn. Denk aan enorme financiële schade, wekenlange uitval van dienstverlening en diefstal van gevoelige gegevens. Het is naast een morele en financiële verantwoordelijkheid ook een wettelijke verplichting om digitale risico's te beheersen. Bestuur en management scheppen de randvoorwaarden voor risicobeheersing. De impact van een digitale aanval raakt direct uw inwoners, ondernemers en uw organisatie. Digitale veiligheid is daarom geen luxe, maar een noodzakelijke voorwaarde om continuïteit en vertrouwen te waarborgen. Onderstaande adviezen helpen gemeenten hierbij.

Risicomanagement als kerntaak, ook digitaal

Eén ding is zeker: digitalisering gaat niet meer weg. Risicomanagement is een kernonderdeel van de functie van bestuurder. U bent niet alleen bestuurder van de fysieke gemeente, maar ook van de digitale gemeente. De moderne bestuurder is daarom ook digitaal bewust en bekwaam. Dat betekent dat u net zo'n goed overzicht heeft van de fysieke als van de digitale risico's.

Juiste kennis, capaciteit en competenties

Twee belangrijke zaken spelen een rol bij de inbedding van informatiebeveiliging en privacy in de organisatie. Een tekort aan mensen (onder meer als gevolg van krapte op de arbeidsmarkt) en een inefficiënte inzet van de mensen die wel beschikbaar zijn.

Digitale veiligheid en gegevensbescherming beginnen bij de juiste hoeveelheid aandacht, kennis, capaciteit en competenties. Anders gezegd: zonder deze aandacht, kennis, capaciteit en competenties is het niet mogelijk om digitale risico's te beheersen. Tegelijkertijd is het eenvoudiger gezegd dan gedaan om hiervoor een team op sterkte te krijgen. In de praktijk ziet de IBD veel (onwenselijke) dubbelfuncties waarbij een adviseur zichzelf controleert of tussen functies conflicterende belangen heeft. Voorbeelden van ongewenste combinaties zijn CISO/Privacy-officer, CISO/ENSIA-coördinator, CISO/ICT-beheerder of CISO/PO en FG.

Meer samenwerking en standaardisatie helpen om schaarse specialisten doeltreffend en doelmatig in te zetten.

Nadat het team op sterkte is, is het een uitdaging om het op de juiste wijze in te zetten als vertrouwd adviseur. De proceseigenaar moet de risico's inschatten van zijn of haar werkproces. De beveiligings- of privacyfunctionaris (CISO, ISO, PO) heeft daar geen verantwoordelijkheid, anders dan op het gebied van bewustwording. Veiligheid is afhankelijk van hoe proceseigenaren risico's inschatten en beheersen voor hun processen en hoe alle medewerkers dagelijks hun werk uitvoeren. Het is slim om beveiligings- en privacyexperts vroeg te betrekken bij nieuwe plannen. Zo kunnen zij meedenken over veilige en privacyvriendelijke werkprocessen, in plaats van achteraf problemen te moeten herkennen en oplossen.

Meer samenwerking en standaardisatie helpen om schaarse specialisten doeltreffend en doelmatig in te zetten. Het uniformeren van werkprocessen, systeeminrichting, beveiligingsmaatregelen en controle hierop, helpt het bestuur om invulling te geven aan hun lokale verantwoordelijkheid. Tegelijkertijd ontzorgt dit gemeenten op generieke en beleidsarme delen van het werk.

Basismaatregelen zijn geen punt van discussie

Basismaatregelen voor digitale veiligheid, waaronder toegangs(rechten)beheer (en multifactorauthenticatie), het up-to-date houden van hard- en software, monitoring en bewaking en bedrijfscontinuïteitsbeheer zijn geen luxeproducten meer. Het ontbreken van een solide basis zoals beschreven in wetten en normen die gelden voor de overheid (AVG, Cbw, BIO) zouden geen politieke thema mogen zijn. Bij elk werkproces moeten digitaal bewuste medewerkers kunnen rekenen op veilig ingerichte systemen. Bij elk plan is er naast een financiële paragraaf ook een paragraaf digitale veiligheid en gegevensbescherming. Deze paragraaf gaat over mensen, techniek en kosten en bevat de verantwoordelijkheden van het bestuur, het management, de medewerkers en de leveranciers.

Opdrachtgeverschap en leveranciersmanagement

Het beheersen van ketenrisico's is geen keuze, maar een wettelijke verantwoordelijkheid. Gemeenten zijn verantwoordelijk voor de digitale risico's, ook als die ontstaan bij hun leveranciers. Dit betekent dat bij elke aanbesteding en contractverlenging expliciete eisen gesteld moeten worden aan beveiliging gegevensbescherming, risicoanalyses en incidentrespons. Bestuurders moeten zich realiseren dat een datalek of verstoring bij een leverancier direct impact heeft op gemeentelijke dienstverlening en het vertrouwen van de inwoners.

Door collectief met andere gemeenten op te trekken in eisen en toetsing van leveranciers, kan de administratieve last worden verminderd en de gezamenlijke onderhandelingspositie worden versterkt. Veilig opdrachtgeverschap is een bestuursverantwoordelijkheid. Niet handelen betekent onaanvaardbare risico's voor de gemeente en haar inwoners.

Bestuurlijke oproep: Kent u uw afhankelijkheden? Zijn uw risico's afdoende beheerst en eist u naleving van beveiligingsstandaarden? Vraagt u aantoonbare controles op en stopt u samenwerkingen met partijen die onvoldoende beveiliging garanderen?

Werk samen

Het behouden van lokale autonomie bij ICT-keuzes lijkt aantrekkelijk, maar levert vaak minder voordelen op dan gedacht. Gemeenten die zelfstandig opereren, ervaren vooral de nadelen: ze hebben te veel werk, onvoldoende capaciteit, onvoldoende kennis, ze zijn afhankelijk van een klein aantal leveranciers, hebben minder onderhandelingskracht en dragen de hoge kosten van maatwerkoplossingen en onderhoud. Tegelijkertijd missen ze de schaalvoordelen, robuustheid en efficiëntie die voortkomen uit gezamenlijke inkoop, standaardisatie en samenwerking. Door collectief standaarden vast te stellen en generieke oplossingen te benutten, kunnen gemeenten kosten verlagen, risico's spreiden en sneller inspelen op dreigingen, zonder de zeggenschap over hun eigen processen volledig te verliezen.

Conclusie en aanbevelingen

Het dreigingslandschap voor gemeenten blijft zich ontwikkelen onder invloed van technologische en maatschappelijke veranderingen. Ransomware, phishing, supply-chain-incidenten en DDoS-aanvallen vormen momenteel de grootste dreigingen voor gemeenten. De gevolgen zijn, ongeacht de oorzaak, al jaren dezelfde: uitval van dienstverlening en ongeoorloofde toegang tot informatie.

De digitale weerbaarheid van gemeenten staat onder druk door financiële krapte, gebrek aan capaciteit en versnippering van het ICT-landschap. Tegelijkertijd verschuift het technisch complexe werk om gemeenten weerbaar te houden steeds meer richting leveranciers van ICT-diensten. Dat vraagt van gemeenten een focus op opdrachtgeverschap. Wat nog meer achterblijft bij gemeenten is de gemeentelijke professionaliteit en de factor mens: privacyvriendelijke en veilige werkprocessen die worden uitgevoerd door bewuste ambtenaren met een gemeentebestuur en een gemeenteraad die de juiste randvoorwaarden scheppen.

Nieuwe en bestaande wettelijke kaders in het digitaliseringsdomein (zoals de Cbw en de AI Act) maken het extra belangrijk om na te gaan hoe het wèl kan. Gemeenten kunnen alleen hun individuele verantwoordelijkheid voor het beheersen van risico's waarmaken door samenwerking. Dat betekent dat verregaande standaardisering, gezamenlijk oppakken van beleidsarme thema's en samenwerking essentieel zijn om weerbaar te blijven tegen huidige én toekomstige dreigingen.

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
Dit dreigingsbeeld is opgesteld op basis van incidenten bij gemeenten, meldingen en vragen van gemeentelijke contactpersonen, het cybersecuritybeeld Nederland, dreigingsgbeelden uit andere sectoren zoals de zorg en het onderwijs, actuele vakliteratuur en interviews met experts. Veel dank aan de vele reviewers van dit document.

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

VNG

INFORMATIE
BEVEILIGINGS
DIENST