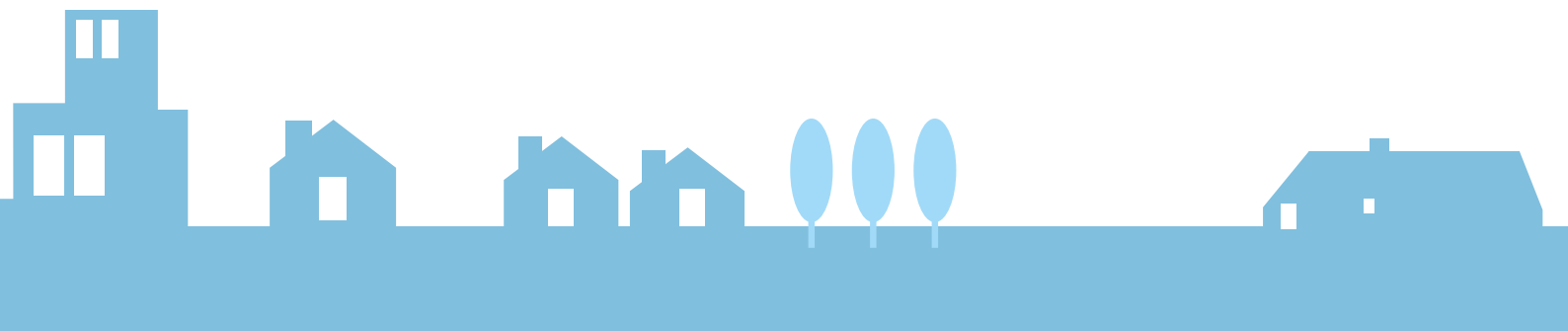
INFORMATIE
BEVEILIGINGS
DIENST

Dreigingsbeeld

Informatiebeveiliging

Nederlandse Gemeenten

2018



"All of life is the management of risk, not its elimination."

– Walter Wriston, Amerikaans bankier

Inleiding

Jaarlijks verschijnt het Nationaal Cybersecuritybeeld (CSBN) van het Nationaal Cyber Security Centrum (NCSC). Het CSBN 2017 beschrijft de belangrijkste risico's voor Nederland als geheel en bedreigingen voor de vitale sectoren in het bijzonder. De conclusies in het meest recente beeld waren als volgt:

Beroepscriminelen en statelijke actoren vormen (…) de grootste dreiging en richten de meeste schade aan;

Digitale aanvallen worden gebruikt om democratische processen te beïnvloeden;

De kwetsbaarheid van het Internet of Things (IoT) [het feit dat veel apparatuur en systemen aan het internet worden gekoppeld, IBD] heeft tot verstorende aanvallen geleid die de noodzaak tot het versterken van de digitale weerbaarheid onderschrijven;

Veel organisaties zijn afhankelijk van een beperkt aantal buitenlandse aanbieders van digitale infrastructuurdiensten waardoor de maatschappelijke impact bij verstoring groot is;

Weerbaarheid van individuen en organisaties blijft achter bij de groei van de dreiging.

Gemeenten hebben de wettelijke taak om een groot aantal diensten te leveren aan inwoners en bedrijven. Diensten die, waar mogelijk, steeds meer digitaal afgehandeld worden. Technologie moet daarbij niet langer gezien worden als 'hulpmiddel' maar als vertrekpunt voor het denken, organiseren en werken van de overheid. Inwoners en bedrijven verwachten een snelle, efficiënte en ook veilige dienstverlening van gemeenten. Gemeenten werken steeds vaker en intensiever samen om uitdagingen in de informatiemaatschappij het hoofd te bieden. Op het gebied van informatiebeveiliging is dat al sinds 2012 de praktijk. In 2013 hebben alle Nederlandse gemeenten zich gebonden aan de gemeenschappelijke

normen die staan beschreven in de Baseline Informatiebeveiliging Gemeenten (BIG).

Gemeenten hebben dagelijks te maken met de dreigingen voor Nederland als geheel maar hebben als meest nabije overheidslaag ook een eigen dreigingsbeeld. De informatiebeveiligingsdienst (IBD) is in 2013 als collectieve voorziening opgericht, door en voor alle Nederlandse gemeenten om hen te ondersteunen bij informatiebeveiliging in de meest brede zin van het woord. Het past bij deze rol om het bestuur, het management en de informatiebeveiligers van Nederlandse gemeenten te adviseren over de belangrijkste risico's en dreigingen die specifiek gelden voor hun organisaties.

Inmiddels is naast alle gemeenten ook een groot aantal gemeentelijke samenwerkingen bij de IBD aangesloten. Ook is een significant deel van de ICT-leveranciers van gemeenten aangesloten op een deel van de IBD dienstverlening. Dat maakt dat sinds 2016 op basis van incidenten en meldingen een integraal landelijk beeld ontstaat van de dreigingen die gelden voor het collectief van alle Nederlandse gemeenten.

CSBN

Het CSBN toont het dreigingsbeeld voor ons hele land en is voornamelijk gericht op de vitale sectoren. Het CSBN gaat dus niet in op de zaken die specifiek voor gemeenten van belang zijn. In aanvulling op het CSBN publiceert de IBD vanaf 2018 het Dreigingsbeeld informatiebeveiliging voor gemeenten. Het risicobeeld stelt bestuurders in staat om in afstemming met de gemeenteraad, het management en de informatiebeveiligers prioriteiten te stellen en bewust risico's te mitigeren of juist te nemen. Daarbij levert het dreigingsbeeld inzichten voor het opstellen van een roadmap, strategie en aanpak van informatiebeveiliging.

Juiste, volledige en beschikbare informatie vormt een belangrijke randvoorwaarde van de dienstverlening van gemeenten. Veel van de gegevens waar gemeenten mee werken zijn openbaar: informatie over de openbare ruimte, plannen, beleid en bestuurlijke aangelegenheden. Informatiebeveiliging is essentieel voor de beschikbaarheid en integriteit van deze gegevens en de systemen waarmee het werk wordt uitgevoerd.

Naast beschikbaarheid en integriteit speelt ook de vertrouwelijkheid van gegevens een rol. Persoonlijke gegevens van inwoners over werk, inkomen, zorg en welzijn maar ook gegevens die om andere redenen dan privacy-bescherming als vertrouwelijk moeten worden aangemerkt vormen de kroonjuwelen van de gemeentelijke informatievoorziening.

Over het dreigingsbeeld informatiebeveiliging Nederlandse gemeenten

Dit beeld is tot stand gekomen op basis van een analyse van meldingen aan de IBD, inhoud van lokale rekenkamerrapporten, bevindingen van de visitatiecommissie informatieveiligheid en interviews met gemeentelijke Chief Information Security Officers (CISO's). Gemeentelijke CISO's hebben commentaar gegeven op het concept-beeld en hun opmerkingen zijn verwerkt in het voorliggende beeld. De conclusies tonen een gemiddeld beeld van het collectief van alle gemeenten. De resultaten zijn niet zonder meer te extrapoleren naar individuele gemeenten.

Het dreigingsbeeld is geschreven voor het management van gemeenten. Hier en daar zal de tekst weliswaar (te) technisch zijn, maar de IBD is ervan overtuigd dat de gemeente een goede CISO heeft die management en bestuur bijstaat en waar nodig uitleg en context kan geven (zie hiervoor ook advies 4 aan het einde van dit document).

Risico's en prioriteiten

Risico's 2017

Mensen maken fouten

Bijvoorbeeld: informatie onveilig verzenden.
› *pag. 10*

Gemeenten zijn kwetsbaar

Veel bijzondere gegevens en onvoldoende kennis.
› *pag. 11*

Dreigingen ook van buiten

Gegevens komen ook van uw leveranciers.
› *pag. 13*

Waan van de dag bepaalt agenda

Er moet nog zoveel. Wie is verantwoordelijk?
› *pag. 14*

We weten niet wat we niet weten

Meten we wel op het netwerk?
› *pag. 15*

Prioriteiten 2018

Maak medewerkers uw verdedigingslinie

Investeer in bewustwording.

› *pag. 18*

Elimineer kwetsbaarheden

Breng risico's in kaart en neem maatregelen.
› *pag. 19*

Zorg voor een plan B

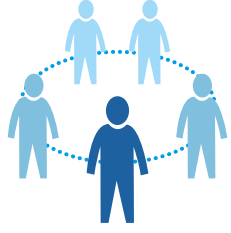
Het gaat ooit fout: wees voorbereid!
› *pag. 21*

Maak uw CISO belangrijk

Laat de CISO de agenda bepalen.
› *pag. 22*

Organiseer het samen

Je kunt het niet zonder je ketenpartners.
› *pag. 22*



Incidenten in 2017

Beschikbaarheid

Distributie **4**

DOS/DDOS **3**

Sabotage **2**

Fraude

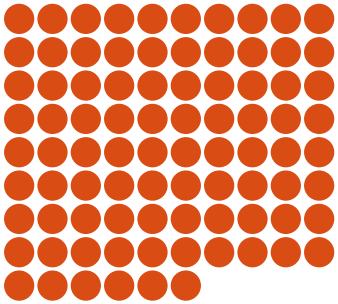
Copyright **1**

Illegaal naam-gebruik **3**

Onrechtmatig gebruik resources **10**

Informatiebeveiliging

Ongeauthenticeerde modificatie **5**



Ongeauthenticeerde toegang **86**

Malafide materiaal

Spam **5**

Malware

Command & Control server **3**

Infectie **9**

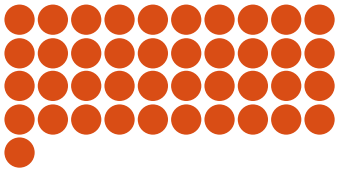
Poging tot binnendringen

Inlogpoging **1**

Misbruik kwetsbaarheid **20**

Succesvolle inbraak

Compromitatie van account **6**



Exploitatie kwetsbaarheid **41**

Verzamelen van informatie

Phishing **21**

Scannen **14**

Sniffen **2**

Dreigingsbeeld Nederlandse Gemeenten

De IBD ondersteunt gemeenten bij het gehele spectrum van informatiebeveiliging en adviseert bij de afhandeling van voorkomende incidenten. Vanuit deze brede blik signaleert de IBD de navolgende belangrijkste dreigingen voor de gemeentelijke informatievoorziening:

1. Mensen maken fouten;
2. Gemeenten zijn, net als alle organisaties, kwetsbaar;
3. Dreigingen liggen ook (vlak) buiten de eigen organisatie;
4. De waan van de dag bepaalt de agenda;
5. We weten niet wat we niet weten.

1. Mensen maken fouten

Er werken meer dan 157.000 mensen bij gemeenten. Daarnaast werken gemeenten veel samen met ketenpartners en maken ze gebruik van producten en diensten van leveranciers. Bij ketenpartners en leveranciers werkt minimaal eenzelfde aantal mensen. Persoonsgegevens van inwoners vormen de basis voor dienstverlening in de verschillende gemeentelijke domeinen. De zorgvuldige en bewuste omgang met informatie door meer dan 300.000 mensen is nodig om de beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van informatie te waarborgen. Sinds 1 januari 2016 geldt de meldplicht datalekken en sinds die tijd zijn er dagelijks meldingen van onzorgvuldige omgang met persoonsgegevens, waarvan het merendeel gemeld moet worden bij de Autoriteit Persoonsgegevens.

Voor een beveiligingsincident dat uitmondt in een datalek is vaak niet meer nodig dan een klik op een verkeerd linkje, een geadresseerde e-mail met gegevens over inwoners, een verloren laptop of het uitlenen van een toegangspas. Het grote aantal mensen dat iedere dag samenwerkt bij gemeenten, ketenpartners en toeleveranciers zorgt voor een verhoogde kans dat er iets gebeurt, of anders geformuleerd: op zo'n aantal mensen is een fout of een onzorgvuldigheid nooit helemaal uit te sluiten. De impact van een incident is hoog: een incident met persoonsgegevens is vrijwel altijd een meldplichtig datalek. Een dergelijk incident heeft impact op het vertrouwen dat inwoners hebben in de overheid. Aandacht in politiek en media versterken deze impact. De combinatie van een hoge kans dat het gebeurt en de hoge impact voor alle betrokken maakt dat de IBD deze dreiging als zeer groot risico classificeert.

Dit risico kan alleen beheerst worden als dag-in-dag-uit gewerkt wordt aan bewustzijn van medewerkers, als medewerkers veilige tools en procedures ter beschikking hebben om hun werk te doen en als bestuurders zelf het goede voorbeeld geven.

2. Gemeenten zijn, net als alle organisaties, kwetsbaar

Alle computersystemen bevatten kwetsbaarheden (lees: gaten in de beveiliging). Deze gaten in de beveiliging kunnen worden misbruikt door hackers, criminelen en statelijke actoren. De kwetsbaarheden kunnen misbruikt worden door kwaadwillenden en meestal gaat dit via een besmet bestand dat via e-mail of een website een computersysteem binnenkomt.

De grootste schade bij gemeenten ontstaat door ongerichte aanvallen van buitenaf, dit blijkt uit de bij de IBD geregistreerde meldingen van het afgelopen jaar.[1] Maar uit deze meldingen blijkt dat de meeste incidenten ontstaan doordat medewerkers van gemeenten:

- besmette websites bezoeken;
- klikken op verkeerde links in mail of klikken op besmette advertenties;
- besmette bijlagen van e-mails openen.

Bij deze besmettingen is de uiteindelijke schade vaak groter door wat er vervolgens mis gaat: bijvoorbeeld het niet goed kunnen herstarten als gevolg van onvolledige back-ups, onvolledig inzicht in het ICT-landschap en alle afhankelijkheden. Zwakheden in systemen en processen, maar ook een ongeoefend incidentmanagementproces versterken het geheel nog eens extra.

1. De IBD weet alleen wat er gemeld is en dus is het beeld mogelijk niet volledig.

E-mailadressen en internetadressen worden voortdurend bestookt met geautomatiseerde aanvalspogingen. De tijd waarbinnen een zwak systeem besmet wordt wanneer dit onbeschermd aan internet gehangen wordt is anno 2017 minder dan 10 seconden. Gemeenten zijn niet immuun voor deze dreigingen van buiten. Phishingmails (ongericht, maar soms juist heel gericht) kunnen leiden tot een verstoring van de bedrijfsvoering en/of dienstverlening. Los van de directe financiële schade ontstaat vaak ook imagoschade voor de gemeente en haar bestuurders.

De schade die ontstaat als gevolg van een verstoring van de dienstverlening komt direct voort uit het feit dat systemen en processen in de normale staat moeten worden hersteld. In de tijd die het vergt om een reservekopie terug te zetten, een controle uit te voeren op de interne systemen en alle transacties met externe systemen weer in lijn te brengen, is in de meeste gevallen een deel van de dienstverlening van de organisatie beperkt of niet beschikbaar. De IBD heeft becijferd dat de kosten van een grote besmetting met bijvoorbeeld gijzelsoftware voor een gemeente kunnen oplopen tot zo'n 100.000 euro.

In de afgelopen periode is een aantal zeer grote en ingrijpende aanvallen waargenomen die internationaal voor zeer veel schade hebben gezorgd. Nederlandse gemeenten zijn voor zover wij hebben kunnen waarnemen niet getroffen geweest. Bij een nieuwe aanval die mogelijk nog niet bekende kwetsbaarheden (zero days) misbruikt zouden gemeenten wel degelijk grote schade kunnen ondervinden. De IBD neemt waar dat deze ongerichte en grootscheepse aanvallen steeds geavanceerder worden. Daarom durven we te stellen dat de vraag niet is òf, maar wannéér de eerstvolgende (groep) gemeenten geraakt zal worden door een dergelijke malwarecampagne.

Gerichte dreigingen, zoals beschreven in het CSBN, komen voor zover de IBD dat kan vaststellen, slechts zeer beperkt voor. Wanneer ze waargenomen worden gaat het vaak om een poging om verkeer naar de gemeentelijke website te verstoren.

Deze dreiging vereist een combinatie van maatregelen, het op orde hebben van de basis, zoals beschreven in de BIG is hierbij een juist begin.

3. Dreigingen liggen ook (vlak) buiten de eigen organisatie

Beveiligingsincidenten in de informatiesystemen en bij toeleveranciers en dienstverleners kunnen voor een gemeente grote gevolgen hebben. Het is daarom belangrijk dat gemeenten regie hebben op de inkoop en volwassen zijn op het gebied van opdrachtgeverschap in alle aspecten. Gemeenten zijn verantwoordelijk voor hun informatieveiligheid en om aan deze verantwoordelijkheid te voldoen hebben zij een gemeenschappelijk normenkader om informatiebeveiliging in te richten. Dat klinkt eenvoudiger dan het in werkelijkheid is. Informatiesystemen worden geleverd en onderhouden door leveranciers en dienstverleners. Vaak zijn deze systemen volgens een bepaald dienstenmodel (als bijvoorbeeld een clouddienst) ingericht en als er dan in een dergelijk systeem persoonsgegevens verwerkt worden, dan moeten afspraken gemaakt worden in een verwerkersovereenkomst. Het blijkt in de praktijk een moeilijk proces om tot overeenstemming te komen over de inhoud van de overeenkomst en vervolgens te sturen op de gemaakte afspraken met derde partijen. Daarmee is het niet eenvoudig om grip te houden op de privacy van burgers en de daarbij horende beveiligingsmaatregelen. De technische aspecten van beveiliging moeten beoordeeld kunnen worden door de gemeente tot op de verkeersstromen van de data van en naar de informatiesystemen.

In de afgelopen periode signaleerde de IBD meerdere malen dat een incident bij een ketenpartner of een leverancier voor problemen zorgde bij meerdere gemeenten. Na analyse blijkt vaak dat er soms wel afspraken zijn, maar dat deze onvoldoende nageleefd werden of dat een discussie liep over de noodzaak van maatregelen en de bijkomende kosten. Maar ook kwam het voor dat de gemeente onvoldoende SMART (specifiek, meetbaar, acceptabel, resultaatgericht en tijdsgebonden) was in het formuleren van, en controleren op beveiligingseisen.

4. De waan van de dag bepaalt de agenda

Gemeentelijke bestuurders zijn van nature bezig met risicomanagement, dat blijkt uit de vele strategische risicoanalyses door gemeentelijke rekenkamers. Een nader onderzoek laat zien dat deze analyses vaak gaan over weerstandsvermogen in het kader van het besluit begroting en verantwoording (BBV) en dus vooral gaan over geld. Wat we nauwelijks zien is (strategisch) risicomanagement in het kader van beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen). Terwijl juiste, tijdige en volledige informatie van cruciaal belang is voor het nemen van de juiste beslissingen binnen alle processen van de gemeente. Risicomanagement op het gebied van informatiebeveiliging is nog niet voldoende volwassen, er is meestal wel beleid, maar dit leeft in het domein van de CISO en niet bij de verantwoordelijke lijnmanager, portefeuillehouder of bestuurder, omdat informatiebeveiliging op de directie- en bestuurstafel vaak niet speelt. "Pas na een incident voelen bestuurders hun verantwoordelijkheid", aldus een van de geïnterviewden.

Het onderwerp informatiebeveiliging lijkt in de praktijk pas echt op de agenda te komen na een datalek of een incident of na een rekenkameronderzoek als gevolg van een incident. De maatregelen die dan worden genomen zijn in de eerste plaats om het datalekken of het bewuste incident in de toekomst te voorkomen. De Algemene Verordening Gegevensbescherming (AVG) zorgt op dit moment wel voor verhoogde aandacht bij bestuur, media en politiek voor de vertrouwelijkheid van persoonsgegevens.

Maar informatiebeveiliging is meer dan de bescherming van persoonsgegevens. Informatiebeveiliging gaat over beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen).

Er moet veel gebeuren om de informatiebeveiliging op orde te krijgen en te houden. Een reactieve benadering (pas iets doen als het misgaat) zorgt ervoor dat een belangrijk basisprincipe naar de achtergrond verdwijnt: informatiebeveiliging is in de eerste plaats risicomanagement. Dat kan alleen met een CISO die voldoende in positie is om vertrouwd adviseur van directie en bestuur te zijn en met procesverantwoordelijken die eigenaarschap tonen. Daarnaast vraagt informatiebeveiliging om doorlopende aandacht, ook als er niets gebeurt, en moet het als proces binnen het gemeentelijk (strategisch) risicomanagement geborgd zijn.

5. We weten niet wat we niet weten

Het feit dat er in een gemeente weinig of geen incidenten lijken te zijn hoeft niet te betekenen dat er niets is gebeurd. Boven tafel krijgen van incidenten vereist een open cultuur waarin medewerkers zich vrij voelen om situaties te melden. Daarnaast is er ook een technische component: systematisch in de gaten houden wat er gebeurt in de gemeentelijke systemen, afwijkingen herkennen en hier vervolgens adequaat op reageren.

Detectie zorgt voor het vroegtijdig signaleren van afwijkingen en bedreigingen en geeft daarmee ruimte om incidenten te voorkomen voordat ze manifest worden. Detectie zorgt dat kosten als gevolg van incidenten laag blijven en incidenten uiteindelijk zelfs voorkomen kunnen worden, maar ook dat zaken die niet of nooit gezien worden wel aan het licht komen en kunnen worden aangepakt. Detectie en de reactie op meldingen vereist echter tijd van beheerders, die vanwege van de waan van de dag deze tijd vaak niet beschikbaar hebben.

Als de gemeente niet weet wat er gebeurt, dan kan ook niet worden gestuurd op risico's. Gebrek aan inzicht in wat er feitelijk gebeurt is onwenselijk omdat dit het bestuur belet om adequaat te kunnen sturen op risico's, ernaar te handelen en ervan te leren.

Het implementeren van de BIG brengt de basis op orde en daarmee kan informatiebeveiliging als proces worden ingericht waarmee de focus op detectie en actieve preventie gezien wordt als de logische vervolgstap. Nog lang niet iedere gemeente is klaar voor deze vervolgstap.

Trends en ontwikkelingen

Gemeenten hebben ook in de afgelopen jaren te maken gehad met nieuwe trends en ontwikkelingen, dit zal ook voor 2018 niet anders zijn. Diverse ontwikkelingen in de nabije toekomst, maar ook van de afgelopen periode, mogen niet onderbelicht blijven. Maar het is niet zo dat deze ontwikkelingen zorgen voor een nieuwe prioritering. In feite zijn de hier uitgewerkte punten ieder voor zich te plotten in de 5 dreigingen. De onderstaande punten moeten meer gezien worden als reminders waar ook rekening mee moet worden gehouden, want een aantal van deze komt vast en zeker een keer op de agenda komen te staan.

- Doorontwikkeling van Ransomware / Gijzelsoftware
- Scada / ICS, Internet of things en Smart Cities
- Schaarste op de arbeidsmarkt
- Cloud
- Shadow IT

Ransomware is gebaseerd op een bepaald verdienmodel en met het nemen van tegenmaatregelen, zullen de organisaties / groeperingen achter dit fenomeen op zoek gaan naar andere manieren om hun verdienmodel in stand te houden. We zagen in het afgelopen jaar al eens berichten over de dreiging van het openbaar maken van versleutelde data, dus behalve versleuteling ook actieve openbaarmaking als niet betaald wordt.

Steeds meer 'dingen' zijn verbonden met het internet. Industriële controlesystemen bedienen vitale processen zoals bijvoorbeeld bruggen, sluizen en toegangspoorten en kunnen op afstand worden bediend. Dit zogenaamde Internet-of-things of IoT krijgt in de gemeente steeds meer voet aan de grond en een toenemend aantal objecten en sensoren zijn onderdeel van het IoT, hiermee verlopen processen in de stad sneller, slimmer en veiliger, een fenomeen dat ook wel geduid wordt als Smart Cities. De keerzijde van deze ontwikkeling is dat er ook hele nieuwe privacy- en beveiligingsissues ontstaan. De eerste Ddos aanvallen met IoT-botnets zijn al waargenomen en niet zelden leiden de ontwikkelingen tot discussies over nut en noodzaak van het verwerken van privacygevoelige informatie. Het behoeft geen betoog dat de bediening van bruggen, sluizen en verkeerslichten niet mag worden gedaan door kwaadwillenden.

Ook schaarste op de arbeidsmarkt moet niet onderschat worden, nu al is het moeilijk om de juiste mensen te vinden. Gemeenten concurreren met alle andere organisaties in ons land om informatiebeveiligingsexperts. De benodigde kennis in combinatie met inzicht in de opgaven voor gemeenten is schaars en daardoor duur aan het worden.

Schaduw-ICT is het fenomeen dat er een hele wereld aan ICT-middelen bestaat buiten de 'officiële' door de organisatie beheerde systemen. Denk hierbij aan het gebruik van eigen laptops, usb-sticks, telefoons, prive-e-mail maar ook diensten als Dropbox, Wetransfer tot aan zelfontwikkelde softwarepakketten. Vaak worden dergelijke middelen gebruikt met het oog op de productiviteit, maar doordat niet is nagedacht over beheer, beveiliging en wettelijke kaders kunnen vervelende situaties ontstaan. Schaduw-ICT is DE driver voor ongewenste risico's zoals bijvoorbeeld datalekken, overtredingen van de wet en ongeautoriseerde toegang.

Vijf prioriteiten in 2018 en verder

Om de vijf belangrijkste risico's te kunnen beheersen is een samenhangende combinatie van technische en organisatorische maatregelen noodzakelijk. De IBD adviseert gemeenten voor 2018 de volgende prioriteiten te stellen:

1. Maak uw medewerkers de eerste verdedigingslinie;
2. Elimineer kwetsbaarheden uit uw organisatie;
3. Zorg voor een plan B;
4. Maak uw CISO belangrijk;
5. Organiseer het samen!

De IBD adviseert het bestuur en het management van gemeente om in samenspraak met de CISO te bepalen welke prioriteiten passen bij uw organisatie. Geen gemeente is immers hetzelfde!

1. Maak uw medewerkers de eerste verdedigingslinie

Of het nu gaat om het voorkomen van datalekken of om het herkennen van onveilige situaties; alle medewerkers zijn daarin de belangrijkste schakel. De IBD adviseert gemeenten om doorlopend werk te maken van bewustwording bij alle medewerkers in de organisatie. Het bestuur en management kunnen hieraan verder bijdragen door veilige gereedschappen ter beschikking te stellen (manieren om eenvoudig en veilig bestanden uit te wisselen, tweefactor-authenticatie, een virusscanner op de thuiswerkplek).

Verder geldt dat het ene personeelslid het andere niet is. Afdelingen, processen en functies hebben allemaal een verschillend risicoprofiel. Als u uw organisatie indeelt in risicoklassen dan kunt u het risico van iedere functie binnen uw gemeente bepalen. Door middel van screening van mensen op vertrouwensfuncties en risicofuncties verlaagt u de risico's op schendingen van de integriteit. Richt uw bewustwordingscampagnes op de verschillende groepen en hun verantwoordelijkheden.

Het management binnen de gemeente is verantwoordelijk voor het in lijn met de risicoklassen veilig maken van de processen waarvoor zij staan opgesteld. Dit vereist dat binnen de gemeente duidelijk moet zijn wat deze verantwoordelijkheden inhouden. Het lijkt erop dat de CISO deze verantwoordelijkheid heeft maar dat is niet waar. De verantwoordelijkheid van de CISO is het ondersteunen en adviseren van bestuur en management bij het invulling geven aan informatiebeveiliging. De managers die verantwoordelijk zijn voor de uitvoering van de processen, zijn zelf verantwoordelijk voor de beveiliging van de informatie die binnen deze processen wordt gebruikt.

Samenvattend

- Zorg voor bewustwording en training;
- Zorg voor veilige tools, veilige bestandsuitwisseling en beveiliging voor de thuiswerkplek;
- Classificeer functies en screen uw personeel;
- Zorg voor juiste autorisaties en functiescheiding;
- Spreek duidelijk uit wat verantwoordelijkheden zijn;
- Benoem deze verantwoordelijkheden bij de functieomschrijving of de jaarlijkse prestatieafspraken;
- Richt een apart deel van de bewustwordingscampagnes op verschillende groepen en hun verantwoordelijkheden.

2. Elimineer kwetsbaarheden uit uw organisatie

Computersystemen zijn niet foutloos, ze zijn immers ook gemaakt door mensen en dus bevatten alle computersystemen zwakheden en kwetsbaarheden. Jaarlijks verstuurt de IBD zo'n 6.000 waarschuwingen en iedere gemeente ontvangt per dag gemiddeld twee waarschuwingen op de eigen systemen. Dat wil zeggen: mits de gemeente aan de IBD de systemen en applicaties doorgeeft waarop zij gewaarschuwd wenst te worden. Nog niet iedere gemeente is aangesloten op deze kwetsbaarhedendienstverlening van de IBD. Voor deze gemeenten geldt de invulling

van stap 4 (de ICT-foto) in het aansluitproces als hoogste prioriteit. Voorkomen is immers beter dan genezen.

We nemen waar dat gemeenten vaak de nadruk leggen op nieuwe processen en systemen (in projectverband), maar dat daardoor het beheer van de bestaande infrastructuur niet de juiste aandacht krijgt. Het beheer van de bestaande processen en systemen moet voldoende aandacht blijven krijgen opdat de bestaande dienstverlening gewaarborgd blijft.

Informatiebeveiliging heeft niet alleen te maken met systemen. Uw organisatie zelf bevat ook kwetsbaarheden. Weet u zeker dat uw bezoekers (ook de ongenode) alleen op plaatsen kunnen komen waar ze mogen komen? De IBD adviseert ook gaten in de fysieke beveiliging in het oog te houden.

Ethische hackers kunnen u helpen om digitale kwetsbaarheden in uw organisatie op te sporen. Een goede omgang met ethische hackers vereist heldere afspraken, een manier om dat in te richten is met een zogenaamd Responsible Disclosure beleid. Voor gemeenten die dat niet hebben adviseert de IBD een beleid te maken op basis van ons voorbeeld en dat te publiceren op de gemeentelijke website. Daarnaast kunnen mystery guests gaten opsporen in uw fysieke beveiliging.

Een penetratietest geeft uw organisatie inzicht in de technische en organisatorische digitale beveiliging. U kunt opdracht geven om de informatiebeveiliging van uw gemeente eens te laten bekijken door de ogen van een onafhankelijke buitenstaander. Dat geeft soms verrassende inzichten.

Een vulnerability scan kan zichtbaar maken welke componenten kwetsbaarheden bevatten omdat ze niet voorzien zijn van de laatste softwareversie en updates. Als blijkt dat er geen oplossing is voor een bepaalde kwetsbaarheid, dan kunt u beslissen om andere maatregelen te nemen om de zwakheid te mitigeren. Daarnaast maakt een dergelijke scan ook inzichtelijk of de apparatuur en software wel voldoende bestand tegen aanvallen van buitenaf.

Samenvattend

- Zorg dat u weet welke systemen uw organisatie gebruikt (denk ook aan IoT). Een assetscan kan helpen te identificeren welke bekende en onbekende componenten zich in een omgeving bevinden;
- Zorg dat u op de hoogte bent van kwetsbaarheden van uw systemen;
- Sluit aan op stap 4 van de IBD-dienstverlening;
- Zorg dat u op de hoogte bent van kwetsbaarheden in uw organisatie;
- Sta open voor meldingen van ethische hackers (en stel hiervoor Responsible Disclosure beleid op);
- Laat regelmatig een penetratietest doen;
- Voer regelmatig vulnerability scans uit van de kroonjuwelen;
- Laat een mystery guest de fysieke veiligheid en bewustwording van medewerkers onderzoeken.

3. Zorg voor een plan B

Als u voldoende inzicht heeft in de risico's die gelden voor uw eigen organisatie dan kunt u maatregelen treffen om de belangrijkste risico's weg te nemen, te beperken of te accepteren. U kunt ook maatregelen treffen om te zorgen dat uw kritische bedrijfsprocessen door kunnen gaan, ongeacht de oorzaak of het risico. De IBD adviseert gemeenten een beleid te maken voor bedrijfscontinuïteit, u kunt hiervoor de handreiking van de IBD gebruiken. Dat houdt in dat u voor de eigen organisatie bepaalt wat de kritische bedrijfsprocessen zijn en op welk niveau u deze processen wilt laten doorgaan in de ergst denkbare gevallen van uitval. Welk risico bent u bereid te accepteren en tegen welke kosten bent u bereid maatregelen te nemen? Tijd voor een goed gesprek tussen de CISO, het management en het bestuur.

Samenvattend

- Definieer uw kritieke processen;
- Maak beleid om uw kritieke bedrijfsprocessen te kunnen laten doorgaan, ook in geval van een incident;
- Beoefen dit bedrijfscontinuïteit beleid minimaal jaarlijks uitgebreid en leer hiervan om het beter te maken.

4. Maak uw CISO belangrijk(er)

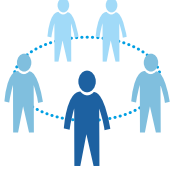
Een sterke inbedding van informatiebeveiliging in de organisatie vraagt om een CISO met voldoende mogelijkheden om effectief te zijn. De CISO zit bij voorkeur iedere maand aan tafel bij de directie / het managementteam en het bestuur om ze bij te praten over de vorderingen en de uitdagingen die hij/zij signaleert in de gemeentelijke organisatie, gevoed vanuit een netwerk van vakgenoten in de regio en daarbuiten.

De nieuwe verantwoordingssystematiek ENSIA (Eenduidige Normatiek Single Information Audit) startte in 2017 en heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen. Uw CISO is bij uitstek de persoon om binnen de gemeente de linking pin te zijn die duiding geeft aan de stand van zaken. De IBD adviseert gemeenten om dit momentum te benutten om uw CISO de positie te geven die recht doet aan de functie.

Samenvattend

- Geef uw CISO positie, tijd en mandaat;
- Geef uw CISO de middelen en tools om inzicht en overzicht te houden (ISMS/GRC);
- Investeer in uw CISO;
- Benut het momentum van ENSIA.

5. Organiseer het samen!



Gemeenten werken allemaal op hun eigen manier en op eigen tempo aan informatiebeveiliging. Er zijn verschillen tussen gemeenten. Toch hebben ze veel gemeen: de taken en verantwoordelijkheden, uitdagingen en toepassingen hebben allemaal aspecten die voor meerdere gemeenten (zo niet alle) toepasbaar zijn. Door kennis te delen en documenten voor anderen beschikbaar te maken helpen gemeenten elkaar. Samen betekent ook dat netwerken met CISO's van bedrijven in de regio een zeer goede aanvulling is en leidt tot verrassende inzichten. We kennen gemeenten die in regionaal verband zeer succesvolle contacten onderhouden wat zorgt voor wederzijdse kennisverhoging en slimme oplossingen. Op bovengemeentelijk niveau fungeert de IBD als verbinder en versneller en zij helpt graag om uw kennis toepasbaar te maken voor alle gemeenten of kennis van andere gemeenten toepasbaar te maken voor uw organisatie. Deel uw praktijkvoorbeelden (op de IBD Community of stuur ze naar de IBD) en maak gebruik van voorbeelden van anderen.

De IBD is 24/7 bereikbaar voor gemeenten om ze bij te staan bij informatiebeveiligingsincidenten. Gemeenten weten de IBD in spoedgevallen goed te vinden. In niet spoedgevallen of in situaties waarin de gemeente de afhandeling zelf goed aankan wordt niet altijd een melding bij de IBD gedaan. Toch is het in het belang van alle gemeenten om dergelijke incidenten toch te melden. Een incident in één gemeente kan eenvoudig uitgroeien tot een incident voor meerdere gemeenten, hoe klein en hoe eenvoudig een incident soms ook op het eerste gezicht lijkt te zijn. De IBD heeft ook een besloten community ingericht waar kennis gedeeld kan worden tussen gemeenten, deze community wordt veel gebruikt om kennis te halen, delen kan nog wat beter.

Samenvattend

- Deel uw kennis met andere gemeenten;
- Onderhoud contacten met (regionale) CISO's uit het bedrijfsleven;
- Maak gebruik van bestaande praktijkvoorbeelden;
- Meld uw incidenten bij de IBD;
- Vorm gebruikersgroepen met andere gemeenten om krachten te bundelen richting bedrijfskritische leveranciers;
- Deel uw kennis en ervaring op de IBD-community.

Colofon

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

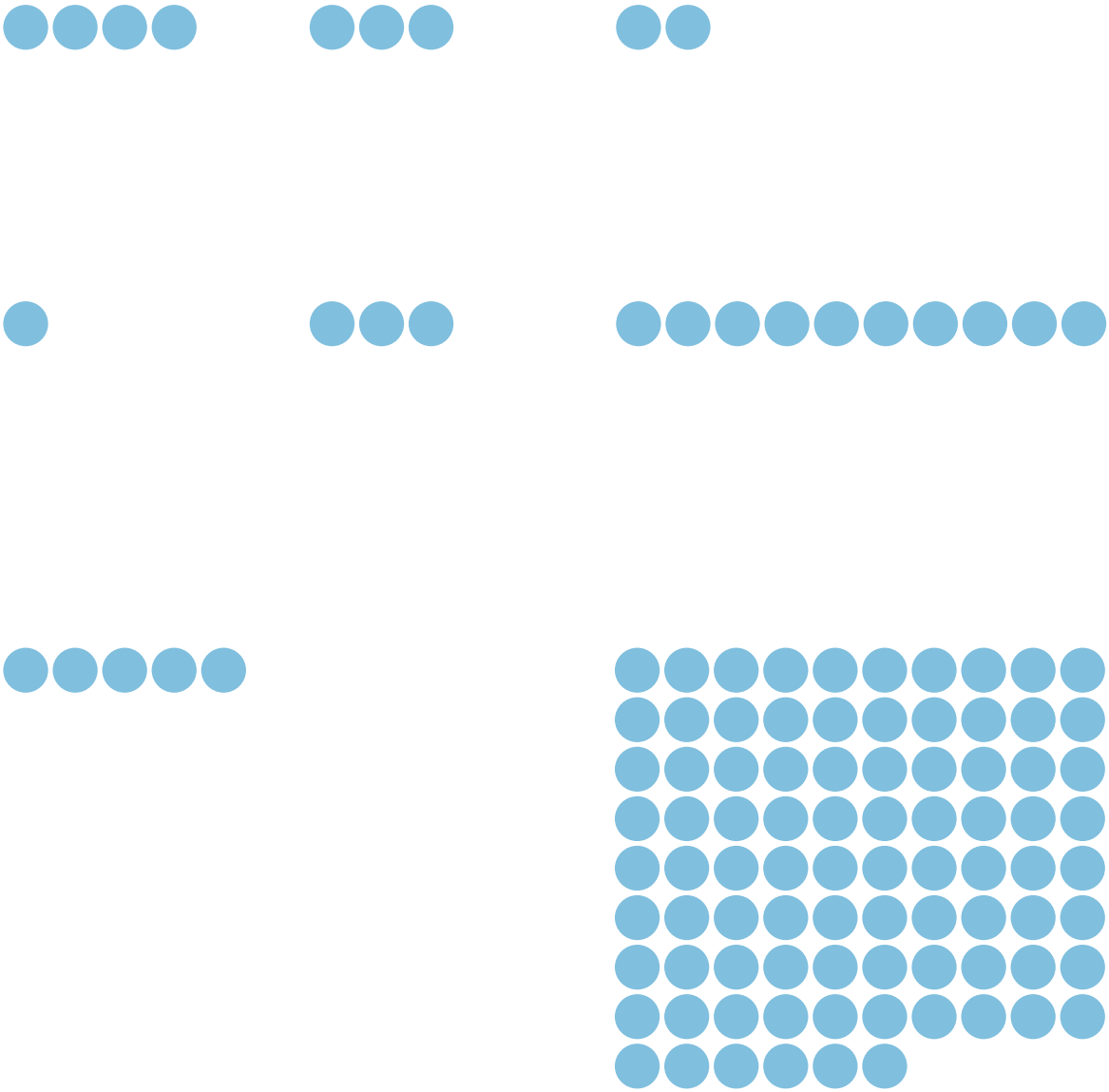
De IBD is ondergebracht bij VNG Realisatie.

Ontwerp

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

INFORMATIE
BEVEILIGINGS
DIENST

VNG
Realisatie



INFORMATIE BEVEILIGINGS DIENST

Nassaulaan 12
2514 JS Den Haag
070 204 55 11
info@IBDGemeenten.nl