Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2021/2022

INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie


Alkmaar Almelo
Bergeijk
Brunssum
Dongeradeel
Franekeradeel
Haaksbergen
Heiloo
Maas
Losser
Mook en Middelaar
Nunspeet
Papendrecht
Rotterdam
Staphorst
Utrechtse Heuvelrug
Wageningen
Woudenberg
INFORMATIE
BEVEILIGINGS
DIENST

Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2021/2022

INFORMATIE
BEVEILIGINGS
DIENST

De IBD heeft het Dreigingsbeeld 2021/22 opgesteld op basis van een analyse van incidentrapportages van gemeenten, meldingen aan de IBD en interviews met gemeentelijke CISO's,- FG's, - managers en gemeentesecretarissen. Het Dreigingsbeeld informatiebeveiliging Nederlandse Gemeenten verschijnt iedere twee jaar.

Inleiding

In het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2021/2022 gaan we specifiek in op de risico's voor de ambtelijke organisatie, het bestuur, de politiek, de inwoners en de ondernemers. Het belang van dit thema komt voort uit gesprekken met gemeente-secretarissen, managers en medewerkers van gemeenten.

Informatiebeveiliging is immers risicomanagement. Het onderwerp lijkt op het eerste gezicht technisch en complex, maar niets is minder waar. Management en bestuur zijn bij uitstek in staat om risico's ten aanzien van de informatievoorziening op waarde te schatten en zelf keuzes te maken. Ook de maatregelen om risico's tot een acceptabel niveau terug te brengen zijn maar deels technisch van aard.

Sturen op veilig gedrag, naast sturen op snel, efficiënt en kosteneffectief werken, vergt doorlopende aandacht van het management. Geen medewerker wil een datalek, een hack of een storing veroorzaken. Toch gebeurt dat af en toe wel doordat men niet wordt beoordeeld op veilig gedrag, en omdat de beschikbare middelen niet aansluiten bij de behoefte van medewerkers. Het is zaak een digitale veiligheidscultuur te cultiveren waarin veilig werken beloond wordt, medewerkers niet schromen om onveilige situaties te melden en waarin onveilige situaties ook daadwerkelijk worden voorkomen of verholpen.

Dit dreigingsbeeld is bedoeld om gemeentemanagers te helpen in hun risicomanagement door de belangrijkste bedreigingen te duiden. We identificeren de belangrijkste risico's voor bestuur, politiek, de ambtelijke organisatie en inwoners en ondernemers en doen suggesties voor handelingsperspectief voor management en directie. We leiden risico's waar mogelijk in met een actueel voorbeeld.

Over de voorbeelden

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

Actueel dreigingsbeeld

De gemeentelijke informatievoorziening is kwetsbaar. We onderscheiden daarin een aantal categorieën van dreigingen in volgorde van belangrijkheid.

Intern en onbedoeld

In de eerste plaats zijn er dreigingen door onbedoelde neveneffecten van logisch menselijk handelen. Medewerkers van gemeenten doen hun best om het werk snel, efficiënt en kwalitatief goed te doen. Bureaucratie is 'uit' en ondernemerschap is 'in'. De kortste weg naar het resultaat is er vaak één met valkuilen. Voorbeelden van dergelijke dreigingen zijn e-mails met gevoelige gegevens aan de verkeerde geadresseerde, verloren USB-sticks en het per ongeluk wissen van bestanden.

Extern, bedoeld maar ongericht

Verreweg het grootste deel van de incidenten vanuit een externe actor komt voort uit geautomatiseerde bulkaanvallen. Kwaadwillenden scannen het internet af op bekende zwakheden in hard- en software, proberen veelvoorkomende gebruikersnaam-wachtwoordcombinaties of sturen honderdduizenden phishingberichten aan elk adres dat ze tot hun beschikking hebben. Gemeenten zijn dan gewoonweg het slachtoffer omdat ze aangesloten zijn op het internet, doorgaans niet omdat ze de Nederlandse overheid zijn. De gevolgen van ongerichte aanvallen kunnen groot zijn: de meeste aanvallen met gijzelsoftware zijn in eerste instantie ongericht. Het komt voor dat buitgemaakte inloggegevens van ongerichte aanvallen worden aangeboden aan de hoogste bieder. In zo'n geval kan een ongerichte aanval het opstapje vormen voor een gerichte aanval.

Extern, bedoeld en gericht

Veel aandacht gaat uit naar gerichte dreigingen van hackers en criminelen. Dit fenomeen levert spannende verhalen op in de media. Dit zijn tevens de gevallen die we maar heel moeilijk kunnen ontdekken[1] en die we bij de IBD (dus) relatief weinig tegenkomen. Een dergelijke gerichte aanval start vaak met onderzoek door de hacker naar informatie die kan worden gebruikt bij een hack. Op sociale media zoals LinkedIn is veel op het oog onschuldige zakelijke informatie te ontdekken waar een kwaadwillende zijn voordeel mee kan doen. De wat meer gesloten bronnen leveren nog meer informatie op.
Er circuleren lijsten met miljarden gestolen gebruikersnamen en wachtwoorden van eerdere hacks.[2] De IBD krijgt meldingen van doelgerichte inlogpogingen op systemen of gerichte phishingmails met een keurige aanhef en een plausibele aanleiding met het doel om geld of (inlog) gegevens buit te maken. Digitaal vandalisme zoals het platleggen van websites[3] scharen we ook onder deze dreigingscategorie.

Een medewerker van de salarisadministratie ontvangt vlak voor de salarisdatum in mei een e-mail van 'een collega' met het verzoek om het rekeningnummer te wijzigen. De medewerker van de salarisadministratie vraagt nog om het volledige IBAN-nummer en maakt ruim 2800 euro over naar het nieuwe rekeningnummer. De echte medewerker trekt iets later aan de bel omdat die geen salaris heeft ontvangen. De gegevens van zowel de medewerker salarisadministratie als de collega zijn op LinkedIn te vinden.[4]

Intern en bedoeld

De meest riskante dreiging komt van binnen de organisatie. Medewerkers met kwade bedoelingen kunnen uit hoofde van hun functie bij veel gegevens en systemen. Vooral medewerkers met verhoogde toegangsrechten zoals ICT-beheerders en management kunnen grote schade aanrichten. Deze dreiging is nog moeilijker te ontdekken. Interne medewerkers kennen de interne processen en controlemechanismen en kunnen die daarom beter omzeilen dan iemand van buiten.

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 gebeurt. Besef dat er in elke organisatie incidenten zijn. Als de directie en het management die niet kennen, dan is dat zorgelijk. Het 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.[5]

Risico's voor de ambtelijke organisatie

De meest prominente risico's manifesteren zich in de ambtelijke organisatie; bij de ambtenaren die iedere dag gebruikmaken van informatie- en communicatiesystemen om hun werk te doen. In het eerste halfjaar van 2020 deden zich twee situaties voor die het belang van beschikbaarheid van informatiesystemen onderstrepen.

Risico: bedrijfscontinuïteit in het geding

Of het nu door een technische oorzaak komt (fouten in hard- en software) of door een niet technische oorzaak (een faillissement van een dienstverlener, een pandemie, een brand, een vlooienplaag, een overstroming, enzovoort). Het kan voorkomen dat het werk niet kan doorgaan zoals dat normaal gaat. Deze risico's vinden een oorzaak in de digitale wereld of ze manifesteren zich uiteindelijk in het feit dat een computersysteem niet werkt.

Kwetsbaarheden in de systemen van Citrix[6], veel gebruikt voor het faciliteren van werken op afstand, waren zo ernstig dat dit systeem een aantal dagen van de buitenwereld moest worden afgesloten. Het gevolg: ambtenaren konden in veel gevallen niet meer thuiswerken, kantoren waren overbelast, werkprocessen lagen in sommige gevallen stil.
Enkele weken later noopten de maatregelen om verspreiding van COVID-19 te voorkomen ertoe dat Nederlanders zo veel mogelijk thuis gingen werken en vergaderen, een situatie die in elk geval tot ver na het verschijnen van dit dreigingsbeeld aanhoudt.

Per proces hoort bekend te zijn wat de kernfunctie is en hoe die door middel van een informatiesysteem wordt ondersteund. Gemeenten dienen een plan te hebben voor uitval of onbeschikbaarheid van een informatiesysteem. Risico's met betrekking tot de bedrijfscontinuïteit nemen toe, omdat online processen steeds meer de standaard worden en de offline alternatieven verdwijnen. Waarbij vroeger voor een aanvraag een papieren

formulier met handtekening nog werd overgenomen in een computersysteem, is nu de online aanvraag de directe start van een aanvraagproces. Wanneer een systeem uitvalt kan niet worden teruggevallen op papieren processen.

Integriteit van gegevens is niet gewaarborgd

U vertrouwt erop dat de persoon die inlogt in een systeem ook degene is aan wie u toestemming heeft gegeven om dat te doen en dat deze persoon op dat moment ook een gegronde reden heeft om in te loggen. Om technische (een hack) en niet-technische (een medewerker met kwade bedoelingen) redenen kan het zijn dat iemand werk uitvoert dat niet de bedoeling is. Een kwaadwillende kan in zo'n geval gegevens wijzigen, wissen of toevoegen. Een onterechte factuur indienen of goedkeuren, vergunning verstrekken, een uitkering toewijzen, het bepalen van een hoogte van een vergoeding, het verstrekken van een paspoort: dat begint allemaal met het invoeren van gegevens in informatiesystemen.

Een ambtenaar van de gemeente is ontslagen nadat hij voor een bedrag van ruim twee miljoen euro had gefraudeerd. De man zou onder meer achteraf passages aan verslagen hebben toegevoegd. De gemeente probeert de schade die uit de fraude voortkomt zoveel mogelijk te verhalen op de ambtenaar. Er is beslag gelegd op de bezittingen van de ex-medewerker.[7]

Vertrouwelijke gegevens in verkeerde handen

Een e-mail aan een verkeerd mailadres, een foutje in de toegangsrechten van een gedeelde map (menselijke fouten) of een onontdekt lek in een systeem (technische fouten) of een ongedicht lek in een systeem (een combinatie van menselijke en technische fouten) kunnen ertoe leiden dat vertrouwelijke informatie onbedoeld onder ogen van ongeautoriseerde personen komt. De gemeente werkt met legio vertrouwelijke gegevens over inwoners, maar ook over de eigen bedrijfsvoering: denk aan aanbestedingen, plannen, memo's, salarissen.

Een ambtenaar van de gemeente stuurde onbedoeld een phishing-mail naar zijn volledige adressenbestand. De e-mail kwam ook bij inwoners terecht. De ambtenaar had zelf een e-mail gekregen van oplichters en klikte op een link in het bericht. Daardoor ontstond een sneeuwbaleffect en werd het bericht doorgestuurd naar honderden contacten.[8]

Bij een mailing aan ondernemers waren e-mailadressen zichtbaar voor anderen, 847 in totaal. De mailing was bedoeld om ondernemers, die zich in het kader van de Tijdelijke overbruggingsregeling zelfstandig ondernemers bij de gemeente hadden gemeld, actief te wijzen op de vervolgregeling. Geen van de ondernemers heeft volgens de gemeente vanuit de mailing alle mailadressen kunnen zien, alleen de mailadressen uit de groep waarin de ondernemer was opgenomen.[9]

Risico's voor het openbaar bestuur en de politiek

Imagoschade

Fouten van medewerkers worden het bestuur aangerekend. Daarnaast krijgen bestuurders en politieke ambtsdragers veel gevoelige en vertrouwelijke informatie onder ogen. Een zorgvuldige omgang is vereist. Het vertrouwen in de gemeente en de ambtsdragers kan ernstig worden aangetast als (vertrouwelijke) informatie wordt gebruikt om er zichzelf of anderen mee te bevoordelen. Belangrijk is ook om (digitale) stukken goed op te bergen en de interne beveiligingsinstructies op te volgen die gelden voor gebruik van smartphones, tablets en pc's, etcetera. Het vertrouwen in de overheid hangt onder meer samen met de wijze waarop men omgaat met gegevens. Dat wil zeggen: inwoners van de gemeenten moeten er op kunnen vertrouwen dat de gemeente gegevens op een passende manier beschermt en plannen uitvoert zoals ze zijn afgesproken.

Na het openbaar maken van persoonlijke gegevens, moest de betreffende wethouder van de post leerlingenvervoer afgehaald worden. De motie is ingediend door drie partijen.[10]

Financiële schade

Op meerdere manieren kan een gemeente geconfronteerd worden met financiële schade als gevolg van ontbrekende informatiebeveiliging. De gemeente Lochem werd op een haar na slachtoffer van gijzelsoftware[11] maar had toch enkele tienduizenden euro's schade als gevolg van het stilleggen van de dienstverlening, het forensisch onderzoek en het herstellen van de ICT-omgeving. Wanneer de gemeente daadwerkelijk zou zijn getroffen door gijzelsoftware hadden de kosten kunnen oplopen tot honderdduizenden of zelfs miljoenen euro's. Een ambtenaar, bestuurder of raadslid kan bedoeld of onbedoeld informatie verschaffen waar een kwaadwillende zijn voordeel mee kan doen (en de

gemeente gedupeerd achterblijft). Informatie rond bestemmingsplannen, aanbestedingen of veranderende regels kan zeer waardevol zijn.

Onzorgvuldige omgang met persoonsgegevens en overtredingen van de Algemene verordening gegevensbescherming (AVG) kunnen leiden tot aansprakelijkheidsstellingen van getroffenen of boetes van de privacy-toezichthouder. Een boete wegens onzorgvuldig handelen met de privacy van inwoners zou bovendien leiden tot grote imagoschade.

In een gemeente moest een bestemmingsplan worden gewijzigd. Een bewoner informeerde ernaar bij een raadslid, een kennis van hem. Gewoon, uit belangstelling, zo leek het. Hij vroeg of het raadslid hem op de hoogte wilde houden. Degene die het vroeg, bleek grondposities te verwerven. Het raadslid had hem, te goeder trouw en zich van geen kwaad bewust, verteld over het bestemmingsplan en hoe dit in de raadsvergaderingen werd besproken. De bewoner is zo grondig geïnformeerd door het raadslid, dat hij tonnen euro's heeft verdiend aan het definitieve bestemmingsplan. Het raadslid had dit niet zien aankomen en is diep door het stof gegaan toen de zaak aan het licht kwam, ook al is hij uiteindelijk niet vervolgd door het OM.[12]

De Amerikaanse stad Baltimore, die in mei 2019 door een omvangrijke aanval met gijzelsoftware werd getroffen, heeft besloten om 6 miljoen dollar die was gereserveerd voor parken en openbare voorzieningen aan cybersecurity uit te geven. Het geld is bedoeld om de impact van het incident te bekostigen.[13] [14]

Schade aan democratische processen

Inbreuken op de beschikbaarheid, integriteit en vertrouwelijkheid van informatiesystemen kunnen het democratische proces aantasten. Dit geldt voor zowel verkiezingen als stemprocessen van volksvertegenwoordigers. Raadsleden moeten ervan op aan kunnen dat hun stem op de juiste wijze wordt verwerkt en dat ze hun stem kunnen baseren op de juiste informatie. Bovendien is bij verkiezingen het stemgeheim een groot goed.

Het kabinet verbiedt het gebruik van de onveilige software waarmee de stemmen van de Tweede Kamerverkiezingen werden opgeteld.[15]

De privégegevens van alle stemgerechtigden in Israël liggen op straat omdat een app gebruikt bij de verkiezingen een datalek had. Dat ontdekte de Israëlische krant Haaretz. Bij het lek kwamen de volledige namen, adressen en identiteitskaartnummers van de 6,5 miljoen burgers op straat te liggen. Dat zijn alle Israëliërs die oud genoeg zijn om te stemmen.[16]

Risico's voor de inwoners en de ondernemers

Gegevens in verkeerde handen

Gemeenten worden geacht als goed huisvader om te gaan met de gegevens die ze onder hun hoede hebben. Als de informatie van de overheid in verkeerde handen komt zijn de mogelijke gevolgen voor inwoners en ondernemers bijna niet te overzien. Inwoners zijn voor veel gevoelige zaken afhankelijk van de overheid: zorg, werk, inkomen en andere voorzieningen. Tijdens de coronacrisis is een derde van de Nederlandse werkenden afhankelijk van regelingen die geheel of gedeeltelijk worden uitgevoerd door gemeenten.[17] Bijna één op de tien kinderen en jongeren maken gebruik van jeugdzorg.[18] Als over individuele gevallen informatie uitlekt, zijn de betrokkenen daar direct de dupe van.

Twee klokkenluiders ontdekten dat door een fout ruim 3000 dossiers van kwetsbare kinderen op internet openbaar werden. Ze stapten naar RTL Nieuws om de zaak aanhangig te maken. In de dossiers is zeer persoonlijke informatie te vinden, zoals psychische stoornissen, details over misbruik en zelfmoordpogingen.[19]

Het Centrum voor Jeugd en Gezin ontdekte dat onbevoegden zich door middel van phishingmails toegang hadden verschaft tot enkele e-mailboxen van medewerkers. Daarop is direct actie ondernomen. Zo is er een melding gedaan bij de Autoriteit Persoonsgegevens en is het interne beleid voor veilig digitaal werken aangescherpt. Aan alle betrokkenen is een brief gestuurd.[20]

Op Telegram, een populaire chat-app, zijn publieke kanalen waar illegale goederen worden verhandeld, met name drugs. In diezelfde kanalen bieden mensen ook aan om de NAW-gegevens van kentekens te achterhalen. 'Binnen één uur een hit met naam en adres', wordt er geadverteerd. De kosten variëren van 50 tot

150 euro. De verkopers, die als tussenpersonen fungeren, stellen 'mensen bij de RDW' te kennen die toegang hebben tot het kentekenregister. Het telefoonnummer werd geregeld via een 'ingang bij de gemeente'.[21]

Dienstverlening van de gemeente niet beschikbaar

Als de dienstverlening van de gemeente niet of verminderd beschikbaar is, dan kunnen inwoners en ondernemers daar hinder van ondervinden. In sommige gevallen zal er sprake zijn van licht ongemak wanneer een inwoner diensten of producten een paar dagen later geleverd krijgt. Uitval van meerdere dagen of zelfs langer kan serieuze maatschappelijke, economische en sociale gevolgen hebben.

De standaardprocedures bij een ICT-storing van de gemeente hadden bij twee grote storingen in 2019 niet het gewenste effect. Ook schoot de communicatie met de stad te kort. De verantwoordelijk wethouder neemt maatregelen.[22]

Ontwrichting van alledaagse processen

Veel van de systemen die ervoor zorgen dat alledaagse processen goed verlopen worden aangestuurd door computersystemen. Procesautomatisering gaat onder andere over doorstroming van het verkeer, regulering van de waterstand of de toegangsverlening tot gebouwen of faciliteiten. Ook hier kunnen menselijk handelen (bedoeld of onbedoeld) of de techniek leiden tot verstoringen van de beschikbaarheid (uitval van systemen) en integriteit (groen licht in plaats van rood licht, brug open in plaats van brug dicht of ontregeling van rioleringspompen).

Een ernstig beveiligingslek in een verkeerslichtcontrolesysteem maakt het mogelijk om het systeem over te nemen en de werking van verkeerslichten te beïnvloeden. Op een schaal van 1 tot en met 10 wat betreft de impact van de kwetsbaarheid is die met een 10 beoordeeld.[23] [24]

De Maastunnel had sinds10:30 uur last van een storing. Rond 15:30 uur werd de route van Noord naar Zuid weer vrijgegeven. Rond 17:00 uur is ook de buis van Zuid naar Noord weer open. Eerder op de ochtend waren er problemen in de buis van Noord naar Zuid. Het besturingssysteem van de tunnel was toen in storing, waardoor de verkeerslichten op rood bleven staan en de slagbomen naar beneden bleven. Bij het herstarten van dit systeem werd het probleem erger, waardoor nu ook de andere tunnelbuis dicht ging. De afsluiting leidde in de stad tot verkeersproblemen. De Laan op Zuid en de Westzeedijk stonden vast.[25]

De storingen bij de Julianabrug komen vermoedelijk door een fout in het besturingssysteem. De aannemer gaat deze week verder met testen en hoopt eind deze week een definitieve uitslag te hebben. Vanwege de storingen is onlangs besloten dat er voorlopig permanent een monteur bij de brug aanwezig moet zijn. De monteur blijft de brug monitoren totdat de brug minimaal twee weken achter elkaar storingsvrij draait.[26]

Handelingsperspectief voor management en directie

Voer de regie over risicomanagement

Het voorkomen van menselijke fouten, opzettelijk handelen, technische fouten en combinaties daarvan is pas echt goed mogelijk door per proces zorgvuldig te kijken naar de risico's. Dat is in de eerste plaats een taak voor het management. 'De business' (het échte werk en het primaire proces) staat centraal wanneer u praat over risico's en mogelijkheden om daarmee om te gaan. De Chief Information Security Officer (CISO) is, mits goed gepositioneerd, in staat om u goed te adviseren over maatregelen om risico's tot een acceptabel niveau terug te brengen. Zorgt u er ook voor dat u bij het risicomanagement periodiek de cyclus van plannen, uitvoeren, controleren en bijstellen doorloopt.

Besef dat techniek niet de belangrijkste factor is

De techniek is niet de belangrijkste factor bij informatiebeveiliging. U kunt immers nog zo'n veilig toegangssysteem installeren, als de pasjesuitgifte niet klopt met rollen en rechten van het actuele personeelsbestand dan bevinden de zwakke schakels zich nog steeds in het werkproces en in de factor mens.

Cultiveer een veilige organisatie

Uiteraard beloont u medewerkers voor snelheid, efficiency en ondernemerschap. Inwoners en ondernemers verwachten niets minder dan een overheid die snel, efficiënt en kwalitatief hoogwaardig werk levert. Probeer ook veilig werken te belonen. Daarbij kan worden gekeken naar hoe men bijvoorbeeld in de bouwsector veiligheid stimuleert.[27] Verlies hierbij de samenwerkingsketens niet uit

het oog. U kunt het nog zo veilig aanpakken, als men er bij een ketenpartner of een leverancier een andere aanpak op nahoudt, kunt u alsnog voor nare verassingen komen te staan. Te allen tijde geldt: de directie en het management geven het goede voorbeeld.

Bied veilige gereedschappen

Zorgt u ervoor dat efficiency, snelheid en ondernemerschap op een veilige manier mogelijk worden gemaakt. In veel gevallen is de snelste weg om informatie van a naar b te krijgen niet de veiligste: even een mailtje of een appje, dat ene grote bestand fijn snel versturen of samenwerken in een gedeelde map via een gratis internetdienst.

Bekijk wat de medewerkers nodig hebben en faciliteer die functionele behoefte als werkgever. Als u ervoor zorgt dat de snelste manier ook de veiligste manier is, of beloont dat medewerkers net dat stapje meer zetten om de veiligheid te waarborgen (leuker kunnen we het niet maken, wel veiliger), dan verhoogt u de veiligheid in uw organisatie.

Zorg voor een open cultuur

Medewerkers moeten zich veilig weten om onveilige situaties, incidenten of ongelukken te melden. In sommige organisaties is sprake van een afrekencultuur waarin fouten maken niet wordt getolereerd. Dat zorgt ervoor dat situaties onder de pet blijven en pas als het veel te laat is naar buiten komen. Zorg ervoor dat medewerkers ook kunnen leren van incidenten.

Faciliteer dat de basis op orde komt

De IBD identificeerde op basis van de normen voor de Nederlandse overheid een set aan basismaatregelen en -processen die gemeenten in elk geval op orde dienen te hebben als basisbescherming voor algemene risico's. De IBD heeft hiervoor het ondersteuningsprogramma 'Verhogen Digitale Weerbaarheid' opgezet. Het is de

inschatting van de IBD dat 99% van alle technische incidenten kan worden voorkomen met het op orde hebben van deze zaken.[28] Het gaat hierbij in het kort om:

1. Weten wat je in huis hebt (configuratiemanagement).
2. Dat up-to-date houden (patchmanagement en changemanagement).
3. Veilig inrichten van de ICT-omgeving (juiste instellingen en de juiste beschermingsmiddelen).
4. Toegangsbeheer (rollen en rechten beheren, veilige manieren van inloggen).
5. Monitoren wat er gebeurt, trends herkennen en afwijkingen signaleren.

Bespaar niet op beheer van ICT

Ad. 1. en 2. zijn beheerfuncties van de ICT-afdeling – een post waar besparing op korte termijn geen nadelige effecten lijken te hebben, maar waarvan de gevolgen op lange termijn rampzalig kunnen zijn.

Koester uw informatiebeveiligingsspecialisten en werk samen

Ad. 3., 4. en 5. zijn specialistische taken van informatiebeveiligers. De expertise is schaars en gemeenten concurreren met de markt om deze expertise. Koester uw eigen specialisten en werk waar mogelijk samen met andere gemeenten. De IBD faciliteert deze samenwerking waar dat kan.

Ons advies: praat regelmatig met uw CISO over de stand van zaken rond het verhogen van de digitale weerbaarheid en identificeer waar u mogelijk drempels kunt wegnemen.

Oefen en wees voorbereid op incidenten

Incidentmanagement is een zaak van directie en management. Het is van groot belang dat u weet wie u aan tafel wilt hebben als een incident dreigt of optreedt. Zorg dat u regelmatig de crisisstructuur oefent en maak hierbij gebruik van voor de eigen organisatie herkenbare scenario's.

Meer weten?

Voor meer informatie over dit onderwerp raadt de IBD de volgende documenten aan:

- De handreiking Risicomanagement door lijnmanagers van de IBD[29]
- De gemeentelijke Agenda Digitale Veiligheid 2020-2024[30]
- Handreiking De 10 bestuurlijke principes voor informatiebeveiliging[31]
- Cybersecuritybeeld Nederland (CSBN) 2020 van het Nationaal Cyber Security Centrum[32]
- Leren van Lochem: lessen uit een informatiebeveiligingsincident[33]
- Kwetsbaarheden in Citrix: Lessen voor gemeenten en de IBD[34]
- Documentatie van de gijzelsoftware-aanval bij de Universiteit Maastricht[35]

Bedreigingen

Ambtelijke organisatie

Bedrijfscontinuïteit in het geding

› pag. 7

Integriteit van gegevens

› pag. 8

Gegevens in verkeerde handen

› pag. 8

Openbaar bestuur en de politiek

Imago-schade

› pag. 10

Financiële schade

› pag. 10

Democratische processen

› pag. 12

Inwoners en de ondernemers

Gegevens in verkeerde handen

› pag. 13

Dienstverlening niet beschikbaar

› pag. 14

Ontwrichting processen

› pag. 14

Handelingsperspectieven

Voer regie over risicomanagement

› pag. 16

Techniek niet de belangrijkste factor

› pag. 16

Cultiveer veilige organisatie

› pag. 16

Bied veilige gereedschappen

› pag. 17

Zorg voor open cultuur

› pag. 17

De basis op orde

› pag. 17

Oefen en wees voorbereid

› pag. 18

Noten

1. Het ontdekken van dergelijke aanvallen vereist een hoog volwassenheidsniveau waarin monitoring en detectie en het controleren van logbestanden onderdeel zijn van de dagelijkse werkprocessen.
2. Vul uw e-mailadres in en kijk of uw gegevens voorkomen in dergelijke lijsten: https://haveibeenpwned.com/
3. DOS/DDOS, zie ook: https://www.politie.nl/themas/ddos.html
4. Melding aan de IBD uit juni 2019
5. Dit constateerden we al in het Dreigingsbeeld 2018, er zijn wel stappen gezet om de basis meer op orde te krijgen en monitoring en detectie in te regelen. De collectieve aanbesteding GGI-Veilig is in dit kader een belangrijke stap vooruit.
6. https://www.informatiebeveiligingsdienst.nl/product/kwetsbaarheden-in-citrix-lessen-voor-gemeenten-en-de-ibd/
7. https://nos.nl/artikel/2339905-ambtenaar-gemeente-den-haag-ontslagen-na-miljoenenfraude.html
8. https://www.nhnieuws.nl/nieuws/258588/foutje-ambtenaar-verstuurt-onbedoeld-phishingmail-naar-complete-adressenlijst
9. https://www.omroepzeeland.nl/nieuws/121172/Datalek-Schouwen-Duiveland-veroorzaakt-door-menselijke-fout
10. https://www.inteylingen.nl/nieuws/wethouder-van-de-post-leerlingen-vervoer-af.html
11. https://www.informatiebeveiligingsdienst.nl/product/leren-van-lochem-lessen-uit-een-informatieveiligingsincident/
12. https://vng.nl/artikelen/ondermijning-gebeurt-soms-onbewust
13. https://www.security.nl/posting/608213/Amerikaanse+stad+Baltimore+getroffen+door+ransomware
14. https://www.security.nl/posting/610517/Baltimore+valt+terug+op+Gmail+na+besmetting+door+ransomware
15. https://www.rtlnieuws.nl/tech/artikel/3938346/lekke-telsoftware-verkiezingen-geschrapt
16. https://www.haaretz.com/israel-news/elections/.premium-app-used-by-netanyahu-s-likud-leaks-israel-s-entire-voter-registry-1.8509696
17. https://www.rtlnieuws.nl/economie/life/artikel/5123626/een-derde-nederlandse-werkenden-afhankelijk-van-overheid-voor-loon

18. https://www.cbs.nl/nl-nl/nieuws/2019/18/428-duizend-jongeren-in-jeugdzorg
19. https://www.rtvutrecht.nl/nieuws/1907072/politici-spreken-schande-over-datalek-wethouder-wil-diepgravend-onderzoek.html
20. https://cjgrijnmond.nl/datalek-bij-cjg-rijnmond/
21. https://www.rtlnieuws.nl/tech/artikel/4789901/handel-rdw-kentekenregister-namen-woonadressen-nederlanders-lek
22. https://www.nu.nl/amsterdam/5963582/standaardprocedures-bij-ict-storingen-gemeente-faalden.html
23. https://www.security.nl/posting/659849/Verkeerslichtsysteem+door+ernstige+kwetsbaarheid+over+te+nemen
24. https://nvd.nist.gov/vuln/detail/CVE-2020-12493
25. https://www.rijnmond.nl/nieuws/195370/Maastunnel-weer-open-na-urenlange-storing
26. https://www.omroepwest.nl/nieuws/3456213/Storingen-Juliana brug-vermoedelijk-door-fout-in-besturingssysteem
27. https://www.safetycultureladder.com/nl/de-veiligheidsladder/ladder-treden/
28. Zie hiervoor de eerdere dreigingsbeelden van de IBD: https://www.informatiebeveiligingsdienst.nl/nieuws/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2018-gepubliceerd/ en https://www.informatiebeveiligingsdienst.nl/nieuws/dreigingsbeeld-informatiebeveiliging-2019-2020/
29. https://www.informatiebeveiligingsdienst.nl/product/handreiking-risicomanagement-door-lijnmanagers/
30. https://vng.nl/publicaties/agenda-digitale-veiligheid-2020-2024
31. https://www.informatiebeveiligingsdienst.nl/product/de-10-bestuurlijke-principes-voor-informatiebeveiliging/
32. https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020
33. https://www.informatiebeveiligingsdienst.nl/product/leren-van-lochem-lessen-uit-een-informatiebeveiligingsincident/
34. https://www.informatiebeveiligingsdienst.nl/nieuws/kwetsbaarheden-in-citrix-lessen-voor-gemeenten-en-de-ibd/
35. https://www.maastrichtuniversity.nl/nl/cybersymposium-um-lessons-learnt

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

INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie


Bergen op Zo
Fryske Marren
Haarlem
Hellendoorn
Huijgevoort
Leek
Marne
Nieuwegei
Oldebroek
Schiedam
Stein
Veenda
Zandvoort
Capelle aan den IJssel
Geldermals
Hulst
Leeuwarden
Nieuwe
Ommen
Reimerswaal
Schinnen
Strijen
Veere
Veld
Westerveld
Zeist

INFORMATIE BEVEILIGINGS DIENST

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