RSIV regionaal samenwerkingsverband integrale veiligheid

Regionaal Samenwerkingsverband Integrale Veiligheid (RSIV)

Eenheid Den Haag

Notitie Cyber

Samen werken aan Veiligheid en Vertrouwen

Vast te stellen op 30-11-2017 door het dagelijks bestuur van het Regionaal Bestuurlijk Overleg

René Hesseling, Kristiaan Schuppers, Jan-Cees Andrea, Dave Lucas (politie eenheid Den Haag),

Barbara Barendrecht (OM)

Marieke Strietman (RSIV)

Versie 17-11-2017

Inhoudsopgave

Deze notitie is een onderbouwing van het document 'handelingskader burgemeesters op het gebied van cyber'

Inleiding

Er is in het Regionaal Bestuurlijk Overleg (RBO) van 6 april 2017 besproken dat er meer inzicht nodig is over aard en omvang van cybercrime. Op basis daarvan kan beter beoordeeld worden of het (lokale) bestuur een verantwoordelijkheid in de aanpak heeft en zo ja, welke bijdrage zou kunnen worden geleverd.

Tegelijkertijd wordt er op lokaal, bovenlokaal en landelijk niveau gesproken met relevante partijen over dit onderwerp. Ook daarvan kan de uitkomst worden benut. Dat leidt tot de doelstelling om te komen tot (een advies voor) concrete maatregelen met een bredere kijk op het onderwerp.

Los van deze notitie is een handelingskader voor burgemeesters op het dossier cyber opgesteld. Zonder geweld te willen doen aan de complexiteit van het onderwerp denken we dat het nuttig is om met kleine stappen te beginnen. Uit onderzoek blijkt tenslotte dat kleine stappen tot een sneeuwbaleffect kunnen leiden.

In deze notitie wordt gestart met het in vogelvlucht benoemen van de aandacht voor cyber in de wereld en in Nederland. Zoals in het handelingskader al wordt aangegeven is het zaak om met het Rijk en andere (grote) partijen in verbinding te blijven zodat taken en verantwoordelijkheden op de verschillende (sub)onderwerpen duidelijk worden en de afstemming daartussen optimaal wordt.

Daarna worden de verschillende definities uitgewerkt en wordt een eerste globaal beeld rondom het thema cyber gegeven. Als laatste wordt benoemd dat gemeenten aan zet zijn om hun afhankelijkheid van digitale systemen in beeld te krijgen, de veiligheid in de digitale én fysieke wereld zoveel mogelijk te borgen en om burgers en bedrijven zo goed mogelijk te informeren over de risico's.

In bijlage 1 is een overzicht van alle in deze notitie voorkomende definities en afkortingen opgenomen. Bijlage 2 is een infographic over het onderzoek Haagse Hogeschool naar cyber in het MKB en bijlage 3 is een infographic waarin aangegeven staat hoe preventie in brede zin vorm kan krijgen.

Gemeente Den Haag blijkt moeilijk te hacken

Wie denkt dat hackers te werk gaan in donkere en afgelegen kamers, heeft het mis. Vandaag kwamen de grootste hackers van de wereld bij elkaar in het atrium van het stadhuis in Den Haag om het systeem van de gemeente te hacken. Ze deden dit tijdens een hackwedstrijd die Den Haag organiseerde. Na drie uur zwoegen konden ze drie relatief kleine fouten vinden. Geen enkel hacker kwam het systeem in.

'Hier staat een trotse wethouder', vertelt wethouder Baldewsingh, die verantwoordelijk is voor de ICT-omgeving van de gemeente. 'Ik ben tevreden dat we dit op een transparante manier konden doen en dat er geen grote lekken zijn gevonden. De fouten die nu naar boven zijn gekomen, zijn in de bovenste laag gevonden, vrij snel, niet te diep in systeem.'

De gemeente heeft samen met het Haagse cyber security bedrijf Cybersprint deze wedstrijd, de Bug Bounty-Challenge, georganiseerd. Het idee hiervoor kwam in eerste instantie van D66. Het samenwerken met de ethical hackers heeft als doel de zwakke punten en onveiligheden in het systeem van de gemeente te ontdekken en te verbeteren.

Kwetsbaar

Het is de eerste keer dat een gemeente zich op deze manier kwetsbaar opstelt voor hackers. 'Het was zeker een beetje spannend. We hadden geen idee wat er vandaag kon gebeuren,' zegt Marijn Fraanje van de ICT-afdeling in Den Haag. 'Maar de hackers zijn verplicht de kwetsbaarheden te melden, dus op dit punt helpt het ons alleen maar.' Pieter Jansen, de directeur van Cybersprint, hoopt dat deze actie een inspiratie kan zijn voor andere gemeentes om hun systeem te laten testen.

Aan het einde van de wedstrijd werden er prijzen uitgereikt aan de hacker die de meest invloedrijke fout vond, de hacker die op de meest verrassende manier te werk ging en aan de hacker die de meest ingewikkelde trucs uithaalde. Per categorie was de prijs 1666 euro, een winnaarsbokaal en natuurlijk de erkenning

Omroep West, 29-9-2017

Aandacht voor cyber op internationaal en nationaal niveau: in vogelvlucht

Al beperken we ons in deze notitie zo veel mogelijk tot de regio, het is duidelijk dat cyberaanvallen een wereldwijd probleem zijn. Hier ligt dan ook een belangrijke taak voor onze regeringsleiders om het probleem met grote spelers op dit vlak verder uit te werken en zo veel mogelijk te beperken.

De verwevenheid tussen bedrijfsleven en overheid is groot

Met deze laatste zin duidt de in cybercrime gespecialiseerde openbaar aanklager onbedoeld maar heel adequaat de verhoudingen binnen de onlinesecuritysector. De verwevenheid tussen overheid en bedrijfsleven is groot — waarbij de eerste sterk afhankelijk is van de kennis en kunde van het laatste.

Er is dan ook een vette kluif te verdelen. Wereldwijd gaat het om een jaaromzet van honderden miljarden euro's, waarbij de Nederlandse markt goed is voor enkele miljarden. Logisch dat de *Big Four*, de grote accountancy- en consultancybedrijven, ieder een eigen cybersecurityafdeling hebben opgericht. In Nederland nam PriceWaterhouseCoopers vorige jaar zelfs een heel onlinebeveiligingsbedrijf over: het Nieuwegeinse Everett.
Cyber is inherent grenzeloos en de werkelijke macht ligt – vooralsnog – bij de *Big Five* van grote internationale techbedrijven (Facebook, Google, Apple, Amazon en Microsoft) en bij wat met een steriele term 'statelijke actoren' heet: de geheime diensten en overheidshackers van landen als Rusland, de Verenigde Staten en China. Daar wordt volop geïnvesteerd in verdedigende én aanvallende cybersecurity

26-9-2017, ftm.nl

Vanuit de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) is het Nationaal Cyber Security Center (NCSC) opgericht. Het NCSC draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief. Zij constateren dat de digitale weerbaarheid in Nederland achterblijft bij de groei van dreigingen. Overheid, bedrijfsleven en burgers nemen veel stappen om de digitale weerbaarheid te vergroten, maar dit gaat niet snel genoeg. Dat blijkt uit het Cybersecuritybeeld Nederland 2017 (CSBN 2017) dat het kabinet Rutte II naar de Tweede Kamer heeft gestuurd.

Op Prinsjesdag werd benadrukt dat bestrijding van cybercrime hoog op de agenda dient te blijven en dat het een grensoverschrijdend karakter heeft. Er gaat structureel 26 miljoen extra naar cybersecurity voor versterking van de veiligheidsketen en bevordering van informatiedeling. De gemeente zal hiervan niet direct profiteren omdat cybersecurity niet begint of ophoudt bij de gemeentegrenzen of landsgrenzen, maar als er slagen worden gemaakt op dit vlak kan dit onze bewoners en ondernemers, die mogelijk slachtoffer kunnen worden van cybercrime, wel ten goede komen.

In het nieuwe regeerakkoord is het opstellen van een ambitieuze cybersecurity-agenda opgenomen met onder meer standaarden voor Internet-of-Things-apparaten, het stimuleren van bedrijven om veiliger software te maken via software-aansprakelijkheid, het versterken van het NCSC als aanspreekpunt van Computer Emergency Response Teams (CERT) van alle sectoren (waarbij de Rijksoverheid en organisaties binnen de kritieke infrastructuur 24-uurs hulp beschikbaar hebben), het stimuleren van cybersecurity-onderzoek en het verbeteren van voorlichtingscampagnes. Bovendien worden middelen vrijgemaakt voor het opzetten van een Digital Trust Center (DTC) om Midden- en Kleinbedrijven (MKB) in staat te stellen hun eigen cybersecurity te organiseren en hen te informeren en adviseren.

In de toekomst moeten organisaties in de vitale sectoren (zoals gas, water, elektriciteit, telecom, financiën, vliegvelden) verplicht melding maken van digitale veiligheidsincidenten. Door de wettelijke meldplicht van ICT-inbreuken kan het NCSC de risico's voor de samenleving inschatten. Het NCSC kan dan hulp verlenen aan de getroffen organisatie. Daarnaast kan het NCSC hierdoor andere organisaties in de vitale sectoren zo nodig waarschuwen en adviseren. Dit wetsvoorstel treedt naar verwachting in per 1 januari 2018.

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben. In bepaalde gevallen moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Vanuit Den Haag zijn er verbindingen met Global Forum on Cyber Expertise (GFCE), dat Nederland in 2015 als een wereldwijd forum voor cyberexpertise gelanceerd heeft. Naast Nederland bestaat dit forum uit 42 landen, intergouvernementele organisaties en bedrijven. Het secretariaat van het GFCE bevindt zich in Den Haag.
Het GFCE heeft de volgende doelen:

1) zorgen dat technische expertise breder beschikbaar komt;
2) fondswerving voor de versterking van cyber security;
3) helpen met de strijd tegen cybercrime;
4) verbetering van databescherming;
5) verbetering van wet- en regelgeving over internet.

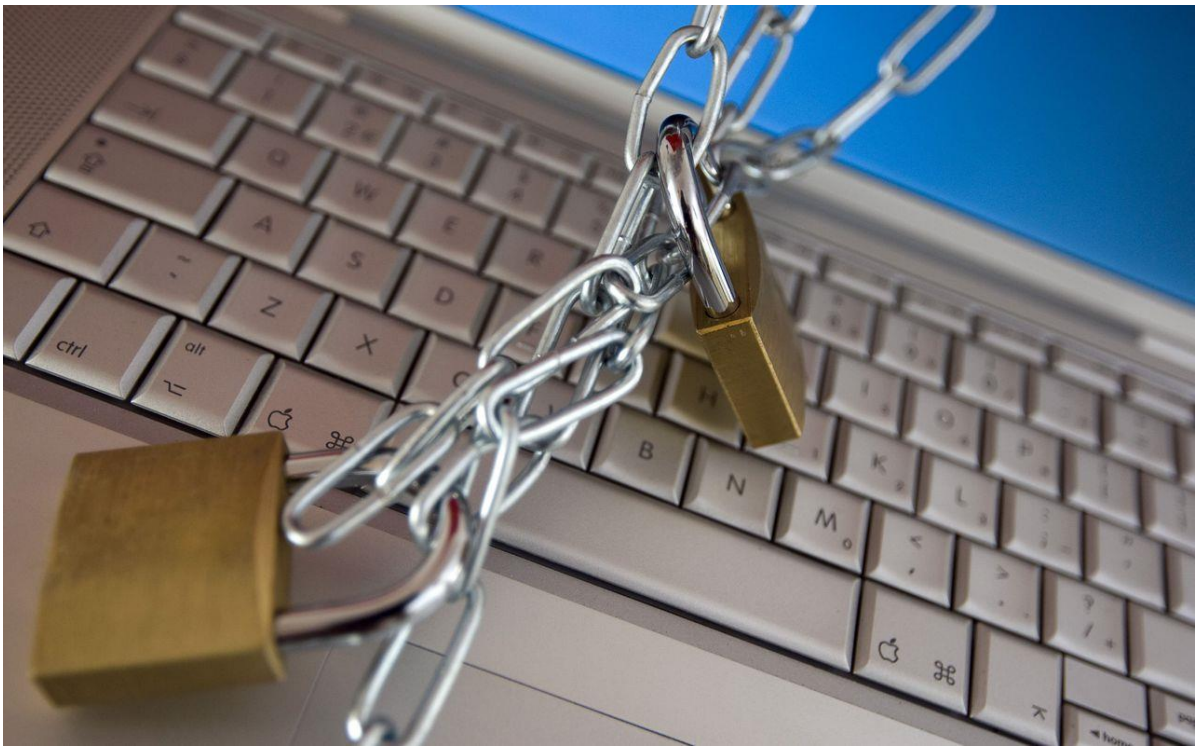
Verder is The Global Counsil of City CIO's (CGCC) in September 2016 opgericht. Het CGCC heeft onder meer als doel om gezamenlijk te werken aan een 'smart cities' model. De Chief Information Officer (CIO) van de gemeente Den Haag participeert hierin.

Tevens is Den Haag aangesloten bij het wereldwijde netwerk van 'Resilient Cities'. Dit netwerk richt zich op de weerbaarheid van steden ten opzichte van onder meer (de gevolgen van) cyberaanvallen.

Bedrijven, kennisinstellingen en overheden die zich hebben aangesloten bij The Hague Security Delta (HSD) werken samen aan kennisontwikkeling en innovaties op het gebied van veiligheid in heel Nederland. Op de campus zijn 50 van de ruim 250 partnerorganisaties van HSD gevestigd. Allen hebben een gezamenlijke ambitie: meer veiligheid en meer banen.

Datalekken bij gemeenten; 'het is een beetje een zooitje'

Bijna tweederde van de gemeenten meldde vorig jaar een datalek van persoonlijke gegevens van burgers.



Gestolen telefoons van ambtenaren of een zoekgeraakte map met gevoelige gegevens. Gemeenten zijn zich in heel verschillende mate bewust van datalekken in hun organisatie, zo blijkt zondagavond uit onderzoek van Reporter Radio (KRO-NCRV) onder 61 gemeenten. De meerderheid meldde vorig jaar een lek aan de Autoriteit Persoonsgegegevens.

Gemeenten blijken datalekken ook meestal niet aan de betrokkenen te melden: bij slechts 18 procent van de lekken gebeurde dat. Officieel moeten zij dat doen wanneer betrokkenen risico lopen op problemen. Identiteitsfraude is een van de doemscenario's rond datalekken.
NRC, 27-1-2017

Definities en globaal beeld

Definities

Cybercrime is een containerbegrip. In deze notitie richten we ons op cyber security, cybercrime en digitale criminaliteit. Zoals hierboven al vermeld worden alle begrippen in de bijlage toegelicht.

Cybersecurity

Cyber security is het geheel aan (technische) Informatie- en communicatietechnologie (ICT)-maatregelen met als doel om vrij te zijn van gevaar of schade veroorzaakt door misbruik, verstoring of uitval van ICT.

Cybercrime

We spreken van cybercrime als het gaat om criminaliteit waarbij ICT zowel het middel als het doelwit is. Omdat de strafbare handelingen hoofdzakelijk gericht zijn op ICT kan gesproken worden van te onderscheiden criminaliteitsverschijnselen. Dit komt ook tot uiting in de specifieke wetgeving op dit gebied zoals beschreven in de Wet Computercriminaliteit I uit 1993, de Wet Computercriminaliteit II uit 2006 en het momenteel bij de Eerste Kamer in behandeling zijnde wetsvoorstel Computercriminaliteit III.

Onder cybercrime hangen op dit moment de volgende wetsartikelen:

Art. 138ab Sr: Computervredebreuk;
Art. 138b Sr: Opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmeren door daaraan gegevens aan te bieden of toe te zenden.
Art. 139c Sr: Met technisch hulpmiddel gegevens afluisteren.
Art. 139d Sr: Plaatsen opname of aftapapparatuur.
Art. 139e Sr: Hebben en gebruiken van door wederrechtelijk afluisteren, aftappen c.q. opnemen verkregen gegevens.
Art. 161sexies Sr: Opzettelijke vernieling geautomatiseerd werk of werk voor telecommunicatie.
Art. 161septies Sr: Culpose vernieling van enig geautomatiseerd werk of werk voor telecommunicatie.
Art. 350a Sr: Aantasting/manipulatie computergegevens (het doleuze misdrijf).
Art. 350b Sr: Aantasting/manipulatie computergegevens (het culpose misdrijf).
Art. 317 Sr lid 2: Afpersing middels bedreiging gegevens middels een geautomatiseerd werk op te slaan, onbruikbaar of ontoegankelijk te maken.
350 c Beschadigen van geautomatiseerd werk
350d Ter beschikking stellen van wachtwoorden en het maken van illegale technische hulpmiddelen

In Nederland hebben we nu vooral te maken met de volgende manifestaties van cybercrime:

1. Afpersing in de vorm van **ransomware**: computers worden **gehackt** of slachtoffers worden misleid en geven onbewust toegang zodat er malware geplaatst kan worden om bestanden te versleutelen op een computer of datadrager waardoor deze onbruikbaar en niet meer toegankelijk is. Personen en bedrijven worden gedwongen om geld over te maken (bijvoorbeeld in bitcoins) zodat men weer toegang krijgt tot de computergegevens;

2. **Hacken en plaatsen van malware, phishing en social engineering** met als doel fraude te plegen met internetbankieren en/of creditcardgegevens en online handel;

3. Het stelen van digitale persoonsgegevens. De gestolen gegevens kunnen ook weer gebruikt worden voor identiteitsfraude. Ook hierin speelt cybercrime, bijvoorbeeld door het **hacken** van een server, een belangrijke rol. Het gaat om diefstal uit financiële of vanuit ideologische motieven. De mogelijkheden hiervoor nemen door de digitalisering van de samenleving steeds meer toe;

4. **ICT verstoren, vernielen of saboteren.** Diverse vormen van cybercrime, zoals een DDoS-aanval en defacement , worden ingezet. Hierbij wordt onder meer gebruik gemaakt van botnets;

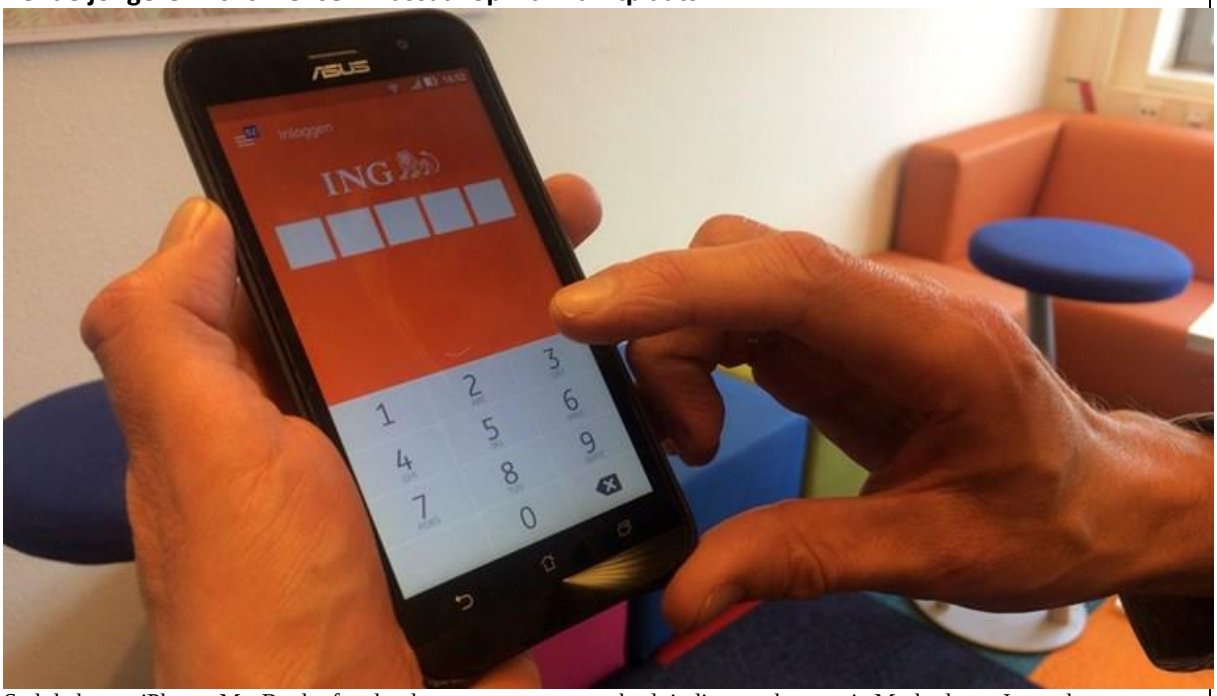
5. High Tech Crime (HTC) omvat vormen van cybercrime met een innovatief en ondermijnend karakter. Het gaat vooral om **digitale aanvallen** op de vitale infrastructuur (zoals olievoorziening, gas, elektriciteit), aanvallen op banken, bedrijfsspionage en hacktivisme (vanuit politieke en/of idealistische overtuigingen). De aanpak van hightech crime is vooral een taak van het Team High Tech Crime (THTC) van de Landelijke Eenheid van de Nationale Politie al spelen de eenheden hier ook en rol in.

Gedigitaliseerde criminaliteit

Er is sprake van gedigitaliseerde criminaliteit als ICT een middel is om traditionele vormen van (commune) criminaliteit te plegen. Dit kan in elke fase van het plegen van het misdrijf: bij de voorbereiding, de uitvoering en de afronding. Eigenlijk wordt tegenwoordig bijna bij alle traditionele misdrijven in meer of mindere mate gebruik gemaakt van ICT.

Het internet wordt dan gebruikt als **koop- en verkoopplaats** waar mensen opgelicht kunnen worden maar waar ook illegale goederen en/of diensten zoals drugs, kinderporno, gestolen goederen en wapens aangeboden worden. Verder fungeert het internet als een **plek om kennis en informatie uit te wisselen** over bijvoorbeeld het selecteren van doelwitten voor woninginbraken. Daarnaast kunnen vanwege de **digitale component van veel gebruiksvoorwerpen (Internet of Things)** apparaten op afstand worden gemanipuleerd. Ook worden bij allerlei misdrijven in de **persoonlijke levenssfeer** zoals bedreiging, stalking, smaad/belediging digitale middelen gebruikt.

Bende jongeren licht mensen massaal op via Marktplaats



Stel: hebt een iPhone, MacBook of ander duur apparaat over en besluit dit te verkopen via Marktplaats. Je maakt een afspraak met iemand die de spullen wel van je wil kopen en er komen twee jonge meiden opdagen. De meisjes maken zelfs de betaling ter plekke over via de app van een bekende bank. Terwijl je erbij staat. Je kunt zelfs meekijken op hun schermpje als ze jouw naam en bedrag naar je overmaken. Zou jij dan argwaan krijgen?
Omroep West, 19-9-2017

Globaal beeld van ICT-gebruik, risico's en aangiften

Zowel in het algemeen als in de eenheid Den Haag is het zicht op aard en omvang (op de verweven vormen) van cybercrime en gedigitaliseerde criminaliteit beperkt en onvolledig. Dit geldt zowel de uitingsvormen, de daders of dadergroepen, de facilitators, de slachtoffers, de werkwijze(n) en de omstandigheden waarin het misdrijf kan plaatsvinden. Dit heeft vermoedelijk de volgende redenen:

- Het aandeel gemelde gevallen en opgenomen aangiften van personen, bedrijven en publieke instellingen bij de politie is bijzonder laag omdat nut en noodzaak niet altijd duidelijk ervaren worden,
- Slachtoffers zijn zich er niet van altijd bewust dat zij te maken hebben gehad met cybercrime (als zijnde een strafbaar feit),
- Naast de politie zijn er vele andere meldpunten zoals de fraudehelpdesk of banken,
- Het vanuit de politiesystemen inventariseren van cijfers om zicht te krijgen op de problematiek is op dit moment niet mogelijk of uitsluitend op basis van zeer tijdrovend dossieronderzoek.

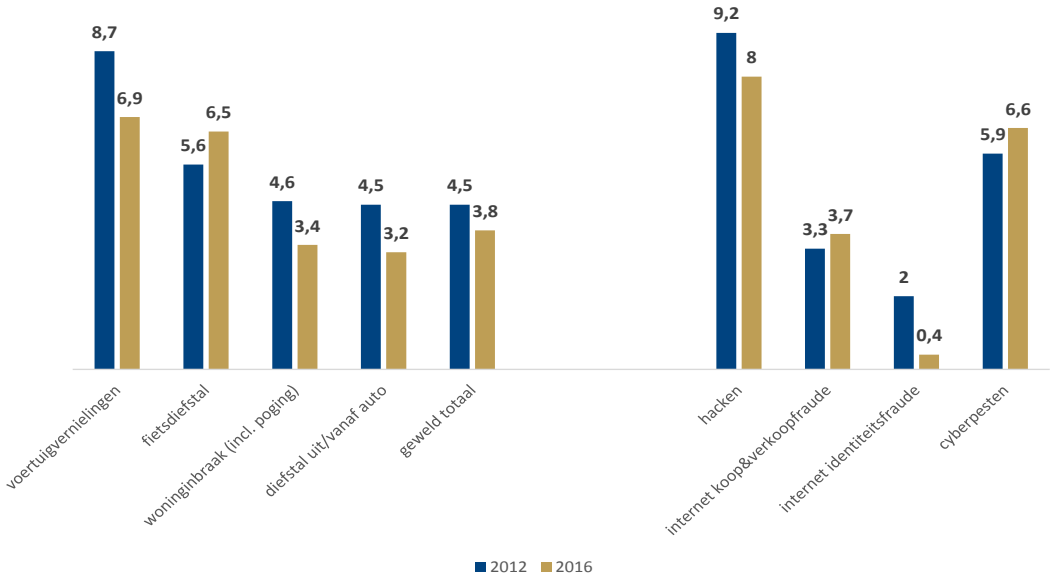
Momenteel wordt gewerkt aan een politieel veiligheidsbeeld van cybercrime en gedigitaliseerde criminaliteit voor de eenheid Den Haag (zie ook het handelingskader). Daarnaast gaat de 'werkgroep aangiftebereidheid' aan de slag met het thema aangifte en/of meldingen, waaronder de aangiften voor cybercriminaliteit.

Burgers

Volgens het Centraal Bureau voor de Statistiek (CBS) beschikte in 2016 89 procent van de Nederlandse huishoudens over een desktop of laptop en had 62 procent een tablet. Smartphones waren bij 80 procent van de huishoudens aanwezig en 92 procent had toegang tot het internet. 82 procent ging vrijwel dagelijks het internet op waar men bezig was met social media als WhatsApp, Facebook of Twitter, e-mailen, online chatten, online bankieren, online winkelen of het opslaan van foto's en databestanden in de cloud.

In 2016 is volgens de Veiligheidsmonitor 11,2 procent van de inwoners in de eenheid Den Haag slachtoffer geworden van een vorm van cybercrime of gedigitaliseerde criminaliteit (in deze veiligheidsmonitor is opgenomen: digitale identiteitsfraude, aan- en verkoopfraude, cyberpesten en hacken). Hacken is zelfs al een vorm van veel voorkomende criminaliteit geworden (zie figuur 1).

Figuur 1: Aantal ondervonden traditionele en cybercrime/gedigitaliseerde misdrijven per 100 inwoners in de Eenheid Den Haag (2012 en 2016). Bron: Veiligheidsmonitor 2016



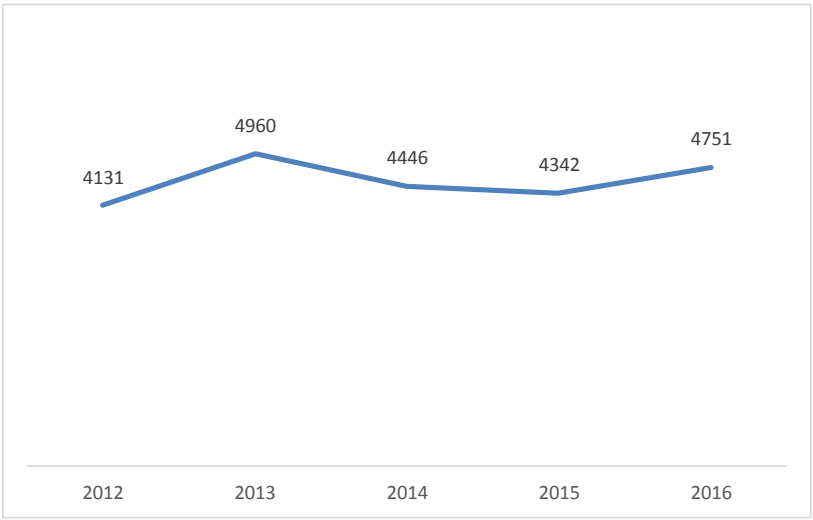
Volgens de CBS-Cybersecuritymonitor varieert het aantal personen dat slachtoffer is van cybercrime naar achtergrondkenmerken. Zo zijn mannen vaker slachtoffer dan vrouwen, vooral van hacken. Jongeren zijn vaker slachtoffer dan ouderen, behalve bij identiteitsfraude. Hiervan zijn 15-25-jarigen het minst vaak slachtoffer. Herkomst speelt nauwelijks een rol. Hoger opgeleiden zijn vaker slachtoffer van identiteitsfraude, koop- en verkoopfraude en hacken dan lager opgeleiden. Verder worden homoseksuelen vaker online gepest. Er zijn nagenoeg geen verschillen tussen steden en dorpen.

Bij hacken en vooral cyberpesten is vaker sprake van herhaald slachtofferschap dan bij koop- of verkoopfraude en identiteitsfraude. Het CBS geeft aan dat dit te maken heeft met op de persoon gerichte karakter van de eerste 2 delicten.
Binnen de categorie hacken is het inbreken op iemands e-mailaccount de meest voorkomende variant, gevolgd door het inbreken op iemands website/profielsite. Koopfraude komt veel vaker voor dan verkoopfraude. Binnen cyberpesten komt laster en stalken het meeste voor.

De meldings- en aangiftebereidheid varieert naar type misdrijf. In 2016 wordt in de Eenheid Den Haag in het algemeen 33 procent van de (traditionele) misdrijven bij de politie gemeld en het aandeel misdrijven waarvan daadwerkelijk aangifte is gedaan, bedraagt 22,9 procent in 2016. Voor identiteitsfraude, koop- en verkoopfraude, hacken en cyberpesten bedraagt het meldingspercentage in de eenheid Den Haag voor ditzelfde jaar echter 11% en het aangiftepercentage slechts 6,2%.

Op basis van cijfers van het Landelijk Meldpunt Internetoplichting (LMIO) neemt in 2016 in de Eenheid Den Haag het aantal aangiften voor internetoplichting toe (figuur 2). Bovendien zijn er aanwijzingen dat ook bij internetoplichting vaker gebruik wordt gemaakt van vormen van cybercrime, zoals het hacken van bepaalde sites.

Figuur 2: Aangiftes internetoplichting in de Eenheid Den Haag. Bron: Landelijk Meldpunt Internetoplichting (LMIO)



Bedrijven

ICT is ook essentieel geworden voor bedrijven. Praktisch alle bedrijven hebben toegang tot het internet, 68 procent van de werknemers gebruikt geregeld een computer met internet voor het werk en 89 procent van de bedrijven heeft een eigen website. Bijna twee op de drie bedrijven maken veelvuldig gebruik van social media en in toenemende mate worden facturen digitaal verwerkt. Bovendien levert de bedrijvigheid in de ICT-sector een belangrijke bijdrage aan de Nederlandse economie. Ten slotte heeft Nederland één van de grootste internetknooppunten ter wereld (De Amsterdam Internet Exchange) en diverse razendsnelle, breedbandige telecomnetwerken waardoor Nederland een van de meest ICT-intensieve economieën van Europa is.

Uit diverse landelijke onderzoeken blijkt een aanzienlijk deel van de bedrijven slachtoffer is geworden van een of meer vormen van cybercrime. Volgens het CBS geeft ruim 20 procent van de

bedrijven met minstens tien werkzame personen in 2016 te maken gehad met de gevolgen van cyberaanvallen. Vooral bedrijven in de financiële sector en de energiesector hadden hier last van.

Om zicht te krijgen op cybersecurity in het MKB heeft de Haagse Hogeschool recent een onderzoek gedaan. 42% van de ondernemers geeft aan te maken te hebben gehad met cybercrime. De top 3 is: malware, phishing, ransomware.

In de bijlage is een infographic opgenomen met de resultaten van het onderzoek.

Ook bij bedrijven is de meldings- en aangiftebereidheid klein. Uit eerder landelijk onderzoek onder het MKB weten we dat bijna 93 procent van de MKB-bedrijven die slachtoffer zijn geworden geen contact opneemt met de politie.

Overheid

Het gebruik van ICT is ook niet meer weg te denken bij de rijksoverheid, gemeenten en andere (semi)publieke instellingen. De Studiegroep Informatiesamenleving en Overheid benoemt dat de overheid momenteel in een tijdvak zit waarin digitale middelen niet alleen de taakuitvoering ondersteunen maar daar ook een integraal onderdeel van de bedrijfsvoering zijn geworden: zowel intern als in het contact met burgers en bedrijven. Zo is de score voor de digitale beschikbaarheid van producten en diensten van Nederlandse gemeenten toegenomen van 78% in 2016 naar 81% in 2017.

Voor heel Nederland blijkt op basis van een steekproef onder 66 gemeenten dat de helft van de datalekken niet door de gemeente wordt gemeld, terwijl bekend is dat een deel van de datalekken het gevolg kan zijn van een cybercrime aanval (NCTV, 2017).

Analyse politiegegevens, trends en ontwikkelingen

Delicten

Op basis van een eerste analyse van cybergerelateerde meldingen en aangiften van burgers bij de politie Eenheid Den Haag in de periode 1 januari 2017 t/m 20 oktober 2017 is naar voren gekomen dat bij het merendeel (van de gemelde/aangegeven incidenten) sprake is van fraude met een financieel oogmerk. In de overige gevallen gaat het om afpersing - veelal met behulp van ransomware - en om smaad/laster, stalking/bedreiging en vernieling/sabotage. Afpersing is hierbij vanuit een financieel motief, maar bij de andere categorieën zijn de motieven uiteenlopend van wraak (relationeel, zakelijke geschillen), baldadigheid (jongeren onderling) tot het benadelen van de concurrentie.

Op dit moment hebben we in Nederland vooral te maken met de volgende manifestaties van cybercrime:

- De meest voorkomende vorm van fraude is **Microsoft Scam**. Hierbij doen criminelen zich voor als medewerker van Microsoft. Ze bellen slachtoffers met de mededeling dat er problemen op hun computer zijn ontdekt met de software van Microsoft. Om dit op te lossen zijn wel de nodige aanpassingen noodzakelijk en er wordt gevraagd of de zogenaamde medewerker toegang kan krijgen tot de computer. Met overname van de computer kunnen criminelen toegang krijgen tot internetbankieren waarmee geldbedragen kunnen worden weggesluisd;

  Een andere vorm is **Chief Executive Officer (CEO)-fraude**, waarbij de crimineel doet voorkomen of de CEO een persoon van het betrokken bedrijf benadert om een betaling te doen.

  Andere veel voorkomende vormen van fraude zijn hacking van e-commerce accounts (ook via het hacken van e-mail accounts) om **goederen te bestellen en elders – al dan niet bij katvangers – te laten bezorgen**. Verder komt voor dat facebookaccounts zijn gehackt om te adverteren (meestal in relatie tot internetoplichting) of krijgen mensen (phishing) mail waarbij **op listige wijze wordt getracht iemand te bewegen tot betaling**. Dit speelt met name bij burgers, al zijn er ook een aantal meldingen van bedrijven waarbij criminelen zich voordoen als leverancier of leidinggevende om geld afhandig te maken;

- De **digitalisering van de samenleving zal de komende jaren alleen maar toenemen** door trends als het Internet of Things (dingen als apparaten, infrastructuur en vervoermiddelen worden via het internet verbonden), cloud computing, mobiele internettechnologie (5G netwerken) en de ontwikkeling dat mensen steeds vaker via het internet worden verbonden ('Internet of People'), bijvoorbeeld via implantaten als een pacemaker;

- De afgelopen jaren is geconstateerd dat vormen van **cybercrime en traditionele criminaliteit steeds sterker verweven** raken. In veel gevallen worden aanvallen gericht op ICT-middelen om andere delicten te kunnen plegen zoals diefstal, fraude en afpersing. Het onderscheid tussen cybercrime en gedigitaliseerde criminaliteit zal steeds minder worden en zal in brede zin de aandacht uit moeten gaan naar de digitalisering van de criminaliteit en de (nieuwe) veiligheidsproblemen die daar mee gepaard gaan;

- De digitalisering van de (traditionele) criminaliteit kan leiden tot een **toenemende ernst** van enkele delicten (zoals bedreiging), de **opkomst van nieuwe type daders, dadergroepen en slachtoffers**. Ook is de verwachting dat de **omvang** bij diverse misdrijven **kan toenemen** zoals merkenfraude, telecomfraude, synthetische drugs, mensenhandel en heling.

Ontwikkelingen bij politie

De politieorganisatie is in beweging op het gebied van cybercrime en gedigitaliseerde criminaliteit. Er is een strategie opgesteld met als uitgangspunt "waakzaam en dienstbaar, voor een veiliger Nederland, ook in het digitale domein". Voor de vertaling wordt ingezet op een zestal speerpunten: Het vergroten van de bewustwording, het versterken van kennis en kunde, verbeteren van de intake en screening, het organiseren van capaciteit, de verbetering van de informatiepositie en het gericht zoeken naar samenwerking.

Een belangrijke stap is het vergroten van de bewustwording ten aanzien van de dreiging van cybercrime, de impact van slachtofferschap en de verantwoordelijkheid die de politie hierin heeft. Een verantwoordelijkheid die steeds meer een gedeelde verantwoordelijkheid betreft waarin politie, bestuur, bedrijfsleven en de burger zowel op het gebied van informatie-uitwisseling als het nemen van maatregelen ieder hun eigen rol vervullen. Een wezenlijk onderdeel hiervan is burgerparticipatie.

Naast bewustwording wordt geïnvesteerd in kennis en kunde. Politiemedewerkers worden geïnformeerd en opgeleid om hun verantwoordelijkheid te nemen ten aanzien van cybercrime en gedigitaliseerde criminaliteit. In de eenheid is er een kennis- en expertisecentrum georganiseerd waar tactiek, intelligence en techniek (samen met het OM) binnengekomen aangiften screenen en een borging zijn/blijven als vraagbaak voor kennis en expertise binnen de organisatie. Niet alleen is de politie via verschillende kanalen 24/7 bereikbaar voor meldingen en/of aangiften, ook kan het slachtoffer direct van het juiste handelingsperspectief worden voorzien. Hierbij dient ook aandacht te zijn voor effectieve bijstand aan grotere bedrijven of instellingen. Daarnaast wordt de informatiepositie versterkt zodat het zicht op de aard en omvang en het beeld van dader- en slachtofferschap wordt vergroot.

De politie zoekt proactief in- en extern de samenwerking op om cybercrime vanuit meerdere invalshoeken aan te vliegen. De samenwerking vindt extern plaats om een meer volledig beeld te krijgen van aard en omvang binnen het MKB door bij bijeenkomsten te presenteren en het gesprek aan te gaan. Op het gebied van de handhaving en preventie is er de samenwerking met gemeenten. Op het gebied van preventie, onderzoeken en kennis is er de samenwerking met partners zoals providers, datacenters, onderzoeksbureaus en het NCSC. Een partner kan in de samenwerking digitale kennis & know-how delen, inzicht geven in complexe en specifieke technische infrastructuren en bijdragen aan het leveren van inzichten in fenomenen en trends.

Het NCSC en de Politie werken bijvoorbeeld samen als een op handen zijnde DDoS aanval op een vitale infrastructuur bekend is geworden op het internet: Het verzamelen van sporen (bewijs) kan direct in gang worden gezet en er kan gezamenlijk gewerkt worden aan het zoveel mogelijk voorkomen van de aanval.

Ontwikkelingen bij OM

Ook bij het Openbaar Ministerie (OM) heeft de aanpak en de bestrijding van cybercrime hoge prioriteit. Intern heeft het parket Den Haag op nationaal niveau een trekkersrol gekregen op het gebied van cybercrime. Het vermoeden is dat in de toekomst het merendeel van de strafzaken een digitale component bevat. Dit betekent dat bewustwording en goede kennis op dit gebied nog belangrijker zullen worden. Het Parket Den Haag investeert op dit moment veel in opleidingen en er is in samenwerking met de politie een aantal awareness bijeenkomsten over dit thema georganiseerd.

Daarnaast is zicht op de instroom van strafzaken van groot belang. Zoals hierboven al benoemd worden elke week de binnengekomen aangiften samen met de politie gescreend en verder uitgezet.

Een goede aanpak van cybercrime vereist innovatie. In het begin van de zomer is samen met de politie eenheid Den Haag gestart met een stakeholdersanalyse, waarbij er gesprekken gevoerd zijn met verschillende organisaties en bedrijven binnen en buiten de regio Den Haag zoals ziekenhuizen, transportbedrijven, scholen/universiteiten, consultancybedrijven en verschillende opsporingsinstanties. Het doel van de stakeholdersanalyse is het verkrijgen van inzicht in de problematiek en de beleving van cybercrime, de mogelijkheden in de aanpak en het verkennen van nieuwe samenwerkingen.

Topman OM: We zijn niet klaar voor cybercriminaliteit

Justitie in Nederland heeft onvoldoende kennis en mankracht om cybercriminaliteit tegen te gaan. Dat stelt topman Gerrit van der Burg van het Openbaar Ministerie zaterdag in het AD. Bovendien blijkt het in de praktijk ingewikkeld de daders te pakken.

'We trekken er hard aan, maar we zijn er nog niet klaar voor', zegt hij in het interview. 'We zijn van oorsprong geen digitale organisatie.' Van der Burg, sinds drie maanden voorzitter van het College van procureurs-generaal van het OM, beschrijft hoe ze probeerden tien officieren van justitie met een cybersecurityachtergrond te krijgen. Hij vond er vier.

Alleen al de ontsleuteling van één iPhone kost volgens hem 'enorm veel mankracht en expertise'. Recent liep ook het kraken van een gecodeerde telefoon, gebruikt door criminelen, volgens hem uit op een mega-onderzoek.

Bijscholen niet genoeg

Het kabinet wil volgens Haagse bronnen in de nieuwe begroting structureel 25 miljoen euro extra vrijmaken voor cyberveiligheid

'De wereld van de technologie verandert zó snel, dat het moeilijk is om bij te houden wat er allemaal gebeurt', aldus Van der Burg. 'Het onvoorstelbare wordt voorstelbaar, als het gaat om cybercrime.'

Het kabinet wil volgens Haagse bronnen in de nieuwe begroting structureel 25 miljoen euro extra vrijmaken voor cyberveiligheid. Deskundigen denken dat dit slechts een fractie is van wat nodig is. D66 pleitte eerder voor een 'Deltaplan cybersecurity'.

Het gebrek aan digitale kennis speelt in veel sectoren. De president van het gerechtshof Den Haag pleitte er onlangs voor elke rechtbank in Nederland uit te rusten met een aparte 'cyberkamer'. Nederland heeft bijvoorbeeld relatief veel te maken met kwaadaardige software (malware). Het alleen maar bijscholen van rechters op dit gebied is volgens hem niet genoeg.

Ook defensie en de inlichtingendiensten kampen met een achterstand. Brigade-generaal Wilfred Rietdijk waarschuwde in een interview met de Volkskrant dat zij de digitale dreiging momenteel niet aankunnen. Volgens hem moet Nederland snel een nieuwe organisatie optuigen om buitenlandse dreiging, zoals manipulatie en beïnvloeding via fake nieuws, in kaart te brengen

Volkskrant, 16-9-2017

Rollen en verantwoordelijkheden gemeenten

Lokaal zijn er risico's voor de gemeentelijke (interne) organisatie, voor ketens waarin met partners wordt samengewerkt en voor burgers en bedrijven. Gemeenten spelen een rol in cyber security door voorlichting en andere preventiemaatregelen in te zetten. Bij rampen, crises en ongevallen pakken zij naast preventieve inzet de nazorg op. We hebben gezien dat de NCSC en andere partijen hier ook een rol in hebben. Binnen de genoemde terreinen moet verder uitgewerkt worden wat ieders rollen en verantwoordelijkheden zijn en waar de aansluiting moet plaatsvinden.

We hebben verder geconstateerd dat het bedrijfsleven voorop loopt als het gaat om digitale kennis en kunde en dat er een sterke afhankelijkheid van private partijen is. Samenwerking binnen de overheid maar ook met externe private partijen is dan ook van cruciaal belang. Dit vraagt om een vernieuwende manier van opereren, waar politie en OM al een start mee gemaakt hebben. Hierin kunnen gemeenten, politie en OM dan ook samenwerken.

Daarnaast kan er door kennis en kunde binnen de eenheid te bundelen efficiënter gewerkt worden en gaat het kennisniveau omhoog. Door samen op te trekken komen ook knelpunten sneller aan het licht die vervolgens bij het Rijk aangekaart kunnen worden, al dan niet samen met andere regio's en/of gemeenten.

We kunnen op het gebied van cyber 2 rollen onderscheiden voor gemeenten.

Rol 1: Verantwoordelijk voor de openbare orde en veiligheid en regierol bij integrale aanpak

De veiligheidspartners gemeenten, politie en OM dragen elk vanuit hun eigen specifieke verantwoordelijkheid en positie bij aan de aanpak van criminaliteit. Vanuit zijn verantwoordelijkheid voor de opsporing en vervolging van strafbare feiten draagt het OM bij aan een veilige en rechtvaardige samenleving. De politie zorgt voor toezicht, hulp en handhaving. De gemeenten zijn verantwoordelijk voor preventie en nazorg en voeren de regie op het lokale veiligheidsbeleid. In de veiligheidsregio's wordt samengewerkt door diensten bij de uitvoering van taken op het terrein van brandweerzorg, rampen- en crisisbeheersing, geneeskundige hulpverlening, openbare orde en veiligheid.

Preventie en nazorg

ICT en internetgebruik houdt niet op bij de gemeentegrens. De overheid heeft dan ook een rol in bewustwording van de risico's. Toch kunnen we hier als gemeente niet bij wegblijven. Casussen die in de openbaarheid komen en voor maatschappelijke onrust zorgen hebben bestuurlijke actie nodig.

Het NCSC stelt in het Cybersecuritybeeld Nederland (CSBN 2017) vast dat het MKB vaak geen goed beeld heeft van benodigde maatregelen en daarom relatief weinig actie onderneemt op het gebied van cybersecurity. Uit de hierboven genoemde cijfers blijkt dat burgers en bedrijven –net als bij overvallen of woninginbraken- gewezen moeten worden op de risico's.

Er is een aantal relatief eenvoudige maatregelen die de risico's drastisch kunnen beperken. Voorlichting is makkelijk en veelvuldig beschikbaar via de verschillende websites. Toch komt het urgentiebesef pas nadat men slachtoffer is geworden. De verwachting is dat dit ook geldt voor burgers.

Net als dit voor de fysieke veiligheid geldt hebben bedrijven en burgers een eigen verantwoordelijkheid als het gaat om het treffen van preventieve maatregelen en zelfredzaamheid. Daar waar het de zelfredzaamheid overstijgt en de risico's bovengemiddeld hoog zijn kan de gemeente inzet plegen. Wanneer dit precies geldt is niet altijd gemakkelijk te duiden. Door hier binnen gemeenten en tussen gemeenten onderling over in gesprek te blijven wordt er in gezamenlijkheid richting aan gegeven.

Hierboven is al aangegeven dat er vanuit het Rijk een Digital Trust Center (DTC) opgericht wordt om Midden- en Kleinbedrijven (MKB) in staat te stellen hun eigen cybersecurity te organiseren en hen te informeren en adviseren. In de bijlage is een overzicht van de belangrijkste aanbieders van campagnes te vinden zoals alertonline.nl en veiliginternetten.nl (gefaciliteerd vanuit het NCTV).

Gemeenten kunnen in samenwerking met politie en OM actief aan de slag door awareness bijeenkomsten te organiseren en campagnes die vanuit de overheid gefaciliteerd worden uit te voeren voor MKB en burgers. Elders in het land is al verbinding gezocht met scholieren/studenten die het MKB helpen met het uitvoeren van scans. Dit zou ook binnen de eenheid Den Haag uitgewerkt kunnen worden.

Als het regionale beeld vanuit de politie gereed is kan gekeken worden naar specifieke informatie over daders, slachtoffer en soorten delicten. Hier kunnen gemeenten specifieke preventiemaatregelen op inzetten.

Een op de vijf bedrijven met minimaal tien medewerkers heeft vorig jaar last gehad van een hackaanval. De helft van die bedrijven heeft dat ook geld gekost. Hackaanvallen komen relatief vaak voor bij bedrijven in de financiële sector en bij energiebedrijven; de horeca is relatief immuun voor aanvallen, blijkt uit cijfers van het CBS.

Bedrijven hebben bijvoorbeeld last van ransomware (13%) of van verstoringen waardoor ze niet meer kunnen werken.

NOS, 25-9-2017

Crisisbeheersing

In gezamenlijkheid geven gemeenten, politie, brandweer en de GHOR de veiligheidsregio's vorm. Alle betrokken veiligheidspartners zijn aan zet om samen goed voorbereid te zijn op dagelijkse maar ook grootschalige incidenten om deze slagvaardig te bestrijden. Ook hier is het van belang dat elke kolom de eigen informatieveiligheid regelt en dat daarnaast de informatieveiligheid binnen de crisisstructuur zo veel mogelijk geborgd is.

Crisistypen zoals overstroming (waterschade), stroomuitval en uitval van internet- of telefoonverkeer zijn opgenomen in de reguliere plannen van de veiligheidsregio's. De hulpdiensten geven dan ook aan dat iedere kolom is voorbereid en maatregelen getroffen heeft om de continuïteit van de kritieke processen te borgen, waardoor gevolgen van een cyberaanval vooralsnog onder de reguliere planvorming binnen de regio vallen.

Op basis van cyber incidenten elders kan gekeken worden naar de leerpunten en kunnen er waar nodig aangepaste maatregelen genomen worden. Er kan in dit geval een vergelijking gemaakt worden met de aanpak van terroristische dreiging of een aanslag: Door kennis te dragen van leerpunten is kritisch gekeken naar de eigen processen. Zo is voor dit specifieke type de rolverdeling tussen de betrokken partijen uitgewerkt.

In het Magazine Nationale Veiligheid en crisisbeheersing 2017-nummer 4 van de NCTV wordt aandacht gevraagd voor het onderzoeken van nieuwe risico's, de kansen dat deze leiden tot een incident of crisis en de impact daarvan. Voor het beheersen van de crisis is vervolgens snelle tweerichtingscommunicatie tussen bedrijven, overheid en burgers, inzichten in cascade effecten en de inzet van de crisisorganisatie van groot belang.

Het NCSC fungeert zoals hierboven beschreven als aanspreekpunt voor organisaties binnen de kritieke infrastructuur met de Computer Emergency Response Teams (CERT).

Uitgezocht moet worden wie, welke verantwoordelijkheden heeft en hoe dit zo goed mogelijk op elkaar afgestemd kan worden.

Rol 2: Hoeder gemeentelijke digitale veiligheid ('eigen huis op orde')

De wijze waarop een organisatie omgaat met cybercrime is altijd de verantwoordelijkheid van de organisatie zelf. Dit geldt ook voor het 'eigen huis', de betreffende gemeente.

Een groot deel van de dienstverlening van gemeenten verloopt inmiddels digitaal en daarnaast hebben veel fysieke objecten een digitale component (The Internet of Things). Binnen de eigen gemeente moet de interne digitale veiligheid dan ook op orde zijn. Burgers moeten er vanuit kunnen gaan dat informatie over inschrijvingen in de basisregistratie, uitkeringen of andere gevoelige informatie niet op straat ligt. Daarnaast moet de gemeente de continuïteit van de diensten die ze leveren kunnen borgen in geval van een al dan niet intentionele cyberaanval. Als laatste moet de gemeente het goede voorbeeld geven aan burgers en bedrijven. Binnen gemeenten is bewustwording op dit onderwerp bij alle betrokken collega's een belangrijk aandachtspunt.

Een eerste begin om informatiebeveiliging binnen organisaties te organiseren is het eenduidig beleggen van de verantwoordelijkheid door het aanstellen van een Chief/Corporate Information Security Officer (CISO). De Informatie Beveiligings Dienst (IBD) noemt als doel van deze functie om op basis van het basisnormenkader Baseline Informatiebeveiliging Gemeenten (BIG) zorg te dragen voor een samenhangend pakket aan maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een gemeente te waarborgen.

Net als bij andere integrale vraagstukken zijn er op het dossier cyber binnen gemeenten de verschillende aspecten vaak ambtelijk en bestuurlijk op verschillende plaatsen belegd. In Den Haag geldt dat bijvoorbeeld voor subonderwerpen als de informatisering, interne dienstverlening, kenniseconomie en MKB.

Inwoners van een gemeente hebben er direct last van als banken, energiebedrijven of internetvoorzieningen niet meer functioneren. Het is noodzakelijk om samen te werken met deze

externe partners en te zien hoe er in gezamenlijkheid opgetreden kan worden in geval van een calamiteit. In een aantal gemeenten wordt hier vanuit de interne veiligheid al aandacht aan besteed.

Dit punt heeft een overlap met het onderwerp crisisbeheersing. Door intern (binnen gemeenten) afgestemd en gecoördineerd aan de slag te zijn is duidelijk wie, welke verantwoordelijkheden heeft voor zowel de interne veiligheid als die van belangrijke partners binnen gemeenten.

Interne informatieveiligheid

Iedere gemeente stelt haar informatiebeveiligingsbeleid vast aan de hand van het BIG. Dit rust op 4 pijlers, waarbij binnen de wettelijke kaders steeds een beslissing over enerzijds kansen (gebruiksgemak) en anderzijds het beperken van risico's gemaakt moet worden:

1) Beschikbaarheid: in hoeverre geeft aan in hoeverre een ICT-dienst, systeem of component toegankelijk is voor de geautoriseerde gebruikers.
2) Integriteit: hoe betrouwbaar is de informatie? Kernwoorden zijn: juist, volledig, tijdig, geautoriseerd
3) Vertrouwelijkheid: gemachtigden voor toegang
4) Privacy: regels rondom registratie, gebruik en opslag van persoonsgegevens. Dit onderdeel is geregeld in de Algemene Verordening Gegevensbescherming (AVG).

De visitatiecommissie Informatieveiligheid (vanuit de VNG) heeft eind september 2017 een evaluatie beschikbaar gemaakt. Enkele conclusies zijn dat er meer bestuurlijke aandacht moet komen voor informatieveiligheid, met een hechtere verbinding tussen bestuurder en de CISO.

Daarnaast signaleert de commissie dat de blijvende technologische dreiging vraagt om samenwerking tussen gemeenten onderling en mogelijk andere regionale partijen om deze daadwerkelijk blijvend het hoofd te kunnen bieden. Dit sluit aan bij ons handelingskader.

Goede voorbeeld

Als overheidsinstantie hebben we de verantwoordelijkheid om te laten zien hoe het moet.
Communicatie omtrent de inspanningen vanuit de gemeente speelt hierin een belangrijke rol.

Rol burgemeester

De burgemeester wordt in deze rol geraakt vanuit zijn of haar verantwoordelijkheden op het vlak van openbare orde en veiligheid (onder meer door de informatie-uitwisseling over bijvoorbeeld veelplegers, daders van huiselijk geweld of overlastgevende/criminele jongeren) maar ook als voorzitter van het college van Burgemeester en Wethouders. De CISO heeft zoals gezegd een spilfunctie maar een besef van de risico's moet breed gedragen worden binnen de organisatie. Dit is nodig om crises in een later stadium te voorkomen en/of de gevolgschade voor de gemeente zelf maar ook voor de inwoners zo veel mogelijk te beperken.