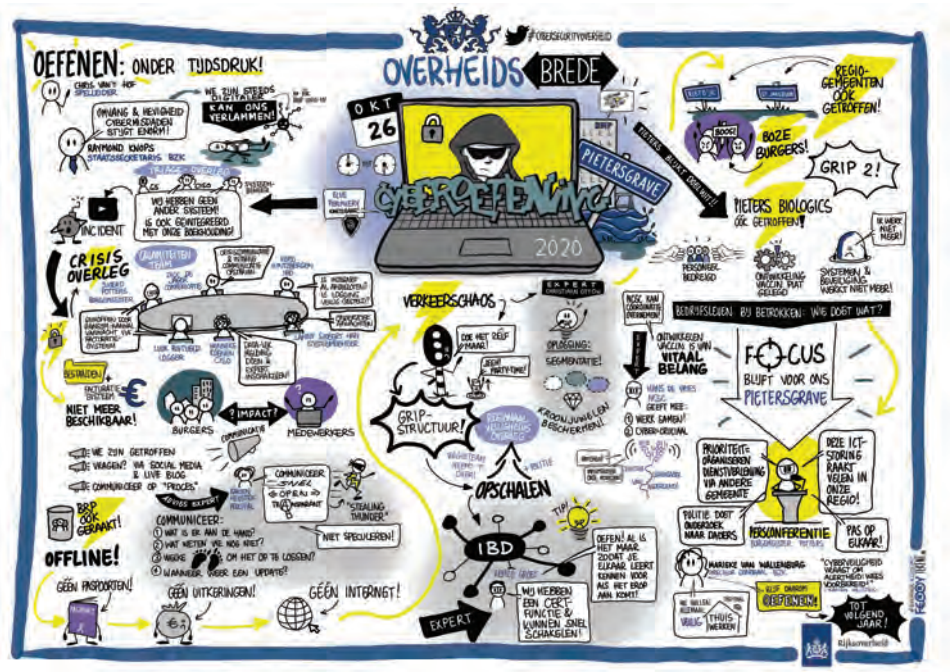
Auteurs: Maurice Derogee en Chris de Vries (informatie)

VNG: overheidsbrede cyberoefening

Oktober was de European Cyber Security Month en kon je ook in Nederland in die maand diverse overheidsbrede cyberwebinars volgen. Het volledig online programma omvatte 12 onderdelen verspreid over 7 dagen. Het beloofde een interessant programma te zijn, waarop Maurice Derogee en Chris de Vries besloten om er gezamenlijk verslag van te doen.



Afbeelding 1 - Visual Overheidsbrede Cyberoefening.

Na de succesvolle inschrijvingen moest uw redacteur Chris de Vries jammer genoeg vernemen dat hij niet tot de doelgroep behoorde, waarom dan ook besloten werd dat Maurice de bijeenkomsten virtueel zou bijwonen en zij beiden samen deze zouden voorbereiden. Doel na te gaan welke innovaties dan wel nieuwe ontwikkelingen te bespeuren waren, welke antwoorden op de kritische risicofactoren te constateren zijn en hoe de overheid zich voorbereidt op diepgaande cyberaanvallen. Per onderwerp onze bevindingen.

01.10.2020

1. Jullie kunnen allemaal de DDoS krijgen!

Sinds het ontstaan van het internet bestaat DDoS. Opvallende recente nieuwsfeiten waren de aanvallen op Ziggo, Amazon en Dell die tot schade hebben geleden. De motieven voor DDoS-aanvallen werden niet uitputtend benoemd, maar ze gaven wel voorbeelden, zoals: de script-kiddie. Die door middel van een tool op internet en instructie de website van een school platlegt en de Anonymous-organisatie, die – bij wijze van activisme – hun volgers opriep een creditcardmaatschappij plat te leggen in het kader van Wikileaks.

Daarna werd de opbouw van een aanval toegelicht en de tools die hiervoor publiekelijk beschikbaar zijn. Er werd redelijk in detail ingegaan op de netwerktechnieken die worden misbruikt voor een DDoS-aanval, waarom en op welke wijze uiteindelijk een website offline gaat. Zo is de DNS-werking toegelicht om domeinnamen van websites te vertalen naar IP-adressen en wordt de werking van het TCP/IP protocol alsook het UDP uitgelegd in het kader van een DDoS-aanval. Het OSI-model kwam ter sprake om aan te geven op welke laag de aanvallen zich richten.

Na dit alles rest dan de vraag wat er aan te doen is. Het redelijk voor de hand liggend antwoord luidde dat het 'zoals altijd een risico afweging betreft die per dienst moet worden bekeken'. Zo kun je gebruik maken voor websites van een content delivery network (CDN) zoals bijvoorbeeld Akamai. Dan richt de aanval zich op het CDN en dat beschikt over voldoende adressen om de aanval af te weren. Dit is een afrader voor authenticatieservices.

Geadviseerd wordt om in het geval van overheidscommunicatie een scheiding te brengen tussen datgene wat via een besloten netwerk dient te gaan, en dat wat via het open internet kan lopen. Nu gaat bij vele instanties alles onnodig veel over het internet. Verrassend was dat enkel het Diginetwerk wordt aangehaald, maar niet het GemNet of het GGI. Sommige gemeentelijke dienstverlening kan namelijk alleen maar via het besloten netwerk met specifiek gestelde eisen aan de communicatie. Ook kan er gebruik worden gemaakt van een Scrubbing-provider; de aanbieder die al het verkeer via hun systemen leidt en toetst of het legitiem is.

Op de vraag wat dit aan vertraging en foutmarges oplevert, werd niet ingegaan. Echter het hoofddoel 'de digitale dienstverlening continueren', wordt hiermee wel bereikt, De Nederlandse ISP's hebben een samenwerking gerealiseerd in de vorm van de Nationale Wasstraat (NAWAS) en daarmee ook een Scrubbing-dienst. Een Anti-DDoS appliance (hardware) in het eigen netwerk plaatsen kan ook, maar is voor weinigen haalbaar vanwege het beheer en de benodigde technische kennis.
Ter bestrijding van deze problemen is er een anti-DDoS coalitie opgericht (1). De onderwerpen die daar worden getackeld: realisatie van een clearinghouse (een database van bekende aanvallen en herkenningspunten), cross-sectorale samenwerking (politie, bankwezen, Logius, overheid), zichtbaarheid (publiek), basisafspraken en het oefenen van incidenten (aanvallen). Als stelregel hanteert men het benutten van een goede analyse als vertrekpunt. Feitelijk komt dat neer op het volgen van de BIO (Baseline Overheid) en dus een inventarisatie van welke dienstverlening, hoe aan te bieden en met welke beschikbaarheid!
Voor iemand met een basisniveau aan netwerkkennis was dit webinar een goede uitleg, wat DDoS en de bijbehorende problematiek betreft. Echter de oplossing ervan zal zelfstandig moeten worden uitgevonden. In het woud van alle aanbieders – met de claim het 'ei 'van Columbus gevonden te hebben – is dit een DDoS op zichzelf. Te veel vragen blijven onbeantwoord. Managers en bestuurders onder de deelnemers zouden vermoedelijk al snel hebben afgehaakt.

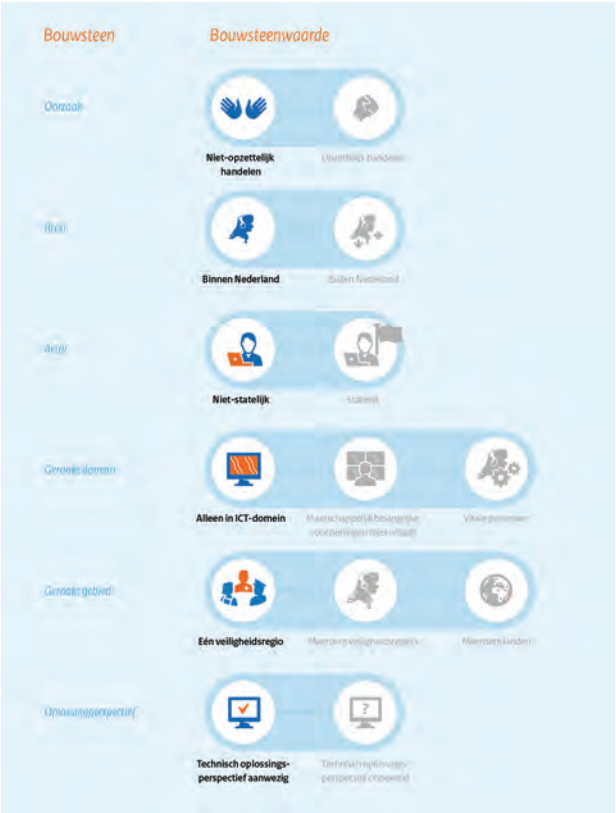
08.10.2020

2. Crisiscommunicatie in een keten - lessons learned

Hier kwamen met name drie thema's aan de orde: de Citrix-kwetsbaarheid en hoe Amsterdam daarmee omging, de invloed van corona op het werk van het UWV en de casus Lochem. Samenvattende conclusie:

- Zorg dat je je crisismanagement op orde hebt;
- Ken je eigen organisatie goed;
- Zorg voor de betrokkenheid van het management en
- Zorg ervoor dat de juiste personen in je team zijn opgenomen.

Amsterdam: een belangrijk moment tijdens de Citrix-crisis was de heropstart van de risico-afweging. Op basis van eigen analyses en advies met second opinions van professionele ondersteuners (Motiv & Foxit), een goed/kritisch overleg met het management, durfde men het aan om op de maandagochtend weer live te gaan.
Communicatie was het centrale punt. Dat varieerde van afstemming met de beveiligingsdienst, de CISO en de GGD tot periodieke updates (NCSC) en niet te vergeten de bestuurlijke communicatie via de wethouder naar de gemeenteraad dan wel de contactmomenten met VNG en het Ministerie van Buitenlandse Zaken. De leerpunten: allereerst, wij moeten veel meer oefenen! Daarnaast: tijdens een crisis kan heel veel en elkaar vinden via apps zoals signal en whatsapp is belangrijk. Bereikbaarheid en beschikken over bellijsten is essentieel. Het kennen van de rollen binnen de crisisorganisatie eveneens en dat omvat ook het beschikken over actueel inzicht over het ICT-landschap en de vitale systemen.
UWV: het belang van het UWV kent iedereen. Het gaat om miljarden aan uitkeringen en miljoenen aan vertrouwelijke registraties van Nederlanders in diverse systemen. Logischerwijs heeft het UWV zich in te passen binnen de wettelijke kaders en dat maakt dat doorlooptijden snel een jaar aan tijd vragen. Ook bij het UWV vinden wij dezelfde kernwaarden terug als we bij het voorbeeld Amsterdam benoemden. Betrokkenheid, communicatie, heldere prioriteiten/doelstellingen en korte lijnen zijn de belangrijkste.



Afbeelding 2 - NCP bouwstenen (Zie sessie 3).

Afbeelding 3 - De cyberwegenkaart (Zie sessie 5).

08.10.2020

3. Nationaal Crisisplan Digitaal (NCP Digitaal)

Het nationaal crisisplan vindt o.a. zijn neerslag in het cybersecuritybeeld Nederland (CSBN 2020) (2). De conclusies daaruit zijn dat onze weerbaarheid groter moet worden, omdat de digitale risico's groot blijven en er samenhang is met andere risico's. Ons maatschappelijk leven wordt bedreigd met ontwrichting, daar is nog te weinig aandacht voor; men richt zich meer op de preventie. Praktijkvoorbeelden zijn de KPN-storing (112-alarmnummer), de ransomware aanval op Maastricht (jaarovergang 2019/2020), de Citrix-affaire en de ransomware aanval op de gemeente Lochem. Doel van het NCP Digitaal is de samenwerking tussen alle organisaties te verbeteren vanuit de nationale crisisaanpak zodat schade beperkt blijft en herstel snel wordt bereikt. De nadruk ligt dus op de keten en de bouwstenen van het plan (3). De bouwstenen zijn: oorzaak, bron, actor, geraakt domein, geraakt gebied en oplossingsperspectief (technisch), zie afbeelding 2. Het gepresenteerde is eigenlijk veel van hetzelfde waarbij de niet-Rijksorganisaties eraan moeten denken de benoemde Rijkszaken aan te passen aan de eigen onderdelen, bijvoorbeeld op gemeenteniveau.

13.10.2020

4. Cyberveiligheid in de waterketen - de fundamenten van de samenleving

Een interessant webinar, omdat daaruit blijkt dat de meeste Operational Technology assets (OT-assets) niet online staan. Hieruit is wel te concluderen dat sommige OT-assets wel online staan. Als vitale elementen in de waterketen worden onder meer gezien het drinkwater en de grote waterkeringen. De lokale waterschappen worden als niet-vitaal ingedeeld. Dit kan mettertijd natuurlijk wel veranderen op basis van de herijking Vitaal. De toetsingskaders kunnen leiden tot een hogere score en dus tot het alsnog vitaal ingedeeld worden. Binnen de sector lopen twee hoofdprojecten, te weten: SOC: opschalen van CERT naar SOC voor Rijkswaterstaat en de waterschappen. Drinkwaterbedrijven volgen een eigen commerciële SOC en een gemeenschappelijk risico-analyse methodiek waardoor ze onder de BIO komen te vallen en niet langer onder de Baseline Informatiebeveiliging Waterschappen (BIWA). Dat laatste betekent een onduidelijkheid over de te volgen richting; aangezien de gezamenlijke risico-analyse methode niet langer meer wordt vastgesteld op basis van een vaste methode dan wel vanuit vaste kwalificaties.

13.10.2020

5. De lokale cyberwegenkaart, drie rollen voor gemeenten

Gemeenten moeten worden geholpen bij het bestrijden van cyber gerelateerde zaken waarbij stakeholders binnen en rondom een gemeente het slachtoffer kunnen worden. Daartoe moeten gemeenten worden geassisteerd om: het eigen huis op orde te krijgen, actie te ondernemen met betrekking tot cybercrisis en -incidenten en bestrijding van cybercrime en gedigitaliseerde criminaliteit. Interessante

constatering is dat men de bestuurlijke verantwoordelijkheid legt bij diegene (de wethouder) die ICT in zijn portefeuille heeft en dat alles binnen het kader van de BIO (Baseline Informatiebeveliging Overheid). Opvallend is verder dat de CISO of de Security Officer een onafhankelijke, toezichthoudende alsook adviserende rol wordt toebedeeld rondom informatieveiligheid. En als derde laag wordt ambtelijk de verantwoordelijkheid neergelegd bij de proceseigenaren. Een gewetensvraag is of gemeenten niet verplicht zouden moeten worden om een toereikend budget voor informatieveiligheid en privacy vast te stellen, zodat de getoonde filmpjes niet alleen een voorbeeld zijn van bestuurders (Bilthoven, De Bilt en Heemstede) die hun verantwoording goed oppakken (het snappen), maar naar anderen toe een aansporing is om het ook zo goed op te pakken. Verrassend genoeg – voor ons – pleiten deze burgemeesters voor aandacht vanuit het rijk ten aanzien budgetten voor de cyberveiligheid met het oog op de existerende achterstanden. Ook voor het opnemen van cybercrime in de uitvoeringsplannen voortkomende uit het Integraal Veiligheidsplan. Dat laatste is bijzonder te noemen want de verantwoordelijkheid ligt al sinds 2013 bij de gemeenten om de zaken op orde te krijgen. En nu – anno 2020 – geven ze aan dat ze daarvoor budget verwachten. Gemeenten werken veelal in samenwerking met het CCV (Centrum voor Criminaliteitspreventie en Veiligheid) en de politie uitmondende in diverse initiatieven. Zichtbaarheid en het snel kunnen behalen van resultaten zal daar niet vreemd aan zijn. Een voorbeeld hiervan is de Citydeal, een samenwerking tussen het ministerie van Buitenlandse Zaken, de ondernemers, hogescholen, politie, CCV en gemeenten onder andere gericht op uitwisseling van kennis ten behoeve van lesprogramma's. Daarbij (wordt dat overwogen?) gaan ze de samenwerking aan met Google en Microsoft in een Publiek Private Samenwerking (PPS); hetgeen een interessant dilemma kan oproepen! Zeker wanneer vele gemeenten hun eigen huis nog niet op orde hebben. Deze cyberwegenkaart is afkomstig van het CCV, ontwikkeld in opdracht van het Ministerie van Justitie en Veiligheid (4).

15.10.2020

6. De geleerde lessen uit Maastricht

De universiteit Maastricht heeft grote transparantie betracht met betrekking tot de ransomware aanval op haar systemen. Zij heeft het rapport van Fox-It openbaar becommentarieerd (5), (6), (7), en haar belangrijkste lessen waren:

1. Verbetering van het bewustzijn en de wijze van afhandeling van 'phishing-mails'.
2. De noodzaak van technische maatregelen m.b.t.:
   a. 'updaten';
   b. verbeterde segmentering van het Windows-domein;
   c. 24/7 monitoring door SIEM en/of SOC en
   d. Het in kaart brengen van de Configuration Management Data Base (d.w.z. het in kaart brengen van (niet meer) actieve computer- en serversystemen binnen het domein en
3. Dubbele back-ups (waaronder offline). Kritische vragen richting de presentator waren onder andere:
   a. waarom geen multi-factor authenticatie naast de invoering van wachtwoorden met 15 karakters? Antwoord: wordt als goede suggestie gezien;
   b. met wie in samenwerking het contact met de Russische hackers verliep? Zowel via de professionele begeleider alsook de politie;
   c. soms is de betaling van ransomware (hier 30 bitcoins een kleine € 200.000,00) goedkoper dan het herstel. Speelde dat ook voor de Universiteit Maastricht? Ja, het werkzaam krijgen van alle universitaire processen (waaronder de examens van januari 2020) woog hier zwaar;
   d. Is er geïntensiveerde samenwerking ontstaan tussen de universiteiten als gevolg van deze aanval? Ja, was er al in het orgaan SURF, maar nu versterkt!

15.10.2020

7. Cyber als onderdeel van hybride dreigingen

Dit was een erg interessant webinar. Dat vanuit de dreigingsoptiek en niet de oplossingen. Kern van de presentatie was dat:

- cyberdreiging moeilijk detecteerbaar is;
- er sprake is van statelijke actoren;
- er is geen sprake van een nieuwe dreiging.

De doelstellingen zijn:

- polarisatie middels fake news;
- het zaaien van verwarring en
- beïnvloeding.

De ingezette middelen omvatten: social media en trolls. (Troll factories: opbouwen van niet bestaande persoonsprofielen voorzien van alle aspecten zoals levensloop, afbeeldingen e.d. van echte mensen. Daardoor kan polarisatie worden nagestreefd, want het lijken meningen van echte personen en niet van nep-profielen.)

- er sprake is van een lange termijn visie derhalve niet als incident behandelbaar is;
- daarom vraagt om een eveneens hybride aanpak en tot slot
- dat het samenwerking vereist tussen veiligheidsregio's, overheid, defensie en Europa.

De Nederlandse overheid kan naast DEF CERT (Defensie), de Marechaussee, de AIVD en misschien ook cyber als wapen inzetten en wel via een offensief cyber onderdeel. Betekent dit dan ook dat de Nederlandse overheid ook desinformatie kan en mag inzetten? Voer voor psychologen?

Het hybride zijn van deze dreigingen is gebaseerd op de mix van civiele - en militaire middelen. Het staat onder het niveau van een militair conflict. De acroniem DIMEFIL zegt alles: Diplomatie, Informatie, Militair, Economie, Financieel, Inlichtingen, Legal. De offensieve dreiging vanuit met name Rusland en China is evident.

Als beoogde doelen onderkent men vanuit Rusland het verzwakken van onze democratische stelsels, de Europese Unie en de NAVO. Vanuit China het erkend worden als de economische supermacht (onze vraag, wanneer wordt dat ook de politieke wereldmacht?) en een wereldorde naar Chinees karakter.

Zelfs COVID-19 wordt gedefinieerd als de snelkookpan voor desinformatie. Openlijk en heimelijk hanteren de spelers ondermijnende narratieven en presenteert men valse gezondheidsinformatie. Een voorbeeld daarvan is het bericht dat de VS een COVID-vaccin uittest op Oekraïense dienstplichtigen. Om de weerstand tegen deze dreigingen te verhogen is het samenwerken in netwerken een vereiste. De verkokering is nog te hoog en DIMEFIL moet met elkaar in verband worden gebracht. Om die reden wordt ook de Wet Veiligheidsrisico (Wvr) geëvalueerd, waarbij beoogd wordt Defensie een meer structurele rol toe te bedelen. De counterhybride oefening heeft laten zien dat tegenstanders zich richten op de breukvlakken in de samenwerking en dat daar Nederland kwetsbaar is. Daarom richt men zich op het ontwikkelen/versterken van de unity-of-command (sorry voor al die Amerikaanse termen). Wat wij ons moeten realiseren is dat de conclusie is dat de hybride-dreiging het nieuwe normaal zal zijn. Daar waar Nederland gebaat is bij een open economie met bijbehorende spelregels (fatsoensnormen), zullen handelsoorlogen zoals die tussen de VS en China daar meer drempels kunnen opwerpen.

20.10.2020

8. Hoe kunnen gemeenten helpen om de cyberweerbaarheid van bedrijven te verhogen?

In het eerste filmpje gaat het over een ondernemer, die na het weekeinde een versleutelde serveromgeving vindt op zijn zaak, maar gelukkig een goede back-up had en alles kon herstellen.

Kern van dit webinar het Digital Trust Center (DTC). Dat is een nieuwe afdeling vanuit het rijk dat zich bezighoudt met het leveren van allerhande informatiemateriaal om gemeenten te helpen burgers en ondernemers te ondersteunen om cyberweerbaar (en bewust) te worden. Een vraag die natuurlijk opplopt bij de gemeente-ambtenaar: "Zijn zij aangesloten bij de VNG?" Antwoord: "Nee, daar wordt nog aan gewerkt."

Het DTC zoekt naar samenwerkingsverbanden met de diverse sectoren en instellingen gericht op bewustwording bij alle betrokkenen. Daartoe heeft zij in afstemming met gemeenten een cybersecurity toolkit (8) ontworpen. Dat om in te spelen op de behoeften aan: kennis, ervaring, capaciteit, budget en zo de gemeente te ontzorgen. De rode draad daar zijn de ambities van de gemeente en de politiek acterenden respectievelijk hun commitment.

Volgende vraag: Is dit een gemeente taak? Formeel niet, want het staat nergens in de wet of in de regelgeving opgenomen, maar de gemeente Breda vindt van wel. En dus geven zij een presentatie hoe je dat dan opzet. Knap, want ze beseffen eigenlijk alleen doorgeefluik te zijn van de informatie vanuit het DTC en toch slagen zij erin allerlei leuke acties met de burgers en zeker met de jongeren te realiseren binnen de gemeente.

Het plan van aanpak is gericht op participatie door de vier doelgroepen te weten: de bewoners (buurtpreventie), de ondernemers (netwerkopbouw, informatievoorziening), de jongeren (via social media en een cybercrime challenge) en de digitaal vitale partners (lokaal ecosysteem, gebaseerd op vertrouwen). Interessant en uit te diepen opmerking is dat men de publieke ruimte niet alleen meer fysiek beoordeelt, maar ook digitaal! Dit roept ons inziens een hele reeks van juridische, sociale en privacy vraagstukken op. Een gewetensvraag is, dat als gemeenten zelf aangeven onvoldoende cyberkennis te hebben, hoe kunnen ze dan de burger, laat staan de ondernemer helpen? Het eerlijke antwoord: doen we ook niet want wij verwijzen door naar het DTC en dat zekert in ieder geval weer het bestaansrecht van deze organisatie. Desalniettemin positief te waarderen, al zouden de gemeenten zichzelf beter moeten verankeren qua cyberkennis. Het één op één doorgeven van de waarheden maakt dat bij vragen veel moet worden terugverwezen en dat versterkt niet de professionele uitstraling van noch het vertrouwen in de gemeenten. Het DTC is gericht op het niet-vitale gedeelte van de samenleving, want voor de vitale sector bestaat het NCSC. De vraag zweeft in de lucht of de IBD (die eenzelfde taak als het DTC bezit, maar dan gericht op gemeenten) niet de logischere partij zou zijn om ook de niet-vitale sector mee te nemen, en dat natuurlijk uit het oogpunt van effectiviteit en efficiëntie (lees schaalgrootte).

Afbeelding 4 - Agenda Digitale Veiligheid 2020 2024, de weg er naar toe. (Zie sessie 11, pagina 43).

20.10.2020

9. Cyberweerbaarheid tijdens verdubbeling van digitale dienstverlening

Een verrassend verhaal over het UWV. Bij die organisatie verwacht je niet dat zij letterlijk het BYOD in de praktijk brengen door met busjes rond te rijden en medewerkers te voorzien van laptops, beeldschermen, telefoons en wat dies nog meer zij in een periode van corona-thuis-werken. Wat wij op ons moesten laten inwerken is dat het UWV anticyclisch werkt, maar bij nader inzien volkomen logisch. Een economisch slechte tijd leidt ertoe dat het UWV meer mensen aanneemt en vice versa. Inmiddels werken zij met meer dan 18.000 personen thuis (4.000 voor corona) en hanteren zij een gedegen bewustwordingsprogramma. Zo gebruiken ze gelukkig ook geen Zoom tijdens het contact tussen medewerkers en klanten. Het UWV streeft er naar MS-Teams als hoofdmiddel voor videocontact te gaan inzetten en dat in plaats van Skype respectievelijk Zoom.

Het UWV besteedt veel van haar ICT-werkzaamheden uit en kan daarom tevreden constateren dat qua beveiliging en ontwikkeling het een en ander wel op rolletjes loopt. Zij ziet zichzelf als een risicogedreven IB&P organisatie met weerbare security. De kern van deze presentatie is:

- flexibiliteit (ook voor beveiliging) is vereist gezien de snelle veranderingen;
- bewustwording wordt heel belangrijk geacht;
- daardoor zijn ze er ook bewust van dat 100% veiligheid een fictie is;
- ze passen veelvuldig risico-analyses toe;
- streven naar security by design;
- letten op hun logging / monitoring en
- bouwen op de SOC-diensten.

Ze sloten af met de opmerking dat geïnteresseerden bij hen makkelijk aan de slag kunnen indien zij goede beveiligers zijn, de behoefte bij hen is groot.

22.10.2020

10. Red Teaming als cyberweerbaarheidsoefening. Hoe werkt dat?

Het is logisch dat bewustwording en het gedrag van mensen (met name het niet naleven van de afspraken, zoals te constateren valt tijdens de huidige epidemie) ook in dit verhaal van de provincie Fryslân aan de orde komt. Waar het in deze presentatie om gaat - naast het feit dat pentesten vooral technisch en niet op de mens organisatie georiënteerd is - dat als een middelgrote gemeente zo'n €20.000,00 tot €25.000,00 investeert, je een PEN-test 'plus plus' hebt. Daarmee is gezegd dat alle kwetsbaarheden binnen de organisatie blootgelegd worden, de belevingswereld van bestuurders en medewerkers wordt aangesproken, en je precies ziet waar het fout gaat.

Hier vraagt de goed geïnformeerde CISO zich af of dat dan al niet duidelijk had moeten worden via de BIG en nu de BIO. Ervaringen bij middelgrote gemeenten leert dat voor €5.000,00 een degelijke PEN-test, maar één keer in de twee jaar lukt.

De provincie Fryslân ziet het voordeel van de BIO vooral wat de eigen betrouwbaarheid en integriteit betreft. Het aangehaalde Citrix voorbeeld laat echter zien dat de BIO dat risico niet kan afdichten. Wij zouden dat willen aanvullen met onder andere de voordelen van: patching, monitoring, hardening, ISMS en incident response.

Dan blijft over dat RED-teaming dus een uitgebreidere toets (combinatie van technische tests, de procedures en het bewustzijn van mensen, dus de organisatie als holistisch geheel) betreft of je als organisatie werkelijk ook echt doet wat je zegt op papier. Dat is zeker waar, maar rechtvaardigt dat de kostprijs om het management daarvan te overtuigen?! Ook is kort ingegaan op purple teaming (samenwerking tussen red & blue teams ter verbetering van de cyberweerbaarheid). Het geheel van deze webinar overziende zal de professional onder ons veel bekend

nieuws hebben ervaren. Het is dan ook een cyclisch proces van plannen maken, uitvoeren, controleren, en bijsturen.

22.10.2020

11. Agenda digitale veiligheid: oefenen!

Onze essentie: meer samenwerken en dat dan ook oefenen! De VNG breekt hier een lans voor haar eigen oefenpakketten en ook voor de eerder besproken dienstverlening van het DTC. Echter, het VNG-pakket is toch meer op gemeenten gericht en ligt meer voor de hand vanuit de gemeenten beschouwd. Feitelijk hadden gemeenten vanaf 2013 de basis op orde moeten hebben. Nu, anno 2020 tot en met 2024 moeten die gemeenten ondernemers en burgers helpen met het cyberweerbaar worden. Daarbij is een vereiste dat de gemeenten meer gaan samenwerken met het rijk, het Openbaar Ministerie (OM), de politie en niet te vergeten met elkaar. Samen oefenen is daarbij essentieel.

De agenda digitale veiligheid 2020-2024 omvat in hoofd- en actielijnen het volgende:

Afbeelding 5 - Agenda digitale veiligheid 2020-2024.

Dat je burgemeesters ook moet betrekken bij de opzet van dergelijke oefeningen mag voor zich spreken, maar is geen automatisme. Dit onderwerp is niet populair binnen de gemeentelijke wereld, dus een mooie ambitie om waar te maken. Gelukkig hebben veel gemeentelijke (C)ISO's heel veel geduld en blijven die stimuleren. Maar vergeet daarbij niet het op orde brengen van de basis is een hartenkreet van vele (C)ISO's.

Het VNG oefenpakket bestaat uit drie modules: continuïteitsfocus, opzet van de driehoek gemeente – OM – politie en de maatschappelijke impact focus. VNG wijst daarbij op haar kant en klare oefenpakketten.

26.10.2020

12. Virtuele overheidsbrede cyberoefening

Jammer genoeg ontbrak een link om deel te kunnen nemen aan deze afsluitende webinar/oefening. De aftermovie hebben we wel bekeken, en dit duidt op een mooi cyberincident scenario, waarin alle onderwerpen behandeld in deze webinarreeks samenkomen, en het belang van alle in dit artikel geschetste onderwerpen worden benadrukt.

Slotopmerkingen

Het is goed dat de Europese Unie en in navolging daarvan de Nederlandse overheden actief zijn op het terrein van de cyberweerbaarheid en de bewustwording daarvan onder het brede publiek wil verspreiden. VNG heeft zeker met deze actie voorzien in de behoefte van een groot deel van haar doelgroep, zij het dat de zeer professionele CISO/ISO/SO bij tijd en wijle afgehaakt zal hebben, maar dat is 'all in the game'. Er waren zeker interessant webinars met inzichten en nieuwtjes die de moeite waard waren. Jammer dat het VNG zich wel bewust is van het feit dat de overheid in een keten werkt, maar blijkbaar haar doelgroepen toch sterk beperkt lijkt te hebben tot diezelfde overheid. Het meer laten deelnemen van niet-overheidsorganisaties zou de discussie verrijken en in ieder geval drempels geslecht hebben. Een overweging voor een volgende oefening. Verder vragen wij ons af, welk vervolg er gegeven wordt aan alle, door de tijd beperkte, onbeantwoorde vragen.
Er is ook een online magazine uitgegeven met interviews en blogs van de verschillende bestuurders, voor meer details (9).

Referenties

(1) https://www.nomore DDoS.org
(2) https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2020/06/29/cybersecuritybeeld-nederland-2020
(3) https://www.nctv.nl/documenten/publicaties/2020/02/21/nctv-nationaal-crisisplan-digitaal-_-webversie
(4) https://www.hetccv.nl/cyber/
(5) https://www.maastrichtuniversity.nl/file/foxitrapportreactieuniversiteitmaastrichtpdf
(6) https://www.maastrichtuniversity.nl/file/49750/download?token=cT_19j-W
(7) www.navaio.com/breakdown-rapport-universiteit-maastricht/ het 'breakdown' rapport
(8) https://www.digitaltrustcenter.nl/toolkit-voor-gemeenten
(9) https://cyber-magazine.nl/