INFORMATIEBEVEILIGING MAGAZINE

- Hoe vatbaar is uw digitale communicatie voor phishing?
- Succesfactoren voor het delen van cybersecurity informatie
- Column – Hoe de class-action naar Nederland kwam

JAARGANG 20 - 2020 - EDITIE 6

Let goed op jezelf en elkaar

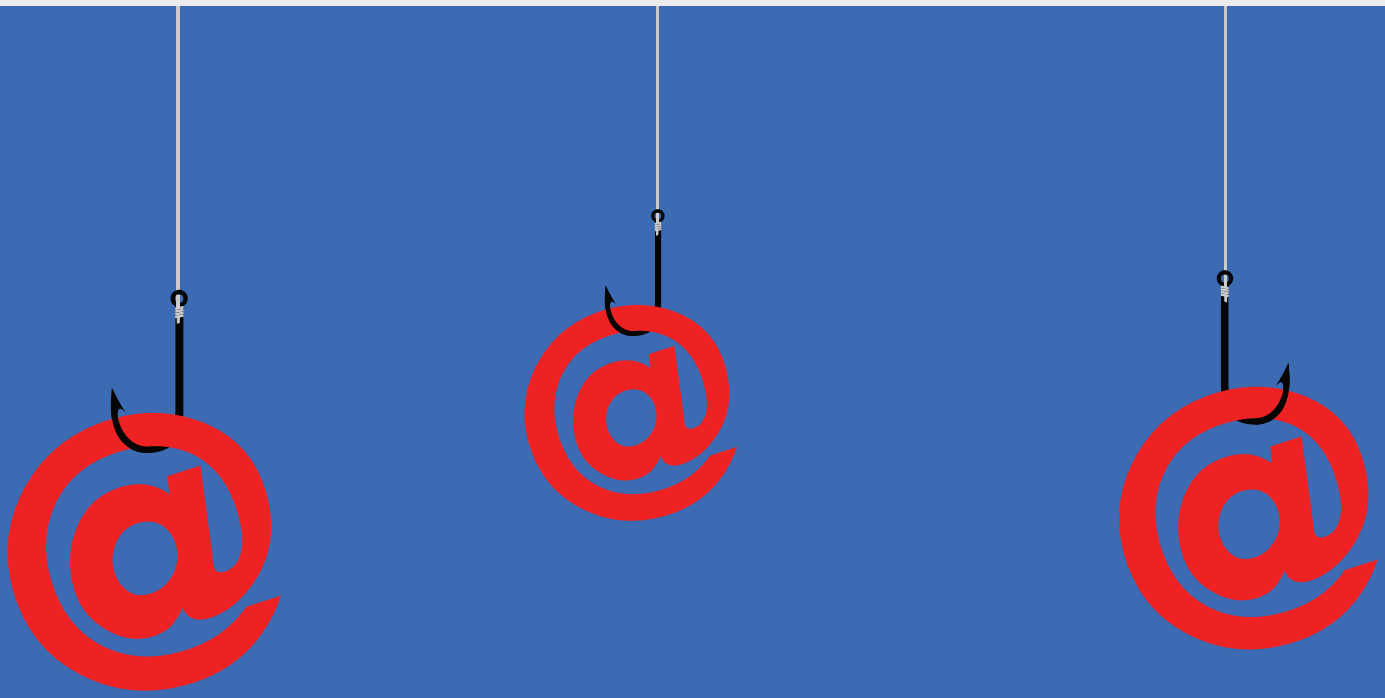
Nicole van Deursen

De redactie is bedroefd door het overlijden van Lex Dunn, die van 2007 tot 2019 deel uitmaakte van ons team en vele collega's heeft geïnspireerd.
Veel mensen willen het jaar 2020 graag snel achter zich laten. Verlies, onmacht, onbegrip, frustratie en eenzaamheid zijn emoties die de meesten van ons meer dan ooit hebben ervaren. Werkgerelateerd hebben informatiebeveiligers deze gevoelens heel vaak (probeer maar eens gedragsverandering in je organisatie te bereiken ...), maar nu doordrongen ze alle aspecten van ons leven. Namens de gehele redactie wens ik iedereen die het nodig heeft kracht en sterkte toe. Gedragsverandering staat op dit moment nog steeds centraal in overheidsbeleid en media-uitingen. In ons vakgebied kennen we de moeilijkheden rondom veilig gedrag maar al te goed. Onze vaste columnisten Inge en Robert schrijven hierover en er is een korte samenvatting van de nieuwe ethische gedragscode. Maar ook het artikel van de onderzoekers van de Haagse Hogeschool is hieraan gerelateerd: zij onderzochten welke factoren bijdragen aan succesvol samenwerkingsgedrag. Samenwerkingen tussen organisaties en daarbij informatie over dreigingen en risico's delen is lastig. TNO doet ook onderzoek naar dit fenomeen en legt uit waarom dat zo'n complex vraagstuk is. Verder hebben we deze keer een artikel over DDoS aanvallen op OSI-laag 7 en een artikel over security monitoring van sensoren op PERA-level 0.
Op het moment dat jullie dit laatste iB-magazine van 2020 ontvangen is de langste nacht van het jaar net geweest en worden de dagen alweer langer. Het extra daglicht geeft ons weer energie om voorzichtig vooruit te kijken. In 2021 zijn de Tweede Kamerverkiezingen en Ard Ruiter introduceert de nieuwe Kamercommissie voor Digitale Zaken die wordt opgericht. De toekomst maken we dus nu, we blijven leren, vernieuwen, samenwerken en het beste voorbeeld geven. Op je gezondheid letten staat overigens ook benoemd als onderdeel van ethisch gedrag in de bovengenoemde gedragscode, dus let goed op jezelf en op elkaar.

Nicole

IN DIT NUMMER

Auteurs: Drs. ing. William Breuer is als cybercrime adviseur werkzaam bij zowel het Cyber Defense Center als de afdeling Cyber Resilience van de Volksbank. Dit artikel is mede tot stand gekomen met hulp van Kim Gunnink (de Volksbank), Jules Stevens (bol.com) en Gunther Cleijn (PostNL), allen op persoonlijke titel. William Breuer is te bereiken via william.breuer@devolksbank.nl.



Hoe vatbaar is uw digitale communicatie voor phishing?

Helaas niet meer weg te denken uit het digitale leven: phishing. Criminelen hengelen naar informatie via e-mails, sms'jes, whatsapp-berichten of zelfs brieven om slachtoffers geld afhandig maken. Om dit voor elkaar te krijgen, doen de criminelen zich voor als betrouwbare partij. Elke organisatie met een significant bereik, zoals banken, pakketbezorgers, retailers en overheidsdiensten, zijn vaak misbruikte 'afzenders'. Maar ook úw bedrijf en handelsnaam kunnen worden misbruikt. Gelukkig kunt u de kans daarop verkleinen met een paar maatregelen.

Phishing is niet alleen schadelijk voor particulieren, maar ook voor de bedrijven wiens handelsnaam wordt misbruikt in de phishingberichten. Het doet uw reputatie geen goed als klanten uit uw naam worden misleid. Aan beide zijden kan veel leed voorkomen worden met het treffen van een paar eenvoudige digitale hygiënemaatregelen. De basis daarvan ligt in een duidelijk communicatiebeleid, zodat de klant uw berichten kan onderscheiden van die van criminelen. Dit geldt voor e-mail, maar net zo goed voor sms-berichten, tweets en andere berichten die u aan uw klanten stuurt. Een logische consequentie is dat uw domeinnaam én uw social media-accounts uw digitale visitekaartjes zijn. Met een goed doordacht én nageleefd domeinbeleid zorgt u dat van het visitekaartje een preventief effect uitgaat vanwege de eenduidigheid, herkenbaarheid en controleerbaarheid voor de klant.

Hoe maak ik mijn e-mailberichten herkenbaar voor klanten?

De meest bekende vorm van phishing is die per e-mail. Op dit gebied valt dan ook veel te winnen. Een eerste stap is in een communicatiebeleid vastleggen dat e-mails altijd vanuit de domeinnaam van uw bedrijf worden verzonden (bijvoorbeeld: verzender@example.nl voor het bedrijf 'Example').

Als u daarnaast opneemt dat in uw e-mail geen hyperlinks staan óf alleen hyperlinks naar webpagina's die eenvoudig herleidbaar zijn aan de domeinnaam van het bedrijf (`linkdomein', bijvoorbeeld: https://example.nl/actie) zit het eigenlijk direct goed met de herkenbaarheid. Het is voor klanten in één oogopslag duidelijk dat ze een e-mail kunnen vertrouwen die aan deze randvoorwaarden voldoet. Ook maken deze twee simpele regels het voor de klant eenvoudig om bij twijfel te achterhalen of het bericht legitiem is: een check op vertrouwde combinatie van afzender én hyperlink zijn de belangrijkste. Het helpt daarbij om deze regels gemakkelijk vindbaar te maken voor de klant, bijvoorbeeld door ze op te nemen in de footertekst van de e-mail en ze te delen via een `zo communiceren wij veilig'-pagina op uw website.

Voorkom hyperlinks naar een externe partij

Eenvoudig als dit mag lijken, gaat het in de praktijk wel eens mis. Soms stoten e-mails zelfs veiligheidsbewuste klanten af omdat de e-mails niet van phishing te onderscheiden zijn. Twee voorkomende voorbeelden zijn het uitsturen van bulkmail en het verzenden van enquêtes. Voor dit soort berichten worden vaak externe partijen ingehuurd. Als bulk e-mail wordt verzonden via een verzendpartij valt het op dat het afzendadres en het linkdomein meestal niet met elkaar overeenstemmen. Zo wordt example.nl ineens example.verzendpartijxyz.nl, en dat laatste zou voor de klant verdacht moeten zijn. Bij het uitsturen van enquêtes aan klanten door een externe partij gebeurt het ook dat er hyperlinks worden gebruikt die verwijzen naar de externe domeinnaam van de enquêteur. Het probleem daarvan is tweeledig: de groep klanten die vasthoudt aan de herkenningspunten uit uw communicatiebeleid zal terecht niet meedoen aan de enquête, en de groep klanten die wél meedoet, is onvoldoende alert en went zich mogelijk aan e-mailberichten te vertrouwen die door een ander uit uw naam worden verzonden. Beide gevolgen zijn onwenselijk. Niet consequent aan de vuistregels vasthouden lijkt hier dus een oorzaak te zijn.

Tip: maak duidelijke afspraken met e-mailverzenders

Vaak is het goed mogelijk om dit soort e-mailmissers te voorkomen. Maak bijvoorbeeld duidelijke afspraken met de enquêteur over het hanteren van uw communicatiebeleid. Zo kan deze een enquête verzenden op een e-mailadres van uw eigen bedrijf, of in ieder geval op een subdomein van uw domeinnaam zoals `enquetes.example.nl'. De hyperlink verwijst naar een informatiepagina op uw eigen bedrijfswebsite. Vanaf die pagina kan de klant doorklikken (of direct worden doorgezet) naar de enquêtepagina van de externe partij. Op deze manier behouden alle bonafide berichten uit uw naam altijd dezelfde uitstraling. Ook bij bulkmail bieden heldere afspraken met de verzendpartij uitkomst. De factsheet `Goede bulkmail lijkt niet op phishing' (1) van het NCSC is een goed begin van uw communicatiebeleid. Met deze afspraken is het ook voor uw klantenservice, webcare en fraude- en compliance-afdeling eveneens eenvoudig te controleren of een e-mail echt is of niet, zelfs als u niet elke e-mail `terugzoekbaar' heeft.

Communiceer uitsluitend via de eigen app

Een andere mogelijkheid is om bepaalde kanalen zoals e-mail uit te sluiten en bijvoorbeeld uitsluitend te communiceren via een eigen app. U kunt dan aan de klant via een notificatie e-mail zonder links laten weten dat er een bericht klaar staat in de app, zoals bijvoorbeeld MijnOverheid dit doet.

Houd het makkelijk en veilig voor de klant: zorg dat uw e-mail goed aankomt
Veruit de meeste phishingmails belanden dankzij een goed spamfilter in de ongewenste mailbox (of spambox). Maar ook een veilige e-mail van uw bedrijf kan bij verkeerd verzenden in een spambox komen. Daarom staat op websites nog weleens als tip: 'heeft u binnen een uur nog geen bericht van ons ontvangen? Kijk dan eens in uw spambox'. Goed bedoeld, maar niet verstandig. U traint zo klanten om een overduidelijke rode vlag – het feit dat de mail als verdacht is aangemerkt – te negeren. De kans bestaat dat een klant vervolgens ook een phishingmail opent die uit uw naam is verzonden en geheel terecht in de spambox terecht kwam.
Vraag uw klanten ook niet om uw e-mailadres in de 'veilige ontvangerslijst' te zetten of, nog erger, om de anti-spamfunctionaliteit uit te schakelen. Weet dat alle e-mails dan, zonder spamcontrole, in de inbox van de klant komen. Ook als uw e-mailadres wordt misbruikt. Komen uw legitieme berichten in een spambox? Onderzoek dan liever waarom dit zo is en pak het probleem aan bij de oorzaak.

Social media en sms (smishing)

Klantcommunicatie kent meer kanalen dan alleen e-mail. Het is dus zaak om kritisch te kijken naar kanalen zoals social media, sms en whatsapp. Criminelen gebruiken deze namelijk net zo goed, maar dan voor smishing: phishing via social media en sms. Gebruik ook bij klantcommunicatie langs deze kanalen (korte) linkjes met uw eigen domeinnaam voor herkenbaarheid, en kies niet voor verkorte URL-diensten van derden (zoals bit.ly, ow.ly of tinyurl.com) waar de klant niet van kan bepalen wat achter de link zit. Houd daarnaast accounts in de gaten die op uw klanten kunnen reageren. Zo reageerde in het verleden een social media-account 'klantenservice' wel eens (ludiek) op vragen van andermans klanten. Zo'n account lijkt misschien betrouwbaar voor de klant, terwijl het geen account is van uw bedrijf. Gebruikt u specifieke social mediakanalen niet? Maak daar dan ook melding van op uw website en registreer bij voorkeur wel uw naam om misbruik te voorkomen.

Spoofing en phishing via de telefoon (vishing)

Criminelen slaan ook telefonisch hun slag met 'voice phishing', ofwel vishing. Zij kunnen daarbij zelfs uw bedrijfstelefoonnummer imiteren om mensen op te lichten. Dan is er sprake van spoofing. We zien dit momenteel gebeuren telefoonnummers van banken.
Vertel uw klanten dat ze bij twijfel altijd de verbinding met de beller kunnen verbreken en een centraal nummer kunnen bellen om het verhaal van de beller te verifiëren. Zo kunnen ze checken of het een legitiem telefoontje was. Communiceer duidelijk naar de klant dat u hen niet opbelt en dan vraagt om op een applicatie in te loggen, of om geld over te maken. Zorg er dus voor dat al uw medewerkers ook echt bereikbaar zijn via het centrale nummer en wees scherp op dit misbruik.

Digitaal visitekaartje

Uw domeinnaam is uw visitekaartje, dus bescherm hem goed. Het is belangrijk dat niemand anders namens uw domeinnaam kan mailen of dat iemand die naam in handen kan krijgen. Bekende beveiligingsmethoden voor e-mail zijn SPF, DKIM en DMARC. Het Nationaal Cyber Security Centrum heeft in de factsheet Bescherm domeinnamen tegen phishing (2) alle informatie samengevat waarmee u uw domeinnaam goed beschermt. Dit kunt u ook nog doen:

- Registreer domeinnamen die erg op de uwe lijken. Een zoekmachine zoals dnstwister kan daarbij helpen;
- Registreer ook domeinen die lijken op subdomeinen, zoals mail-example.nl. Die zien er namelijk net zo vertrouwd uit voor klanten als uw eigen domein. Parkeer deze domeinen, beveilig ze tegen misbruik, maar gebruik ze niet;
- Voorkom dat instellingen van uw domeinnaam aangepast kunnen worden zonder dat u dit weet, bijvoorbeeld met .nl control van SIDN (3);
- Bewaak eventuele domeinen die worden geregistreerd door anderen, maar die erg lijken op uw domeinnaam. Bijvoorbeeld met de DomeinnaamBewakingsService (3) van SIDN waarover uw eigen domeinregistrator kan u hier meer over vertellen. Er zijn zelfs bedrijven die uw volledige digitale profiel, inclusief deep,- en darkweb kunnen bewaken;

Franchise-ondernemingen
Als een bedrijfsnaam ook gebruikt wordt door franchisenemers, is het risico op misbruik van domeinnamen groter (denk aan 'example-amsterdam.nl', of zelf 'example.amsterdam'). Maak dan duidelijke afspraken, bijvoorbeeld over het bijhouden en delen van lijsten met geregistreerde domeinnamen en social media accounts, zodat ook uw klantenservice en/of fraudeafdeling op de hoogte zijn van de franchise-kanalen. Dit voorkomt dat door franchisers geregistreerde domeinnamen oppoppen in monitoringsystemen en worden aangezien als phishingsite.

- Controleer de beveiligings-instellingen van de domeinnaam eens op internet.nl;
- Laat, bij klant bekende, domeinen nooit zomaar verlopen. Ook niet bij een overname of een verandering van uw handelsnaam. Gevoelige e-mail kan jaren later nog worden verzonden naar oude domeinen.

Maak het uzelf makkelijk en gebruik zo min mogelijk domeinnamen. Kies bijvoorbeeld liever voor 'actie.example.nl' (subdomein) dan voor 'example-actie.nl' (echt domein). Veiligheidsbewuste klanten kunnen immers van die eerste aannemen dat het echt bij uw bedrijf hoort, maar van die tweede niet. Vat het voor alle collega's duidelijk samen in een domeinbeleid en voorkom een wildgroei aan domeinen die amper te beschermen zijn. Kennen klanten u onder meerdere handelsnamen, zoals bij 'de Volksbank' de handelsnamen 'ASN Bank' 'RegioBank', 'SNS' en 'BLG Wonen'? Een gouden spelregel zou dan kunnen zijn: 'maximaal één actieve domeinnaam per handelsnaam die de klant kent'.

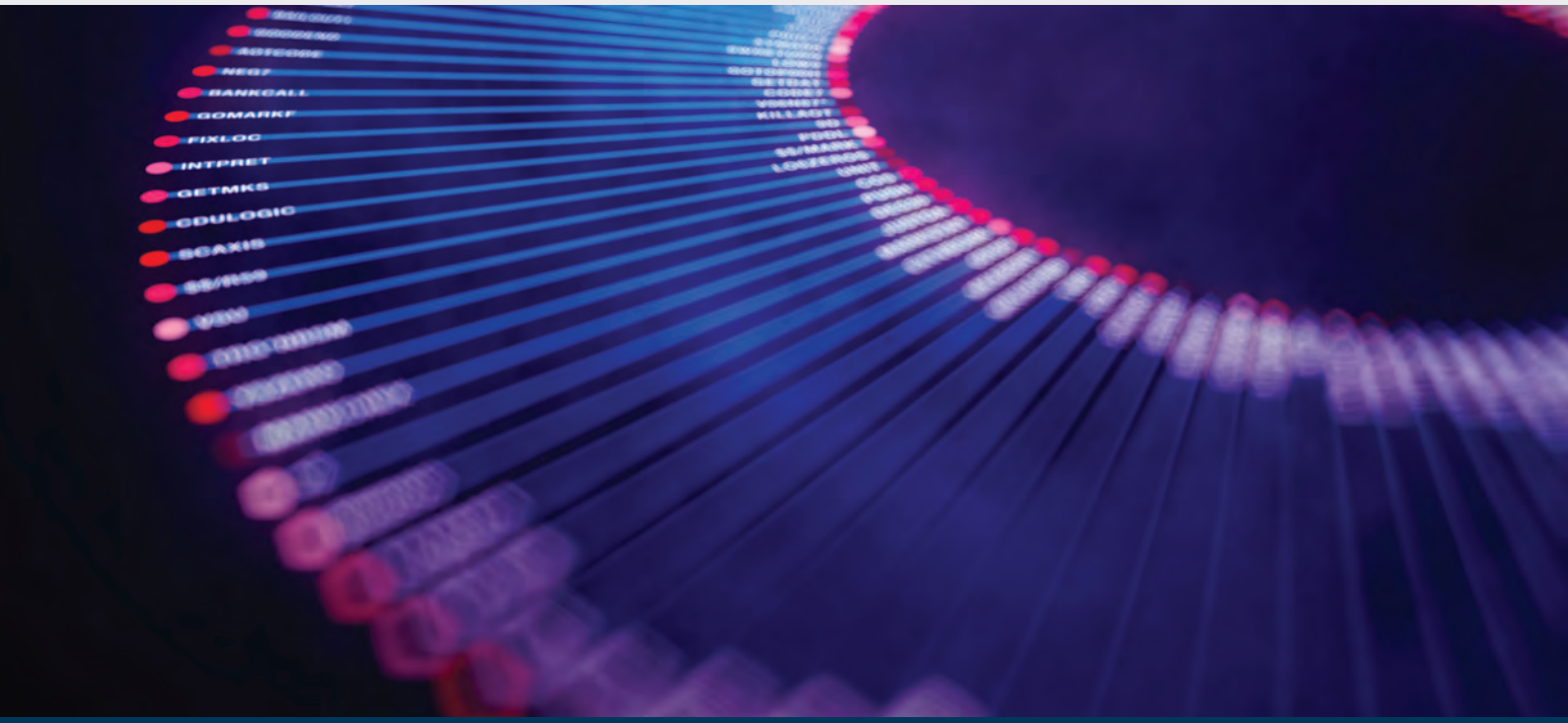
Tot slot: maak het mogelijk om misbruik te melden

Het inschakelen van zogenaamde DMARC-rapportages is van belang om inzicht te krijgen in mogelijk misbruik (of verkeerd gebruik) van het e-mailverkeer. DMARC-rapportages maken echter niet alle vormen van misbruik inzichtelijk. Het blijft dus noodzakelijk om met klanten in contact te blijven. Maak bijvoorbeeld een meldportaal aan met een e-mailadres als valse-email@example.nl of phishing@example.nl, publiceer dat e-mailadres op uw website en zorg dat het inkomende spamfilter meldingen van klanten niet tegenhoudt. Als een klant twijfelt over een e-mail kan deze middels het meldportaal eenvoudig de juiste afdeling bereiken. Mocht de als verdacht aangemerkte e-mail dan toch een legitieme mail betreffen, dan kunt u verbeteringen doorvoeren die helpen voorkomen dat dit in de toekomst nog eens gebeurt. Reageren op de melding is overigens cruciaal! Wanneer melders geen terugkoppeling ontvangen, zal het aantal meldingen (en dus uw kans om ervan te leren) snel afnemen. Een eenvoudig 'bedankt voor uw melding, wij gaan dit bericht onderzoeken en waar nodig vervolgacties ondernemen' kan voldoende zijn. Met zo'n klein blijk van waardering vergroot u de betrokkenheid van uw klant met uw bedrijf. En dat is al snel de moeite waard!

Referenties

(1) Goede bulkmail lijkt niet op phishing, https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-goede-bulkmail-lijkt-niet-op-phishingmail
(2) 'Bescherm domeinnamen tegen phishing', https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-bescherm-domeinnamen-tegen-phishing n.b. Delen van dit artikel eerder verschenen zijn als nieuwsbericht voor zakelijke Regiobank klanten op https://www.regiobank.nl/nieuws/actueel/bericht/bescherm-uw-bedrijf-beter-tegen-phishing-6-tips.html.
(3) https://www.sidn.nl/product/dbs

Auteurs: Luuk Bekkers is junior onderzoeker bij het Centre of Expertise Cyber Security van de Haagse Hogeschool en bereikbaar via l.m.j.bekkers@hhs.nl. Rick van der Kleij is senior onderzoeker bij het Centre of Expertise Cyber Security van de Haagse Hogeschool en TNO en is bereikbaar via r.vanderkleij@hhs.nl. Rutger Leukfeldt is senior onderzoeker bij het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving (NSCR) en directeur van het Centre of Expertise Cyber Security en is bereikbaar via e.r.leukfeldt@hhs.nl.



Succesfactoren voor het delen van cybersecurity informatie

In de afgelopen jaren zijn diverse cyberveiligheid informatiedeling-initiatieven opgericht. Dergelijke samenwerkingsverbanden zijn van groot belang om cyberdreigingen het hoofd te kunnen bieden. Maar welke factoren zorgen ervoor dat die initiatieven succesvol zijn?

Bedrijven maken tegenwoordig vaak deel uit van een keten. Een keten kan worden be¬schouwd als een verzameling organisaties waar informatie, diensten, goederen of geld doorheen stroomt (1). Hierbij staat ICT veelal centraal. Deze rol van ICT maakt dat cybergerelateerde risico's een opmars maken binnen ketens. Maar niet elke organisatie beschikt over de middelen en kennis om zichzelf te beschermen: om tot sterke ketens te komen is informatiedeling tussen ketenorganisaties over actuele dreigingen en incidenten van belang.

Digitale weerbaarheid

Er zijn dan ook diverse cyberveiligheid informatiedeling-initiatieven ontwikkeld. Deze samenwerkingsverbanden kunnen van grote waarde zijn voor organisaties om het risico op cyberincidenten te verkleinen. Met behulp van de informatie die wordt gedeeld zijn de deelnemende organisaties namelijk beter in staat hun eigen risicoanalyse uit te voeren en bijpassende maatregelen te treffen. Hierdoor vergroten zij de digitale weerbaarheid van de eigen organisatie en van de sector als geheel. Het is alleen nog onduidelijk welke factoren van invloed zijn op het succes van cyberveiligheid informatiedeling-initiatieven. Inzicht in dergelijke succesfactoren kan door overheidspartijen en andere belanghebbenden gebruikt worden om bedrijven te adviseren en bestaande of toekomstige samenwerkingsverbanden te ondersteunen. De Haagse Hogeschool heeft daarom in opdracht van het Nationaal Cyber Security Centrum een verkennende studie uitgevoerd naar succesfactoren van cyberveiligheid informatiedeling-initiatieven. Dit artikel bevat een overzicht van de belangrijkste resultaten. Voor een volledig overzicht van de resultaten verwijzen we naar de onderzoeksrapportage (2). Het onderzoek richtte zich op twee informatiedeling-initiatieven in de energiesector en een informatiedeling-initiatief van managed serviceproviders. Om succesfactoren te identificeren, voerden wij interviews uit met in totaal zes deelnemers. Alle respondenten zijn informatiebeveiligingsexperts die namens nationale en internationale bedrijven zijn aangesloten bij de informatiedeling-initiatieven.

Vier belangrijkste factoren voor succesvolle informatiedeling-initiatieven

In totaal zijn twintig factoren geïdentificeerd die bijdragen aan succesvolle informatiedeling-initiatieven op het gebied van cyberveiligheid. Vier factoren die door vrijwel alle respondenten zijn benoemd en daarmee worden beschouwd als de belangrijkste zijn: expertise onder de leden, vertrouwen, lidmaatschapseisen en een structurele opzet. Deze vier factoren worden nu kort toegelicht.

Vertrouwen is een thema dat bij alle respondenten aan bod komt als kritieke succesfactor: een hoge mate van vertrouwen tussen leden is vereist voor de bereidheid om informatie te delen. Met vertrouwen doelen we op de overtuiging van een lid dat andere leden de juiste bedoelingen hebben en om die reden bereid is afhankelijk te zijn van de daden van die andere leden. Ook lijkt vertrouwen gerelateerd aan veel andere factoren die zijn geïdentificeerd. Het nemen van tijd wordt door respondenten aangehaald als belangrijkste bouwsteen voor vertrouwen: er is tijd nodig om vertrouwen in de relatie te ontwikkelen. Naast het nemen van tijd, zijn andere bouwstenen voor vertrouwen volgens respondenten: er sprake is van een stabiele bezetting, de deelnemende bedrijven en diens vertegenwoordigers worden nauwkeurig in overleg gekozen, alle vertegenwoordigers zijn informatiebeveiligingsexperts en hebben overlappende vakinhoudelijke kennis (common body of knowledge). Zodra het onderlinge vertrouwen wordt geschaad, bijvoorbeeld als vertrouwelijke informatie voor commercieel gewin wordt verkocht, houdt direct alle informatiedeling op met die partij, zo stellen de respondenten.

Naast vertrouwen noemen alle respondenten expertise onder de leden als belangrijke factor voor succes. Zo zijn alle deelnemers van de onderzochte informatiedeling-initiatieven informatiebeveiligingsexperts, in tegenstelling tot sommige andere samenwerkingsverbanden waar ook beleidsmakers aansluiten. Doordat de deelnemers vakinhoudelijke kennis hebben en 'dezelfde taal spreken' wordt er relevante kennis gedeeld, weten de deelnemers hoe ze moeten handelen met die kennis en is het onderling vertrouwen hoog. Deze expertise helpt leden ook bij het maken van een afweging of bepaalde informatie toegevoegde waarde heeft en dus gedeeld zou moeten worden. De deelnemende bedrijven en diens vertegenwoordigers zijn op basis van lidmaatschapseisen gerechtigd om aan te sluiten. Zo geldt bij een van de onderzochte informatiedeling-initiatieven dat een bedrijf minimaal drie vitale

klanten moet bedienen voordat deelname mogelijk is. De vertegenwoordiger moet tevens op senior niveau verantwoordelijk zijn voor de informatiebeveiliging binnen diens organisatie en daar een goede informatiepositie hebben. Een dergelijke ballotage is tevens nodig voor het ontwikkelen van vertrouwen en speelt daarom een belangrijke rol bij succesvolle informatiedeling.

De informatiedeling-initiatieven zijn tevens succesvol door een gestructureerde opzet, zoals een vaste frequentie van bijeenkomsten, een stabiele bezetting en een vaste agenda. Dit is nodig om tot resultaat te komen en verhoogt het vertrouwen tussen leden, aldus de respondenten. Een belangrijke factor hierbij is de aanwezigheid van afspraken over hoe om te gaan met de informatie die de leden hebben, zoals het 'traffic light protocol'. Daarmee wordt voor alle deelnemers helder welke afspraken er zijn omtrent het delen van informatie en worden onnodige discussies vermeden. Verder draagt ook een jaarplan bij aan de gestructureerde opzet. Aan de hand van het jaarplan bepalen de leden welke onderwerpen op de agenda komen.

Naast de succesfactoren is er ook gevraagd naar de aanleiding en de meerwaarde voor de respondenten van de initiatieven. Zo blijkt uit de interviews dat de onderzochte informatiedeling-initiatieven zijn ontstaan vanuit het idee om Nederland veiliger te maken op het gebied van cyberveiligheid, mede op initiatief van en in samenwerking met overheidspartijen. Het valt op dat de initiator een belangrijke rol heeft bij het opstarten, bijvoorbeeld door organisaties en experts binnen de eigen sector te enthousiasmeren en te motiveren om deel te nemen aan een samenwerking. De meerwaarde van de initiatieven is voor alle door ons gesproken respondenten drieledig: netwerken met collegae, leren van elkaar en verbetering van de eigen bedrijfsvoering.

Vragen voor vervolgonderzoek

Het onderzoek laat zien dat er een groot aantal factoren zijn die bijdragen aan het succes van informatiedeling-initiatieven op het gebied van cyberveiligheid. Deze factoren kunnen door de overheid, maar ook door organisaties zelf, gebruikt worden om bestaande en toekomstige samenwerkingsverbanden te ondersteunen. De verkennende aard van het onderzoek maakt echter dat er nog een aantal vragen of onderwerpen zijn die nader onderzoek verdienen. Zo zou vervolgonderzoek zich kunnen richten op het identificeren van strategieën voor het opstarten van informatiedeling-initiatieven op het gebied van cyberveiligheid en hoe relevante partijen daar in eerste instantie voor bij elkaar kunnen worden gebracht. Daarbij is het ook de vraag hoe een samenwerkingsverband een zelfstandig functionerende eenheid wordt over de tijd heen en minder afhankelijk kan worden gemaakt van de inspanningen van één of enkele personen, zoals de initiator of voorzitter.

Zoals genoemd, is de factor vertrouwen cruciaal gebleken voor het succes van de door ons onderzochte samenwerkingsverbanden. Toekomstig onderzoek zou zich kunnen richten op strategieën om het onderling vertrouwen tussen deelnemers te initiëren, faciliteren en behouden over de tijd. Op basis van het huidig onderzoek kan niet (voldoende) worden geconcludeerd of en op welke manier de geïdentificeerde factoren samenhangen met elkaar. Vervolgonderzoek zou zich dus ook kunnen richten op het duiden van de onderlinge (causale) samenhang tussen succesfactoren en hoe de factoren zich ontwikkelen binnen samenwerkingsverbanden.

Een laatste mogelijkheid voor vervolgonderzoek die wij hier willen noemen is gericht op de vraag hoe de samenwerking tussen ketenpartners op het gebied van cyberveiligheid buiten formele informatiedeling-initiatieven is ingericht. Focus hierbij op leveranciers, afnemers en overheidsinstanties van niet-vitale processen. Onderzoek zou zich hierbij kunnen richten op de samenwerking tussen grootbedrijven en het midden- en kleinbedrijf van wie ICT niet de corebusiness is, aangezien dergelijke bedrijven veelal als risicovol voor cybersecurity worden beschouwd.

Referenties

(1) Urciuoli, L. (2015). Cyber-resilience: a strategic approach for supply chain management. Technology Innovation Management Review, 5(4).

(2) https//:www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/rapport-a4-lectoraat-cybersecurity-in-het-mkb.pdf

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Hoe de class-action naar Nederland kwam

Een van de meest krachtige voortstuwende bewegingen die de AVG op haar conto mag schrijven is het grotere privacybewustzijn bij mensen en het besef dat hun privacy gevaar kan lopen. De Autoriteit Persoonsgegevens zette daar in de campagnes van 2018 dan ook fors op in, waarbij zelfs de social media niet geschuwd werden om het punt te maken. De privacywaakhond gaat inmiddels zwaar gebukt onder het privacysucces en haar eigen magere bezetting. In de laatste budgetrondes in het Haagse, verloor ze daarnaast ook nog eens een miljoen op de begroting.

Trouw kopte op 10 november 2020 zelfs: 'Voorzitter Autoriteit Persoonsgegevens: De achterstanden zijn zo groot, dat het lachwekkend is'. Ik begrijp dat je soms best even moet roepen om politiek te bedrijven, maar de voorzitter, Aleid Wolfsen, heeft natuurlijk wel een fair punt. Sterk inzetten op privacy met krachtige wetgeving en dan niet afdoende kunnen handhaven is niet te verkroppen.

Steeds meer bezorgde burgers en klanten vinden de weg naar AP en naar overheid en bedrijven. Ze klimmen in de pen om de Functionaris Gegevensbescherming in te schakelen en schrijven bedrijven aan met inzageverzoeken. Massaal worden ook klachten ingediend bij de toezichthouder. Helaas kunnen die vaak pas op zijn vroegst na een half jaar behandeld worden. Dat is overigens nog relatief kort vergeleken bij de periode van 5 tot 7 jaar die het moet duren voor een bedrijf de door hen voorgestelde Binding Corporate Rules (BCR) behandeld ziet door AP. Die BCR's zijn vaak wel broodnodig om gegevensdoorgifte in internationale bedrijven goed in te regelen. Maar dat laatste vooral terzijde en ter illustratie.

Hoewel het dus wel voor iedereen veel werk oplevert en sommigen meer op het bord hebben dan ze aankunnen, zie ik daar vooral ook een ontzettend positieve beweging in. Mensen pikken het niet langer dat gegevens zomaar gebruikt worden voor allerhande doelen. En waar er voorheen soms nog best een defaitistische houding volgde, want 'het is toch vechten tegen de bierkaai en wat voor verschil kan ik nu maken?', is nu meer activisme ontstaan. Zoveel zelfs dat we inmiddels een heuse class-action hebben (dat ken je vast wel uit Amerikaanse spannende films) op het gebied van privacy.

Bezorgde internetgebruikers (en laten we eerlijk zijn, wie is dat nou niet?) pikken het niet langer en dagen Salesforce en Oracle voor de rechter. The Privacy Collective, bijgestaan door Christiaan Alberdink Thijm, dient een massaschadeclaim in van 10 miljard euro voor inbreuk op de AVG. Zij ageren voornamelijk tegen het op grote schaal en voortdurend profileren van personen door bovengemelde bedrijven. Internetgebruikers kunnen zich aansluiten bij deze claim en op het moment van schrijven hebben zich al 48.492 ondertekenaars gemeld en ik denk dat dat aantal nog wel zal stijgen. Christiaan Alberdink Thijm is ook niet voor een kleintje vervaard; hij verkreeg zijn bekendheid rond 2000 door het bijstaan van KaZaA, de toen befaamde muziekuitwisselingssite die de muziekindustrie over zich heen kreeg. Hoe dan ook is het voor Nederlandse begrippen een unieke zaak en ik ga het dan ook zeker op de voet volgen. De cola en chips staan al klaar.

Rachel

Auteur: mr. A.IJ. (Ard) Ruiter werkt als privacy- en beveiligingsfunctionaris/senior inspecteur bij de ILT Inlichtingen- en Opsporingsdienst (ILT-IOD). Hij schreef dit artikel op persoonlijke titel en is bereikbaar via ardlinkedin@hotmail.com.

Parliament goes digital

Over Kamercommissie Digitale Zaken en informatiebeveiliging

Na de Tweede Kamerverkiezingen op 17 maart 2021 zal het parlement uit een nieuwe, vakoverstijgende vakgroep bestaan: de vaste commissie voor Digitale Zaken. Logisch: de digitale transitie raakt alle onderdelen van ons leven. Dit comité zal een kennis-impuls voor het parlement kunnen worden. Een beschouwing om te zien of deze ontwikkeling aansluit bij informatiebeveiliging en cybersecurity.

Natuurlijk is deze ontwikkeling ook relevant voor het bedrijfsleven. Bijna iedereen en alle bedrijven werken met ICT en veel data vliegt over het net. Het parlement controleert de 'raad van bestuur' van de bv Nederland en heeft een wetgevende taak. In een Kamerbrief over de toegenomen externe inhuur van ICT-personeel is vermeld dat de Rijksoverheid steeds ICT-intensiever wordt. "Dat leidt tot een toenemende (flexibele) vraag naar ICT-capaciteit. Een deel van die vraag wordt door externen ingevuld. De genoemde redenen voor externe inhuur gelden ook, zo niet sterker, voor ICT-inhuur. Juist in het vakgebied ICT is veel sprake van tijdelijke projecten, piekbelastingen en/ of specifiek benodigde expertise, waarbij externe inhuur de meest doelmatige oplossing biedt. Zonder externe ICT'ers zou het Rijk minder flexibel zijn, oftewel minder taken tijdig kunnen uitvoeren, minder kwaliteit kunnen bieden en minder snel kunnen omgaan met veranderende behoeften." (1) Voor de inhuur van ICT'ers worden ook raamovereenkomsten gesloten (2).

Parlementaire belangstelling voor digitale transitie

Hoe de uitslag van de verkiezingen voor de leden van de Tweede Kamer der Staten-Generaal zal uitvallen, zullen we pas weten tijdens en na de verkiezingsavond. Wat al wel vaststaat, is dat de nieuwe Kamer met een nieuwe commissie zal zijn uitgebreid: de vaste commissie voor Digitale Zaken. Daarmee wordt structureel de parlementaire belangstelling voor digitale transitie geborgd (3). Die commissie zal ervoor moeten zorgen dat de kennispositie van de volksvertegenwoordiging wordt versterkt op het gebied van digitalisering en dat zij meer grip krijgt op gewenste en ongewenste ontwikkelingen die samenhangen met digitalisering. Gedebatteerd kan worden over privacy en eigendom van data. Wie bezit de gegevens, onder welke voorwaarden mogen deze gedeeld worden, wie is verantwoordelijk en aansprakelijk? Naast vragen over verticale privacy, tussen overheid en burgers, roept digitalisering ook vragen op over horizontale privacy: hoe worden burgers beschermd tegen bedrijven en elkaar? "De technologie biedt kansen, (…) maar zij brengt ook een breed scala aan nieuwe vraagstukken met zich mee, onder meer op het gebied van privacy."

Aanloop, achtergrond, taken

Tot de nieuwe commissie werd besloten als vervolg op het eindrapport van de tijdelijke Kamercommissie Digitale toekomst (TCDT) (4) die onderzocht hoe het parlement meer grip kan krijgen op het thema digitalisering. "Het is de taak van de Tweede Kamer om ook hierbij de Nederlanders te vertegenwoordigen: grip krijgen op onze digitale toekomst en op die manier de meningen van de Nederlanders recht doen." De TCDT constateerde dat digitalisering een steeds belangrijker onderwerp is geworden en in steeds meer domeinen van de samenleving doordringt. De aanbevelingen zijn:

- Richt een vaste Tweede Kamercommissie voor Digitale Zaken op;
- Bepaal welke kennis over digitalisering nodig is;
- Ondersteun andere Kamercommissies over digitalisering;
- Zorg voor passende regelgeving voor digitalisering en stem goed af met de toezichthouders op digitalisering;
- Weet wat er speelt in de Europese Unie en bepaal met de regering wat Nederland daar inbrengt over digitalisering.

De vaste commissie voor Digitale Zaken krijgt de volgende taken:

- Het controleren en behandelen van wetgeving van de bewindspersoon die verantwoordelijk is voor digitalisering of, in de afwezigheid daarvan, van de bewindspersoon die de eindverantwoordelijkheid heeft voor het thema;
- Het verkennen, doordenken en agenderen van huidige en toekomstige commissie-overstijgende ontwikkelingen op het gebied van digitalisering;
- Het informeren van andere commissies over relevante ontwikkelingen op het gebied van digitalisering;
- Het voortouw nemen bij coherente en integrale behandeling van commissie-overstijgende digitaliseringsvraagstukken;
- Het fungeren als aanspreekpunt voor digitaliseringskwesties voor zowel het kabinet als maatschappelijke groepen, bedrijfsleven, wetenschap en anderen.

De gekozen variant lijkt veel op die van de Duitse deelstaat NRW. De Landtag Nordrhein-Westfalen heeft een 'Ausschuss Digitalisierung und Innovation' en houdt zich bezig met de thema's digitalisering, innovatie, technologie en automatisering (5). Op federaal niveau heeft de Bundestag een 'Ausschuss Digitale Agenda'; deze begeleidt andere Bundestagausschüsse vanuit een digitaal beleidsperspectief, maar heeft weinig leidende thema's toegewezen gekregen. De vaste commissies voor 'Technikfolgenabschätzung' en 'digitale Infrastruktur' houden zich meer met digitale thema's bezig. Nog vermeldenswaardig is dat op 28 oktober 2020 de Bundestagausschuss 'Künstliche Intelligenz' een rapport over artifical intelligence publiceerde (6).

Informatiebeveiliging is de achilleshiel van het informatietijdperk

Wat zijn Digitale Zaken?

Het eerste hoofdstuk van het eindrapport 'Update vereist' onder de titel 'Digitale transitie: nieuwe maatschappelijke vraagstukken', is een mooie, goed onderbouwde schets van diverse (nieuwe) maatschappelijke vraagstukken die de digitale transitie met zich meebrengt en die de aandacht vragen van de politiek. Hoofdstuk 2 is een zelfreflectie van de Tweede Kamer en hoofdstuk 3 bevat voorstellen voor meer grip.
Het eindrapport is een aanrader voor studenten en eigenlijk voor iedereen die goed inzicht wil krijgen in nieuwe technologieën zoals Internet of Things (IoT), camera's en sensoren, biometrie, persuasieve technologie, digitale platformen, virtual en augmented reality, big data, navigatieclicks, social media posts, app downloads, robots en apps en al wat dies meer zij én zeker ook welke invloed dat heeft of kan hebben op:

- het fysieke domein (publieke ruimte, binnenshuis, op ons lichaam, onderliggende infrastructuur),
- het biologische domein (menselijk lichaam, het herkennen van personen en emoties, de beïnvloeding van gedrag) en
- ook het sociaal-culturele domein (communicatie en cultuur, organisatiemodellen).

Maar wat zijn eigenlijk 'Digitale Zaken'? In het eindrapport staat 'Digitalisering is een breed begrip' en de term 'digitalisering' (wordt gebruikt – red.) voor de ontwikkelingen in de samenleving die te maken hebben met het toenemend gebruik van digitale informatie, data en apparaten.
Door de omvang en het tempo waarin dit gebeurt, blijkt digitalisering de motor achter een transitie die de samenleving radicaal verandert en nieuwe kansen en risico's met zich meebrengt. Niet helemaal helder is of een onderscheid kenbaar is tussen de begrippen feiten, gegevens, data, informatie, kennis en competenties (7), business intelligence, informatiegestuurd en/of datagedreven werken. Bij datamanagement gaat het om het bereiken van de waarde van data én het goed balanceren tussen theorie en praktijk (8). In een informatiecyclus is het van belang deze voortdurend te spiegelen aan de feiten. Een zogezegde toets aan de werkelijkheid voorkomt dat data - die al dan niet in een abusievelijk onjuiste context is geïnterpreteerd - een vervolgens feitelijk onjuist eigen leven gaan leiden. Op die manier verkrijgt data de meest actuele, juiste en hoogst haalbare, accurate waarde.

De digitale transitie is enorm en gaat ongekend snel. De grote veranderingen zijn te herleiden tot drie grote ontwikkelingen: (9)

- Technologische systemen worden steeds beter, sneller en preciezer;
- Technologie zal, nog meer dan nu, integreren in onze samenleving en
- Steeds meer aspecten van onze samenleving zullen gekwantificeerd worden.

Informatiebeveiliging en cybersecurity

"Informatiebeveiliging is de achilleshiel van het informatietijdperk", zo werd eens gesteld in de Duitse Bundestag (10). In het eindrapport van de TCDT komt de term 'informatiebeveiliging' (helaas) slechts éénmaal en in de marge voor: 'Een ander risico, naast de kwetsbaarheid in informatiebeveiliging, is dat verzamelde data aan elkaar gekoppeld worden, zonder rekening te houden met bestaande wet- en regelgeving'. De risico's worden wel degelijk genoemd bij de groeiende digitalisering van de onderliggende infrastructuur. 'Cyberaanvallen, maar ook menselijke fouten, kapotte servers, softwareproblemen of externe factoren als kabelbreuken of elektriciteitsstoringen kunnen zo leiden tot wat de Wetenschappelijke Raad voor het Regeringsbeleid 'digitale ontwrichting' noemt' (11). 'Het MKB en de burger staan bloot aan de steeds professionelere methoden van cybercriminelen en de opkomst van het Internet of Things vergroot de kwetsbaarheid voor cyberaanvallen. Dit en meer maakt dat cybersecurity niet eerder zo belangrijk is geweest.' Ook zijn er al vele nota's van de Kamer zelf geweest waarin bijzondere aandacht gevraagd wordt voor de gevolgen van digitale ontwikkelingen voor publieke waarden als veiligheid, privacy en controle van de mens over technologie. Vaak is geadviseerd om 'meer oog (…) voor risico's, maar tegelijkertijd kansen niet onbenut te laten' (12).

Tien jaar Rekenkameronderzoek

In het verlengde daarvan is de aan de Kamer aangeboden factsheet 'Grip op digitalisering: rode draden uit tien jaar Rekenkameronderzoek' interessant: een handzaam overzicht van onderzoeken die de Algemene Rekenkamer opnieuw heeft geanalyseerd (13).

Op de website: https://www.rekenkamer.nl/onderwerpen-/ict-en-digitalisering is de factsheet en een doorklikbaar webdossier te vinden. De Rekenkamer onderzoekt cybersecurity en informatiebeveiliging, digitalisering van de Rijksoverheid, ICT-lifecyclemanagement en IT-beheer. Op basis daarvan worden drie belangrijke opgaven geformuleerd voor grip op digitalisering.
Het is van belang dat:
1. de gebruiker centraal staat;
2. de gewenste (digitale) doelstellingen worden gerealiseerd en
3. het parlement de digitalisering goed kan controleren.
Daar vernemen we interessante aspecten over ons werkgebied. Gebiedend schrijft de Rekenkamer: 'Een digitaliserende overheid dient eerst en vooral op een zorgvuldige manier met data om te gaan, door het borgen van privacy en het adequaat beveiligen van informatie'. Burgers, bedrijven en ambtenaren hebben behoefte aan gebruiksvriendelijke systemen.

Voldoende regie is wenselijk op gegevens die in de systemen van de overheid staan. Een veilige, betrouwbare en gebruikersvriendelijk frontoffice begint 'onder de motorkap'. Daar is transparantie over het gebruik van (persoonlijke) data van burgers en bedrijven van belang wanneer de overheid afwegingen maakt.
Voorts adviseert de Rekenkamer – uiteraard – tot goede informatiebeveiliging. Digitale dienstverlening efficiënter en effectiever inrichten kan door te standaardiseren en te sturen op een gemeenschappelijke ICT-taal. Het perspectief van de gebruiker vraagt om dienstverlening waarbij overheidsorganisaties goed samenwerken in een keten of een stelsel.

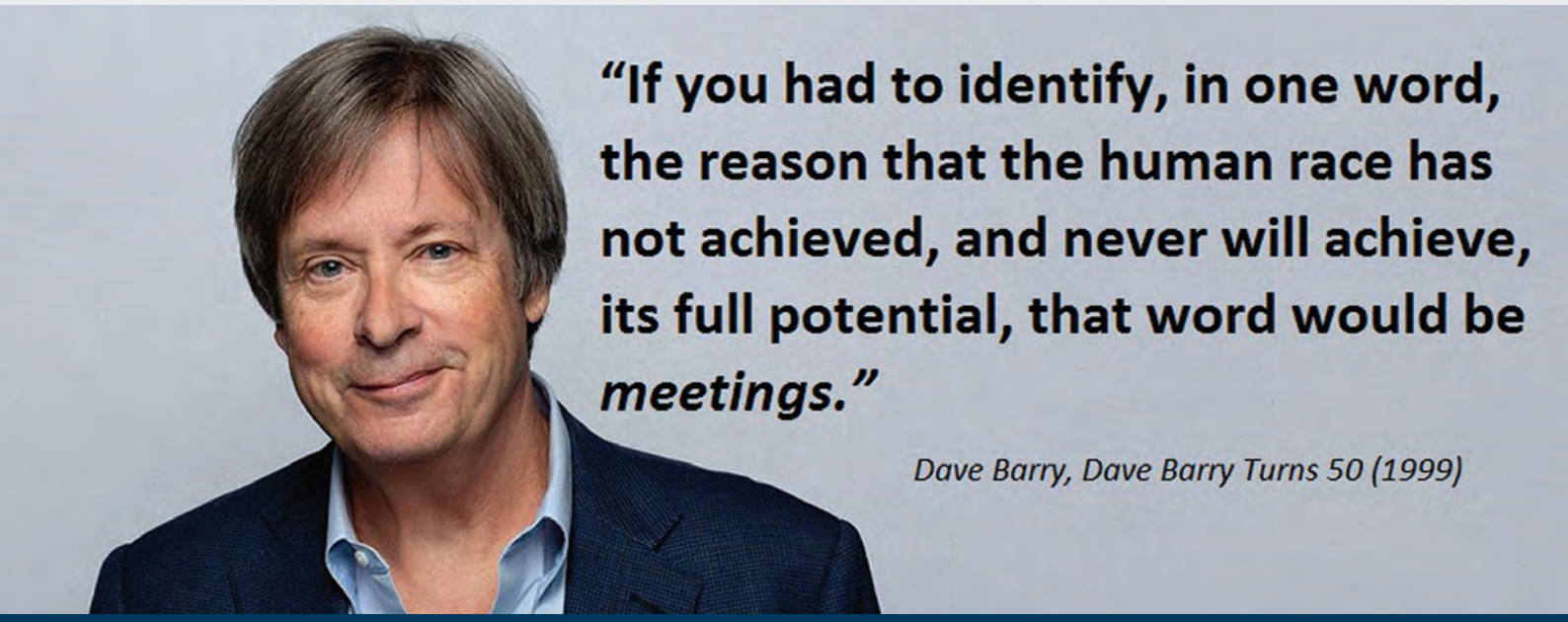
Het ICT-landschap moet goed onderhouden en functioneel zijn: lifecyclemanagement vergt inzicht in bestaande ICT alsook concrete plannen voor beheer, onderhoud én vernieuwing. Voorts adviseert de Rekenkamer om beter inzicht in de kosten van de ICT - zodat de juiste investeringsbeslissingen worden genomen - en dat er voldoende zicht is op de kwaliteit en efficiëntie van IT-beheer. De Rekenkamer constateert verder dat er onvoldoende eisen worden gesteld aan lifecyclemanagement, kosten alsook kwaliteit. Ook kan gekeken worden naar een meer gemeenschappelijk en gestandaardiseerd kwaliteitsmanagement. De Rekenkamer constateert verder dat er onvoldoende eisen worden gesteld aan lifecyclemanagement, kosten alsook kwaliteit.

Het overzicht van Rekenkameronderzoeken geeft in enkele oogwenken goede handvatten en aanknopingspunten. De voornoemde website is het raadplegen waard en geeft inzicht voor allen in het taakveld om verbeteringen door te voeren. Kortom: er valt nog wat te kiezen; niet alleen voor de Kamerverkiezingen, maar ook over privacybescherming en informatietechnologie.

Referenties

(1) Kamerbrief 'Toelichting op toename externe inhuur (ICT) personeel Rijk', Kamerstukken II 2018-19, 31 490, 254
(2) https://www.pianoo.nl/nl/markten/ict/ict-categorieen/inhuur-ict-personeel, https://www.consultancy.nl/nieuws/13253/raamovereenkomsten-ict-inhuur-voor-bzk-gegund-aan-acht-partijen en https://www.consultancy.nl/nieuws/30830/zes-partijen-leveren-it-experts-aan-overheidsdienstverlener-logius
(3) Kamerstukken II 2020-21, 35229, 12
(4) Tijdelijke commissie digitale toekomst, Buitenweg, K.M. (2020). Update vereist: Naar meer parlementaire grip op digitalisering. Den Haag: Tweede Kamer der Staten-Generaal; Kamerstukken II 2019-20, 35 229, nr. 10. In dit artikel aangehaalde citaten komen uit dit rapport. https://www.tweedekamer.nl/sites/default/files/atoms/files/eindrapport_tijdelijke_commissie_digitale_toekomst_tweede_kamer_der_staten-generaal.pdf
(5) Onduidelijk is waarom deze variant niet is genoemd in het rapport Jong, R. de, Keulen, I. van, Hove, L. van & Munnichs, G. (2020). Meer grip op digitalisering – Een internationale vergelijking van parlementaire werkvormen. Den Haag: Rathenau Instituut; Kamerstukken II 2019-20, 35229, 12
(6) https://dip21.bundestag.de/dip21/btd/19/237/1923700.pdf
(7) Ook wel aangeduid als de informatieladder, zie: Bruins, R., Pinkster, B. (2015) Informatiemanagement, Amsterdam: Pearson Benelux; Grit, R. (2019), Informatiemanagement, Groningen: Noordhoff Uitgevers, p. 22
(8) Gils, B. van. (2020) Data Management: a gentle introduction, Balancing theory and practice, 's-Hertogenbosch: Van Haren Publishing; Vries, C. de. 'Boekreview Data Management: a gentle introduction, Informatiebeveiliging Magazine, 2020, nr. 4, p. 12-13
(9) Susskind, J. (2018). Future politics – Living Together in a World Transformed by Tech. Oxford: Oxford University Press; Behr, R., Future Politics by Jamie Susskind review – when life-changing decisions are made by machines, the Guardian 5 December 2018; https://www.theguardian.com/books/2018/dec/05/future-politics-by-jamie-susskind-review-when-life-changing-decisions-are-made-by-machines
(10) Manuel Höferlin (FDP) nannte die IT-Sicherheit die "Achillesferse des Informationszeitalters" in: H. Stoltenberg ‚Streit um Digitalpolitik – IT-Sicherheit – Opposition hält Regierung Versäumnisse vor' Das Parlement, nr. 8. Berlin, 18. Februari 2019, p. 4; http://epaper.das-parlament.de/2019/8/index.html#4
(11) Wetenschappelijke Raad voor het Regeringsbeleid (2019). Voorbereiden op digitale ontwrichting (WRR-rapport nr. 101). Den Haag: WRR
(12) Kaal, H., Hoetink, C. (2020). Doordacht digitaliseren. Digitalisering doordacht. Resultaten van een onderzoek naar het parlementaire debat over digitaliseringsvraagstukken, 2009-2019. Nijmegen: Radboud Universiteit
(13) Algemene Rekenkamer (2020). Grip op digitalisering: rode draden uit tien jaar Rekenkameronderzoek. Den Haag, Kamerstukken II 2019-20, 35229, 6

Auteur: Robert Metsemakers schrijft op persoonlijke titel en is als ervaren IT-auditor en informatiebeveiligings-expert beschikbaar voor security-advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.



BLOG

Stapsgewijs aanpakken van negatief gedrag in vergaderingen

In zijn boek `Dave Barry Turns 50' schreef hij: `If you had to identify, in one word, the reason that the human race has not achieved, and never will achieve, its full potential, that word would be meetings'. We kunnen niet uitsluiten dat ooit een vergadering tot een positief resultaat heeft geleid, maar veel vergaderingen zijn helaas zonder doel of resultaat en daarmee zonder nut. Door negatief gedrag van deelnemers zijn vergaderingen vaak bijzonder onplezierig voor de overige aanwezige personen en zonde van hun tijd.

Gebruik van de tabel

Neem deze tabel door en pik er het storende gedrag uit dat je zelf laat zien in vergaderingen en neem je voor om precies dit in de eerstvolgende vergadering (Zoom, Teams of fysiek) eens een keer niet te vertonen. Het resultaat is te versterken door de lijst met alle deelnemers te delen. Zodat iedereen voor zich (in het geheim) een eigen verbeterpunt kan kiezen. Die verbeterpunten gaan dan allemaal tegelijkertijd werken. Wat een feest om daar bij te zijn.

Sommige mensen hebben geluk en kunnen uit meerdere acties kiezen. Beperk het echter tot één aanpassing per vergadering. In het bijzondere geval dat alle gedragingen bij één bepaalde rol in de tabel van toepassing zijn, mag je jezelf wel lichte zorgen maken. Hoewel we allemaal volledige mensen zijn en niet uitsluitend de rol die we in vergaderingen spelen, past die stereotiepe rol dan toch wel heel erg goed bij jou. Je staat als het ware aan de rand van de afgrond en bent met dit `standaardgedrag' al bijna veranderd in het stereotype, mogelijk ook buiten vergaderin-

Blocker
- Blokkeert de voortgang van de groep door afleidende of tangentiële discussies op gang te brengen
- Verwerpt ideeën zonder enige overweging
- Brengt voortdurend oude problemen naar voren die de groep eerder heeft opgelost

Attacker
- Bekritiseert, beschuldigt of beschuldigt teamleden
- Valt degenen aan die het niet (met hem) eens zijn

Attention seeker
- Zoekt erkenning door opscheppen
- Vertoont storend gedrag
- Promoot extreme ideeën
- Vertoont ander egocentrisch gedrag

Withdrawer
- Handelt passief en niet toegewijd aan de groep
- Kan niet deelnemen (aan werkgroepen) of toegewezen taken voltooien
- Mist vergaderingen (of komt te laat, loopt weg voor telefoon of vertrekt eerder)
- Neemt passief-agressief toevlucht tot buitensporige formaliteit bij het aanspreken van andere groepsleden

Monopolizer
- Zoekt erkenning en aandacht door het gesprek te monopoliseren
- Onderbreekt anderen voordat ze hun mening volledig hebben geuit
- Concurreert met andere groepsleden om aandacht

Poor listener
- Begrijpt vaak verkeerd wat anderen zeggen. Soms door na te denken over wat ze hierna zelf willen zeggen in plaats van te focussen op wat de huidige spreker zegt

Dominator
- Manipuleert individuele groepsleden of de hele groep door op ongepaste wijze echte of zelfgepercipieerde autoriteit uit te oefenen

Zealot [1]
- Probeert (voortdurend) leden te bekeren tot favoriet idee of stokpaardje
- Geeft preken aan groep over de toestand van de (hele) wereld
- Vertoont fanatisme

Cynic [2]
- Geeft een zuur uitzicht
- Houdt zich bezig met het opsporen van fouten
- Richt zich op negatieve aspecten
- Voorspelt het falen van de groep

gen. Nog een stap verder en je zegt: 'Ja die gedragingen van die rol doe ik allemaal, maar ik zie niet in wat daar negatief aan is. Sterker nog, die acties maken mij juist zo effectief'. Ook dan is nog niet alles verloren, want je kunt nog steeds heel bewust één van de gedragingen als experiment een keer niet doen en kijken wat dat oplevert. Kijk na afloop terug op de vergadering – was de sfeer, het tempo, het resultaat en je gevoel over 'volgende week weer met deze lui vergaderen', anders door jouw veranderde gedrag? Zo ja, dan volhouden. Zo nee, de verandering proberen in een andere vergadering met andere deelnemers of met een ander gedrag uit de tabel. Want misschien herkende je zelf niet meteen je echte grootste vergaderfout.

Versnellen of vertragen

Als voorzitter van een vergadering kun je deelnemers ook nog op een andere manier helpen. Stem voor de bijeenkomst met twee personen individueel af. Tegen persoon A zeg je de indruk te hebben dat de vergadering te snel gaat voor sommige participanten. Zij kunnen het niet bijhouden en hun toch belangrijke input en denkkracht wordt daardoor gemist. Aan persoon A daarom de vraag al het mogelijke in te zetten om de vergadering en besluitvorming te vertragen, zodat deze deelnemers mee kunnen komen. Tegen persoon B zeg je juist dat er klachten zijn van deelnemers dat de vergadering te langzaam gaat en zonde van de tijd, saai en vervelend is. Persoon B krijgt dus het verzoek (of de opdracht, afhankelijk van de organisatiecultuur) alles te doen om de vergadering te versnellen, bochten af te snijden en sneller tot beslissingen te komen. Na de vergadering spreek je beide personen over het bereikte resultaat en hun ervaringen. Een durfal doet dit in een driegesprek; licht dan wel aan het begin je goede bedoelingen met die twee tegenstrijdige opdrachten toe. Meestal zal blijken dat alle acties van persoon A en B precies het tegenovergestelde effect hebben gehad. Door het vooraf exact bepaalde doel en een grondige evaluatie ontstaan vele leermomenten voor jullie. Het effect is te vergroten door de A en B opdracht aan precies de juiste deelnemers te geven, namelijk aansluitend bij zijn/haar gebruikelijke rol als versneller of vertrager in eerdere vergaderingen. Of precies tegengesteld daaraan, want in beide richtingen kun je iets leren om het ongelijk van Dave Barry (zie citaat) aan te tonen.

Referenties

(1) Zealot = a person who is fanatical and uncompromising in pursuit of their religious, political, or other ideals.

(2) Cynic = a person who believes that people are motivated purely by self-interest rather than acting for honorable or unselfish reasons. Small Group Processes For Intelligence Analyse (unclassified report for Sherman Kent School CIA) - Richards Heuer jr., July 28, 2008. Tabel met 'disruptive group members' is volgens dit artikel gebaseerd op inmiddels verdwenen website van Phoenix Rising Coaching per August 14, 2007.

Auteurs: Puck van den Brink, Hanneke Duijnhoven, Ignas Melman, Bram Poppink en André Smulders zijn werkzaam bij TNO, unit Defensie en Veiligheid & unit ICT. Voor vragen is Puck van den Brink te bereiken via puck.vandenbrink@tno.nl.

ICT-supply chain risicomanagement: een veelzijdig vraagstuk

TNO doet onderzoek naar ICT-supply chain risicomanagement binnen de meerjarige onderzoeksagenda van het NCSC. Dit artikel is gebaseerd op een eerste verkenning in 2020 en gaat in op de complexiteit van het vraagstuk. Er worden vijf perspectieven beschreven om de risico's die samenhangen met ICT-supply chains beter te duiden. Deze eerste stap is een opmaat voor vervolgonderzoek naar het vergroten van het handelingsperspectief op dit thema voor overheid en bedrijfsleven.

Organisaties zijn voor de continuïteit en veiligheid van hun bedrijfsvoering in toenemende mate afhankelijk van een netwerk van ICT-aanbieders en -gebruikers, wat het aanvalsoppervlak voor cyberaanvallen met keteneffecten via derde partijen vergroot (1), (2), (3), (4). Naar schatting vindt zo'n 80% van de cyberaanvallen wereldwijd plaats via de supply chain (5). Bekende voorbeelden van ICT-supply chain incidenten zijn de ontdekte kwetsbaarheden in de systemen van Citrix (2019), waarbij een groot aantal organisaties wereldwijd – in Nederland naar schatting zo'n 3700 organisaties (6) – risico liepen om gehackt te worden en (vergaande) maatregelen moesten treffen. Ook het incident NotPetya (2018) zorgde ervoor dat via veelgebruikte administratiesoftware een wiperware zich kon verspreiden over een groot aantal organisaties wereldwijd (7). De LockerGoga ransomware aanvallen (2019) gericht op industriële controle systemen, hadden vergaande gevolgen op de logistieke en productieprocessen van de getroffen industriële organisaties (8). Deze gebeurtenissen zorgen voor steeds meer onzekerheid en zorgen over de risico's in de (digitale) supply chains en de weerbaarheid tegen deze risico's. In recente publicaties van onder andere de NCTV, de WRR, de Cyber Security Raad en het CBS wordt gewezen op de risico's die samenhangen met de steeds complexere, vaak grensoverschrijdende digitale supply chains waar wij als samenleving van afhankelijk zijn en de onzekerheid die heerst over de kennis en mate van grip die men heeft op deze risico's (6), (7), (9), (10), (11).

Omgaan met de verschillende typen risico's die voortkomen uit complexe digitale ketens vergt aandacht voor en begrip van verschillende aspecten en niveaus van de ICT-supply chain. Op basis van een verkenning naar bestaande ICT-supply chain risicomanagement methoden en gesprekken met verschillende grote organisaties onderscheiden we in dit artikel vooralsnog vijf perspectieven om naar ICT-supply chain risico's te kijken. We denken dat het onderscheiden van verschillende perspectieven kan helpen om meer grip te krijgen op ICT-supply chain risicomanagement, omdat het hanteren en bij elkaar brengen van meerdere perspectieven ervoor kan zorgen dat andere risico's of mogelijke aangrijpingspunten voor risicobeheersing in beeld komen.

Verschillende aspecten van de supply chain

Een supply chain is een systeem van organisaties, mensen, technologie, activiteiten, informatie en resources die nodig zijn om een product of dienst aan een eindgebruiker te leveren (1), (12). De verschillende aspecten in het supply chain 'systeem' bieden relevante invalshoeken om naar ICT-supply chain risico's te kijken. Met de vergaande digitalisering zijn dit in toenemende mate digitale aspecten. Een ICT-supply chain kan gaan om de productie van een ICT-product (bijvoorbeeld hardware, software of een informatiedienst), maar ook om de levering van producten of diensten die gerelateerd zijn aan deze ICT-producten, of die op basis van (de informatie uit) deze ICT-producten tot stand komen (12). Als je alleen al naar één organisatie kijkt is er dus niet zoiets als 'de' supply chain, maar is er sprake van vele verschillende ketens en relaties, waarbij de complexiteit wordt versterkt door de toenemende verwevenheid van fysieke en digitale aspecten (12). Als we grip willen krijgen op de kwetsbaarheden en risico's van de ICT-supply chains, is het dan ook van belang om naar al deze aspecten en relaties te kijken. Een eenzijdig perspectief kan er namelijk voor zorgen dat bepaalde risico's en kwetsbaarheden buiten beeld blijven of onderbelicht raken. Daarnaast is het ook van belang om naar de supply chain als geheel te kijken en de manier waarop deze samenhangt met andere supply chains op het niveau van de samenleving. Hierbij komen ook andere aspecten in beeld die van belang zijn voor het vergroten van de cybersecurity van supply chains, zoals wet- en regelgeving, het maatschappelijk belang van bepaalde supply chains voor de continuïteit van vitale processen en nationale veiligheidsvraagstukken. In dit artikel gaan we met name in op de supply chain zelf (de verschillende aspecten die een rol spelen bij het leveringsproces) om organisaties te helpen meer inzicht te krijgen in de risico's. Uiteindelijk zal dit ook aanknopingspunten bieden om op het niveau van de keten, het niveau van netwerken van ketens en de samenleving meer grip te krijgen op supply chain risico's.

Vijf perspectieven om naar ICT-supply chains te kijken

Wij zien ten minste vijf perspectieven op ICT-supply chains waarmee risico's gecategoriseerd kunnen worden. Het onderscheiden van deze perspectieven draagt bij aan het ontwikkelen van een integraal perspectief op supply chain risicomanagement omdat het de complexiteit van digitale ketens in kaart brengt. Hierdoor komen verschillende kwetsbaarheden en risico's in beeld en kunnen deze ook beter met elkaar in verband worden gezien. Hiermee ontstaan handvatten voor organisaties om hun (ICT) supply chain risicomanagement vorm te geven en aan te vullen.

1. Actorenperspectief

Wanneer men naar de ICT-supply chain kijkt vanuit het perspectief van actoren, kan men kijken naar het totaal aan organisaties (leveranciers, afnemers) dat betrokken is in een ICT-supply chain, om zo risico's in beeld te krijgen voor de continuïteit van het leveringsproces. Hierbij ligt de nadruk op het inzichtelijk krijgen in en afstemmen over de relaties tussen organisaties (afspraken tussen leverancier en afnemer, zicht op afhankelijkheden tussen verschillende leveranciers, etc.). De uitdaging hierbij is dat het afstemmen op het niveau van een keten alleen mogelijk is als de verschillende organisaties in die keten het belang daarvan voelen. Niet alle organisaties die bijdragen aan een supply chain zullen zichzelf nadrukkelijk zien als mede-eigenaar van het ketenbelang. Met name leveranciers die hun producten leveren aan heel veel verschillende partijen zullen het ketenbelang minder sterk voelen.

Een tweede manier om het actorenperspectief te hanteren is om vanuit één organisatie te kijken naar de verschillende ICT-toeleveringsketens waar de organisatie een rol in speelt (als afnemer, als leverancier, als dienstverlener, als toezichthouder, etc.). Voor elk van die rollen zal de organisatie op een andere manier maatregelen nemen. Als afnemer gaat het bijvoorbeeld om het maken van afspraken met de leveranciers (zoals SLAs). Als leverancier gaat het erom grip te krijgen op de risico's die tot gevolg kunnen hebben dat de organisatie haar afspraken met afnemers niet kan nakomen (13). Voor elke rol zijn andere aspecten van belang en komen er ook andere risico's in beeld. Een belangrijke uitdaging hier is om te prioriteren op welke ICT-supply chains men zich moet richten. De hoeveelheid aan ICT-supply chains waar één organisatie een rol in speelt is namelijk enorm. Het is dus vrijwel onmogelijk om alle ketens waar een organisatie een rol in speelt volledig in kaart te brengen. Om hier meer richting aan te geven kunnen ook de overige perspectieven een waardevolle rol spelen.

2. ICT-producten perspectief

Een andere manier om naar ICT-supply chain risico's te kijken is door te kijken vanuit de ICT-producten. Dit is het perspectief van hardware en software. Het gaat hierbij om de supply chains van ICT-producten variërend van een (relatief simpel) stuk software, zoals een telefoon, een autonoom functionerend voertuig of de automatische aansturing van operationele technologie (OT) voor vitale processen. In al deze producten komen verschillende systeemonderdelen samen vanuit verschillende leveranciers. Het kan zijn dat het product zelf (bijvoorbeeld in het geval van een softwarepakket) bij de afnemer weer wordt geïntegreerd of toegepast binnen een ander systeem. Bij het NotPetya incident (14) werd boekhoudsoftware vermoedelijk als aanvalsvector gebruikt om binnen te komen in een specifiek systeem. Maar omdat veel organisaties deze software gebruikten, werden zij meegesleept in een (geopolitiek) conflict waar ze niets mee te maken hadden. Deze organisaties namen een softwarepakket af van een leverancier zonder dat zij zicht hadden op de achterliggende leveranciers en de mogelijke risico's daarvan. Uit meerdere gesprekken komt naar voren dat het vaak een uitdaging is om inzicht en grip te krijgen op de keten van leveranciers achter een leverancier van een specifiek ICT-product. De vraag is dan ook in welke mate men zicht kan krijgen op wat er in de eigen organisatie aan ICT-producten wordt binnengehaald. Belangrijk hierbij is om zicht te hebben op de ICT-producten in de organisatie en de manier waarop zij bijdragen aan de bedrijfscontinuïteit van de organisatie. Welke producten zijn kritiek? Welke componenten horen er in het programma of systeem te zitten en wat zit er daadwerkelijk in?

3. Informatieperspectief

In het derde perspectief wordt vanuit de informatie naar een ICT-supply chain gekeken. In dit perspectief wordt gekeken naar welke informatiestromen en informatieproducten (die tot stand zijn gekomen door gebruik te maken van ICT-middelen) een rol spelen bij de toelevering van een product of dienst, of bij de ondersteuning van bedrijfsprocessen. Voorbeelden zijn de totstandkoming van rapportages van de kwaliteitscontroles die nodig zijn om de levering van een chemisch product te autoriseren, informatiestromen uit sensoren die van belang zijn bij de aansturing of controle van bepaalde OT, of het delen van klantgegevens met een bezorgdienst voor de levering van producten. Bij MAERSK werden veel systemen geraakt door de NotPetya wiperware, waardoor ook de informatievoorziening naar de klanten werd verstoord (15). Hierdoor werden ook organisaties geraakt die zelf niet geïnfecteerd waren omdat de informatie die zij voor hun processen nodig

Data is in toenemende mate niet meer in beheer van de eigen organisatie

hadden niet (volledig of tijdig) beschikbaar was. Een ander aspect van het informatieperspectief is de opslag en het gebruik van data. Data is in toenemende mate niet meer in beheer van de eigen organisatie, of meerdere organisaties maken gebruik van dezelfde data. Dit heeft als gevolg dat meerdere organisaties worden geraakt als zich een incident voordoet met deze data of de plek van opslag. Als bijvoorbeeld de patiënten data van een medisch laboratorium wordt gemanipuleerd, kunnen patiënten in ziekenhuizen vanwege onjuiste data de verkeerde behandeling krijgen (16). Hoe kan men achterhalen dat data is gemanipuleerd als deze data niet binnen de eigen organisatie wordt beheerd en hoe kan men hier op handelen? Door naar de belangrijke informatiestormen en producten te kijken.

4. ICT-diensten perspectief

In veel supply chains zullen ook ICT-diensten een rol spelen, niet alleen als onderdeel van het toeleveringsproces van een product of dienst, maar ook als eindproduct van een supply chain. ICT-diensten zijn diensten waar ICT-middelen voor nodig zijn om ze te kunnen gebruiken. Voorbeelden zijn telecomdiensten, clouddiensten of het leveren van remote onderhoud op systemen. Een voorbeeld van een supply chain incident waarbij ICT-diensten een grote rol speelden, is de DDoS aanval op de DNS provider Dyn in 2016 (17). Door de aanval op Dyn was voor een groot deel van Noord-Amerika de toegang tot het internet gedurende bijna een hele dag verstoord en veel verschillende diensten en platformen, zoals Spotify, waren daardoor niet beschikbaar. Binnen dit ICT-diensten perspectief is het feit dat heel veel organisaties afhankelijk zijn van een beperkt aantal grote ICT-dienstleveranciers een belangrijke uitdaging. Deze uitdaging geldt met name voor organisaties die van ICT-diensten afhankelijk zijn om hun bijdrage aan vitale processen te waarborgen. Denk aan de afhankelijkheid van een internet- of telecommunicatieleverancier of een leverancier van cloudopslag.

5. Productiemiddelen perspectief

Ten slotte spelen ook andere (niet-ICT-)producten of diensten een rol in ICT-supply chains die afhankelijk zijn van ICT-middelen. De bedrijfsprocessen waar deze productiemiddelen een rol in spelen hebben niet een directe koppeling met ICT-middelen, maar worden wel geleverd of aangestuurd met behulp van ICT-middelen. Denk aan een logistiek proces waarbij het transport zelf niet geautomatiseerd is, maar waarbij wel de logistieke planning met behulp van een ICT-middel wordt uitgevoerd. Om grip te krijgen op ICT-supply chain risico's is dit perspectief, samen met het informatieproducten perspectief, extra interessant omdat dit een blinde vlek kan zijn bij het identificeren van ICT-risico's, het gaat immers om risico's die niet direct gerelateerd zijn aan ICT. Het incident NotPetya en de verstoringen bij MAERSK laten zien dat het transport van fysieke goederen van andere organisaties ook stil kwam te liggen, terwijl de logistieke processen van deze organisaties in veel gevallen op geen enkele manier verbonden waren met de ICT-systemen van MAERSK (14). In dit perspectief ligt de nadruk op het in kaart brengen van producten en diensten waar bedrijfsprocessen van afhankelijk zijn en hoe die vervolgens afhankelijk zijn van andere (al dan niet ICT-) producten en diensten. Het zorgt ervoor dat niet uitsluitend naar ICT-afhankelijkheden wordt gekeken, waardoor bepaalde risico's buiten beeld zouden blijven.

Conclusie

Voor organisaties bieden de voorgaande perspectieven een bredere, meer integrale blik op ICT-supply chain risico's. Ze laten zien dat de veelzijdigheid van ICT-supply chains vraagt om een bredere blik waarmee risico's vanuit alle perspectieven inzichtelijk gemaakt kunnen worden en met elkaar gerelateerd kunnen worden. Dit inzicht kan ook aanknopingspunten bieden om bestaande ICT-supply chain risicomanagement aanpakken te versterken. Er zijn nog andere perspectieven denkbaar. Bijvoorbeeld het perspectief van de mens in ICT-supply chains (afhanke-

lijkheid van de mens (goed gebruik) of om te laten zien dat de ICT-supply chain tot daar doorloopt) of perspectieven op de manier waarop processen zijn ingericht en afgestemd in een supply chain (just-in time principes, tijdsdimensies van afhankelijkheden, redundantie die aanwezig is). Voor nu denken wij dat deze vijf een goed startpunt zijn om op een meer integrale manier naar ICT-supply chain risicomanagement te kijken. Ons onderzoek richt zich de komende tijd op het verder uitwerken van deze perspectieven en op het analyseren van supply chain risicomanagement aanpakken vanuit deze perspectieven. Het doel is om bij te dragen aan het ontwikkelen van handelingsperspectief voor het beter beheersen van ICT-supply chain risico's. Wij gaan hiervoor graag in gesprek met geïnteresseerden vanuit de overheid, het bedrijfsleven en andere onderzoeksinstituten. Daarbij dagen wij alle organisaties uit om de perspectieven die in dit artikel staan geschetst te gebruiken en om te kijken op welke punten dit een mogelijke aanvulling biedt op de huidige supply chain risicomanagement of bedrijfscontinuïteitsmanagement processen.

Referenties

(1) ENISA (2015). Supply Chain Integrity: An overview of the ICT-supply chain risks and challenges, and vision for the way forward. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/publications/sci-2015

(2) AON (2019). Cyber Perils in a Growing Market. White paper. https://www.aon.com/unitedkingdom/insights/cyber-perils-in-a-growing-market.jsp

(3) Soare, B. (2020). Supply Chain Cyber Security: What are the Risks? Heimdal Security. https://heimdalsecurity.com/blog/supply-chain-cyber-security/

(4) Ghadge, A., Weiß, M., Caldwell, N.D. & Wilding, R. (2019). Managing cyber risk in supply chains: a review and research agenda. Supply Chain Management, Vol. 25 No. 2, pp. 223-240. https://doi.org/10.1108/SCM-10-2018-0357

(5) Boyens, J. (2016) in Bailey, D. (2018). Lumberjacks and Supply Chain Cybersecurity: Take Time to Prepare. Blogrige, The Offiial Baldrige Blog. https://www.nist.gov/blogs/blogrige/lumberjacks-and-supply-chain-cybersecurity-take-time-prepare

(6) NCTV (2020). Cybersecurity Beeld Nederland (CSBN) 2020. Den Haag: Ministerie van Justitie en Veiligheid. https://www.rijksoverheid.nl/documenten/rapporten/2020/06/29/tk-bijlage-2-cybersecuritybeeld-nederland-csbn-2020

(7) NCTV (2019). Cybersecurity Beeld Nederland (CSBN) 2019. Den Haag: Ministerie van Justitie en Veiligheid. https://www.rijksoverheid.nl/documenten/rapporten/2019/06/12/tk-bijlage-cybersecuritybeeld-nederland-csbn-2019

(8) Reich, J. (2020) Nearly 300 cybersecurity incidents impacted supply chain entities in 2019. TechRepublic. https://www.techrepublic.com/article/nearly-300-cybersecurity-incidents-impacted-supply-chain-entities-in-2019

(9) Wetenschappelijke Raad voor het Regeringsbeleid (2019). Voorbereiden op digitale ontwrichting. Den Haag. https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

(10) Cyber Security Raad (2016). Digitale ketenveiligheid krijgt veel te weinig aandacht. https://www.cybersecurityraad.nl/010_Actueel/digitale-ketenveiligheid-krijgt-veel-te-weinig-aandacht.aspx

(11) CBS (2018). Cybersecuritymonitor 2018. Een verkenning van dreigingen, incidenten en maatregelen. Den Haag: CBS. https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018

(12) Van Ruijven, T. & Keijser, B. (2017). Ketenweerbaarheid tegen cyberdreigingen. Whitepaper. Den Haag: TNO. https://www.tno.nl/nl/aandachtsgebieden/defensie-veiligheid/roadmaps/nationale-veiligheid/cybersecurity-het-belang-van-integrale-oplossingen/cybersecurity-ketens-en-processen-in-beeld/whitepaper-ketenweerbaarheid-tegen-cyberdreigingen/

(13) Joosten, H.J.M. & Smulders, A. (2014). Networked Risk Management: How to Sucessfully Manage Risks in Hyperconnected Value Networks. Delft: TNO.

(14) Crosignani, M., Macchiavelli, M. & Silva, A.F. (2020). Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains. Federal Reserve Bank of New York Staff Reports, no. 937. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr937.pdf

(15) Greenberg, A. (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

(16) University of California - San Diego. (2018). How unsecured medical record systems and medical devices put patient lives at risk. ScienceDaily. https://www.sciencedaily.com/releases/2018/08/180829115554.html

(17) Johnson, K. (2019). What is digital supply chain management? Bitsight. https://www.bitsight.com/blog/what-is-digital-supply-chain-management#:~:text=The%20second%20definition%20%E2%80%94%20that%20the,coined%20in%20a%202001%20paper

Goed voorbeeld...

Recent werd in onze organisatie een mailtje rondgestuurd met de vraag of iedereen de e-learning over informatiebeveiliging wilde maken. Ik had het mailtje netjes doorgelezen en ik dacht nog: Fijn dat er aandacht voor ons onderwerp is!
Een aantal weken later kwam een reminder. Mooi, mijn collega's zitten er kort op! En toen kreeg ik een mailtje van mijn directe collega: "Hey Inge, ik zie in het systeem dat jij de e-learning nog steeds niet hebt gemaakt. Misschien toch handig als je dat wel even doet, zodat we in ieder geval kunnen laten zien dat ons team zelf ook netjes de procedure volgt."

Wow. Ik was dus in staat om mailtjes gericht aan iedereen te negeren alsof ze niet voor mij bedoeld zijn. Alsof ik niet onder 'iedereen' val! Daar had ik laatst nog een uitgesproken mening over gehad. Voor een grote organisatie werd een programma uitgerold met als één van de onderdelen een e-learning en test over privacy en informatiebeveiliging. Het programma werd breed gedragen door het MT en zelfs de e-mail over de e-learning was vanuit het management gekomen. Wat hadden ze vervolgens zelf gedaan? Tijdens een vergadering al hun laptops open naast elkaar gezet zodat de secretaresse even voor het hele MT tegelijk de test kon voltooien.
They whát?!

Maar wacht eens even. Eerst ben ik verbaasd dat managers het logisch vinden dat de regel niet voor hen geldt en vervolgens doe ik precies hetzelfde. Zo werkt dat dus in ons brein! We kennen de regels wel, maar we kunnen vrij gemakkelijk een argument vinden waarom deze regel niet voor onszelf geldt. Of waarom we ons er voor deze ene keer even niet aan houden. Kijk eens even om je heen (of naar jezelf) als het gaat over de COVID-19 maatregelen; wij zijn echt heel goed in beargumenteren waarom wij zelf wél onze verjaardag mogen vieren, op reis mogen of naar het werk. Die nuance zien we namelijk veel beter voor onszelf dan voor anderen. Dat is menselijk ….

Voor de meeste medewerkers van organisaties is informatiebeveiliging namelijk niet hun core business. Die hebben dus andere prioriteiten en verantwoordelijkheden, en daarmee waarschijnlijk ook weer andere argumenten waarom zij de e-learning nu even niet gaan doen. Dus! Laten we beginnen met het juiste voorbeeldgedrag. Ook al denken we de antwoorden vooraf al te weten. Laat de afdelingen security en IT en het management 100% scoren op het voltooien! Voorbeeldgedrag, zo belangrijk!

Dus daar zat ik dezelfde middag, braaf gehoor te geven aan de oproep om de e-learning te maken. De oproep aan iedereen geldt namelijk ook voor mij. En jou. Voorbeeldgedrag …. Misschien wel een mooi onderwerp voor een volgende e-learning.

Inge

Auteur: Inge Wetzer is sociaal psycholoog cybersecurity & compliance. Zij werkt bij Secura, waar zij zich druk maakt over het menselijk gedrag in (cyber)security, en hoe dat te verbeteren. Inge is bereikbaar via inge@secura.com.

Auteurs: Ilan Sosnovitch is Global Sales Manager, SIGA OT Solutions (https://sigasec.com/), partner van Aexus. Frank van der Meulen is bereikbaar via frank@aexus-europe.com

Een paradigmaverschuiving in de detectie van cyberdreigingen bij machines en apparatuur in operationele en ICS-omgevingen

De onbetwistbare waarde van LEVEL 0 - elektrische signalen liegen niet

Zonder afbreuk te doen aan het belang van netwerkmonitoring bij bescherming van industrial control systems (ICS) in operational technology (OT) omgevingen, is het essentieel om het belang in te zien van monitoring en detectie van veld- en procesgeoriënteerde afwijkingen op Level 0: de sensoren en actuatoren op apparatuur- en machineniveau. Alleen zo ben je in staat om een OT-systeem holistisch te beschermen.

De term Level 0 is een onderdeel van de purdue enterprise reference architecture (PERA). Dit model beschrijft in een hiërarchische structuur de lagen die van toepassing zijn op procesautomatisering. Het model bevat zes niveaus. Bovenaan op Level 5 bevindt zich de internet DMZ. Level 4 is het bedrijfsnetwerk van de organisatie. Level 3 is de productiezone of het hoofdcontrolecentrum, dat communiceert met human-machine-interface (HMI)-controlepunten op Level 2. Deze HMI's communiceren met Level 1-controllers en Level 0-veldapparatuur. Vanuit cyberperspectief bevatten de Levels 1 tot en met 5 traditionele IT-cyberoplossingen, bestaande uit servers, werkstations, switches, routers en firewalls. Op Level 0 is de omgeving echter significant anders. Controllers (PLCs) dicteren de fysieke ruimte en communiceren met apparatuur door middel van stroom- en voltagesignalen. Daarom moet cybersecurity op Level 0 heel anders worden aangepakt.

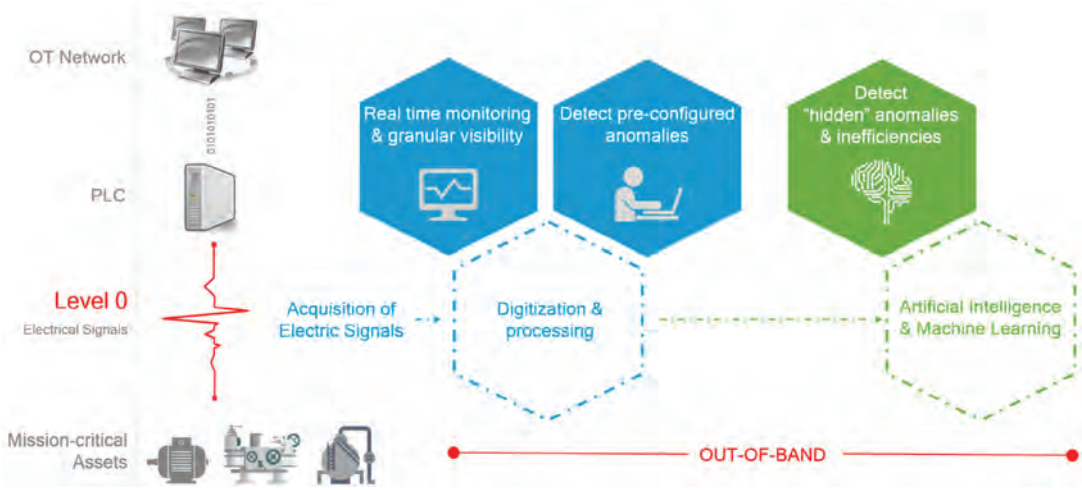
Kwetsbaarheid OT-infrastructuren

Het monitoren van de elektrische signalen, die direct vanaf de kritieke assets worden verzonden, is een zeer waardevolle en betrouwbare manier om kwaadwillende cyberaanvallen op operationele machines en apparatuur te detecteren. In tegenstelling tot intrusion detection solutions op netwerkniveau, die vaak afgeschermd zijn van het eigenlijke proces, kan monitoring en diagnose van ongefilterde en niet te hacken elektrische signalen op Level 0 leiden tot waterdichte bescherming van bedrijfskritieke operationele assets.

Veel cyberaanvallen, zoals Stuxnet, Irongate en de meest recente cyberaanvallen op watervoorzieningen, onderstrepen de kwetsbaarheid van OT-infrastructuren wereldwijd. Omdat monitoring van Level 0 volledig losstaat van het Level 1 netwerk, zorgt dit voor operationele weerbaarheid. Zelfs wanneer cyberaanvallen erin slagen om de logica van ICS controllers te manipuleren. Het belang van Level 0-monitoring is al gevalideerd en weergegeven in recente regelgevende richtlijnen voor kritieke infrastructuur, en door vooroplopende experts en opiniemakers wereldwijd.

OT- versus IT-beveiliging

Control systems maken gebruik van commerciële 'off-the-shelf' human-machine interfaces met communicatienetwerken en daarnaast veldapparatuur (processensoren, actuatoren en aandrijvingen) met hun veldniveau-netwerken. Oorspronkelijk kent cybersecurity in OT-omgevingen een top-downbenadering. Eerst worden digitale muren rond de digitale assets gebouwd, gevolgd door identificatie van malware en netwerkafwijkingen in de IP-netwerken. Dit komt doordat voor IT-afdelingen de beveiliging van procesapparatuur ophoudt bij de netwerklaag. De IT-benadering is uitgebreid om ook control systems te beveiligen, door het monitoren van operational technology (OT) control system ethernet netwerken. Deze benadering is noodzakelijk, maar niet volledig toereikend om control systems veilig te maken en ernstige schade aan OT-apparatuur en machines te voorkomen. Netwerkbeveiliging gaat namelijk nooit in staat zijn om de echte



Aanval op Israëlische watervoorzieningen
Eind april 2020 onderstreepte een Stuxnet-achtige aanval op de Israëlische watervoorzieningen het vitale belang van Level 0-monitoring. Klaarblijkelijk was het doel om het chloorgehalte in de watervoorziening te verhogen door de logica van de PLC te veranderen zonder alarmen te laten afgaan. "… Ze probeerden de chloorniveaus te manipuleren en op hetzelfde moment beheerders een signaal te sturen dat de chloorniveaus naar behoren waren," aldus cybersecurity experts (2). Deze cyberaanvallen markeren de kwetsbaarheid van de water- en energie-infrastructuur wereldwijd.

assets van de OT-architectuur volledig af te schermen: de fysieke apparatuur en processen, of in andere woorden, Level 0-apparatuur. Cybersecurity detectiesystemen voor netwerkafwijkingen gaan ervan uit dat processensoren veilige, geauthentiseerde input bieden. Echter, deze apparaten of apparaat-netwerken kennen geen beveiliging of authenticatie. Sterker nog, verouderde control system apparatuur heeft geen opties voor beveiliging of authenticatie, en toont ook niet welke specifieke control system apparatuur (zoals pompen, ventielen, motoren en relais) kwetsbaar zijn voor netwerkaanvallen. Daardoor kan de IT/OT-benadering geen betrouwbaarheid, weerbaarheid of veiligheidsoverwegingen ondersteunen, noch het systeem dat de control systems vormt veilig maken. Een hardnekkig probleem.

Wie is verantwoordelijk?

Het beschermen van control systems zou gebaseerd moeten zijn op de engineeringprioriteiten veiligheid voor mens & apparatuur en betrouwbaarheid, gevolgd door cybersecurity – daar waar een cyberincident invloed kan hebben op veiligheid en betrouwbaarheid. Verouderde processensoren (zoals druk, niveau, flow, temperatuur, voltage, stroom, enzovoort) zijn mechanische en/of elektrische apparaten die beschikken over faalmodi, maar niet over beveiliging of authenticatie. Voorbeelden waarbij sensoren bijdroegen aan catastrofaal falen zijn onder meer het kernongeval van Three Mile Island, een explosie op de raffinaderij in Texas City, en de tankparkexplosie in Buncefield, in Groot-Brittannië. Grote apparatuur, zoals generatoren, motoren, pompen en relais bevatten 'do not operate' zones die voor beschermingsdoeleinden gebouwd zijn, maar tevens voor catastrofale schade kunnen zorgen. Zo werd de Aurora vulnerability bijvoorbeeld ingezet om apparatuur onjuist te laten werken in deze 'do not operate' zones, wat leidde tot catastrofaal falen, zonder digitale sporen. Uit onderzoek blijkt dat de Aurora vulnerability een netwerk voor een heel lange periode (vele maanden) kan platleggen door kritieke apparatuur te beschadigen (3).
Het realtime monitoren van elektrische eigenschappen van processensoren gaat volledig om de detectie van procesafwijkingen, in plaats van detectie van netwerkafwijkingen. Procesafwijkingen kunnen om allerlei redenen voorkomen, inclusief cyberdreigingen. Als de sensoren die de daadwerkelijke situatie weergeven niet overeenkomen met het netwerk, is het netwerk verdacht. Van cybersecurity ook een engineeringprobleem maken kan voordelen bieden. Een hardnekkig netwerkprobleem wordt oplosbaar, je voorkomt een langdurige schade, verbetert de veiligheid en betrouwbaarheid en je kunt sneller de impact van mogelijke bedreigingen uit apparatuur zelf identificeren. Sensormonitoring kan bovendien helpen de culturele kloof tussen engineering- en beveiligingsorganisaties te overbruggen. Control systems kunnen niet beveiligd worden zonder deze kloof te overbruggen.

Focus OT-engineer vs control system-engineer

Er is een groot verschil tussen hoe OT-engineers naar cybersecurity van

Kritieke infrastructuur security showdown (CISS)
Augustus 2019, Singapore, realtime veldtest van OT-cybersecurity-detectie-tools. Het volledige rapport is recent gepubliceerd (1) en uit de resultaten blijkt dat een Cyber Intrusion Detection Systeem dat op Level 0 monitorde het hoogste scoorde op het gebied van detectie van cyberaanval-afwijkingen in relatie tot het OT-proces. De resultaten laten duidelijk zien dat monitoring van elektrische signalen op Level 0 cruciaal is voor elk cybersecurity-beschermingsplatform in industriële omgevingen. Er zijn veel incidenten, met zowel analoge als digitale sensoren, waarbij onnauwkeurige sensoren voor catastrofaal falen hebben gezorgd. Er is tenminste één incident waarbij een sensor kwaadwillend werd gehackt en het systeem als gevolg daarvan niet meer functioneerde.

control systems kijken en hoe control system-engineers dat doen. Voor control system engineers draait alles om de beveiliging van het netwerk, niet de daadwerkelijke impact op systemen. Wanneer ze malware of netwerkafwijkingen vinden, kunnen ze deze niet direct relateren aan specifieke veldapparatuur, zoals pompen, ventielen, motoren, relais, etc. Wanneer je mij, als OT-engineer, niet kunt uitleggen welke specifieke apparatuur getroffen kan worden en hoe, wat heb ik er dan aan? Bij OT-engineers ligt de focus juist op het proces. Werkt dit zoals ontworpen en treedt er slijtage van de apparatuur op, ongeacht of dat kwaadwillend of onbedoeld is? Verreweg de meeste control system incidenten zijn niet cyber gerelateerd (of tenminste niet identificeerbaar als zijnde cyber) maar het is nog steeds belangrijk om de staat van het proces te weten. Wil OT van waarde zijn voor engineers, dan moet netwerk cybersecurity helpen met deze problemen. De vraag is echter hoe vereisten voor veiligheid en betrouwbaarheid worden beïnvloed door een gebrek aan cybersecurity van processensoren, actuatoren en aandrijvingen. Als je de metingen niet kunt vertrouwen, heb je een probleem. Sensoren, actuatoren en aandrijvingen zijn engineering systemen, geen netwerkapparaten. Ze moeten voldoen aan operationele en designvereisten om processen veilig en betrouwbaar te laten zijn. Cybersecurity is slechts één 'bedreiging' in het voldoen aan design- en operationele vereisten van sensoren.

Het begint allemaal met Level 0

Op dit moment bestaan er geen cybersecurityvereisten voor processensoren, actuatoren en aandrijvingen. Maar zelfs als deze er zouden zijn, lost dat nog steeds niet het probleem op dat een getroffen PLC (of elke andere net entiteit) verkeerde of gemaskeerde informatie heeft, ongeacht welke maatregelen op het gebied van authenticatie of beveiliging zijn getroffen. Deze apparaten hebben een aantal zwakten: de sensoren zelf, de sensornetwerken en de serial-to-ethernet convertors (gateways). Bestaande processensoren zijn mogelijk niet in staat om zelfs minimale cybersecurity te ondersteunen. Als de sensoren zijn gecompromitteerd (wanneer de sensorwaarden of -instellingen 'incorrect' zijn, door onbedoelde of kwaadwillende oorzaak) voordat de gateways de data converteren naar ethernetpakketjes, hebben de PLC en HMI's niet in de gaten dat de sensorwaarden en -instellingen gecompromitteerd zijn. Er zijn een aantal manieren om sensoren elektronisch te compromitteren. De gevolgen daarvan lopen uiteen van een denial-of-service, tot het effectief verwijderen van beveiligingssystemen door manipulatie van sensor-instelpunten. Er vindt momenteel geen cybersecurityonderzoek plaats van de processensor vóór de elektrische signalen ethernet-pakketjes worden. Daardoor is het ook niet duidelijk of een sensor getroffen is met onbedoelde of kwaadwillende redenen. Voor een engineer maakt dat echter niet uit.

Bruikbare inzichten van Level 0

We moeten serieus anders gaan denken over het monitoren van de veiligheid van ICS. Het monitoren van Level 0 combineert cybersecurity en operationele methodologieën, om unieke detectie van elk noemenswaardig procesevent te bieden. Een detectiesysteem voor procesafwijkingen, dat kritieke assets monitort door middel van elektrische signaal gebaseerde geavanceerde analytics, kunstmatige intelligentie en machine learning, als aanvullende en synergetische cyberdetectielaag. In elk end-to-end cyber Intrusion Detection System (IDS) in OT-omgevingen zou dit moeten worden overwogen. Daar waar de aansturing van de elektrische signalen kan worden gehackt of gemanipuleerd, geven de signalen zelf altijd de absolute waarheid weer. Daardoor bieden ze een rijkdom aan informatie om te kunnen zorgen voor operationele betrouwbaarheid, procesoptimalisatie en cyberbeveiliging. Focussen op elektrische signalen, vóór ze zijn geconverteerd naar datapakketjes en zijn gefilterd door de PLC, is vermoedelijk de meest effectieve techniek voor het nauwkeurig identificeren van een operationele afwijkingen, ongeacht de oorzaak.

Monitoring van elektrische signalen op Level 0 gebeurt volledig out-of-band, los van het OT-netwerk en werkt onafhankelijk van het ICS/SCADA-systeem. Dit maakt het de meest veilige en betrouwbare oplossing om afwijkingen te detecteren.

Referenties

(1) https://itrust.sutd.edu.sg/ciss-2019/
(2) https://www.haaretz.com/israel-news/iranian-cyberattack-aimed-to-raise-chlorine-level-in-israeli-water-report-says-1.8886235
https://www.israeldefense.co.il/en/node/43311
www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/
https://www.ynetnews.com/article/H1pA5mM2L
(3) https://blog.trendmicro.com/the-aurora-power-grid-vulnerability-and-the-blackenergy-trojan/
https://www.controlglobal.com/blogs/unfettered/the-aurora-vulnerability-still-being-shunned-by-the-electric-industry-where-is-the-education/

DIGIVAARDIGE OUDEREN

Het jaar is al weer bijna om. Het lijkt wel of het jaar is omgevlogen ondanks de voor mij saaie tijd van de COVID-19 pandemie. Er waren wel heel veel webinars en Zoom/MS Teams meetings. Het werkt allemaal wel, maar ik heb persoonlijk toch liever fysieke bijeenkomsten.

Voor de redactie was de impact van de pandemie minder, omdat de redactievergaderingen toch al telefonisch waren. Daarnaast hebben we een jaarlijkse fysieke vergadering om elkaar te zien en te spreken. Die ging dit jaar helaas niet door.

Ik ben gevraagd om ambassadeur te worden van SeniorWeb. Tot voor kort was ik niet bekend met deze vereniging. Zij helpen ouderen wegwijs (digivaardig) te maken in de IT via cursussen, workshops, spreekuren voor (pc-)hulp (ook wel Computer Cafés genoemd), hulp aan huis of op afstand (via Teamviewer).
Ben ik gevraagd mede vanwege mijn leeftijd? Ik hoop van niet, maar laten we aannemen vanwege mijn ervaring en ook omdat ik mij bezighoud met informatiebeveiliging. Aan dat laatste is voor mijn gevoel binnen de seniorengemeenschap nog heel veel te doen.
We zien dat ouderen veelvuldig door criminelen worden belaagd met phishing, babbeltrucs en de laatste weken met spoofing, waarbij criminelen vaak grote bedragen wegsluizen. Blijkbaar een makkelijk doelwit. Ja, ook is er bij SeniorWeb wel aandacht voor informatiebeveiliging door voorlichting te geven en cursussen aan te bieden.
Cursussen, workshops en hulp op de spreekuren worden voornamelijk georganiseerd op locaties zoals bibliotheken, buurthuizen, verzorgingshuizen e.d. maar zijn in deze coronatijd niet altijd mogelijk. Daarom is er voor kennisdeling en voorlichting overgegaan op MS Teams, Zoom en webinars. Pc-hulp uitsluitend op afstand. Deze wijze van online communiceren is binnen deze doelgroep een zeer grote uitdaging qua (digi)vaardigheid en ik denk dat er waarschijnlijk daarom veel leden afhaken. In mijn regio zie je dan ook dat er voor hulp vrijwel geen verzoeken meer binnenkomen. Een bijkomend punt is de sociale functie van de spreekuren. Even bijpraten met een kopje koffie. Door het wegvallen daarvan 'vereenzamen' veel ouderen zo nog meer.
Als PvIB leggen we vooral de focus op organisaties, omdat het overgrote deel van onze leden daar werkzaam is. Daarnaast besteden we veel aandacht aan het onderwijs. We hebben wel vaker in het bestuur gediscussieerd wat ons doel is, onze maatschappelijke rol. Daar kwam uit: 'Nederland veiliger maken'. Dat kun je breed zien; dus wat mij betreft naast organisaties ook individuen. De samenleving dus. Vooral jongeren en ouderen zijn kwetsbaar. Jongeren omdat zij zich vaak minder bewust zijn van de privacyrisico's en ouderen omdat zij goedgeloviger zijn en mensen vaker vertrouwen of juist angstig zijn door alle nare berichtgevingen. Wellicht kunnen we verenigingen zoals SeniorWeb ook inhoudelijk bijstaan?

Deze maand ben ik benaderd door SeniorWeb of ik mee wil helpen bij de geplande themamaand 'Veiligheid & Privacy' in maart 2021. Uiteraard heb ik 'ja' gezegd.
Privacybewustzijn bij ouderen doet me denken, heel lang geleden, aan mijn destijds 90-jarige grootvader in het bejaardentehuis. Hij was in paniek omdat mijn vader zijn cash(!) AOW-uitkering natelde (ja, dat was toen), terwijl de tv aanstond. 'Die meneer op de tv kan ook meekijken!', riep hij. Hij was op zijn eigen manier 'aware'. Hij dacht 45 jaar geleden al aan smart tv's!

Zijn er (oudere) PvIB leden die toevallig ook lid en/of ambassadeur zijn van SeniorWeb? Laat het me weten.

Tom Bakker

Auteur: Dré Lameir is CISO en CTO bij Enovation Group en is bereikbaar via linkedin.com/in/lameir/

FOMI (Fear Of Missing Intel)

En zij dan?

We zijn best streng voor onszelf hier in huis. Vrienden en familie, we houden ze op afstand. Ook de kinderen nemen we mee in deze hygiënische pandemieroutine, want dat is het inmiddels gek genoeg, routine. Dat blijkt maar weer eens wanneer ik met de jongste (net 9) een fors rondje door de bossen aan het fietsen ben. Bijna terug bij huis zien we een groepje opgeschoten gasten langs fietsen. Vijf vrienden, dollend, duwend en trekkend alsof er geen COVID-19 probleem is.

"NOU!"

Zegt mijn knul best wel hardop.

"Ze zijn met 5! Da's 3 te veel en het zijn echt helemaal niet allemaal broers hoor!"

"En die wonen helemaal niet in hetzelfde huis denk ik pap."

En, na wat meters doorfietsen…

"Zo krijgen we straks allemaal corona!"

Ik moet lachen om zijn serieuze en strenge opmerkingen. Maar tegelijkertijd proef ik ook wel zijn jaloezie. Hij mist het kroelen, boksen en voetballen met opa en stoeien met al zijn vriendjes is er ook niet bij. Niet iedereen houdt zich aan de 'regels' en hij heeft heus wel door dat enkele klasgenootjes meer 'geluk' hebben thuis. Uit het schaarse contact blijkt dat sommigen ervoor kiezen om nog wel samen te komen en dus lol te hebben. Hij heeft het gevoel iets mis te lopen. Anderen hebben lol en hij niet.

Typisch FOMO, Fear Of Missing Out. Daar heeft hij last van!

De definitie op Wikipedia zegt het volgende:
FOMO refers to the apprehension that one is either not in-the-know or is out of touch with social events, experiences, and interactions. People who grapple with it may not know exactly what they are missing but can still fear that others are having a much better time or doing something better than they are, without them. FOMO could result from not knowing about a conversation, missing a TV show, not attending a wedding or party, or hearing that others have discovered a new restaurant.

'Hoe zit dat met mij?', denk ik ineens. We hebben normaal gezien best een druk sociaal leven en ik ervaar het 'tandje' minder in deze periode als een zege. Maar ik voel wel een bepaalde onrust, niet privé maar op het werk.

Bubbel

Vroeger waren mensen ook al jaloers op elkaar hoor, maar de opkomst van social media heeft het echt enorm versterkt. Want 24/7 hebben we toegang tot wat de ander doet, kan, koopt of meemaakt. Het gevoel iets te missen wordt daardoor enorm versterkt. Maar is wel heel afhankelijk van de filter waardoor je die informatie tot je neemt. De 'bubbel' waarin je zit.

Qua werk zit ik nu ook gedwongen in een bubbel. Ga maar na:

- alle contact is via een scherm, ik ervaar dat alles letterlijk vervlakt, je mist veel;
- ik spreek mijn collega's via Microsoft Teams en heb geen zicht op hun omgeving;
- soms hebben ze grappige achtergronden of alles is wazig gemaakt;
- het is moeilijker iemands emotie te lezen. Het blijkt dat sommige mensen stiller of juist feller zijn via een videoverbinding;
- de kanalen op dit moment zijn: e-mail, chat, telefoon en video;
- door de strakke opeenvolging van gesprekken is er NUL ruimte voor andere zaken of rustig evalueren.

Bovenop dat alles, is het niet zeker dat de manier waarop we nu met elkaar communiceren passend is voor wat je wilt overbrengen. Videobellen is niet altijd oké, soms is gewoon een telefoontje zonder beeld of juist elkaar op gepaste afstand in het echt zien beter.

Wat mis ik dan? Ik mis vooral:

- context
- alerts
- serendipity

Context

Als iemand me aanspreekt via de camera over een situatie, zeg een security incident, dan wil je ook kijken naar de houding, lichaamstaal. Dat gaat slecht. Vaak bespreek je dit met meerdere betrokkenen zodat je verschillende invalshoeken meekrijgt. Juist de groepsdynamiek of de omgeving spelen dan een grote rol. In een videogesprek met 9 'platte' collega's, die vaak ook nog afgeleid zijn door meerdere kanalen, verlies je context.

Alerts

Het oude spreekwoord luidt: 'Geen nieuws is goed nieuws.' In normale tijden voelen security officers dit al anders, laat staan nu. Het uitblijven van slecht nieuws wil immers niet zeggen dat er niets fout gaat. Met je beperkte blik op de remote organisatie, is het helemaal erg. Nogmaals FOMO: "... People who grapple with it may not know exactly what they are missing ...". Ik moet echt zelf op zoek naar alerts, triggers en informatie, collega's gaan videobellen!

Serendipity

En dan is er, wat de Engelsen zo mooi noemen, serendipity. Oftewel, het onverwachte of de toevalligheid. Als ik op kantoor rondloop, dan zie ik die open deur, een rondslingerend rapport, de niet afgesloten laptop. Tijdens een rondje vang ik gesprekken op tussen collega's over een storing, een gek mailtje, downtime door werkzaamheden, phishing. Natuurlijk worden zaken gemeld via de beschikbare kanalen, maar toch. Je bent gewoon eenvoudiger te benaderen bij de koffiemachine dan wanneer iemand ergens een tijdslot moet prikken in de overvolle Teams-agenda. Net zoals thuis wordt je wereldje kleiner en spreek ik alleen de collega's waar op dat moment overleg gepland staat of waarmee ik werkzaamheden heb. Een beperkte gefilterde blik op de organisatie dus.

Alles bij elkaar mis ik actuele nuttige informatie over de stand van zaken op kantoor en over onze dienstverlening.

"I need more intel people!"

intel noun
in·tel | \ 'in-ˌtel\
Definition of intel: useful information concerning a subject of interest (such as an enemy).
Tijdens de koude oorlog, als je geen zicht hebt op de activiteiten van de vijand. Als je niet achter het ijzeren gordijn kan kijken. Juist dan heb je intel nodig. En natuurlijk is die intel er wel, maar krijg ik het niet voldoende of erger nog .... Misschien is het er niet en vrees ik niet voldoende te krijgen. Geen nieuws is goed nieuws toch?

Vandaar mijn FOMI, Fear Of Missing Intel.

En dan?
Nu heb ik natuurlijk twee opties:

Optie 1: Anxiety

Onrustig worden, eindeloos scrollen door mijn mail en de overige kanalen, contact zoeken met alle thuiswerkende collega's, nieuws doorspitten, NCSC volgen, alerts instellen op allerlei logging, extra pentesten laten doen, awareness verhogen, iedereen stalken, enzovoort. Kortom toegeven aan mijn eigen FOMI.

Optie 2: Trust

Of ... erop vertrouwen dat ten tijde van een pandemie iedereen gewoon zijn werk blijft doen. Vertrouw op je genomen maatregelen. Vertrouw erop dat iedereen ook de thuiswerkplek veilig behandelt. Geniet van je tijdelijke filter, straks komt de overkill aan 'intel' weer terug. Misschien ... effe checken? Het is tenslotte 'Trust but verify' toch?

Ik heb nog niet gekozen ... u wel?

Auteur: Paul Vankan werkt bij het NCSC en is bereikbaar via paul.vankan@ncsc.nl.

De (on)zichtbaarheid van applicatielaag DDoS-aanvallen

Distributed-Denial-of-Service-aanvallen (DDoS-aanvallen) vormen al geruime tijd een bedreiging voor de beschikbaarheid van op internet aangesloten systemen. Deze dreiging bestaat onder andere omdat de aanvallen ontwikkelen in vorm en omvang. Eén van de ontwikkelingen in DDoS-aanvallen vormen de zogenaamde applicatielaag-aanvallen of laag-7 aanvallen, verwijzend naar laag 7 van het OSI-model. Dit artikel gaat in op dit type aanvallen, hoe ze zich onderscheiden van andere DDoS-aanvallen, hoe je ze kunt zien en wat je eraan kunt doen.

Na de Denial-of-Service-aanvallen (DoS-aanvallen), waarbij een enkel netwerkpakketje de beschikbaarheid van een server of service kon verstoren, ontstonden de DDoS-aanvallen. Deze DDoS-aanvallen maken misbruik van een (mogelijk groot) aantal aanvallende apparaten om een door een aanvaller beoogd doelwit uit te schakelen. Daarbij worden grote hoeveelheden netwerkverkeer en/of malafide verzoeken afgevuurd, die ervoor zorgen dat dienstverlening verstoord raakt, eventueel met grote gevolgschade. De omvang van dit type aanvallen, gemeten in zowel bits per seconde als in pakketten per seconde, neemt gestaag toe. Ook lijkt er een trend te ontstaan waarbij het aantal kleine aanvallen toeneemt.

Applicatielaag 7

Een DDoS-aanval kan zich richten op tal van verschillende componenten in een netwerk en netwerkinfrastructuur: switches, firewalls, DNS-services, webservices, webapplicaties, enzovoort. Daarbij heeft elke component een grens in capaciteit waarboven geen antwoord meer gegeven kan worden op een legitiem verzoek door de brute omvang

van een aanval. Deze aanvallen leveren last op voor gebruikers. Veel organisaties nemen daarom gespecialiseerde diensten af die malafide verzoeken uit het netwerkverkeer kunnen filteren. Hierdoor is een website of andere infrastructuur beter bestand tegen dergelijke aanvallen. In plaats van een grote omvang aan verkeer op een doelwit te lanceren, kan een aanvaller ook subtieler te werk gaan. Door een specifieke aanval op te zetten, kan de vorm van de verzoeken een verstoring van de beschikbaarheid veroorzaken. Daarbij richt een aanvaller zich dan niet op de onderste vier lagen van het OSI-model, maar op de bovenste laag: de toepassings- of applicatielaag (application layer), laag 7. Een specifiek verzoek kan een (te) grote hoeveelheid middelen vragen. Met een serie van deze verzoeken kunnen alle beschikbare middelen toegewezen worden aan malafide verzoeken, waardoor een legitiem verzoek geen reactie krijgt. Een variant kan zich richten op het veroorzaken van een fout in de applicatie, die hetzelfde resultaat geeft als de fout niet goed afgehandeld wordt.

Complicaties

Omdat applicatielaag DDoS-aanvallen een ander karakter hebben dan overige DDoS-aanvallen, vereisen ze ook andere maatregelen om de verstoring te verhelpen. Dat betekent dat het ook nut heeft om er gericht naar te kijken. Bij dit type aanval is er vaak met een veel kleiner aantal netwerkpakketten een verstoring te veroorzaken. Zeker als dit gecombineerd wordt in een hybride aanval met een grote omvang aan ander verkeer, kunnen deze aanvallen lastig waar te nemen zijn en verdwijnen ze in de stormvloed. In plaats van grote hoeveelheden netwerkverkeer (pakketten per seconde of gigabits per seconde), uiten dit soort aanvallen zich in een hoog geheugen- of processorgebruik of door foutmeldingen in logbestanden. Lastig is daarbij dat anomalieën in processor- en geheugengebruik of foutmeldingen in logbestanden ook andere oorzaken kunnen hebben dan een aanval, zodat een aanval soms over het hoofd kan worden gezien. Wanneer er anti-DDoS maatregelen zijn getroffen bij een provider, zal daar een volume gebaseerde aanval makkelijker worden geconstateerd en gefilterd dan een aanval waarbij de inhoud van het verkeer moet worden geanalyseerd. Een goede analyse kan het beste worden gedaan met kennis van het interne netwerk en de services en applicaties zoals die zijn ingericht. TLS- en SSL-verkeer kan voor analyse een extra complicatie vormen, omdat het verkeer versleuteld is en de inhoud dus niet bekeken kan worden. Malafide verzoeken aan een applicatie kunnen in dat versleutelde verkeer niet herkend worden. De analyse van het inhoudelijke netwerkverkeer kan pas worden gedaan na de component in het netwerk waar TLS/SSL-offloading plaatsvindt, vaak binnen het netwerk van de organisatie. Overigens kan ook in het geval van TLS- en SSL-verkeer de monitoring van resourcegebruik een indicatie geven van mogelijke applicatielaag DDoS-aanvallen.

Hoe te kijken naar applicatielaag DDoS-aanvallen

Er is geen eenvoudig of eenduidig recept te geven om een applicatielaag DDoS-aanval te herkennen. Vaak is de aanleiding van onderzoek een verstoring van de dienstverlening. Dat hoeft geen DDoS-aanval te betreffen. Bij het achterhalen van de oorzaak is het goed om alle mogelijkheden open te houden en te onderkennen dat een mogelijke oorzaak van uitval een applicatielaag gerichte DDoS-aanval kan zijn. Of als alternatief dat als een aanval niet aangetoond kan worden er mogelijk een andere oorzaak van uitval is. Voor de analyse kan het nodig zijn om in logbestanden te kijken of om netwerkverkeer te analyseren. Het kan noodzakelijk zijn hiervoor logbestanden te genereren of logbestanden met een ander detailniveau te genereren (indien dat mogelijk is). En netwerkverkeer moet mogelijk worden vastgelegd in packet captures. Het is waarschijnlijk dat een combinatie van deze zaken nodig is om tot een resultaat te kunnen komen. Vaak is de hoeveelheid gegenereerde gegevens omvangrijk en kan er van een beperkt tijdsinterval een gedetailleerde analyse worden gedaan.

Wat levert het onderzoek op?

Het heeft zin om onderzoek te doen naar applicatielaag DDoS-aanvallen. Daarvoor zijn verschillende redenen aan te geven. Als eerste is een applicatielaag gerichte aanval moeilijker te spoofen (voor te wenden van een andere bron afkomstig te zijn). Vaak moet de 3-staps TCP handshake zijn afgerond om een op TCP gebaseerd protocol te misbruiken voor een aanval. Dat betekent dat het afzenderadres met grotere mate van betrouwbaarheid kan worden vastgesteld, hetgeen bijvoorbeeld relevant is bij het instellen van filtering of bij het verrichten van aangifte bij de politie. Daarnaast heeft een laag-7 aanval vaak een zeer specifieke vorm en kan daardoor ook gericht worden gefilterd of gestopt door de configuratie van een systeem aan te passen (bijvoorbeeld het aantal gelijktijdige connecties (per IP-adres) of de connectieduur). Hiervoor hoeft niet noodzakelijk aparte infrastructuur aangeschaft te worden maar kan de bestaande infrastructuur robuuster worden gemaakt.

En nu verder

Na het vaststellen van de aanval zijn maatregelen mogelijk om de aanval gericht te mitigeren. Daarbij houdt het echter niet op. De opgedane kennis is waardevol om te delen. Anderen hebben er immers ook baat bij, zowel om hun eigen analyses verder te helpen als om (preventief) maatregelen te nemen wanneer er een aanval plaatsvindt. En niet alleen de resultaten van de analyse zijn waardevol, ook de vastgelegde informatie in de vorm van de logbestanden en de packet captures van het netwerkverkeer. Deze informatie kan een aangifte bij de politie ondersteunen. Wanneer iemand wordt aangewezen als de veroorzaker van een DDoS aanval, wordt het uitvoeren van dergelijke aanvallen een stuk minder aantrekkelijk.

Bij het NCSC zijn we geïnteresseerd in de bevindingen van onderzoeken van applicatielaag-gerichte DDoS aanvallen en horen we graag wat er is gevonden of welke ervaringen zijn opgedaan.

Dit artikel verscheen eerder als expertblog op ncsc.nl

Auteur: Nicole van Deursen is hoofdredacteur van iB-magazine en is bereikbaar via nicole.vandeursen@pvib.nl

Ethische gedragscode voor incident responders gepubliceerd

In oktober publiceerde FIRST, de internationale organisatie voor security incident response teams, de Code of Ethics. Deze richtlijn heeft als doel om cybersecurity professionals te ondersteunen bij professionele en ethische dilemma's waar zij in hun werk tegenaan kunnen lopen.

Binnen de FIRST organisatie is de special interest group ethicsfIRST opgericht ter inspiratie en begeleiding van ethisch gedrag van onder andere security professionals, instructeurs, studenten en influencers. Iedereen die computertechnologie gebruikt en de kennis en vaardigheden heeft om hiermee impact op de samenleving te veroorzaken, moet de verantwoordelijkheid die dat met zich meebrengt erkennen. De groep heeft vanaf 2016 gewerkt aan een code om impliciet verwacht gedrag van securityprofessionals expliciet te benoemen. De code is in oktober 2020 gepubliceerd. Elk principe in het document is uitvoerig gereviewed en besproken door ervaren cybersecurity-experts, fabrikanten en overheidsmedewerkers uit de hele wereld en zijn gebaseerd op waargebeurde scenario's.

12 verantwoordelijkheden

Het document is te vinden op de website van ethicsfIRST (1) en bevat een lijst van principes die de verantwoordelijkheden van de professional weergeven. Er zijn 12 verantwoordelijkheden in het document uitgewerkt. De eerste en belangrijkste is: vertrouwen. Dit is de kern van alle andere principes. Vertrouwen is de basis voor relaties tussen securityprofessionals en de basis waarop informatie wordt uitgewisseld en gedrag wordt verwacht. De overige principes werken uit welk gedrag bijdraagt aan de vertrouwensrelatie en die zijn: coordinated vulnerability disclosure, vertrouwelijkheid respecteren, bevestiging van ontvangst en actie, verantwoordelijk omgaan met autorisaties, informeren waar nodig, mensenrechten respecteren, letten op gezondheid, vaardigheden onderhouden, data verzamelen, wetten respecteren, en bewijsvoering.

In de praktijk kunnen deze principes soms met elkaar in conflict zijn. Dan staat de securityprofessional voor een dilemma welk principe te volgen. De code kan hiermee helpen. In 2021 wordt nog een uitbreiding verwacht waarin met behulp van vele voorbeelden wordt geïllustreerd wat de impact is van de verschillende keuzes.

Referentie

(1) https://ethicsfirst.org/

COLUMN Berry

Proficiat. Of toch maar niet

Het schrijven van deze column is eigenlijk nooit echt een probleem. Het vinden van een onderwerp wel. Mijn wereldje is momenteel heel erg klein, maar daar zal ik niet de enige in zijn. Als ik een beetje aan het surfen ben op mijn pc, dan kom ik vandaag de dag alleen maar berichten tegen over de veroorzaker van ons thuiszitten en welke beoogde president van de VS thuis mag gaan zitten. Over beide onderwerpen is natuurlijk wel heel erg veel te zeggen als het gaat over het manipuleren van de waarheid en het bespelen van journalisten.

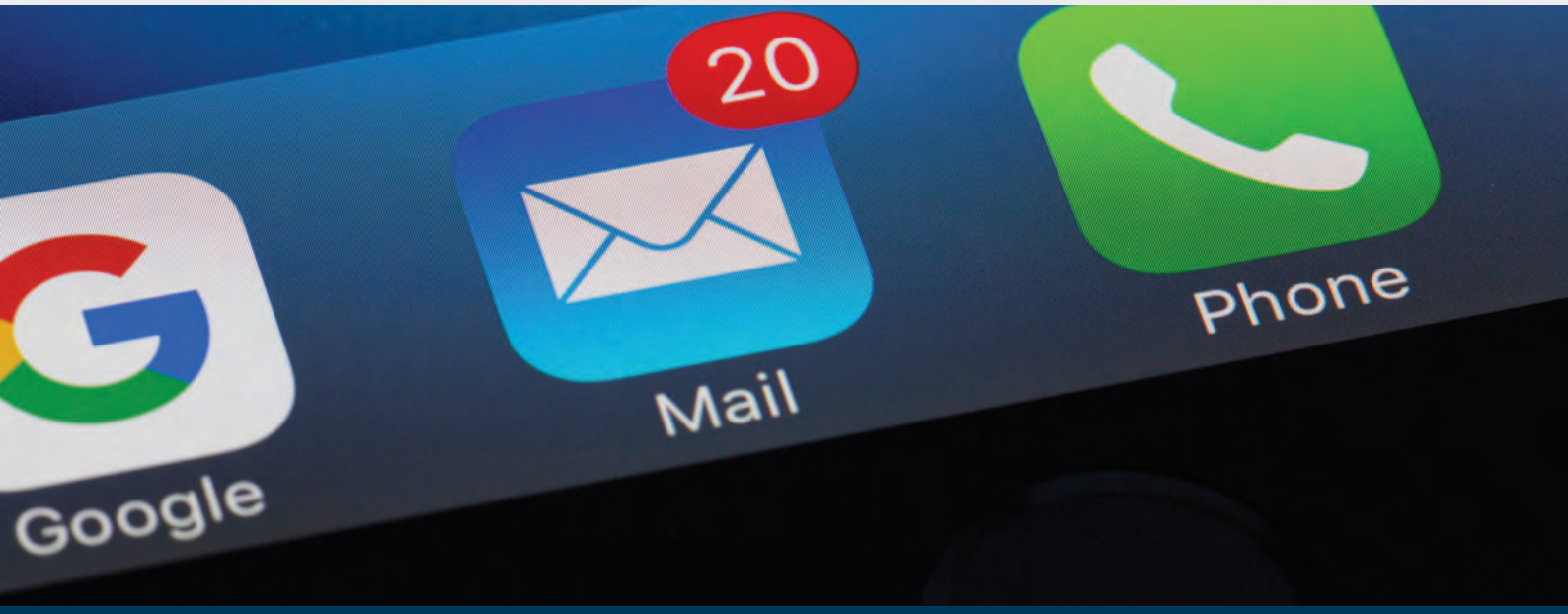
De huidige president (probeer zijn naam niet op te schrijven) maakt het wel erg bont: hij manipuleert de waarheid en er is één ding wat beslist niet kan en dat is deze verkiezingen verliezen. In de aanloop naar deze verkiezingen nam hij al veel maatregelen om het de kiezers in de staten waar de democraten vaak winnen, moeilijk zo niet onmogelijk te maken om een stem te kunnen uitbrengen. Sommigen stonden 8 uur te wachten voor het stemlokaal. Ook riep de huidige president dat alle stemmen die niet geteld waren voor het einde van de verkiezingsdag, ongeldig verklaard moesten worden, evenals alle stemmen die per post waren uitgebracht. De huidige president claimt overwinningen in staten waar nog volop geteld wordt. Natuurlijk liet hij de afgelopen jaren ook al zien dat hij een bijzonder ruime fantasie heeft en dat er op geen enkele manier bewijzen zijn te vinden voor zijn beweringen. Ik begrijp er niets van dat er zoveel mensen op hem stemmen. Wat hij doet is de bestaande orde ondermijnen. Roepen dat er gesjoemeld wordt zonder dat hij ook maar enig bewijs heeft. Insinueren dat er ineens duizenden stemmen tevoorschijn worden getoverd waardoor Biden meer stemmen krijgt.

Onze topman van de republikeinen beweerde dat er bij de verkiezingen is gefraudeerd zonder die claim verder te verduidelijken. Ook riep hij de overwinning uit, terwijl er nog miljoenen stemmen moesten worden geteld. Verder wil hij dat rechters het tellen van de stemmen stopzetten.

Nee, wat dat betreft is de huidige president van de VS maar een sneu amateurtje, die denkt dat de wereld van hem is en dat zijn twitteraccount niet gehackt kan worden. En met die woorden vraag je erom om gehackt te worden, wat ook niet moeilijk was met zijn eenvoudig raadbare wachtwoord. Al het nieuws wat hem niet aanstaat wordt bestempeld als fakenews. Ik ben benieuwd of hij Biden gaat feliciteren met zijn overwininning, nou nee eigenlijk niet. Gaat niet gebeuren.

Berry

Auteurs: Bertine Uithoven is senior productmanager ZorgMail bij Enovation Group en sinds 2017 werkzaam bij Enovation Group in Capelle aan den IJssel. Bertine is te bereiken via bertine.uithoven@enovationgroup.com.



Veilig mailen in de zorg

Er wordt volop digitaal gecommuniceerd over en met collega zorgprofessionals, patiënten, cliënten en alle betrokkenen eromheen. Veel van deze informatie-uitwisseling binnen en tussen instellingen is system-to-system communicatie. Dat wil zeggen een directe – versleutelde – verbinding tussen systemen zonder menselijke tussenkomst. Maar zorgprofessionals maken ook gebruik van mail en whatsapp. Hoe zit het met de privacybescherming daarvan?

De Autoriteit Persoonsgegevens (AP) heeft daar ook zo haar vraagtekens bijgeplaatst. Vandaar dat in mei 2018 op de health care Information and management systems society (HIMMS) in Barcelona de aftrap is gegeven voor het project 'Veilig Mailen in de Zorg' door het Informatieberaad in de Zorg. 'Normaal' mailverkeer, zonder aanvullende maatregelen, voldoet niet aan de eisen als het gaat om privacybescherming. De AP heeft het ministerie van Volksgezondheid, Welzijn en Sport (VWS) daarom gevraagd om duidelijkheid te scheppen over welke voorwaarden van toepassing zouden moeten zijn om veilig en in overeenstemming met de AVG te kunnen mailen in de zorg. In oktober 2018 is VWS samen met de NEN het project 'Veilige Mail' gestart en dit heeft in mei 2019 geresulteerd in de NTA7516 (Nederlands Technische Afspraak).

Een werkgroep met daarin een sterke vertegenwoordiging van leveranciers, het zorgveld, koepels, patiëntvertegenwoordigers en certificerende instanties hebben functionele eisen beschreven waaraan e-mail met daarin persoonlijke gezondheidsinformatie zou moeten voldoen om als veilig gekwalificeerd te worden. Hierin zijn onder andere aspecten als Integriteit, Vertrouwelijkheid en Beschikbaarheid meegenomen.

Mailen mag, maar wel veilig

De NTA is gebaseerd op bestaande wet- en regelgeving alsmede bestaande normenkaders rondom privacy en informatiebeveiliging en uitwisseling zoals de eIDAS, AVG en ISO27001. De NTA7516 valt in de groep waarin ook de NEN7510 zit met betrekking tot informatiebeveiliging in de zorg. Immers, mailen mag natuurlijk, maar moet wel veilig. Primair is de NTA dus bedoeld voor zorgprofessionals die besluiten veilige mail te gebruiken als communicatiemiddel. De NTA beschrijft hierbij de uitgangspunten en voorwaarden waarbij mail als veilig middel kan

worden ingezet. Echter, de zorgprofessionals nemen natuurlijk altijd een dienst af bij een leverancier voor veilig mailen. Daarmee is de NTA minstens, zo niet evenzo, belangrijk voor leveranciers, de zogenaamde communicatiedienstenaanbieders. Voor deze leveranciers stelt de NTA heel concreet functionele én technische eisen waaraan de dienst(en) moet voldoen. Het mooie is dat veilig mailen in de zorg niet iets nieuws is. Verschillende leveranciers bieden al diverse jaren veilige mailoplossingen aan. Vaak ook met een specifieke focus op de zorg. Niet raar als je bedenkt dat dit bij uitstek een sector is waar veel vertrouwelijke informatie wordt uitgewisseld. En waarin, helaas, ook nog (te)veel gebruik wordt gemaakt van 'normale' mail vanuit gemak. Je kent 't wel: even snel een afspraakbevestiging versturen, een uitslag doorgeven of een consultatie inwinnen bij een collega zorgprofessional.

En juist omdat er flink wat use cases zijn waarin system-to-system communicatie niet voorhanden is of minder geschikt voor is, wil je als zorgprofessional van een laagdrempelige maar ook veilige person-to-person communicatie gebruik kunnen maken. Kijkend naar de cijfers van de AP werden in 2019 de meeste datalekken gemeld door de zorgsector. Het idee dat gevoelige data te eenvoudig onbedoeld in verkeerde handen kan vallen is geen prettige gedachte. Om die reden heeft een breed gremium aan stakeholders de handen ineengeslagen om de 'next step' te zetten in privacybescherming door middel van een hoger niveau van standaardisatie en securitymaatregelen.

Deze stappen zijn duidelijk terug te zien in de veelal technische maatregelen op het vlak van Beschikbaarheid, Integriteit en Vertrouwelijkheid. Implementatie van technische standaarden, opgenomen in de Technische Handreiking voor Leveranciers, die ervoor moeten zorgen dat grotere zekerheden worden bereikt op het vlak van onder meer datatransport, dataopslag, authenticatie van verzender en ontvanger, minimale beschikbaarheid en maximale uitvalduur. Anders gesteld: geen juiste privacybescherming zonder passende informatiebeveiliging.

Interoperabiliteit en gebruikersgemak

Tegelijkertijd is er in het NTA7516 traject veel aandacht uitgegaan naar een gezonde balans tussen bovengenoemde, veelal technische, maatregelen en het borgen van voldoende gebruikersgemak. Juist bij e-mailen – wat we allemaal frequent doen – is dit net als bij een telefoontje plegen cruciaal voor het welslagen. Bij telefonie weten we al niet beter dat we, zonder dat we erover hoeven na te denken, iedereen direct kunnen bereiken onafhankelijk bij welke provider iemand is aangesloten. Met een duur woord heet dit 'interoperabiliteit', zodat een gebruiker in de keten optimaal wordt ondersteund.

Beide aspecten, interoperabiliteit en gebruikersgemak, hebben dan ook een prominente positie in NTA7516 gekregen. Patiënten/cliënten die een veilige mail van hun zorgprofessional ontvangen, hebben de mogelijkheid om een bericht en eventuele bijlagen te downloaden, beantwoorden of doorsturen. En als zowel verzender als ontvanger aantoonbaar voldoen aan NTA7516 kan een veilige mail – net zoals bij een telefoontje – direct worden afgeleverd. Dus rechtstreeks in de 'inbox' van de ontvanger. En niet langer in een portaal of viewer omgeving waarbij extra handelingen nodig zijn om het bericht te kunnen lezen.

Een groot deel van de criteria uit NTA7516 kan worden ingevuld door de communicatiedienstenaanbieders (leveranciers) voor wie een certificeringsschema beschikbaar is. Waarmee zorgaanbieders fors ontzorgd worden in de hoeveelheid acties om eveneens aantoonbaar te voldoen. Ten tijde van dit schrijven zijn zes leveranciers officieel gecertificeerd. Op 17 december 2019 vond de Projectathon 'Veilig mailen in de zorg' plaats waarbij de deelnemende leveranciers hebben laten zien dat interoperabiliteit tussen oplossingen van verschillende leveranciers mogelijk is. Onmiddellijk gevolgd door de 'proof in the pudding' in de Wvggz-keten (Wet verplichte GGZ) vanaf 1 januari 2020 en nu in de NTA7516 uitrol.

Vanuit beveiligingsoptiek is het wenselijk/noodzakelijk dat ook andere dan bovengenoemde communicatiestromen veilig zijn. Denk hierbij aan mailen vanuit het EPD met andere zorgprofessionals of met patiënten/cliënten/burgers – ook wel genaamd 'personen' in NTA7516. En naast veilig ook eenvoudig te koppelen aan het dossier van de persoon. Een aantal leveranciers biedt deze integratie.

'Alleen samen'

En 'last but not least' eist NTA7516 van een zorgprofessional dat deze een veilig ad hoc communicatiemiddel moet bieden waarmee personen op eigen initiatief een veilig bericht kunnen sturen aan de zorgprofessional. Met als laagdrempelige oplossing een beveiligd webformulier op de website van de zorgprofessional, gekoppeld aan mailadres van waaruit veilig kan worden geantwoord. Ook op dit vlak bieden verschillende leveranciers een oplossing.

Om als zorgprofessional aantoonbaar te kunnen voldoen aan NTA7516, middels het inleveren van een ondertekende zelfverklaring aan de communicatiedienstenaanbieder, zijn aan de kant van de zorgprofessional acties nodig op de volgende onderdelen:

- technische implementatie
- functionele instellingen
- werkwijze aanpassen
- beleid beschrijven

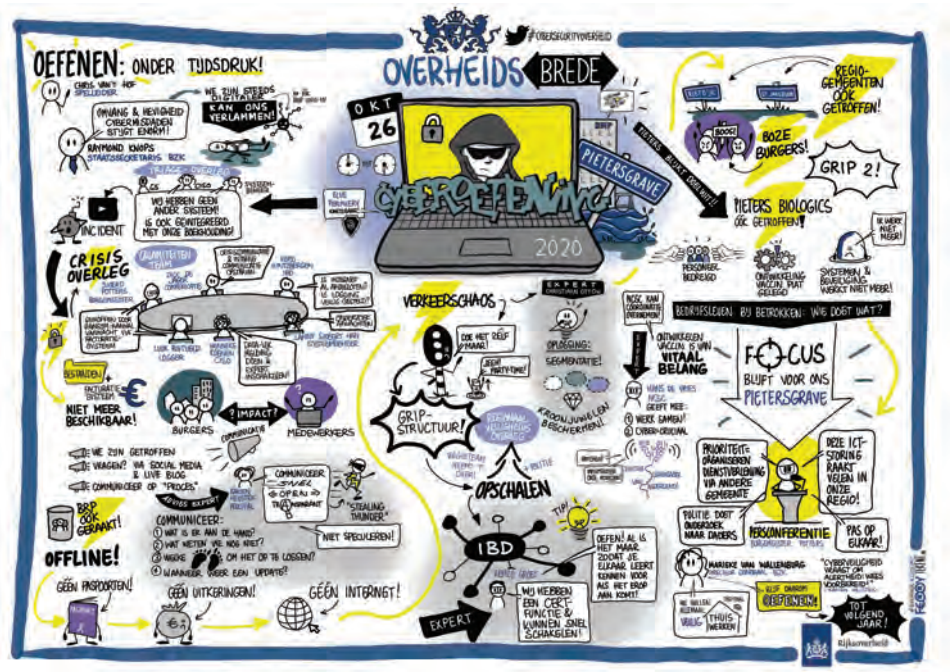
En ben je zover dan krijg je de beschikking over de software waarmee je interoperabel berichten kunt versturen en ontvangen. Het succes van de interoperabiliteit staat of valt met de inspanning van de communicatiedienstenaanbieders én van de zorgprofessionals om dit gezamenlijk te willen bereiken. De slogan van de coronacampagne 'alleen-samen' gaat ook op voor interoperabiliteit: we zijn allemaal aan zet!

Kortom, ben je zorgprofessional, adviseer je er een of mail je wel eens met je eigen zorgaanbieder? Let dan op of het mailen veilig en conform NTA7516 gebeurt. Immers, mailen is makkelijk en snel, maar zeker met zorggegevens moet het wel veilig.

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.

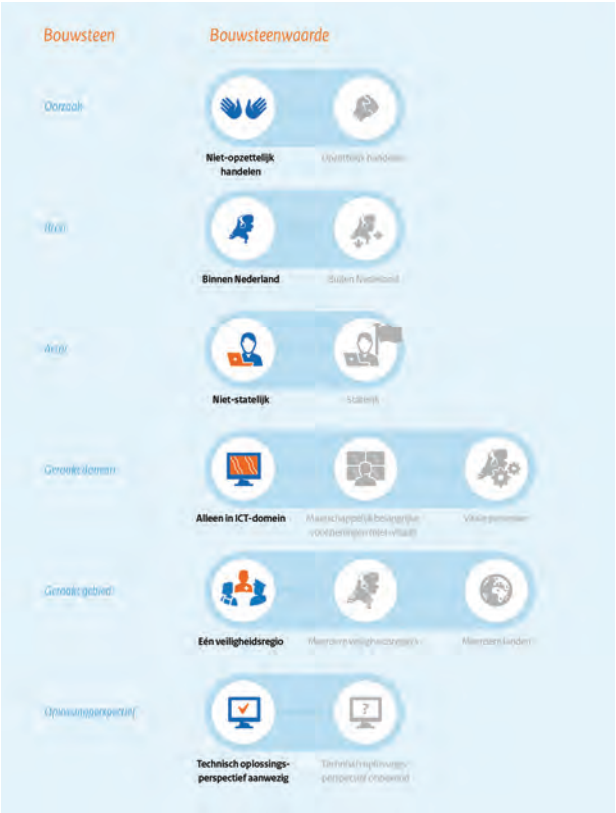
08.10.2020

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/

In deze rubriek geven enkele iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

Overheid raakt 6,9 miljoen gegevens uit donorregister kwijt

Minister Tamara van Ark voor Medische Zorg en Sport deelde de voorzitter van de Tweede Kamer op 6 november jl. mee, dat: "Dit onderzoek (redactie: onafhankelijk onderzoek van de Audit Dienst Rijk (ADR) inzake het datalek bij het donorregister) omvangrijker was dan tevoren verwacht. Zorgvuldige uitvoering van dit onderzoek en de daarbij benodigde afstemming tussen de ADR en CIBG hebben meer tijd gevraagd. Ik kan de Kamer daarom naar verwachting begin 2021 het onderzoeksrapport, inclusief mijn reactie daarop, toezenden."

Het gaat hierbij om een op 6 maart gemeld datalek door verlies van twee harde schijven, op 9 maart kenbaar gemaakt aan de minister (2), op 10 maart door minister Hugo de Jonge van Volksgezondheid, Welzijn en Sport verzonden aan de voorzitter van de Tweede Kamer (3). Op 30 april volgde een Kamerbrief over het datalek (4) met als één van de belangrijke conclusies: "Het CIBG heeft aangegeven dat de zoektocht inmiddels is afgerond. Het CIBG heeft tot en met 12 maart gezocht naar de schijven. De schijven zijn niet meer gevonden en ik acht de kans minimaal dat de schijven alsnog op een later moment worden teruggevonden."

Uiteindelijk uitmondend in de brief van 6 november jl. (1) waarbij in een klein jaar tijd het verlies van 6,9 miljoen gegevens nog onopgelost en de ernst van dit verlies gekwalificeerd wordt als een met beperkt risico, waarbij alle partijen benadrukken hoe belangrijk de handhaving dan wel herstel van het vertrouwen essentieel is.

All animals are equal, but some are more equal than others! - Chris de Vries

Literair geïnteresseerden herkennen in dit citaat George Orwells Animal Farm. Naast '1984' één van de belangrijkste werken van hem. Wat heeft dat nu te maken met


Chris de Vries


Fook Hwa Tan

informatiebeveiliging? Veel, want als een bedrijf belangrijke databestanden kwijtraakt, dan treft dat bedrijf de verontwaardiging van de overheid en het volk en zijn boetes, straf en wellicht een faillissement niet ver weg. Wat nu als de overheid een dergelijke fout maakt? Dan lezen wij: `De minister acht de kans op misbruik klein …' en dan stelt het Centraal Meldpunt Identiteitsfraude en -fouten zich op het standpunt: `… NAW-gegevens en geboortegegevens zijn ook via sociale media of zoekmachines te vinden …' en: `De kans op misbruik met het Burgerservicenummer is volgens hem (minister de Jonge – red.) klein, `… omdat dit nummer enkel wordt gebruikt bij onder andere de overheid en in de zorgsector'. (5) Hier wordt met twee maten gemeten. Politici en ambtenaren zijn in de praktijk onaantastbaar en worden zelden of nooit bestraft. Zouden ze al beboet worden, dan is het uiteindelijk de burger die de boetenota betaalt in de vorm van belastingen, heffingen of ingetrokken subsidies. Ronduit ernstig is het feit dat in conflicten tussen de overheid en de burger en/of het bedrijfsleven vaak de bewijslast wordt omgedraaid en dat de burger zijn gelijk te bewijzen heeft of te bewijzen heeft dat de overheid ongelijk heeft.

Hoe doe je dat als de overheid navolgende gegevens 'kwijtraakt':
- voor- & achternaam;
- geslacht;
- geboortedatum;
- adresgegevens;
- donorkeuze;
- handtekening en
- burgerservicenummers

van slechts 6.058.250 unieke Nederlanders (over de periode februari 1998 en juni 2010)? (5)

Onderzoek leidt vaak niet tot de waarheid - Fook Hwa Tan

Een melding in maart met een rapport in november als gevolg. Datalekken dienen binnen 72 uur bij de autoriteit gemeld te worden. Voor onderzoek naar de oorzaak of impact is geen tijdslijn ingesteld. Is dat terecht of niet?

Aan de ene kant is het logisch dat oorzaakanalyse tijd nodig heeft, maar aan de andere kant is adequaat en snel handelen ook een prioriteit bij een datalek. Dit om impact en consequentie op de gedupeerden te minimaliseren. Dit voorval is samen te vatten als het verlies van twee harde schijven, maar hoe het heeft kunnen komen tot het verlies is na een half jaar onderzoek niet te achterhalen. Is het gemis aan beleid en regels? Of hebben mensen zich niet aan de regels gehouden? Een simpel voorval blijkt vaak toch wel erg complex. Vervolgens krijg je onze complexe overheid met de vele lagen en schijven, die zich ermee gaan bemoeien of moeten bemoeien. Je hebt vaak te maken met een veelvoud aan stakeholders, die allemaal een eigen belang hebben en vaak ook hun eigen regels hebben gevolgd waardoor het voorval niet had mogen gebeuren. Al met al een scala aan mensen, die deels verantwoordelijk zijn. Dit betekent vaak, dat er moeilijk naar één persoon gewezen kan worden die de schuldige is. De overheid is daarvoor mogelijk te complex. Als het mogelijk was geweest om wel te achterhalen wat er was gebeurd en wie daarvoor de directe aanleiding heeft gegeven dan zou je vrij gemakkelijk tot de verantwoordelijke komen. De vraag is echter wel of er in dit soort gevallen wel sprake van een schuldige partij of dader kan zijn? Als deze wel gevonden kan worden, is nog de vraag wat het lekken van de gegevens als gevolg heeft voor de betrokkenen. Alleen op basis daarvan kun je de ernst van de zaak bepalen. En dan kom je in de wondere wereld van data en informatiebeveiliging. Deze dataset kan mogelijk onschuldig lijken, maar in combinatie met andere uitgelekte of legitieme databronnen kun je wel degelijk interessante data creëren voor geldelijk gewin door bijvoorbeeld identiteitsfraude. Dit maakt impactanalyse ook erg complex als je niet in een zee van aannames wil komen. Al met al zien we, dat we bij een datalek bij de overheid te maken hebben met een complex incident met mogelijk vele oorzaken, een complexe overheid en een vaak niet makkelijk te bepalen impact. Ons vakgebied is nog jong en hier hebben we mee te maken. Maar het goede nieuws is, dat we ook leren en ik geloof, dat we hier in korte tijd een oplossing voor hebben. Dit betekent vaak wel weer meer metadata bijhouden om de bestaande data te beschermen.

Referenties

(1) https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z20885&did=2020D44719

(2) https://www.rijksoverheid.nl/documenten/brieven/2020/03/09/onvindbare-externe-gegevensdrager-donorregister

(3) https://www.rijksoverheid.nl/documenten/kamerstukken/2020/03/10/kamerbrief-over-datalek-donorregister

(4) https://www.rijksoverheid.nl/documenten/kamerstukken-/2020/04/30/kamerbrief-over-schriftelijk-overleg-so-inzake-so-datalek-donorregister

(5) https://tweakers.net/nieuws/166664/minister-acht-kans-op-terugvinden-kwijtgeraakte-hdds-donorregister-klein.html

In Memoriam Lex Dunn
13/09/1957 – 10/11/2020

Can death be sleep, when life is but a dream,
And scenes of bliss pass as a phantom by?
The transient pleasures as a vision seem,
And yet we think the greatest pain's to die.

How strange it is that man on earth should roam,
And lead a life of woe, but not forsake
His rugged path; nor dare he view alone
His future doom which is but to awake.

~John Keats

Geliefd en gerespecteerd

Met een grote glimlach en pretogen die altijd meer leken te weten dan zijn mond verraadde, leeft Lex voort in onze gedachten. Op 10 november 2020 is Lex Dunn overleden in zijn geliefde Frankrijk waar hij samen met zijn vrouw Maria de zon wilde zien ondergaan.

Lex heeft zich vele jaren met hart en ziel ingezet voor de redactie van het iB-Magazine en het PvIB. Met zijn markante persoonlijkheid, inclusief prachtige hoed en cowboystropdas, veroverde hij met gemak ieders hart. En de eerlijkheid gebiedt ons te zeggen dat Lex waarschijnlijk meer over informatiebeveiliging vergeten is, dan wij ooit zullen weten. In 2007 verscheen zijn naam voor het eerst als redactielid in het colofon en pas in 2019 nam hij afscheid van de redactie met de wens ook vanuit Frankrijk door te blijven schrijven. Die passie voor en toewijding aan het vak was onuitwisbaar diep verweven met zijn persoonlijkheid. In zijn afscheidsinterview blikte hij vol trots terug op zijn bijdrage aan het iB-magazine, de rubriek 'Achter het Nieuws'. In die rubriek geven iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. "Persoonlijke meningen die niet noodzakelijk het officiële standpunt weergeven van hun werkgever of van het PvIB", legt Lex uit. "Maar juist daarom interessant omdat we op deze manier discussie proberen uit te lokken met leden en lezers. Interactie met onze lezers waar we als redactie behoefte aan hebben."

Zoals Keats al schreef in zijn gedicht over de dood, is het leven er onlosmakelijk mee verbonden. Maar als de dood dan intreed, is het lijden gedaan. Lieve Lex, we missen je. Namens alle (oud)-redactieleden veel sterkte voor Maria en familie in deze zware tijd.
Rachel Marbus

"Ik ken Lex al vanaf het ontstaan van PvIB (de fusie tussen PI en GvIB) in 2007. Lex was zeer geliefd, gewaardeerd en een vaste waarde in de redactieraad. Je kon altijd op hem rekenen. Met zijn ideeën heeft hij veel bijgedragen aan de ontwikkeling van het blad. Hij had een groot netwerk waaruit vele auteurs een bijdrage hebben geleverd. Bij zijn afscheid is hij niet voor niets erelid gemaakt! Het is diep treurig dat Lex zo kort na zijn pensionering het leven zo vroeg heeft moeten verlaten. Een groot verlies."
Tom Bakker, redactievoorzitter van iB-Magazine

"Ik heb dierbare herinneringen aan Lex. Hij heeft me het mooie van het vak informatiebeveiliging laten zien toen ik bij Capgemini startte en me meegenomen in de professional boards bij Capgemini en het PvIB. Van Lex leerde ik dat de aanpak van informatiebeveiliging gebaseerd is op logische grondbeginselen en dat je onvermoeibaar moet zijn in het uitdragen daarvan. Security heeft ook een gezicht nodig, iemand die het verhaal vertelt en jonkies zoals ik was op sleeptouw neemt. Lex was dat gezicht voor mij. Ik ga je missen, Lex." **Aart Jochem**

"Lex heeft de laatste twee en half jaar van zijn carrière fantastisch werk geleverd bij Pon Holdings. Ook wist hij met veel passie zijn collega's te coachen en op te leiden. Lex was niet alleen een fijne collega, maar ook een mentor en een vriend. Heel veel sterkte voor Maria, familie en vrienden met dit enorme verlies. We zullen je missen." Namens alle collega's bij Pon, **Rence Damming**

COLOFON

IB is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

PvIB
Platform voor InformatieBeveiliging

HOOFDREDACTEUR
Nicole van Deursen

REDACTIE
Tom Bakker
Bianca Brooijmans
Maarten Hartsuijker
Lilian Knippenberg
Rachel Marbus
Fook Hwa Tan
Chris de Vries

BLADMANAGEMENT
MOS bv
Caroline Knobbe
Sam Dekkers
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE
MOS bv
E acquisitie@mos-net.nl
T 033 247 34 00

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

UITGEVER
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
E secretariaat@pvib.nl
W www.pvib.nl

ABONNEMENTEN
De abonnementsprijs in 2020 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

ABONNEMENTENADMINISTRATIE
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
E secretariaat@pvib.nl

ISSN 1569-1063

TRAININGEN INFORMATIEBEVEILIGING BIJ DNV GL

NORMKENNIS ISO 27001	27	JANUARI
LEAD AUDITOR ISO 27001	8 - 12	FEBRUARI

KIJK OP: **WWW.DNVGL.NL/TRAININGSAANBOD**

STARTEN MET INFORMATIEBEVEILIGING?

Maak informatiebeveiliging aantoonbaar met ISO 27001

ISO 27001 is de bekendste internationale norm voor informatiebeveiliging. In 2019 is het aantal ISO 27001-certificaten in Nederland verdubbeld.

Wilt u uw informatiebeveiligingsbeleid extern aantoonbaar maken? Kies voor een gecertificeerd managementsysteem voor informatiebeveiliging (ISMS) volgens ISO 27001.

DNV GL staat bekend om haar pragmatische audits, een auditteam met expertise binnen uw sector. In uw auditrapportage ziet u niet alleen de tekortkomingen maar ook de sterke punten van uw organisatie.

Wat is een ISMS?

Hierin staat een stappenplan voor het opzetten van een Information Security Management System (ISMS).

Download de whitepaper via

www.dnvgl.nl/isms

U kunt ons bereiken via **010 2922 700** of **www.dnvgl.nl/informatiebeveiliging**