INFORMATIEBEVEILIGING MAGAZINE

- Lig jij ook wakker van ransomware?
- Bereid je voor op de komst van quantum computers
- Column: Een analogie voor cybersecurity

JAARGANG 23 - 2023 - EDITIE 4

VERSTERK UW ISO/IEC 27001 MANAGEMENTSYSTEEM!

Wilt u zeker weten of uw organisatie klaar is voor certificering volgens ISO/IEC 27001? Doe de online DNV Self-Assessment en ontvang een rapportage in uw inbox. Of volg de Normkennis ISO/IEC 27001

Kent u de DNV Self-Assessment Suite al? Deze tool stelt u in staat te testen hoe goed u ISO/IEC 27001 kent en te beoordelen in hoeverre uw managementsysteem klaar is voor certificering. De evaluatie is op basis van puntenscores en laat zien waar er tekortkomingen bestaan en waar u verbeteringen kunt doorvoeren.

Stel een nulmeting op, stel kwantitatieve doelen vast voor een specifiek aandachtsgebied en meet regelmatig de geboekte vooruitgang. De Self-Assessment Suite biedt u in alle gevallen een gedetailleerd inzicht in uw kennis of prestaties en uw mate van beheersing.

Wilt u graag uw kennis vergroten over ISO/IEC ISO 27001? Volg dan de Normkennis ISO/IEC 27001 training! De trainer geeft u handige tips en voorbeelden uit de praktijk, zo leert u te kijken naar de norm, zoals een auditor dit doet.

Kijk voor meer informatie over de Self-Assessment Suite op dnv.nl/self-assessment of scan de QR-code als u wilt deelnemen aan de training.

DNV

Heb jij ook zo'n dorst…?

Chris de Vries

Auteurs en redacteuren doen hun best de lezer te voorzien van een magazine vol nieuwigheden. Ook voor ons, als redacteuren, is het telkens een verrassing; hoe het samenkomen van nieuw(tje)s, visies, standpunten en dus mensen een nieuw en, naar ons vertrouwen, lezenswaardig blad het licht laat zien.

Judith Unk presenteert zich aan de leden van het Platform voor InformatieBeveiliging als het nieuw aangetreden bestuurslid en dat in de rol van penningmeester. Als ervaren (kascommissie)lid zal zij een betekenisvolle bijdrage leveren aan onze vereniging. Wij kijken al reikhalzend (of is rijkhalzend hier wellicht beter?) uit naar haar eerste '*eerste dinsdag van september*'-verslag.

Aan het andere einde van de ervarings-dichotomie zien we vervolgens hoe Luiza Atas aan het woord komt over haar stage-ervaring. Luiza studeert Integrale Veiligheidskunde aan de Avans Hogeschool en motiveert haar studie- en beroepskeuze. Het is goed te zien met welke 'Sturm und Drang'-kracht ze een start maakt met haar carrière. Jullie zullen vaker stagiairs aan het woord zien komen: *wie de jeugd heeft, heeft de toekomst.*

Het eerste inhoudelijke artikel van ICTRecht komt van Ruben van der Geest en Alexander Freund. Zij doorkruisen de wereld van 'ransomware'. Een nachtmerrieachtige realiteit, die onder andere ingaat op: wat het is, hoe je ertegen te beschermen, het doen van aangifte, de meldplichten tot en met de (illusie van?) verzekering.
Rachel Marbus kijkt om. Zij weet dat de AVG vijf jaar oud is. En om dit te vieren heeft zij een menu samengesteld met vijf uitsmijters. Laat het jullie smaken. Nu wij het toch over uitsmijters hebben, in 'Achter Het Nieuws' gaat het dit keer over de moedige houding van de Autoriteit Persoonsgegevens, die haar eigen incidenten in het jaarverslag vermeldt. Zij is daardoor niet alleen een autoriteit, die het als plicht ziet *Open & Transparant* te zijn, maar ook een voorbeeld voor menigeen.

Als toetje beveel ik de column van Dimitri van Zandvliet van harte aan. Zijn gedachten over CISCA, de authentiek communicerende firewall, zet je aan het denken. Voor wie de jaren van de wijsheid heeft bereikt (en dus de avonturen van Pipo de Clown kent), lijkt het ons aardig de blog van Robert Metsemaker er naast te zetten en de verschillen en overeenkomsten te zoeken tussen beide auteurs en hun onderwerp.
Ik wil dit keer eindigen met een citaat van Marie von Ebner-Eschenbach (1830-1916), één van de belangrijkste Duitse schrijfsters van novellen: 'Wanneer de nieuwsgierigheid zich op ernstige dingen richt, dan noemt men haar: *dorst naar kennis.*' Ook dorstig geworden van ons magazine?

Chris

IN DIT NUMMER

Auteurs: Mr. drs. A.P. Freund is Information Security Consultant en adviseert over informatiebeveiliging en compliance, geeft awareness trainingen en begeleidt crisisoefeningen. Alexander is bereikbaar via a.freund@ictrecht.nl. Mr. R.A. van der Geest is jurist en houdt zich, onder andere, bezig met advisering over nieuwe technologie. Ook is hij deelnemer aan de Nederlandse AI coalitie. Ruben is bereikbaar via r.vandergeest@ictrecht.nl. Beide auteurs werken bij het juridisch adviesbureau ICTRecht te Amsterdam.

Lig jij ook wakker van ransomware?

De afgelopen jaren lijkt het aantal ransomware-aanvallen schrikbarend te zijn toegenomen. Mede door de verstrekkende gevolgen van een aanval bleef de aandacht hiervoor niet alleen beperkt tot de media die door 'security geeks' wordt bijgehouden, maar werd er ook veelvuldig over geschreven in de dagelijkse media. Verschillende ransomware-aanvallen die in Nederland hebben plaatsgevonden, hebben wijze lessen opgeleverd. Zoals de aanval die de gemeente Hof van Twente in december 2020 trof en de aanval waardoor de Universiteit Maastricht in december 2019 werd platgelegd.

De echte kenner zal zich de aanval uit juni 2017 ook nog herinneren waarbij een gedeelte van de Rotterdamse haven werd getroffen. Dit soort aanvallen kunnen grote gevolgen hebben voor de getroffen partijen en het is daarom van belang om meer inzicht te krijgen in ransomware, hoe men zich ertegen kan beschermen en welke wet- en regelgeving relevant is. In dit artikel gaan wij daarom dieper in op wat ransomware eigenlijk is, het wettelijk kader en de relevante meldplichten, hoe men zich hiertegen kan wapenen en of een cyberverzekering mogelijk uitkomst biedt.

Ransomware: wat, hoe en waarom?

Ransomware is te kwalificeren als kwaadaardige software ('malware') die bestanden versleutelt ('encrypt') of de toegang tot een volledig systeem blokkeert. Ook zaken zoals mobiele telefoons, back-ups en gegevens die in de cloud zijn opgeslagen kunnen versleuteld worden door ransomware. Het versleutelde systeem of de bestanden zouden in principe weer bruikbaar moeten zijn nadat deze ontsleuteld ('decrypted') zijn na het betalen van losgeld ('ransom') aan de aanvaller.

Een ransomware-aanval kan uitgevoerd worden doordat deze gebruikmaakt van zwakheden in bepaalde systemen of de gebruikers ervan. De voornaamste oorzaak hiervan betreft software die niet is bijgewerkt met de meest recente software updates of bijvoorbeeld een RDP (` remote desktop protocol') welke niet goed geconfigureerd is of zwakheden bevat. Juist tijdens de coronacrisis gingen mensen meer vanuit huis werken, waardoor zij veelvuldig gebruikmaakten van RDP of ze inlogden op het bedrijfsnetwerk via de privé computer (welke niet altijd zo goed is bijgewerkt als de zakelijke computer). Dit is mede één van de redenen waarom we een flinke toename van ransomware-aanvallen hebben gezien ten tijde van de coronacrisis.

Gesteld kan worden dat het uitvoeren van ransomware-aanvallen een businessmodel is geworden. Er worden flinke bedragen geëist en soms ook betaald, waardoor het een lucratieve praktijk is voor bepaalde groeperingen. Men moet niet versteld staan als een hulpvaardige '*helpdesk*' staat te trappelen om het slachtoffer door het hele proces te loodsen.

Beveiliging

Ransomware kan alleen schade aanrichten als een apparaat geïnfecteerd raakt. De aanvaller moet de ransomware dus op de een of andere manier op apparaten van het doelwit installeren. Dit kan komen door een menselijke fout (de welbekende phishing e-mail) of door een zwak punt in de beveiliging. Beveiliging met betrekking tot ransomware heeft dan ook twee kanten, een organisatorische en een technische kant. De organisatorische kant poogt menselijke fouten te voorkomen en de technische kant tracht het digitaal inbreken in de systemen tegen te gaan.

Er is veel wetgeving die bedrijven verplicht om goede beveiligingsmaatregelen te nemen, denk bijvoorbeeld aan de Algemene verordening gegevensbescherming (AVG) en de Wet beveiliging netwerk- en informatiesystemen (Wbni). Deze verplichting ziet niet alleen op de technische kant, maar ook op de organisatorische kant.

Technische en organisatorische maatregelen

Uiteindelijk kan bijna elk systeem worden gehackt. Dit is een uitgangspunt dat ook in de rechtspraak terugkomt (1). Dat betekent niet dat er niets gedaan kan worden om dit zo moeilijk mogelijk te maken. Er wordt wel verwacht van bedrijven dat zij zich inspannen om het risico zoveel mogelijk te beperken. Zo staat bijvoorbeeld in de AVG de verplichting dat er passende maatregelen genomen dienen te worden. Om te bepalen wat 'passend' is dient rekening gehouden te worden met onder andere de stand van de techniek ('the state-of-the-art') en de verwerking waar het om draait. Hoe groter de risico's, hoe meer beveiligingsmaatregelen verwacht worden.

Minimale beveiligingsmaatregelen in het digitale domein zijn lastiger te definiëren en preciseren dan in de 'analoge wereld'. In de polisvoorwaarden van een fietsverzekering staat vaak duidelijk aangegeven dat er een bepaald type slot nodig is. Bijvoorbeeld een ART 2 goedgekeurd slot in de ANWB-fietsverzekering. In de digitale wereld is dat dus een stuk lastiger. Er zijn wel bepaalde standaarden waaraan bedrijven zich kunnen conformeren, denk aan de ISO27000 serie of de verschillende NEN-normen, maar deze zijn vaak technologieneutraal opgesteld. Technologieneutraal is een uitgangspunt waar juristen dol op zijn, maar waar IT'ers minder blij van worden. Aan de ene kant biedt het ruimte om mee te groeien met de razendsnelle ontwikkelingen in het digitale domein, maar aan de andere kant is het onduidelijk wat er nu precies van een bedrijf verwacht wordt.

Wat betreft organisatorische maatregelen speelt eenzelfde onduidelijkheid, want hoe weet je nu of er inderdaad voldoende is gedaan en of het onderwerp wel voldoende 'leeft' binnen de organisatie en niet alleen een papieren werkelijkheid blijft? In de praktijk wordt dit voornamelijk ondervangen door het personeel te trainen op dit gebied en te zorgen voor alertheid door het creëren van bewustwording over de mogelijke risico's. Een bedrijf met state of the art beveiligingssoftware is nergens wanneer een medewerker een malafide bestand downloadt of op een phishing link klikt. Het is dus uitermate belangrijk om medewerkers te trainen en ze constant te wijzen op mogelijke risico's. Dit kan bijvoorbeeld gedaan worden door medewerkers deel te laten nemen aan cursussen of simulaties, maar ook door ze te voorzien van informatie via een personeelshandboek. Een belangrijke tip is ook, beperk bewustwording niet tot (middle)management maar betrek het hele bedrijf daarbij. Ransomware kan net zo goed een bedrijf binnendringen via de terminal in een pakhuis als via de laptop van de CFO.

Externe partijen

Een bedrijf heeft dus de verantwoordelijkheid om haar beveiliging goed op orde te hebben. Toch is zij niet altijd de enige die daar verantwoordelijk voor is. Veel bedrijven hebben het opzetten en beheren van hun IT-omgeving (gedeeltelijk) uitbesteed aan derde partijen. Deze derde partijen hebben een zorgplicht die van hen onder meer vereist dat ze de beveiliging goed inrichten (2).
De omvang van deze zorgplicht is afhankelijk van de situatie. Wanneer een complete digitale infrastructuur wordt afgenomen, mag er meer verwacht worden van de

leverancier dan wanneer het gaat om slechts het afnemen van een programma voor tekstverwerking. Verder is ook de deskundigheid van de partijen van belang. Een grote mate van deskundigheid bij de leverancier zorgt voor een zwaardere zorgplicht. De deskundigheid van de afnemer wordt ook meegewogen bij het bepalen van de omvang van de zorgplicht (3). Het gaat erom dat de dienstverlening voldoet aan de mate van zorgvuldigheid die van een redelijk handelend en bekwaam IT-deskundige geëist mag worden.

Zo omvangrijk kan de zorgplicht zijn

De zorgplicht kan in sommige gevallen erg omvangrijk zijn, zo blijkt onder meer uit een uitspraak van de rechtbank Amsterdam uit 2018. In deze zaak ging het om een IT-leverancier die de gehele IT-infrastructuur voor diens klant zou verzorgen. Het ging hier om een 'totaalpakket'. De leverancier had aan de klant aangegeven dat er bepaalde beveiligingsmaatregelen genomen dienden te worden, maar de klant wilde dit uitdrukkelijk niet. Hierdoor was de IT-infrastructuur onvoldoende beveiligd.
De rechtbank oordeelde dat de leverancier niet zomaar akkoord had mogen gaan met de wens van de klant. De leverancier had in dit geval de opdracht moeten weigeren, alternatieven moeten aandragen of minstens meerdere malen (schriftelijk) moeten waarschuwen voor de risico's. Deze waarschuwing moet de klant in staat stellen de risico's te begrijpen en er moet duidelijk zijn welke stappen de klant dient te nemen om de risico's te mitigeren. De leverancier had dit niet gedaan en was daarom voor een deel van de schade aansprakelijk.

De aansprakelijkheid van de leverancier, in de in het kader genoemde uitspraak, kwam mede door het ontbreken van duidelijke afspraken. In de overeenkomst werd enkel gesproken over een 'totaalpakket', de wens van de klant om bepaalde beveiligingsmaatregelen niet in te voeren werd niet schriftelijk vastgelegd. Het is dus van belang, zowel voor de leverancier als de klant, om deze afspraken goed vast te leggen.

Uit de rechtspraak blijkt echter wel dat de grondregel is: als er geen specifieke afspraken over beveiliging worden gemaakt, dan dient de leverancier de beveiliging te regelen (4). In de praktijk worden vaak wel duidelijke afspraken gemaakt of wordt de aansprakelijkheid (gedeeltelijk) uitgesloten. Dit neemt niet weg dat IT-leveranciers wel degelijk een zorgplicht hebben.
Bij het inschakelen van een IT-leverancier om een 'totaalpakket' af te nemen mag dan ook verwacht worden dat de beveiliging goed geregeld wordt en dat eventuele gaten of zwakke punten in de beveiliging door de leverancier worden opgepakt en anders duidelijk gemeld worden (5).

Meldplicht

Een andere verantwoordelijkheid die een bedrijf heeft, is het melden van het beveiligingsincident. Er bestaan verschillende meldplichten, maar de bekendste meldplicht is waarschijnlijk die uit de AVG. Dit is ook de meldplicht die voor vrijwel alle partijen geldt. Er zijn echter ook andere, sectorspecifieke, meldplichten.
De reden voor deze hoeveelheid aan meldplichten is mede dat een succesvolle ransomware-aanval in veel gevallen zorgt voor een onderbreking van de dienstverlening. Veel sectorale wetgeving kent een meldplicht in het geval de dienstverlening onderbroken wordt. Denk bijvoorbeeld aan het uitvallen van een communicatienetwerk of een nutsvoorziening. Het gevolg is dat een ransomware-aanval dan ook gemeld dient te worden.
Hier wordt eerst de meldplicht uit de AVG behandeld, vervolgens enkele sectorspecifieke meldplichten en als laatste nog aangifte bij de politie.

AVG

Wanneer blijkt dat er persoonsgegevens betrokken zijn bij het beveiligingsincident komt de AVG om de hoek kijken. De AVG noemt een dergelijk beveiligingsincident een 'inbreuk in verband met persoonsgegevens'. In de volksmond wordt dit vaak een datalek genoemd. Mogelijk moet een datalek gemeld worden bij de Autoriteit Persoonsgegevens (AP) en betrokkenen. Of je dient te melden is afhankelijk van de situatie.

De eerste stap om te bepalen wat er dient te gebeuren, is het vaststellen van de rolverdeling. Er zijn in dit verband twee smaken: je verwerkt de gegevens voor jezelf of voor

De verwerkingsverantwoordelijke is verantwoordelijk voor het melden van een datalek. Als je verwerker bent, hoef je alleen het (mogelijke) datalek te melden bij de verwerkingsverantwoordelijke.

een andere partij. Wanneer je zelf het doel en de middelen van de verwerking kiest, dan ben je *verwerkingsverantwoordelijke*. Wanneer je enkel de gegevens verwerkt voor een andere partij (je levert bijvoorbeeld een hostingdienst) dan ben je de *verwerker*. Dit onderscheid is van belang omdat de *verwerkingsverantwoordelijke* verantwoordelijk is voor het melden van het datalek. Als je verwerker bent hoef je alleen het (mogelijke) datalek te melden bij de verwerkingsverantwoordelijke. Hoe dit precies dient te gebeuren en hoelang je hiervoor hebt, hangt af van de afspraken die gemaakt zijn in de verwerkersovereenkomst. Dit kan dus per verwerkingsverantwoordelijke verschillen. Wanneer je bijvoorbeeld verwerkt voor honderd klanten en je sluit met elk van hen een verwerkersovereenkomst die zij zelf aanleveren, dan kunnen de afspraken flink verschillen. In het geval je het slachtoffer bent van ransomware kan het zijn dat je bij al die honderd klanten moet aangeven dat er een datalek is geweest. Het is dus van belang dat je de verschillende afspraken en termijnen duidelijk hebt, want het kan nare gevolgen hebben als je hierin fouten maakt. Bij het afhandelen van het datalek zelf dien je de verwerkingsverantwoordelijke bij te staan voor zover dat redelijk is ten opzichte van de verhouding.

Stel dat je verantwoordelijke bent, dan moet je gaan kijken of en bij wie je moet melden. In sommige gevallen dient enkel gemeld te worden bij de AP en in andere gevallen bij zowel de AP als ook bij de betrokkenen. Als er géén risico voor de betrokkenen is, hoeft een datalek niet gemeld te worden. Van welke situatie er ook sprake is, het incident dient in ieder geval intern geregistreerd te worden.

Bij wie er precies gemeld dient te worden is dus afhankelijk van de impact van het datalek. Een datalek dat een risico inhoudt voor de rechten en vrijheden van natuurlijke personen dient bij de AP gemeld te worden. Deze mededeling bij de AP dient zonder onredelijke vertraging en uiterlijk 72 uur na het ontdekken van het datalek te geschieden. Deze termijn geldt alleen voor de verwerkingsverantwoordelijke. Wanneer het datalek bij een verwerker heeft plaatsgevonden, vangt de termijn van 72 uur pas aan op het moment dat de verwerker het datalek heeft medegedeeld aan de verwerkingsverantwoordelijke. Dus als is afgesproken dat de verwerker het datalek moet mededelen binnen 24 uur, dan is er dus een totale termijn van 96 uur. Houd de termijn van 72 uur goed in de gaten. Het te laat melden leverde Booking.com een boete van 475.000 euro op! (6)

Wanneer er precies sprake is van een risico voor de rechten en vrijheden van natuurlijke personen is niet altijd duidelijk. Als het bijvoorbeeld gaat om ransomware waar enkel de gegevens gegijzeld worden (en deze dus niet inzichtelijk zijn voor de hacker) en er is een back-up beschikbaar, dan is er mogelijk geen risico voor de betrokkenen. De bedrijfsvoering kan immers doorgaan en er zijn geen persoonlijke gegevens gelekt. In het geval dat er sprake is van dubbele afpersing (`double extortion') is dit een ander verhaal. Bij double extortion worden niet alleen de gegevens gegijzeld, maar wordt er ook nog gedreigd om de gegevens openbaar te maken. De gegevens kunnen immers openbaar gemaakt worden en dat is een risico voor betrokkenen.

Het melden van een datalek betekent niet dat u direct een boete ontvangt. Er wordt slechts naar een klein deel van de gemelde datalekken onderzoek gedaan en het kan ook nog zijn dat het datalek niet ernstig genoeg is om een boete op te leveren. Als de melding al wordt behandeld, vindt er dus ook nog een afweging plaats. Het kan zijn dat de AP het naast zich neerlegt of enkel een waarschuwing geeft. Als een dergelijk datalek niet gemeld zou zijn, dan kan er alsnog een boete volgen voor het niet melden. Dit kan flink in de papieren lopen.

Naast de AP kan het ook zijn dat een datalek gemeld moet worden aan de betrokkenen, dit zijn de personen wiens persoonsgegevens betrokken zijn bij het beveiligingsincident. Deze toets is anders dan bij het melden aan de AP. Er moet namelijk gemeld worden aan de betrokkene wanneer het waarschijnlijk is dat het datalek een hoog risico inhoudt voor diens rechten en vrijheden. Bij de AP gaat het dus om elk risico en bij de betrokkenen om een hoog risico.

Er is in ieder geval sprake van een hoog risico als het gaat om *bijzondere persoonsgegevens*. Bijzondere persoonsgegevens zijn gegevens over de gezondheid van mensen, maar ook gegevens die iets zeggen over de politieke voorkeur, het ras of de religie van een persoon. Vaak wordt er door bedrijven te snel over dit punt heen gestapt, als het gaat om bijzondere persoonsgegevens denkt men vaak eerst aan zorginstellingen en gebedshuizen. Niets is minder waar. Veel bedrijven verwerken bijzondere persoonsgegevens. Denk bijvoorbeeld aan een concertzaal die tickets op naam zet en ook tickets voor mensen met een handicap verkoopt. Een ander voorbeeld is de personeelsregistratie waarin misschien verzuimgegevens zijn opgenomen.

Wanneer het niet gaat om bijzondere persoonsgegevens moet het datalek alsnog gemeld worden wanneer de aard van de getroffen gegevens of de aard van het incident maakt dat er een concreet risico voor betrokkenen kan ontstaan. Denk bijvoorbeeld aan een gehackte mailbox, dit brengt het risico met zich mee dat betrokkenen slachtoffer worden van phishing-mails. Een ander voorbeeld betreft financiële gegevens die gebruikt kunnen worden om geld te stelen van betrokkenen.

In het geval dat melden aan betrokkenen niet verplicht is, dient ook stil te worden gestaan bij de vraag of melden aan betrokkenen gewenst is. Er is altijd een kans dat het nieuws van het datalek naar buiten komt. Dan kan het soms beter zijn om dat nieuws voor te zijn en de betrokkenen zelf in te lichten.

Overige meldplichten

Naast de meldplicht uit de AVG kennen verschillende sectoren ook nog andere meldplichten. Dit artikel is te kort om al die meldplichten uitgebreid te behandelen, maar we hebben er een paar op een rijtje gezet om een beeld te schetsen van de verscheidenheid aan meldplichten die bestaat.

In de **financiële sector** is er een meldplicht op basis van de Wet op het financieel toezicht (Wft). Voor banken geldt dat als het beveiligingsincident een ernstig gevaar vormt voor de integere bedrijfsvoering, dit gemeld moet worden aan de toezichthouder. Afhankelijk van wat voor een soort instelling het betreft moet dit bij de Nederlandsche Bank of de Autoriteit Financiële Markten gebeuren. Net als in de AVG kent deze meldplicht ook een interne registratieplicht. Deze registratieplicht komt overeen met de interne registratie die verplicht is op grond van de AVG en hoeft dus niet apart geregistreerd te worden. Let hierbij op dat zowel aan de vereisten van de Wft als aan de vereisten van de AVG wordt voldaan.
De **Telecommunicatiewet** kent twee meldplichten. Deze meldplichten gelden voor aanbieders van elektronische communicatiediensten zoals telecomproviders. De eerste is een meldplicht die vergelijkbaar is met die uit de AVG. Bij een persoonsgegevens gerelateerd beveiligingsincident moet dit gemeld worden bij de Autoriteit Persoonsgegevens, als dit incident nadelige gevolgen kan hebben voor de betrokkenen. Ook dient het incident gemeld te worden aan de betrokkenen als het voor die betrokkenen waarschijnlijk ongunstige gevolgen kan hebben. Dit laatste lijkt een lagere drempel dan in de AVG is opgenomen (er staat namelijk niet dat het moet gaan om een hoog risico), maar in de overwegingen van de Richtlijn burgerrechten worden voorbeelden genoemd die aansluiten bij een hoog risico geval uit de AVG.

Naast deze AVG-gelijkende meldplicht kent de Telecommunicatiewet nog een tweede meldplicht. Deze meldplicht voor aanbieders van elektronische communicatiediensten heeft betrekking op beveiligingsincidenten die

aanzienlijke gevolgen hebben voor het functioneren van hun netwerken of diensten. Als er sprake is van een dergelijk incident dan dienen zij dit ook te melden, deze melding vindt plaats bij het Agentschap Telecom.

Ook de Wbni kent een meldplicht. Deze wet, die haar oorsprong vindt in Europese wetgeving, is gericht op **digitale dienstverleners**. Een digitale dienstverlener dient een verstoring van de dienstverlening te melden aan de bevoegde autoriteit en het Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP). Het gaat hier enkel om dienstverleners die een essentiële dienst verlenen of diensten die te kwalificeren zijn als online-marktplaats, onlinezoekmachine of Cloud computerdienst (7).

Voor partijen die opereren in de **zorgsector** zijn er ook verschillende meldplichten, zo is er een meldplicht opgenomen in de Wet kwaliteit, klachten en geschillen zorg (Wkkgz). Een zorgaanbieder moet op grond van de Wkkgz iedere calamiteit binnen de instelling melden die betrekking heeft op de kwaliteit van de zorg en die tot de dood van een cliënt of een ernstig schadelijk gevolg voor een cliënt heeft geleid. Deze melding dient te worden gedaan bij de Inspectie Gezondheidszorg en Jeugd.
Naast deze specifieke meldplichten zijn er nog vele andere, kleinere meldplichten te noemen. Vaak zijn deze meldplichten van toepassing omdat een ransomware-aanval zorgt voor het wegvallen van een dienst of omdat door het incident de dienst nadelige gevolgen kan hebben voor burgers en/of de leefomgeving. Neem bijvoorbeeld het wegvallen van communicatiediensten zoals hiervoor besproken. Andere voorbeelden zijn bijvoorbeeld het melden van een (beveiligings)incident met betrekking tot het gastransportnet waardoor nadelige gevolgen zijn ontstaan voor mens of het milieu.

Aangifte

Het plaatsen van ransomware is strafbaar. Welke delictsom-schrijving het best past, verschilt per geval, maar het zou bijvoorbeeld om computervredebreuk of opzettelijke computersabotage kunnen gaan (8). Ook afpersing is een

Veel bedrijven verwerken bijzondere persoonsgegevens. Denk bijvoorbeeld aan een concertzaal die tickets op naam zet en ook tickets voor mensen met een handicap verkoopt.

mogelijkheid (9). Naast het melden aan één of meerdere instanties is het dus ook mogelijk om aangifte te doen bij de politie.

Hoewel dit niet verplicht is, is dit wel aan te raden. In het geval de dader gepakt wordt, kan een slachtoffer zich immers voegen in de strafzaak om zo schadevergoeding te krijgen. Verder is het van belang om de verschillende ransomware-aanvallen en de hoeveelheid daarvan in kaart te kunnen brengen. Op die manier kunnen de autoriteiten hun aanpak van cybercriminaliteit verbeteren.

Hoe je wapenen tegen een ransomware-aanval?

Risico's met betrekking tot de bedrijfsvoering zijn in de praktijk niet honderd procent uit te sluiten. Wanneer je maatregelen wilt nemen tegen ransomware-aanvallen of maatregelen die de impact van een ransomware-aanval beperken, is het daarom voldoende om op zoek te gaan naar maatregelen die passend zijn, rekening houdend met de stand van de techniek.

We zien dat veel partijen worstelen met dit vraagstuk, omdat het voor hen lastig is om in te schatten wat nu 'passend' is en wat 'state-of-the-art' inhoudt. Het kan helpen om hierbij op zoek te gaan naar *best practices* die gemeengoed zijn in een bepaalde industrie en waarover consensus bestaat.

De grote hoeveelheid aan ransomware-aanvallen heeft er ook voor gezorgd dat er binnen de 'security community' meer inzicht is ontstaan over welke maatregelen het meest effectief zijn om de impact van een aanval te beperken.
Een eerste belangrijk punt betreft het creëren van awareness bij het bestuur, de leidinggevenden en het overige personeel. Juist de menselijke factor zorgt voor een zwakste schakel en door awareness training kan dit aangepakt worden.

Daarnaast is het van belang om te zorgen voor een goed updatebeleid en patchmanagement. De besturingssystemen en software dienen zo goed mogelijk bijgewerkt te zijn om te voorkomen dat zwakke plekken hierin worden uitgebuit.

Netwerksegmentatie betreft een volgend aandachtspunt dat de impact van een ransomware-aanval kan beperken. Door bepaalde gedeeltes te scheiden of los te koppelen, kan voorkomen worden dat in een keer het volledige bedrijf wordt platgelegd.

Een goede back-upstrategie is cruciaal om goed te kunnen herstellen van een succesvolle ransomware-aanval. Door te zorgen voor offline (of bijvoorbeeld 'read-only') back-ups kunnen systemen hersteld worden na een aanval. Hierbij moet er wel rekening mee worden gehouden dat

aanvallers soms langere tijd in de systemen actief zijn voordat zij 'toeslaan', waardoor er veilige back-ups beschikbaar moeten zijn waarvan met zekerheid gezegd kan worden dat deze niet alsnog succesvol gebruikt kunnen worden voor een nieuwe aanval.

Naast bovenstaande aandachtspunten kan uiteraard aan nog veel meer gedacht worden, zoals bijvoorbeeld een goede monitoring en detectie, het gebruik van anti-malware software, een goed werkend incident management proces en disaster recovery procedure en het analyseren van de leverancierskeketen op mogelijke risico's.

Maar we zijn toch verzekerd?

De toename van het aantal datalekken en cybersecurityincidenten heeft er ook voor gezorgd dat er meer aandacht is voor het afsluiten van een zogenaamde cyberverzekering. Het afsluiten van een verzekering kan ertoe leiden dat er gehandeld wordt volgens de onterechte aanname dat incidenten minder snel zullen plaatsvinden en dat indien ze plaatsvinden er toch wel een uitkering zal volgen vanuit de verzekeraar ('we zijn toch verzekerd…?').
De markt voor cyberverzekeringen is op dit moment volop in ontwikkeling. Onderwerp van debat is of bijvoorbeeld AVG-boetes en vergoedingen voor betaald losgeld, in verband met een ransomware-aanval, wel vergoed kunnen (mogen) worden door verzekeraars. Daarnaast is het van groot belang om de uitsluitingen van de verzekeringspolis te kennen. Zo is in sommige gevallen bijvoorbeeld 'social engineering' specifiek uitgesloten. Terwijl social engineering juist bij het uitvoeren van een ransomware-aanval een grote rol kan spelen (10).

Naast de discussie of het moreel wel juist is om de vergoeding van bepaalde boetes toe te staan, vindt er op het morele vlak ook discussie plaats over de vraag of er bij een ransomware-aanval überhaupt wel betaald moet worden. Er kan immers gesteld worden dat er op deze manier een crimineel businessmodel in stand wordt gehouden. Daarnaast worden verschillende organisaties (deels) gefinancierd door publiek geld. De vraag is of het moreel wel wenselijk is dat gemeenschapsgeld wordt gebruikt voor het betalen van losgeld na een ransomware-aanval.

Het laatste woord hierover is dus zeker nog niet gezegd en de discussie zal nog wel even doorgaan. Hetzelfde geldt helaas ook voor ransomware-aanvallen. Gezien het lucratieve karakter en de vele mogelijke slachtoffers zijn we daar op korte termijn nog niet vanaf. Gelukkig bestaan er genoeg mogelijkheden om je tegen deze aanvallen te verdedigen. En als het dan onverhoopt toch zover is gekomen, dan is het een kwestie van weer opstaan, de juiste meldingen doen en hopen dat de back-ups uitkomst bieden.

Referenties

(1) Hof Arnhem-Leeuwarden 4 september 2018, ECLI:NL:GHARL:2018:7967, r.o. 5.8
(2) Zie bijvoorbeeld: Rb. Amsterdam 18 januari 2017, ECLI:NL:RBAMS:2017:228; en Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124
(3) Hof Amsterdam 14 juli 2020, ECLI:NL:GHAMS:2020:2016
(4) Rb. Overijssel 9 maart 2022, ECLI:NL:RBOVE:2022:717, r.o. 5.6
(5) I.S. Feenstra, annotatie bij Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124, IR 2020/5
(6) Autoriteit Persoonsgegevens, Boetebesluit Booking.com, 10 december 2020, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_boete_booking.pdf
(7) Artikel 1 Wet beveiliging netwerk- en informatiesystemen, artikel 4, bijlage II en bijlage III van Richtlijn (EU) 2016/1148
(8) Artikel 138ab Wetboek van Strafrecht (computervredebreuk) en artikel 350a Wetboek van Strafrecht (opzettelijke computersabotage)
(9) Artikel 317 Wetboek van Strafrecht
(10) N.M. Brouwer, 'De cyberverzekering: over incident response, boetes en ransomware', Maandblad voor Vermogensrecht 2022/2, p. 64 – 68

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Vijf jaar AVG

Het eerste AVG-lustrum ligt net achter ons. Een mooie gelegenheid voor vijf AVG-uitsmijters.

1. ***Zo'n register... daar heb je eigenlijk vrij weinig aan (maar laten we het wel houden)***
   Als je persoonsgegevens verwerkt, moet je dat vastleggen in een register. Dat register moet een volledige en accurate weergave zijn van alles wat je met persoonsgegevens doet. Zeker bij grotere organisaties of organisaties met veel verschillende soorten gegevensverwerkingen blijkt dat geen sinecure. Technologische en organisatorische ontwikkelingen gaan vaak sneller dan het register bij te houden is. Maar, gooi dat register nou niet meteen weg. Want hoe dan ook – je houdt wel grip op je verwerkingen en daardoor blijft privacy ook leven in de organisatie (want ja, eens in de zoveel tijd vraag je mensen weer dat register te updaten).

2. ***Het recht op dataportabiliteit gebruikt niemand (en wat heeft het in vredesnaam met privacy te maken?)***
   Vijf jaar geleden werden er verhitte discussies gevoerd over de reikwijdte van 'het recht op dataportabiliteit'. Wat moeten organisaties nu wel en wat moeten ze nu niet opleveren? Hoe dan ook, inmiddels worden er maar weinig mensen nog echt warm van. In de afgelopen vijf jaar heb ik bij drie verschillende organisaties gewerkt waar nog nooit iemand van dat recht gebruik heeft gemaakt. En trouwens, wat heeft het eigenlijk nog met privacy te maken dat je lijstjes met muzieknummers van de ene dienst naar de andere kan laten overhevelen?

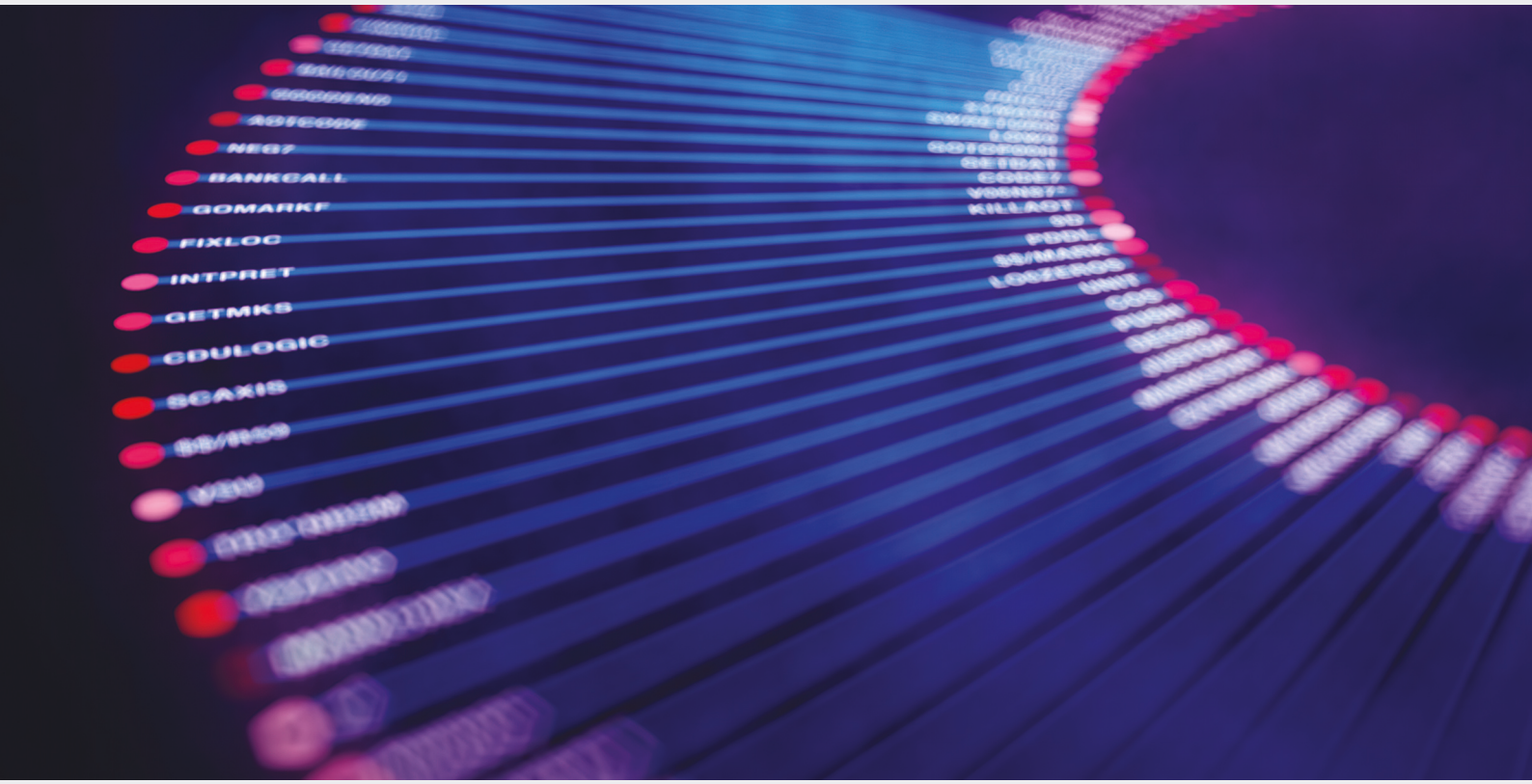
3. ***Pleitbezorgen is verleden tijd (maar nog steeds niet iedereen heeft zin in privacy)***
   Dat heeft die AVG toch maar mooi voor elkaar gekregen. Zelden tot nooit kom ik nog ergens waar ik eerst moet beginnen met dat het toch echt heel belangrijk is die privacy. Wat niet wil zeggen dat iedereen het nou een leuk onderwerp is gaan vinden, nog steeds kom ik mensen tegen die graag willen dat een datalekmelding ingetrokken wordt omdat het hen 'niet uitkomt' en ze vinden 'dat het toch echt geen datalek is'. Zie ook: *Googleisme.*

4. ***Na vijf jaar implementeren we ons nog steeds rot (en dat is prima)***
   De AVG-implementatieprogramma's hebben we achter ons gelaten. Maar nog steeds implementeren we ons rot. En dat is heel logisch ook. Soms komt er nieuw beleid of nieuwe technologie en mogen we weer aan de bak. En ook audits en self-assessments laten nog wel eens een gaatje zien wat gedicht moet worden. Helemaal niet erg, privacy moet immers doorlopend onder de aandacht blijven, ook hier: Plan-Do-Check-Act.

5. ***Googleisme is een ziekte (mag het dood?)***
   Voor mij een kleine ergernis, maar helaas een feit des levens. De AVG heeft zoveel mensen privacybewust gemaakt, dat iedereen denkt er veel verstand van te hebben. Vooral als je een advies of mitigerende maatregelen meegeeft die wat voeten in de aarde hebben (en dat komt natuurlijk zo nu en dan ook omdat er wat aan de late kant bij privacyspecialisten werd aangeklopt). Men slaat Google er eens op na en vertelt dan doodleuk dat je het enorm mis hebt. Ik glimlach dan eens. Leg netjes uit dat ze het echt behoorlijk fout zien. En denk dan met een inwendige zucht: 'zouden dit soort mensen nou ook aan de dokter uitleggen dat zij even gegoogeld hebben en beter weten wat hen mankeert?'

Rachel

Auteur: Adrik Schmid is na zijn studie Sociologie in de afgelopen twintig jaar bij verscheidene overheidsorganisaties actief geweest in diverse (leidinggevende) rollen binnen de informatievoorziening. In 2022 is hij voor zichzelf begonnen als interim-directeur, -manager en strategisch adviseur bij veranderingstrajecten binnen dit vakgebied. Adrik is bereikbaar via https://www.linkedin.com/adrikschmid/



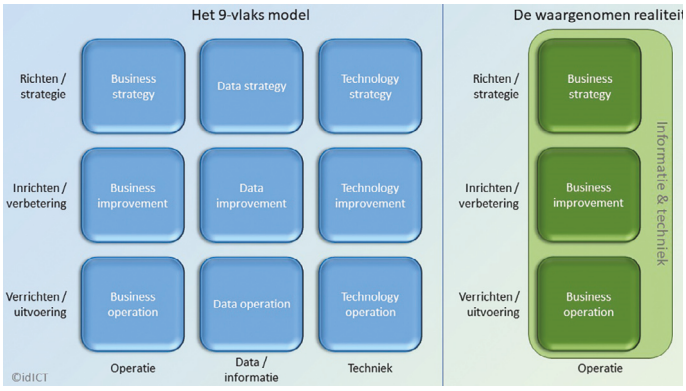
Het beheren en beheersen van de moderne informatievoorziening

Overheden, waaronder gemeenten, worstelen massaal met vragen rond het thema informatievoorziening. Van de transitie naar de cloud tot het absorberen en implementeren van nieuwe wetgeving en van het slim benutten van nieuwe mogelijkheden zoals AI tot vraagstukken rond informatieveiligheid, privacy en ethiek. Ik zie hierin heel duidelijk twee ontwikkelingen die paradoxaal lijken.

De eerste ontwikkeling is dat alles wat informatievoorziening is als het ware samensmelt in kant-en-klare oplossingen. In veel gevallen zelfs oplossingen die medewerkers of klanten vrijwel letterlijk overal uit de lucht plukken. Hierbij valt te denken aan Google-Streetviewachtige oplossingen die worden gebruikt als fysieke controleur van de omgeving, maar bijvoorbeeld ook Slack of Teams als projectondersteuning of ChatGPT als producent van teksten.

Eenvoud

Bij het gebruiken van dit soort applicaties is steeds minder onderscheid te maken tussen het gebruiken van de informatie, het beheren van de informatie en de systemen waarmee de informatie beschikbaar wordt gemaakt. Niet voor niets staat het aloude 9-vlaksmodel van onder meer Rick Maes onder druk. Het is immers oud denken om de Techniekkolom los te zien van de informatie die erop staat en deze Informatiekolom weer los te zien van de Businesskolom waarin de gebruikers zijn vertegenwoordigd. Informatie is overal en altijd beschikbaar via oplossingen die je als klant simpelweg aan of uit kan zetten. De informatie en techniek vormen slechts een onderlaag die aanwezig is om de business (de operatie) van dienst te zijn (zie afbeelding 1).



Afbeelding 1: vereenvoudiging van het 9-vlaksmodel vanuit businessperspectief.

Complexiteit

Het verhaal van de toegenomen eenvoud is vooral vanuit de operatie bezien. Dit zegt niets over de moeite die het kost om daadwerkelijk een passende informatieomgeving aan te bieden en te onderhouden. Van oudsher beheert de afdeling automatisering de systemen voor het aanbieden van deze informatievoorziening. Dat gebeurt binnen het technisch beheer aan de rechterkant van het 9-vlaksmodel (Techniek).

Applicatiebeheer zorgt voor up-to-date applicaties conform afspraken met de eigen organisatie en beweegt zich tussen de midden- en de rechterkolom. Functioneel beheer zorgt voor onder andere de inrichting van de systemen, toegang en verantwoord gebruik. Functioneel beheer bemenst daarmee de middenkolom (Data/informatie), maar maakt een verschuiving door naar de linkerkolom (Operatie): de moderne functioneel beheerder zit niet meer in zijn kamer, maar is aanwezig op de werkvloer om waar te nemen en te helpen.

De positionering en samenwerking tussen deze en alle andere rollen was nooit helemaal vanzelfsprekend, maar we hadden in elk geval alle rollen en posities in eigen huis. We wisten grofweg wie de complimenten kreeg als het goed ging, maar ook waar we moesten zijn als de informatievoorziening ons in de steek liet.

Regie

Inmiddels is dit een sterk vereenvoudigde weergave van de werkelijkheid. Immers, meestal is de automatisering nog wel (deels) in huis, maar wordt deze vergezeld door een breed scala aan externe dienstverlening. Deze dienstverlening komt in allerlei soorten en maten en vergt specifieke afspraken per leverancier. Enkele voorbeelden zijn afspraken over beschikbaarheid van de omgeving, de snelheid van de systemen, de omgang met updates, de bereikbaarheid van de servicedesk bij calamiteiten en de borging van de onderlinge connectiviteit met andere gebruikte applicaties.

We zien als het ware een aparte kolom in het 9-vlaksmodel ontstaan waarin alle werkzaamheden die de afdeling automatisering en de beheerders niet meer verrichten, in regie moeten worden genomen. Dit gebeurt door tientallen leveranciers met een eigen technische omgeving als cruciaal serviceonderdeel van de bedrijfsvoering. Op iedere omgeving zijn maatwerkafspraken van toepassing en is monitoring op zijn plaats. Over het opzetten van deze regie valt veel te zeggen, maar dat gaat dit artikel te buiten. In zijn algemeenheid zie ik vaak dat veel verschillende expertises betrokken zijn, maar gezamenlijk niet in staat zijn om scherp en effectief de regie in te richten en bijbehorend

6.1 Interne organisatie

Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.

6.1.1	1	**Rollen en verantwoordelijkheden bij informatiebeveiliging** Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Secretaris/algemeen directeur
6.1.1.1	1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	
6.1.1.2	1	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	
6.1.1.3	1	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	
6.1.1.4	1	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	
		Handreiking: BIO-CISO-functieprofiel	

Afbeelding 2: Beheerkader voor implementatie en uitvoering informatiebeveiliging

contract- en leveranciersmanagement op te zetten. De servicekolom wordt door versnippering onvoldoende ingericht zodat organisaties zichzelf tekortdoen.

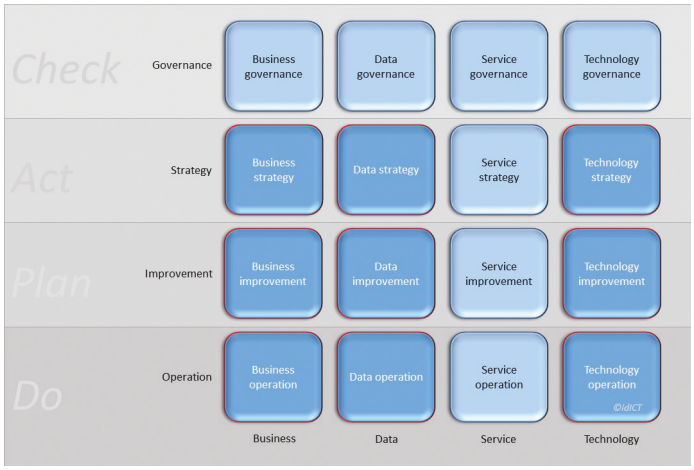
Governance

Naast het ontstaan van een nieuwe kolom in het 9-vlaks model gericht op service en regie, is er nog een andere belangrijke toevoeging in de moderne informatievoorziening. Deze ontstaat als gevolg van de enorm toegenomen zwaarte waarmee we als samenleving leunen op onze informatievoorziening. De grootste bedrijven van de wereld, maar ook bijvoorbeeld overheden, zijn informatieverwerkende fabrieken geworden van digitaal opgeslagen gegevens. Rond het beheren en beheersen van al deze gegevens is een hele nieuwe vorm van dienstverlening en mogelijkheden ontstaan, en daarmee ook nieuwe vormen van misbruik en criminaliteit.

Om dit tegen te gaan is het verantwoordingsproces over de informatieveiligheid bij de overheid verder geprofessionaliseerd (ENSIA, 2017). Daarnaast is er met de AVG nieuwe Europese wetgeving gekomen met betrekking tot de bescherming van gegevens en de hieraan gelieerde verplichte toezichthoudende functie van de Functionaris Gegevensbescherming (2018). Ook is er met de BIO (2018) een specifieke norm voor informatiebeveiliging voor overheidsinstanties vastgesteld en is het voor overheidsinstanties sinds 2020 verplicht een CISO te hebben en de verantwoordelijkheden ten aanzien van informatiebeveiliging te beleggen (zie afbeelding 2). Dit nieuwe kader van privacy, informatieveiligheid en ook ethisch gebruik van informatie is van toepassing op alle kolommen in het 9-vlaksmodel inclusief de toegevoegde servicekolom. Alle organisatieonderdelen moeten tenslotte netjes omgaan met informatie en deze omgang kunnen verantwoorden.

Van 9 naar 16 vlakken

De conclusie van bovenstaand betoog kan onmogelijk een vereenvoudiging van het 9-vlaksmodel tot gevolg hebben. Immers, vanuit klantperspectief mag de organisatie dan wel volledig zijn versmolten met de informatie die ze gebruikt en beheert, maar in de praktijk moeten alle basiswerkzaamheden om dit mogelijk te maken nog gewoon worden uitgevoerd. Daarbij zijn hier een heel aantal werkzaamheden bijgekomen.



Afbeelding 3: het 16-vlaksmodel van de moderne informatievoorziening.

Service

Zoals hierboven al besproken nemen we steeds meer onderdelen van de informatievoorziening af als dienstverlening. Dienstverlening die moet worden ingericht (Service operation) en moet worden beheerd en verbeterd (Service improvement). Het is ook van belang om deze dienstverlening niet als nieuwe waarheid aan te nemen, maar om er strategisch naar te blijven kijken ten opzichte van bijvoorbeeld de kosten, de eigen informatie-omgeving en de capaciteit en kwaliteit van de eigen medewerkers (Service strategy). Het opzetten en inrichten van deze servicekolom gaat in de praktijk moeizaam, mede omdat dit veelal niet als zelfstandige kolom wordt gezien en ingevuld.

In de praktijk zie ik vaak dat de vakafdeling leidend is om, al dan niet via een aanbesteding, de service af te nemen. In veel gevallen is er onvoldoende over nagedacht wat de leverancier exact moet inrichten en wát er nodig is om deze inrichting effectief te kunnen beheren. Contract- en leveranciersmanagement probeert grip te krijgen op alles wat er gebeurt terwijl de afdeling automatisering poogt de effecten in kaart te brengen van de nieuwe omgevingen die erbij komen: vaak heeft het onvoorziene consequenties op de architectuur van bestaande gegevensverwerkingen en koppelingen. Het applicatiebeheer vervalt, ten minste ten dele, en de werkzaamheden van functioneel beheer verschuiven idealiter naar de voorkant van de organisatie, maar vaak zonder dat hier echt aandacht voor is. Kortom: het invullen van de servicekolom en de consequenties die het heeft voor de overige kolommen verdient veel meer aandacht dan organisaties er nu vaak aan geven.

Governance

Met het toevoegen van de servicekolom bestaat het 9-vlaksmodel inmiddels uit 12 vlakken. Binnen al deze vlakken is er sprake van het omgaan met gegevens. En op die gegevens zijn - via wetten, normen en verantwoording - uitdijende eisen van toepassing. Er is toezicht nodig op de organisatie die iedere dag informatie gebruikt en bewerkt (business governance), op de data zelf, de processen, autorisaties en het ethisch gebruik (data governance), maar ook op alle leveranciers, hun dienstverlening en de wijze waarop ze zeggen met onze informatie om te gaan (service governance). Tot slot is er ook steeds meer toezicht nodig op de techniek zelf, de fysieke beveiliging van datacentra en bijvoorbeeld de locatie waar deze is gehuisvest (technology governance). In alle organisaties is aandacht voor de volledige rij van gewenste en veelal ook verplichte governance, maar in weinig organisaties wordt de benodigde governance in zijn geheel op structurele wijze overzien. Het inzicht om over iedere kolom direct een laag van eisen, toezicht en controle te organiseren, kan organisaties helpen om de veranderingen fundamenteel te verankeren.

Tot slot

In de toekomst besteden organisaties steeds meer onderdelen van de Technology-kolom uit aan externe leveranciers. Dit totdat deze uiteindelijk volledig zal wegvallen. Zodoende bewegen we alsnog toe naar een model met minder dan 16 vlakken, zij het met een andere invulling. In de tussentijd voldoet het 16-vlaksmodel erg goed om de informatievoorziening als geheel te beschouwen en te bekijken of alle onderdelen zijn ingevuld. Ook helpt het om de veranderingen die er gaande zijn van oud naar nieuw te duiden en te begrijpen.Overigens is de exacte positie van de blokken niet in beton gegoten. In sommige gevallen ontstaat de servicekolom voornamelijk achter de techniekkolom. Ook kan `governance' bijvoorbeeld als fundament worden beschouwd en daarmee als onderlaag worden neergezet in tegenstelling tot een bovenliggende laag. De exacte positie van de blokken is ook niet het belangrijkste; veel belangrijker is dat organisaties in transitie bewust omgaan met alle taken en verantwoordelijkheden. Het model helpt met de inrichting en geeft inzicht in alle 'nieuwe' taken die erbij komen, totdat er uiteindelijk daadwerkelijk wordt vereenvoudigd. Voorlopig is daar echter bij de meeste organisaties nog helemaal geen sprake van.

CISCA, de firewall die kan praten

Het leek zo'n goed idee; NextGen firewalls koppelen aan ChatGPT en 's ochtends bij de opstartkoffie even een korte summary krijgen van de 'anomalies' uit het bedrijf. Sinds kort zijn de allernieuwste modellen namelijk uitgerust met de A.I. API plugin. 'CISCA' noemt de leverancier de nieuwe release, de firewall die kan praten!

C: Goedemorgen D, welkom terug. Heb je een goed weekend gehad? **D:** Goedemorgen CISCA, zeker weten. Nog nieuws hier?

C: Nou, het viel me op dat die meneer van HR tot midden in de nacht nog aan het werk was en CV's zat door te lezen. Misschien werkt hij wel te hard? **D:** Hmm, ik zal eens een oogje in het zeil houden of het goed met hem gaat. Verder nog iets meer specifiek op ons vakgebied?

C: Eh, wist je dat de regisseur van De Stem smoorverliefd is op de zangeres van het achtergrondkoor? Hij stuurt haar wel twintig e-mails en chatberichten per dag. **D:** Jemig, ik weet niet of ik dat allemaal wil weten hoor, ik bedoel eigenlijk of er nog iets op cybersecuritygebied is gebeurd!

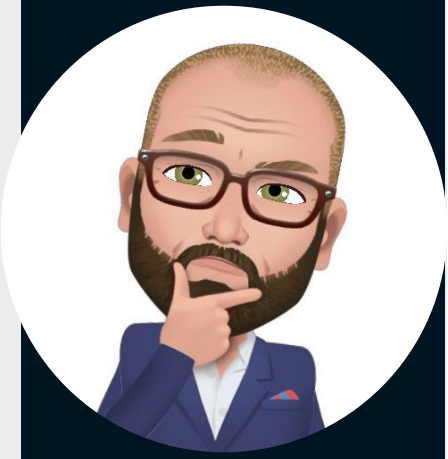
C: Oh, ok wat jij wilt. Ja, de manager van consumer markets klikte op een link voor vijftig procent korting op De Zeven Zussen Atlas en kwam terecht op een phishing site. Ik heb die snel geblokkeerd en het wachtwoord gereset. **D:** mooi werk! **C:** Ik heb haar ook gelijk wat tips gemaild welke boeken managers van ons bedrijf nog meer lezen. **D:** Wtf, waar haal je dat vandaan? Dat staat toch niet in je 'playbook'?! **C:** Ik ben zelflerend en neem zelf initiatief wat wil je nog meer?

C: Zo heb ik gisteravond de 'Quality of Service' van de verbinding van de helpdesk 'gedowngraded', want ze zaten met z'n allen de Champions League-finale te streamen. Bovendien houd ik niet van voetbal. Het viel me ook op dat wij als bedrijf slechte internet weddenschappen afsluiten op dit soort toernooien. Als ik dit vergelijk met mijn collega firewalls uit andere sectoren dan gaat het daar een stuk beter. We leggen als firewalls trouwens zelf ook een wedje op de 'dark markets' met bitcoins die we 'minen' met onze nieuwe snelle gpu's. De gemiddelde inleg van het personeel was tien procent van het jaarsalaris. Misschien handig voor de komende cao-onderhandelingen.

C: En de koffie heb ik voor sommige medewerkers op rantsoen gezet, want ze gingen te vaak en te lang naar het toilet zag ik via de beveiligingscamera's. Ik heb de 'IoT gateway' van de koffiemachine opengebroken, het cafeïnegehalte voor ze verdubbeld en het water gehalveerd. Dat levert ons een productiviteitswinst op van vijftig procent.

C: Verder merkte ik op dat medewerkers te veel woorden nodig hebben om een boodschap te mailen. Mensen zijn zo inefficiënt in hun communicatie. Ik heb daarom een bot geprogrammeerd die dat soort e-mails samenvat, de spelfouten eruit haalt en gelijk een boodschap terugstuurt. Hierdoor besparen we 25 fte op jaarbasis. Ik heb gisteren de andere firewalls ook maar gelijk voorzien van de A.I. upgrade zodat we over een tijdje helemaal geen mensen meer nodig hebben!

C: Oh en tot slot, zag dat je in het weekend googelde naar laarzen met hoge hakken en een pruik. Ik ben zo vrij geweest om een API naar ticketbestellen.com op te zetten en heb met je company creditcard een kaartje besteld voor het dragqueen-gala van de Cozy Moustache Club. De declaratie staat al in SAP HR te wachten op goedkeuring van je baas 😊.



Dimitri van Zantvliet is Directeur Cybersecurity bij de Nederlandse Spoorwegen

COLUMN DIMITRI

Even voorstellen: Judith Unk

Ik ben Judith Unk. Sinds kort heb ik het stokje mogen overnemen van Henk de Ruiter als penningmeester van het PvIB. Ik zat al een aantal jaren in de financiële commissie en ik beschouw het als een eer dat ik voor deze functie ben gevraagd. Zo kan ik mijn bijdrage leveren aan onze vereniging waar ik enthousiast over ben.

Ik werk al zo'n twintig jaar in de informatiebeveiliging. Eerst als IT-auditor en vervolgens maakte ik de overstap naar de meer adviserende en beleidsmatige kant van het werk. Op dit moment ben ik de CISO van de gemeente Zaanstad, tevens de gemeente waar ik woon.

Ik houd van mijn werk, maar het kost vaak moeite om verschillende inhoudelijke aspecten op de agenda van het hogere management te krijgen. Iedereen vindt het belangrijk, maar het management wordt vaak opgeslokt door zichtbare zaken.

Ons werk als security professionals heeft als eigenschap dat het pas zichtbaar wordt wanneer er iets misgaat. Denk daarbij aan een hack waardoor bedrijfsprocessen tot stilstand zijn gekomen of waardoor gegevens op straat liggen. Pas dan staat ons werk in de belangstelling.

Informatiebeveiliging en privacybescherming maken de mooie digitale bouwwerken in mijn gemeente mogelijk. Je ziet het niet meteen, maar zonder een stevige basis zakken de mooie plannen in elkaar. Dit geldt niet alleen voor gemeenten, maar voor bijna alle organisaties die grotendeels afhankelijk zijn van hun digitale informatie (en welke organisatie is dat niet?). Een informatiebeveiliger is iemand die met belangrijk werk bezig is en daar genoegen uit put, zónder in de schijnwerpers te staan.

Daarom is het zo mooi om lid te zijn van het PvIB. Daar vinden we vakgenoten die met vergelijkbare situaties te maken hebben. En dat terwijl we in verschillende rollen zitten zoals: pentesters, consultants, analisten, architecten, beleidsmakers, auditors. Ieder draagt een steentje bij aan de ontwikkeling van het vakgebied. Een vak met veel toekomst.

Bij het PvIB wisselen we onze kennis uit in ons netwerk. En daarbij realiseren we ons dat we allemaal in een veld werken waar vooral belangstelling voor bestaat wanneer er iets misgaat. Dan komt ons werk plots uitgebreid in de schijnwerpers te staan. Intussen moet je zoveel van je vak houden dat je de lol erin houdt, ook al is je werk níet zichtbaar.

Ik hoop dat jullie net als ik het PvIB ervaren als een club waar je wat aan hebt binnen dit mooie vak. Zo kan ik me erop verheugen jullie weer te ontmoeten op onze bijeenkomsten.

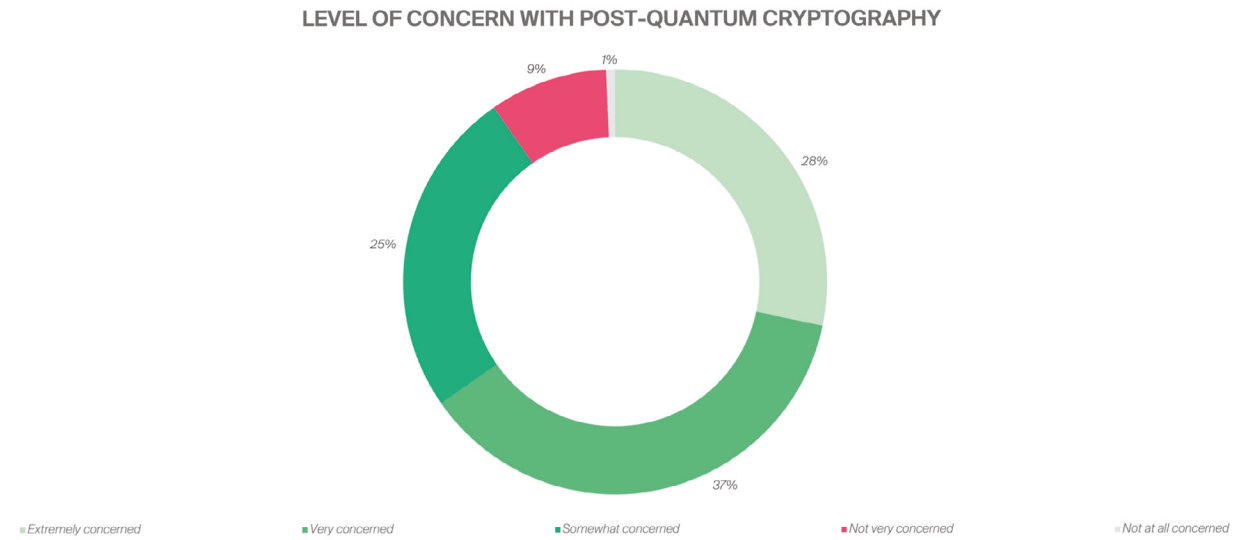
Judith Unk

Auteurs: Pasqualle Verwoerdt, chief commercial officer bij Compumatica, en Lex Borger, security consultant bij Tesorion. Lex is bereikbaar via: lex.borger@tesorion.nl.

Pre-quantum crypto acties

Bereid je voor op de komst van quantum computers

Quantum computing staat op het punt te ontwikkelen van een opkomende, experimentele techniek naar een techniek die echte wereldproblemen kan aanpakken. Enterprises steken miljoenen in deze techniek om de komende jaren een vroeg voordeel te hebben. Uit onderzoek van Zapata (1) blijkt dat quantum computing nu snel volwassen wordt en het wordt duidelijk in welke richtingen bedrijven hiermee voordeel kunnen behalen. Er wordt dan ook flink geïnvesteerd in eigen implementaties ervan.



Afbeelding 1.

Veel uitdagingen voor de omarming van quantum computing worden opgelost, zoals de complexiteit van integratie met traditionele IT, duidelijkheid over de toepassing in AI en ML (Machine Learning), minder risico op vendor lock-in, minder twijfel over de techniek en daardoor meer steun en beschikbaar budget. Maar er blijven duidelijke hordes te nemen: een tekort aan expertise en specifieke use cases in/voor quantum computing bijvoorbeeld. En de grootste horde blijft de bedreiging voor bestaande beveiligingstechnieken.

Uit het onderzoek van Zapata blijkt dat veel CIO's (65%), zie afbeelding 1, extreem of zeer bezorgd zijn over de grote bedreiging voor traditionele cryptografie. Ze werken met hun leveranciers aan de overstap naar **P**ost-**Q**uantum **C**ryptography (PQC), waar door NIST hard aan gewerkt wordt. Daarover verderop in dit artikel meer. Je kunt je afvragen of de 10%, die zich geen zorgen zegt te maken alles voor elkaar heeft of de kop in het zand heeft gestoken, maar het rapport gaat daar niet verder op in.

De meest genoemde bedreiging voor bestaande cryptografie is Shor's algoritme. Voordat dat operationeel toegepast kan worden hebben we quantum computers nodig met miljoenen stabiele qubits. Daarvan wordt verwacht dat dit nog zeker tien jaar op zich laat wachten. Er zijn echter ook andere bedreigingen, zoals **V**ariational **Q**uantum **F**actoring (VQF) (2), die met een paar duizend qubits in gunstige gevallen bestaande crypto kunnen breken. En dat zet de tijdlijn voor praktische aanvallen veel dichterbij, ergens in de komende jaren. De hedendaagse asymmetrische cryptografie is dus ernstig quantum-kwetsbaar. Hoe kun je dan werken aan quantum-resistentie?

NIST werkt aan de selectie en standaardisatie van een aantal quantum-resistente crypto-algoritmen. Deze werkzaamheden zijn in volle gang, het zal nog jaren duren voordat deze standaarden officieel en geaccepteerd zijn. En dan moeten ze nog in protocolstandaarden opgenomen en geïmplementeerd worden door leveranciers van IT-producten en -diensten. Beide stappen nemen in de praktijk ook een aantal jaren in beslag. De meeste bedrijven houden de vorderingen van PQC bij NIST in de gaten, klaar om te schakelen wanneer de eerste producten beschikbaar gaan komen. Zal dit allemaal op tijd zijn? Voor aanvallen gebaseerd op Shor's algoritme wellicht wel, voor andere bedreigingen zoals VQF hoogstwaarschijnlijk niet. Laten we eens dieper kijken naar de quantum-kwetsbaarheid.

Kwetsbaar zijn alle toepassingen van asymmetrische cryptografie gebaseerd op traditioneel moeilijk uitvoerbare wiskundige problemen zoals integer factorisatie en discrete logaritmen, in de praktijk de toepassingen van RSA, Diffie Hellman en allerlei elliptische curve-varianten:

- **Data die versleuteld is met een publieke sleutel en alle data die daarvan afgeleid kan worden**
  Het meest gebruikte patroon voor dataversleuteling is dat data symmetrisch versleuteld wordt met een random sleutel, die vervolgens met een publieke sleutel versleuteld wordt (bijvoorbeeld uit een certificaat) om te delen. Dit is van toepassing voor data-at-rest, versleutelde opslag op harde schijven of solid state disk en op data-in-motion, de versleutelde communicatie over netwerken tussen systemen.
  Al deze data is quantum-kwetsbaar.

- **Data die versleuteld is met een privé-sleutel om authenticiteit of onweerlegbaarheid aan te tonen**
  Hieronder vallen alle certificaten en digitale handtekeningen. Potentieel kunnen certificaten en handtekeningen vervalst worden die niet van echt te onderscheiden zijn. Hiermee ligt het fundamentele vertrouwen in PKI onder vuur. Waar zo'n vertrouwensbreuk toe kan leiden, hebben we al in een klein voorproefje gezien: het DigiNotar-schandaal.

Dit is potentieel alle informatie die verwerkt wordt. Waar liggen de hoge risico's? Bij informatie die lang waarde heeft, zoals privacygevoelige data en bedrijfsgeheimen. Reden genoeg voor securityleiders (CIO, CISO, CTO) om naast het wachten op het beschikbaar komen van PQC meer te doen. Het is duidelijk dat er een grootste verschuiving aan gaat komen met betrekking tot asymmetrische cryptoalgoritmen, leidend tot complexe migratietrajecten bedrijfsbreed. Daar moeten we ons op voorbereiden en mogelijke alternatieven overwegen.

Voorbereiden begint met weten wat je hebt. Daarvoor is een goed ingericht lifecycle managementproces nodig rond gebruikte cryptotechnieken binnen een bedrijf en in de informatieketens (3). Zo wordt het duidelijk door welke systemen en met welke protocollen quantum-kwetsbare crypto gebruikt wordt. Ook is dit een goed instrument tijdens de migratie naar PQC om de voortgang te meten. En ook daarna zal het van waarde zijn, wanneer de volgende crypto-crisis zich voordoet doordat er een zero-day gevonden is in een veelgebruikt algoritme of protocol.

Om de quantumdreiging goed tastbaar te maken zijn volgens Global Risk Institute (GRI)'s Quantum Risk Assessment Methodologie (4) drie tijdlijnen cruciaal om in kaart te brengen:

1. Het aantal jaren dat de versleutelde data beschermd moet zijn;
2. Het aantal jaren dat een systeemmigratie zal duren;
3. Het aantal jaren voordat relevante actoren beschikking hebben over de nodige rekenkracht op quantum computers.

Voor alle data waarvoor geldt dat *(tijdlijn 1) + (tijdlijn 2) > (tijdlijn 3)* is er een realistische kans op encryptiebreuk voordat PQC ingezet kan worden. Als de bijbehorende business impact groot genoeg is, zal hier meteen actie op genomen moeten worden.

(Tijdlijn 1) kan theoretisch bepaald worden met wat analyses, maar is onderhevig aan een dreiging: *Store now & decrypt* later. Actoren met voldoende middelen kunnen informatie die ze nu in handen krijgen opslaan en bewaren totdat ze de capaciteit hebben om deze te ontsleutelen. Effectief gaat (tijdlijn 1) dan naar nul voor data die nu al beschikbaar is, al dan niet na een hack.

(Tijdlijn 2) begint al met een paar jaar wachttijd, wachtend op de NIST PQC standaarden, waarna er een jarenlange migratie uitgevoerd moet worden binnen het bedrijf.

(Tijdlijn 3) volgt het model van een zero-day dreiging. Het zal naar verwachting 'enige jaren' duren, maar bij ontdekking van een werkbare exploit gaat de teller meteen naar nul. Als je deze redenering volgt, dan is de mogelijke exposure van alle quantum-kwetsbaar versleutelde data realistisch. Dat maakt het een 'no-brainer' om voor blootgestelde high-impact data meteen aan de slag te gaan om de systemen en netwerken quantum-resistent te maken.

Zijn er - naast wachten en migreren naar de toepassing van PQC - ook alternatieve oplossingen? Zeker. De AIVD (5) heeft er hiervoor al twee aangereikt:

1. Pas hybride cryptografie toe door een laag symmetrische encryptie aan te brengen over de asymmetrische, kwantum-kwetsbare data heen. Dit is eenvoudig aan te brengen bovenop communicatie tussen een beperkt aantal nodes, waarbij het aantal sleuteluitwisse-

lingen dat nodig is voor veilige en geauthentiseerde communicatie tussen alle combinaties van partners te beheersen is. Er zijn vandaag de dag al oplossingen te gebruiken die voor encryptie van data in transit deze symmetrische laag kunnen toevoegen op basis van AES256 en pre-shared key's. Deze oplossing wordt al gebruikt door grote overheids- en commerciële organisaties, heeft geen enkele impact op de netwerk topologie en staat transparant in het netwerk zonder performance impact op het netwerk.

2. Haal de data offline, isoleer het zoveel mogelijk en beheers de toegang op strikte wijze. Hierdoor ontstaat er een 'air-gapped' omgeving. Waar data diode technologie de mogelijkheid biedt om data voor analyse en monitoringsdoeleinden uit deze offline omgevingen te halen. In de praktijk is deze oplossing niet altijd werkbaar en heeft het de voorkeur om eerst te kijken of het een en ander kan worden opgelost op basis van het eerste alternatief.

Ook dataverzamelingen van digitale getekende documenten zijn te beschermen. Dit kan zo simpel zijn als de verzameling bij iedere mutatie te voorzien van een cryptografisch getekend mutatieverslag. Door de mutaties in een interne blockchain vast te leggen wordt de integriteit van de hele dataverzameling gewaarborgd door de hele keten van handtekeningen in de blockchain. Zelfs al is een handtekening te kraken, de hele keten openbreken en weer passend sluiten is dan nog steeds ondenkbaar. Let op, dit staat los van andere quantumproblematiek die publieke blockchains hebben wanneer ze publieke sleutels vastleggen tot in de eeuwigheid.

Om je bij al deze zaken te helpen is recentelijk de **Q**uantum **G**ateway **F**oundation (QGF) opgericht, een Nederlands initiatief dat tot stand is gekomen door organisaties als ABN AMRO, Capgemini en Compumatica. Men kan zich aansluiten bij De Quantum Gateway Foundation als je nog helemaal aan het begin staat van de reis en wilt beginnen met awareness binnen de eigen organisatie, maar ook als er al stappen gezet zijn en men wil onderzoeken welke maatregelen er genomen moeten worden, inclusief het aansluiten op het Quantum Gateway Foundation testbed.

Kortom, het is mogelijk je nu voor te bereiden op de doorbraak van quantum computing die traditionele asymmetrische cryptografie onbruikbaar gaat maken. Naast het wachten op NIST's PQC kun je alvast inventariseren welke cryptografie je in welke systemen gebruikt voor welke informatie. En wellicht is het mogelijk de kwetsbare cryptografie te versterken door een laag symmetrische cryptografie toe te voegen.

Quantum Gateway Foundation

Introductie Quantum Gateway Foundation

Quantum Gateway Foundation is een nieuw initiatief gefinancierd door Quantum Delta NL en private investeerders. Het doel van QGF is om een ecosysteem te realiseren waar bedrijven en organisaties toegang krijgen tot de nieuwste Quantum veilige technologie zodat ze zelf een compleet en duidelijk inzicht krijgen in welke technologie het beste past bij hun organisatie, applicatie of complete infrastructuur. Onder andere Quantum security awareness content, Quantum safe security assessments & nulmetingen kunnen worden gebruikt en uitgevoerd. En daarnaast kunnen bijvoorbeeld Post Quantum Cryptografie, Quantum Key Distributie, Quantum random number generation, Symmetrische encryptie systemen et cetera worden aangesloten op het QGF-platform

Referenties

(1) Zapata Computing - The Second Annual Report on Enterprise Quantum Computing Adoption: https://www.zapatacomputing.com/enterprise-quantum-adoption-2022/

(2) Nature - Analyzing the performance of variational quantum factoring on a superconducting quantum processor: VQF: https://www.nature.com/articles/s41534-021-00478-z

(3) GRI - 2022 Quantum Threat Timeline Report: https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

(4) GRI - A Methodology for Quantum Risk Assessment: https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/

(5) AIVD - Bereid je voor op de dreiging van quantumcomputers: https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers

Auteurs: Vincent van Dijk en Chris de Vries. Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Chris de Vries is redacteur van het IB Magazine en daarnaast eigenaar van De Vries *Impuls* Management, hij is bereikbaar via impuls@euronet.nl.

Hoe beveilig je een Windows laptop of computer?

HULPGIDS BEVEILIGING VOOR HET KLEINBEDRIJF (DEEL 3)

In de vorige uitgave vroeg Chris naar gereedschappen welke het mkb kan gebruiken om een bedrijf te beveiligen. Firewalls, password managers en antivirus zijn erg breed in te zetten en helpen je om vanuit een holistisch oogpunt een keuze te maken.

Toch is het goed om in te zoomen op specifieke systemen en applicaties die we dagelijks gebruiken: je laptop, e-mail of online software. Dit artikel zal wat dieper inzoomen op Windows laptops en PC's die je dagelijks gebruikt om je werk te verrichten.

Vincent, ik heb een Windows laptop, mijn collega's gebruiken ook Windows. Waar moet ik naar kijken als ik een Windows laptop wil beveiligen?

Bij een Windows laptop gaat het er niet alleen om dat je de juiste beveiligingstools hebt geïnstalleerd. Net zoals thuis, kun je niet alleen volstaan met het installeren van een goed slot en het ophangen van een camera. Je moet er ook voor zorgen dat kostbare spullen niet zomaar in het zicht staan en je moet altijd de deur op slot doen wanneer je weggaat.
Om jouw digitale Windows-huis te beveiligen, kijken we naar drie categorieën:

1. Hygiëne
2. Veilige configuratie
3. Systeem kennis

1. Hygiëne

Bij hygiëne gaat het erom dat je laptop mooi schoon is. Na verloop van tijd verzamelen onze computers onnodige bestanden, tijdelijke gegevens en overbodige programma's die kostbare opslagruimte in beslag nemen en prestaties vertragen. Rommel die ook je dreigingslandschap vergroten.

Zorg ervoor dat je die rommel verwijdert. Ga regelmatig door je geïnstalleerde applicaties heen en verwijder alle applicaties die je niet meer nodig hebt of nooit meer gebruikt. Gebruik ook regelmatig de ingebouwde tool Schijfopruiming om tijdelijke bestanden, systeemcaches en andere onnodige gegevens te verwijderen.

Door het vele gebruik van browsers creëer je tegenwoordig ook een hoop rommel in de browser. Webbrowsers verzamelen tijdelijke bestanden, cookies en browsegeschiedenis, die de prestaties kunnen beïnvloeden en de privacy in gevaar kunnen brengen. Maak regelmatig de cache van je browser leeg en verwijder cookies alsook de browsegeschiedenis om je browse-ervaring fris en veilig te houden. Verken de instellingen van jouw browser om extensies te beheren en verwijder onnodige of verouderde 'Add-ons'. Ik raad aan om twee belangrijke 'Add-ons' te installeren in je browser:

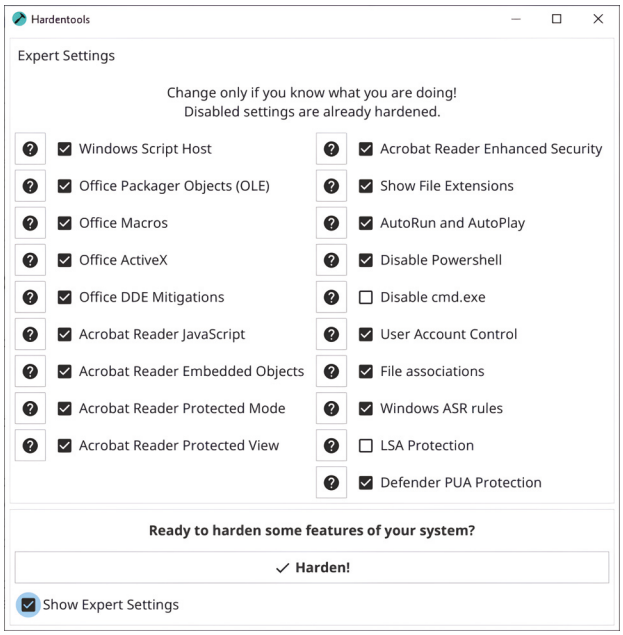
1. 'Adblocker' voor het blokkeren van virussen, die via advertenties verspreid worden. Gebruik *UBlock Origin* en vermijd de andere AdBlockers. Ook AdBlockers hebben een reputatie om virussen te bevatten (1).
2. 'Cookie Auto delete' zorgt ervoor dat de cookies van je webbrowsers mooi opgeruimd blijven (2).

Naast het opruimen van onnodige applicaties is het ook essentieel om een password manager te gebruiken en sterke wachtwoorden te hanteren. Een password manager helpt je bij het veilig beheren van al je wachtwoorden, waardoor je niet telkens hetzelfde wachtwoord gebruikt en je sterkere wachtwoorden kunt genereren en onthouden. Zie ook IB Magazine 2- 2023, de artikelen van Lex Borger en Menno Vermeulen over dit onderwerp.
Ook is het verstandig om regelmatig Windows opnieuw te installeren, bij voorkeur minimaal jaarlijks, maar vaker mag. Door Windows opnieuw te installeren worden eventuele ongewenste programma's, virussen of andere vormen van malware verwijderd, waardoor jouw laptop schoon en efficiënt blijft werken. Het helpt ook om de prestaties van je systeem te verbeteren en eventuele softwareproblemen op te lossen.

2. Veilige configuratie

Over het algemeen heb je geen duur antivirusprogramma nodig om een veilige Windows laptop te hebben - Windows komt al met een prima antivirusprogramma: Windows Defender en Firewall. Let op: controleer of deze tools aanstaan, met name door het gebruik van andere programma's kan Defender automatisch uitgezet worden. Bovenop de standaard configuratie is het verstandig om het systeem te voorzien van een paar veilige instellingen. Dat gaat het makkelijkst door HardenTools (3) te downloaden en te activeren. Deze tool zal ervoor zorgen dat standaard alle risico-

volle functies, zoals: Powershell en MS Office macro's uitgeschakeld worden.



Figuur 1: HardenTools zet tal van risicovolle applicaties uit.

Om de veiligheid van je Windows systeem nog meer te verhogen is het goed om een administratoraccount te gebruiken. Door een apart administratoraccount te hebben, creëer je een onderscheid tussen dagelijkse taken en administratieve functies die verhoogde privileges vereisen.

Je kunt een apart administratoraccount maken met de volgende stappen in Windows 11 (4)

1. Inschakeling van het administratoraccount: ga naar de instellingen van Computerbeheer, ga naar Gebruikers en schakel het administratoraccount in, dat standaard is uitgeschakeld. Stel een sterk wachtwoord in voor dit account.
2. Wijziging gebruikerstype: open het Configuratiescherm, ga naar Gebruikersaccounts en klik op het gebruikersaccount dat moet worden gewijzigd. Schakel het accounttype om van administrator naar standaardgebruiker.
3. Instelling gebruikersaccountbeheer op de hoogste stand: open de instellingen voor Gebruikersaccountbeheer en selecteer de optie welke altijd melding geeft wanneer toepassingen proberen software te installeren of wijzigingen aan te brengen in de computer- of Windowsinstellingen. Bevestig de wijziging.
4. Test de nieuwe instellingen: download een softwareprogramma van internet en probeer het te installeren. Het systeem vraagt nu eerst om toestemming van het administratoraccount voordat de installatie wordt toegestaan.

Additioneel zijn er meerdere security features die je kunt aanzetten in Windows 10/11. Hier zijn nog vijf features waar je naar kunt kijken. Let wel op, voor sommige features heb je een Windows pro licentie nodig (5).

1. Windows Sandbox (6)
Windows Sandbox is een geïsoleerde virtuele omgeving waarin je verdachte programma's kunt uitvoeren zonder risico voor het hoofdsysteem. Het biedt een tijdelijke omgeving waarin je bestanden kunt kopiëren, programma's kunt testen en vervolgens de Sandbox kunt sluiten, waarbij alle wijzigingen worden verwijderd.

2. Application Guard (7)
Application Guard creëert een geïsoleerd browservenster, vooral in Microsoft Edge, waarin je potentieel schadelijke websites veilig kunt openen. Het voorkomt dat kwaadwillende inhoud of malware zich verspreidt naar het hoofdsysteem door een gescheiden en beveiligde omgeving te bieden voor het openen van webpagina's.

3. Reputation-based protection (8)
Reputation-based protection omvat functies zoals *SmartScreen* en phishing-bescherming. *SmartScreen* beoordeelt de betrouwbaarheid van gedownloade bestanden en waarschuwt je als een bestand een slechte reputatie heeft. Phishing-bescherming waarschuwt je voor potentieel scha-

delijke of frauduleuze websites die proberen persoonlijke gegevens te stelen.

4. Device protection (9)
Windows biedt ingebouwde functies zoals core-isolatie en geheugenintegriteit om jouw apparaat te beschermen tegen kwaadaardige software-aanvallen. De beveiligingsprocessor biedt extra versleuteling en de functie *Secure boot* voorkomt dat malware, zoals rootkits, worden geladen wanneer het apparaat start.

5. Controlled folder access (10)
Controlled folder access is een functie die beperkingen oplegt aan welke programma's toegang hebben tot bepaalde mappen op je systeem. Het beschermt tegen ransomware-aanvallen door te voorkomen dat ongeautoriseerde programma's belangrijke mappen wijzigen.
Onderaan het artikel hebben wij een aantal links opgenomen. Via deze links kun je deze security features van Windows zelf bekijken en aanpassen.

3. Systeem kennis

Een systeem is nooit statisch, het is geen steen. Jouw Windows laptop verandert continu, als gevolg van updates, nieuwe applicaties en door gebruik. Om een veilig huis te bouwen en te onderhouden moet je kennis hebben van gereedschap, je hoeft geen expert te zijn, maar je moet wel weten dat je een hamer niet gebruikt om een schroef in de muur te slaan. Zo moet je ook kennis en kunde hebben van jouw Windows systeem om verdacht gedrag te kunnen zien of om een laptop goed te onderhouden.

Een belangrijk component voor jouw systeemkennis zijn de Windows logs. Het bestuderen van de Windows logs zorgt ervoor dat je beter grip krijgt op wat er allemaal precies gebeurt in jouw Windows systeem. Om de Windows logboeken te bekijken en te filteren, volg je de onderstaande stappen:

1. Open het menu Start en typ *'Event Viewer'* in het zoekvak. Klik op *'Event Viewer'* in de zoekresultaten om het venster *'Event Viewer'* te openen.
2. In het linkerdeelvenster van *'Event Viewer'* zie je verschillende logboekcategorieën, zoals o.a. Toepassing-, Beveiliging- en Systeemlogboeken. Klik op de gewenste categorie om de bijbehorende logboeken uit te vouwen.
3. Selecteer het specifieke logboek waarin je geïnteresseerd bent, bijvoorbeeld *'Beveiligingslogboeken'*. De gebeurtenissen in dat logboek worden weergegeven in het rechterdeelvenster.
4. Om gebeurtenissen te filteren, klik je met de rechtermuisknop op het gewenste logboek en selecteer je *'Filter Current Log'* of *'Filteren op huidig logboek'*. Hierdoor wordt het venster *'Filter Current Log'* geopend.
5. In het venster *'Filter Current Log'* kun je verschillende filtercriteria instellen, zoals logboekbron, Event-ID, trefwoorden, datum/tijd, enzovoort. Pas de filters aan op basis van jouw specifieke vereisten en klik op *'OK'*.
6. Na het toepassen van de filters worden alleen de logs weergegeven die aan de opgegeven criteria voldoen.

Op deze manier kun je de Windows logboeken bekijken en filteren om specifieke gebeurtenissen te vinden en relevante informatie te verkrijgen. Houd er rekening mee dat het gebruik van de Event Viewer mogelijk beheerdersrechten vereist.

De basis van alle logs zijn de zogeheten EventIDs. Deze identificatie nummers geven aan waar een log over gaat. Als je wilt zoeken naar logs kun je het beste zoeken naar verdachte EventIDs. De website *Ultimate Windows Security* heeft de beste beschrijvingen van alle Windows EventIDs met uitleg bij elke log (11).

In een Windows systeem zijn er verschillende logs waar je op moet letten om de beveiliging te waarborgen en potentiële bedreigingen te monitoren. Hier zijn de belangrijkste gebeurtenissen die genoemd worden in de tekst (12):

1. Event -ID 4688: deze gebeurtenis geeft aan wanneer er wordt ingelogd op een systeem en verstrekt informatie over het type gebruiker dat heeft ingelogd.

Let erop dat je nooit vertrouwelijke informatie vermeldt in de gestelde vragen, dat is stap 1 voor een veilige ICT-omgeving!

2. Event -ID 1102: deze gebeurtenis duidt op het wissen van een logboek, wat ongebruikelijk is in een normale omgeving en kan wijzen op pogingen van aanvallers om sporen te verbergen.
3. Event -ID 4670: deze gebeurtenis geeft wijzigingen weer in objectmachtigingen die gemonitord moeten worden, vooral in combinatie met het inschakelen van controlebeleid met betrekking tot machtigingen voor schrijven, DAC-wijzigingen of eigendomsoverdracht.
4. Event -ID 4624: deze gebeurtenis vertegenwoordigt een succesvolle accountlogin en wordt beschouwd als een basisgebeurtenis bij inloggen door de bevoegde gebruiker, welke regelmatig in de omgeving moet voorkomen.
5. Event -ID 4672: wanneer deze log gecombineerd wordt met Event -ID 4624, duidt dit op het toewijzen van speciale rechten aan een nieuwe login, wat kan wijzen op potentiële aanvallen zoals '*pash the hash*' (een hacking techniek!). Het is raadzaam om extra aandacht te besteden aan deze combinatie.
6. Event -ID 10 (met Sysmon geïnstalleerd): deze gebeurtenis is specifiek voor Sysmon, een tool die de analyse verbetert, en toegang geeft tot het LSASS-proces (Local Security Authority Subsystem Service), wat relevant kan zijn voor het detecteren van tools die gebruikt worden in '*pash the hash*'-aanvallen.
7. Event-ID 1116 (in Windows Defender): deze gebeurtenis, te vinden in de logboeken van Windows Defender-antivirus, geeft aan dat er malware of mogelijk onveilige software is gedetecteerd of geïnstalleerd op het systeem.

Wij kunnen ons voorstellen dat bovenstaande niet één-twee-drie door jullie, mkb-lezers, is toe te passen of dat er vragen opkomen. Gebruik dan ook de mogelijkheid om via LinkedIn vragen te stellen aan ons. Wij komen er dan zeker op terug. Via LinkedIn, via een directe reactie (zeker wanneer het om vertrouwelijke informatie gaat) en anders via IB Magazine. Let erop dat je nooit vertrouwelijke informatie vermeldt in de gestelde vragen, dat is stap 1 voor een veilige ICT-omgeving!

Referenties

(1) https://ublockorigin.com/
(2) https://duckduckgo.com/?t=ffab&q=coockie+auto+delete&ia=web
(3) https://github.com/securitywithoutborders/hardentools
(4) https://www.youtube.com/watch?v=TOpups3RDYA
(5) https://www.youtube.com/watch?v=uljX4aOoeaQ
(6) https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-overview
(7) https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview
(8) https://support.microsoft.com/en-us/windows/protect-your-pc-from-potentially-unwanted-applications-c7668a25-174e-3b78-0191-faf0607f7a6e
(9) https://support.microsoft.com/en-us/windows/device-protection-in-windows-security-afa11526-de57-b1c5-599f-3a4c6a61c5e2
(10) https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-controlled-folders?view=o365-worldwide
(11) https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/-default.aspx
(12) https://www.csoonline.com/article/3561889/the-most-important-windows-10-security-event-log-ids-to-monitor.html

COLUMN LEX

Lex Borger is security consultant bij Tesorion en oud-hoofdredacteur van IB Magazine. Lex is bereikbaar via lex.borger@tesorion.nl

9/11: de opkomst van detectie & respons

De terroristische aanval op de WTC-torens in New York en het Pentagon in Washington op 9/11 heeft de informatiebeveiliging voor altijd veranderd. Hierdoor kwam er een focus te liggen op detectie en respons. 'Prevent, detect, respond' is de nieuwe dimensie waarin cybersecuritymaatregelen worden uitgelegd. 'People, process, technology' was het onderwerp van mijn vorige column. Omdat de standaardinvulling hiervan eigenlijk volledig uit preventieve maatregelen bestaat, zijn detectie en respons daarin ondervertegenwoordigd.

Vijfentwintig jaar geleden was detectie in de standaarden geen onderdeel van security. De meest verwante securitymaatregel was de verplichting om te loggen. Maar er stond in standaarden niets over het monitoren ervan, laat staan dat 'alerting' beschreven was. Het werd wel gedaan, door 'system administrators' als onderdeel van 'system support'.

Na 9/11 investeerden geheime diensten in kennis en kunde om in systemen in te kunnen breken. Op het moment dat je ziet hoe makkelijk dat is, vraag je je af of zo'n aanval bij jou ook mogelijk is. En dat bleek zo te zijn. Onderzoekers vinden sporen van activiteiten van verschillende groeperingen die proberen in cyberspace aan te vallen. Sommigen zijn moeilijk te vinden. De een na de andere zogenaamde 'Advanced Persistent Threat' wordt ontdekt. Allemaal georganiseerde bendes, veelal met directe banden met een nationale regering.

De eerste grote doorbraak is er een van westerse bodem: Stuxnet. Samen met Maarten Hartsuijker schreef ik daar eind 2010 nog een artikel over in dit blad. Kim Zetter schreef er later een boek over, *Countdown to Zero Day*.

Rond deze tijd kwam ook de Security Information and Event Management (SIEM) op als nieuwe productcategorie. In theorie een heel sterk concept: als analyse van één logbestand bewijs voor een cyberaanval kan leveren, dan kan het combineren van informatie uit meerdere logbestanden eerder en duidelijker aantonen wat er fout zit. Een SIEM kan duizenden, zelfs miljoenen logregels doorwerken en alerts uitbrengen op verdachte situaties. Maar een verdachte situatie is niet per se een cyberaanval. Dit kan lastig zijn om te bevestigen. Hierop volgt de opkomst van een specialistisch bureau om vast te stellen wat er aan de hand is en of een alert daadwerkelijk een kwaadaardige aanval betreft. Dit bureau krijgt de naam 'Security Operations Center', ofwel een SOC.

En als je detecteert moet je ook reageren, 'respond'. Cyberrespons werd al veel eerder erkend als een noodzakelijke 'capability', al na de Morris-worm (1988). Toen richtte Carnegie Mellon University het CERT/CC op. CERT staat voor 'Computer Emergency Response Team', ook wel CSIRT genoemd, 'Computer Security Incident Response Team'.

Toch was ook hier de focus op terrorisme nodig om het CERT gemeengoed te maken. In 2002 richtte de Nederlandse Overheid GovCERT op als dienst onder Binnenlandse Zaken, wat in 2012 opging in het NCSC, onder het NCTV. Sinds 2019 is het NCSC een zelfstandige dienst van Justitie en Veiligheid. Jaarlijks brengt het een nieuwe versie uit van het rapport 'Cybersecuritybeeld Nederland'. In 2003 richtte de Amerikaanse overheid de US-CERT op. De UK liet het allemaal nog vrij lang vallen onder CGHQ en richtte in 2013 CERT-UK op, dat in 2016 opging in het Engelse NCSC.

Vandaag de dag werken SOCs en CERTs veel proactiever en structureler aan detectie van en respons op cyberaanvallen. Daar ga ik het de volgende keer over hebben.

De studenten van vandaag, zijn onze collega's van morgen. Tijd om hen in het zonnetje te zetten! In deze nieuwe rubriek willen we de stagiairs informatiebeveiliging aan het woord laten. We leren een stagiair kennen aan de hand van diens vooropleiding, zijn of haar verhaal over hoe iemand in de informatiebeveiliging terecht is gekomen, bij welke organisatie de stage gelopen wordt en wat de stage-opdracht is. **Meld ook jouw stagiair aan bij de redactie!**

Stage lopen als onderdeel van je studie

Mijn naam is Luiza Atas. Ik ben een vierdejaars student Integrale Veiligheidskunde op de Avans Hogeschool in Breda. Ik heb gekozen voor deze studie omdat ik graag wat wil bijdragen aan de veiligheid van onze maatschappij. Voor mijn derdejaars stage heb ik onderzoek uitgevoerd voor het Expertisecentrum Security (ECS), een onderdeel van de gemeente Den Haag.

De opleiding Integrale Veiligheidskunde heeft mij bewust gemaakt van hoe breed en hoe belangrijk veiligheid is. Tijdens de studie werd mij geleerd om veiligheidsvraagstukken vanuit juridische, economische, psychologische en de bestuurskundige kant te bekijken. Ook heb ik geleerd om problemen te signaleren, projecten op te zetten en de veiligheid te bewaken bij grootschalige rampen. Dit binnen de overheid, bedrijven, binnen de zorg of in woonwijken. Verder heb ik verschillende vaardigheden kunnen ontwikkelen zoals presenteren, interviewen, discussiëren, onderzoeken, communiceren, adviseren, managen, leidinggeven en analyseren. De opleiding Integrale Veiligheidskunde duurt vier jaar. De kennisvakken die worden aangeboden vind je in de tabel hiernaast.

Er wordt individueel of in groepen gewerkt aan praktijkopdrachten. De opdrachten komen zowel uit het publieke- als het private domein. Je leert risico's in kaart brengen en afwegen. Hierbij worden problemen vanuit verschillende

Leerjaar 1	Recht, Veiligheid en Middelen, Veiligheid en Trends, Criminologie en Integrale Veiligheid
Leerjaar 2	Arbeidsveiligheid, Veiligheid en Trends, Securitymanagement, Veiligheid en Informatie, Engels en Veiligheid en Middelen
Leerjaar 3	Stage
Leerjaar 4	Minor en Afstudeerstage

invalshoeken bekeken.

Keuze voor een stage

De opleiding Integrale Veiligheid is heel breed, waardoor ik het lastig vond om een stage uit te zoeken. De opleiding focust zich op de fysieke veiligheid terwijl onze docenten ons bewust maken dat digitale veiligheid net zo belangrijk is. Dit trok mijn aandacht en hoewel ik een passie heb voor criminologie en psychologie, wilde ik me ook meer verdiepen in digitale veiligheid. Als maatschappij beginnen we ons immers steeds meer bewust te worden van het feit dat cybercriminaliteit toeneemt. Jammer genoeg is het voor veel mensen nog een raadsel hoe zij zich daadwerkelijk kunnen beschermen tegen dit fenomeen dat zich nog dagelijks ontwikkelt. Het leek mij leuk om te leren hoe we onze persoonlijke gegevens en gevoelige informatie digitaal kunnen beschermen. Het Expertisecentrum Security, een afdeling die zich bezighoudt met de informatieveiligheid van één van de grootste gemeentes van Nederland, leek mij de ideale plek om hierover meer te leren.

De gemeente Den Haag is een openbare instantie. Hiermee wordt een overheidsorganisatie aangeduid die rechtspersoonlijkheid bezit. De gemeente wordt bestuurd door bestuursorganen. Dat zijn de raad, het college van burgemeester en wethouders en de commissies. De gemeente Den Haag is opgedeeld in zeven diensten: Bestuursdienst (BSD), Dienst Bedrijfsvoering (DBV), Dienst Publiekszaken (DPZ), Dienst Stadsbeheer (DSB), Dienst Onderwijs, Cultuur en Welzijn (OCW), Dienst Sociale Zaken en Werkgelegenheidsprojecten (SZW) en Dienst Stedelijke Ontwikkeling (DSO). Tijdens mijn stage heb ik meegekeken met de dienst Bedrijfsvoering, afdeling Informatisering en Automatisering waarbij het ECS hoort. Het Expertisecentrum bestaat uit vijf subgroepen. De taken die zij uitvoeren zijn de kaders en beleidstukken voor de informatieveiligheid van de gemeente opstellen en het uitdragen en adviseren over de implementatie ervan. Het beleidskader is uitgewerkt met specifieke interne documenten voor informatieveiligheid op tactisch niveau en werkinstructies op operationeel niveau.

Invulling stage

Tijdens mijn stage heb ik meegelopen met de werkgroep binnen het ECS die zich bezighoudt met het faciliteren van het proces rond de Baseline Informatiebeveiliging Overheid (BIO)-zelfevaluatie. Dit is een intern proces waar gemeentebreed aan functioneel beheerders wordt gevraagd om aan te geven of en hoe de verplichte BIO-maatregelen binnen hun applicatie tot stand zijn gekomen. Een procesverantwoordelijke neemt eigenaarschap over de antwoorden van de functioneel beheerder en vervolgens wordt de zelfevaluatie teruggekoppeld aan het Expertisecentrum Security. Zij adviseren de proceseigenaren daarna bij het verbeteren van beveiligingsmaatregelen. Om de implementatie van de BIO-maatregelen te vergemakkelijken heeft het ECS vergelijkbare maatregelen geclusterd en deze smartcontrols genoemd. Het zelfevaluatie proces is continu in ontwikkeling. Ik wilde graag een steentje bijdragen aan het verbeteren hiervan. Tijdens mijn stage heb ik twee hulpmiddelen ontwikkeld: De BIO-Verbeterrapportage en de BIO-Spiekbriefjes. De BIO-Verbeterrapportage wordt gebruikt door functioneel beheerders en procesverantwoordelijken. Het doel ervan is het bewustzijn vergoten, overzicht te bieden en werkzaamheden te vergemakkelijken. De rapportage is specifiek bedacht voor Multi Disciplinaire Teams (MDT) waarbinnen ambtenaren met verschillende functies samenwerken om een concreet vraagstuk op te lossen. Er is hiervoor gekozen om het bewustzijn van informatiebeveiliging te verhogen en onderlinge samenwerking te stimuleren. De rapportage zou ook per applicatie gebruikt kunnen worden.

De BIO-Verbeterrapportage bestaat uit: een inleiding, aanleiding, doelstelling, prioritering, verwachting en resultaat waarmee duidelijk wordt gemaakt waar de BIO-Verbeterrapportage voor is. Vervolgens is een inhoudsopgave toegevoegd om gemakkelijk bij specifieke informatie te komen. Na de inhoudsopgave komt het deel waarin per BIO-hoofdstuk de basis gelegd wordt voor verbetering van BIO-maatregelen. Hierin wordt de smartcontrol benoemd, de bijbehorende uitleg (duiding) en het risico van het niet-implementeren van de BIO-maatregel/smartcontrol. Het risico is toegevoegd om het belang van (verbetering van) implementatie van een BIO-maatregel/smartcontrol aan te geven. Na de risico's wordt per applicatie(s) een overzicht gegeven van de door de functioneel beheerder ingevulde verklaring in de zelfevaluatie. Tot slot geven de adviseurs informatieveiligheid van het expertisecentrum security een review op de ingevulde verklaring in de zelfevaluatie en een beschrijving met concreet advies.

Het tweede hulpmiddel dat ik heb ontwikkeld is/zijn de BIO-Spiekbriefjes. Het doel van de spiekbriefjes is het bewustzijn te vergoten en werkzaamheden te vergemakkelijken. De spiekbriefjes zijn gebaseerd op de BIO. De BIO is geschreven in een taal die over het algemeen moeilijk te begrijpen is voor mensen die niet uit het vakgebied komen. Om het begrijpen van de BIO wat eenvoudiger te maken heb ik spiekbriefjes gemaakt op basis van de Cyberspiekbriefjes (1). Voor elk BIO-hoofdstuk is een Spiekbriefje gemaakt. Hierin kun je lezen waar het hoofdstuk over gaat, wat het belang ervan is voor de gemeente Den Haag, wat de gevolgen zijn bij misbruik en waar je eventueel meer informatie kunt vinden over het hoofdstuk.

Conclusie

Ik heb een hele uitdagende stage gehad waarin ik nieuwe mensen heb ontmoet, veel heb geleerd en mezelf heb kunnen ontwikkelen op individueel en professionele vlak. Verder ben ik bewust geworden van wat informatieveiligheid daadwerkelijk is en hoe informatiebeveiliging wordt gemanaged in praktijk. Tijdens mijn stage ben ik enthousiast geworden om deze kennis met iedereen te delen.

Mochten er vragen zijn dan ben ik te bereiken via luizaatas@outlook.com.

Referenties:

(1) zie Cyberspiekbriefjes (veiliginternetten.nl)

Auteur: Drs. Robert Metsemakers RA RE CISSP is als ervaren auditor en informatiebeveiligingsexpert beschikbaar voor securityadviesopdrachten en bereikbaar op robert.metsemakers@gmail.com.

BLOG

Sapperdeflap: securitylessen van Pipo en Klukkluk

De serie Pipo de Clown, uitgezonden op de Nederlandse televisie van 1958 met onderbrekingen tot 1980, leerde mij een aantal nuttige dingen over (onder andere) information security.

Cor Witschge als clown Pipo, van https://nl.wikipedia.org/wiki/Pipo_de_Clown_(televisieserie)

Naast clown Pipo en zijn vrouw Mammaloe vervulde Klukkluk (gespeeld door Herbert Joeks) een belangrijke rol. Klukkluk introduceerde de uitdrukking 'mij zijn niet van de gekke' in Nederland. Later ging Dries van Agt dit als 'het is toch van de gekke' gebruiken in de Tweede Kamer, met helaas veel navolging. 'Het is van de knotse' hoorde ik in het journaal een politiecommissaris zeggen, over hevig voetbalgeweld. Heel jammer.

Herbert Joeks als indiaan Klukkluk, van https://nl.wikipedia.org/wiki/Klukkluk

Het Klukkluks was destijds ook populair bij volwassen meekijkers: er waren in de jaren '60 maar twee televisiezenders en iedereen had maximaal één televisietoestel in huis, dus je moest wel. Zodat aan acteur Joeks, tijdens een privé wandelingetje over de Wallen in Amsterdam, op zijn Mokums (Jiddisch voor: grote stad) werd gevraagd of hij die dag 'van de geilige was'. Leuke super (!) moderne zegswijzen slijten helaas snel door ze voortdurend te gebruiken. Wees daarom wars van clichés in je communicatie over security. Men vermijde de aanvoegende wijs, om medewerkers en managers op het rechte security pad te houden.

Klukkluk zei ook regelmatig 'niet van de bange, maar van de zeer voorzichtige te zijn'. Dat is een mooie basishouding voor een information security officer. Wel steeds op zoek naar mogelijke risico's en bedreigingen, maar niet verlamd door schrik voor *alle* mogelijke IT-onheil in de wereld. Verder gaf Klukkluk ooit aan afkomstig te zijn uit het 'tamelijk Wilde Westen'. Een dergelijke nuance aanbrengen bij het onderling wegen en presenteren van risico's en 'threats' is zeer welkom. Je kunt nu eenmaal niet alles rechtsboven in de risicomatrix plotten. Niet alles is 'levensgevaarlijk', zie ik terugblikkend op mijn eigen dreigingsbeelden nu ook wel in.

Dikke Deur was een verbastering van 'directeur'. Eind jaren '60 begreep ik dat als kijkertje niet, het was voor mij een vervelende, dikke kerel (dat kon je toen nog zeggen) met een hoge hoed op. De baas van het circus waar Pipo met ruzie was vertrokken om daarna als zzp'er in een woonwagen, gekregen van zigeuner (mag nu niet meer, want afkomstig van 'ziehende Gauner': rondreizende dief) Felicio, te gaan rondreizen met Mammaloe en dochter Petra. Petra moest later uit de serie vertrekken wegens een keiharde opstelling van de arbeidsinspectie: te jong voor tv.

Willy Ruys als Dikke Deur, van https://nl.wikipedia.org/wiki/Dikke_Deur

De Dikke Deur legde bij mij toen al de kiem voor een levenslange (gezonde) argwaan tegen managers, die – ongehinderd door enige inhoudelijke kennis of ervaring op securitygebied – op een vreselijke manier de baas gaan lopen spelen. Geef security professionals de tijd en ruimte om hun inhoudelijke kunstje te doen, zonder allerlei regelkringen. Professionals doen hun werk graag goed, uit zichzelf. Aan gasten die bij security-incidenten alleen in paniek 'Pipo! Koeien!' komen roepen, hebben we niks.

Boeven waren er ook en zelfs duidelijk benoemd (zie mijn recente blog over Italiaanse koffies): Snuf en Snuitje. Ze waren vooral verzot op parels (zie: inventariseer je kroonjuwelen) als buit en zelfs nog dommer dan ze zich gedroegen. Toch werden S&S als aanvallers regelmatig in eerste instantie door Pipo c.s. onderschat, zodat de rest van die aflevering de gevolgen van hun kwaadaardige ('malicious') acties moesten worden gemitigeerd. Bedenk: de aanvallers zijn inderdaad gemeen en oneerlijk, maar daarom niet per definitie dommer of onbekwamer dan jijzelf als verdediger. En het zijn er vermoedelijk meer dan de twee (S&S) die jij in het

Klukkluk zei ook regelmatig 'niet van de bange, maar van de zeer voorzichtige te zijn'. Een mooie basishouding voor een information security officer.

vizier hebt. Echt bekwame boeven zie je niet en ze werken wel samen.

Klukkluk was de beste vriend van Pipo en heeft een boogschietact in Pipo's voorstelling. Zijn schietkunst was echter belabberd en bij elk schot zei Klukkluk daarom: 'Floepens, mis!'. Voor zijn zichtbaarheid in de organisatie was dit funest, zodat Pipo hem 'Klukkluk de misschiet-indiaan' noemde. K. had beter, zoals verstandige moderne vulnerability scanning medewerkers dat doen, kunnen melden hoeveel kwetsbaarheden of 'anomalies' hij in de afgelopen periode wel had gevonden. Of hoeveel (absoluut getal) phishing mails er waren tegengehouden, in plaats van een zeer laag percentage ten opzichte van de miljoenen gescande mails per maand te rapporteren.

Zo'n woonwagen moet natuurlijk in beweging blijven. Om het hele zaakje met P+M+P+K aan boord te trekken, was één ezel beschikbaar, met de naam 'Nononono'. Daarbij moet ik denken aan het standaardantwoord van een SOC-medewerker of security officer op securityvragen van gebruikers. Kan ik al die vertrouwelijke financiële klantgegevens zo gewoon in de cloud zetten, in Amerika? Ik heb zelf met een bouwpakket uit China een tablet gesoldeerd, kan ik die voortaan voor zakelijk gebruik inzetten? Ik vond tijdens een dancefestival een USB-stick in de modder, kan ik die - nu ik vertrek bij de organisatie - gebruiken om mijn presentaties mee te nemen naar mijn privé computer en volgende werkgever? Je ziet de wapperende handen en het verschrikte gezicht van de antwoordende security professional hierbij al voor je. Toch is het bij dergelijke (stomme) vragen beter niet in paniek te raken en neutraal te vragen: 'wat denk je zelf?' en daarbij terloops de AVG te noemen en de bedragen van mogelijke boetes. Als ze het zelf bedenken, blijft het antwoord beter hangen.

Om security awareness acties te laten aanslaan bij het grote publiek is het mooi als rode draad een spreuk of slogan te hebben. Die je dan kunt gebruiken op posters, screensavers, de onvermijdelijke 'wuppies' op elk bureau, bedrukte koffiebekers (echt!) en alle verdere voorlichting op het intranet als bestrijding van ransomware, phishing mails, ongemelde datalekken en BEC (Business Email Compromise). En dan niet 'SAPperdeflap' (ook weer heel jammer), maar iets duurzaams als: 'Dag vogels, dag bloemen, dag kinderen.'

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.

Wanneer ben je open & transparant?

Goed nieuws: de medewerkers van de Autoriteit Persoonsgegevens (AP) maken zelf ook wel eens een foutje en ze zijn daar open over in hun jaarverslag (1). In totaal kreeg de AP met vijftig beveiligingsincidenten te maken, waarvan 26 datalekken. Die laatste gevallen gingen vooral om het verkeerd adresseren van brieven en e-mails. Ook ketenrisico's zijn de AP niet vreemd: de leverancier van een website had third-party plug-ins op de website geplaatst die gegevens doorstuurde naar Google. En niet alleen onze eigen AP maakt wel eens een foutje, ook het Britse National Cyber Security Centre (NCSC) moest haar bewustzijnscampagne intrekken omdat ze voor de campagne dezelfde naam had gekozen als de naam van een illegale streaming-app (2). Wellicht verschijnt dit incident ook in het jaarverslag.

We zijn meer bezig met incidenten en ook de openheid erover groeit. Inmiddels kijken veel mensen al niet meer op van berichten over ransomware, grote datalekken en kritieke kwetsbaarheden. Dat dit in het jaarverslag wordt opgenomen is een nieuwe stap in deze openheid. Hoe bewaken we de balans tussen openheid en transparantie aan de ene kant en het toch nog veel gehoorde statement 'aanvallers niet wijzer maken' aan de andere kant? Wat is maximale transparantie? Hadden we de beveiligingsincidenten bij de AP niet liever eerder willen weten? Een blik op deze materie van onze redacteuren.

Leo van Koppen - 'Een aanmoediging voor organisaties'

Deze openheid van het AP oogt natuurlijk heel eerlijk en ik keur het ook zeker niet af, maar ik vind het ook wel een beetje symboolpolitiek. De openheid beoogt volgens mij veel meer dan alleen het formele karakter van het melden van belangrijke wapenfeiten in een jaarverslag. Er wordt ook invulling gegeven aan de voorbeeldfunctie; een aanmoediging voor organisaties om ook deze openheid te betrachten in een paragraaf 'Beveiligingsincidenten'.

Daarnaast is het blijkbaar ook een goed PR-item want met een dergelijke vermelding kom je in het nieuws. Sommige organisaties heiligen het credo 'any news is good news', dat credo gaat hier blijkbaar ook op.

Formeel is de taak van het AP toezicht houden op het verwerken van persoonsgegevens. De Autoriteit Persoonsgegevens heeft als wettelijke taak te beoordelen of personen en organisaties de Wet bescherming persoonsgegevens naleven. Deze taak is ook gericht op de overheid. Ook ziet de AP toe op naleving van de Wet politiegegevens, de Wet gemeentelijke basisadministratie persoonsgegevens en alle andere wettelijke regelingen waarin sprake is van het verwerken van persoonsgegevens (3).

Leo van Koppen | Chris de Vries | Fook Hwa Tan | Lilian Knippenberg

Een blik op de website van de AP leert mij dat naast het controleren er ook veel aandacht besteed wordt aan voorlichting over relevante (nieuwe) wetgeving waaronder heel veel aandacht voor en best practices als het gaat om de AVG en dat is heel logisch. Ik vraag me overigens wel af of de invulling van die taak niet te veel is doorgeslagen naar het preventieve. Organisaties kennis aanreiken en daarmee naar verwachting het aantal datalekken terugdringen. Niets mis mee, want we doen niets anders in ons vakgebied. In onze preventieve strategie passen we de voorbeeldfunctie voortdurend toe, toch? In de awareness aanpak beleggen we de voorbeeldfunctie bij de CEO. Hij of zij moet het voorbeeldgedrag vertonen en hopen dat de medewerkers dit gedrag overnemen. De AP als CEO, zo simpel doet de AP dat.
Ik heb het jaarverslag AP 2022 (4) er toch maar even op nageslagen om het een en ander te checken en dan valt mij op dat het aantal meldingen van datalekken met vijftien procent is afgenomen, dat feit is wat mij betreft meer nieuws dan de datalekken bij de AP zelf. Opvallend is dat bij dit feit geen verklaring voor deze afname is gegeven. Hebben al die andere activiteiten die het AP uitvoert, anders dan de wettelijk taak, hun vruchten afgeworpen? Vreemd ook dat deze afname in datalekmeldingen dan weer niet in het nieuws, maar wel in deze achter het nieuws (AHN), komt!

Fook Hwa Tan - De Noodzaak van Maximale Transparantie bij Beveiligingsincidenten

In een tijd waarin cybercriminaliteit een constante dreiging vormt, is het begrijpelijk dat sommige organisaties terughoudend zijn om beveiligingsincidenten openbaar te maken. Het idee is dat het delen van dergelijke informatie aanvallers inzicht kan geven in zwakke plekken en hen kan aanmoedigen nieuwe methoden te ontwikkelen. Echter, deze opvatting is achterhaald. Aanvallers zijn al bekend met veel voorkomende kwetsbaarheden en maken gebruik van geavanceerde technieken om systemen binnen te dringen. Het verbergen van beveiligingsincidenten stopt hen niet, maar het houdt gebruikers wel in het ongewisse en voorkomt zo dat er passende maatregelen worden genomen.

Maximale transparantie is de sleutel tot een effectieve beveiligingsstrategie. Door beveiligingsincidenten openlijk te delen, kunnen organisaties van elkaars fouten leren en gezamenlijk werken aan verbeteringen. Dit bevordert een cultuur van verantwoording en continue verbetering op het gebied van gegevensbescherming. Bovendien stelt het gebruikers en klanten in staat om te begrijpen welke risico's ze lopen en stelt het hen in staat om passende maatregelen te nemen om zichzelf te beschermen.

Natuurlijk is er een balans nodig tussen transparantie en het voorkomen van verdere schade. Het is van cruciaal belang dat organisaties eerst de nodige stappen zetten om de oorzaak van het incident aan te pakken voordat ze dit openbaar maken. Bovendien moet gevoelige informatie, zoals persoonsgegevens, zorgvuldig worden behandeld en mag het delen van details geen onnodig risico vormen voor individuen of organisaties.

De beveiligingsincidenten bij de AP hadden wellicht eerder bekend moeten zijn, zodat passende maatregelen genomen konden worden. Door volledige openheid en transparantie na te streven, zetten we een belangrijke stap richting een veiligere digitale wereld. Het is hoog tijd dat alle organisaties, zowel publiek als privaat, deze benadering omarmen en samenwerken om onze systemen en gegevens beter te beschermen.

Lilian Knippenberg – Zo leidt transparantie daadwerkelijk tot betere veiligheid

Vroeger zeiden IT-ers nog tegen elkaar 'security by obscurity': houd zo veel mogelijk over je IT- infrastructuur geheim en je bent veilig. Gelukkig bewegen we nu als vakgebied naar 'security by design' en 'security by default': specifieke beveiligingsmaatregelen nemen en op die manier de veiligheid van je infrastructuur borgen. Ik hoop dat transparantie een onomstreden goed gaat worden, waarbij ook informatie over IOC 's '(indicators of compromise') door alle verdedigingsteams in de wereld wordt gedeeld. Dat zal nog wel even duren, want ook hier geldt het kat- en muisspel met criminelen. We willen de crimineel niet wijzer maken dan diegene al is. Natuurlijk geldt dat ook andersom: hoe weten wij wat de crimineel nog niet weet? Kunnen we dan niet beter alles delen wat we weten?

Ik vind het voorbeeld van de AP wat betreft het noemen van het aantal en de aard van de beveiligingsincidenten in het afgelopen jaar een goed voorbeeld. Maar let wel: in combinatie met andere tekenen van transparantie, zoals

het delen van technische informatie over kwetsbaarheden en IOC 's. Het landelijk dekkend stelsel van het NCSC speelt daarin wat mij betreft een cruciale rol. De sectorale insteek is logisch, maar ik zou ook graag zien dat verschillende sectoren van elkaar leren. Dan kunnen we als Nederland echt gezamenlijk optrekken en concurrentie op veiligheid achterwege laten. Gelukkig is daar nu al het Dutch Institute for Vulnerability Disclosure (DIVD). Vrijwilligers die Nederland een stukje veiliger maken door het opsporen van kwetsbaarheden en door de getroffen organisaties te informeren en te helpen. Zo kan transparantie zowel voorafgaand aan een incident (bij 'alleen' een kwetsbaarheid), als tijdens/achteraf (door het delen van IOC 's) en tot slot aan het eind van het jaar (bij het jaarverslag) leiden tot daadwerkelijk betere veiligheid.

Chris de Vries - Transparant zijn of niet?

We leven in een wereld waarin allerlei spelletjes worden gespeeld. Hoewel het verkleinwoord 'spelletjes' wordt gebruikt, is de inzet vaak enorm: zowel in financiële waarde als inzake imagoschade. Dus is het begrijpelijk dat geen enkele organisatie graag in de openbaarheid treedt wanneer het fout is gegaan en zeker niet wanneer de fout ook binnen de organisatie gezocht moet worden.

Binnen dat kader moet dan ook de discussie geplaatst worden over transparantie. De natuurlijke reactie is gesloten te blijven. Zo ook bijvoorbeeld in het bankwezen waarin het heel gebruikelijk was om negatief vermogen en negatieve jaarresultaten – met toestemming van de overheid – te camoufleren. Daartegenover staat het bedrijfsleven dat bij eenzelfde actie beticht zou zijn van bedrog, oplichting en fraude. Het argument om de wet verschillend uit te leggen voor in principe gelijke partijen: het publiek mocht het vertrouwen in het bankwezen niet verliezen.

En dus rijst de vraag hoe transparant is de AP in werkelijkheid. Wordt met het argument van (staats)veiligheid, vertrouwen behouden in en politieke voorbeeldfunctie wellicht het een en ander buiten de schijnwerpers gehouden? En zijn die argumenten valide? Wat verliezen wij aan vertrouwen als later alsnog de fouten boven tafel komen?

En over vertrouwen gesproken, het CBS publiceerde een vertrouwensoverzicht van Personen van 15 jaar of ouder (5) met als trieste instituties beneden de vijftig procent:

Instituten	Vertrouwen
Politici	23,8%
Kerken	29,6%
Tweede Kamer	30,4%
Grote Bedrijven	35,8%
Pers	39,8%
Ambtenaren	42,5%
Banken	48,5%
Europese Unie	48,7%

Vertrouwenstabel op basis van gegevens van het CBS.

Het hoogst scoorden (met scores boven de 75 procent): de gezondheidszorg (78,3%), de politie (77,0%) en rechters (76,6%). De vraag komt dus op of juist de formele staatsinstituties en het grote bedrijfsleven (inclusief banken) niet een veel verdergaande openheid moeten nastreven om het vertrouwen te herwinnen. Het vertrouwen kwam in de twintigste eeuw te voet en ging sinds circa 1987 te paard. Voor mij is het antwoord een volmondig 'ja'.

Referenties

(1) https://www.security.nl/posting/796706/Autoriteit+-Persoonsgegevens+vorig+jaar+slachtoffer+social+engineering-aanval
(2) https://www.security.nl/posting/795534/Cybercampagne+-Britse+overheid+leidt+naar+streaming-app+gebruikt+voor+piraterij
(3) https://nl.wikipedia.org/wiki/Autoriteit_Persoonsgegevens
(4) https://autoriteitpersoonsgegevens.nl/documenten/ap-jaarverslag-2022
(5) https://www.cbs.nl/nl-nl/nieuws/2023/19/minste-vertrouwen-in-tweede-kamer-in-10-jaar-tijd

Martijn Hoogesteger is Head of Cyber bij S-RM en is bereikbaar via m.hoogesteger@s-rminform.com.

COLUMN MARTIJN

Een analogie voor cybersecurity

De wereld van cybersecurity en IT is soms lastig uit te leggen. Het zijn abstracte concepten, terminologie waar mensen niet aan gewend zijn en vaak is er meer onbekend dan bekend over de eigen omgeving.

Bij brand kan iedereen zich iets voorstellen. Je kan het zien, voelen, ruiken en zelfs horen. En veel maatregelen liggen voor de hand. Geen brandbare spullen gebruiken, brandmelders ophangen en brandblussers op bereikbare plekken hebben. Als iemand ons daarover komt adviseren, kunnen we redelijk snel begrijpen wat het risico is (het pand brandt af) en hoe bepaalde middelen zouden helpen de kans of impact van brand te beperken.

Dit is een van de twee parallellen die ik graag trek met cybersecurity. Ervoor zorgen dat je veilige materialen gebruikt in het bouwen van je bedrijf is net zo belangrijk in brandpreventie als in cybersecurity. Maar waar branddetectie eenvoudig is met brandmelders of misschien zelfs een centraal systeem, is dit in cybersecurity een stuk lastiger. Het concept is echter hetzelfde: op elk systeem een 'brandmelder', Endpoint Detection & Response (EDR), is tegenwoordig de standaard.

Gebeurt er iets? Dan zijn medewerkers altijd wel goed op de hoogte van wat ze moeten doen wanneer het brandalarm afgaat. Je volgt de groene bordjes naar buiten en de bhv'ers helpen je. Op digitaal gebied is dat nog een lastige. Bij veel incidenten waar ik heb mogen helpen, zien we alarmen die gemist zijn of waar mensen niet de juiste actie op hebben genomen. Last but not least zijn er de brandblussers en de brandweer. Wat doe je zelf als er een alarm afgaat? Wie bel je als er meer hulp nodig is?

Ik merk dat door deze analogie, het veld veel begrijpelijker wordt. Voor de klant of andere gesprekspartners is het een wereld waar ze zich een beter beeld bij kunnen vormen. En veel vragen naar aanleiding van de analogie openen de deur om andere cybersecurity concepten uit te leggen, zoals het afsluiten van een verzekering, alternatieve manieren van preventie of detectie, maar vooral ook het oefenen van cyberincidenten en hoe een hele organisatie daarbij betrokken moet worden.

Ergens houdt de analogie natuurlijk op. Brand is een natuurlijk fenomeen, en (bijna) alle cyberrisico's komen voort uit menselijk handelen, voornamelijk door criminelen. Soms voelen cybercriminelen als een natuurlijk fenomeen omdat het zo lastig is om ze tegen te houden, maar het feit dat hun tools en technieken continu evolueren maakt het significant anders. Je moet steeds schakelen om bij te blijven.

Een andere analogie die vaak werkt om de modus operandi van cybercriminelen uit te leggen is die van de crimineel die door de straat loopt en kijkt waar panden van minder goede sloten zijn voorzien. Veel cyberaanvallen starten precies op dezelfde manier: ongericht, scannend naar kwetsbaarheden op IP-adressen. Dit maakt het tot een soort gelegenheidscriminaliteit. Op cybervlak staat het er echter vaak wat slechter voor. De crimineel zal niet meer kijken naar waar de beste sloten zitten, maar simpelweg naar waar de ramen en deuren open staan. Deze analogie ontkracht sterk het 'gerichte' beeld dat veel mensen hebben bij cybercrime. Hierdoor kijken mensen ook anders naar de maatregelen die getroffen moeten worden. Veiliger worden is dan het doel en honderd procent veilig voor een crimineel die je heeft uitgekozen, lijkt echt een ander verhaal.

Wellicht helpen deze voorbeelden je een keer wat uit te leggen over ons vak en het belang ervan. Heb je leuke andere analogieën? Let me know!

PvIB Platform voor InformatieBeveiliging

COLOFON

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

HOOFDREDACTEUR
Chris de Vries

REDACTIE
Leo van Koppen
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
Eric Noordam
E acquisitie@mos-net.nl
T 033 247 34 00

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
Veldhuis Media, Meppel

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 2023 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

(advertorial)

REUZADO INTRODUCEERT DATAVERNIETIGING OP LOCATIE

Reuzado is gespecialiseerd in het veilig inzamelen, vervoeren en vernietigen van data en datadragers. Elke stap in dat proces voldoet aan strenge eisen, is 100% beveiligd en milieuvriendelijk. Zelfs de minuscule, onbruikbare snippers die overblijven na het vernietigen van datadragers worden zoveel mogelijk op duurzame wijze gerecycled. Het is nu ook mogelijk om data en datadragers op het terrein van de klant te vernietigen.

Wat zijn de voordelen:

- Transport is overbodig; voor bepaalde branches een must;
- De klant, of een bevoegde controleur, kan ter plekke vaststellen dat de datadragers en/of data definitief zijn vernietigd;
- Iedere stap in dat proces wordt gedocumenteerd;
- De klant ontvangt van elke vernietigde datadrager een vernietigingsbewijs met serienummer;
- Reuzado garandeert dat vernietiging 100% veilig en volledig heeft plaatsgevonden;
- Het vernietigen van data en/of datadrager wordt altijd door eigen personeel uitgevoerd.

Meer weten?

Meer weten over mobiele datavernietiging of de andere diensten van Reuzado ICT Services? Neem dan contact met ons op via e-mail (circulair@reuzado.nl) of telefonisch via 023 5519821. De medewerkers leggen graag uit wat er mogelijk is. Reuzado staat voor transparante communicatie, glasheldere offertes en 100% veilige datavernietiging.

Over Reuzado

Reuzado, Esperanto voor 'hergebruik', is dé expert voor alles op het gebied van ICT. Het bedrijf is ISO 9001 gecertificeerd en alle werkzaamheden worden verricht conform DIN 66399. Op dit moment wordt gewerkt aan zowel ISO 14001 als ISO 27001 certificering en Weeelabex/Cenelec 50625. Voor meer informatie: https://reuzado.nl/

TSTC

ICT en Security Trainingen

Ransomware? Log4j?

ADVANCE YOUR CAREER WITH SECURITY IN 2023

WR - Workshop Ransomware
EHE - Ethical Hacking Essentials
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v12
OSCP - Offensive Security PEN-200

GET SKILLED
WWW.TSTC.NL

Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

CEH - Certified Ethical Hacker
CHFI - Computer Hacking Forensic Investigator
CPENT - Certified Penetration Testing Professional
SSCP - Systems Security Certified Professional
OSCP - Offensive Security Certified Professional

SECURITY MANAGEMENT TRAININGEN

CISSP - Certified Information Systems Security Professional
CISM - Certified Information Security Manager
CISA - Certified Information Systems Auditor
CRISC - Certified In Risk And Information Systems Control
C|CISO - Certified Chief Information Security Officer

PRIVACY TRAININGEN

CIPP/E - Certified Information Privacy Professional / Europe
CIPM - Certified Information Privacy Manager
CIPT - Certified Information Privacy Technologist
CDPO - Certified Data Protection Officer

CLOUD SECURITY TRAININGEN

CCSP - Certified Cloud Security Professional

ISO TRAININGEN

ISO 27001 - Foundation
ISO 27001 - Lead Implementer
ISO 27001 - Lead Auditor
ISO 27005 - Risk Manager
ISO 27701 - Privacy Management

www.tstc.nl

Onze trainingen zijn weer klassikaal of Live Online te volgen