15 PvIB reconnect in cyber security

ib
INFORMATIEBEVEILIGING MAGAZINE

- Wat motiveert mkb'ers om actie te ondernemen tegen ransomware?
- Kraak de kluis. Hoe wachtwoordkluizen kinderlijk eenvoudig te kraken zijn
- Column: Stel: je wordt cybercrimineel

JAARGANG 22 - 2022 - EDITIE 6

Afscheid

Tom Bakker

Voor je ligt alweer het laatste iB-Magazine van 2022, in het derde lustrumjaar van PvIB. Na twee jaar gekluisterd te hebben gezeten aan een beeldscherm om via Teams en andere tools contact te houden, konden we afgelopen jaar eindelijk weer fysiek bijeenkomen. Mooi op tijd zodat we het lustrum feestelijk hebben kunnen vieren op een wel bijzondere locatie: de Koepelgevangenis van Arnhem. De redactie was daar uiteraard ook bij aanwezig om naast het feesten, ideeën voor artikelen en potentiële auteurs te verzamelen. Daar zijn aardig wat reacties op gekomen waar we wat mee kunnen.
In dit laatste nummer vind je een verslagje door redactielid Lilian van het door het NCSC georganiseerde ONE Conference. Het was een recordopkomst met 2200 (!) deelnemers.
Er is veel te doen rond de beveiliging van het mkb. Blijft lastig. Twee artikelen gaan dieper in op deze problematiek.

Hoe technologische oplossingen soms zwakkere schakels zijn dan het idee dat de mens de zwakste schakel is, beschrijft redactielid Maarten. Achter Het Nieuws (AHN) zwengelt de discussie aan over wanneer iets desinformatie of 'vrijheid van meningsuiting' is en wie er nu verantwoordelijk is voor de juistheid (en volledigheid) van informatie. Zoals gebruikelijk het jaaroverzicht waarin je nog even kan terugzoeken waar dat interessante artikel ook weer te vinden is. Natuurlijk de interessante columns van onze vaste columnisten. Genoeg leesplezier.

Ten slotte, dit voorwoord is mijn laatste bijdrage aan het magazine en tevens mijn laatste taak als voorzitter van de redactie. In de laatste ALV heb ik mij niet meer herkiesbaar gesteld als bestuurslid en neem daarmee dus ook afscheid van de redactie. Na bijna veertien fijne en boeiende jaren is het hoog tijd dat iemand anders het stokje overneemt. Ik heb altijd met veel plezier met de redactie, MOS en het PvIB-bestuur samengewerkt. Er waren in de redactie soms wel wat ups en downs maar dat was meer door het grillige aanbod van artikelen. We hebben het, dankzij onze inzet en onze netwerken, altijd gered om elke keer weer een mooi magazine neer te zetten!

Ik blijf wel lid van het PvIB dus geen vaarwel maar tot ziens!

IN DIT NUMMER

Auteur: Lilian Knippenberg is redactielid en senior information security officer en schrijft op persoonlijke titel. Ze is te bereiken via LinkedIn.

Terugblik op ONE Conference ‘we are all connected’

Op dinsdag 18 en woensdag 19 oktober 2022 vond de ONE conference in Den Haag plaats. In mijn werkomgeving wordt daarnaar ook wel verwezen als ‘de’ ONE, wat iets zegt over hoezeer ernaar uitgekeken wordt. Een terugblik.

Veel mensen met verschillende achtergronden en dus ook verschillende blikken op cybersecurity en relatief veel vrouwelijke sprekers.

Het thema van deze 2022 editie is 'we are all connected'. Prachtig thema als je het mij vraagt, na twee coronajaren waarin de conferentie online te volgen was. De voertaal van de ONE is Engels en spreekt zo een breed publiek aan. De organisatie is in handen van drie partijen: het Nationaal Cyber Security Centrum (NCSC), het Ministerie van Economische Zaken en de Gemeente Den Haag, waarbij de logistiek en aanmeldingen etc. georganiseerd worden door het ECP (Platform voor de InformatieSamenleving). Het is een invite-only event, wat niet betekent dat het klein is, maar wel dat er alleen mensen zijn die een functie in cybersecurity hebben.

Slingerende rij

Ik dacht: als de opening om 9.15 uur is en ik ben er om 9 uur, is dat prima op tijd. Dat bleek een beetje naïef te zijn, want ik was niet de enige met die gedachte. De rij voor de aanmelding slingerde zich helemaal om het gebouw en het duurde wel even voordat ik binnen stond. Volgende keer dus veel ruimer op tijd komen! Toch heeft ieder nadeel zijn voordeel, want elkaar ontmoeten en spreken begon in de rij al. Het was me in elk geval duidelijk dat de animo en de opkomst voor de ONE groot was.

Tracks: de keuze was reuze

Voor ieder wat wils op de ONE: waar conferenties die ik ken meestal ofwel technische sprekers ofwel organisatorische sprekers kennen, kon ik hier juist voor beiden kiezen. Er waren een aantal tracks: technical, research, law enforcement, governance, innovation. Bij iedere sessie was het technisch niveau van de sessie aangegeven van 1 tot 3. Ik vond het moeilijk kiezen, want op ieder moment waren er meerdere aansprekende opties beschikbaar. Daarnaast waren de ruimtes soms al vol, wat het ook wel weer makkelijker maakte om te kiezen waar ik naartoe wilde. Wat ik ook een groot pluspunt van de ONE vind is dat de sprekers divers zijn. Veel mensen met verschillende achtergronden en dus ook verschillende blikken op cybersecurity en relatief veel vrouwelijke sprekers.

Netwerken

Er is genoeg ruimte om mensen te ontmoeten. Letterlijk door de 'meeting zone', waar je afspraken kunt maken met mensen die je nog niet kende, maar ook spontaan tussen de vele breaks door. Ondanks de hoge opkomst kwam het op mij niet over als te druk qua hoeveelheid ruimte. Behalve natuurlijk bij de lekkere koffie, een witte bus beneden waar de hele dag een rij stond.

Iedere zichzelf respecterende conferentie heeft tegenwoordig een app met het programma, zo ook de ONE. Maar wat de app van de ONE extra handig maakt, is dat er hier opties waren om ook met deelnemers te chatten of iemands naam op te zoeken als je net een leuk gesprek gehad had. Dat maakt het een stuk makkelijker om contact te leggen via bijvoorbeeld LinkedIn. Ook de innovation expo draagt daaraan bij, met stands van verschillende organisaties. Zo kun je wat makkelijker en laagdrempeliger in contact komen met organisaties met een interessant product. Al blijft het ook de kunst voor beide partijen om vooral contact te maken, wat vragen over en weer te stellen en geen verkooppraatjes te houden.

E-magazine: de moeite waard om terug te lezen

Dan wil ik ook de aandacht nog vestigen op het e-magazine van de ONE met een aantal leuke artikelen over onderwerpen die ook terugkwamen tijdens de conferentie. Van tips van een ethical hacker om veilig te migreren naar de cloud tot de cyberspiekbriefjes (zie iB-Magazine 2022 editie 5 voor een artikel hierover) tot een awareness tool: het staat er allemaal in. Wat mij betreft dus ook de moeite waard om even naar terug te kijken als je dat nog niet gedaan hebt.

Kortom: een geslaagde ONE. Volgend jaar ga ik weer!
Meer informatie kun je vinden op www.one-conference.nl. Hier vind je ook het programma, de sprekers, impressies, het e-magazine en de historie.

COLUMN LEX

Intelligente fraude

AI (Artificial Intelligence) is niet meer weg te denken uit de IT. De rol die het speelt in detectie van de inbreuken van cybersecurity groeit ook. We weten dat AI ingezet wordt om fraude te detecteren. Is AI ook in staat fraudeurs te helpen? Daar moest ik over denken toen ik berichten las over de schaakpartijen tussen Magnus Carlsen en Hans Niemann. Het is al weer vijfentwintig jaar geleden dat een computer (IBM's Deep Blue) in staat was te winnen van een grootmeester (Gary Kasparov). Daar gaat deze column niet over. Maar sinds die winst is er natuurlijk wel een manier voor schakers om vals te spelen met de hulp van een computer.

Schaken is een gewild onderwerp voor valsspelers. Voor de schaakcomputer was er de schaakrobot, de mechanische Turk (1). Dit was echter geen robot, het interne mechanisme werd bestuurd door een dwerg die goed kon schaken. In die tijd kon de mens beter schaken dan de machine. Maar zoals gezegd, die tijd is passé.

En in het internettijdperk is het ook ondenkbaar dat je meldingen kunt vertragen, zodat je je eigen werkelijkheid kunt voorspellen omdat jouw verleden nog de toekomst moet worden waar anderen op wachten, zoals de fraude in de film *The Sting* (2). En voor wie niet oud genoeg is om de film te kennen: een aanrader met in de hoofdrollen Paul Newman en Robert Redford.

Het is dus geen verrassing dat er in deze tijd gewaakt wordt voor een meeschakende supercomputer die zetten voorzegt. Dit is niet zo makkelijk uit te voeren bij livetoernooien, maar onmogelijk is het ook niet. Kuchen uit het publiek of een op afstand bedienbaar trilplaatje in schoenen zijn manieren die in het verleden gevonden zijn bij het ontmaskeren van fraudeurs. Het is uniek dat een hoogstaande schaakspeler publiekelijk van fraude beschuldigd wordt, zonder te zeggen hoe de fraude uitgevoerd wordt.

Grootmeester Magnus Carlsen beschuldigt nieuwkomer Hans Niemann van fraude op basis van gedrag en resultaat. Hans zou niet geconcentreerd genoeg zijn, niet gespannen genoeg op de moeilijke momenten. En dan komen de AI-analyses voor detectie. Het is onwaarschijnlijk dat een schaaktalent zo snel opkomt. Het is onwaarschijnlijk dat hij de sterke zetten zet die hij zette, zonder de hulp van een schaakcomputer, tenminste. En tja, Hans heeft in het verleden valsgespeeld en zijn mentor waarschijnlijk ook.

Het is lastig. Het heeft een hoog 'Computer says Fraud' gehalte. Precies datgene waar we ons tegen willen verzetten wanneer AI gebruikt wordt om een selectie te maken uit een verzameling sollicitanten en we de selectie niet kunnen verklaren. Hebben we het in dit geval over een grootmeester die vergelijkbaar zegt dat Hans niet door de selectie komt? Of is Hans het slachtoffer van een overijverige AI die zijn oppermacht op het schaakbord niet erkent omdat het niet in de leerset zat?

Er gaan stemmen op dat het Hans lukt te frauderen omdat hij niet de hele tijd valsspeelt. Daardoor is er geen afwijkend patroon te herkennen. En daar maak ik me vooral zorgen om. Wat als AI nu ingezet kan worden als counterintelligence om genoeg twijfel te zaaien in de resultaten zodat een AI die ingezet is om fraudedetectie intelligence te verzamelen niet genoeg voer te geven. 'Spy vs. spy' in cyberstijl.

Als dit mogelijk is, dan is het waarschijnlijk ook mogelijk dit soort counterintelligence in te zetten tegen het detecteren van financiële fraude. En dat terwijl AI juist opkomt als detector van verdachte transacties. Staan we aan het begin van een nieuwe wapenwedloop? AI-driven detectie vs. AI-driven deceptie? Wat als AI gaat bepalen waar de cybercriminelen hun pijlen op moeten richten? Mogelijkheden te over.

Referenties
(1) https://en.wikipedia.org/wiki/Mechanical_Turk
(2) https://www.imdb.com/title/tt0070735/

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

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

De bancaire sleepwet

Bij mij om de hoek zat een weelderige interieurwinkel met prachtig potsierlijke objecten. Niet dat er ooit echt klanten binnenkwamen, de prijzen waren exorbitant hoog, de stijl niet geheel passend bij de inwoners van het toch wat kakkerig chique Statenkwartier. De winkel kreeg pas echt bekijks toen de politie met enig bombarie de zaak binnenviel en vervolgens met tape afsloot. De eigenaresse werd in boeien afgevoerd. Eindelijk gebeurde er weer eens wat spannends in deze doorgaans toch beschaafde, rustige wijk. Enige tijd later werd de inventaris per veiling verkocht. Op de ophaaldag zat de eigenaresse – inmiddels weer op vrije voeten – in haar auto iedereen te filmen die met 'haar' waren de winkel verliet. Deze meubelzaak, en een aantal andere zaken, bleken gebruikt te worden om crimineel geld wit te wassen.

Banken en andere financiële instellingen hebben het er maar druk mee. Honderden medewerkers worden ingezet om te kunnen voldoen aan de vanuit de EU afkomstige wetgeving ter bestrijding van witwassen en het financieren van terrorisme. Dat doen zij door personen en bedrijven te screenen en verdachte transacties te melden. Heel veel gebeurt nog ouderwets met de hand en is daardoor enorm arbeidsintensief. In Noorwegen maken ze een begin met het automatiseren van een en ander door de inzet van algoritmes. Hoewel een logische ontwikkeling, kleven ook daar weer haken en ogen aan – ons eigen Nederlandse toeslagenschandaal indachtig.

Onze Nederlandse wetgever doet er een schepje bovenop en wil graag ook nog eigen wetgeving invoeren. Daarin stelt zij voor om in een centrale database alle transacties van alle Nederlanders vast te leggen. De monitoring van die transacties gebeurt door middel van – je raadt het al – algoritmes. In Nederland kon je de diepe zucht en de face palm van alle privacy- en securityspecialisten tot in de verte horen. Zij voelen zich daarin gesteund door de Autoriteit Persoonsgegevens die in haar wetgevingsadvies zeldzaam vernietigend over dit voorstel spreekt. Het voorgestelde systeem komt in essentie neer op een bancair sleepnet, aldus de AP. *'Goede wetgeving draagt bij aan het aanpakken van witwassen zonder onnodig de grondrechten van alle burgers in te perken. Dat is met dit voorstel zeker niet het geval. Mensen zijn onschuldig tot het tegendeel is bewezen. Door iedereen standaard in de gaten te houden, wordt er aan dit fundamentele beginsel van de rechtsstaat getornd.'*

De niet mis te verstane kritiek op het wetsvoorstel werd ook bevestigd door de Raad van State. De RvS schrijft in zijn wetgevingsadvies: *'Hoe belangrijk de bestrijding van witwassen en van financiering van terrorisme ook is, bij deze maatregelen is de vraag of het doel de middelen die worden voorgesteld, wel heiligt. Deze middelen gaan in de huidige opzet van het wetsvoorstel te ver.'* De RvS ziet ook gevaren voor uitsluiting en discriminatie en hekelt het feit dat de wet niet voorziet in maatregelen om de rechten en vrijheden van burgers te beschermen. Het kabinet heeft zich de felle kritiek aangetrokken en heeft inmiddels toegezegd dat zij het wetsvoorstel zal aanpassen. De reikwijdte wordt beperkt en er zullen waarborgen worden ingebouwd. Over die centrale database heeft het kabinet zich niet uitgelaten, helaas.

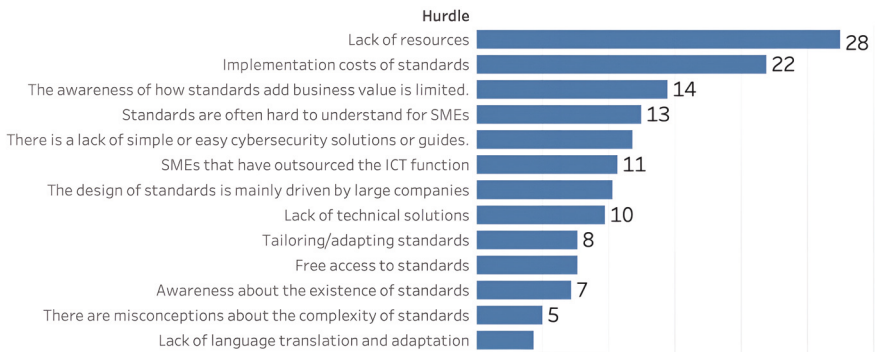
Rachel

Auteur: Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Dit artikel is geschreven op persoonlijke titel.

Cybersecurityinzichten voor het mkb

Midden- en kleinbedrijven (mkb) zijn de drijfveer van de meeste economieën op de wereld (1): ongeveer 99% van de economische activiteiten binnen Europa zijn te herleiden naar het mkb (2). Het doorgaans lage eigen vermogen van het mkb maakt hen gevoelig voor risico's (3); 60% van de cyberaanvallen zorgt voor een faillissement bij het mkb (4).

Het beveiligen van het mkb is dus belangrijk. Toch is er weinig aandacht voor cybersecurity bij het mkb. Cybersecurityframeworks, en standaarden zijn niet gericht op kleinere bedrijven, en wetenschappelijk onderzoek heeft tot nu toe ook (te) weinig aandacht gegeven aan dit thema (5). Het afgelopen jaar heb ik samen met de Antwerp Management School onderzoek gedaan naar cybersecurity bij het MKB. In dit artikel deel ik drie inzichten van dat onderzoek.



Figuur 1 - Puntenverdeling door onderzoekdeelnemers over 13 hindernissen.

Inzicht 1 - Factoren die de implementatie van een standaard verhinderen

Om de impact van cyberrisico's te verminderen, moeten organisaties hun niveau van cybersecurityvolwassenheid afstemmen op het risico dat ze bereid zijn te nemen. Echter, heeft het mkb niet de middelen om volwassenheid te kunnen bereiken (5). En dat heeft grote gevolgen voor het mkb, maar eveneens bij grotere organisaties omdat bij 99% van de economische activiteiten het mkb actief is.

Omdat het mkb dus zo economisch actief, is het van belang dat het mkb digitaal veiliger wordt. Alleen kan het mkb dat niet enkel op eigen kracht. Hulp zou kunnen komen in de vorm van subsidies, niet ter beschikking gestelde tools van grote organisaties of door ondersteuning van banken en hun netwerken. Om richting te geven zouden er ook duidelijkere standaarden gemaakt kunnen worden voor het mkb. Zo is het European Digital SME Alliance onder andere bezig met het ontwikkelen van standaarden (6).

Accountancy, een branche die al volwassen is in het stellen van internationale standaarden, heeft ook aanpassingen aan de standaarden gemaakt voor het mkb. Toen de Financial Reporting Standard (ISRS) gepubliceerd werd, bleek dat het implementeren van deze standaard niet ten goede kwam aan het mkb, vooral omdat kleinere bedrijven niet over passende middelen beschikken. Uiteindelijk publiceerde de International Accounting Standards Board (IASB) een aangepaste standaard voor het mkb. In een publicatie van de European Digital SME Alliance worden 13 hindernissen opgesomd die het voor de midden- en kleinbedrijven moeilijk maken om een standaard te implementeren (7). Tijdens een onderzoeksessie gaven de deelnemers met behulp van een puntensysteem aan welke van deze hindernissen het meest verstorend waren.

Twee hindernissen staken uit boven de rest:

1. Gebrek aan middelen;
2. De kosten voor het implementeren van de standaard.

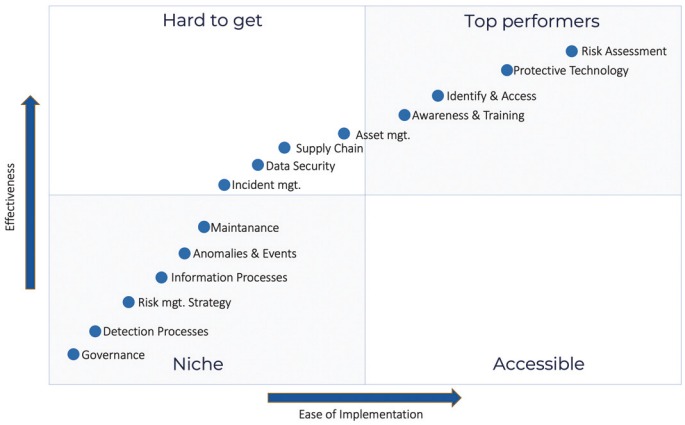
Het gebrek aan middelen en de kosten van implementatie blijken veruit de grootste hindernissen te zijn voor het invoeren van een cybersecuritystandaard bij het mkb. Om het probleem om te lossen zou het mkb beter geïnformeerd moeten worden om de juiste prioriteiten te stellen. Daarnaast zouden grotere organisaties het mkb kunnen steunen door informatie en middelen te delen met het mkb.

Inzicht 2 - Focus

In het onderzoek hebben experts de categorieën van het NIST Cybersecurity Framework beoordeeld. Elke categorie werd geëvalueerd op effectiviteit en het gemak van implementatie. Hieruit is het `SMB Cybersecurity Quadrant' ontstaan (figuur 2). Dit Quadrant onthult welke maatregelen effectief zijn en welke juist helemaal niet. Zo blijkt uit het onderzoek dat een riscoassessment de beste categorie is om te implementeren. In tegenstelling blijkt `governance' niet goed te scoren in een mkb-context. De maatregelen bij het mkb moeten vooral praktisch en simpel zijn en niet te veel middelen kosten.

Het Quadrant legt vier focuspunten bloot voor goede cybersecuritymaatregelen voor het mkb:

1. Risicoassessment;
2. Protective Technology;
3. Identity & Access;
4. Awareness & Training.



Figuur 2 - SMB Cybersecurity Quadrant (V. van Dijk, 2022).

Risicoassessment

Het merendeel van de lezers heeft wel eens een risicoassessment gedaan. Toch worden deze assessments vaak overgeslagen bij het mkb. Een risicoassessment werkt bij het mkb namelijk ook net wat anders dan gebruikelijk. Bij het mkb is het handig om risico niet alleen te zien als 'kans maal impact'. Gebruik in plaats daarvan de ISO-definitie: 'The effect of uncertainty on objectives' (het effect van onzekerheid op de doelstellingen).
Je kunt een risicoassessment bij het mkb in drie simpele stappen doen. Ga niet te veel de diepte in, want dan sla je de plank mis:

1. Bepaal de doelstellingen van het bedrijf;
2. Bepaal de doelstellingsonzekerheden;
3. Zoom daarna in op de (cyber)risico's.

Bedenk dat dit niet betekent dat je als ondernemer enkel oog moet hebben voor de (cyber)risico's, maar er juist op moet letten dat je het bedrijf als geheel (holistisch) blijft bekijken. Het mkb behandelt namelijk alle risico's onder de algemene bedrijfsvoering; zonder de bedrijfsrisico's kun je geen goede vergelijking maken. En zonder een goede vergelijkingsbasis wordt het nemen van goede beslissingen lastig. Het kan namelijk zo zijn dat een hoog risico buiten de cyberspace meer aandacht en budget nodig heeft dan een cyberrisico.

Protective Technology

Na het nagaan van je risico's is het tijd om aan de slag te gaan met protective technology. Met andere woorden: securityproducten die je gemakkelijk kunt implementeren en waarnaar je weinig omkijken hebt. Denk hierbij aan firewalls, endpoint protection, backups en managed cybersecurityservices.
Zorg ervoor dat de kosten die je maakt logisch zijn. Gemiddeld genomen heeft het mkb een winstmarge van 5 tot 10%. Als we uitgaan van 10% betekent dit, dat een midden- en kleinbedrijf met 10 miljoen euro omzet, 1 miljoen euro winst maakt. Een securityoplossing van 100.000 euro per jaar snoept dan dus meteen 10% van de winst weg en is wellicht niet rationeel qua omvang!

Identity & Access

Meestal heb je bij kleinere bedrijven geen extra producten nodig om Identity & Access goed te regelen. Identity & Access gaat namelijk vooral om het invoeren van een goed en sterk proces, waarbij de toegang wordt goedgekeurd en er een overzicht is van de uitgegeven rechten, gebruikers en applicaties. Met een eenvoudig maar degelijk proces kun je bij het mkb prima besparen op je maatregelen, omdat je niet per se nieuwe technologie hoeft aan te schaffen.

Awareness & Training

Awareness & Training is een categorie van maatregelen waarvoor je niet per se dure technologie hoeft aan te schaffen. Zo kun je 1 à 2 personen opleiden tot security champions. Deze champions kunnen de awareness en trainingen geven en daarnaast vragen beantwoorden. In plaats van trainingen zou je ook kunnen denken aan coaching. Het is een optie om security champions maandelijks te coachen bij het uitvoeren van hun training en awareness-activiteiten.

Inzicht 3: Flexibiliteit by design

Het mkb staat bekend om zijn flexibiliteit. In tegenstelling tot grote organisaties, kan het mkb zichzelf eenvoudiger en sneller veranderen. En dat moet ook wel: flexibiliteit is één van de meest gewaardeerde eigenschappen van het mkb. De huidige zakelijke omgeving is ingewikkeld en lastig te voorspellen, dus bedrijven moeten flexibel zijn om te blijven draaien. In de snelle en altijd veranderende wereld van vandaag is het vermogen van een organisatie om te veranderen een concurrentievoordeel. Mee veranderen met de omgeving is voor het voortbestaan van het mkb essentieel. De wetenschap ondersteunt het idee dat het mkb flexibel moet zijn. Uit onderzoek blijkt bijvoorbeeld dat er vanuit strategisch oogpunt een positieve connectie bestaat tussen

strategische flexibiliteit en de prestaties van het mkb. Cyberbeveiligingsstrategieën moeten ook flexibel zijn, zodat midden- en kleinbedrijven zich kunnen aanpassen aan het dynamische karakter van de bestaande en toekomstige risico's.
Uit onderzoek is gebleken dat een cybersecuritystrategie flexibel moet zijn by design, oftewel, de focus moet vanaf het begin op flexibiliteit liggen (5). Op basis van deze criteria is er een flexibele aanpak ontstaan: het Cybersecurity Canvas. Met dit Canvas kan je pragmatisch een cybersecuritystrategie opstellen.

Figuur 3 - Een voorbeeld van Cybersecurity Canvas dat is opgesteld tijdens een workshop met 20 Vlaamse gemeentes.

Het Cybersecurity Canvas bestaat uit twee componenten:

- Aan de linkerkant het bedrijf;
- Aan de rechterkant de maatregelen.

Aan de linkerkant, binnen de bedrijfscomponent, wordt de vraag gesteld: waarom? Waarom moet het bedrijf zich bezighouden met cybersecurity? Daarnaast worden de risico's genoemd. De rechterkant houdt zich bezig met de maatregelen. Deze worden gekozen op basis van de meest effectieve categorieën aan de hand van de specifieke risico's die de organisatie ervaart.

Conclusie

Ongeveer 99% van de economische activiteiten binnen Europa zijn te herleiden naar het mkb (2), maar het mkb kan zichzelf op het moment niet goed beveiligen (5). Meer organisaties moeten betrokken worden bij het beveiligen van het mkb. Zo zouden grotere organisaties maatregelen en informatie kunnen delen met de midden- en kleinbedrijven met wie ze zaken doen.

Hulp zou ook kunnen komen in de vorm van subsidies of gratis middelen vanuit grote organisaties.
Daarnaast moet cybersecurity anders aangepakt worden bij het mkb. Het beveiligen van het mkb werkt namelijk net wat anders. Het mkb heeft een pragmatische, simpele en flexibele aanpak nodig (8). Om richting te geven zouden er ook duidelijkere standaarden gemaakt kunnen worden voor het mkb die pragmatisch, eenvoudig en flexibel zijn.
De nieuwe aanpak moet focus aanbrengen op de vier meest effectieve NIST-categorieën (9). Zo zullen we het mkb en daarmee ook de (Nederlandse) economie een stukje veiliger maken.

Referenties

(1) Burgstaller, J., & Wagner, E. (2015). How do family ownership and founder management affect capital structure decisions and adjustment of SMEs? *Journal of Risk Finance

(2) Gama, A. P. M., & Geraldes, H. S. A. (2012). Credit risk assessment and the impact of the New Basel Capital Accord on small and medium-sized enterprises. Management Research Review, 35(8), 727–749.

(3) Altman, E. I., Sabato, G., & Wilson, N. (2008). The Value of Non-Financial Information in SME Risk Management. https://doi.org/10.2139/ssrn.1320612

(4) Munro, D. 2013. A Guide to Financing SMEs. New York: Palgrave Macmillan.

(5) van Dijk, V. (2022, July 4). Research - A cybersecurity standard for SME. Security Scientist. https://www.securityscientist.net/blog/research-a-cybersecurity-standard-for-sme/

(6) Zie https://www.digitalsme.eu/

(7) European Digital SME Alliance. (2020). *The EU Cybersecurity Act and the role of standards for SMEs*. https://www.digitalsme.eu/digital/uploads/The-EU-Cybersecurity-Act-and-the-Role-of-Standards-for-SMEs.pdf

(8) Het is goed om bewust ervan te zijn dat het MKB een speciale cybersecurity aanpak nodig heeft. Dat is de conclusie uit het onderzoek. De speciale aanpak bestaat uit een pragmatische, simpele en flexibele aanpak. Het resulteerde in twee prachtige gereedschappen: het "SMB Cybersecurity Quadrant" en het "Cybersecurity Canvas". https://www.securityscientist.net/blog/research-a-cybersecurity-standard-for-sme/

(9) Het Quadrant legt vier focuspunten bloot voor goede cybersecuritymaatregelen voor het MKB: 1. Risk Assessment 2. Protective Technology 3. Identity & Access 4. Awareness & Training

Auteur: Maarten Hartsuijker is redactielid van iB-Magazine en helpt als ethisch hacker organisaties met het pentesten en scannen van applicaties en netwerken. Maarten is te bereiken via: m.hartsuijker@classity.nl.

Kraak de kluis

Ocean's Eleven, King of Thieves, The Italian Job… In Hollywood grossieren ze in films waarin good guys of bad guys een meesterplan bedenken voor het kraken van de kluis. Tegenwoordig niet zelden samen met een meesterhacker die de laatste technologische beveiligingen moet zien te kraken. Zelf maken we op internet ook steeds vaker gebruik van een kluis: de wachtwoordkluis. En soms blijkt het kraken van die kluis kinderlijk eenvoudig.

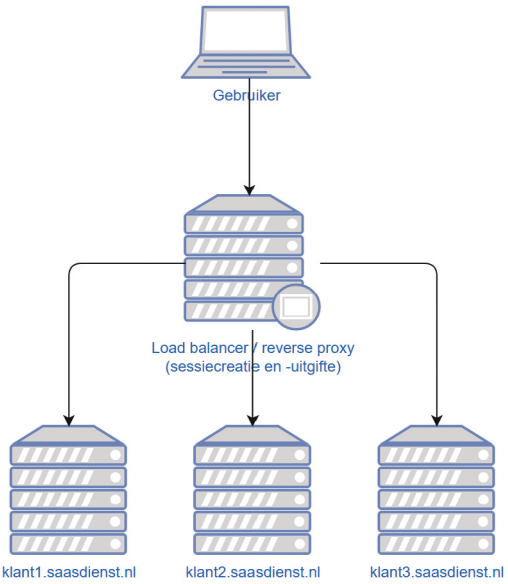
Een goede wachtwoordkluis heeft natuurlijk end-to-end-beveiliging die borgt dat wachtwoorden vóórdat ze naar de opslaglocatie worden verzonden, versleuteld worden met een encryptiesleutel die is afgeleid van een door de eigenaar verzonden hoofdwachtwoord. Deze aanpak borgt dat iemand die de kluis kraakt alleen versleutelde wachtwoorden kan stelen. En niet de wachtwoorden zelf. Dit klinkt logisch (en veel wachtwoordkluizen hanteren deze aanpak), maar sommige kluizen hebben deze extra beveiliging niet. Toegang tot een gebruikersaccount betekent in dat geval toegang tot de wachtwoorden in de kluis.

Security by design: persoonlijk encryptiesleutel

Inmiddels alweer een paar jaar geleden mocht ik voor een klant een Identity en Access Management-oplossing onderzoeken. De tool zou de gebruikers van de organisatie gaan helpen om via één plek alle applicaties toegankelijk te maken. Gebruikers hoefden per applicatie slechts één keer hun wachtwoord in te geven, dat vervolgens de kluis in ging om automatisch te worden ingevuld zodra er op een applicatie werd ingelogd. Het principe werkte prachtig en was al bij vele Nederlandse organisaties succesvol in gebruik. De eerste security by design-bevinding werd direct zichtbaar: gebruikers hoefden alleen op een webportaal in te loggen om hun wachtwoorden te gebruiken. Er werd geen hoofdwachtwoord gevraagd. Hierdoor kon elke beheerder na een wachtwoord reset van het kluisaccount een medewerkersidentiteit overnemen. De mogelijkheid impliceert ook dat de wachtwoorden in de kluis niet volledig end-to-end beschermd zijn. Een inbraak in deze cloud zou daardoor eenvoudig tot een grote supply chain aanval kunnen leiden. Waaronder op de organisatie van mijn klant, die daarom besloot de applicatie onafhankelijk te laten toetsen zodat hij de beveiligingsrobuustheid beter kon inschatten. Zoals van dit product verwacht mag worden was de basisbeveiliging op orde. Firewalls, reverse proxies, beveiligingsupdates, wachtwoordpolicy, datavalidatie, MFA-mogelijkheden… De usual suspects leverden niet direct iets op. Maar in het sessiemanagement was iets vreemds aan de hand.

Opzet van de dienst

Klanten van de dienst werden voorzien van hun eigen virtuele bedrijfskluis: klant.saasdienst.nl. Elke kluis had zijn eigen accountbeheer, kluisopslag, et cetera. Voor de klantomgevingen stond een centrale toegangsvoorziening (load balancer). Iedereen die succesvol inlogde kreeg van de toegangsvoorziening een sessiecookie. Op het klantsysteem kon aan de hand van het sessiecookie worden gecontroleerd wie de gebruiker was. Tot zover leek er weinig mis. De sessiecookies waren door hun willekeurigheid niet te voorspellen. En zonder sessiecookie kon de toegangsvoorziening niet worden gepasseerd en was er geen toegang tot de klantkluis mogelijk. En toch bleek deze sessiecookie de sleutel tot het overnemen van de hele SAAS-dienst en alle kluizen.



Figuur 1 - Diagram kraak de kluis.

Geen tenant controle

De architectuurkeuze om het sessiemanagement te ontkoppelen van de klantomgevingen zorgde ervoor dat sessiecookies binnen alle klantomgevingen bruikbaar waren. Want hoewel de klantapplicaties aan de hand van het cookie controleerde welke gebruiker er aan het cookie was gekoppeld, werd er niet vastgesteld voor welke klantomgeving het cookie was uitgegeven. Een beheerder hoefde daardoor enkel een account aan te maken met een gebruikersnaam gelijk aan een gebruiker van een andere omgeving om (in combinatie met een kleine aanpassing in de applicatieverzoeken) toegang te krijgen tot dat account in die omgeving. Daarbij werd hij overigens geholpen door het feit dat de naam van de key-user in alle klantomgevingen gelijk was. De kluis kon in dit geval dus eigenlijk 'gekraakt' worden doordat de sessiesleutel onbedoeld een loper was geworden. Een loper die het mogelijk maakte om alle kluizen te openen waarin zich de sleutels van vele bedrijfsapplicaties van alle klanten van deze IAM-dienst bevonden. En een loper waarvan de applicatiearchitect vol ongeloof eerst de werking wilde zien voordat hij écht overtuigd was dat hij bestond. Twee uur later was de loper overigens onbruikbaar. Met de oplostijd was niets mis.

Ignorance is bliss

Net als in Hollywood hebben ook in dit geval de eigenaren van de kluis vermoedelijk nooit geweten hoe eenvoudig hun kroonjuwelen in die kluis voor onbevoegden toegankelijk waren. Maar het ontwerp van de kluis had iedereen eigenlijk vrij eenvoudig kunnen valideren. Want een wachtwoordkluis in de cloud zonder een van een persoonlijk masterwachtwoord afgeleide encryptiesleutel, hoor je eigenlijk vandaag de dag niet meer in gebruik te nemen.

Auteurs: Luuk Bekkers, MSc. PhD-kandidaat, hij is te bereiken via: l.m.j.bekkers@hhs.nl. Dr. Susanne van 't Hoff-de Goede, onderzoeker, zij is te bereiken via: m.s.vanthoff-degoede@hhs.nl. Dr. Rutger Leukfeldt, directeur & lector. Allen werken zij voor het Centre of Expertise Cyber Security, De Haagse Hogeschool. Rutger is ook senior onderzoeker bij het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving. Rutger is te bereiken via: e.r.leukfeldt@hhs.nl. Dr. Remco Spithoven is lector, Lectoraat Maatschappelijke Veiligheid, Hogeschool Saxion en te bereiken via: r.spithoven@saxion.nl.

Wat motiveert mkb'ers om actie te ondernemen tegen ransomware?

Slachtofferschap van ransomware – software die bestanden of systemen versleutelt als drukmiddel om slachtoffers losgeld te laten betalen – is een groeiend probleem voor bedrijven in Nederland. Tot wel 17% van de Nederlandse mkb'ers zegt ooit slachtoffer te zijn geworden van dit delict. Toch nemen ondernemers nog te weinig maatregelen om hun bedrijf tegen ransomware en andere vormen van cybercriminaliteit te beschermen. Hoe kunnen we de weerbaarheid van het mkb vergroten?

Tegenwoordig behoort ransomware tot de meest voorkomende vormen van cybercriminaliteit onder het mkb (1,2). Ransomware is kwaadaardige software die data of een computer(systeem) versleutelt, waardoor de toegang tot die data wordt ontzegd (3). Pas als het slachtoffer een geldbedrag betaalt ('losgeld'), maken criminelen de gegevens weer beschikbaar. Midden- en kleinbedrijven vormen in het bijzonder een doelwit omdat hun cybersecurity vaak onvoldoende is. Vaak ontbreekt cybersecuritybeleid, worden wachtwoorden opnieuw gebruikt en zijn de maatregelen die worden genomen onder de maat of worden deze slecht geïmplementeerd (2,4,5). Met andere woorden: Nederlandse ondernemers hebben doorgaans een lage mate van cyberweerbaarheid en zijn daarom kwetsbaar voor slachtofferschap van ransomware.

Onbekend is echter nog hoe het komt dat ondernemers maar weinig maatregelen nemen en hoe ze gemotiveerd kunnen worden hun bedrijf beter te beschermen tegen ransomware. Daarom hebben De Haagse Hogeschool en Hogeschool Saxion recent met verschillende partners (o.a. gemeenten, regionale veiligheidsnetwerken, de FraudeHelpdesk en het CCV) een onderzoek uitgevoerd naar psychologische processen die kunnen verklaren waarom ondernemers zich wel of niet beschermen tegen ransomware. Hierbij is ook onderzocht wat verschillen zijn tussen ondernemers die een extern cybersecuritybedrijf inschakelen en ondernemers die dat niet doen. Met deze kennis zijn overheidspartijen en IT-professionals beter in staat om ondernemers te helpen zich te wapenen te voorkomen om slachtoffer te worden van ransomware. In dit artikel bespreken we de belangrijkste bevindingen van het onderzoek.

Factoren die een rol spelen bij zelf-beschermend gedrag: PMT

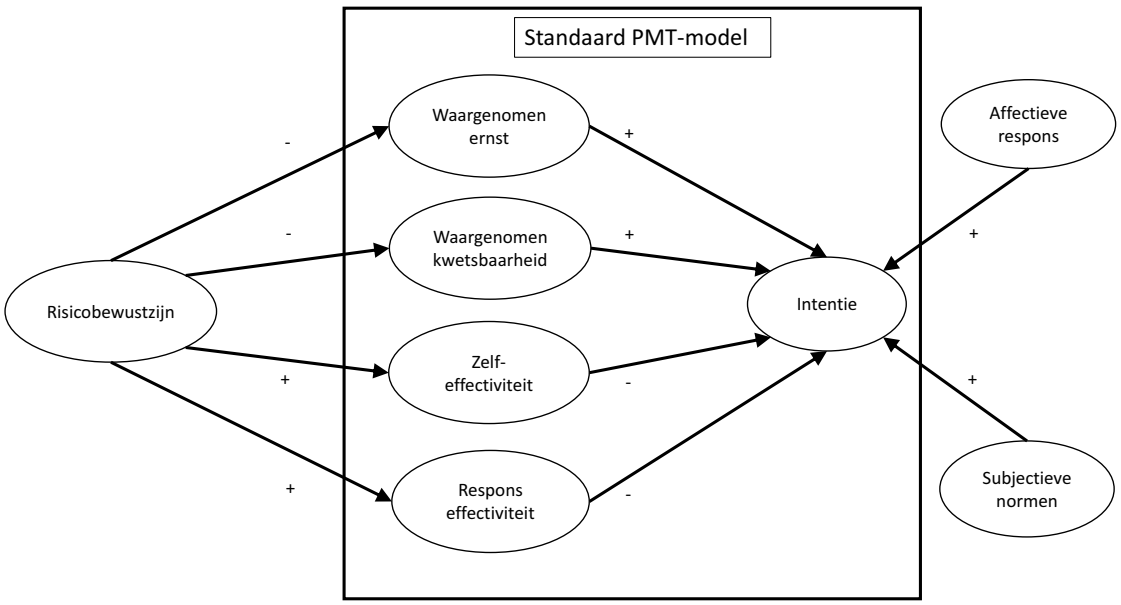
In het onderzoek fungeert de 'Protectie-Motivatie Theorie' (PMT) als het theoretisch raamwerk (6,7). PMT tracht te verklaren waarom mensen de intentie hebben om zich tegen een bepaald risico te beschermen. Toegepast op ransomware, veronderstelt de theorie dat ondernemers zelf-beschermend gedrag vertonen als ze denken dat hun bedrijf kwetsbaar is voor ransomware (waargenomen kwetsbaarheid) en als ze overtuigd zijn dat blootstelling aan ransomware ook ernstige gevolgen kan hebben voor hun bedrijf (waargenomen ernst). Daarnaast is ook respons effectiviteit van belang, ofwel de mate waarin ondernemers van mening zijn dat het zin heeft om hun bedrijf te beschermen tegen ransomware. Ten slotte veronderstelt de theorie dat mensen een schatting maken over hun eigen capaciteiten (zelf-effectiviteit): pas als ondernemers zichzelf in staat achten hun bedrijf te kunnen beschermen, gaan ze dat ook doen. Samen spelen deze vier factoren van het PMT-model mogelijk een rol bij de intentie van ondernemers om cybersecuritymaatregelen te nemen tegen ransomware.

Uitbreiden PMT-model

Hoewel het PMT-model waardevolle inzichten biedt, is het niet volledig bruikbaar als we deze toepassen op de weerbaarheid van het mkb tegen ransomware, want ook andere factoren hebben mogelijk een invloed op het zelf-beschermend gedrag van ondernemers. Daarom hebben we voor dit onderzoek op basis van bestaande literatuur drie factoren toegevoegd aan het PMT-model: 'risicobewustzijn' (8,9), 'affectieve respons' (8) en 'subjectieve normen' (9,10). Risicobewustzijn gaat over de mate waarin ondernemers weten wat de risico's zijn van ransomware. Affectieve respons heeft betrekking op de gevoelsmatige reactie op ransomware, ofwel de mate waarin ondernemers zich zorgen maken: de verwachting is dat hoe meer zorgen ze zich maken, hoe groter de kans dat ze maatregelen nemen. Ten slotte refereert subjectieve norm aan de waargenomen sociale druk van mensen uit de sociale omgeving om maatregelen te nemen. We veronderstelden dat wanneer ondernemers denken dat branchegenoten of ketenpartners van hen verwachten dat ze hun eigen bedrijf beschermen, de ondernemers eerder geneigd zijn dat ook te doen.

Unieke dataset

Op basis van wetenschappelijke literatuur is een vragenlijst ontwikkeld om de genoemde factoren te meten. Deze vragenlijst is vervolgens uitgezet onder een groot panel van 2000 Nederlandse zzp'ers en eigenaren van bedrijven tot 250 werknemers. In totaal hebben 1020 respondenten de vragenlijst volledig ingevuld. Deze unieke, grote dataset geeft inzicht in een populatie die relatief kwetsbaar is voor slachtofferschap van cybercriminaliteit, maar doorgaans zeer moeilijk is te bereiken voor wetenschappelijk onderzoek. Nadat de data was verzameld, zijn statistische analyses uitgevoerd om een gedetailleerd beeld te krijgen van de invloed van de bovengenoemde factoren op de gedragsintentie ten aanzien van het nemen van maatregelen tegen ransomware in de toekomst.



Figuur 1 - Resultatenanalyse.

Bevindingen

Figuur 1 betreft een overzicht van de resultaten van de analyse. Een + (plus) geeft een positief verband weer: hoe hoger de score op de ene variabele, hoe hoger de score op de ander. Een – (min) daarentegen vertegenwoordigt een negatief verband: hoe hoger de score op de variabele aan het begin van de pijl, hoe lager de score op de variabele aan het einde van de pijl.

Uit onze analyse blijkt dat de intentie om meer maatregelen tegen ransomware te nemen direct wordt verhoogd wanneer ondernemers zich zorgen maken over de risico's (affectieve respons) en wanneer ze ervan overtuigd zijn dat andere mensen in hun omgeving verwachten dat zij maatregelen nemen (subjectieve normen). Ook is de kans groter dat ondernemers hun bedrijf beschermen tegen ransomware wanneer zij hun bedrijf kwetsbaar achten voor slachtofferschap van ransomware (waargenomen kwetsbaarheid) en als zij van mening zijn dat dit kan leiden tot ernstige gevolgen in termen van verlies van geld en tijd (waargenomen ernst). Al deze bevindingen waren in lijn met onze verwachtingen. Dit beeld bleek echter wel anders te zijn voor de groep ondernemers die hun cybersecurity uitbesteedt: zij beschouwen hun bedrijf minder kwetsbaar voor ransomware, waardoor ze minder gemotiveerd zijn om zelfbeschermend gedrag te vertonen.

Verder komt naar voren dat ondernemers juist minder geneigd zijn zich te beschermen tegen ransomware als zij geloven dat zij daartoe in staat zijn (zelf-effectiviteit) en overtuigd zijn dat het nemen van maatregelen ook zin heeft (respons effectiviteit). Deze bevindingen stonden haaks op onze verwachtingen. Een mogelijke verklaring hiervoor is dat ondernemers zichzelf overschatten: zodra ondernemers denken dat zij hun bedrijf inderdaad kunnen beschermen tegen ransomware, zien ze mogelijk minder risico in ransomware en nemen ze dus minder snel actie. De notie van overschatting komt ook terug bij de rol van risicobewustzijn in de analyse: als ondernemers meer weten over de risico's van ransomware, beschouwen zij zichzelf minder kwetsbaar en schatten ze de gevolgen van een ransomware aanval minder hoog in, waardoor ze geen aanvullende maatregelen nemen. Meer onderzoek is nog wel nodig om de mogelijke rol van overschatting bij ondernemers beter in kaart te brengen.

Hoe weerbaarheid tegen ransomware verhogen?

Onze resultaten wijzen erop dat het informeren van ondernemers over ransomware een uiterst gevoelige benadering vereist. Het verstrekken van informatie kan er immers toe leiden dat ondernemers hun eigen capaciteiten onrealistisch hoog inschatten, zichzelf veilig wanen en hun bedrijf daarom juist minder goed beschermen. Dat is in het bijzonder het geval voor ondernemers die hun cybersecurity extern hebben belegd. Het uitbesteden van cybersecurity wil echter niet zeggen dat een bedrijf ook veilig is en geen slachtoffer meer kan worden. Daarom is het belangrijk dat IT-dienstverleners een open en eerlijke relatie onderhouden met hun cliënten, specifiek benadrukken dat ondernemers zelf de eindverantwoordelijkheid hebben om slachtofferschap van ransomware te voorkomen en naast het nemen van technische en organisatorische maatregelen ook het personeel alert maken. Bovendien blijken ondernemers gevoelig voor invloeden vanuit hun omgeving. Benoem dus expliciet dat andere ondernemers hun bedrijf ook beschermen: dat is de norm. Collega-ondernemingen die maatregelen hebben genomen, eventueel nadat zijzelf slachtoffer van ransomware zijn geworden, kunnen als rolmodel fungeren.

Verder komt uit ons onderzoek naar voren dat tijd, geld en complexiteit van cybersecurity belangrijke barrières zijn voor ondernemers. Adviseer ondernemers daarom over gebruiksvriendelijke maatregelen en biedt ze perspectief op hoe zij concreet kunnen handelen om het risico op ransomware in hun specifieke situatie te beperken. Hierbij kan het helpen om een emotionele reactie onder de ondernemers teweeg te brengen, bijvoorbeeld door te benoemen dat ook de individuele ondernemer kans heeft om slachtoffer te worden en door uit te leggen dat slachtofferschap grote consequenties kan hebben voor het bedrijf.

Conclusie

In deze studie hebben wij onderzocht hoe het komt dat Nederlandse ondernemers hun bedrijf vaak slecht beschermen tegen ransomware en hoe ze gemotiveerd kunnen worden meer maatregelen te nemen. Hieruit is gebleken dat de motivatie van ondernemers wordt beïnvloed door een vrij complex samenspel van verschillende sociaalpsychologische factoren. Zo zijn ondernemers van plan zich beter te beschermen tegen ransomware wanneer zij zich zorgen maken over de risico's, wanneer ze denken dat andere mensen in hun omgeving van ze verwachten dat ze maatregelen nemen, wanneer ze hun bedrijf kwetsbaar achten en wanneer ze ervan overtuigd zijn dat slachtofferschap grote gevolgen kan hebben. Ondernemers nemen opvallend genoeg juist minder snel maatregelen wanneer zij geloven dat ze daartoe in staat zijn en wanneer ze overtuigd zijn dat het zin heeft om maatregelen te nemen. Dat komt mogelijk omdat ondernemers zichzelf overschatten. Professionals kunnen onze resultaten gebruiken om het gedrag van ondernemers te veranderen en daarmee de weerbaarheid tegen ransomware-aanvallen te verhogen.

Referenties

(1) Notté, R. J., Slot, L., van 't Hoff-de Goede, S. & Leukfeldt, E. R. (2019). Cybersecurity in het mkb. De Haagse Hogeschool.

(2) Johns, E. (2021). Cyber Security Breaches Survey. Department for Digital, Culture, Media & Sport.

(3) Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10-21.

(4) Rohn, E., Sabari, G., & Leshem, G. (2016). Explaining small business InfoSec posture using social theories. Information & Computer Security, 24(5), 434-556.

(5) Osborn, E., & Simpson, A. (2018). Risk and the small-scale cyber security decision making dialogue- UK case study.

(6) Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93-114.

(7) Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A Revised theory of protection motivation. In J. T. Cacioppo, & R. E. Petty (Eds.), Social Psychophysiology: a source book (pp. 153-176).

(8) De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 1-13.

(9) Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. Computers in Human Behavior, 92, 139-150.

(10) Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter? Systemes d'Information Management, 22(3), 7-45.

Informatiebeveiliging heeft een proces van continu verbeteren nodig!

Wat een jaar hebben we weer gehad. De crisissen volgden elkaar op, van covid naar de oorlog in Oekraïne, naar de energie- en inflatiecrisis als gevolg van enerzijds de oorlog maar ook dat we helemaal 'los' gingen na de lockdownperiode. En nu ondervinden we weer de eerste signalen van een volgende covidbesmettingsgolf. Kortom: de toekomst is steeds moeilijker te voorspellen. En het is steeds onduidelijker wat je nu precies moet doen om 'voldoende' weerbaar te zijn op security- en privacyvlak én te blijven in deze veranderende wereld.
Als achtergrond voor degenen die mij (helemaal) niet kennen: ik maak al meer dan negen jaar deel uit van het PvIB-bestuur als penningmeester. Dat laatste betekent niet dat ik op jullie geld zit. Aan de ene kant gaat het om (on)kosten in de gaten te houden zodat het geld juist en effectief wordt besteed. Anderzijds draag ik er zorg voor dat we als vereniging mooie, interessante en nuttige zaken voor en met jullie kunnen doen. Ook andere bestuursleden hebben het al gezegd: wij zijn bijzonder geïnteresseerd in hoe jullie ervaren wat wij als vereniging doen of wat we eigenlijk (nog meer of anders) zouden moeten doen. Vooral hoe we jullie nog beter kunnen laten groeien in ons vakgebied. Want dat is en blijft hard nodig.
Naast mijn PvIB-activiteit ben ik als Trusted Advisor Cybersecurity vanuit Sogeti betrokken bij complexe en inspirerende verbetertrajecten op het vlak van GRC (Governance, Risk & Compliance). Bij deze activiteiten word ik vaak betrokken bij projecten die nodig zijn om een organisatie op het vlak van informatiebeveiliging on-par te krijgen. Gezien het steeds veranderende landschap (zoals naleving van regelgeving, interne aanpassingen en externe bedreigingen), moet er prioriteit gegeven worden aan hiaten vanuit het perspectief van bedrijfsrisico's. Mijn visie is dat het hebben van een robuust beveiligingsmodel niet betekent dat alle hiaten direct en tegelijk moeten worden aangepakt. Ja natuurlijk moet er nagedacht en gewerkt worden aan een securityvisie en -strategie. Echter voor de korte termijn: wees eerst maar eens bewust onbekwaam en richt je bij de volgende stappen op wat nú nodig is binnen een continu verbeterproces. Oftewel: maak de eerste stappen richting het gewenste volwassenheidsniveau. Het begint met het inschatten van het dreigingslandschap en het bepalen van de urgentie. Integreer securityassessments in elke fase waardoor de cultuur van continu verbeteren wordt verankerd. Het volwassenheidsniveau bereiken is immers niet genoeg – het beheren en behouden van volwassenheid op het gebied van beveiliging is de échte uitdaging.

Om bovenstaande mogelijk te maken zijn jullie hard nodig. Maar dan wel met elkaar. Wij zijn een gigantische denktank voor onszelf, voor de organisaties waarvoor we werken, alsook voor de (Nederlandse) bevolking die dagelijks geconfronteerd wordt met de cybersecurity-angsten en -aanvallen. Volg de online en of fysieke sessies en voeg jouw ervaringen en meningen toe om onze gezamenlijke toegevoegde waarde nog groter te maken. Tot snel!

Henk de Ruiter
penningmeester@pvib.nl

Dimitri van Zantvliet is CISO bij de Nederlandse Spoorwegen en columnist van iB-Magazine.

COLUMN DIMITRI

De cyber poverty line, de nieuwe digitale armoedegrens

Soms kun je op de carrièreladder niet veel zichtbaarder worden dan de eindbaas zijn van iets in de VS. Ik denk dat dit ook opgaat in ons vakgebied. Een tijdje geleden mocht ik met vijf andere vakspecialisten, uitgenodigd door de NCSC directie, aanschuiven op de Amerikaanse ambassade voor een gesprek met Chris Inglis. Hij was vorig jaar door president Biden aangewezen als de eerste National Cyber Director. De kersverse USA cyber-top-dog kwam naar Nederland om zijn strategische aanpak te bespreken.

In de aanloop naar de meeting sprak men over de dresscode en zwichtte ik voor de groepsdruk om mezelf ook weer eens in een pak met das te hijsen. Ik was bang dat het op zou vallen dat mijn pak na de coronaperiode wat strakker zat dan voorheen, maar flauwe grappen werden er niet gemaakt. Het werd een interessante, uiterst serieuze en diplomatieke meeting waar o.a. een onderwerp besproken werd dat ik de laatste tijd steeds vaker hoor: de cyber poverty line.
Deze digitale armoedegrens is een denkbeeldige lijn tussen organisaties die in staat zijn om deugdelijke cyberweerbaarheid op te bouwen en te behouden en organisaties die daar niet (meer) toe in staat zijn. De term werd gemunt door analist Wendy Nather van CISCO in 2012 en een decennium later lezen we het vaker en vaker terug in de vakbladen en researchpapers.
Tijdens onze meeting werd besproken dat onderzoek in de VS heeft uitgewezen dat organisaties onder de cyber-poverty-line van 1B dollar omzet getarget wordt door ransomware. Hackerscollectieven verwachten dat alles wat erboven zit sowieso door de NSA/FBI geholpen wordt of zelf de weerbaarheid beter op orde heeft. Hyena's mikken immers ook op de zwakke dieren in de groep.

Het mkb zal de komende winter aanlopen tegen enorme energieprijsverhogingen. Mensen/werknemers komen met de piekende energieprijzen en de inflatie in de schulden, ziekteverzuim zal toenemen en we zullen sterk verlaagde verdedigingslinies zien bij bedrijven die proberen te overleven. Resources kunnen namelijk maar een keer besteed worden. Het stemt me somber dat de kloof tussen rijk en arm, groot en klein, zich nu ook meer en meer in ons vakgebied zal manifesteren. Ransomware, ook wel technical debt collection genoemd, zal verder toenemen en organisaties onder de CPL het faillissement in storten want verzekeren is al tijden niet meer rendabel. Grote organisaties zullen te maken krijgen met besmette supply chainpartijen en hele sectoren kunnen hiermee onder druk komen te staan, ook de vitale. Wraakzuchtige actoren uit het Kremlin, aangevuld met fancy-, cozy-, voodoo- of berserkberen zullen toeslaan juist tijdens zwakke momenten.

Voordat digitale veiligheid een universeel mensenrecht wordt, en dat wordt het, zullen we steviger moeten samenwerken om de organisaties die onder de CPL vallen op proactieve, collectieve, onbaatzuchtige en democratische wijze te ondersteunen. Allemaal een percentage van onze resources besteden aan het helpen van de zwakkere broeders en zusters. Organisaties dus niet enkel afwijzen als ze hun BIO, ISO27001, ISAE3402 of SOC2/2 nog niet op orde hebben, maar ze helpen deze te behalen. Elkaar proactief informeren als we verse combo's op het darkweb vinden of typo squatted domeinen aantreffen bij de buren. Cybercollectivisme is het antwoord, ondersteund door een proactieve overheid met top notch ondersteunende cyberdiensten. Sterke onderlinge samenwerkingsverbanden als fundament om onze vitale infrastructuur overeind te houden.

Een (en nul) voor allen, allen voor een (en nul). Wij kunnen dit!

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

BLOG

Luchtvaartlessen voor security officers

In een vliegtuig kunnen security officers diverse nuttige dingen leren. De informatie hieronder kreeg ik van piloten. Ze zijn nogal cynisch over risico's in hun werk en ten aanzien van de activiteiten van de andere bemanningsleden.

De demonstratie van veiligheidsattributen en nooduitgangen aan het begin van elke vliegreis lijkt op een security-awarenessactie voor al het personeel. De helft van de reizigers kan het verhaal dromen en kijkt uit het raampje of in het magazine, gevonden in de stoelzak onder het klaptafeltje. Een derde deel hoort de informatie voor het eerst en kan deze slechts moeizaam begrijpen, laat staan direct toepassen. Dit komt door het geroutineerd afraffelen, het gebruik van vreemde gebaren (met twee aaneengesloten vingers wijzen naar net gebruikte ingangen die ineens ook nooduitgang zijn) en verhullende eufemismen (‘Indien door enige reden tijdens de vlucht de luchtdruk in de cabine wegvalt’). Een zesde deel van de reizigers is uitstekend ingevoerd in de materie en luistert alleen om de uitleggende stewardess te betrappen op onlogische of onjuiste informatie of (dubbelzinnige) versprekingen.

Tot die laatste groep behoor ik. De demo begint meestal met het zwemvest. Van Schiphol naar Mallorca vlieg je ongeveer vijf minuten van de ruim anderhalf uur boven water. Het zou toch wel heel toevallig zijn als je net daar en dan neerstort? Wanneer je bij een ander vliegtraject in een ijskoude oceaan valt, raak je binnen vijf tot tien minuten onderkoeld. Het blaaspijpje, om ‘indien gewenst na verloop van tijd’ het automatisch opgeblazen zwemvest zelf bij te vullen, is dan overbodig. Of het plastic van de zwemvesten is juist, na jarenlang ongebruikt opgevouwen onder een stoel te hebben gelegen, zo poreus dat je al binnen vijf minuten bij moet blazen. De in een apart zakje (haha) op het vest verstrekte fluit (hahaha) ‘om de aandacht te trekken’ is ook zoiets. Iedereen heeft dezelfde fluit, dus in een groep van 100 tot 200 oranje dobberaars val je echt niet op. Je kunt beter een doedelzak meenemen. Als ik die tijdens het eventuele neerstorten opblaas, heb ik ook drijfvermogen en een uniek, doordringend geluid. Het zwemvest lijkt wel wat op een antivirusprogramma: helemaal zonder krijg je zeker problemen, maar het is niet zaligmakend, want het herkent alleen de al bekende virussignaturen en gedragingen.

Fasten your seatbelts

Het inchecken verbindt je naam aan een stoelnummer. Met de veiligheidsriem (eufemisme: seatbelt) verbind je jezelf aan die betreffende stoel. Zodat na een crash je lichaam zich zo dicht mogelijk bij de geregistreerde zitplaats bevindt.
Kwade tongen beweren dat stewardessen alleen aan boord zijn om het de captain op allerlei manieren naar de zin te maken. Of om eten uit te delen en lege borden op te halen. Of met name om taxfree artikelen te verkopen. De belangrijkste taak is echter om bij een crash heel hard ‘KEEP YOUR HEAD DOWN!’, te roepen tegen de passagiers. Zoals ook een security officer dat uitroept tijdens stakeholdermanagementactiviteiten. En tevens accounts en autorisaties verstrekt en deze ooit weer intrekt. Hij/zij houdt vanuit security via het aspect ‘vertrouwelijkheid’ bovendien de privacy in de gaten. Maar de belangrijkste taak is steeds de mogelijke risico’s van (voorgenomen) gebruik van IT en informatie uit te leggen aan de medewerkers en managers van de organisatie.

Het ‘KYHD’ is een aanvullende securitymaatregel voor het dragen van alleen een heupgordel. Door je hoofd tussen je knieën te houden tijdens een ‘onverwachte landing’, verklein je de kans dat je gezicht en gebit beschadigd raken door de stoel of wand voor je. Biometrische identificatie, altijd belangrijk, met paspoort en tandartsgegevens is daardoor eenvoudiger.

‘This is your captain speaking’

In de cockpit van een vliegtuig zijn twee piloten (1) aanwezig. Een van hen is de gezagvoerder (functie), die heeft altijd de rang van captain. De tweede piloot heeft tenminste de rang

Bij verleende toestemmingen geldt dat de gezagvoerder verantwoordelijk is voor het besluit om er werkelijk gebruik van te maken.

eerste luitenant, maar kan ook captain zijn. De gezagvoerder op een vlucht bepaalt wie de PF (pilot flying, dus rol) en wie de PM (pilot monitoring) is. Monitoren is inclusief bedienen van de radio, communicatie met de verkeersleiders in de toren en met ground control inclusief de pushbacktruckchauffeur, het controleren van de brandstofhoeveelheid en het bedienen van allerlei knoppen en schakelaars in opdracht van de PF. Omdat iedere piloot zijn jaarlijkse vlieguren moet halen, wordt PF vs. PM natuurlijk wel eerlijk verdeeld. Ik heen, jij terug.

Een bekende template voor het welkomstwoord is: "Goedemorgen/middag, mede namens (naam luchtvaartmaatschappij), gezagvoerder (naam gezagvoerder) en de rest van de bemanning heet ik u van harte welkom aan boord van de (individuele vliegtuignaam, bijvoorbeeld Karel Doorman). We gaan vliegen op een hoogte van 30.000 voet met een buitentemperatuur van -25 graden Celsius, naar de luchthaven (naam luchthaven). Het weer is goed, maar er kan enige turbulentie optreden. De meeste ervaren reizigers houden de hele reis hun gordel losjes om".

Een groot deel van deze informatie is niet relevant voor de reizigers of niet te controleren. De boardingpass hebben ze net ingeleverd en daarop stond alleen het vluchtnummer, niet de naam van het vliegtuig. De 30.000 voet is zeer precies, maar je hebt er weinig aan. Niemand in Nederland drukt hoogtes uit in voeten, want meters of kilometers is veel gebruikelijker. En ja, buiten is het koud, maar wie boeit dat, we gaan immers naar Spanje nota bene! En voor wie nu denkt: "Palma de Mallorca is verwarrend voor reizigers die denken naar Mallorca te gaan", op de terugweg is het nog ingewikkelder. Passagiers denken terug te keren naar Schiphol zoals bekend gelegen in de gemeente Haarlemmermeer. En dan gaan ze ineens terug naar Amsterdam Airport! Zeg dan gewoon niks, in plaats van bij iedereen verwarring te stichten. En gebruik zeker geen afkortingen, die bij de genoemde luchthavens (PMA vs. AMS) ook nog onlogisch zijn.

Ik ben, kort gezegd, ontevreden met het traditionele welkomstwoord. Maak je security-awareness teksten daarom niet obligaat en zorg voor iets nieuws, ook voor de grote massa die naar eigen inschatting eigenlijk 'alles' al weet over security. Gebruik klare taal, vermijd afkortingen en leg dingen duidelijk uit voor nieuwelingen. En zorg dat (security)medewerkers geen gaten in je verhaal kunnen schieten met gevatte opmerkingen of gelach vanuit de zaal.

Heel goed vind ik echter de afsluitende zin: 'attention cabin crew, arm slides, cross check and report please'. Deze veiligheidsmaatregel is, zoals alle niet voor passagiers bedoelde mededelingen aan boord, in het Engels en begint bovendien met de selecte groep personen voor wie hij bestemd is. Aan de buitenkant van de deuren zijn glijbanen (slides) bevestigd. Via die glijbanen kunnen passagiers bij gebrek aan een 'slurf' (Schiphol) of rijdende trap, zoals na een noodlanding op oceaan, zee, meer, rivier, kanaal of een verlaten stuk autosnelweg toch, zonder te springen, uit het metershoge vliegtuig komen. De grap is dat de slides automatisch worden opgeblazen zodra de deuren worden geopend. De luchtpompen moeten dan natuurlijk wel zijn ingeschakeld voor vertrek vanaf de gate. Een collega binnen de cabin crew dient te controleren (vierogenprincipe) dat dit inschakelen correct is gedaan en moet dit vervolgens expliciet rapporteren aan de senior cabin crew (of air purser). Dit gaat via een conference call waarbij je als cabin crew member niet je naam zegt, maar het nummer van de deur (L1, L2, R1, R2) die naar tevredenheid gecontroleerd is.
Om de teamgeest te bevorderen, zeggen ze na het driedubbele verzoek ook 'please'. Dit motiveert beter dan het in procedures meestal gebruikte 'u moet/dient'.

Ready for take off

Nadat de piloten alle verplichte checklists hebben afgewerkt, is het vliegtuig klaar om te vertrekken vanaf de gate. Een vliegtuig kan zelf niet achteruitrijden (2), daarvoor is een pushbacktruck nodig. De PM (zie hiervoor) roept: 'ground control' door zijn eigen roepnaam (het vluchtnummer, bijvoorbeeld MH-18) te noemen, gevolgd door: 'ready for startup and pushback'. De groundluchtverkeersleider geeft toestemming met: 'MH-18, cleared for pushback'. De PM herhaalt dan die tekst, dus de gegeven toestemming, zodat de verkeersleider weet dat de piloot het heeft begrepen.

De pushbacktruck rijdt voor en de piloot communiceert via een kabel met de chauffeur. Tijdens de pushback worden de motoren één voor één ingeschakeld. Aan het eind van de pushback staat het vliegtuig op de juiste plek op het platform en koppelt de chauffeur de kabel af. Dan vraagt de PM om een toestemming om te mogen taxiën naar de runway die in zijn vluchtplan is genoemd. De (ground) luchtverkeersleider geeft die toestemming en noemt de taxibanen die nodig zijn om daar te komen. Moderne vliegtuigen hebben een navigatiesysteem zodat je als piloot ook bij dichte mist (!) comfortabel bij de runway kunt komen. De PM herhaalt ook deze toestemming.

Bij de runway aangekomen, stopt de piloot voor de gele streep, haaks op de runway. Hij wisselt van radiofrequentie om nu de towerverkeersleider om een toestemming te vragen: 'MH-18, ready for departure (ook wel: take off) runway 24'. Na het herhalen van de gekregen toestemming 'MH-18, cleared for take off' gaat het pilotenteam echt aan het werk. De PF houdt het toestel in het midden van de baan en de PM houdt de instrumenten nauwlettend in de gaten en geeft de PF informatie over het take offproces. Het vliegtuig versnelt tot de rotatiesnelheid (3) is bereikt: 'V1-rotate' (of Vr). Dit is een point of no return. Totdat V1 is bereikt, kan de start nog op een veilige manier worden afgebroken, bijvoorbeeld bij een motorstoring. Nadat Velocity 1 bereikt is, moet en kan de take off worden voortgezet, ook al is één van de motoren uitgevallen. Zodra het vliegtuig de snelheid 'V1-rotate' heeft, trekt de PF de knuppel naar zich toe en de neus van het vliegtuig gaat omhoog. Daarna geldt knuppel naar je toe, huisjes worden kleiner, knuppel van je af, huisjes worden (snel) groter.

Bij alle door luchtverkeersleiders (ground en tower) verleende toestemmingen geldt dat de gezagvoerder verantwoordelijk is voor het besluit om er werkelijk gebruik van te maken. Ongeveer zoals de taakverdeling is tussen enerzijds managers die nieuwe systemen willen introduceren of in de cloud plaatsen en anderzijds hun security officers.
Ook voor het landen na de vlucht heeft de piloot toestemming nodig. Echter, die toestemming wordt niet altijd (meteen) gegeven. Piloten moeten dan weleens uren rondvliegen voordat ze kunnen landen en soms zelfs uitwijken naar een andere luchthaven. Dit lijkt op de situatie waarin een security officer wel toestemming heeft gegeven om een IT-project, ondanks door hem gesignaleerde risico's, te starten. Terwijl later dezelfde (of een andere) security officer, gezien de niet-geïmplementeerde securitymaatregelen, géén toestemming geeft om met het ontwikkelde systeem live te gaan in de productie-omgeving.
Het expliciet laten herhalen door de vragende manager van het gegeven advies (de toestemming) als teken dat hij/zij het werkelijk begrepen heeft, is een goede tip voor security officers. Ook wel bekend als: CYA.

Referenties

(1) https://scandinaviantraveler.com/en/aviation/the-sas-pilot-answers-your-questionslucht-haven
(2) https://yellowwingstrainingen.nl/alle-fasen-van-een-vlucht/
(3) https://www.luchtvaartnieuws.nl/nieuws/categorie/72/algemeen/luchtvaartvrgen-wat-betekent-v1-rotate

Achter Het Nieuws

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.


Chris de Vries


Fook Hwa Tan

Desinformatie: trial by media?

Vrijheid van meningsuiting en een vrije pers zijn belangrijke fundamenten voor een goed functionerende democratie. Onlangs kwam journalist Rudy Bouma (1) met een reconstructie van de neptransacties van Jaap van Dissel. Hij liet hierin zien hoe een feitelijk onjuist stuk 'bewijs' door social media niet alleen tot een hoop tweets leidde, maar ook tot Kamervragen. Er zijn veel meer voorbeelden. Als informatiebeveiligers proberen we de integriteit, vertrouwelijkheid en beschikbaarheid van informatie te borgen, maar in hoeverre zijn we verantwoordelijk voor de juistheid van de inhoud, context en interpretatie van de informatie? Oftewel: tot welk niveau is wie verantwoordelijk? Een reflectie van de redactie.

Iedereen is verantwoordelijk! - Fook Hwa Tan

De security professional is verantwoordelijk voor het borgen van de integriteit van data en informatie. Betekent het dat de security officer ook verantwoordelijk is voor de juistheid van de informatie over de organisatie? Of is dit bij iemand anders belegd binnen de organisatie? Sommigen zeggen dat techgiganten zoals Microsoft, Google en Facebook hiervoor verantwoordelijk zijn. Zij bieden een platform voor het verspreiden van informatie en moeten dan ook zorgdragen voor de correctheid van de informatie. Aan de andere kant voelt dit ook als censuur door grote bedrijven. Zoals gezegd, vrijheid van meningsuiting is een groot goed. Betekent dat ook, dat alles gezegd of geschreven mag worden?

Als laatste kun je het natuurlijk ook de verantwoordelijkheid van de overheid maken. Als ultieme autoriteit in een land zou de overheid, als goed huisvaderschap, dit moeten regelen. Misschien een onmogelijke taak gezien het succes van de ICT-projecten bij de overheid. Maar is het wel wenselijk?

Ik denk daarom dat eenieder voorzichtig moet zijn met oordelen en rustig de feiten tot zich moet nemen alvorens conclusies te trekken wat waar of niet waar is. Met andere woorden, eenieder moet zijn of haar eigen verantwoordelijkheid nemen.

Desinformeer jij ook? - Chris de Vries

Het is simpel: desinformatie is fout, oneerlijk en politiek. Maar wanneer is informatie 'fout'? Ook dat is simpel: Indien het niet overeenkomt met de werkelijkheid! En dan rijst de ultieme vraag: wiens werkelijkheid? Bij desinformatie moeten wij stilstaan bij de impliciete, achterliggende boodschap, in 'goed Nederlands': dog whistling. Extreme partijen zijn er goed in. Echter, ook wijzelf kunnen goed bedoeld de fout ingaan. Denk aan de ongeremdheid om meteen op elk wissewasje, snotje of wat dan ook te reageren op Twitter. Welke zichzelf respecterende politicus/politica reageert niet binnen seconden op andermans ontlading op Twitter of op LinkedIn of in een of ander praatprogramma dat vooral mikt op ruzie tussen de extreme standpunt vertegenwoordigers (zijn dat dan extremisten?) over een basaal, ongeremd en onoverdachte emotie of gevoel? Denk hierbij ook aan de niet uitgesproken, maar wel meegegeven, (met name negatieve) ladingen die in elk woord opgesloten kunnen zijn.

Hoe voorkom je desinformatie? Dat is simpel, door niet meteen te reageren. Door eerst de grijze massa in het hoofd het werk te laten doen. Je kunt zeggen: door ouderwetser te worden en terug te keren tot een brief, een praatstuk of een reflectie. Weg van slimme telefoons of tablets, weg van de Twitterapps, de televisieprogramma's en weg van elke reactie die niet een tweede of een derde of zelfs een vierde keer opnieuw doordacht, bekeken en aangepast is. Maar ook door zelfkritisch te zijn en eigen standpunten te controleren. Dus de verantwoordelijkheid ter voorkoming van desinformatie ligt bij ieder mens. Bij jou en dus ook bij mij.

(1) https://nos.nl/nieuwsuur/artikel/2447464-jaap-van-dissel-over-verdachtmakingen-het-was-een-poging-tot-karaktermoord

Jaaroverzicht

Column Martijn Hoogesteger

Artikel van het jaar

Bestuurscolumn

Artikelen

(a) artikel (i) interview (o) onderzoek

(a) artikel (i) interview (o) onderzoek

AT heet vanaf 2023 RDI

In iB-Magazine 2022 editie 5 staat een interview met de titel *Securitycertificering steeds meer een Europese aangelegenheid* met Johan van den Bosch, projectleider NCCA bij het AT. In dat interview spraken we over de nieuwe taak van Agentschap Telecom (AT) als de Nationale Cybersecuritycertificeringsautoriteit (NNCA). De in 1929 als Radiocontroledienst opgerichte overheidstoezichthouder heeft zich uiteindelijk steeds verder ontwikkelt, parallel aan de maatschappelijke en technische en digitale veranderingen in de maatschappij. Recent is bekend geworden dat het AT een nieuwe naam krijgt: de Rijksinspectie Digitale Infrastructuur (RDI). Vraagstukken over digitalisering en energie hebben steeds meer een samenhangend beleid nodig; dit gaat over alle overheidstoezichthouders die raakvlakken hebben met het werk van AT. Telecommunicatie gaat niet meer over een dun koperen draadje, maar behelst een complexe digitale infrastructuur, met ingrijpende maatschappelijke consequenties. Om die reden gaat de AT vanaf 2023 verder als Rijksinspectie Digitale Infrastructuur (RDI), een naam die de lading beter dekt.
In de kantoren van de RDI in Groningen en Amersfoort werken naast controllers, frequentieplanners en juristen ook netwerkspecialisten, cybersecurityexperts en data-architecten. Zij waken over cyberveiligheid van internetapparatuur en het Internet of Things (IoT).

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

COLUMN MARTIJN

Stel: je wordt cybercrimineel

Stel, vanaf volgende week werk je aan de andere kant van de cybersecurity, je wordt crimineel. Wat ga je doen?

Boeven en beschaving gaan hand in hand. Uit overleving, hebzucht, verveeldheid, jaloezie, de redenen zijn eindeloos. Waar er waarde wordt gecreëerd moet deze beschermd worden, want anderen zoeken misschien een korter pad naar deze waarde. Criminaliteit past zich altijd aan aan de omgeving, een ware evolutie. Zet je politie in de ene wijk neer, wordt een andere wijk geraakt. Maak jij je sloten op jouw deur beter, ben je minder interessant dan jouw buren. Zorg je dat de boef makkelijk gepakt kan worden als hij bij jou steelt, durven ze niet meer binnen te komen.

Wanneer we het hebben over waarde in de cyberwereld gaat het vaak om een ding: informatie. Ten opzichte van normale criminaliteit kan je niet echt iets stelen of iemand gijzelen. Digitale informatie kan je simpelweg kopiëren, aanpassen, of onbeschikbaar maken. De welbekende CIA-driehoek. Eerdere cybercriminaliteit ging dan ook heel direct om twee dingen: waardevolle informatie of geld.
Daar begon cybercriminaliteit, en daar kunnen we volgende week ook mee beginnen. Direct geld proberen te stelen. Vroeger hadden we nog Gozi, Zeus, Trickbot of Emotet, virussen die probeerde inloggegevens voor banken te stelen. Goede business, maar tegenwoordig niet de meest lucratieve. Nee, als we deel worden van de criminele cyberwereld zullen we snel merken dat dit niet meer is hoe onze collega's Trickbot inzetten.

Oké. En interessante informatie stelen? Dat is best een lastige, want aan wie gaan we die verkopen? Er is in ieder geval één iemand die de informatie wil, en dat is degene van wie we de informatie stelen. De waarde die we in onze digitale systemen hebben gestoken is exponentieel gegroeid het afgelopen decennium. Normale (georganiseerde) criminaliteit is bijna niet meer interessant vergeleken met de waarde die in cyber zit, vooral gecombineerd met de lage pakkans. Dit betekent een ding: criminaliteit in de cyberwereld gaat in ieder geval niet meer weg. Het verandert echter van maand tot maand, dus de race is om bij te blijven.

En bijblijven hebben onze collega's gedaan. Een banking malware wereld waarmee toegang op computers verkregen kan worden komt samen met een nieuwe techniek: we maken de informatie onbeschikbaar voor ons doelwit met versleuteling. Hier kunnen we nog smaakjes kiezen. Stelen we de informatie en dreigen we alleen daarmee? Versleutelen we de data (dan moeten we nog ransomwaresoftware inkopen)? Of vernietigen we gewoon alles? Verschillende criminele groepen hebben hier weer andere tactieken die, net als bij normale criminaliteit, evolueren op basis van wat we aan het doen zijn aan de verdedigende kant. Dat is wat we om ons heen zullen zien in de criminele wereld: iedereen heeft zijn aandacht op ransomware.

Dit is duidelijk optie één voor ons, we kunnen meedraaien met 90% van de cybercriminelen en met ransomware aan de slag. Maar wat als we wat innovatiever willen zijn? Wat komt er 'na' ransomware? Ransomware is puur de sticker die we op dit moment op een bepaalde modus operandi hebben geplakt. Criminelen hebben altijd al toegang gekregen tot systemen en data, alleen wat ze met die toegang doen evolueert.

Dus wat zou jij doen? Hoe maak je misbruik van de waarde die we in de cyberwereld hebben gestopt? Val je terug in oudere vormen van criminaliteit en ga je voor de financiële informatie maar op een nieuwe manier? Specialiseer je je in het doorverkopen van informatie en blijf je onder de radar? Ik wil het graag weten! Voor je het weet zitten we met zijn allen in de ransomwaretunnel en zitten de criminelen op een boot.

15 PvIB reconnect in cyber security

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
Tom Bakker

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

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

ADVERTENTIE-ACQUISITIE
MOS bv
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 2022 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

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