PvIB 15 reconnect in cyber security

INFORMATIEBEVEILIGING MAGAZINE

- Ongestructureerde data beveiligen: onderzoek naar dit hoofdpijndossier
- Laatste deel drieluik: veilig gedrag in informatiebeveiliging
- Het Artikel van het Jaar 2021

JAARGANG 22 - 2022 - EDITIE 3

WAT IS ISO 27701?

De 15 meest gestelde vragen over de privacy management norm ISO 27701.

De garantie dat persoonlijke informatie door organisaties op de juiste manier beschermd wordt, groeit. Privacyrichtlijnen zoals de AVG verplichten organisaties om de bescherming van persoonsgegevens te garanderen. De internationale ISO 27701 standaard is een uitbreiding op de bestaande informatiebeveiligingsnorm ISO 27001 en biedt richtlijnen voor de bescherming van privacy. De norm helpt organisaties om informatie op een correcte manier te beheren en privacywetgevingen na te leven.

Vraagt u zich af wat de meerwaarde van ISO 27701 certificering is of wilt u weten of ISO 27701 certificering voor uw organisatie verplicht is? Rob Jansen, IT-security auditor en trainer, geeft u antwoord op de meest gestelde vragen als het gaat om privacy management en de ISO 27701 norm.

Lees de antwoorden op de vragen op www.dnv.nl/watisISO27701 of scan de QR-code.

DNV

Op weg

Nicole van Deursen

Deze derde uitgave van dit jaar biedt weer veel uiteenlopende artikelen. Een goed begin is het halve werk en informatiebeveiliging begint bij het inkopen en aanbesteden van IT-oplossingen. Is de oplossing eenmaal operationeel, dan moet het wel worden onderhouden. Patchen dus, wie kent het niet. Maar hoe werkt dat bij OT-systemen in de watersector? En als er dan toch zwakke plekken in je systemen zitten en door buitenstaanders worden ontdekt, dan wil je dat als organisatie graag horen. Dus zorg je dat je op je website informatie geeft hoe je die informatie wilt ontvangen.

De collega's die de IT-oplossingen gebruiken moet je ook op weg helpen. Je moet ze daarbij de juiste omgeving bieden en je kunt meten of verschillende interventies het gewenste effect hebben. Tijdens het werken produceren die collega's allemaal veel ongestructureerde data. Denk aan e-mails, audio- en videobestanden, maar ook allerhande tekstdocumenten met persoonsgegevens. In de financiële sector onderzoekt TNO of die data met machine learning kan worden gevonden en gelabeld (en beveiligd).

Wist je trouwens dat je prijzen kunt winnen als je een artikel voor iB-Magazine schrijft? Ieder jaar kiest een onafhankelijke jury drie prijswinnaars uit en die worden goed beloond! Als je ook een idee hebt voor een artikel, maar niet zo goed weet hoe je moet beginnen met schrijven, neem dan contact met ons op. We helpen je graag op weg.

Nicole

IN DIT NUMMER

Auteurs: Sandra Kagie is freelance tekstschrijver (Sanscript Tekstproducties). Sandra is bereikbaar via info@sanscriptproducties.nl. Chris de Vries is redactielid van iB-Magazine. Hij werkt als zelfstandig professional onder de naam: De Vries Impuls Management. Chris is bereikbaar via impuls@euronet.nl.

INTERVIEW

Ongestructureerde data beveiligen: onderzoek naar dit hoofdpijndossier voor menig CISO

Maaike de Boer

Rick van der Kleij

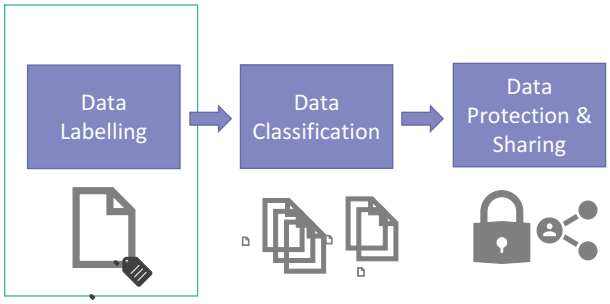
Binnen grote (financiële) organisaties circuleert een enorme hoeveelheid data, waarvan een groot deel ongestructureerd. Denk aan e-mails, audio- en videobestanden, maar ook allerhande tekstdocumenten. Deze bestanden en documenten zijn vaak niet geclassificeerd, maar kunnen vertrouwelijke informatie bevatten. Medische gegevens, fraude gerelateerde data of personal identifiable information (PII) bijvoorbeeld. Een hoofdpijndossier voor menig CISO. "Hier ligt een CISO wakker van", concludeerde het Partnership for Cyber Security Innovation (PCSI) (1) waarbinnen TNO en een aantal grote financiële instellingen als Achmea, ABN AMRO, ING en de Volksbank samenwerken om cybersecurity op een hoger plan te brengen.

Uit een ideation-sessie kwam het idee naar voren om machine learning (ML) toe te passen met betrekking tot de dreigingen van ongestructureerde data. De uitkomsten waren voor PCSI reden om eind 2020 een project te starten met als doel het zoeken naar de mogelijkheid om middels geautomatiseerde labelling als organisatie grip te krijgen op ongestructureerde data. Daarbij kwamen PII-, medische- en fraude gerelateerde data als eerste in beeld.

Waarom geautomatiseerde labelling?

Geautomatiseerde labelling omdat het handmatig etiketteren van ongestructureerde data zeer complex en tijdrovend is, waardoor het bijna onmogelijk is om de grote hoeveelheden ongestructureerde gegevens goed te labelen, vervolgens te classificeren en uiteindelijk te beschermen. Het proces dat binnen het project doorlopen wordt, kent vier stadia. Allereerst de explore-fase waarin geconstateerd werd dat de berg aan ongestructureerde data veelal niet op het gewenste niveau beveiligd was. Vervolgens de Proof of Concept-fase, gerelateerd aan Open Source data. Als derde de pilot-fase die al een werkend prototype

opleverde, kort cyclisch qua opzet en gebaseerd op een agile werkwijze. En tot slot de exploit-fase waarin het project zich nu bevindt.
De volgende afbeelding geeft een impressie van de gewenste werking van het prototype.



Figuur 1 - Van data-etikettering tot databescherming en -deling (2).

Begin dit jaar presenteerde PCSI zijn eerste conclusies in een whitepaper. Reden voor een gesprek met dr. Rick van der Kleij, senior research psychologist cybersecurity en projectleider namens TNO, en dr. Maaike de Boer, data-scientist bij TNO.

De centrale vraag

In het nog lopende project staat volgens Rick van der Kleij de vraag centraal of met kunstmatige intelligentie (KI/AI) op basis van machine learning er een hoge mate van betrouwbaarheid kan worden gerealiseerd als het gaat om het labelen van ongestructureerde data. "Komen er op deze manier betrouwbare labels tot stand op basis waarvan data geclassificeerd en uiteindelijk ook beter beschermd kunnen worden, zodat we uiteindelijk met z'n allen beter zicht kunnen houden op deze data?", specificeert Van der Kleij de onderzoeksvraag. Hij noemt de resultaten tot nu toe 'veelbelovend' met een 'nauwkeurigheid van meer dan 80%' ook als het gaat om meer complexe of gedetailleerde labels. Labels dus die verder gaan dan het etiket 'CV' of 'contract'. "Basis van het project zijn nu vooral tekst(document)en", legt Maaike de Boer uit. In dit soort documenten is de woordvolgorde belangrijk om tot een juiste herkenning en daarmee classificatie te komen."
Ze benadrukt verder dat er binnen het project gebruik wordt gemaakt van de bredere definitie van Artificial Intelligence. "In de nauwe definitie (strong AI) leert de 'robot' zoals de mens en neemt deze het proces geheel over. Terwijl de bredere definitie (weak AI) uitgaat van bijvoorbeeld het goed uitvoeren van één taak, waarbij in dit geval een systeem wordt gevoed met documenten op basis waarvan een kansberekening, geavanceerder dan statistiek, plaatsvindt om vast te stellen of een document bijvoorbeeld PII-gegevens bevat, een CV of een medisch document is. Om hier vervolgens een bijbehorende classificatie en beveiliging aan te koppelen."

Kansen nieuwe methodiek

Het doel van het project is volgens Van der Kleij ook om met een flexibele en schaalbare aanpak te komen, zodat er in de loop der tijd labels kunnen worden toegevoegd. Daarnaast biedt de nieuwe methodiek organisaties volgens hem betere mogelijkheden om transparanter te kunnen communiceren en (vertrouwelijke) informatie te delen.
De onderzoekers stellen in hun whitepaper dat er met dit doel weliswaar diverse tools en pakketten op de markt zijn, maar dat er nog vele (ontwikkel)uitdagingen bestaan die grootschalige toepassing van geautomatiseerde data labelling binnen (financiële) organisaties in de weg staan. Er zijn ten aanzien van het PCSI-prototype vijf waardeproposities te onderscheiden, te weten:

- Nauwkeurigheid
- Flexibiliteit
- Complexiteit
- Granulariteit
- Uitlegbaarheid

Voor een uitgebreide toelichting op de vijf punten zie de whitepaper (3).
Juist financials hebben in de woorden van de TNO-onderzoekers vaak 'net wat meer nodig' op de genoemde vijf waarden. Dit omdat de financiële sector rekening heeft te houden met de eisen van toezichthouders zoals De Nederlandsche Bank en de Autoriteit Financiële Markten. "We vertrouwen erop met ons onderzoek marktpartijen te stimuleren dat stapje extra te zetten", stelt Van der Kleij. Organisaties zitten vaak niet te wachten op nóg een tool zo blijkt volgens hem uit diverse gesprekken met zowel organisaties binnen PCSI als daarbuiten. "Ze zijn veel meer geïnteresseerd in een verbetering op de voor hen cruciale punten van de tools van bijvoorbeeld Microsoft en Proofpoint die ze nu gebruiken."

De Boer geeft aan dat het probleem dat automatische labelling oplost, ook nadrukkelijk een menselijk aspect omvat. Namelijk de belasting van de mens. Handmatig labelen is namelijk een tijdrovende en intensieve taak. De Boer: "Geautomatiseerde labelling voorkomt fouten die ondanks goede bedoelingen van medewerkers ontstaan.

Het ontlast medewerkers en het voorkomt de inwerkingtreding van het bekende adagium: 'Garbage in, garbage out!'"

"Onze methodiek van geautomatiseerde labelling is een semi-supervised methode", gaat ze verder. "Door menselijke terugkoppeling leert het systeem en zorgt het voor vastlegging en vorming van noodzakelijke trainingen binnen een organisatie. Aan de werking hiervan gaat een discussie met materiedeskundigen vooraf. Waarin ze kunnen aangeven wat voor hen belangrijk is en wat zij als essentiële definities zien. Dat betekent dat per sector verschillen kunnen en mogen bestaan, ook in geval van gelijknamige begrippen."

Uitnodiging aan marktpartijen

De TNO-onderzoekers zien hun eerste conclusies nadrukkelijk als een uitnodiging naar marktpartijen, sectorpartijen en vendors, om met elkaar in gesprek te gaan. "We nodigen leveranciers en andere geïnteresseerden uit om samen te bekijken hoe we onze bevindingen in de (inter)nationale praktijk kunnen brengen. Dit niet alleen binnen de financiële sector, maar juist ook in de bredere security community. Zodat we samen antwoorden kunnen vinden op dit vraagstuk waarvan een CISO wakker ligt", besluit Van der Kleij.

Referenties

(1) https://pcsi.nl/

(2) Whitepaper PCSI, 'Protecting unstructured data – challenges and opportunities of automated labelling

(3) https://pcsi.nl/news/protecting-unstructured-data-challenges-and-opportunities-of-automated-labelling/

In onderstaande interviews geven ABN AMRO en Achmea weer hoe zij omgaan met de classificering van ongestructureerde data binnen hun organisaties.

ABN AMRO verwacht PCSI-model binnen een jaar toe te passen

"Het probleem van het classificeren van grote hoeveelheden ongestructureerde data binnen organisaties bestaat al heel lang. Er zijn een aantal commerciële oplossingen op de markt, maar deze lossen het probleem niet écht op. We hebben gegevens waarvan we geacht worden dat we er zorgvuldig mee omgaan of waarvan we zelf willen weten waar ze blijven, maar in het geval van ongestructureerde data is er geen gemakkelijke manier voor ons om die gegevens op te sporen. We zoeken een oplossing aan de voorkant om de data te kunnen vinden om deze aan de achterkant te kunnen beveiligen."

Noor Spanjaard

Olaf Streutker

Deze aftrap doet Olaf Streutker, Strategisch Adviseur bij het Corporate Information Security Office van ABN AMRO Bank. We spreken hem en zijn collega Noor Spanjaard, Enterprise Data Governance Adviseur bij ABN AMRO Bank, over het Automated Data Labelling project. De bank is als partner binnen PCSI een van de deelnemers aan het project.

"De documenten zoals word-bestanden, excel-sheets en pdf's, waar het om gaat, kunnen echt door iedereen binnen de organisatie worden gemaakt met allerlei verschillende doeleinden", verduidelijkt Spanjaard. "Terwijl gestructureerde informatie vaak via een applicatie, via een front-end, op een bepaalde manier en met een bepaald doel wordt ingevuld. Veel makkelijker van tevoren te classificeren dus, omdat er sprake is van een duidelijke doelkoppeling. Een koppeling die in het geval van ongestructureerde data ontbreekt."

Onderscheid labelen en classificeren

Heel veel oplossingen die nu op de markt zijn, richten zich volgens Spanjaard op het classificatieprobleem, maar dan mis je in haar woorden 'de granulariteit van het labelen'. Precies de reden waarom in het PCSI-onderzoek volgens Streutker zo nadrukkelijk het onderscheid wordt gemaakt tussen labelen, 'het objectief vaststellen of een document bijvoorbeeld persoonsgegevens bevat', en classificeren, 'in welk bakje stop ik het en hoe moet ik het beschermen, een subjectieve beoordeling'.

"Voor bedrijven die niet zo streng gereguleerd zijn als een financiële instelling kan zo'n classificatieoplossing prima werken", vervolgt zijn collega. "Maar juist wanneer je heel specifieke regelgeving hebt waaraan je moet voldoen dan blijkt het in de praktijk onvoldoende te werken." Een generiek probleem, zo heeft de bank in zijn zoektocht naar de oplossing geconstateerd.

Lesson learned

Het meest in het oog springende dat ABN AMRO tot nu toe heeft geleerd van dit PCSI-project is volgens Spanjaard dat het begrip van de voorwaarden waaronder Machine Learning (ML-)technieken goed kunnen werken, binnen de organisatie niet wijd verspreid is. "Dit maakt het lastig omdat je voor een succesvolle toepassing van deze techniek vooraf een klein beetje moet investeren voordat je de vruchten kunt plukken", legt ze uit. De investering behelst het annoteren van gegevens in de systeemdataset. Je moet een aantal voorbeelden geven van hoe jij informatie wilt labelen en vervolgens kan het systeem die labelling veel breder gaan toepassen op alle documenten. Je moet dus een klein voorzetje geven, voordat het algoritme zelf verder kan leren."

"Probleem is nu dat mensen binnen de organisatie de urgentie van het probleem weliswaar zien, maar dat ze door een gebrek aan begrip van de techniek geen of te weinig tijd vrij maken voor die kleine investering wat betreft het annoteren van data."

Het grote voordeel van het PCSI-model is volgens beiden juist dat je niet langer afhankelijk bent van de individuele inschatting van medewerkers die hun documenten moeten classificeren, maar dat het model zelf steeds beter wordt in het betrouwbaar labelen van documenten. Het aantal labels dat je potentieel kunt toekennen aan documenten is onbegrensd."

Potentie PCSI-model

Wanneer je de basis van labelling goed op orde hebt, kan het PCSI-model volgens Streutker veel breder worden ingezet dan voor security-doeleinden alleen. Een goed gelabeld document maakt volgens hem namelijk meerdere classificaties naast elkaar mogelijk. "Een security classificatie is wat anders dan een business classificatie of een krediet classificatie."

Voor een concrete implementatie binnen de bank van het PCSI-model is het volgens Streutker nog net wat te vroeg. Die opschaling moet volgens hem nog komen. "We zitten nog in de fase waarin we aantonen dat het werkt om het probleem van ongestructureerde data op te lossen met behulp van dit model", geeft hij aan. "Gelukkig zijn we een stuk verder dan in 2013, toen het alleen nog maar in een research omgeving mogelijk was om experimenten uit te voeren", vult Spanjaard aan. Toen bleek de implementatie in de organisatie van zo'n ML-oplossing volgens haar te moeilijk.

"Daar waren destijds te veel expertise en te grote investe-

ringen voor nodig. Wat we nu samen met TNO hebben ontdekt is dat met een kleine effort dit model al getraind kan worden. Het loopt nu alleen nog vast op het op weg helpen van het model met de juiste trainingsdata. Wat we wel hebben gecheckt is dat onze IT-organisatie dit model lokaal kan draaien. Qua volwassenheid van de techniek binnen onze financiële organisatie zijn we de afgelopen jaren enorm gegroeid."

Toepassing binnen een jaar

Streutker verwacht dan ook dat het model binnen ABN AMRO binnen een jaar daadwerkelijk gebruikt gaat worden. "De voorwaarden daarvoor zijn aanwezig", weet hij. Voor organisaties met een vergelijkbaar volwassenheidsniveau zien hij en Spanjaard zeker ook mogelijkheden om concrete data beveiligingsproblemen aan te pakken. Waarbij ze nadrukkelijk wijzen op overheidsorganisaties en andere financiële instellingen.

Omdat zij net als ABN AMRO beschikken over een goed toegerust data science team. "Een voorwaarde omdat het toepassen van kunstmatige intelligentie (KI) in informatiebeveiliging kansen biedt, maar ook risico's met zich meebrengt", waarschuwt Spanjaard. "Risico's van misbruik. Om dat te voorkomen heb je wel een bepaald volwassenheidsniveau op het gebied van KI binnen je organisatie nodig." Organisaties die hierover niet beschikken adviseert ze daarom te kiezen voor een oplossing van een van de partijen die al beschikbaar is, 'off the shelf' dus.
"Dit model maakt het mogelijk dingen die je kwijt bent te vinden én te beveiligen", concludeert Streutker. Daar moet iedere informatiebeveiliger volgens hem warm van worden. "Zeker als je kijkt dat de labels uit ons model ook uitleesbaar moeten zijn voor andere security protection tooling", haakt Spanjaard in. Om zo een vendor lock-in te voorkomen. De twee benadrukken dat ze hopen dat de bevindingen uit het huidige PCSI-onderzoek ontwikkelaars van off the shelf-oplossingen inspireren hun pakketten te verbeteren. Vooral op het vlak van flexibiliteit en granulariteit. "Ze beloven de oplossing voor alle problemen te zijn als het gaat om ongestructureerde data. Maar wanneer je doorvraagt en verder kijkt, zijn ze dat voor een organisatie als de onze nét niet helemaal."

Verdere toekomst

In een utopische wereld tot slot ziet Streutker ook kansen voor het PCSI-model als het gaat om het attribute based access control waarin je op basis van attributen toegang verleent. "Labels zijn attributen. Je zou dus kunnen zeggen wanneer ik meer gegranuleerde labels kan toekennen, kan ik ook betere beslissingen nemen over wie er wel of niet bij bepaalde informatie mag."

'We hebben als Achmea al gigantische vooruitgang geboekt'

Michaël Stekkinger

Achmea is als partner binnen PCSI een van de deelnemers aan het project Automated Data Labelling. "We beschikken bij Achmea, zoals vrijwel alle moderne organisaties, over een enorme hoeveelheid data. Lang niet allemaal geordend of gestructureerd binnen een bepaalde applicatie of rond een naam of andere persoonsgegevens die nodig zijn voor het afsluiten van een verzekering of het organiseren van een afhandeling bij schade. Het is nogal een taak om die stroom aan data goed en veilig te organiseren", legt Michaël Stekkinger, Information Security en Compliance Officer bij Achmea, de urgentie van het project uit.

"Bij Achmea staan we voor duurzaam samen leven."

Waarbij het volgens hem een belangrijk punt is dat je als organisatie wilt weten welke gevoeligheid een bepaald document heeft binnen je organisatie. Zodat je zaken die extra gevoelig liggen, ook extra kunt beveiligen. Dit in samenhang met eisen van het Information Rights- en Data Loss Management. Zodat je in zijn woorden 'tegenstanders het voortouw kunt ontnemen'. Juist dit inzicht verkrijgen in die enorme hoeveelheid aan ongestructureerde data noemt Stekkinger 'een noodzakelijk kwaad en niet zo gemakkelijk'.

"Niet zo gemakkelijk omdat we hierin, tot op heden, grotendeels afhankelijk zijn van medewerkers", gaat hij verder. "Zij moeten documenten classificeren en op de juiste plek opslaan: stelselmatig en met het juiste label", legt hij uit. "Een kennisintensief proces dat ook tijd en aandacht vergt. En hoe welwillend en getraind medewerkers ook zijn. Het gaat wel eens mis."

Behoefte aan een zelflerend algoritme

Als problemen waar je tegen aanloopt, noemt hij bijvoorbeeld data die in het verleden al opgeslagen zijn en zelden tot nooit geraadpleegd worden, data die niet gelabeld zijn en data met vergelijkbare labels, maar in verschillende talen. Dit alles vereist volgens Stekkinger een algoritme dat multi-lingual is, dat de mogelijkheid biedt eigen labels toe te voegen en dat het toestaat dat een label binnen de ene organisatie een andere betekenis heeft dan binnen een andere organisatie. "Dit zijn gezamenlijke eisen vanuit de deelnemende financiële dienstverleners. Complexe materie die vraagt om de inzetbaarheid van een zelflerend algoritme", concludeert hij.

Randvoorwaarden die hierbij voor Achmea een belangrijke rol spelen zijn onder meer:

- compliance vereisten (waaronder uitlegbaarheid van de gekozen labels door een algoritme)
- bruikbaarheid in een complexe IT-omgeving en niet gelimiteerd aan één vendor/product.

Kan het niet efficiënter?

Kernvraag voor Achmea binnen het project is nu uit te zoeken of het labelen van ongestructureerde data efficiënter en georganiseerder kan door de inzet van een zelflerend algoritme. "Wetende dat dit een complexe zaak is, dat het accuraat moet gebeuren en dat resultaten ook uitlegbaar moeten zijn", benadrukt Stekkinger.

Hij ziet voor Achmea nu al, terwijl het project nog loopt, een 'gigantische vooruitgang'. "We weten meer en we kunnen meer", geeft hij aan. Zo kunnen we in de toekomst dankzij automatische labelling middels een zelflerend algoritme meer duidelijkheid creëren in ongestructureerde data. Daarbij kunnen we medewerkers ontlasten in het complexe proces zodat ze meer tijd beschikbaar hebben voor andere taken. En we zien ook nog eens mogelijkheden om eenzelfde soort algoritme te gebruiken om andere uitdagingen te tackelen, zoals data retentie."

Wat hij ook vooral waardeert, is het innovatieve aspect van het onderzoek binnen PCSI met als facilitator TNO. "Je ziet hierdoor dat bijvoorbeeld ook bepaalde vendors interesse hebben in onze onderzoeksresultaten. Waardoor je beweging ziet in het hele veld. Een ontwikkeling waar uiteindelijk niet alleen wij en andere financials binnen PCSI profijt van hebben, maar iedereen."

Hoog op agenda

"Bij Achmea staan we voor duurzaam samen leven", stelt hij tot slot. Hierbinnen lossen we samen met onze klanten, strategische partners en relaties grote maatschappelijke vraagstukken op rond gezondheid, wonen & werken, mobiliteit en inkomen. Dan moet je zorgen dat je meegaat in digitale ontwikkelingen en dat je datahuishouding op orde is. Je wordt geen digitale verzekeraar zónder dat dit hoog op de agenda staat. En dan doel ik op het allerhoogste niveau: bij de Raad van Bestuur. Een probleem als ongestructureerde data tackelen, staat daarom als vanzelfsprekend hoog op onze IT-agenda. Heel mooi dus dat we deze uitdaging binnen PCSI samen met partners/peers met een gelijke focus kunnen oppakken."

Het Artikel van het Jaar 2021

Op 12 april 2022 was weer de uitreiking van Het Artikel van het Jaar 2021 door de juryvoorzitter Ellen Wesselingh en Tom Bakker, voorzitter van de redactiecommissie. Na twee jaar 'virtuele' uitreikingen, via de post, eindelijk weer een fysieke uitreiking met publiek. De afgelopen twee keer werden de prijswinnaars verzocht een selfie met hun prijs op te sturen voor publicatie in het magazine. Nu hebben we weer echte foto's. Graag willen we juryleden Ellen Wesselingh, Jurgen van de Vlugt en Aart Jochem weer bedanken voor hun inspanningen.

Sprintjes

Niets is wat het lijkt. Nou ja, afgezien van iB-Magazine artikel-prijsjuryberaadslagingen misschien. Die ook dit jaar nog even op fysieke afstand waren. Dat was geen enkel beletsel voor creatief overleg; de afgelopen jaren hebben veel geleerd over het opvoeren van productiviteit – buiten kantoor.

Of we ook in de Great Resignation zitten – of nog gaan komen –, die elders aan de gang lijkt te zijn, is nog niet te zeggen. Wel dat we nu al een groot tekort hebben aan essentiële krachten in essentiële sectoren. In de zorg, in de horeca, in de bouw en in de scooterbezorgsector.

De 'iets op kantoor'-sector is er niet bepaald een waar nou zulke enorme gaten zichtbaar zijn geworden; kennelijk niet essentieel genoeg…. Maar desondanks, de vraag, nee de schreeuw om vooral veel méér CISO's en scriptkiddies lijkt onstilbaar. Nu nog ontdekken of we ons daarmee eindelijk, na decennia roepen, kunnen losmaken uit 'iets op kantoor' en ook bij het Essentieel-clubje mogen aanschuiven.

Daarom moesten ook wij maar eens omzien naar slimmere manieren van werken. Als vanouds weten we: dat betekent Automatiseren! Gelukkig was dat terug te zien in de artikelen die de jury ter beoordeling kreeg. Aandacht voor de menselijke factor, de menselijke tekorten, én voor IT zowat als compensatie.

Veel korte artikelen

Opvallend was wel dat er zoveel wat kortere artikelen waren, deze keer. One-pagers, naar letter of geest. Enkele hersenkraak-soundbites. Met als gevolg dat er niet altijd ruimte was voor, wat de jury zo graag ziet, het ontwikkelen van een coherente gedachte vanuit een aantal invals-

hoeken. Meer weging van argumenten, combineren van alternatieven tot een nieuwe synthese, genereren van direct toepasbare handvatten willen we zien! We blijven het toch zeggen, hoor. En met als gevolg dat auteurs nog wel eens op het randje van juistheid schrijven, qua gebruik van vaktermen. Volledigheid, ach. Een duidelijke boodschap: die zien we graag. Maar de jury kwam wel vrij snel tot enige unanimiteit over de kopgroep die van het peloton wegsprintte voor de podiumplaatsen.

Derde plaats: Rémon Verkerk en Ard Ruiter

Thuiswerken en hybride werken zijn een belangrijk en blijvend thema. Lessons learned zijn zeer te verwelkomen, daar zou een PvIB-werkgroep zich op moeten werpen. Na een goed gesprek en het wegen van de relatieve scores kwamen hier ex aequo als derde, twee artikelen schouderduwend over de finish die minder dan een ventieldikte scheelden. *Menselijk schild: gebruikers als frontlinie in de organisatie* van Rémon Verkerk en *Security overwegingen bij hybride werken* van Ard Ruiter geven beide heel veel informatie in beperkte ruimte. Daardoor was net wat te onduidelijk welke fans werden aangesproken.

Tweede plaats: Rik van Dijk

Dat smijten met krachten leidde ertoe dat er nog een artikel langs kon schieten vlak voor de finish. *Wat te doen aan kwetsbaarheden in TCP/IP-Stacks?* van Rik van Dijk werd zonder heel veel jurydiscussie tweede. Helder: een duidelijk geschreven stuk, met leads voor verdere verdieping. Het onderwerp is relevant, de inhoud is vooral gericht op professionals die zich oriënteren op het onderwerp. Maar het blijft desondanks wel boeiend voor andere lezers om te zien dat ook op het gebied van, zo zou het kunnen lijken, volwassen technologie nog het nodige aan verbetering te bereiken is – buiten de techniek, maar wel in de inrichting van de informatiemaatschappij. Relevant voor de toekomst waar nog veel nieuwe technologie op maatschappelijk inbedding wacht. Wie is waarvoor verantwoordelijk?

Eerste plaats: Reinder Wolthuis en Frank Fransen

De jury was dit jaar unaniem over de eerste plaats. 'Leesbaar', 'diepgaand, vooruitstrevend artikel', 'goed onderbouwd', 'een plezier om te lezen'. Nog afgezien van goede en hoge scores op de formele criteria zijn dat toch indrukwekkende kwalificaties van een jury die met plezier kritisch is. Met een pluk van dat Automation wat we zo nodig hebben. Met een flink uitgebreide, niet onzelfkritische beschrijving van onderzoekswerk.
Misschien dat er nog wel dat zeurende jurysplintertje is van Concrete Handvatten, maar ja, het gaat over een project dat nog doorloopt. Desalniettemin zou de jury graag zien dat er meer wordt geschreven over zulke ontwikkelprojecten in ons vak. Omdat we zo graag zulke echte ontwikkelprojecten zien. Groot of klein – er is nog veel te doen. Afstudeerders komen met ontdekkingen (zie vorig jaar), professionals komen met het werk – zie dit jaar. U allen op naar de volgende etappe!

Met voorsprong bij de rest weggesprint was het (grote) team van *Soccrates - security automatation in SOC & CSIRT environments* met Reinder Wolthuis en Frank Fransen als kopmannen, de winnaars. **Gefeliciteerd!**

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

Veilig gedrag in informatiebeveiliging: leren, motiveren, faciliteren

Deel 3 van drieluik 'Onderzoek naar de human factor in informatiebeveiliging'

Dit drieluik beschrijft onderzoek naar de menselijke factor in informatiebeveiliging. De eerste twee artikelen uit deze reeks lieten zien hoe het gesteld is met het huidige kennisniveau en gedrag ten aanzien van 15 verschillende onderwerpen in informatiebeveiliging. Deze data toonden aan dat voor een aanzienlijk deel van onveilig gedrag in informatiebeveiliging, kennis wel aanwezig is. Het laatste artikel in deze reeks gaat in op handvatten om juist die gedragingen te veranderen; waar mensen al wel weten wat ze zouden moeten doen, maar nog niet doen.

Cyberdreigingen zijn actueler dan ooit. Dat de menselijke factor een wezenlijk onderdeel van de weerbaarheid uitmaakt, is inmiddels ook bekend. Organisaties zien ook steeds meer het belang in van daadwerkelijke gedragsverandering, dus niet stoppen bij het zenden van kennis maar kijken naar alle factoren die gedrag beïnvloeden. Wat nog lastig blijft is, hoe te komen tot die daadwerkelijke gedragsverandering.

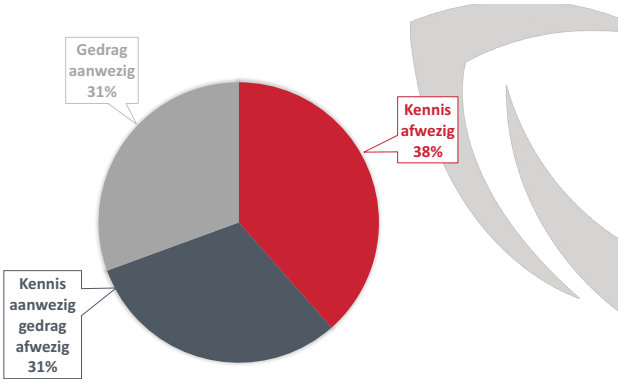
De menselijke factor in informatiebeveiliging

Gedrag in informatiebeveiliging. Een uitdaging voor iedere (C)ISO. Want opstellen van een passend beleid is één ding, maar zorgen dat iedereen zich daar ook aan houdt, een tweede. In het dagelijks leven zien we voortdurend situaties waarin mensen wel wéten wat ze eigenlijk zouden moeten doen, maar zich er toch niet aan houden. Denk aan het niet insmeren om wat sneller bruin te worden, het negeren van het thuiswerkadvies of het appen op de fiets. Deze kloof tussen kennis en gedrag kan worden verklaard door het feit dat gedrag het resultaat is van meerdere factoren, niet alleen kennis. In dit artikel wordt beschreven welke factoren dat zijn en hoe dit kan helpen bij het bereiken van gewenste gedragsverandering.

Het onderzoek tot nu toe

In de eerste twee artikelen van dit drieluik werd onderzoek beschreven naar het huidige kennisniveau, onder 1155 respondenten van 20 organisaties (1), (2). Het onderzoek betrof 15 onderwerpen met betrekking tot informatieveiligheid, waarvoor zowel kennis als gedrag werd gemeten. De resultaten lieten zien dat gemiddeld genomen over 15 onderwerpen, in 38% van de gevallen kennis de ontbrekende factor is. Met andere woorden: voor iets meer dan een derde van de gevallen heeft het wel degelijk zin om mensen kennis aan te bieden! Het is alleen wel zaak te weten voor wélke onderwerpen dat is, zodat deze kennis gericht kan worden aangeboden. Dit werd uitgebreid beschreven in het eerste artikel van dit drieluik (1).

Daarnaast lieten de resulaten zien dat in 31% van de gevallen, het juiste gedrag al wordt vertoond (2). Deze onderwerpen behoeven dus de minste aandacht, want hier gaat het immers al goed. Maar dan blijft er nog 31% van de gevallen over, waarbij de kennis wel aanwezig is, maar het gedrag niet. Voor deze gevallen heeft het uiteraard geen zin om verder in te zetten op kennisverhogende activiteiten, omdat men voor deze onderwerpen wel hoog scoorde op kennis. Voor deze onderwerpen is dus sprake van de kennis-gedragskloof. Kennis zenden kan in deze gevallen zelfs weerstand oproepen, omdat mensen hier niets meer van leren en juist andere redenen hebben om zich toch anders te gedragen. Om deze kloof te overbruggen, zal dus verder gekeken moeten worden; welke andere aspecten beïnvloeden het menselijk gedrag nog meer? En hoe kunnen we daarop ingrijpen als we gedrag willen veranderen?



Figuur 1 - Kennis en gedrag in cybersecurity gemiddeld over 15 onderwerpen.

De psychologie over gedrag

Als we kijken naar een basale theorie van gedrag uit de psychologie, zien we dat gedrag wordt bepaald door drie factoren (3). Allereerst is gedrag afhankelijk van iemands capaciteit: is iemand wel in staat om het te doen, weet iemand wat er verwacht wordt en beschikt hij/zij over de vaardigheden? Hieronder valt dus het stukje bewustwording waar de meeste campagnes in het verleden op gebaseerd waren. Naast kennis wordt gedrag echter ook bepaald door iemands motivatie: Wil iemand het wel doen, vindt deze persoon het wel belangrijk genoeg? De derde factor die gedrag bepaalt is gelegenheid: Wordt iemand wel in staat gesteld om het te doen en krijgt deze persoon wel de kans om het te doen? Voor de onderwerpen waarbij kennis wel aanwezig is maar gedrag niet, zal voor gedragsverandering dus ingezet moeten worden op deze twee factoren: motivatie en gelegenheid.

Motivatie

Zoals hierboven beschreven, is het niet alleen belangrijk of iemand een regel kent en weet wat er verwacht wordt. Minstens zo belangrijk is het willen! Deze motivatie voor bepaald gedrag kan volgens de psychologie in verschillende typen worden onderverdeeld:

Intrinsieke motivatie

Intrinsiek gemotiveerd zijn betekent dat je als individu handelt vanuit je eigen wil/verlangen. De motivatie komt vanuit iemand zelf. Met andere woorden: je doet iets omdat je het zelf graag wil.

Extrinsieke motivatie

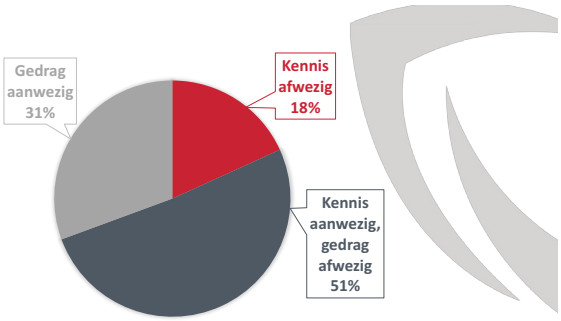
De motivatie die wordt ingegeven door een extern doel dat iemand kan bereiken met informatieveiligheid. Bijvoorbeeld: het ontvangen van een 'beloning' (bv. waardering) of het vermijden van straf.

Zelfeffectiviteit (Self-efficacy)

Het vertrouwen in je eigen bekwaamheid om met succes een bepaalde taak te volbrengen. Met andere woorden; het vertrouwen dat je kunt wat er van je gevraagd wordt. Dit is dus het geloof in eigen kunnen (4).

Motivatie het probleem? Motiveren de oplossing!

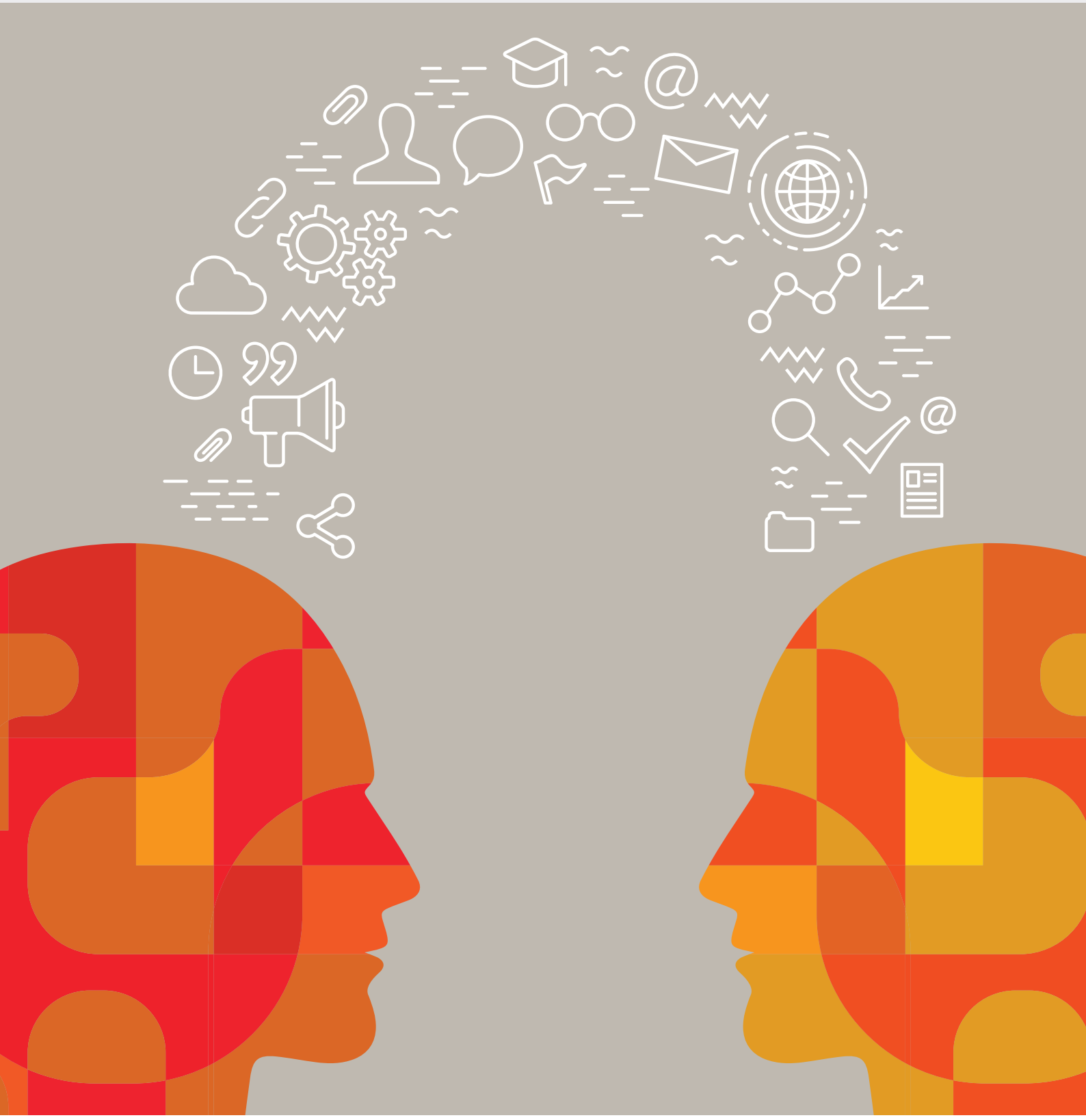
Op het moment dat blijkt dat kennis niet ontbreekt maar gedrag wel, is het interessant om een stap verder te kijken: Vindt men het wel belangrijk genoeg? Ziet men het risico? Als voorbeeld kijken we naar het onderwerp 'sterk wachtwoord'. De data in Figuur 2 laten zien dat maar liefst 82% van de respondenten in de kennistest kan aanwijzen welke van vier wachtwoorden het sterkste is. Als vervolgens gevraagd wordt of zij zelf ook een sterk wachtwoord gebruiken, geeft slechts 31% aan dat te doen. Dus 51% van de respondenten weet wel wat een sterk wachtwoord is, maar gebruikt het zelf niet. Wat is hier aan de hand?



Figuur 2 - Sterk wachtwoord.

Waarschijnlijk motivatie! Of nou ja, een gebrek daaraan dus. Voor sommige organisaties voeren wij aanvullend een reeks interviews uit. In deze interviews is ruimte om dieper in te gaan op de barrières die medewerkers ervaren waardoor ze bepaald gedrag niet vertonen. Wanneer het over 'niet willen' gaat, kunnen daar veel redenen aan ten grondslag liggen. Uit interviews met medewerkers in verschillende organisaties, bleek dat mensen zich vaak laten weerhouden een sterk wachtwoord te kiezen omdat ze het lastig vinden om dat te onthouden. Hoe krijgen we deze mensen dan toch zover dat zij deze barrière kunnen overwinnen? Door ze uit te leggen hoe je een wachtwoord kunt maken dat sterk is maar dat je óók nog kunt onthouden! Of door ze uit te leggen hoe je hiervoor gebruik kunt maken van een wachtwoordmanager. Het inspelen op de reden om niet te willen, motiveert mensen om het ander gedrag te gaan vertonen.

Een ander voorbeeld: wij hielpen een organisatie waar nooit informatiebeveiligingsincidenten gemeld werden. Nooit…. Gewoon geen dus. Heel even zou je kunnen denken dat dat een goed teken is, maar wie iets verder doordenkt, begrijpt dat het waarschijnlijk betekent dat er wel incidenten zijn, maar dat deze niet gemeld worden. Uit de kennistest bleek echter dat veruit het grootste deel van de medewerkers wel wist wat er gemeld diende te worden en waar. Capaciteit op orde dus en het herhalen van de regels niet zinvol meer. Toen we vervolgens met diepte-interviews ingingen op de barrières voor mensen om toch



die stap naar het melden te maken, bleek dat zij niet meer meldden omdat men in het verleden meerdere malen had gemeld, maar daar nooit iets over terug had gehoord. Hierdoor had men de conclusie getrokken dat incidenten niet werden opgepakt en dat melden dus eigenlijk voor niets was. De oplossing in dit geval is dus: motiveren door het laten weten dat meldingen wel degelijk opgepakt worden! Een persoonlijke feedbackmail op een melding in combinatie met een maandelijks overzichtsmail van alle meldingen, wat daarmee gedaan was én wat er door deze meldingen voorkomen was, was voor deze organisatie de sleutel naar gedragsverandering.

Gelegenheid

Naast motivatie is er nog een derde variabele die een sterke invloed op gedrag heeft: gelegenheid. Want wat nou als iemand wel wéét dat hij alleen in zijn eigen account mag werken (capaciteit) en dat ook wel wíl (motivatie), maar dat niet kán omdat hij niet de juiste autorisaties heeft om bij de systemen te kunnen waar hij bij zou moeten kunnen? Gelegenheid kan worden onderverdeeld in context en cultuur.

Context

Bij het bepalen van gedrag, speelt context een belangrijke rol. Immers, de omgeving moet wel toelaten dat mensen kunnen doen wat er van hen verwacht wordt. We kunnen bijvoorbeeld niet verwachten dat mensen documenten met gevoelige informatie veilig weggooien als er geen mogelijkheden voor zijn zoals een shredder. Of dat ze gevoelige informatie niet per mail delen terwijl er geen veilig alternatief is. Vaker dan misschien gedacht wordt, ontbreekt het nog aan dit soort praktische zaken. Wanneer er sprake is van een hoog kennisniveau maar weinig gedrag, is het daarom van belang om zorgvuldig na te gaan of de context voldoende ondersteunend is. Door de medewerkers zelf te vragen! Onze ervaring leert dat security professionals vaak aannemen dat bepaalde zaken voldoende zijn ingeregeld, maar dat ze in de praktijk uiteindelijk niet blijken te werken.

Cultuur

Naast context wordt gelegenheid bepaald door de cultuur in een organisatie. Cultuur speelt een niet te onderschatten rol in wat wel en niet van mensen verwacht kan worden. Zo kan het op papier wel duidelijk zijn dat iedereen wordt geacht elkaar aan te spreken op bijvoorbeeld het niet vergrendelen van een computerscherm of het niet dragen van een pas, maar als de organisatie geen aanspreekcultuur heeft, is elkaar aanspreken wellicht helemaal (nog) niet geaccepteerd en durft niemand zich eraan te branden. Dus wanneer het gaat om het overbruggen van de kennis-gedragskloof, zal ook naar het cultuuraspect gekeken moeten worden: laat de cultuur van de organisatie wel toe dat mensen doen wat van hen gevraagd wordt?

Gelegenheid het probleem? Faciliteren de oplossing!

Wanneer er sprake is van een kloof tussen kennis en gedrag, kan dit dus het gevolg zijn van een gebrek aan gelegenheid. Met andere woorden: mensen vertonen het gedrag niet omdat ze daar de kans niet (voldoende) voor krijgen. Als er in dit soort gevallen wordt ingezet op het communiceren van de regels, kan dit leiden tot frustratie en weerstand. Mensen wéten immers heus wel wat er van hen verwacht wordt, maar ze zijn niet in de gelegenheid om te handelen. Bijvoorbeeld wanneer het systeem om bezoekers aan te melden niet goed werkt, je niet de juiste authorisaties hebt om je werk goed te kunnen doen, of de cultuur niet toestaat dat je anderen zomaar aanspreekt. In deze gevallen heeft het veel meer zin om in te zetten op faciliteren: zorg dat procedureel en technisch goed ingeregeld is dat mensen kunnen doen wat er van hen verwacht wordt en dat de cultuur dit toestaat. Dat is uiteraard makkelijker gezegd dan gedaan, zeker wanneer er cultuurverandering nodig is. Maar het begint allemaal met het besef waar de focus op gelegd moet worden.

Door te begrijpen aan welke knop gedraaid moet worden om gedragsverandering te bewerkstelligen, wordt al een enorme stap voorwaarts gezet. Hierdoor wordt niet langer geïnvesteerd in intiatieven die niet de oplossing zijn en kan juist worden gezocht naar manieren die wel bij de actuele behoefte aansluiten. Efficiënter en effectiever

Referenties

(1) Wetzer, I. M. (2021). Het begint met bewustwording. Hoe ver zijn we daar inmiddelsmee? Informatie Beveiliging, 6, 26-29.

(2) Wetzer, I. M. (2022). De kloof tussen awareness en gedrag. Informatie Beveiliging, 1,14-17.

(3) MacInnis, D. J., Moorman, C., & Jaworski, B. J. (1991). Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads. Journal of Marketing, 55, 32-53.

(4) Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84, 191-215.

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Praat eens met pubers

De sigarettenrook drijft met de zachte zeewind mee. Een zonnestraaltje laat zich voorzichtig zien. Het is vakantie en de deuren van school zitten al een week op slot. Op mijn balkon zit een groep pubers de zondagmiddag te overpeinzen. Te jong om een biertje te drinken in de kroeg, te oud om 'gezellig' dingen met hun ouders te doen. Maar met meer dan volwassen meningen over privacy. En met een haarscherp gevoel voor waar het aan privacy ontbreekt als je een puber bent.

We raken in gesprek over privacy en het duurt niet lang voor de eerste anekdotes zich aandoen. Over de camera die in de meisjestoiletten hangt op school, weliswaar niet in de hokjes zelf, maar is het nou wel echt nodig dat die camera daar hangt? En hoewel die camera dan niet direct op een toiletpot gericht is, kun je wel rechtstreeks vanaf buiten door een raampje inkijken. Meewarig worden hoofden geschud. Op de lagere school trouwens, verhaalt een ander, mogen de juffen en meesters na het sporten in de kleedkamers komen als de kinderen zich aankleden. Geen van hen heeft zich daar heel prettig bij gevoeld en al snel komen dan ook de verhalen over die ene pedofiel die in de kleuterklassen assisteerde*.

Absoluut eensgezind zijn ze over technologie die hen kan tracken: geen van allen zien ze dit zitten en hoewel ze absoluut begrip hebben voor bezorgde ouders, vinden ze het niet te doen om telkens maar overal en altijd gevolgd te worden. Ook een systeem als Magister wordt gehekeld. Hierin worden leerlingen tot op de minuut gevolgd wat betreft onder meer hun prestaties, aanwezigheid, afwezigheid en de redenen daartoe. Niet alleen alle docenten hebben daar toegang toe, ook de ouders en verzorgers. Althans als ze gebruik maken van die app uiteraard. Hoe a-relaxed is het als je ouders al eerder dan jij weten dat je een 3 voor wiskunde hebt gehaald en dat je gymles hebt geskipt? De ouders hadden al een pushmelding gekregen van het systeem voordat je thuiskwam.

Het zal jullie niet verbazen dat ik een groot deel van de aversie met ze deel, dergelijke systemen vormen een enorme inbreuk op het grondrecht op privacy van kinderen. Er is geen ruimte voor onbevangen kind zijn en de randjes opzoeken. En het panoptisch effect moet hier denk ik ook absoluut niet onderschat worden. We voeden een generatie kinderen op die altijd met de dreiging leeft continue bekeken te kunnen worden, maar nooit precies weet wanneer dat het geval zal zijn en wie er dan op een gegeven moment kijkt. Het lijkt me overigens een prachtig onderwerp voor wetenschappelijk multidisciplinair onderzoek, maar dat terzijde.

Ik denk oprecht dat we eens wat vaker met kinderen moeten praten in plaats van ze te volgen met allemaal apps. En niets nieuws onder de horizon, want als ze al die tracking van ouders zat zijn, gaan ze met z'n allen naar een locatie, zetten daarna de telefoon keihard uit en lopen lekker ergens anders heen.

Dank je wel Sydney, Broucke, Naomi, Emma, Storm, Teun en Gina voor jullie wijsheid.

Rachel

*Ik noem in dit stuk geen naam van de school, maar weet uit eigen hand dat dit daadwerkelijk heeft plaatsgevonden en dat de betreffende persoon indertijd gearresteerd is door de politie.

Auteur: Ronald Eygendaal schrijft sinds 1990 over informatiebeveiliging, beveiliging van industriële automatisering en elektronische & technische beveiliging, voor de toonaangevende vakbladen in Nederland en België. Ronald is te bereiken via: info@cqure.nl.

Vernieuwde aanpak voor securitymeldingen

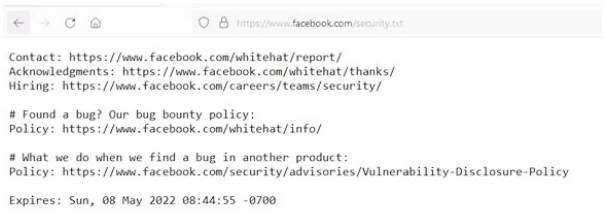
In de beginjaren van het internet was er het Internet Mail Consortium (IMC) dat zich richtte op het gezamenlijk beheren en promoten van standaardisatie voor elektronische post op internet. Zo hebben we in 1997 met het IMC afspraken gemaakt over het gebruik van e-mailadressen. Afgesproken werd voor welke doelen bepaalde e-mailadressen gebruikt mogen (moeten) worden. Deze afspraken zijn uiteindelijk voorgesteld als standaard en zijn vastgelegd in de RFC 2142 (1). Deze RFC heeft de naam `Mailbox Names for Common Services, Roles and Functions' gekregen.

Vele jarenlang vervulde een aantal van deze 'verplichte' adressen een belangrijk rol bij het veilig houden van internet. Zo is het adres abuse@domeinnaam bedoeld om ongewenste e-mails en chatberichten en ander ongepast internetgedrag te melden. Het 'verplichte' e-mailadres security@domeinnaam biedt de mogelijkheid bepaalde dreigingen en kwetsbaarheden te melden. Het melden van kwetsbaarheden wordt ook wel Coordinated Vulnerability Disclosure (CVD) of Responsible Disclosure proces genoemd. Dit proces regelt hoe we op een verantwoorde wijze en in gezamenlijkheid ICT-kwetsbaarheden melden en openbaar maken. Iedereen kan een Responsible Disclosure-melding doen bij een bedrijf, overheidsinstantie of andere organisatie. De organisatie heeft dan de kans om de kwetsbaarheid op te lossen. Voor het melden van een CVD dient, conform RFC 2142, dient het e-mailadres security@domeinnaam te worden gebruikt. Ook wordt geadviseerd om de e-mail adressen zoals abuse@domeinnaam en security@domeinnaam op de hoofdpagina van de website te zetten zodat melders en klagers de adressen makkelijk kunnen vinden. Door de opkomst van contentmanagers, websiteredacteuren en andere editors die de hoofdpagina's vullen, zijn de vermeldingen van de abuse en secure e-mailadressen op hoofdpagina's verdwenen. In veel gevallen zijn de 'verplichte' adressen helemaal verdwenen.

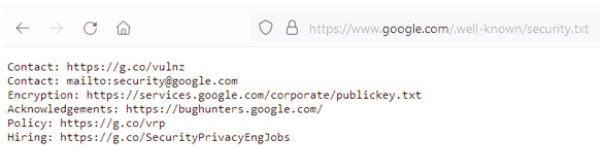
Voorspelbare locatie

In augustus 2021 hebben Edwin Foudil en Yakov Shafranovich bij het Internet Engineering Task Force (IETF) een voorstel ingediend om te komen tot RFC 9116 (2). Deze RFC heeft de naam 'A File Format to Aid in Security Vulnerability Disclosure'. De RFC beschrijft een andere methode om het e-mailadres bekend te maken waarop kwetsbaarheden kunnen worden gemeld. Het idee achter de RFC is eenvoudig: men plaatst een bestand met de naam security.txt op een voorspelbare locatie op de site. Dit is een locatie waar de 'content jongens en meisjes' geen last van hebben en dus de hoofdpagina kunnen volplempen met content. Zoals RFC 9116 aangeeft kan het security.txt bestand in de hoofddirectory van het domein worden geplaatst. Bijvoorbeeld https://www.domeinnaam/security.txt

Hieronder een voorbeeld hoe Facebook dit gedaan heeft:



Maar er zijn ook partijen die de security.txt in de .well-known directory zetten, zoals bijvoorbeeld google:



De inhoud van het security.txt-bestand varieert enigszins, maar de meeste bevatten links naar informatie over het beveiligingsbeleid van de organisatie en een e-mailadres voor het melden van kwetsbaarheden alsook een verloopdatum.
Komende maanden zal het Internet Engineering Task Force (IETF) besluiten of RFC 9116 geformaliseerd wordt. Het lijkt erop dat de internetgemeenschap security.txt gaat omarmen. In Nederland hebben het Digital Trust Center en het NCSC positief gereageerd op security.txt. Nu nog de implementatie. Aan de slag dus en creëer meer ruimte voor content op de hoofdpagina van uw website.
Nagekomen, zie ook het recente bericht van Tweakersnet d.d. 28.04.2022 (3), waarbij de Internet Engineering Task Force (IETF) een nieuwe standaard (RFC 9116 (4)) voorstelt.

Referenties

(1) https://www.rfc-archive.org/getrfc?rfc=2142#gsc.tab=0
(2) https://www.rfc-editor.org/rfc/authors/rfc9116.html
(3) https://tweakers.net/nieuws/196102/ontwikkelaars-stellen-security-punt-txt-standaard-voor-melden-beveiligingsfouten-voor.html?utm_source=nieuwsbrief&utm_medium=email&utm_campaign=twk_nieuwsbrief
(4) https://www.rfc-editor.org/rfc/rfc9116

Auteurs: Jessica Maes is Programmamanager Versterken Cyberweerbaarheid in de Watersector, bereikbaar via jessica.maes@minienw.nl. Rik van Dijk is onderzoeker bij het NCSC en houdt zich daar onder andere bezig met vraagstukken rondom IACS-security en het duiden van kwetsbaarheden. Hij is bereikbaar via rik.vanDijk@ncsc.nl.

Patchmanagement in OT-omgevingen

Een rondgang langs de Infrastructuur & Waterstaat (I&W) sectoren

Patchen, patchen, patchen… patchen. Het advies dat menig securityspecialist geeft aan organisaties zodat ze beter in staat zijn om zich te verweren tegen aanvallers. Het snel patchen van kwetsbaarheden is voor IT-systemen een beproefde methode om snel en efficiënt kwetsbaarheden in systemen te verhelpen en de systemen zo weerbaarder te maken. Maar is dat patchen wel zo eenvoudig in industriële omgevingen met veel operationele technologie?

Steeds meer kaders en normen schrijven voor dat je het patchen op een goede manier hebt ingericht in je organisatie. Binnenkort wordt er in Europees verband besloten over een nieuwe versie van de Europese Directive on security of network and information systems (de NIS Directive (1), ook wel NIB-richtlijn genoemd). Hiermee zal waarschijnlijk de zorgplicht voor organisaties, ook met betrekking tot patchmanagement verder worden uitgebreid.

In OT-omgevingen kan het patchen van je systemen maanden kosten, is downtime onacceptabel en moet je 100% zeker zijn dat de nieuwe update geen onveilige situaties creëert. Allemaal afwegingen waar beheerders van industriële automatisering en controlesystemen (Industrial Automation and Control Systems, IACS) dagelijks mee te maken hebben. Op 24 maart 2022 gingen we in gesprek met de sectoren binnen I&W over verplichtingen, best practices en handvatten voor het patchen van IACS-systemen in de watersector.

Tijdens het webinar werd deelnemers gevraagd of zij wisten welke eisen er gesteld werden aan patchmanagement binnen hun organisatie. 70% van de deelnemers gaf aan dat ze dit niet wisten. Ook gaf 64% van de deelnemers aan dat zij erg veel moeite ervaren om kwetsbaarheden in hun systemen te identificeren. Deze uitkomsten geven aan dat het patchmanagement binnen deze doelgroep nog niet zo gemakkelijk gerealiseerd wordt. Het patchproces, van het identificeren van kwetsbaarheden tot het doorvoeren van de patch, is ingewikkeld en verdient meer aandacht. Om meer duidelijkheid te verschaffen beschrijven we hieronder welke aanpak helpt bij patchen in industriële omgevingen.

Hoe pak je dat aan, risicogericht patchen?

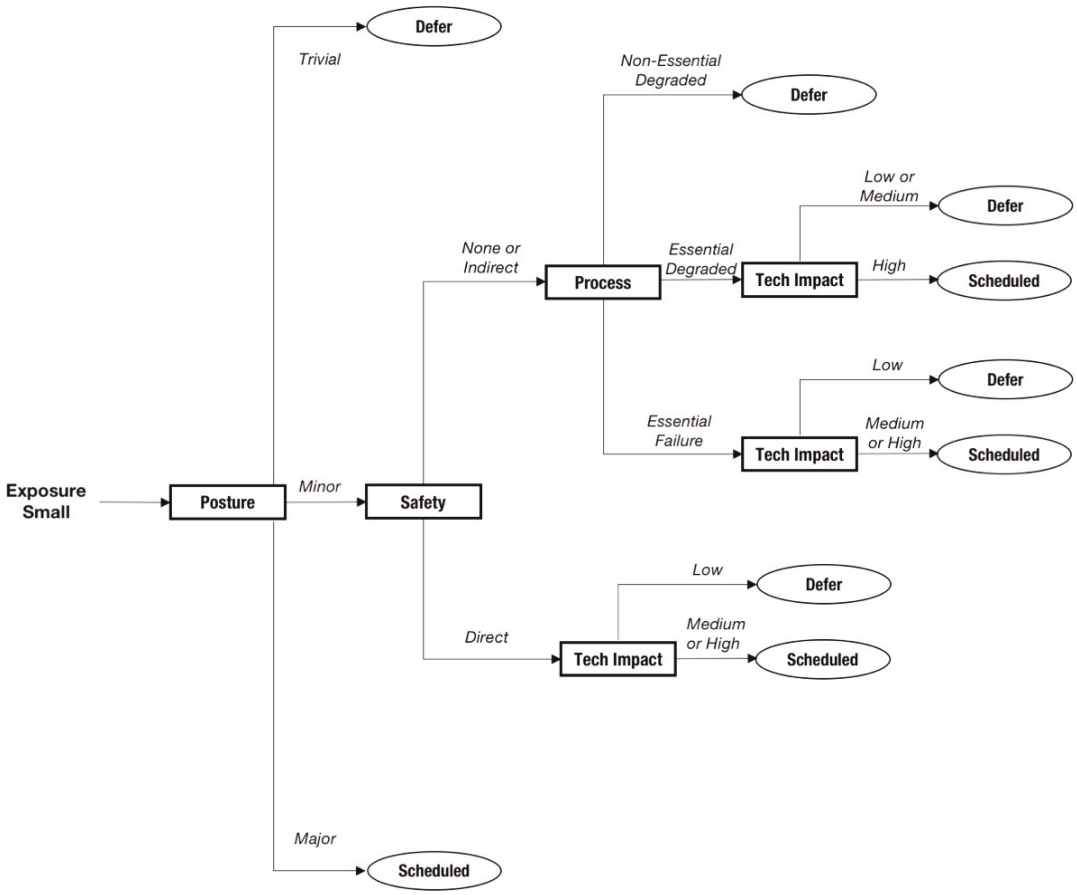
Verschillende standaarden bieden handvatten aan organisaties om hun patchmanagement in te richten. Voor IACS is de meest bekende standaard de IEC 62433 (2). De standaard gaat uit van een risk based approach voor organisaties om hun patchmanagement te doen. Dit houdt in, dat het organisaties aanmoedigt om wel of niet te patchen op basis van een eigen risicoafweging. De IEC 62433 biedt een workflow om patches binnen IACS-omgevingen uit te rollen. Per stap geeft de standaard een aantal handvatten.

Figuur 1 - IEC 62443 workflow. Bron: IEC 62443 2-2.

Om een goede risicoafweging te maken is het belangrijk dat de organisatie goed in beeld heeft welke assets er zijn (assetmanagement), welke componenten, systemen, soft- en hardware. Dit betekent niet enkel de naam en versie van het systeem maar veel meer. IEC 62433 biedt een goed overzicht welke informatie over het systeem verzameld moet worden. Leer het systeem kennen en documenteer dat goed. Daarbij is het belangrijk een duidelijk proces te hebben voor het verzamelen en bewaren van de juiste informatie over de kwetsbaarheid.

Vulnerability scannen heet hangijzer

Vulnerability scannen in IACS-omgevingen is (terecht) een heet hangijzer. Iedereen kent een verhaal waarbij een actieve scan ervoor zorgde dat een proces werd ontregeld. Veel IACS, zeker de oudere systemen, kunnen instabiel gedrag vertonen na een actieve scan. Toch is dat geen reden om scanning helemaal uit te sluiten. Vulnerability scanners kunnen veel toegevoegde waarde hebben; ze kunnen snel en efficiënt kwetsbaarheden identificeren. Bekijk per systeem of het geschikt is om er een scan op uit te voeren. Overleg met de leverancier en vergeet dit ook niet toe te voegen aan de documentatie over het systeem. Het aanschaffen van een vulnerability scanner is ook in IACS-omgevingen zeker het overwegen waard.



Figuur 2 - De SSVC-methode. Bron: first.org (4).

Vervolgens kan met de verzamelde informatie de risicoafweging gemaakt worden. Voor het bepalen van het risico zijn altijd twee elementen belangrijk: impact en kans. In het geval van het patchen in IACS moet niet alleen de vraag worden gesteld: welk risico introduceert een kwetsbaarheid in een IACS, maar ook wat is het risico dat de patch zelf met zich meebrengt? Wat voor kwetsbaarheid verhelpt de patch precies en op welke manieren kan dit uitgebuit worden? Zijn er misschien mitigerende maatregelen voorhanden? Ook het bepalen van de aard van het risico dat een kwetsbaarheid introduceert in het systeem is niet eenvoudig. Hoe meer kennis de organisatie heeft verzameld in de eerdere stap, hoe gemakkelijker de afweging kan worden gemaakt.

De organisatie kan dan een snelle triage doen via bijvoorbeeld een methode als Stakeholder Specific Vulnerability Categorization (SSVC) (3) van Carnegie Mellon. Dit biedt de uitvoerder een korte beslisboom met daarin een aantal vragen die het risico van een kwetsbaarheid verduidelijken. Het begeleidt de gebruiker naar een antwoord dat aansluit op de eigen organisatie.

Daarna kan worden overgegaan op een uitgebreidere risicomethode. Hiervoor biedt de CSIR 3.0 (5) van Rijkswaterstaat een aantal concrete handvatten. Via de RAMSHEEP-methode (6), waarbij ook aandacht voor de impact op de veiligheid en betrouwbaarheid van het aangestuurde proces belangrijk is, kan een uitvoerder een

In OT-omgevingen kan het patchen van je systemen maanden kosten.

goede risico-inschatting van de kwetsbaarheid op het systeem en het aangestuurde proces maken. Een andere strategie die duidelijkheid verschaft is om een Bowtie methode (7) te gebruiken om de invloed van de kwetsbaarheid op de bestaande controls inzichtelijk te maken.

Mocht uit de analyse komen dat patchen de beste strategie is, bereid het management erop voor dat de patch niet morgen al is doorgevoerd of dat de patch kostbaar is om door te voeren. Hier komen we zo op terug. Als laatste volgt een uitgebreid testproces waar de patch eerst wordt uitgerold op test- of niet-kritieke systemen voordat de patch op belangrijkere systemen geplaatst wordt.

Het patchproces is tijdrovend en kost flinke capaciteit omdat de organisatie er zeker van moet zijn dat de patch geen problemen oplevert voor het systeem en de processen die het aanstuurt of monitort. Een duidelijke rolverdeling, waarbij iedereen weet welke taak en rol hij of zij oppakt, wanneer er een kwetsbaarheid met een hoog risico wordt geïdentificeerd, is essentieel. Het kost tijd om in te richten maar scheelt achteraf een hoop tijd en geld elke keer dat een kwetsbaarheid moet worden verholpen.

De businesscase

Zoals gezegd: in tegenstelling tot IT-systemen is patchen voor IACS niet altijd de meest logische keuze. De beslissing om te patchen moet voortkomen uit een goede risicoanalyse en hierbij een gewogen kosten- en batenanalyse. Voor deze beslissing is uiteindelijk het bestuur verantwoordelijk. Vergeet als verantwoordelijke niet te hameren op de laatste stap in de workflow: verificatie en vastleggen.

Het helpt om de argumenten – voor het wel of niet patchen van een systeem – toe te lichten en vast te leggen door termen te gebruiken die de taal van de organisatie en het management reflecteren. Wat voor impact kan een kwetsbaarheid hebben op de bedrijfsvoering? Wat zijn de kosten voor het verhelpen van die kwetsbaarheid? Hoeveel tijd kost het verhelpen en hebben we de juiste kennis in huis? Management, OT-Specialisten en patchmanagers moeten om de tafel om deze onderwerpen te bespreken en om taalbarrières te slechten.

Om een goede businesscase te bouwen moet dan ook geen sprake zijn van taalverwarring tussen de uitvoerders en het management. Dit betekent dat beide partijen de tijd moeten nemen om elkaars werelden te begrijpen. Besteed hierbij aandacht aan het duidelijk uitleggen van het afwegingsproces dat een uitvoerder maakt. Eerdere genoemde middelen zoals een Bowtie kunnen helpen om het afwegingsproces ook voor anderen inzichtelijk te maken.

Duidelijkheid in taal tussen de verschillende stakeholders binnen de organisatie maken het beslissingsproces rondom het oplossen van kwetsbaarheden gemakkelijker en dragen bij aan een beter begrip tussen management en uitvoerders met betrekking tot de risico's waar de organisatie mee te maken heeft.

Hoe nu verder?

Zoals eerder benoemd is het patchen van IACS een ingewikkeld en tijdrovend proces. De focus zou moeten liggen op het maken van een goede risicoafweging. Uitvoerders hebben weinig aan stoere uitspraken en silver bullets. Deelnemers aan het webinar gaven aan dat zij behoefte hebben aan praktische handvatten en middelen. Soms zijn deze praktische richtlijnen er al, zoals de CSIR 3.0 waar ook het patchmanagement uitvoerig in wordt beschreven.

Als we het patchmanagement in IACS serieus nemen, moeten we begrip tonen voor de complexe werkelijkheid en tegelijkertijd handreikingen doen om de stappen die moeten worden doorlopen te vergemakkelijken. Dit artikel biedt een aantal eerste stappen die gezet kunnen worden maar volgende stappen zijn absoluut noodzakelijk. Daarom investeert het NCSC in verder onderzoek naar het vergemakkelijken van het patchmanagement in OT-omgevingen en werkt zij samen met I&W om organisaties bewuster te maken van het belang van risicogericht patchen.

Referenties

(1) https://digital-strategy.ec.europa.eu/en/policies/nis-directive
(2) https://en.wikipedia.org/wiki/IEC_62443
(3) GitHub - CERTCC/SSVC: Stakeholder-Specific Vulnerability Categorization
(4) https://www.first.org/
(5) csir-34-definitief-concept-20210914.pdf (cip-overheid.nl) en
https://www.magazinesrijkswaterstaat.nl/zakelijkeninnovatie/2022/01/cybersecurity
(6) https://repository.tudelft.nl/islandora/object/uuid:bfeae01d-cfbc-4749-bf2c-531fc7d802d0
(7) https://www.cgerisk.com/knowledgebase/The_bowtie_method

Even voorstellen

Audits, **R**isico- & securitycompliancemanagement, **D**ataprotectie; dat is waar ik mij mee bezighoudt. Sinds kort mag ik daaraan toevoegen dat ik mij als algemeen bestuurslid zal inzetten voor het PvIB. Op deze pagina mag ik mij even voorstellen: "mijn naam is Ruiter, Ard Ruiter".

Het begint natuurlijk met de A, de A van actief. Al enkele jaren zet ik mij actief in voor het PvIB. Dat is hartstikke leuk om te doen, zowel vanwege de inhoud van dit mooie vakgebied van de informatiebeveiliging alsook vanwege het kennisplatform met vakgenoten. Er zijn vele professionals binnen het PvIB met een groot arsenaal aan kennis, kunde en vaardigheden. Dat merk ik temeer bij de bijeenkomsten van de vereniging als ik in de aanloop, de pauze of na afloop in gesprek ga met de leden: met jullie dus. In die gesprekken merk ik hoeveel potentie er in de vereniging is en dat we met z'n allen deze vereniging nog beter, leuker en interessanter kunnen maken dan het PvIB nu al is.

Aan de Rijksuniversiteit Groningen heb ik rechten gestudeerd. Na mijn rechtenstudie heb ik juridische functies verricht. Vanuit het juridische metier werd mijn belangstelling gewekt voor de gegevensbescherming en privacy; het betreft een interessant spanningsveld tussen het belang van de openbaarheid van informatie, het verder verwerken van informatie en het individuele recht op privacy- en gegevensbescherming. Het was destijds een vrij onontgonnen gebied. In mijn zoektocht naar kennis kwam ik in aanraking met het PvIB en mocht ik mijn eerste artikel voor iB-Magazine schrijven onder de titel 'Privacybescherming en politiegegevens' (1). Langzaam maar zeker verbreedde mijn belangstelling zich voor de aanpalende thema's als governance, compliance, riskmanagement, de integrale beveiliging en met name de informatiebeveiliging (én cyber- en datasecurity). Het 'PvIB: Platform voor informatiebeveiliging' – zoals onze vereniging officieel volgens het Handelsregister heet – is dan ook de perfecte omgeving om goed op de hoogte komen én te blijven van dit vakgebied. Daaruit ontstonden bij mij ideeën om nog meer te gaan doen met het PvIB en mijn enthousiasme is kennelijk voldoende gebleken om te mogen toetreden tot het PvIB-bestuur. Met de doorlopende digitale transformatie wordt ons brede vakgebied ook nog eens boeiender.

Mijn speerpunt zal zijn om al die potentie die 'wij' als vereniging hebben op meer terreinen in te zetten: op verbinding tussen bestuur én de professionele leden, waarin ik het bestuur als een actieve facilitator zie om de leden met hun kennis, kunde en vaardigheden nog meer en/of beter te kunnen laten schitteren. Samen met de collega-bestuursleden ga ik bezien hoe we de ideeën in daden kunnen omzetten. Zo denk ik aan het maken van infographics, het instellen van kennisgroepen, het nog meer betrekken van de klankbordgroep en meer profileren als PvIB.

We gaan elkaar vast en zeker tegenkomen op een van de vele PvIB-bijeenkomsten. Jeuken jouw vingers ook, barst je van ideeën, of wil je 'gewoon' eens sparren om te kijken wat we met jouw ideeën kunnen doen? Schroom dan niet om contact op te nemen. Jouw betrokkenheid wordt gewaardeerd. Stuur een e-mail naar secretariaat@pvib.nl.
Ik ga ervoor. Immers, niets is moeilijk voor hen die willen, of in het Latijn: nil volentibus arduum.

Graag tot ziens, tot horens, via de e-mail of in het echt!
Met vriendelijke groet,
Ard Ruiter

[1] http://docplayer.nl/20314927-Privacy-juridische-aspecten-van-informatiebeveiliging-vaak-onderbelicht-revocable-privacy-slaat-brug-tussen-veiligheid-en-privacybelang.html

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

COLUMN DIMITRI

Ken je die mop van de BSM's?

De Basis Security Maatregelen ook wel BSM's genoemd. Wie kent ze niet? Ze horen thuis in het rijtje van de schijf van vijf, 3x per dag tanden poetsen, schone sokken en ondergoed en andere rudimentaire hygiëne maatregelen die we onszelf als maatschappij opleggen. Toch?

Was het maar zo. Veertig jaar geleden werd e-mail bedacht, het world wide web volgde snel en werd vormgegeven rondom SMTP poort 25 (Simple Mail Transfer Protocol) en HTTP poort 80. Achter de HTTP is inmiddels een s gekomen, die staat voor secure. E-mailen doen we veertig jaar na dato nog steeds onbeschermd en ongeverifieerd. En dat terwijl we dagelijks lezen dat het klikken op phishing mails leidt tot ransomware aanvallen. Wordt er wel een certificaat gebruikt, dan staat de e-mail weer onversleuteld op de mailserver waardoor de admin en de 16-jarige puber uit Engeland, die inmiddels ook admin is, lekker mee kunnen lezen. Wekelijks ligt de boel op straat of wordt verhandeld op het darkweb.

Kijkend naar de Faalkaart (1), een kaart waarop de mate van online veiligheid (website en externe netwerkdiensten) van lokale overheden in beeld wordt gebracht, zie je al jarenlang rode gemeenten, provincies, zorgorganisaties, enz. De groene uitzonderingen moet je met een vergrootglas zoeken. Het is al jaren rood en het staat al jaren 'op de bestuurlijke agenda'. Ja ik weet dat niet al die categorieën even belangrijk zijn en IPv6 nog jaren duurt. En dat gemeente Ameland (op 7 na beste!) niet hetzelfde is als gemeente Groningen (slechtste) terwijl ze bijna naast elkaar liggen. Maar toch, als je het dan niet voor je eigen inwoners doet, doe het dan als wethouder vanwege je beroepseer. Dat je kwaliteit wilt leveren misschien? Dat je je digitale vuile was niet buiten wilt hebben hangen?

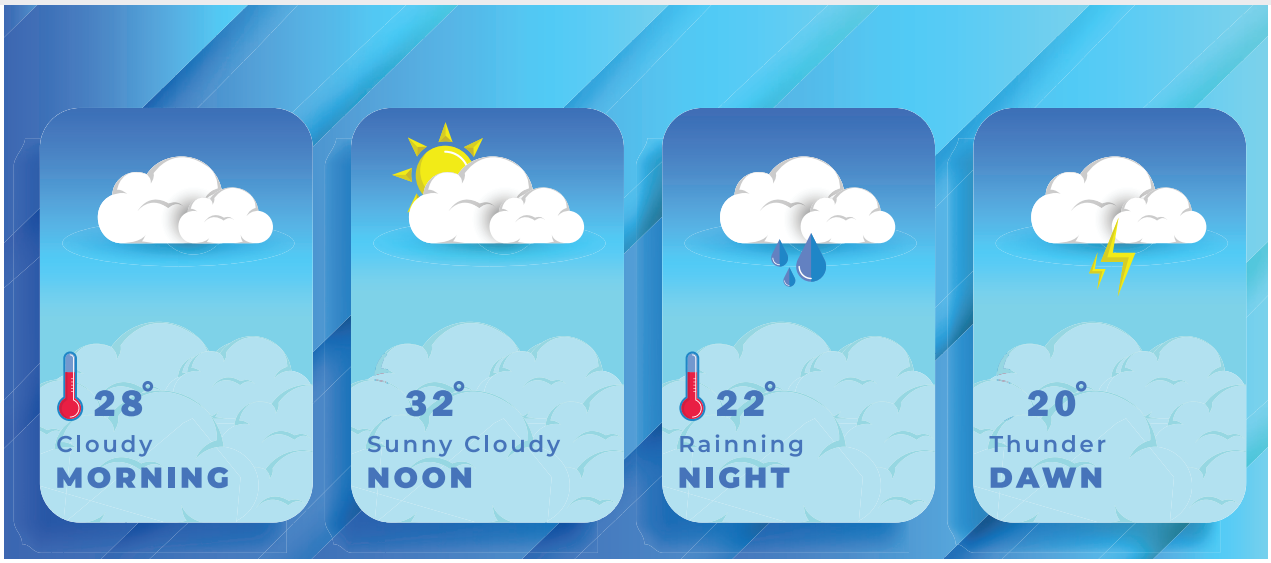
Het CyberSecurity Beeld Nederland (CSBN) is niet veel beter. Het NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid) schetst al elf (!) jaar lang een bedroevend beeld van de weerbaarheid van de Nederlandse digitale infrastructuur tegen cyberdreigingen. Sinds 2011 wordt ieder jaar gemeld dat de basale beveiligingsmaatregelen niet op orde zijn. 'Investeren in mensen' is de oplossing volgens de auteurs. Een paar bestuurders ontslaan lijkt me een beter signaal. Even voor de duidelijkheid: we hebben het in al die rapporten niet over investeren in dure anomaly detectie, vette soc/siems, iedereen een E5 licentie of PhD's in threathunting aanstellen. We hebben het nog steeds over de Basishygiëne. Tenenkaas!

De Onderzoeksraad voor Veiligheid rapporteerde over de Citrix ellende en noemde haar rapport 'Kwetsbaar door Software'. Het sprak over 'fabrikanten die te weinig prikkels ontvangen' en 'producenten die doen aan symptoombestrijding'. Inmiddels zijn we een SolarWinds, Kaseya en LOG4J verder en weten we allemaal dat cyber selectiecriteria, controle op de werking van de ISAE3402 controls, een actuele goedgevulde CMDB/SBOM en patchen de basis dienen te vormen om weerbaar te kunnen zijn tegen supplychain risico's. Basishygiëne! Ze hadden het rapport ook 'Kwetsbaar door automutilatie' mogen noemen.
Daar zitten we dan, met ons vuile digitale ondergoed in een hybride oorlog aan de rand van de EU. NATO-partners om ons heen hebben cyber Shields-Up decreten gestart en dwingen met wetgeving de toepassing van de basis cyberhygiëne en het melden van incidenten af. De Europese NIS2 Directive gaat bestuurders aansprakelijk stellen voor het falen op de BSM's. Het werd een keer tijd.

Het is daarom ook te makkelijk om de openingsvraag: 'Ken je die mop van de BSM's?' te beantwoorden met: 'Die kwamen niet!'. Ze gaan er komen en ze móeten er komen. Door wetgeving en door collectieve boycot van digitale bedrijven die weigeren hun zaken op orde te brengen. Aan het werk!

Referentie: (1) De Faalkaart is te vinden op: www.basisbeveiliging.nl.

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



BLOG

‘I think it is going to rain today’: een duidelijke threat intelligence

Hoe duidelijker je wanneer, wie, waar, wat en hoe (waarom) van je verwachting benoemt, des te hoger is de effectiviteit van je threat intelligence. In dit artikel geef ik aanbevelingen voor het preciseren ervan.

UB40

`I think it is going to rain today’ is onderdeel van het debuutalbum (1980) van UB40. Een groep werkeloze Britse jongeren begon bij gebrek aan inkomen een reggaeband. Het aanvraagformulier `Unemployment Benefit 40’ is afgekort de bandnaam en staat op de albumhoes. De albumtitel `Signing off’ betekent `afhaken’, maar ook `stempelen’. Dat is de Belgische term voor wat een uitkeringsgerechtigde doet als hij `in de WW loopt’.

Vanuit die context en tijd is het lied niet alleen een weersverwachting, maar een onheilsboodschap. Dat is een mooie Nederlandse term voor `threat intelligence’: informatie, over naderend onheil, waarvan de kans van optreden dus niet exact te bepalen is. Regen is geen IT-dreiging, maar wel een dreiging. Niemand houdt van een onverwacht nat pak en als iemand je waarschuwt dat het vandaag gaat regenen, kun je voorbereidingen treffen (thuiswerken, of regenpak en paraplu meenemen).

Wanneer – de periode

Het lied is niet ambitieus in de voorspellingsperiode – nog korter, en je komt uit op `Het regent, het regent, de pannen worden nat’. Dat kinderliedje is 100% nauwkeurig, beschrijft de situatie accuraat en objectief en bevat de voor sommige lezers zo belangrijke herhaling van belangrijke punten. Het kijkt echter nauwelijks vooruit. Vroeg in de morgen is de regenvoorspelling waardevoller dan pas bij het toetje na

het avondeten. Een voorspelling als 'op 27 april 2024 gaat het regenen' heeft in 2022 echter ook weinig betekenis, door het gekozen regenvoorbeeld.

De periode van de voorspelling moet dus niet te kort en niet te lang zijn, en daarbij inspelen op het belang van wat voorspeld wordt. Bij korte voorspelperiodes is zelfs het moment van de uitspraak van belang. Leg dit dus duidelijk vast.

Wie – de voorspeller en zijn bronnen

Het lied is geschreven door Randy Newman, UB40 is de boodschapper. Het is daarmee onduidelijk wie de 'ik' uit de titel is. Maar voor de ontvanger van de threat intel is dit wel van groot belang. Het maakt verschil of (wijlen) Jan Pelleboer, Piet Paulusma (helaas…), een reggaeband of prof. Jaap van Dissel bij je aanbelt met deze mededeling.
De ontvanger heeft dus informatie nodig over de brenger van de boodschap om de waarde of het belang ervan goed in te kunnen schatten. Heeft hij het zelf verzonnen of bedacht? Of is de voorspelling gebaseerd op uitgebreid brononderzoek en analyse en hoe betrouwbaar zijn die bronnen zelf dan?
Objectieve metingen en een proven track record van de adviseur laat ik weg. Van beleggingsproducten weten we: 'behaalde resultaten in het verleden zijn geen garantie voor de toekomst'. Aan de andere kant: na 13 dagen regen op de camping wordt de laatste vakantiedag waarschijnlijk ook wel slecht. Dus tellingen van opgetreden incidenten hebben wel een beetje nut voor informatie over komende dreigingen.
Voor sommige lezers doe je het trouwens nooit goed. Ik had ooit een manager die over mijn threat intelligence zei dat het nu al de derde keer in korte tijd was dat hij over een bepaalde dreiging hoorde. Hij raakte het beu en was er, in 2022-termen, wel klaar mee. Maar als je het advies van 'The boy who cried wolf' de vierde keer niet serieus neemt, ligt het risico dat er nu wél een echte bijtende wolf (invasie, virusvariant, dictatuur) arriveert, geheel bij degene die het vierde advies compleet negeert.

Waar – het geografisch gebied

Ook is van belang dat het lied staat op een 33 toeren langspeelplaat uit 1980 en het niet live op straat of bij de voordeur door de zanger wordt verkondigd. Wanneer de threat intelligence schriftelijk wordt gedeeld, moet uit de mededeling zelf duidelijk zijn wanneer de voorspelling is gedaan. Wanneer de informatie van een externe bron, via modernere media (SMS, whatsapp, mail, tweet) opnieuw wordt gedeeld, zal de ontvanger logischerwijs aannemen dat het een actuele voorspelling is. De tekst van 'I think…' noemt geen geografische plaats. Wanneer een DJ in een radio-uitzending of op een festival het lied afspeelt, zullen de luisteraars denken dat het een voorspelling is voor Nederland of het festivalterrein.

Om threat intelligence toepasbaar ('actionable') te maken, moet je natuurlijk vermelden waar het onheil (naar verwachting) zal gaan optreden. In Nederland of daarbuiten, alleen op Android of ook IOS, welke versie van het operating system is kwetsbaar, enzovoort.

Wat en hoe – wat gaat er gebeuren

De melding is niet concreet: 'going to rain' is een breed begrip en varieert van miezerregen, motregen, hoosbui, het giet, het staat te regenen (in West-Brabant), 't is nat (in Groningen) tot zware of hevige regenbuien (journaal). Wanneer er nog hagel, storm, hevige wind, onweer of een overstroming bij komt, klopt de voorspelling wel, maar voor de slachtoffers van de natuurramp maakt het een groot verschil.
Een specifiekere voorspelling, zoals 'Het gaat regenen en óók onweren', heeft een hogere waarde voor de ontvanger. De kans dat het precies zó uitpakt als voorspeld wordt wel kleiner. Maar jezelf als leverancier van threat intelligence tegen falen compleet in te dekken door te komen met 'Het weer wordt volgende maand anders', voegt geen waarde toe.

Kans van optreden – hoe zeker ben je van je zaak

De kern van de voorspelling in dit lied zit in 'think'. Het Nederlands heeft diverse varianten op 'Ik denk dat…'. Sommige uitdrukkingen zijn sterker (overtuigd, weet zeker, vast en zeker, het zal), andere zijn zwakker (ik vermoed, misschien, er is een kans dat, het zou kunnen dat). Er zijn manieren om een eigen voorkeur in de verwachting aan te geven (ik hoop, reken erop, verwacht) – hiermee kan de leverancier tonen hoe subjectief hij in de wedstrijd zit. Die transparantie wordt soms (wereldoorlog) opzettelijk weggelaten uit politiek geladen threat intelligence.
Termen als 'mij lijkt', 'ik heb het gevoel', 'volgens mij', 'ik heb zoiets van' tonen dat jij als auteur het ook niet weet, maar (CYA = cover your ass) het toch even wilt melden. Dergelijke termen zou ik weglaten uit een professioneel threat intelligence rapport. Probeer de ingeschatte kans van optreden

De kwaliteit van threat intelligence en eruit resulterende acties neemt toe wanneer leverancier en afzender de verschillende niveaus van zekerheid benoemen, bespreken en er duidelijke afspraken over maken.

zo concreet mogelijk te maken in je formulering (zie voorbeelden hieronder).

Met het simpele woordje 'niet' kun je trouwens threat intelligence (onbedoeld) onduidelijker maken: het verschil tussen 'ik weet zeker dat…' en 'ik weet niet zeker dat…'. Hier is de ontkenning aan het weten gekoppeld en niet aan de voorspelling zelf. Of 'ik twijfel of…' versus 'ik twijfel niet of…'. De ontkenning draait de betekenis niet 100% om: wie niet zeker weet of het vandaag gaat regenen, zegt niet dat hij zeker weet dat het vandaag droog blijft. 'Niet' kan ook intelligence van concurrerende voorspellers afzwakken. Zeg gewoon als reactie op een rapport van een andere threat intelligence leverancier: 'ik weet niet of…' (zelfs als je het nog niet gelezen hebt) en de twijfel rijst al. Let nauwkeurig op het gebruik van 'niet' in (eigen) rapportages.

Standaard zekerheidsniveaus

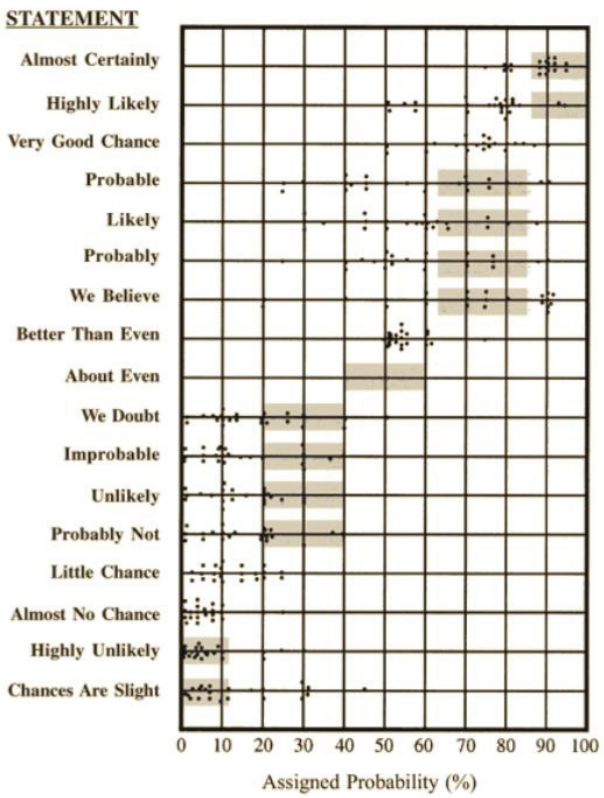
Voor mij klinkt iemand die iets vermoedt, onzekerder van zijn/haar zaak dan wie iets denkt. Bij iemand die zegt iets zeker te weten, neem ik aan dat het geen pure fantasie is en dat er andere bronnen aan ten grondslag liggen. Bij iemand die mij zegt 'dat wil je niet weten', vraag ik altijd door om het wél te weten komen, want ik verwacht dan dat hij/zij het zelf niet weet.

Het liefst heb je dat de Intel leverancier kan stellen: dit weet ik 80% zeker en dat 20% zeker. Zover is het helaas nog niet. Maar als tussenoplossing kun je als leverancier en ontvanger samen, binnen je organisatie of branche, een aantal standaardtermen over zekerheid afspreken en daarbinnen een vaste rangschikking bepalen en die dan in alle threat intelligence rapporten hanteren.
Ik doe een ruw voorstel, aflopend gesorteerd in kans van optreden:
1. Ik weet zeker, er zal…
2. Met aan zekerheid grenzende waarschijnlijkheid
3. (Zeer) waarschijnlijk
4. De kans is (zeer) groot dat
5. Het kan vriezen/dooien (50/50) (is eigenlijk: ik heb geen idee, kan nog alle kanten op)
6. De kans is (zeer) klein dat
7. Het is/lijkt onwaarschijnlijk
8. Ben/weet vrijwel zeker dat niet….
9. Ik eet mijn hoed op, als…
10. Echt niet, zeker weten, ik zweer het op mijn moeder/kinderen, nooit.

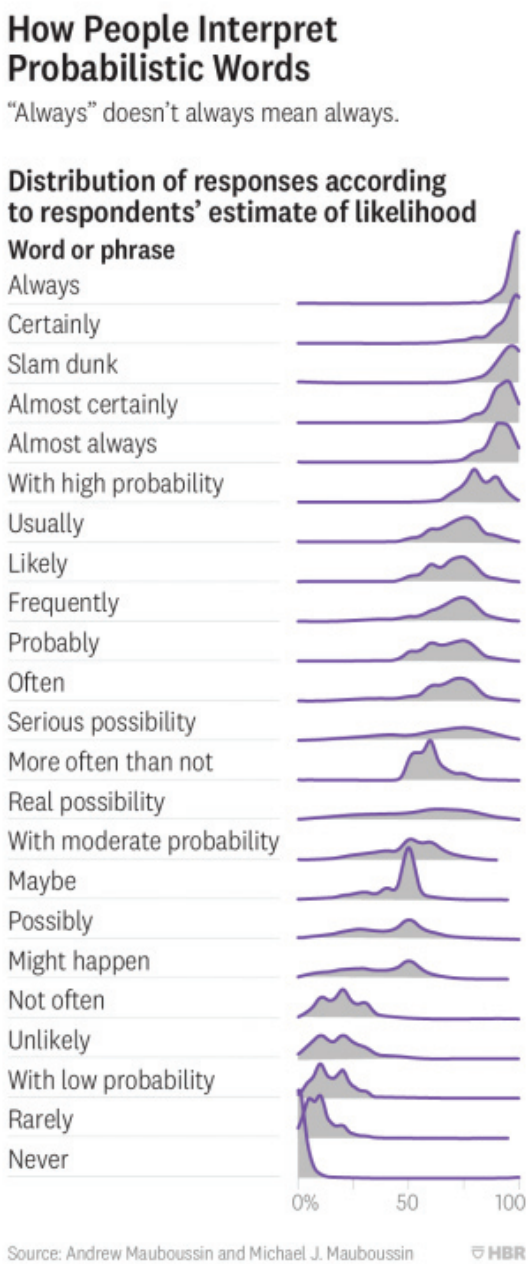
Nummer 5 is gevaarlijk, want waarom meld je het dan als mogelijke dreiging? Door bij 4 en 6 te kiezen voor zéér groot/klein blijf je als organisatie zoveel mogelijk uit het wazige en nietszeggende midden.

Achtergrondinformatie

Het volgende schema komt uit CIA-pensionado Richards Heuer boek 'Psychology of Intelligence Analysis' (1).



Figuur 1 - Schema Richards Heuer - NATO puntenwolken.



Figuur 2 - How people interpret probabilistic words. Bron: Andrew Mauboussin and Michael J. Mauboussin.

Een groep van twee dozijn NATO-officieren (de afzonderlijke puntjes per regel), gewend aan het lezen van intelligence rapporten, gaven hun inschatting van de procentuele kans van optreden bij het lezen van de statements in de linkerkolom. De puntenwolken zijn duidelijk verspreid door de verschillende interpretaties.

Op 3 juli 2018 publiceerden Andrew Mauboussin and Michael Mauboussin in Harvard Business Review het artikel: 'If you say something Is 'likely,' how likely do people think it is?' (2)

De grafieken (de sparklines van Edward Tufte, daarover een volgende keer meer) (zie figuur 2) tonen hoe hun 1.700 respondenten termen vertaalden naar een procentuele kans. Vooral de uitdrukking 'real possibility' werd zeer breed geïnterpreteerd als 'tussen de 20 en 80% kans'. Ook ogenschijnlijk absolute begrippen als 'always' en 'never' blijken niet voor iedereen altijd (100%) en nooit (0%) te betekenen. 'Slam dunk' is als Amerikaanse sportterm cultureel bepaald en voor lezers uit een andere cultuur veel moeilijker te begrijpen. Ook iets om op te letten in je threat intelligence rapporten.

Referenties

(1) https://hbr.org/2018/07/if-you-say-something-is-likely-how-likely-do-people-think-it-is.

(2) https://www.cia.gov/static/9a5f1162fd0932c29bfed1c030edf4ae/Pyschology-of-Intelligence-Analysis.pdf

Auteur: Renco Schoemaker is senior adviseur informatiebeveiliging en privacy en werkt als zelfstandige onder de naam `qeep IT safe' voor (lokale) overheden. Hij is bereikbaar via r.schoemaker@qeep.nl.

Aanbesteden en informatiebeveiliging – drie smaken

Aanbesteden is een vak op zich omdat het gebonden is aan de nodige regels. Als CISO wil je graag dat informatiebeveiligingseisen aan het begin van het (inkoop)proces worden meegenomen: security-by-design. In de praktijk van de afgelopen jaren zie ik dat opdrachtgevers vrij veel tijd kwijt zijn met het bedenken van (dezelfde) eisen of zeer gedetailleerde eisen stellen. In dit artikel werk ik drie smaken uit van het opnemen van informatiebeveiliging in een aanbesteding.

In overheidsland wordt er heel wat aanbesteed. Aanbesteden is een vaak wettelijke verplichte methode van inkoop waarbij de opdrachtgever kenbaar maakt welke opdracht er aan komt. Een aanbesteding gaat gepaard met een programma van eisen waar inschrijvers aan moeten voldoen indien zij een offerte wensen in te dienen. Aan het einde van de rit wordt de opdracht gegund aan één inschrijver.
Het idee achter aanbesteden is dat uiteenlopende aanbieders (groot én klein) overheidsopdrachten kunnen binnenhalen en overheden een grotere kans hebben op een optimale prijs-kwaliteitverhouding. Of dat lukt valt te bediscussiëren, maar liever zoom ik in op informatiebeveiliging. Wordt daar een optimale prijs-kwaliteit behaald? Aan welke knoppen valt te draaien om zo invloed op die prijs-kwaliteit uit te oefenen?

De drie smaken

Het van toepassing verklaren van de juiste inkoopvoorwaarden en format verwerkersovereenkomst is het eenvoudige werk. Hoe ga je als opdrachtgever, informatiebeveiliging opnemen in het programma van eisen? Dat kan op de volgende drie manieren:

1. **Geschiktheidseisen**: met geschiktheidseisen toetst een opdrachtgever of een inschrijver geschikt is om de opdracht uit te voeren. Dit zijn dus eisen die gesteld worden aan een bedrijf.
2. **Gunningseisen**: met gunningseisen toets een opdrachtgever of de IT-oplossing van de inschrijver voldoet aan het gewenste 'niveau'. Dit zijn dus eisen die gesteld worden aan de IT-oplossing.
3. **Gunningscriteria**: met gunningscriteria toetst een opdrachtgever bij het Beste Prijs-KwaliteitsVerhouding (BPKV) criterium wat de beste inschrijving is. Dit zijn dus geen eisen waaraan moet worden voldaan, maar (selectie)criteria voor gunning.

Smaak 1: Geschiktheidseisen

Dit zijn eisen die gesteld worden aan een bedrijf, ofwel de inschrijver. Andersom kunnen dit dus geen eisen aan de IT-oplossing zijn die wordt aangeboden. Toegepast op informatiebeveiliging is mijn advies om als geschiktheidseis het hebben van een managementsysteem voor informatiebeveiliging dat voldoet aan de eisen van ISO 27001, NEN 7510 of gelijkwaardig op te nemen. Dat is bewust wat voorzichtig geformuleerd omdat de wetgever heeft bepaald dat 'of gelijkwaardig' moet worden toegevoegd en daarom kan je niet alleen als geschiktheidseis het hebben van bijv. een ISO 27001 certificaat opnemen.
Voldoen aan deze eis voor een 'managementsysteem voor informatiebeveiliging' gaat natuurlijk het eenvoudigst door het overleggen van een ISO 27001 of NEN 7510 certificaat. Enkele aandachtpunten daarbij:

- het moet gaan om een managementsysteem bij de inschrijver zelf;
- het certificaat dient te zijn afgegeven door een daartoe geaccrediteerde organisatie;
- de bijbehorende Verklaring van Toepasselijkheid (VVT) mag niet ontbreken.

Eventueel kun je op voorhand aangeven welke beheersmaatregelen wel/niet 'buiten scope' mogen zijn in de VVT. Tot slot is het van belang te definiëren op welke wijze de opdrachtgever vaststelt hoe het managementsysteem voldoet aan de eisen van ISO 27001 of NEN 7510 zónder dat de inschrijver één van beide certificaten kan tonen. Het managementsysteem heeft wat mij betreft minimaal een actueel en compleet kwaliteitshandboek informatiebeveiliging, een beveiligingsorganisatie en een jaarlijkse, onafhankelijke toetsing op de getroffen beveiligingsmaatregelen.
Ik zie te weinig dat informatiebeveiliging is opgenomen als geschiktheidseis bij aanbestedingen, terwijl het wel vaak als

Inkoopvoorwaarden en verwerkersovereenkomst

Het van toepassing verklaren van de ARBIT (rijksoverheid) GIBIT (gemeenten) als inkoopvoorwaarden voor IT-opdrachten lijkt me een open deur. Dat moet je zeker doen indien het hoofdonderwerp van de aanbesteding dat toelaat. Niet iedereen zal positief reageren op dit standpunt en ik kan het boek 'Reset de gemeentelijke ICT' van Kees Groeneveld en Herman Timmermans in dat licht aanbevelen.
Indien er persoonsgegevens worden verwerkt binnen de opdracht die wordt aanbesteed, stel dan een format verwerkersovereenkomst verplicht. Een tweede open deur gezien het verplichtende karakter van het VNG-format voor gemeenten. Voor de rijksoverheid is er een model dat aansluit op de ARBIT, maar het gebruik daarvan is niet verplicht.

De drie smaken zijn uitstekend met elkaar te combineren zolang je weet wat je doet; niet alle combinaties zijn logisch.

gunningseis opgenomen wordt (smaak 2). Mijn advies is hiervoor de geschiktheidseis in te zetten en níet de gunningseis. Dit omdat het managementsysteem immers primair toeziet op de inschrijvende organisatie en niet op de IT-oplossing.

Smaak 2: Gunningseisen

Dit zijn de eisen die worden gesteld aan de IT-oplossing. Hier heb je eigenlijk twee afslagen: 1) gunningseisen in aanvulling op bovengenoemde geschiktheidseis, en 2) gunningseisen zónder bovengenoemde geschiktheidseis. In het eerste geval neem je als eis nummer één op dat de IT-oplossing dient te vallen onder de reikwijdte van het al dan niet gecertificeerde managementsysteem. Vervolgens kan je eisen opnemen over bijvoorbeeld SLA, framework voor softwareontwikkeling, hardeningsrichtlijnen, logische scheiding bij cloudinfrastructuur en talloze andere, specifieke gunningseisen waar de IT-oplossing aan moet voldoen. Te denken valt aan verplichte standaarden, koppelvlakken, protocollen etc.

Ontdubbel je eisen wel met de inkoopvoorwaarden en de verwerkersovereenkomst en neem alleen specifiekere zaken op dan wat de ISO 27001 annex A al benoemt. Dus bijvoorbeeld beveiligingsmaatregelen waarvan je zeker wilt weten dat ze conform ISO ISO 2700/BIO zijn geïmplementeerd bij de IT-oplossing. Verder is het mijns inziens van (groot) belang duidelijk te benoemen (of eisen) dat de inschrijver jaarlijks middels een auditrapport – opgesteld door een onafhankelijke derde – dient aan te tonen dat de beveiligingsmaatregelen, zoals geïmplementeerd bij de IT-oplossing, werken. Indien ISO 27001/NEN 7510/gelijkwaardig als geschiktheidseis is opgenomen ben je nu klaar wat mij betreft. Heb je die geschiktheidseis (smaak 1) niet opgenomen, dan raad ik aan tenminste gunningseisen op het gebied van General IT Controls (GITC) op te nemen. Verwijs niet naar de gehele ISO27002/BIO bij de gunningseisen en ga er niet alle maatregelen uit kopiëren. Indien je ISO 27001/NEN 7510/gelijkwaardig niet of zelden als geschiktheidseis wilt opnemen, dan zou ik een standaard lijst met gunningeisen opstellen. Onthoud daarbij dat voor alle geschiktheids- en gunningseisen geldt dat níet voldoen een 'exit' betekent voor de inschrijver. Het zijn dus 'knock-out' criteria.

Smaak 3: Gunningscriteria

Zoals de naam al doet vermoeden, gaat het hier echt om iets anders. Dit zijn geen eisen aan de inschrijvende organisatie of de IT-oplossing, maar criteria waarlangs de aanbesteding gegund kan worden. Vaak zijn er uiteenlopende gunningscriteria en één of meer daarvan kan een criterium zijn op het gebied van informatiebeveiliging. Omdat er meerdere criteria zijn resulteert een slechte score op het gunningscriterium over informatiebeveiliging niet tot diskwalificatie. Sterker nog, indien deze inschrijver op andere criteria zeer goed scoort kan ze de aanbesteding winnen.

Omdat je als opdrachtgever geen zekerheid verkrijgt over informatiebeveiliging bij een gunningscriterium is het niet raadzaam informatiebeveiliging alleen op te nemen op deze wijze. Je kunt natuurlijk wel combineren met geschiktheids- en/of gunningseisen, maar voorkom overlap. In de praktijk zal natuurlijk ook hier de prijs een belangrijke factor zijn. Tezamen spreek je dan van Beste PrijsKwaliteitVerhouding (BPKV).

Smaken samenvoegen

De voornoemde drie smaken zijn uitstekend met elkaar te combineren zolang je weet wat je doet; niet alle combinaties zijn logisch en leveren derhalve een smaakvol gerecht op. Ik pleit voor meer gebruik van de geschiktheidseis op het managementsysteem volgens de eisen van ISO 27001. Uiteindelijk wil je als opdrachtgever dat de inschrijver zelf verantwoordelijkheid neemt op het gebied van informatiebeveiliging. Ik ben van mening dat je dat bereikt door genoegen te nemen met een degelijk managementsysteem dat door een geaccrediteerde organisatie is gecertificeerd, eventueel aangevuld met een pentest en/of auditrapport, en de gunningseisen echt te beperken tot het noodzakelijke. Let wel, dat kunnen nog steeds heel wat eisen zijn naar gelang de complexiteit van de uitgevraagde IT-oplossing. En benut ook de mogelijkheden van een gunningscriterium.

Inkopen is een vak, net als informatiebeveiliging. Werk daarom altijd nauw samen met een inkoopadviseur en/of aanbestedingsjurist.

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

COLUMN MARTIJN

Omdenken met ransomware

Ransomware na ransomware na ransomware-zaak. Het is sinds het conflict in Oekraïne zeker niet afgenomen. Wat wel zwaar is veranderd, is de hele politieke wereld tussen en binnenin criminele cyberbendes. Een ware soapserie waar verraad, wraak en het kiezen van kanten, de cyberwereld heeft veranderd. De sancties in de 'echte' wereld hebben hier ook sterk invloed op. Ransomware-bendes die nu toch zwaar betrokken lijken te zijn bij Rusland (niemand had het gedacht…) kunnen haast geen betalingen meer ontvangen zonder onder sancties te vallen. Misschien is dat juist wel een reden waarom het aantal slachtoffers alleen maar hoger wordt. Minder opbrengst per slachtoffer, dan maar meer organisaties aanvallen. Het is voor hen ook gewoon een business natuurlijk.

Over de business van cybercriminelen weten we ondertussen steeds meer. Conti, een van de bekendste ransomware-groepen, heeft nu al meermaals een grootschalig lek gehad. Eind 2021 werd hun 'playbook', de precieze handleiding die ze volgen om een organisatie binnen te dringen en te gijzelen, publiek. Recentelijk ook veel van hun interne communicatie, de 'conti leaks'. Dat is een goudmijn om ze goed te begrijpen en moet je echt een keer lezen! We weten dat ze 100 man in dienst hebben, dat ze werktijden hanteren, hoe ze mensen aannemen, en ook hoe ze (waarschijnlijk) beïnvloed worden door de FSB. Ik ben, ondanks dat ik het al wist, onder de indruk van de mate van professionaliteit die ze hanteren.

De belangrijkste dingen die we hieruit leren? Precies de dingen die we als securitywereld al vaak genoeg roepen. Ze vallen alle technische kwetsbaarheden aan, dat wat aan jouw internet hangt, via password spraying tot en met phising campagnes.

Mijn vraag is niet hoe je jezelf hiertegen verdedigt, maar hoe je hun aanvallen stopt, of op z'n minst moeilijker maakt. Dat klinkt hetzelfde, maar het perspectief is anders! Richt je op hoe ze aanvallen, outside-in denken. Pragmatisch. Vanuit je organisatie denken en hoe je die specifieke maatregel gaat implementeren, is het inside-out. Vaak kom je dan juist een hoop drempels tegen.

Dus hoe ga je zorgen dat ze alles wat je aan het internet hebt hangen niet aanvallen? Begin eerst met onderzoeken wat daar allemaal wel niet leeft…. Nog beter, doe dat op de manier hoe aanvallers dat ook doen! Terugwerken vanaf je domeinnaam, zoeken op shodan, noem het maar op. Dat kun je zelf doen, maar je kunt ook een externe partij eens laten kijken. Laat ze maar eens de aanvaller spelen. Wat is er dan allemaal interessant, met die 'aanvallerpet' op? Alles waarmee je remote kunt inloggen, staat bovenaan de lijst.

Hetzelfde voor de password spraying aanvallen. Doe maar eens! Lastig zijn ze niet hoor. Het is net alsof een crimineel de hele dag voor je deur staat sleuteltjes te proberen. Moeilijk is het niet, wel heel effectief. Een bende van een beetje niveau zal eerst goed proberen te begrijpen hoe je accountnamen er uit zien. voorletter.achternaam@domein? voornaam.achternaam@domein? Even een uurtje op je website en LinkedIn en ze hebben waarschijnlijk een lijst die pretty darn good is. Wat doe je er dan tegen? Een tweede factor voor inloggen, overal. Of als je helemaal trendy bent, gewoon zonder wachtwoord! Dan blijft een lastige over, de phishingaanvallen. Het is niet voor niets dat dit bijna een aparte criminele industrie is, want ze zijn zeer effectief. Net als elke wapenwedloop, betekent dit dat ertegen beveiligen ook een flinke investering is. De volgende keer neem ik je mee in die wereld!

Auteurs: Lourens Dijkstra werkt als CISO bij ggz-instelling Lentis. Als organisatiepsycholoog/adviseur is hij verbonden aan het traject informatieveilig gedrag in de zorg. Martine van de Merwe werkt met haar bedrijf PrivacyLab als adviseur bewustwording/gedrag op het gebied van informatiebeveiliging en privacy bij zorginstellingen en als adviseur bij het project Informatieveilig gedrag in de zorg. Lourens en Martine zijn auteurs van de Wegwijzer. *Aan de slag met informatieveilig gedrag* (www.informatieveiliggedragzorg.nl).

Hoe kies je effectieve interventies voor informatieveilig gedrag?

Een gedragsaanpak in zes stappen

Wereldwijd wordt er 700 miljoen dollar besteed aan e-learning interventies op het gebied van informatieveiligheid (1). Maar zorgen deze interventies er ook voor dat medewerkers zich informatieveiliger gaan gedragen? Leidt bewustwording ook daadwerkelijk tot informatieveilig gedrag?

Bewustwording leidt niet altijd tot informatieveilig gedrag, blijkt uit het artikel Human Factors (2) in iB-Magazine 1 2022. Zeker in 31% van de gevallen blijken kennis of bewustzijn wel aanwezig, maar leiden niet altijd tot het juiste gedrag. Dit roept de vraag op of we wel de juiste interventies kiezen en, minstens zo belangrijk, of we weten wat het effect van deze interventies is?

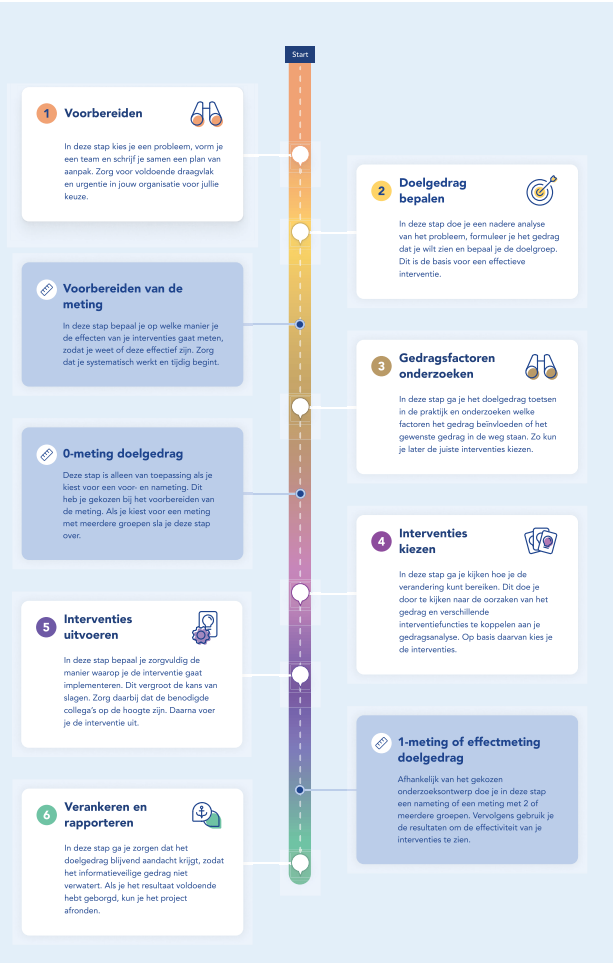
Onder de vlag van ICTU ontwikkelden we als expertteam een methode waarmee zorgorganisaties in zes stappen effectieve gedragsinterventies kunnen uitvoeren om informatieveiligheid te verbeteren.

Op gevoel

Als informatieveiligheidsprofessionals gaan we er vaak van uit dat de mens een rationeel wezen is. Dat medewerkers hun gedrag aanpassen als we vertellen wat de bedoeling is, bijvoorbeeld via e-mail of presentaties. Helaas: iets weten, is niet automatisch dat ook doen. Uit eigen onderzoek ontdekte ons projectteam dat er een overvloed bestaat aan interventies om de informatieveiligheid te verhogen, waaruit vaak op gevoel wordt gekozen. Risico is dat de gekozen interventie niet aansluit op wat nodig is. Of erger nog: een averechts effect heeft. De kosten voor interventies kunnen hoog zijn: niet alleen tijd en geld van de security officer, maar ook kostbare tijd en energie van medewerkers. Terwijl over de effectiviteit van deze interventies weinig bekend is.

Bewezen effectief

Bij de start van het project Informatieveilig gedrag in de Zorg gaven de Brancheorganisaties Zorg (BoZ) en het ministerie van VWS de opdracht om een gedragsaanpak te ontwikkelen, waarmee zorgorganisaties zelf hun informatieveiligheidsproblemen konden oplossen met effectieve interventies op maat. Het was nadrukkelijk niet de bedoeling om met generieke interventies te komen. Het projectteam maakte gebruik van het gedragsveranderingswiel van Susan Michie (3). Deze is opgesteld vanuit negentien veranderingsraamwerken en biedt hiermee een samenvatting van de meest actuele kennis op het gebied van gedragsverandering. Om dit voor de praktijk van zorgorganisaties toepasbaar te maken, deed het projectteam pilots in verschillende zorgbranches. In iedere pilot hielp een multidisciplinair kernteam van deskundigen de organisatie om oplossingen voor informatieveiligheidsproblemen te vinden. Zo scherpte het projectteam de methode steeds verder aan op basis van de zorgpraktijk en ontwikkelde het een stappenplan: de Wegwijzer *Aan de slag met informatieveilig gedrag.*



Figuur 1 - Stappenplan de Wegwijzer 'Aan de slag met informatieveilig gedrag'.

Project

Het project Informatieveilig gedrag in de zorg werd van 2019 tot begin 2022, in opdracht van de Brancheorganisaties Zorg (BoZ) en het ministerie van VWS, uitgevoerd door stichting ICTU. Het project is nu ondergebracht bij ECP, Platform voor de Informatiesamenleving, ook bekend van Alert Online. Alle producten zijn vrij te gebruiken. De producten zijn ontwikkeld voor de zorg, maar zijn breder toepasbaar in diverse sectoren.

We doorlopen de stappen uit het model en laten daarbij steeds zien hoe het in de praktijk is uitgevoerd bij de pilot-organisatie Lentis. Lentis biedt geestelijke gezondheidszorg, forensische zorg en ouderenzorg in Noord-Nederland. Lentis heeft meer dan 4000 medewerkers.

Stap 1 Voorbereiding

Een goede voorbereiding is het halve werk. In deze stap kies je het meest urgente informatieveiligheidsprobleem met een gedragscomponent waar je mee aan de slag gaat. Werk het probleem uit in gedragstermen. Wat voor gedrag laten medewerkers onvoldoende zien? Kies je multidisciplinaire kernteam afhankelijk van je probleem. Denk hierbij aan de volgende rollen: medewerker uit de doelgroep, CISO, FG, leidinggevende, functioneel beheerder, communicatieadviseur, etc. Met het kernteam stel je de eerste versie van het plan van aanpak op en overleg je wekelijks om de voortgang af te stemmen. Zorg voor commitment van de top, door ze als 'opdrachtgever' direct bij de start te betrekken en houd ze gedurende het traject goed op de hoogte. Zo ben je verzekerd van prioriteit en financiering voor je traject. Maak in deze fase ook alvast een 'roadmap' van de verschillende stappen in het traject en wie je wanneer en voor hoeveel tijd nodig denkt te hebben. Bedenk ook alvast wie eigenaar wordt van het vervolg van het project.

Wegwijzer in de praktijk

Bij Lentis zijn we door een minor afwijking uit de audit NEN7510 aan de slag gegaan met het issue dat we niet altijd konden verantwoorden waarom medewerkers gebruikmaakten van de buiten-autorisatie in het Elektronisch Patiënten Dossier (EPD). Indien er geen behandelrelatie is met de patiënt dan kan de behandelaar gebruikmaken van een noodprocedure: de buiten-autorisatie. Met deze opdracht vanuit de Raad van Bestuur zijn we aan de slag gegaan met een team bestaande uit een teamleider/behandelaar, een secretaresse, een CISO, een functioneel beheerder, een BI-adviseur en een FG. Wekelijks hadden we een digitaal overleg waarin de analyses werden gedaan en de voortgang van het traject werd gemonitord.

Stap 2 Doelgedrag bepalen

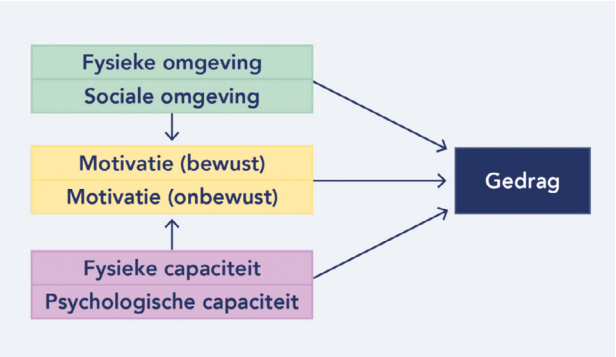
Bij deze stap bepaal je samen met het kernteam het doelgedrag. Dit is de omschrijving van het gedrag dat je bij medewerkers zou willen zien om het probleem op te lossen of te verminderen. Bepaal om welke groep medewerkers het gaat en waar en wanneer je het doelgedrag wil zien. Vaak zijn er meerdere gedragsalternatieven. Kies het gedrag met de meeste impact op het probleem en waarvan de kans het grootst is dat medewerkers het gaan vertonen.

Wegwijzer in de praktijk

Bij Lentis is gekozen voor het doelgedrag: medewerkers moeten het gebruik van het EPD via de buiten-autorisatie altijd verantwoorden. Als doelgroep kozen we voor de behandelaren. Bij verandering van hun gedrag zouden we de grootste impact realiseren.

Stap 3 Gedragsfactoren onderzoeken

Je gaat het gedrag in de praktijk checken. Kijk op locatie en ga in gesprek met de doelgroep. Start met een open blik, ben nieuwsgierig, probeer het gedrag ook zelf eens uit in de werkomgeving van de doelgroep. Probeer te analyseren welke factoren wellicht het doelgedrag stimuleren en welke factoren het gedrag belemmeren.



Figuur 2 - Informatieveilig gedrag zorg volgens het COM-B model.

Bij de gedragsanalyse kun je gebruikmaken van het COM-B-model dat ervan uitgaat dat er drie factoren (Capability, Opportunity en Motivation) van invloed zijn op het gedrag (Behaviour). Per factor onderscheiden we twee typen en zo komen we tot zes categorieën: fysieke omgeving, sociale omgeving, motivatie (bewust), motivatie (onbewust), fysieke capaciteit en psychologische capaciteit. In de gratis Wegwijzer vind je een mooie uitwerking van de factoren, welke vragen je kunt stellen en hoe de factoren te analyseren en te prioriteren.

Wegwijzer in de praktijk

In het kernteam hebben we aan de hand van werkbladen een voorlopige gedragsanalyse gemaakt en op basis hiervan een interview-opzet gemaakt. We hebben een tiental behandelaren/teamleiders geïnterviewd en de rode draad uit de uitkomsten verwerkt in de COM-B analyse.

Voorbeeld

Bij een zorgorganisatie verantwoorden medewerkers onvoldoende het gebruik van de buitenautorisatie (noodknop) in het Elektronisch Patiëntendossier (EPD). Uit de interviews kwamen de volgende uitkomsten per factor naar voren:

Figuur 3 - Informatieveilig gedrag zorg analyse COM-B model.

Een paar in onze ogen opvallende uitkomsten waren dat de behandelaren de buiten-autorisatie niet als noodprocedure bestempelden, maar als een van de mogelijkheden om snel in het EPD te komen. Er was weinig kennis over richtlijnen voor het gebruik van de buiten-autorisaties. In het teamoverleg werd door de teamleider weinig aandacht besteed aan het gebruik van de buiten-autorisatie. Aan de andere kant gaven behandelaren aan intrinsiek gemotiveerd te zijn om het juist te doen. Deze uitkomsten gaven goede input om na te denken over mogelijke interventies om het gedrag te kunnen beïnvloeden.

Nulmeting

In deze stap ga je bepalen op welke manier je de effecten van je interventies op het doelgedrag gaat meten. Zo weet je zeker of je de juiste interventies hebt gekozen om het gedrag te beïnvloeden. Een meting kan bijvoorbeeld bestaan uit observaties op de afdeling, het analyseren van de logging uit een systeem of een vragenlijst die medewerkers invullen. Is het belangrijk om een zuivere meting uit te voeren, overweeg dan om een controlegroep in te zetten die de interventies niet ondergaat.

Wegwijzer in de praktijk

Bij een eerste handmatige meting bleek uit de logging dat In 14% van de gevallen het gebruik van de buiten-autorisatie niet juist door de medewerkers werd verantwoord. Om de voortgang van de gedragsverandering geautomatiseerd te kunnen volgen, is er door de afdeling Business Intelligence (BI) een dashboard gemaakt in applicatie Zorgcontrol. Zo konden we als team realtime goede analyses maken van het gedrag.

Stap 4 interventies kiezen

Pas bij deze stap ga je nadenken over mogelijke gedragsinterventies. Met de uitkomsten van de gedragsanalyse op zak ga je met je team brainstormen over mogelijke gedragsinterventies. Kies met behulp van een aantal criteria, zoals bijvoorbeeld kosten, tijdsinzet en met behulp van interventiefuncties (zie Wegwijzer p. 51) de juiste interventies die het doelgedrag bevorderen. Vaak is het handig om in deze fase ook een communicatieadviseur mee te laten denken in het kernteam voor de juiste uitvoering van de interventies.

Wegwijzer in de praktijk

Uit de brainstorm kwamen een twintigtal mogelijke interventies. Deze interventies hebben we op basis van de gedragsanalyse gerangschikt en geprioriteerd: quick wins, hoge impact en lage kosten.

De volgende interventies zijn gekozen:

- aandacht voor het onderwerp in werkoverleggen om ervaringen te delen en processen te verbeteren;
- sturing door teamleiders;
- medewerkers informeren om het belang aan te geven van de juiste verantwoording.

Relatie met ISO 27001/NEN 7510

De kern van ISO 27001/NEN 7510 is dat je zelf vaststelt welke maatregelen noodzakelijk zijn en dat je vervolgens meet of deze effectief werken. Bij bewustwordingsactiviteiten worden nu vaak de inspanningen gemeten: hoeveel mensen hebben de e-learning gevolgd; hoeveel nieuwsbrieven zijn verspreid? Ook auditoren nemen hiermee vaak genoegen. Het gebruik van de Wegwijzer stelt je in staat effectmetingen te doen: is het gedrag veranderd en is de informatie nu beter beschermd?

Stap 5 Interventies uitvoeren

Om de kans van slagen van de interventies te vergroten, bepaal je zorgvuldig de manier waarop je de interventies uitvoert. Denk hierbij aan 'tone of voice', namens wie wordt de boodschap verspreid, wat werkt goed binnen de organisatie en wat is het juiste moment en de juiste volgorde. Wijs per gedragsinterventie een actiehouder aan die verantwoordelijk is voor de uitvoering.

Wegwijzer in de praktijk

Bij Lentis werd periodiek een infographic geplaatst op het intranet om de medewerkers te informeren over het belang van het verantwoorden. Hierin werd ook de voortgang getoond. Ook verscheen een nieuwe richtlijn die werd besproken in het werkoverleg. Aan de hand hiervan werden er verbeteringen doorgevoerd in het proces van autoriseren. We ontwikkelden een dashboard voor leidinggevenden, zodat ze kunnen sturen op de cijfers van de buiten-autorisatie binnen het eigen team. Ook werden de cijfers meegenomen in de kwartaalrapportage voor de Raad van Bestuur.

Stap meting: 1-meting/effectmeting doelgedrag

Om er zeker van te zijn of je effectieve interventies hebt uitgevoerd, voer je een vervolgmeting uit. Deze 1-meting dient vergelijkbaar uitgevoerd te worden als de 0-meting. De vergelijking van de resultaten van je metingen geven je inzicht in de effectiviteit van de interventies. Bij een goed resultaat kun je je uitgaven en inzet verantwoorden aan de organisatie en aantonen dat je interventies echt hebben geleid tot informatieveiliger gedrag.
Mocht je echter constateren dat de interventies een gering of weinig effect hebben, dan is dat ook waardevolle informatie. Dan ga je terug in het proces en onderzoek je of je andere interventies zou moeten kiezen.

Wegwijzer in de praktijk

Lentis kan nu realtime monitoren wat het effect is van de interventies op het gedrag (zie figuur Resultateninterventies), maar ook hoe het gedrag zich verder ontwikkelt.

Figuur 4 - Resultaten gedragsmetingen per maand (jan. 2020-aug. 2021).

Tips

Tip 1 Vraag je doelgroep eens waarom ze doen wat ze doen. Dit kan snel belangrijke inzichten opleveren!
Tip 2 Wees niet te ambitieus: maak het klein. Juist in samen kleine stappen zetten, schuilt het succes.
Tip 3 Probeer niet alles alleen op te lossen, maar werk samen in een multidisciplinair projectteam.

In 2020 zat Lentis op een gemiddelde van 14,3% van de medewerkers die niet het gewenste doelgedrag vertoonden. In 2021 zien we het gemiddelde teruggaan naar 9,9%. Echter, er is nog werk aan de winkel omdat onze ambitie 5% is.

Stap 6 Verankering en rapporteren

Uiteraard is het leuk om effect te zien op het gedrag van de medewerkers. Gedurende het project is er veel aandacht en inzet voor het onderwerp. Het wordt pas echt interessant als we kunnen spreken over een blijvende gedragsverandering. Wil je dat de getoonde verandering het nieuwe normaal wordt, dan moet er structureel aandacht aan worden besteed. Daarvoor moeten de uitkomsten van het project worden overgedragen aan het lijnmanagement en zo worden verankerd binnen de organisatie. Zorg voor een heldere adviesrapportage en draag zorg voor een goede overdracht. Hiervoor kun je gebruikmaken van het 'verankeringsdocument' uit de Wegwijzer (p.66).

Figuur 5 - Resultaten gedragsmetingen per maand (jan. 2020-jan. 2022).

Wegwijzer in de praktijk

Binnen Lentis was de verankering een lastig onderdeel. Bij de start van het traject hebben we als kernteam hier onvoldoende bij stilgestaan. Na afronding van het project was er minder aandacht voor het onderwerp. We zagen dit terug in de monitor die een lichte stijging liet zien. Inmiddels zijn we drukdoende om de kpi's van infor-

matieveiligheid en privacy te laten opnemen in de planning- en control cyclus van het management. Zo is blijvende aandacht en opvolging verzekerd.

Afsluitend: Wees effectief

Samengevat kunnen we stellen dat het effect van gekozen interventies vaak onbekend is. Door deze methode te gebruiken, stijgt de informatieveiligheid, omdat de gekozen interventies wél effectief zijn. Gebrek aan kennis is vaak niet het probleem. De interventies richten zich op de werkelijke redenen waarom medewerkers het doelgedrag niet vertonen. Daarnaast verspil je geen tijd en energie van medewerkers met niet-effectieve interventies.

Als je nieuwsgierig bent naar waarom mensen doen wat ze doen, leer je veel. Gebruik die inzichten, én je metingen, om de risico's uit gedrag te beheersen.

Wil je voortaan ook anders te werk gaan? De Wegwijzer is ontwikkeld voor de zorg, maar ook prima toepasbaar in andere sectoren. Op de website www.informatieveiliggedragzorg.nl vind je alle stappen met uitleg, voorbeelden en handige werkbladen om direct zelf te starten. Voor zorgorganisaties biedt ECP kosteloos ondersteuning bij het werken aan informatieveilig gedrag met een wekelijks spreekuur, webinars, workshops en een masterclass. Het aanbod staat vermeld op de website.

Referenties

(1) Gartner Report 2020 World wide turnover computer based training

(2) Artikel Human Factors: de kloof tussen awareness en gedrag, Inge Wetzer, deel 2 van drieluik, Informatiebeveiliging Magazine (Jaargang 22 2022, editie 1)

(3) Wegwijzer Aan de slag met informatieveilig gedrag www.informatieveiliggedragzorg.nl

(4) Michie, S., Atkins, L. en West, R., 2018. Het gedragsveranderingswiel 8 stappen naar succesvolle interventies. Amsterdam: Amsterdam University Press.

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.

De sociaal-maatschappelijke orde en informatiebeveiliging

De Europese Unie en de Verenigde Staten staan regelmatig tegenover elkaar, ook al zijn zij in wezen gelijkgezinde economische en technische partners. Gelijkgezind, omdat beide entiteiten uitgaan van democratische principes en derhalve van economische vrijheid, gekoppeld aan vertrouwen in technologische vooruitgang. En toch… op één belangrijk punt verschillen zij als dag en nacht.

In de Verenigde Staten gelooft men in het bedrijfsleven en de absolute vrijheid voor de ondernemer. De staat is slechts het noodzakelijk kwaad om oorlog buiten de deur te houden en een ambassadeur uit te zenden om de eigen belangen te verdedigen en uit te bouwen. Europese landen hebben veelal een transparante en integrale samenleving, waarbij de sociaal-maatschappelijke orde bewaakt wordt door een voldoende krachtige overheid met gelijktijdige, begrensde vrijheid voor ondernemers.

Naast de basis van de samenleving die door overheden zijn gebouwd, bestaat er ook marktwerking. De macht van het bedrijfsleven in onze huidige tijd is groot, wat betekent dat de directies en leiding van deze bedrijven invloed hebben op onze samenleving. Digitale autonomie is een steeds belangrijker begrip aan het worden. Zo schreef de EU al (1) dat strategische autonomie voor individuele landen en de EU als geheel heroverwogen dient te worden in ons huidige digitale tijdperk. Wat betekent dit voor de informatiebeveiliging en ons vak?

Wie dient wie? – Chris de Vries

Er zijn EU/nationale wetten, (op)gevolgd door 'alle' betrokkenen in Europa: de overheden zelf, ideële tot aan bedrijfsorganisaties toe alsook de burger, het individu; u en ik dus. Er zijn wetshandhavers, die de belangen bewaken, bij veronachtzaming leidt dat theoretisch tot boetes/straffen.

Eén praktijkvoorbeeld: de NAM verloor in 2021 data aan criminelen m.b.t. 19.000 Groningers, zoals eind 2020 onnodig gegevens van duizenden Groningers geleverd zijn aan het Ministerie van Economische Zaken (dit niet meldende aan de AP, noch wetende welke gegevens in dat bestand hebben gestaan!) (2). De Nederlandse Aardolie Maatschappij (3) dus de overheid? Nee, want het betreft Exxon Mobil en Shell (net vertrokken uit Nederland), die zich onttrekken aan de Groningse compensatievergoedingen, maar wellicht ook aan 'reclaim' investeringen na beëindiging van hun olie- en gaswinningsactiviteiten, zie voor 'reclaim' de 'Corporate Finance' handboeken aan het eind van de 20e eeuw (4). Wordt er dus gehandhaafd? Het

Chris de Vries | Fook Hwa Tan | Lilian Knippenberg

lijkt er eerder op dat de nationale overheden de multinational(s) dienen. Een ander initiatief; de 'European Data Protection Supervisor (EDPS)' start een sociale-netwerken-pilot: 'EU Voice & EU Video' (5). Uitgangspunt: 'Volgens de privacytoezichthouder wordt data van de platforms niet gedeeld buiten de EU en de Europese Economische Ruimte, zijn er geen advertenties op het platform en worden gebruikers niet geprofileerd.' En dat leidt op termijn tot: 'alternatieve social-media-platforms ... die prioriteit geven aan individuen en hun recht op privacy en gegevensbescherming'. Dit is andere koek vanuit de supranationale entiteit, de Europese Unie, die haar burgers dient. Dit doet dus Europa voor u en mij en in toenemende mate gericht op een ICT-autonomie in de wereld.

Vrijheid en controle moeten samen! – Fook Hwa Tan

Met alle maatschappelijke issues in de afgelopen jaren zien we dat overheden en burgers niet helemaal meer weten wat de normale gang van zaken is. Na een pandemie die alles en iedereen heeft beïnvloed en mogelijk heeft veranderd, een economie met hoge inflatie die probeert te herstellen en een oorlog in Oekraïne waar sancties en verlies van productiecapaciteit nog vele na-effecten zullen hebben. Wat betekent dit voor informatiebeveiliging? Vrijheid is een groot goed in het Westen. Het recht om zelf te mogen kiezen en te kiezen hoe je je leven in wil richten wordt met de paplepel ingegoten. Tijdens deze grote gebeurtenissen wordt echter gevraagd aan een grotere macht als de overheid om in te grijpen en de controle van het leven tijdelijk over te nemen omdat het individu te weinig macht heeft om verandering teweeg te brengen. Het is dan wel de bedoeling dat, nadat de overheid adequaat heeft ingegrepen, de vrijheid wordt hersteld. Wanneer echter de overheid controle van het leven voor een grote menigte overneemt, is het dan ook belangrijk dat ze transparant opereert. Dit betekent, dat burgers kunnen controleren waarom de overheid bepaalde beslissingen heeft genomen en als zij dat niet goed heeft gedaan, dat aan de kaak te stellen. Als dit daadwerkelijk zo geregeld is, dan zou ons vakgebied ervoor moeten zorgen dat de flow van informatie tussen overheid en burger op een adequaat veilige wijze plaatsvindt. Dit betekent dan ook, dat indien informatie niet vrij en veilig kan bewegen tussen overheid en maatschappij we vrijheid en controle niet samen kunnen laten bestaan.

Pleit voor weerbaarheid – Lilian Knippenberg

Het woord 'techreus' is wat mij betreft een mooie suggestie voor het 'woord van het jaar' verkiezing die de Van Dale ieder jaar houdt. Waar tot voor kort nog niemand van het woord gehoord had, begint dat in rap tempo te veranderen. Zeker aangezien in maart bekend werd dat de EU een akkoord heeft bereikt over strengere regels voor aanbieders van online diensten in de Digital Markets Act (6). Sancties tegen techreuzen als Google en Facebook moeten hiermee mogelijk worden, maar wellicht kan dit ook deuren openen voor nieuwe aanbieders. Uit onderzoek van datacenter Bit (7) bleek in februari van dit jaar dat 62% van de IT beslissers bang is voor de groeiende macht van techreuzen. Nog saillanter is dat een ruim aandeel vertrouwen zou hebben in een Europese cloudoplossing ten opzichte van een aanbieder uit een ander deel van de wereld. Ook interessant in dat kader is het advies dat de Cyber Security Raad (CSR) in mei 2021 uitbracht over digitale autonomie en cybersecurity (8). Hierin werd zelfs het woord 'techkolonisatie' gebruikt. Waar we vroeger vooral de voordelen zagen van de innovatie van Silicon Valley, zien we nu ook steeds meer de schaduwzijde daarvan. Het wordt de uitdaging van de komende tijd om zowel de voordelen van innovatie te behouden, maar ook om onze privacy daarin leidend te laten zijn. Ik geloof dat daarvoor mensen zoals wij nodig zijn: professionals die kunnen duiden welke risico's onze organisatie loopt als gekozen wordt voor applicatie A of B, die adequate screeningen en awareness-campagnes organiseren voor collega's en op nog veel meer manieren meebouwen aan een informatieveiliger Nederland. Veiligheid is daarbij een lastig begrip (je bent nooit 100% veilig), daarom pleit ik graag voor weerbaarheid. Zorg voor een goede respons op incidenten, oefen je plannen en neem mensen mee in het belang van informatieveiligheid en de maatregelen die je neemt. Samen komen we er wel!

Referenties

(1) Rethinking strategic autonomy in the digital age - Publications Office of the EU (europa.eu)

(2) https://tweakers.net/nieuws/196098/nam-stuurde-eind-2020-gegevens-van-meer-nederlanders-dan-nodig-naar-ministerie.html?utm_source=nieuwsbrief&utm_medium=email&utm_campaign=twk_nieuwsbrief

(3) Zie voor een juridische kijk op de NAM en haar aandeelhouders een artikel in de serie 'Aardbevingen in Groningen en het vermogensrecht' van mr.dr. E.C.A. Nass, bron: Maandblad voor Vermogensrecht, aflevering 4, 2020 – URL: http://openaccessadvocate.tijdschriften.budh.nl/tijdschrift/maandbladvermogensrecht/2020/4/MvV_1574-5767_2020_030_004_002

(4) Principles of corporate finance, fourth edition – Brealey & Myers, 1991

(5) https://tweakers.net/nieuws/196124/europese-privacytoezichthouder-start-pilot-met-eigen-sociale-netwerken.html?utm_source=nieuwsbrief&utm_medium=email&utm_campaign=twk_nieuwsbrief

(6) https://nos.nl/artikel/2422563-akkoord-over-europese-wetgeving-om-macht-techreuzen-te-beteugelen

(7) https://www.bit.nl/news/3124/88/Zes-op-de-tien-IT-beslissers-bang-voor-groeiende-macht-techreuzen

(8) https://www.cybersecurityraad.nl/documenten/adviezen/2021/05/14/csr-advies-nederlandse-digitale-autonomie-en-cybersecurity---csr-advies-2021-nr.-3

COLUMN LEX

De herrijzing van de QR-code

Ten tijde van de COVID-19 pandemie werd de wereld geconfronteerd met een noodzaak om contacten te vermijden. Eerst strikt met sluiting, maar uiteindelijk mochten we weer activiteiten ondernemen. De QR-code bleek toen heel handig. Een klein symbooltje dat snel alle nodige informatie kan verstrekken, zoals bezoekersregistratie, een menu, andere aanwijzingen of achtergrondinformatie. Vervolgens kwam de CoronaCheck app. Een app die zo rondom de QR-code was gebouwd dat het app-logo een QR-code is.

Tien jaar geleden was dat wel anders. Toen ik nog hoofdredacteur was probeerde ik referenties bij artikelen te voorzien van een QR-code. Ze werden niet gebruikt. Ze waren onbetrouwbaar op langere termijn, want de geldigheid kon niet gegarandeerd worden. Dit heeft gemaakt dat we het gebruik van QR-codes stopten.

Maar de QR-code is weer helemaal terug, omdat camera apps ze nu standaard herkennen. Omdat het handig was voor de aanrakingsvrije wereld die we kregen weet iedereen nu ook wat een QR-code is en hoe die eruit ziet, of je nu voor- of tegenstander was van de coronamaatregelen. Dit gebruik is een functioneel goed en veilig gebruik: scannen gebeurt in een herkenbare situatie, er is een zorgvuldig gedocumenteerd proces van een betrouwbare bron en je gebruikt een vertrouwde en specifieke app om dit te doen. Denk ook aan de QR-codes in de DigiD app, bankieren apps en authenticator apps.

Er is nog een reden voor de nieuwe populariteit, vanwege een privacy succes op een ander vlak: de browserfabrikanten zijn er eindelijk in geslaagd om third-party tracking tegen te gaan. Dit maakt het moeilijker voor websites om gedragsinformatie over hun bezoekers te verzamelen. Daar is een weg omheen gevonden: de 'dynamische' QR-code. Dit is een QR-code die zich met speciale inkt kan aanpassen aan de omstandigheden waarin die bekeken wordt. (Pauze…) Nee, het is al 1 april geweest.

Een dynamische QR-code is net zo statisch als een traditionele QR-code, maar verwijst naar een reclamebedrijf/tracking service. Deze toont een reclameboodschap of verwijst hier naar door en houdt klik-statistieken bij. Omdat dit een directe, first-party interactie is via de browser, kunnen ze ook volledig de browser-attributen van de bezoeker raadplegen en dus als vanouds tracken. Het aantal leveranciers van deze diensten is groeiende. Ongemerkt word je blootgesteld aan een groter aanbod van QR-codes. Als je deze scant, weet dan dat je als vanouds getrackt wordt zonder dat de nieuwe spelregels overtreden worden. En als over een jaar of wat de eerste faillissementen in deze branche zich aandienen, heb je tóch weer ongeldige, hijackbare QR-codes… Al met al, nieuwe veiligheidssores.

En als uitsmijter, in het kader van 'What could possibly go wrong?': de collectebus wordt vervangen door een collectant met een QR-code. De potentiële gever, de persoon die de deur opent, zal geconfronteerd worden met deze nieuwe mogelijkheid. Hoe geïnformeerd zal die zijn over het betaalproces, hoe het uit te voeren en wat te controleren. Het is een heel ander proces met een heel ander risicoprofiel. Er moet een blind vertrouwen gesteld worden in de instructie van de collectant, terwijl we mensen juist proberen te leren dat mensen die onverwachts contact met je zoeken en om een financiële transactie vragen juist gewantrouwd moeten worden.

Bij de traditionele collecte met contant geld weet de gever duidelijk wat zijn impact is: het bedrag dat hij geeft. Vertrouw je de collectant niet, dan kun je om identificatie vragen. Mocht het desondanks toch een zwendelaar geweest zijn, ben je netto niets meer kwijt dan het giftbedrag, waar je emotioneel toch al afstand van had genomen. De impact van een QR-code en wat social engineering met eventueel wat kwaadaardige cybertechniek kan potentieel veel hoger zijn, tot aan opnamelimieten of erger.

De collecterende organisaties en de banken zullen duidelijke informatiecampagnes moeten aanbieden om mensen bewust te maken van het proces en de controlepunten. Ik vraag me af hoe snel deze wijze van collecteren breed geaccepteerd zal worden en hoe snel hier intelligente aanvallen op bedacht worden.

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

15 PvIB reconnect in cyber security

COLOFON

iB is het huisorgaan van het Platform Informatiebeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

HOOFDREDACTEUR
Nicole van Deursen

REDACTIE
Tom Bakker
Bianca Brooijmans
Maarten Hartsuijker
Lilian Knippenberg
Rachel Marbus
Fook Hwa Tan
Ard Ruiter
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, Raalte

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

ADVANCE YOUR CAREER WITH SECURITY IN 2022

CSA - Certified SOC Analyst
GSEC - Giac Security Essentials
GPEN - Giac Penetration Tester
EDRP - Disaster Recovery Professional
EHF - Ethical Hacking Foundation
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v11
CPENT - Certified Penetration Testing Professional

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