INFORMATIEBEVEILIGING
MAGAZINE

"We'll never guess her password."

- Interview: Bart Jacobs en Roelof Meijer over authenticatieapp IRMA: 'We hoeven niet alles te doen zoals Silicon Valley het voorschrijft'
- Drieluik over cyberveilig gedrag. Deel 1: Het begint met bewustwording
- Column: Regeldrift en de zucht naar ethiek

JAARGANG 21 - 2021 - EDITIE 6

Bijna jarig

September 2022

We zijn bijna jarig en vieren groots, feestelijk en gezellig ons derde lustrum.

PvIB
Platform voor InformatieBeveiliging

Humor

Nicole van Deursen

Aan het einde van het jaar lijkt het vaak alsof we druk zijn met te veel verschillende dingen. Ik zie het ook in deze uitgave, we vliegen van een onderwerp als ransomware naar AI en van crisisoefening naar honeypots. Intussen moeten we onze medemensen blijven stimuleren om verantwoordelijk om te gaan met ICT-middelen en moeten we ze enthousiast maken voor onze regels en adviezen. Maar hoe blijven we zelf enthousiast als de druk hoog is en juist de feestdagen vaak worden overschaduwd door incidenten?

Humor is een goed wapen tegen stress en beroepshumor versterkt zelfs de onderliggende band van collega's. Humor is vaak gebaseerd op ellende, en dat is ook terug te zien in cartoons, gedichten, en grappen die met ons vak te maken hebben. Het gedicht rechts, van Kenn Nesbitt past wel bij een Nederlandse decembermaand. Ik zie voor me dat je je collega's of familie een passwordmanager cadeau geeft, met een chocoladeletter P erbij en dit gedicht. Ik wens jullie veilige feestdagen toe.

Nicole

I made a new password
That no one could guess.
It's long and confusing
And truly a mess.
It has random letters
and numbers galore,
with dozens of symbols
and spaces and more.
My password is perfect,
completely secure,
and no one will break it;
of that I am sure.
It's flawless and foolproof.
I don't have a doubt.
But, whoops! I forgot it
and now I'm locked out.

— Kenn Nesbitt
(https://twitter.com/poetry4kids)

IN DIT NUMMER

03 Voorwoord – Humor
04 Interview SIDN-directeur Roelof Meijer – 'We hoeven niet alles te doen zoals Silicon Valley het voorschrijft'
08 De onmeetbare impact van ransomware
10 Security podcasts
12 'Het is niet mijn verantwoordelijkheid'
17 Column Privacy – Regeldrift en de zucht naar ethiek
18 Geëmuleerde honeypots in de strijd tegen hackers
21 AI, Max! (deel 3 van 3)
26 Het begint met bewustwording
30 Blog – Wat ik weet uit de wijnkelder
32 Het NIST CyberSecurity Framework als kans?
34 Overheidsbrede cyberoefening
36 Achter Het Nieuws – Artificial Intelligence een nieuwe bedreiging?
38 Jaaroverzicht artikelen 2021

Auteurs: Tom Bakker is redactielid van iB-Magazine. Tom is bereikbaar via tombakker@pvib.nl. Sandra Kagie is freelance tekstschrijver (Sanscript tekstproducties). Sandra is bereikbaar via info@sanscriptproducties.nl.

INTERVIEW

Geestelijk vader Bart Jacobs en SIDN-directeur Roelof Meijer over authenticatieapp IRMA:

‘We hoeven niet alles te doen zoals Silicon Valley het voorschrijft’

Je voor het minste of geringste moeten identificeren met je ID-bewijs, een kopie van je paspoort achterlaten om een auto te kunnen huren of een uitgebreid persoonlijk profiel aan moeten maken op een website voordat je kunt inloggen. Bart Jacobs, hoogleraar Security, Privacy en Identity aan de Radboud Universiteit in Nijmegen vindt het van de gekke. Geef nooit meer persoonsgegevens (attributen) prijs dan strikt noodzakelijk, is zijn devies.

Laat dit dan ook precies het principe zijn achter de door hem ontwikkelde app IRMA, 'I Reveal My Attributes'. Een app waarmee je in zijn woorden 'veilig bewijst wie je bent, zonder dat je teveel informatie over jezelf prijsgeeft'.

'Ja, ik ben ouder dan achttien dus ik mag alcohol kopen'. Of 'ja, ik woon in dit postcodegebied dus ik mag meebeslissen en stemmen over de speeltuin in de buurt'. Dat is de informatie die je via IRMA prijsgeeft wanneer je moet aantonen dat je achttien jaar of ouder bent of dat je in een bepaalde wijk woont. Niet je exacte leeftijd, niet je complete adres en zeker niet je volledige voor- en achternaam, je geboortedatum, je nationaliteit én je foto. Gegevens die je bijvoorbeeld als jongere nu wel prijsgeeft wanneer je in de supermarkt je ID-bewijs moet laten zien omdat je een paar flesjes bier wilt kopen. Terwijl de caissière alleen maar hoeft te weten of je ouder bent dan achttien.

Stevinpremie

IRMA is één van de redenen voor de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) om de Stevinpremie - samen met de Spinozapremie de hoogste onderscheiding in de Nederlandse wetenschap - dit jaar toe te kennen aan Jacobs. Reden voor een gesprek met de geestelijk vader van de app. We spreken hem en Roelof Meijer, algemeen directeur van SIDN. De organisatie achter het .nl-domein die sinds enkele jaren nauw betrokken is bij de uitrol van IRMA.

"IRMA komt voort uit wetenschappelijk onderzoek aan de universiteit in mijn groep. Onderzoek dat al in 2008 is gestart", gaat Jacobs terug naar het prille begin. "In 2016 is IRMA vervolgens in overleg met de universiteit buiten de universiteit ondergebracht. Dit bij de stichting Privacy by Design, waarvan ik sindsdien voorzitter ben. Onbezoldigd, zeg ik daar altijd meteen bij."

Om het gebruik van IRMA van de grond te krijgen, zocht Privacy by Design samenwerking met andere partijen. Zo ontstond de samenwerking met SIDN, de beheerder van het .nl-domein. Een samenwerking die in september 2019 officieel werd bekrachtigd. Sindsdien is IRMA 'powered by SIDN'. Wat betekent dat SIDN, ook een non-profit organisatie, verantwoordelijk is voor de governance, de technische ontwikkeling en het beheer van de backbone van IRMA.

Samen proberen beide partijen het gebruik van IRMA een impuls te geven. Inmiddels beschikt SIDN dan ook over een eigen team van zo'n tien mensen om IRMA op de kaart te zetten. "Waarom we er ons als SIDN aan hebben verbonden? Omdat IRMA vooralsnog de enige oplossing voor eID in Nederland is die voldoet aan de principes die wij voorwaardelijk vinden: privacy by design, decentraal, open source en de gebruiker heeft de regie over zijn gegevens", legt Meijer uit.

Hoe werkt IRMA?

Het begint met het downloaden van de app op je smartphone en vervolgens voeg je in de app 'kaartjes' toe met daarop gegevens als je naam, je leeftijd en je adres. Kaartjes die komen van officiële instanties als de rijksoverheid of je gemeente. De gegevens zijn cryptografisch beschermd. De gegevens die jij via IRMA deelt, zijn daarmee echt, en echt van jou.

Met de IRMA-app deel je deze gegevens vervolgens met organisaties die daarom vragen. Hierbij zie je altijd wat een organisatie van je wil weten. En je bepaalt vervolgens zelf of je deze informatie wilt delen. Een proces waarbij niemand meekijkt, want je gegevens of attributen staan alléén op je smartphone en nergens anders. Ze worden dus nergens centraal opgeslagen.

Dat iemand zich kan identificeren met de telefoon van iemand anders wordt volgens de bedenkers van IRMA allereerst voorkomen door de beveiliging (biometrie of pincode) van de telefoon zelf. Daarnaast is toegang tot de IRMA-app zelf beveiligd met een 6-cijferige pincode.

Als iemand bewust zijn ontgrendelde telefoon met geopende IRMA-app aan iemand overhandigt, kan die persoon volgens de bedenkers van de app attributen verstrekken als ware hij of zij de eigenaar van de telefoon én de IRMA- gebruiker. "Analoog aan het bewust overhandigen van je ID-kaart aan een ander, zodat hij of zij daarmee bijvoorbeeld toegang krijgt tot een nachtclub of het kopen van alcohol", geven ze aan.

Meer informatie over de werking van IRMA zowel voor gebruikers als organisaties is te vinden op de website van SIDN (https://www.sidn.nl/online-identity/irma).

Bart Jacobs, hoogleraar Security, Privacy en Identity aan de Radboud Universiteit in Nijmegen

Roelof Meijer, algemeen directeur SIDN (Foto: Maarten de Kok)

‘Nog niet de grote doorbraak’

Anno 2021 hebben bijna vijftigduizend mensen IRMA op hun telefoon staan. Wereldwijd, maar toch vooral in Nederland. “Een aantal dat groeit met ongeveer honderd tot honderdvijftig per dag. Niet triviaal, maar ook nog niet de grote doorbraak. Het komt langzaam van de grond”, concludeert Jacobs.

“Langzamer dan ik had verwacht? Ach, natuurlijk had ik toen we IRMA introduceerden en vrijgaven de naïeve hoop dat iedereen het zou omarmen en zou gaan integreren”, gaat de hoogleraar verder. “Maar je hebt keyspelers nodig. Neem Marktplaats, we kennen allemaal de verhalen van fraude en oplichting via dit platform. Wanneer zij IRMA zouden gebruiken om vast te stellen wie een verkoper is door via IRMA te vragen naar je BRP (Basisregistratie Personen)-adres dan zou heel Nederland de app volgende week hebben: we zijn immers een land van sjacheraars en verkopers. Markplaats zou dat gratis kunnen doen. Het is dus een interessante vraag waarom ze dat niet doen.”

“Digitale identiteit komt het beste van de grond in gereguleerde markten”, geeft Jacobs een deel van het antwoord op die vraag. “Plekken dus waaraan vanuit de overheid eisen worden gesteld als het gaat om het vaststellen van de identiteit van iemand met wie je te maken hebt. In de zorg dus, bij de overheid zelf, in de bankensector en in de telecomsector bijvoorbeeld. Staat zoiets niet in de wet dan doen partijen het niet of maar half. Voor Markplaats is het dus een commerciële afweging: is die fraude zo erg dat we het aandurven om onze klanten extra verplichtingen op te leggen of lopen die klanten dan weg naar een ander platform?”

“Het gaat dit soort partijen uiteindelijk om de opbrengst en dan misschien maar niet helemaal kosjer”, vult Meijer aan. Toch had hij een sneller adoptie van IRMA verwacht. “Toen ik het voor het eerst zag en toen ik goed kreeg uitgelegd hoe de app werkt, dacht ik: ‘ik wil dit vanaf morgen gaan gebruiken’. Ik zou er bijvoorbeeld al mijn online aankopen mee willen doen, maar het komt moeizaam van de grond. Heel veel bedrijven vinden het nu eenmaal nog heel prettig om mijn gegevens te verzamelen en dus bieden ze niet de mogelijkheid via IRMA in te loggen op hun website”, stelt hij.

‘Vaak no-brainers’

“Ik zie zoveel toepassingen voor de app”, gaat hij verder. “En het zijn vaak echt no-brainers. Neem de nieuwe alcoholwet en de online verkoop van drank”, geeft hij als voorbeeld. “Met die nieuwe alcoholwet moet je straks als koper niet alleen online kunnen aantonen dat je achttien jaar of ouder bent – daar zou je IRMA voor kunnen gebruiken. Maar vervolgens als het pakketje bij je thuis wordt afgeleverd, moet je als ontvanger opnieuw kunnen aantonen dat je boven de achttien bent en dat jij degene bent die de bestelling heeft gedaan. Dit moet met een wettelijk ID-bewijs. Dus dan moet je aan de bezorger je paspoort of rijbewijs laten zien, terwijl

‘Wat wij met IRMA duidelijk willen maken, is: er is een keuze.’

Betrouwbaarheidsniveau IRMA?
Op de vraag op welk betrouwbaarheidsniveau van eIDAS IRMA zit, geeft Bart Jacobs aan dat dat niet zo eenvoudig te zeggen is. Het hangt af van de uitgever (issuer) van een kaartje dat je toevoegt in je app op je telefoon. Als bijvoorbeeld een commerciële partij als Albert Heijn een kaartje uitgeeft, zal dat niveau LAAG zijn, maar wanneer de rijksoverheid of een gemeente een kaartje uitgeeft, kan dat niveau HOOG zijn.
eIDAS staat voor 'Electronic Identities And Trust Services'. Met EIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen. eIDAS kent de niveaus LAAG, SUBSTANTIEEL en HOOG.

dat niet nodig is.”
“Het levert die bezorger vervolgens ook nog een hoop gedoe op, want hij moet bewijzen dat hij dit gecontroleerd heeft en hij moet dit ook op een of andere manier ergens vastleggen. Als ik PostNL was, wist ik het wel. Met IRMA is dit allemaal zoveel makkelijker.”

Hoop gericht op consument

Hoop put Meijer uit onderzoeken waaruit volgens hem blijkt dat het aantal mensen groeit dat aangeeft: ‘ik wil zelf de regie hebben over de gegevens die ik deel en ik wil zo min mogelijk gegevens delen’. Dit bewustzijn dat we toch wat voorzichtiger moeten zijn dan we de afgelopen tijd zijn geweest, ontstaat volgens hem ‘langzaam, maar zéker’. “Als gebruikers het gaan vragen, kan het veilig en makkelijk inloggen een unique selling point worden voor een webwinkel”, concludeert hij.
“We hebben als twee stichtingen geen omvangrijk marketingbudget. We moeten het vooral hebben van mond-tot-mondreclame”, haakt Jacobs in. “IRMA wordt met andere woorden niet als commercieel product in de markt gezet. Daar hebben we het ooit wel eens over gehad, maar het past gewoon niet zo heel erg bij ons als stichtingen.”
“Wat wij met IRMA duidelijk willen maken, is: er is een keuze. We hoeven niet alles te doen zoals Silicon Valley het voorschrijft vanuit hun agressieve verdienmodellen waarin publieke waarden geen rol spelen.”

Rijksoverheid ‘in verzet’

Gevraagd naar het soort organisaties dat IRMA, een open source oplossing, al heeft omarmd, ziet Jacobs vooral veel interesse en enthousiasme vanuit de zorg en vanuit lokale overheden. Terwijl de rijksoverheid in zijn woorden ‘in verzet is’. Dat het achterliggende gedachtegoed van IRMA in juni door de Europese Commissie is overgenomen voor de ontwikkeling van een nieuwe Europese identity wallet heeft wat dat laatste betreft volgens hem (nog) geen verandering gebracht. En dat verbaast hem hooglijk: “Je zou op zo’n moment verwachten dat de Nederlandse overheid opspringt en zegt wij gaan deze voorsprong qua kennis en ervaring uitnutten.”
“Maar niks daarvan”, stelt hij. “Sterker nog, onlangs werd bekend dat Nederland gaat samenwerken met Duitsland op het vlak van digitale identiteit aan een achterhaalde Duitse blockchainoplossing.” En zo laat Nederland volgens Jacobs een kans liggen om voorop te lopen in de Europese ontwikkeling van meer aandacht voor de publieke zaak in de digitale wereld. Iets waarvoor wat hem betreft in politiek Den Haag sowieso te weinig aandacht is. “Een algemeen punt van zorg”, noemt hij het.
“Te weinig aandacht en te weinig kennis ook”, vult Meijer aan. “Het is bijna een anachronisme dat in tijden van hyperdigitalisering zoals we dat de afgelopen anderhalf jaar hebben gezien, de digitale kennis in onze politieke besturen afneemt. Een heel gevaarlijke combinatie: dat kan niet zolang goed gaan, zou je zeggen.”

Auteurs: Nicole van Deursen is hoofdredacteur van iB-Magazine en bereikbaar via nicolevandeursen@pvib.nl. Fook Hwa Tan is Chief Quality Officer van Northwave en bereikbaar via fookhwa.tan@northwave-security.com.

De onmeetbare impact van ransomware

De vorige uitgave van ons magazine (iB5) opende met een interview over het Data Breach Investigations Report van Verizon. Al in de eerste paar zinnen leek te worden gezegd dat de impact van de meeste ransomware aanvallen wel meevalt. Slechts 10% van de ransomware-aanvallen leidt daadwerkelijk tot financiële schade, aldus het rapport, waarbij de mediaan van betaalde bedragen slechts $11.150 is. In deze woorden gesteld lijkt het wel alsof een organisatie de kans op schade en hoogte van mogelijke schade van ransomware kan indelen op laag-laag in hun risicoanalyse

In Nederland kijken we op een andere manier naar de situatie: bij cybersecurity bedrijven staat de telefoon roodgloeiend met hulpvragen van slachtoffers van ransomware en de overheid noemt ransomware een bedreiging voor de nationale veiligheid. Wetenschappers doen onderzoek naar het thema en er is een constante stroom van televisie-uitzendingen, artikelen, rapporten en podcasts. Wij maken ons allemaal heel druk over ransomware, maar niet alleen vanwege de hoogte van het losgeld of de financiële schade.

Als je een cyberverzekeringspolis hebt, dan valt het betalen van het ransom onder de vergoeding van de polis. Een aantal jaren terug was het voor de verzekeraar een rekensom die ze vaker hebben uitgerekend, ook in andere domeinen. Ze maken een inschatting van de kosten van de schade en herstel en op basis van de kans van uitkeren kunnen ze een premie bepalen. De laatste twee jaar merk je echter, waarschijnlijk door het hoge aantal incidenten, dat ook verzekeraars voorzichtiger zijn. Bij sommige verzekeraars kunnen organisaties binnen vitale sectoren zich al niet meer verzekeren en bij andere moet een organisatie eerst een grondig onderzoek doorstaan door een cybersecurity bedrijf voordat een polis wordt afgesloten.

De onderzoekspopulatie van het Verizon rapport (1) is wellicht wel opgewassen tegen een financiële tegenvaller, zeker als ze een verzekering hebben afgesloten. Echter, door het betalen van het losgeld ben je als organisatie natuurlijk niet ineens uit de problemen. Los van de vraag of het überhaupt lukt om daarna alles weer te ontsleutelen zijn er nog de indirecte kosten, zoals de maatschappelijke en persoonlijke impact.

Maatschappelijke en persoonlijke impact

Een beschrijving van de maatschappelijke of persoonlijke impact zie je bijna nooit terug in financiële rapporten en statistieken. Toch kan die impact enorm zijn. Het PvIB organiseerde in juni een talkshow waarin een ondernemer vertelde hoe een cyberaanval zijn bedrijf, gezondheid en gezin had geschaad. Wanneer een onderneming failliet gaat laat dat diepe sporen na bij de ondernemers, hun klanten, maar ook bij de medewerkers die hun baan verliezen, en dus ook bij hun gezinnen. Een ander voorbeeld kennen we uit Duitsland, waar een jaar geleden in Düsseldorf een vrouw kwam te overlijden omdat het dichtstbijzijnde ziekenhuis onder een aanval met ransomware lag. Daarnaast valt een hack, malware of phishing bijna altijd aan te merken als een datalek, waarbij los van de mogelijke boete er ook persoonsgegevens kunnen worden gepubliceerd of misbruikt, met alle gevolgen van dien. Bovendien kan ransomware ook gevolgen hebben in een keten waar een organisatie deel van uitmaakt. Geen kaas in de schappen van de supermarkt, veroorzaakt door ransomware in de distributieketen staat voorgoed als nationaal trauma (en als 'kaas-hack') in ons collectief geheugen gegrift. Stel je voor dat de volgende keer die keten onze drinkwatervoorziening of elektriciteit is?

Maatschappelijke impact kan ook gaan over de stress waaronder incident responders moeten opereren na een ransomware aanval. De gezondheid van deze medewerkers leidt eronder als ze wekenlang onder hoge druk moeten werken, soms dag en nacht, om de gevolgen van de aanval te verwerken. Ook het andere uiterste komt voor: medewerkers die dagenlang juist niet mogen werken en worden verzocht hun verlofdagen op te nemen. Wanneer we deze indirecte schade meenemen in de risico-afweging, dan kan deze schade zwaarder wegen dan een concreet geldbedrag.

Meten is weten?

Het gestructureerd bijhouden en delen van data over de financiële en maatschappelijke impact van ransomware ontbreekt in Nederland. Zelfs als getroffen organisaties alle gevolgen administreren, dan delen ze die niet publiekelijk. Dat levert het risico op dat organisatorische maatregelen en zelfs overheidsbeleid worden gebaseerd op onvolledige risicoanalyses, onderbuikgevoel en publieke opinie. Ook in het Verizon rapport wordt de financiële impact niet verder uitgesplitst. Het uiteindelijke losgeldbedrag is natuurlijk een meetbare kostenpost. Maar of je dat nu betaalt of niet: bijna geen enkele organisatie kan verder zonder de hulp van ingehuurde cybersecurity bedrijven, juristen, en eventueel woordvoerders en bedrijfsartsen. Vervolgens zijn er andere concrete kosten zoals de (mogelijke) boete van de Autoriteit Persoonsgegevens, gedaalde beurswaarde, schade van het niet kunnen leveren van diensten aan de klanten, de nieuw aan te schaffen bedrijfsmiddelen, overuren en overwerkte medewerkers, inhuurkrachten, de communicatie en voorlichting, en versnelde afschrijving van bedrijfsmiddelen. Deze kosten zijn meetbaar, het is alleen veel werk om het bij te houden. De vraag is ook wanneer het voorbij is: wanneer ben je klaar met het repareren van de schade? De burgemeester van de Gemeente Hof van Twente vertelde in een recente televisie-uitzending (Zembla) dat de gemeente wel twee jaar nodig zal hebben om volledig van de gevolgen van de ransomware aanval te herstellen.

In openbare bronnen zijn maar beperkte gegevens beschikbaar en die gegevens missen soms ook context. Bijvoorbeeld in de Cybersecuritymonitor 2020 van het CBS (2) lijkt het aantal aanvallen van buitenaf (waar ransomware onder valt) de laatste jaren juist af te nemen. Op basis van die beperkte data kan men geneigd zijn te denken dat het dus inderdaad allemaal wel meevalt met de incidenten en dat we steeds beter zijn voorbereid. We moeten echter niet vergeten dat deze cijfers niet het hele verhaal vertellen en dat we veel meer zouden moeten weten over het fenomeen ransomware om er conclusies aan te kunnen verbinden.

Goed meten van ransomware impact is ingewikkeld maar niet onmogelijk. Het zal veel tijd kosten, maar het levert onmisbare kennis op over het fenomeen. Het aggregeren en delen van die data draagt bij aan bewustwording voor de urgentie van preventieve maatregelen. Jaren geleden werden risicoanalyses altijd kwalitatief uitgevoerd, omdat we geen data hadden om het kwantitatief te kunnen doen. Als we er met elkaar in slagen om meer van die data wel boven tafel te krijgen kunnen we completere risicoanalyses uitvoeren, beter beleid maken en bestuurders overtuigen tot investeren in preventieve maatregelen. We hebben daarbij wel hulp nodig van data professionals, want kijken naar alleen een mediaan van financiële schade (zoals in het Verizon rapport (1)) heeft weinig betekenis gezien de complexiteit van het fenomeen. We moeten ook kijken naar context, gemiddelden, uitsplitsingen in categorieën en naar outliers in de data (die vaak juist worden uitgesloten van analyse) omdat die leerzame verhalen vertellen. Laten we elkaar blijven steunen en in openheid informeren over incidenten en de gevolgen ervan, zodat we in de toekomst allemaal weerbaarder kunnen worden.

Referenties

(1) https://www.verizon.com/business/resources/reports/dbir/

(2) https://www.cbs.nl/nl-nl/publicatie/2021/18/cybersecuritymonitor-2020

Auteur: Lilian Knippenberg is senior information security officer & plaatsvervangend CISO bij de Gemeente Den Haag. Dit artikel is op persoonlijke titel geschreven. Je kunt Lilian bereiken via LinkedIn.

Security podcasts

In de vorige editie van iB-Magazine schreef ik dat ik helemaal om ben voor de podcast. In iB5 vond je privacy podcasts, in dit artikel security podcasts. Informatieveiligheid/cybersecurity is duidelijk een populair onderwerp bij podcastmakers. Om overzicht te houden en je te helpen kiezen, vind je in dit artikel mijn persoonlijke top 6 plus een eigen groepering van podcasts.

1: Cyberhelden
Podcast van Ronald Prins, onder andere bekend als oprichter van FOX-IT. Elke donderdag komt er een nieuwe podcast online, waarin Ronald spreekt met een cybersecurity held in Nederland. In deze podcast zie je hoe ontzettend breed ons prachtige vakgebied is en wat mij betreft zijn alle afleveringen het terugluisteren waard. Elke cybersecurityheld heeft een eigen verhaal over hoe hij/zij in het vakgebied terecht is gekomen. In deze podcast staan deze verhalen centraal, waarbij Ronald ook de kritische vragen niet schuwt om erachter te komen hoe zijn gast denkt over de uitdagingen van onze tijd als security professionals. Zie cyberhelden.nl.

2: Darknet Diaries
Dit zijn de verhalen van de schaduwkant van het internet. Spannende misdaadverhalen waar de digitale en fysieke wereld elkaar ontmoeten. In elke podcast vertelt een gast zijn/haar ervaring over hacks, datalekken, cybercriminaliteit en zelfs spionage. Podcast wordt gemaakt door journalist Jack Rhysider, zie darknetdiaries.com

Zo veel podcasts! Waar kun je beginnen?
Ik houd overzicht met onderstaande door mij bedachte groepen.

Het laatste nieuws:
- SecurityTalks (NL)
- Angry Nerds (NL)
- Hack van de dam (NL)
- State of the hack (EN)
- Security Now! (EN)
- Cyber Security Today (EN)
- Paul's security weekly (EN)
- ITBros-de podcast over Identity, Security en de moderne werkplek (NL)
- Smashing Security (EN)
- Cyber Security Headlines (EN)
- SANS Storm Center (EN)
- Security This Week (EN)
- Navaio IT security nieuwsbulletin (NL)
- Unsupervised Learning (EN)

Threat Intelligence & OSINT:
- Fortiguard Threat Intelligence podcast (EN)
- Recorded Future – Inside security intelligence (EN)
- CPradio (EN)
- Breadcrumbs (EN)
- The Privacy, Security & OSINT Show (EN)
- Shadowtalk Threat intel (EN)
- Layer 8 podcast (EN)
- Symantec Cyber Security Brief Podcast (EN)

Cybercrime:
- Darknet Diaries (zie top X)
- Cybercrimeology (EN)
- Hacked (EN)
- Shadowspeak (EN)
- Cyber chill (EN)
- Malicious Life (EN)
- ThugCrowd (EN)

Met gasten in gesprek:
- Cyberhelden (NL)
- Risky business (EN)
- Blak Cyber (EN)
- De Cyberstelling (NL)
- The Hacker Next Door (EN)
- The official offensive security (EN)
- CyberspeaksLIVE (EN)
- ProteQtor Cybersecurity stories (NL)
- 7 Minute security (EN)
- SecurityVIP Podcast (EN)
- Cyber Security Inside (EN)
- Security Confidential (EN)
- Security Stories (EN)
- Career Notes (EN)
- What the hack with Adam Levin (EN)
- Getting into Infosec (EN)
- Hacker Valley Blue (EN)
- Hacker Valley Studio (EN)
- Hacker Valley Red (EN)
- Tesorion podcast (NL)

Onderwerpen per aflevering:
- Cyber Work podcast (EN)
- Open Source security podcast (EN)
- Security Science (EN)
- Eye on security (EN)
- IT Privacy and Security Weekly Update (EN)
- Security in Five Podcast (EN)
- Cyber security Sauna (EN)
- The Security Shit Show (EN)
- Wat de Hack? (NL)
- You don't need anyone (EN)
- Partners in security (NL)

Organisatorische blik:
- Oh, Behaav! (NL)
- Cyberwork (EN)
- Career Notes (EN)
- Human Factor Security (EN)
- The Cyber Security Podcast (EN)
- The social engineer podcast (EN)

Technische blik:
- Section 9 Cyber Security (EN)
- Naked security (EN)
- Security Unlocked (EN)
- The Azure Security Podcast (EN)
- Cybersecurity Architecture Podcast (EN)
- Inside Security (EN)
- Cloud Security Podcast (EN)
- Cloud security Podcast by Google (EN)
- The 443 – Security Simplified (EN)
- Purple squad security (EN)

3: The hacker next door

Deze podcast is gemaakt door een journalist die in gesprek gaat met een gast die op zijn of haar eigen manier een hacker is. Hierbij wordt het woord 'hacker' breed geïnterpreteerd en gaat het niet alleen over de hacker die op zoek gaat naar kwetsbaarheden in een systeem. Gemaakt door Jeremy N. Smith. http://hackernextdoor.com/

4: Hacked

Dit is een ontzettend goede samenwerking: een journalist (verhalenverteller) die met een technisch specialist spreekt over allerlei onderwerpen. Ieder onderwerp wordt geïntroduceerd door een verhaal dat persoonlijk aandoet en vervolgens bespreken de twee hosts wat er precies (technisch) gebeurt en welke effecten dat heeft. Gemaakt door Jordan Bloemen en Scott Francis Winder. Zie http://www.jordanbloemen.com/hacked-show

5: Wat the Hack?

Show van drie jonge security enthousiastelingen. Leuke podcast met inmiddels het tweede seizoen. Leuke gesprekken over bepaalde gasten. Eerste seizoen nog onwennig, nu een echte en professionelere podcast. Leuk dat ze aan het eind het cybermodewoord kiezen o.b.v. actualiteit. Zie watdehackpodcast.nl

6: Angrynerds

Deze podcast luistert alsof ik in de kroeg of vrijdagmiddagborrel sta met een drankje in de hand, waarbij ik een stel collega's/vakidioten een gesprek hoor voeren. Ongedwongen, veel grappen en zijwegen tussendoor, maar ook veel kennis van zaken en duiding van actuele onderwerpen. Ongeveer elke twee weken komt er een nieuwe aflevering online. Je kunt ook de video terugkijken op YouTube. Deze podcast is wel redelijk lang, anderhalf tot twee uur, maar dat deert de vakidioot niet, toch? Zie angrynerdspodcast.nl

Wellicht heb ik jou ook enthousiast gemaakt voor podcasts en weet je nu waar te beginnen. Maak vooral je eigen lijst! Disclaimer: van security podcasts zijn er zo ontzettend veel, dat ik niet alle shows heb geluisterd en vast nog shows gemist heb. De top 6 die ik deel, bevat mijn favorieten. Daarnaast probeer ik steeds nieuwe podcasts te ontdekken. Tenslotte nog een mooi voordeel: je kunt een beluisterde podcast ook gebruiken voor je CPE-punten.

Auteurs: Dr. Rick van der Kleij is senior onderzoeker bij TNO en de Haagse Hogeschool en is bereikbaar via rick.vanderkleij@tno.nl. Tineke Hof is senior onderzoeker bij TNO en is bereikbaar via tineke.hof@tno.nl.

'Het is niet mijn verantwoordelijkheid'

Over de excuses die mensen gebruiken om het niet naleven van informatiebeveiligingsregels voor zichzelf te rechtvaardigen

Herkenbaar? Je ontvangt een Engelstalige e-mail en om de inhoud iets sneller te begrijpen kopieer je de tekst en plak je deze in Google Translate. Op basis van de Nederlandse vertaling die direct in jouw scherm verschijnt, kun je makkelijker een antwoord naar de afzender formuleren. Maar wist je dat veel bedrijven een protocol hebben opgesteld waarin staat dat het gebruik van deze vertaalwebsite verboden is?

Uit internationaal onderzoek is bekend dat mensen die zich niet volgens de regels gedragen hun ongewenste gedrag goedpraten (1). Mensen weten vaak wel dat ze zich op een bepaalde manier behoren te gedragen, maar gebruiken excuses, ofwel neutralisatietechnieken, om het gewenste gedrag niet te hoeven vertonen. Met andere woorden: ze redeneren het onprettige gevoel dat het overtreden van regels met zich meebrengt weg. Ze denken bijvoorbeeld: 'het is niet mijn verantwoordelijkheid', 'het kan geen kwaad', 'ik heb geen andere keuze' of 'vergeleken met wat anderen doen, valt dit wel mee'.

In dit artikel bespreken we een recent TNO-onderzoek waarbij we de vraag stellen: is het mogelijk om regelopvolging op het gebied van informatiebeveiliging te vergroten door het uitschakelen van neutralisatietechnieken door een gedragsinterventie? Recente andere onderzoeken laten namelijk zien dat training of communicatie kan leiden tot een vermindering van het gebruik van neutralisatietechnieken door medewerkers en tot een sterkere intentie om veilig gedrag te vertonen (2), (3).

Cyberveilig gedrag

Eerder onderzoek uit 2020 van TNO naar cyberveilig gedrag laat zien dat bewustzijn in de vorm van kennis weliswaar een belangrijke voorspeller is van gedrag, maar dat medewerkers ook gemotiveerd moeten zijn en de gelegenheid moeten krijgen om het gewenste gedrag te vertonen (4). Alleen weten dat (en hoe) je als medewerker iets wel of niet behoort te doen is niet genoeg. Denk bijvoorbeeld aan het vergrendelen van je computer of documenten alleen op een veilige wijze delen. Soms ontbreekt de motivatie om gewenst gedrag te vertonen. In andere gevallen kan de motivatie zelfs negatief zijn, bijvoorbeeld als het opvolgen van informatiebeveiligingsregels medewerkers (gevoelsmatig of daadwerkelijk) belemmert in het effectief uitvoeren van hun werk. Dit is terug te zien in de verklaringen die medewerkers geven voor hun ongewenste gedrag: ze passen neutralisatietechnieken toe om hun gedrag te rechtvaardigen. Denk hierbij aan argumenten als het kost teveel tijd, het is te moeilijk, niemand heeft er last van, of het kan toch geen kwaad. De mate waarin medewerkers gebruik maken van neutralisatietechnieken lijkt daarmee een belangrijke indicator voor het niet opvolgen van regels op het gebied van informatiebeveiliging (1), (5), (6).

Onderzoek naar regelopvolging

In ons recente onderzoek nemen we de regelopvolging rondom twee vormen van cyberveilig gedrag onder de loep bij financiële instellingen: (1) het melden van verdachte e-mails en (2) het gebruik van alleen door de organisatie toegestane applicaties en diensten. Een eerste stap in het onderzoek was het bepalen of

Onderdeel	Meetvragen [antwoordschaal]
Excuses	**Ik vind dat ik verdachte e-mails niet hoef te melden …**
Ontkenning schade of nadeel	als niemand er nadeel van ondervindt; als de organisatie er geen schade van ondervindt; als er geen schade optreedt
Ontkenning van verantwoordelijkheid	als ik niet precies weet wat het beleid daarover is; als ik het beleid daarover niet begrijp; omdat anderen het waarschijnlijk al melden.
Beroep op hogere plichten	als ik een belangrijke klus voor mijn leidinggevende aan het doen ben; als het helpt om mijn klus af te krijgen.
Veroordeling van de veroordelaars	als het me teveel tijd kost om het op de voorgeschreven manier te doen; als het beleid daarover onredelijk is; omdat ik denk dat er niets met mijn melding wordt gedaan.
Metafoor van het kasboek	omdat ik verder uitstekend presteer op werk; omdat ik hard werk voor de bank; omdat ik me verder altijd keurig aan alle regels houd.
Verdediging van noodzaak	wanneer ik haast heb; in situaties waarin ik geen andere keuze lijk te hebben; wanneer ik te maken heb met een strakke deadline.
Claim normaal te zijn	omdat bijna niemand dat doet.

Figuur 1 - Vragenlijst naar het gebruik van excuses bij het niet melden van verdachte e-mails. Links staan categorieën van excuses. Rechts de vragen waarmee het gebruik ervan is gemeten. Om de antwoorden vast te leggen is een 5-punts Likertschaal gebruikt, die loopt van oneens (1) tot eens (5).

Protocol gebruik Google Translate
De tekst die je kopieert vanuit de ontvangen e-mail kan vertrouwelijke informatie bevatten, die met jouw handeling daardoor in een paar tellen ook bij Google bekend is. Door het gebruik van deze vertaaltool houd je je dus niet aan de bedrijfsregels. Maar zo belangrijk was de informatie uit de e-mail toch helemaal niet? En met de snelle vertaling begreep je de kern van de boodschap veel beter, waardoor je kostbare tijd bespaarde... .

medewerkers de regels opvolgen rondom deze vormen van gedrag. Vervolgens, als dit niet het geval was, onderzochten we of en welke neutralisatietechnieken zij gebruiken. Hiertoe hebben we een vragenlijst-onderzoek gedaan onder meer dan 600 medewerkers van drie financiële instellingen. Een deel van deze vragenlijst is te vinden in tabel 1. Tenslotte hebben we gekeken of een interventie voor veranderend gedrag zorgt.

Verdachte e-mails

De resultaten van dit vragenlijstonderzoek zijn positief te noemen. Bijna alle deelnemers weten dat zij verdachte e-mails (phishing-mails) moeten melden. De intentie om te melden is hoog en de meeste deelnemers geven bovendien aan dat zij verdachte e-mails ook daadwerkelijk altijd melden. Een kleine groep zegt echter verdachte e-mails niet (altijd) te melden. Volgens verwachting gebruiken deze medewerkers neutralisatietechnieken om dit gedrag voor zichzelf te rechtvaardigen.

De meest gebruikte neutralisatietechniek bij deze kleine groep die geen melding maakte is 'ontkenning van verantwoordelijkheid'. Deze medewerkers vinden dat zij geen verdachte e-mails hoeven te melden omdat 'het beleid daarover naar hun mening niet is gecommuniceerd, ze het beleid niet kennen of begrijpen, of omdat anderen het waarschijnlijk al melden'. Ook 'verdediging van noodzaak' wordt gebruikt als excuus. Vooral het hebben van haast wordt aangewend als excuus binnen deze categorie. Maar over het algemeen kunnen we concluderen dat medewerkers zich correct gedragen als zij e-mails uit onbetrouwbare bron ontvangen.

Toegestane applicaties en diensten

Soms worden applicaties en diensten gebruikt die niet door de organisatie zijn toegestaan, zoals bepaalde filesharingdiensten, presentatietools of samenwerkingstools. Dit wordt ook wel schaduw IT genoemd. Deze diensten vormen een bedreiging voor de informatiebeveiliging omdat zij kunnen leiden tot een datalek of de installatie van malware op de bedrijfssystemen. De deelnemers aan dit onderzoek maken naar eigen zeggen weinig gebruik van niet-toegestane applicaties en diensten, met uitzondering van zogenaamde productiviteitstools, zoals Slideshare, Twilio en Google translate. Ongeveer 28% van de deelnemers maakt hiervan wel eens gebruik.

De meest gebruikte excuses om het gebruik van deze tools te rechtvaardigen vallen in de categorie 'Ontkenning van schade of nadeel'. De deelnemers die gebruik maken van deze niet-toegestane tools vinden dat zij deze applicaties en diensten voor hun werk mogen gebruiken omdat de organisatie er volgens hen geen schade van ondervindt. Ook excuses binnen de categorie 'ontkenning van verantwoordelijkheid' zien we hier terug.

Vergroten regelopvolging door interventie

Nu we weten dat niet alle medewerkers de regels op het gebied van informatiebeveiliging opvolgen en neutralisatietechnieken gebruiken om dit gedrag voor zichzelf te rechtvaardigen, is de volgende vraag: kan het gebruik van excuses, en daarmee regelopvolging, beïnvloed worden door een gedragsinterventie? Op basis van veelbelovende resultaten uit internationaal onderzoek (2) hebben we besloten om op maat gemaakt anti-neutralisatie communicatiecampagnes te ontwerpen. Hiermee willen we de meest gebruikte excuses verminderen die medewerkers soms aanwenden om zich niet aan het informatiebeveiligingsbeleid te houden.

Een anti-neutralisatie communicatiecampagne wordt ingezet om het proces van goedpraten van onveilig gedrag van medewerkers zichtbaar te maken. De campagne laat hen zien dat er geen enkele situatie is waarin riskant gedrag te rechtvaardigen is. Daarnaast worden medewerkers actief opgeroepen om, wanneer excuses zich voordoen, deze te negeren en de informatiebeveiligingsregels op te volgen (voor meer informatie, zie (2)).

Communicatiecampagne

De interventie zou oorspronkelijk worden getest voor beide vormen van gedrag die centraal stonden in deze studie. Onze meting van het gedrag 'melden van verdachte e-mails' laat echter zien dat de intentie om te melden hoog is en dat dit in de praktijk al bijna altijd gebeurt. Een interventie zou hier slechts

Onderwerp: gebruik van goedgekeurde applicaties en online diensten

Van: [redacted]

Aan: [redacted]

Beste [redacted]

Zoals vermeld in onze informatiebeveiligingsvoorschriften, is het niet toegestaan om ongeautoriseerde applicaties en online diensten (zoals presentatietools, productiviteitstools, samenwerkingstools en filesharediensten) te installeren of te gebruiken voor jouw werk zonder expliciete toestemming van onze IT afdeling.

Sommige medewerkers hebben het idee dat gebruik van ongeautoriseerde applicaties en online diensten in bepaalde gevallen te verdedigen is. Dat is begrijpelijk, maar het gebruik hiervan is in geen enkel geval te accepteren. Ook niet als je denkt dat [redacted] hierdoor geen schade ondervindt of als je vindt dat het beleid hierover niet duidelijk is gecommuniceerd. Want ongemerkt en indirect kan [redacted] wel degelijk schade ondervinden, zoals derden die ongewenste toegang tot vertrouwelijke informatie krijgen.

Daarom geldt: gebruik voor jouw werk alleen door onze IT afdeling goedgekeurde applicaties en online diensten.

Je leest alle beveiligingsvoorschriften op het intranet via [redacted]

Heb je nog vragen? Laat het me gerust weten, ik help je graag.

Met vriendelijke groeten,

[redacted]
Teamlead afdeling Security

Figuur 2 - Anti-neutralisatiecommunicatie.

beperkt nut hebben. In dit artikel zoomen we daarom in op de interventie om regelopvolging te vergroten rondom gebruik van door de organisatie toegestane applicaties en diensten. De in dit onderzoek gebruikte communicatiecampagne voor dit doel is te vinden in figuur 1.

Om de effecten van de gedragsinterventie te kunnen bepalen, is deze getest binnen een financiële instelling. 242 medewerkers zijn verdeeld over twee groepen. Medewerkers in groep 1 kregen de anti-neutralisatiecommunicatie van hun leidinggevende via de e-mail. Medewerkers in groep 2 kregen geen e-mail. Enkele weken na de interventie is het gedrag gemeten via een vragenlijst. Daarbij is ook de mogelijke afname van het gebruik van excuses ten gevolge van de gedragsinterventie meegenomen in de meting. De metingen zijn zowel vooraf als naderhand gedaan bij beide groepen.

Resultaten

Verrassend genoeg zien we geen effect van de gedragsinterventie maar wel van tijd. Bij beide groepen is een afname gemeten over de duur van het onderzoek in het zelf-gerapporteerde gebruik van niet toegestane productiviteitstools. Ook is een afname vastgesteld over de tijd in het gebruik van excuses. Deze effecten zijn voor beide groepen echter even sterk. Zowel in de groep die de gedragsinterventie heeft ontvangen als in de groep die geen interventie heeft gekregen zien we een verschuiving in de gewenste richting. Het zelf-gerapporteerde gebruik van niet toegestane productiviteitstools nam af in de tijd met 63%.

Conclusie

Dit onderzoek heeft gekeken naar de mate waarin medewerkers van financiële instellingen zich zeggen te gedragen conform gedragsregels op het gebied van informatiebeveiliging. Ook is gemeten of en welke excuses zij gebruiken om het niet naleven van regels voor zichzelf goed te praten en of het mogelijk is regelopvolging te vergroten.

De resultaten van dit onderzoek laten zien dat het merendeel van de medewerkers de gedragsregels volgens het beleid omtrent informatiebeveiliging keurig opvolgen. De groep die dat niet doet, gebruikt in de meeste gevallen productiviteitstools die niet zijn toegestaan door de organisatie. De mate waarin medewerkers zich onveilig gedragen, verschilt per type van gedrag. Als medewerkers productiviteitstools gebruiken die niet zijn toegestaan, wil dit niet automatisch zeggen dat zij zich op andere gebieden ook veilig gedragen. De resultaten van dit onderzoek laten ook zien dat medewerkers excuses gebruiken om het ongewenste gedrag voor zichzelf goed te praten. Het soort van excuses dat medewerkers gebruiken, verschilt daarbij per doelgedrag. Dit toont maar weer aan dat er geen silver bullet, een kant-en-klare oplossing, bestaat voor het tegengaan van cyberonveilig gedrag op de werkvloer, maar dat maatwerk telkens is vereist.

Om het gebruik van excuses tegen te gaan is een gedragsinterventie ingezet. Deze anti-neutralisatiecommunicatie laat echter geen eenduidig effect zien. Er treedt een daling op in het zelf-gerapporteerde ongewenste gedrag alsmede in het gebruik van excuses. Omdat de dalingen ook zijn gevonden bij een controlegroep kunnen deze niet worden toegeschreven aan de gedragsinterventie. Een mogelijke storende factor kan zijn dat de deelnemers in beide groepen zich anders zijn gaan gedragen omdat zij wisten dat zij deelnamen aan een onderzoek. Waarbij het enkele feit dat er meer aandacht is voor een bepaald proces er al voor kan zorgen dat het proces beter gaat lopen (7). Ook de vragenlijst die deelnemers voorafgaand aan het onderzoek hebben ingevuld, kan de bewustwording over het beleid hebben vergroot en de regelopvolging hebben doen laten toenemen.

Mogelijkheden vervolgonderzoek

In het verlengde van dit onderzoek zien wij meerwaarde in onderzoek naar andere manieren om regelopvolging te

vergroten door het uitschakelen van neutralisatietechnieken. Zo is er evidentie dat een op maat gemaakte training over neutralisatietechnieken het gebruik van excuses zou kunnen ontmoedigen. Hoe een training kan worden ontwikkeld voor de praktijk, of deze succesvol is in het tegengaan van excuses en leidt tot gedragsverandering, zou het onderwerp kunnen zijn van vervolgonderzoek.

Een herhaling van het huidige onderzoek maar dan voor andere gedragingen is ook denkbaar. De gedragsinterventie is getest bij een specifiek soort van gedrag: het gebruik van productiviteitstools die door de organisatie niet zijn toegestaan. Het effect van de interventie op het tegengaan van ander onveilig gedrag of juist promoten van cyberveilig gedrag in de organisatie zou tevens onderwerp voor vervolgonderzoek kunnen zijn.

Er zijn bovendien andere maatregelen denkbaar die een effect kunnen hebben op het gebruik van excuses door medewerkers, zoals aanpassen van beleid of het beschikbaar stellen van veiligheidsmaatregelen die veilige gedragskeuzes ondersteunen. Denk hierbij aan een meldknop in het mailprogramma om het melden van verdachte e-mails makkelijk te maken voor de eindgebruiker. Ook hier liggen mogelijkheden tot een verdieping van het huidige onderzoek.

Referenties

(1) Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 34(3), 487-502.

(2) Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don’t even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. Journal of the Association for Information Systems, 19(8), 3.

(3) Siponen, M., Puhakainen, P., & Vance, A. (2020). Can individuals’ neutralization techniques be overcome? A field experiment on password policy. Computers & Security, 88, 101617.

(4) Van der Kleij, R., Wijn, R., & Hof, T. (2020). An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. Computers & Security, 97, 101970.

(5) Morris, R. G., & Higgins, G. E. (2009). Neutralizing potential and self-reported digital piracy: A multi-theoretical exploration among college undergraduates. Criminal Justice Review, 34(2), 173-195.

(6) Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. Information & management, 54(8), 1023-1037.

(7) McCarney, R., Warner, J., Iliffe, S., Van Haselen, R., Griffin, M., & Fisher, P. (2007). The Hawthorne Effect: a randomised, controlled trial. BMC medical research methodology, 7(1), 1-8.

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Regeldrift en de zucht naar ethiek

Op het Malieveld in Den Haag zwaaien demonstranten met vlaggen. Door de stad wordt gemarcheerd in protest tegen besluiten, tegen besluiteloosheid, tegen te veel regels en tegen te weinig regels. Op het Binnenhof en op het Plein staan boze moeders, vaders, gedupeerden en mensen die geen plek meer kunnen vinden in de maatschappij. Voor het Ministerie van Volksgezondheid zit een eenzame protesterende vrouw in psychische nood die al jaren op zorgwachtlijsten staat. Bij het Torentje slaat een groepje burgers met lepels op pannen om gehoord te worden.

Ik woon in Den Haag en zie en hoor alle protesten. De wanhoop en de boosheid. Het optimisme en de doorzettingskracht. Wat heel veel van deze protesterende mensen gemeen hebben, is dat zij ageren tegen regels. Regels die willen dat gegevens verzameld worden over persoonlijke zaken. Regels die autonomie inperken en registraties van burgers stimuleren. Regels die gegevensverzameling van bepaalde groepen mensen afdwingen en daar dan rechtsgevolgen aan verbinden.

En dat gaat lang niet altijd goed. Sterker nog, in het ergste geval is die regel en de uitvoering ervan zo vreselijk slecht dat mensen jarenlang in acute nood verkeren. Dat een regel niet werkt, verkeerd geïmplementeerd is of misschien zelfs ronduit discriminerend is, is van alle tijden. Denk alleen maar aan het feit dat het vrouwenkiesrecht afgedwongen moest worden omdat het hen jarenlang door een regel verboden was te stemmen. Een situatie of regel veranderen kan alleen als mensen gehoord worden en er opvolging aan die geluiden gegeven wordt. In steeds meer bedrijven zie je daarom dat ethiek binnen de bedrijfsprocessen aan de orde komt en de vraag 'maar doen we nog wel het juiste?' een plaats krijgt in de discussie naast (en soms zelfs boven) het enkele voldoen aan een regel. Juist omdat regels soms akelig tekortschieten en je met een ethisch debat naar boven brengt waar de schoen kan wringen.

Zo bestaat er bijvoorbeeld in de verzekeringsbranche een Kader voor Ethiek bij datagedreven besluitvorming. In het bedrijf waar ik werk hebben we dat kader geïmplementeerd in ons beleid en hebben we een Ethiek werkgroep opgericht die – met mandaat – ethische vraagstukken behandelt. Een regel is niet per definitie goed of slecht, en juist daarom is het essentieel dat met iedereen die onderworpen wordt aan de regel erover van gedachten gewisseld wordt. En dat na die discussie de nodige bijsturing plaatsvindt.

Onlangs schreef de Raad van Europa een vrij negatief rapport over het tekortschieten van de democratie in Nederland. Volgens dat rapport zijn verregaande hervormingen nodig in wetgeving, uitvoering en rechtspraak om een nieuwe toeslagenaffaire te voorkomen. Persoonlijk denk ik dat onze Trias Polititica een stuk welvarender zou zijn met een gezond ethisch debat. En daarbij zou een minister van ethische zaken en/of een ethisch ombudspersoon voor de wetgevende macht niet misstaan. Op naar een nieuwe ethische democratie!

Rachel

Auteur: James Cheney, Technical Consultant, SRC Secure Solutions BV. James is te bereiken via jcheney@srcsecuresolutions.eu. Bewerkt en vertaald door SRC Secure Solutions B.V.

Geëmuleerde honeypots in de strijd tegen hackers

Honeypots worden al jaren gebruikt om aanvallers te lokken en te onthullen wie ze zijn, welke methoden ze gebruiken en hoe je moet reageren zonder de werkelijke bedrijfsmiddelen in gevaar te brengen. Door zich voor te doen als een server of ander waardevol aan het netwerk verbonden bedrijfsmiddel, lokt de honeypot aanvallers. De honeypot gebruikt fictieve gegevens, is geïsoleerd van het netwerk en wordt nauwlettend in de gaten gehouden voor het verzamelen van informatie.

Dit artikel beschrijft de geschiedenis van geëmuleerde honeypots en legt uit hoe geëmuleerde apparaten van allerlei aard kunnen dienen als valstrikken die veel verder gaan dan het verzamelen van informatie om cyberbeveiligingsteams te helpen een aanval op te sporen en tegen te houden.

Honeypots zijn het tegenovergestelde van conventionele beveiligingstools, die echte netwerkactiviteiten scannen en enorme hoeveelheden gegevens over activiteiten verzamelen. Honeypots zijn passief. Ze verzamelen geen gegevens over netwerkonderdelen, maar lokken aanvallers en verleiden ze tot het onthullen van informatie die tegen hen kan worden gebruikt.
Het honeypotconcept is al zo oud als de eerste echte computerhack, die Clifford Stoll gedetailleerd beschreef in zijn boek The Cuckoo's Egg. Stoll vertelt het verhaal van zijn jacht op een hacker die in 1980 inbrak in een computer van het Lawrence Berkeley National Laboratory (LBNL). Met behulp van Tymnet en verschillende overheidsinstanties ontdekte Stoll dat de inbraak via een satelliettelefoon afkomstig was van een universiteit in Duitsland en blijkbaar militaire bases als doelwit had om meer te weten te komen over het Strategic Defence Initiative (SDI), het Star Wars-project. Om de hacker over te halen zich bekend te maken, creëerde Stoll een primitieve honeypot - een fictieve afdeling bij het LBNL met een nepaccount van SDInet, vol met realistische en verleidelijke bestanden. Het daagde de hacker uit om dit systeem aan te vallen. De aanval werd getraceerd naar Markus Hess, die gestolen informatie verkocht aan de inlichtingendienst van de toenmalige Sovjet-Unie, de KGB.
Moderne honeypots maken gebruik van virtualisatie en AI om het gebruik ervan te vereenvoudigen. In deze blog noemen we ze 'honeypots met hoge interactie'. Hoewel ze moderner zijn dan de oorspronkelijke honeypots, zijn ze uiteindelijk conceptueel hetzelfde: kwetsbare middelen die zijn gebouwd om ervan te leren.

De noodzaak van misleiding

Of het nu gaat om sport, spel of oorlogsvoering, misleiding is essentieel voor elke succesvolle strategie. Het is duidelijk dat cyberaanvallers niet zonder misleiding kunnen. Als dat zo is, waarom is misleiding dan niet een steunpilaar in elk Security Operations Centre (SOC)? Misschien komt dat door het vroege succes en de reputatie van legacy honeypots. Het honeypotconcept heeft een imagoprobleem onder beveiligingsprofessionals die een verouderd idee hebben van het doel ervan. Velen beschouwen een honeypot als iets dat alleen geschikt is voor onderzoek op het gebied van cyberspionage, en zien ze daarom als geavanceerde extra's. Ten tweede brengt effectief gebruik van honeypots kosten en complexiteit met zich mee. Die beperken de mogelijkheden van een organisatie om honeypots op grote schaal in te zetten. Omdat het gebruik ervan in grote aantallen geen optie is, kunnen beveiligers ze niet verstoppen in een menigte. Daardoor kunnen honeypots alleen informatie verzamelen, en geen risico's beperken en systemen verdedigen. Het verouderde beeld van honeypots is een reëel probleem. Gezien de grote van het huidige doelwit, dat virtualisatie, cloud, IoT connected devices, shadow IT, werken op afstand en IT/OT-convergentie omvat. Ook al zijn virtuele honeypots eenvoudiger te implementeren dan fysieke, ze vereisen nog steeds isolatie, licenties voor de lokmiddelen, risicobeheer en monitoring.

Verborgen juweel

De honeypotgeschiedenis kent een verborgen juweel: de geëmuleerde honeypot. In tegenstelling tot een legacy honeypot, gebruikt een geëmuleerde honeypot geen werkelijke activiteiten om aanvallers te lokken. In plaats daarvan fungeert het als een normale asset, maar werkt het als een virtuele imitatie van een echt netwerk segment (inclusief servers en andere assets) . Aangezien de 'asset' virtueel is, is hij snel en eenvoudig in te zetten. En dan wordt het gebruik op grote schaal opeens een optie. Het doel ervan is om aanvallers te vangen, niet om ze te bestuderen.
Jammer genoeg vervagen door het grote aanbod de grenzen tussen legacy honeypots, geëmuleerde honeypots en lokmiddelen (valse bestanden, gegevens, enz.), waardoor organisaties denken dat ze de ene moeten kiezen boven de andere. Maar alle honeypots zijn waardevol als je ze op de juiste manier gebruikt. Hoe het ook zij, honeypots hebben een goed imago sinds hun uitvinding. Deze perceptie doet de unieke waarde van emulatie enigszins teniet.

Valstrikken - die een moderne versie van geëmuleerde honeypots zijn - zijn goedkoop en kunnen automatisch worden bewaakt, waardoor ze zeer praktisch zijn om snel en op grote schaal in te zetten.

Korte geschiedenis van geëmuleerde honeypots

De bekendste geëmuleerde honeypottechnologie is de opensourcesoftware Honeyd voor UNIX/Linux, die is ontwikkeld en wordt onderhouden door Neils Provos. Het kan verschillende besturingssystemen en diensten emuleren op TCP/IP-stackniveau. Het primaire doel van Honeyd is het detecteren van inbraken door alle ongebruikte IP-adressen in een netwerk tegelijkertijd te contro-

leren. Elke poging om verbinding te maken met een ongebruikt IP-adres wordt beschouwd als een ongeoorloofde of kwaadaardige activiteit. De eerste grote release dateert van 2003. Om dit in context te plaatsen: toen Honeyd werd gelanceerd, bestonden geavanceerde aanhoudende bedreigingen (APT's) nog niet. Evenmin als Facebook, LinkedIn, Gmail, iPhones of de cloud. Internet en telecommunicatie waren nog niet geconvergeerd. De IT-omgeving van vandaag de dag is heel anders en vraagt om een ander type geëmuleerde honeypot.

Geëmuleerde honeypots

Geëmuleerde honeypots worden ook wel medium interaction honeypots of traps genoemd). Deze honeypots hebben een IP-adres en zijn niet te onderscheiden van echte assets, maar zijn geen volledig uitgebouwde assets die licenties en computer en storage resources vereisen. In tegenstelling tot zuivere of traditionele honeypots die zijn gebouwd om te leren, zijn geëmuleerde honeypots gebouwd om aanvallers te vangen en bijvoorbeeld een sandbox omgeving in te sturen. Dit vereist slechts voldoende interactie om de aanvallers te identificeren en hun technieken te documenteren. Deze lichtgewicht en lowtouch benadering biedt unieke voordelen ten opzichte van honeypots met volledige interactie:

- Brede schaalbaarheid;
- Snelle inzetbaarheid;
- Laag risico voor dataverlies, omdat het geen echte, kwetsbare asset is;
- Agentloos;
- Ondersteuning voor operationele technologie (OT) en Internet of Things (IoT).

Geëmuleerde honeypots bieden nieuwe mogelijkheden voor misleiding. Hoewel het contra-intuïtief lijkt, kunt u hiermee risico's beperken door uw aanvalsgebied uit te breiden met vervalsingen. Het uitbreiden van het aanvalsgebied druist in tegen de conventionele cyberbeveiligingswijsheid, maar omdat de uitbreiding bestaat uit geëmuleerde assets is de strategie is zeer effectief.
Met emulatie kunt u nu groots inzetten en echte activiteiten verbergen. Organisaties met een volwassen beveiligingsbeleid dekken meer dan 30% van hun IP-portfolio af met geëmuleerde honeypots. Zij verminderen risico's door het waarschijnlijker te maken dat een aanvaller een valstrik zal raken dan een echt bedrijfsmiddel. Geëmuleerde honeypots zijn bij uitstek geschikt voor de bescherming van OT en IoT. Aangezien geëmuleerde honeypots agentless zijn, niet in contact komen met echte controllers en apparaten, en geen gevoelige informatie verzamelen, kunnen ze naadloos worden geïntegreerd in een productie-, energie- of gezondheidszorgomgeving, zonder de activiteiten te verstoren.

Geëmuleerde honeypots voldoen aan de meeste eisen voor misleiding, maar niet aan alle. Honeypots met een hoge mate van interactie (bijvoorbeeld volledige OS honeypots), met referenties, links en bestanden voorzien in een unieke behoefte en vullen geëmuleerde honeypots aan.

Opkomst van misleidingstechnologie

Miljoenen aangesloten apparaten (medische wearables, sensoren, controllers, slimme printers, camera's, koffiezetapparaten, thermostaten, speelgoed, geldautomaten, enzovoort) hebben een wirwar aan aanvalsmogelijkheden gecreëerd, waarvan cybercriminelen misbruik kunnen maken. Er zijn voorbeelden te over. De SolarWinds-aanval, met een zeer kleine malware-voetafdruk, die maandenlang onopgemerkt bleef, bewijst eens te meer dat aanvallers zich waarschijnlijk al in uw netwerk bevinden en weten hoe ze detectie kunnen vermijden;
Recente ransomwareaanvallen, zoals die op JBS Foods en Colonial Pipeline, maken duidelijk dat OT-netwerken gemakkelijke en lucratieve doelwitten zijn voor aanvallers.

De aanvallers van vandaag maken gebruik van aanvalstechnieken, waartegen conventionele beveiliging niet werkt. Veel aanvallen blijken onzichtbaar voor traditionele beveiligingstools, waardoor systemen en apparaten kwetsbaar zijn.
Moderne misleidingstechnologie met behulp van geëmuleerde valstrikken kan helpen dit nieuwe bedreigingsscenario te bestrijden. Ook binnen het actieve verdedigingsraamwerk Shield van MITRE speelt misleiding een sleutelrol in een modernere cyberbeveiligingsstrategie.
Misleidingstechnologie geeft cybercriminelen een vals gevoel van succes door hen te laten geloven dat ze voet aan de grond hebben gekregen in het netwerk. Deze truc geeft organisaties de tijd om op te treden tegen de aanvallers, terwijl de echte activiteiten worden beschermd.
De voordelen van deception technology zijn onder meer:

- Vroege detectie na een inbraak;
- Gemakkelijke schaalbaarheid (lage kosten en complexiteit);
- Laag risico voor de werkelijke activiteiten;
- Compatibiliteit met elk apparaat met een IP-adres.

Wat oud is, is weer nieuw

Het is tijd om geëmuleerde honeypots uit de beperkte context van de vroege jaren 2000 te halen en ze opnieuw toe te passen waar ze thuishoren: in het beveiligingslandschap van vandaag. IT/OT-convergentie, cloud en thuiswerken zijn het nieuwe normaal. Dekking van het aanvalsgebied met breed ingezette en aanpasbare misleiding is precies wat de dokter heeft voorgeschreven.

Auteur: Ir.drs J. van der Vlugt CISA CRISC. Jurgen is zelfstandig professional voor Information governance- en risk management advisering en audit. Jurgen is te bereiken via jvdvlugt@xs4all.nl.

AI, Max!

In deel 1 zagen we dat zelfrijdende auto's – zelfs in combinatie met menselijke back-up chauffeurs – nog (veel) te weinig zelf kunnen om veilig zelfstandig de weg op te mogen (1). Waarbij voor het gemak nog voorbij was gegaan aan de kwetsbaarheden die aan al die software kleven. Er schijnt in Gelderland een stuk weg te zijn waar al diverse T…'s (betreffende autofabrikant zal wel anoniem willen blijven) naast de weg in de sloot zijn beland. Een soort anti-lane departure correctie. Is dat nou een feature of een bug (2)?

Deel 3 van 3: Auto's, besturing en reflexen

Zo zullen er ongetwijfeld nog vele kleine 'dingetjes' net niet helemaal netjes zijn uitgewerkt. Het is evenmin zo dat iedereen doelgerichte proefritten gaat maken om nieuwe functionaliteiten te testen om zo een patch op het motormanagement door te (laten) voeren. Dat doen uw IT-beheerders voor nieuwe software-patches wel, waarom zouden de 'eindgebruikers' dat voor auto's niet hoeven doen? Aansprakelijkheid is een heikel ding, in de autowereld.
Andere kwetsbaarheden die nog ongenoemd waren, liggen op het vlak van beheer en beveiliging in engere zin (afscherming). Wie denkt dat het met het Identity- en Access Management (IAM) wel goed zit, heeft hopelijk een goede levensverzekering voor de nabestaanden. Zie bijvoorbeeld het prijswinnende Hacker gehackt van Joost Geerts in iB-Magazine 2020-5: een inbraak zit in een klein hoekje. En het gaat niet alleen om de spraakmakende inbraken waarbij een complete autobesturing wordt overgenomen (qua haalbaarheid al aangetoond) – wat in zulke gevallen bijna gelijk een class break is; alle auto's met dezelfde software kunnen door hetzelfde gaatje worden gehackt. Het gaat óók over de hele software-ontwikkelketen. Waar ransomware steeds vaker via supply chain attacks binnenkomt, zal dat voor autosoftware-kraken zeker ook een optie zijn en blijven.
Waar we in de informatiebeveiligingswereld onszelf bezighielden met statische servers (3) en de in de loop der tijd geëvolueerde software-ontwikkelmethodieken alsook informatiebeveiligingsformules (denk aan 'standaard' IAM, OTAP-straten, Change Management-procedures, et al.), zien we dus een forse toename in de reikwijdte van ons werk; waarvoor we nog bezig zijn de standaarden te ontwikkelen. Evolutie van de huidige standaarden kan al te weinig zijn om de exponentiële complexiteitsgroei van de problematiek aan te kunnen. En uiteraard is OT-security (4) voor velen een nog veel te onontgonnen terrein: voor vakgenoten én voor onze klanten; in het land der blinden lijkt eenoog al snel koning. Dus wie een halve-carrièreswitch overweegt: Kijk eens naar dat OT-security…!

Sturing door overheid

In deel 2 bleek ook dat 'centrale' aansturing of hulp niet gaat helpen of van de wal in de sloot qua privacy en eigen verantwoordelijkheid (5). Misschien kunnen we nog wel wat met dynamische wegmarkering – maar dat riekt natuurlijk direct weer naar 'sturing door een overheid' en de ervaring leert dat zulks niet vanzelf altijd maar goed gaat. Smart parkeerplaatsen, verkeerslichten: idem – stel je voor dat een fabrikant het voor elkaar krijgt om de eigen auto's bij de verkeerslichten voorrang te laten krijgen (6). Al hetgeen met centrale besturing samenhangt, komt al snel uit bij de Grote Drie van bezwaren tegen overheidsbemoeienis:

1. Ik wil niet dat de overheid weet waar ik ben;
2. Ik wil niet dat de overheid stuurt op basis van potentieel (sic) willekeurige discriminatie of wat dan ook tegen art.1 van de Grondwet;
3. Integriteit van data is niet in het belang voor diegene die de integriteit kan beheersen.

De overheid heeft geen belang bij de integriteit, die mij specifiek zou kunnen hinderen, u en ik wel. Voor toezichts- of controlemogelijkheden is het andersom, een typisch geval van verkeerd belegde incentives en afschuifbare externaliteiten.
Vooralsnog blijken ook degenen die middenin de ontwikkelingen rond zelfrijdendheid (7) bezig zijn, te beseffen dat de wereld iets ingewikkelder is dan gedacht. Het als grote jongen roepen van uitdagen¬de doelstellingen is altijd een risico en zeker als het om realiseringsdatums voor zelfrijdende auto's gaat. Ene Elon M. van garage T. moest al op zijn beloften terugkomen (8). Ook anderen zijn voorzichtiger geworden of zijn zelfs opgehouden met vooraan te willen lopen.

Complex

Als tussentijdse conclusie moet dan ook gelden dat de 'AI' van zelfrijdende auto's niet verder is dan bijvoorbeeld dat andere 'poster child' Watson in het medische domein; namelijk, echt nog niet beter dan mensen (9). Ook de winst van Watson (niet één maar 42 samenwerkende machine learning systemen!) bij Jeopardy was niet zo indrukwekkend als men wel denkt. De vragen waren in een nog steeds relatief gesloten, beperkt domein. Watson won maar net en had een aantal domme foute antwoorden en onbegrijpelijke missers. En het basis opzoek- en rekenwerk was niet zo 'intelligent' (10).
Het enige werkveld waar redelijk ongestoord voortgang wordt gemaakt, is er een waar we dat misschien niet echt zouden moeten willen: autonoom schietende killer bots. Nu nog heel experimenteel in het militaire domein, met de nodige blunders, ethische vragen (11) en praktische problemen. Zo meteen misschien al paramilitair of 'orde handhavend' bij onwelgezinde politieke demonstraties? Hoewel deze auteur nog wel nut ziet in na-montage van zoiets als accessoire (12).
De autowereld heeft natuurlijk bovendien ook wel bij uitstek te maken met complexiteit. Binnen de auto (het blijft een beperkte fysieke ruimte en het functioneren van de onderdelen

is gesneden koek), maar vooral ook in de omgeving. Zóveel actoren en passieve objecten vind je niet snel in andere domeinen waar het met AI ook al niet opschiet, dus voor auto's wordt het lastig. Waar vinden we zoveel actoren?

Tot nu toe bleek een fietser die achter een stilstaand voorwerp vandaan komt – waar die eerst achter uit beeld raakte – twee verschillende objecten met onbekende bewegingsrichting en -snelheid (13). Een bal die, om het nog erger te maken, onverwachts de weg op stuitert wordt nogal eens gevolgd door een klein kind; veel kwetsbaarder dan die bal op zich. Dat weet iedereen. Maar uw auto nog lang niet. Logisch (sic) maar niet handig.

Training

Waar is de niet-acterende, passieve omgeving zó complex en onregelmatig? De ene boom ziet er net wat anders uit dan de andere. En verkeersdrempeltjes zijn soms slechts chauffeur wakker schuddend, soms forse hobbels. Je ziet het niet altijd aankomen. En er verandert zo veel in de omgeving, zelfs wat stil lijkt te staan. Omleidingen, rijbaanverleggingen, etc. – ja, de wereld om ons heen verandert voortdurend (14). Waarnaast natuurlijk het rijgedrag van overige weggebruikers hoogst variabel is. De ene fietser reageert beslist anders dan de andere. Succes, zelfrijdende auto in Amsterdam…! Maar ook… de ene oude-Saab-rijder reageert nog slechter dan de andere (15).

Wat dus nodig zal zijn – en de eerste ontwikkelingen in labopstelling gaan die kant gelukkig ook op – is een exponentiële schaalvergroting in de complexiteit van algoritmiek en berekening. Niet alleen een enorme schaalvergroting en -verdieping van neurale netwerken kan ons redden. Hoeveel lagen méér we nodig hebben en hoeveel breder die moeten zijn (mét variaties in de triggerfuncties op de nodes, de backpropagation etc. etc.), met navenant méér trainingsdata; wie het weet mag het zeggen. "Heul veul," is wel het minste.

En dan houden we over de issues met:

De huidige 'AI'/ machine learning;

Van het alleen maar kunnen interpoleren met de zo snelle afname van relevantie bij extrapolatie;

Eerste en tweede ordefouten, die niet noodzakelijkerwijs kleiner worden, etc.

Wat erbij nodig zal zijn, is een koppeling met elementen uit de aloude Expert Systemen met hun relatief abstracte symboolmanipulatie op basis van declaratie van axioma's ('feiten') en productieregels. In combinatie met rechttoe-rechtaan gewone procedurele algoritmen (16) én anderzijds fuzzy logic. Of is dat laatste een, overgeslagen, extra stap bij machine learning? Gooi er dan nog een forse scheut seeding en tweetraps leren bij (inprogrammeren van heuristieken uit data

> Nee, voorlopig zullen we het moeten doen met, als het eventueel toch zou lukken, een Formule A(utomatically driven by software). De formule 1 e.v. waren toch altijd officieel bedoeld als testomgevingen voor het neusje van de zalm qua techniek. Nou, daar past het zelfrijdende, dat als neusje van de zalm qua autotechniek geldt (of ooit zal gelden), toch mooi bij? De belofte was 'juist het stukje Sturen te automatiseren' – dat was zowat als enige deelprobleem niet met techniek oplosbaar, maar nu wellicht wel. In plaats van wat waaghalzen-met-andermans-kapitaal kunnen we nu terug naar het testen van de beste nieuwe technieken! Maar dan is het geen showbizz meer maar (software-)vendors die tegen elkaar pitchen.
>
> Ga maar na: De situational awareness (andere Auto's, gele vlaggen wegens olielekken etc.), is voor alle teams gelijk te trekken met centraal verwerkte en doorgegeven beelden want het privacy-idee van artikel II is hier niet relevant. En wie wat extra's wil qua omgevingsawareness kan dat gemakkelijk toevoegen. Bandeslijtage, specifieke eigen technische parameters: laat maar zien dat die 'perfect' worden verwerkt. De verwerking van al die data kan in de auto óf gewoon in de pits zoals nu al wordt gedaan, toch?
>
> Het zal wat ver buiten ons beeld zijn – want saai (geen Max- maar Lewis-stijl) – en stil want we gaan er wel vanuit dat elektrisch de toekomst heeft. Dus is het voor publiek niet aantrekkelijk om te zien: live dan wel vanuit huis. Maar het kan bij uitstek een enigszins beperkt complexe 'omgeving' realiseren om het zelfrijdende van auto's steeds verder te ontwikkelen. Tot ze de weg op kunnen. Er is zelfs een minieme kans dat Tesla dan nog bestaat.

of menselijke ervaringen, semi-symbolisch, waarna verder kan worden getraind op data) met flexibele neurale-netwerkstructuren en wie weet krijgen we iets zinvols.

Ook pruning, het snoeiwerk in neurale netwerken, is vooralsnog te weinig van de grond gekomen. En als er na snoeien weinig connecties overblijven, misschien kunnen we dan terug redenerend wel tot kennelijke algoritmen komen, bij wijze van emergent properties in de data?! Pas dan hebben we inductieve wetenschap. Nou ja, inductieve berekeningen; naast de deductieve traditionele algoritmen.

Zo ver zijn we helaas nog lang niet. We zullen met 'AI' nog een derde keer (17) een 'AI-winter' ingaan. Hoewel vorige keren óók een klein aantal toepassingsgebieden best van de grond leken te komen, zal dit in het publieke discours beperkt zichtbaar blijven. Afgezien van die paar verschrik¬kelijk verkeerde toepassingen:

- Discriminerend, zodra (18) door de overheid ingezet;
- Privégegevens stelend, (19) als het door private partijen gebeurt en
- Ach, de paar puntoplossingen die 'AI' nu automatiseert in bedrijfsprocessen.

RPA is ten slotte ook maar het oude straight-through processing gekoppeld aan een net wat bredere variatiemogelijkheid in transacties dan het (sic) Six Sigma-denken (20). AI zijn er nog steeds een aantal betrokkenen die geloven dat het met rechttoe-rechtaan hard doorwerken zou moeten kunnen lukken, met automatisch rijdende auto's (21).

AI verder helpen

En laten we ondertussen in de gaten houden waar we met puntoplossingen puntproblemen kunnen aanpakken. Dus niet al te complex, want het lijkt wel alsof complexiteit van problematiek - inhoudelijk en qua context - de achilleshiel is van AI/machine learning. Misschien moeten we juist veel meer experimenteren met bijvoorbeeld RPA? AI is het een klein issue, met klein nut, we kunnen wel leren wat het kan en vooral wat het niet kan.

En we kunnen op zoek naar vergelijkbare 'probleemgebieden' om AI verder te helpen.

Zo ben ik vanuit een brede interesse in alles wat met wijn te maken heeft, heel blij met de ontwikkeling van geautomatiseerd wijngaardbeheer. Drones kunnen individuele stokken met spectraalanalyse controleren op het begin van ziektes en (rondrijdende) drones kunnen dan alleen de stokken die het nodig hebben, bespuiten met bestrijdingsmiddelen (22). Dat scheelt een hoop bestrijding! We zijn bijna zover: alleen de geautomatiseerde koppeling van lucht naar grond ontbreekt nog. Nu nog het snoeien en de pluk automatiseren. Moeilijk, want fysiek delicaat en zeer ervaring gebonden. En het proeven (23), dat mag u aan mij overlaten.

We zijn bijna zover: alleen de geautomatiseerde koppeling van lucht naar grond ontbreekt nog.

Referenties

(1) Goto HumanDriver Considered Dangerous, iB-Magazine 2021-3.
(2) Het is min of meer formeel gedocumenteerd, ergens, dus zouden sommigen het een feature noemen. Maar voor de gebruiker (de backup-chauffeur!) is dat niet leesbare commentaar dus een bug..?
(3) Ook de cloud is slechts 'andermans servers die fysiek ergens staan'.
(4) De Operational Technology in de auto, maar buiten scope van dit artikel ook in 'de' fabriek. De 'koppeling' van OT aan kantoorautomatisering staat qua integrale beveiliging ook nog in de kinderschoenen.
(5) Aangestuurd autorijden, iB-Magazine 2021-5
(6) Zo zou het een fabrikant ook niet kunnen schelen dat verkeerd gedrag van één Saab-rijder in software-updates zou worden verwerkt en alle Saab-rijders agressiever zou afstraffen. Zie ook (14)
(7) Men vreze, dat dit zojuist verzonnen woord niet in de nieuwste Van Dale is opgenomen.
(8) Eerst was het: www.inc.com/nick-hobson/elon-musk-says-hes-close-to-solving-one-of-hardest-technical-problems-thats-ever-existed-is-he-really.html maar ook toen was er al www.wsj.com/articles/self-driving-cars-could-be-decades-away-no-matter-what-elon-musk-said-11622865615, waarna Musk in www.theverge.com/2021/7/5/22563751/tesla-elon-musk-full-self-driving-admission-autopilot-crash moest terugkrabbelen.
(9) Met enige regelmaat komen er fraaie verhalen de wereld inzeilen, maar serieuze analyses gooien die verhalen telkens weer van tafel.
(10) Zie https://codeburst.io/ken-jennings-and-brad-rutter-were-tricked-by-watson-they-should-demand-a-rematch-6a5ba2661ab0
(11) Wie denkt dat zij/hij begrijpt hoe non-discriminatie- en ethische afwegingen in AI zouden moeten, kan https://pair-code.github.io/what-if-tool/ai-fairness.html bestuderen en oefenen. Eenduidige antwoorden zijn er niet.
(12) Zie ook (14).
(13) Gelukkig dat Heisenberg's Onzekerheidsprincipe op deze schaal niet van toepassing is. Voor de jeugdige lezers: dit betreft Heisenberg, de gigant in de theoretische fysica, niet die van de Netflix-serie.
(14) Hierin zit dus een hint: Vertrouw niet te veel op centraal verzamelde omgevingsdata! Maar ja, die zijn wel de basis voor routeberekeningen en het 'plaatsen' van gedetecteerde objecten. Of moet 'alle' omgevingsdetectie dan maar altijd opnieuw ter plekke worden gedaan door iedere zelfrijdende auto...?
(15) Ervaringsfeit van ondergetekende, geen Saab-fan.
(16) Tsja, ook gewoon programmeerwerk met Let, If-Then en Jump. Dat zijn de enige primitieven die nodig zijn...! Ook Call-Return, While, For-Next... u noemt ze maar, zijn herleidbaar tot die drie. Ook dit soort 'programma's' implementeren algoritmen! Dat de wereld zich de laatste vijf jaar zo druk maakt met het toezicht op 'algoritmes', is dus een halve eeuw te laat. Laten we hopen dat er in al die (overheids- en andere) systemen niet al te veel discriminatie is verwerkt.
(17) Na de jaren 50-70 en eind jaren '90.
(18) Noem eens een systeem waar de overheid niet in discrimineert.
(19) Social media krijgen betaald voor uw gegevens, dús zijn ze wat waard. Wat ziet u ervan terug? Verkokering (filter bubble)? Dat is inbreuk op privacy want de keuzevrijheid belemmerend.
(20) Dat eindelijk ontmaskerd is als nauwelijks verholen opvolger van Operations Research en daarvoor Scientific Management: Alles voor het terugdringen van afwijkingen, terwijl de klant juist meer flexibiliteit blijft vragen.
(21) Zie bijvoorbeeld boek: Autonomy The Quest to Build the Driverless Car and How It Will Reshape Our World van Lawrence Burns
(22) Wetende dat tot in de meest biodynamische methoden het platspuiten met kopersulfaat gewoon 'mag'. Dat is vreemd hè, want kopersulfaat is best agressief chemisch en vervuilt de bodem.
(23) Eenieder die weet wat proeven inhoudt, weet dat niet 'drinken' laat staan 'grote hoeveelheden drinken' bedoeld is!

Authors: 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.

Het begint met bewustwording

Hoe ver zijn we daar inmiddels mee?

Deel 1 van drieluik 'Onderzoek naar de human factor in informatiebeveiliging'

Tijd voor een nieuw drieluik over cyberveilig gedrag. Omdat de aanvallen op de menskant in cybersecurity steeds geavanceerder worden, is het belangrijk om ook continu te blijven streven naar vernieuwende manieren om mensen weerbaar te maken. Dit drieluik beschrijft de resultaten van nieuw onderzoek naar de menskant van informatiebeveiliging. In dit eerste deel wordt aandacht besteed aan het huidige kennisniveau: Wat wéten mensen tegenwoordig wel en niet over cybersecurity?

De resultaten van het in de lead aangehaalde onderzoek, geven waardevolle inzichten in wat je kunt doen om het gedrag van medewerkers veiliger te maken. Nog vaak wordt er standaard gegrepen naar pogingen om regels te communiceren, zoals e-learnings, informatieve posters of awarenesstrainingen. Dit is echter alleen zinvol als ook echt blijkt dat die kennis ook daadwerkelijk ontbreekt. Is dat nog wel het geval?

Niet weten of niet doen?

Je wéét dat je niet mag appen in de auto, maar betekent dat ook dat je het nooit doet? Je wéét dat je genoeg moet bewegen en op tijd naar bed moet (zonder schermpje), maar doe je dat altijd? In ons dagelijks leven zien we overal voorbeelden van gedrag dat niet strookt met regels die we kennen, of met wat we weten dat goed voor ons is. Dat mensen zich niet volgens de regels gedragen lijkt een geaccepteerd feit; er is niemand die vreemd opkijkt als een voetganger snel even oversteekt terwijl het licht nog op rood staat maar er verder geen verkeer aankomt. Anderhalf jaar lang zagen we onze minister-president worstelen met het meekrijgen van de bevolking om de opgelegde regels na te leven; via aanspreken op verantwoordelijkheid, motiveren door te zeggen dat we er bijna zijn, streng worden als het niet goed ging. Uit alles mag duidelijk zijn dat menselijk gedrag zich niet makkelijk laat sturen.

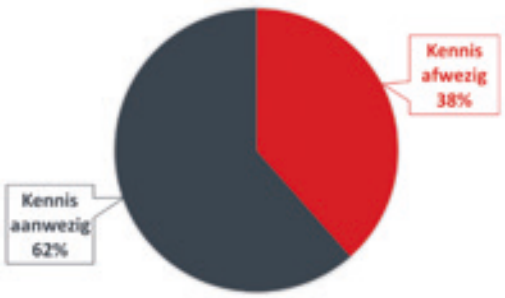
In de wereld van informatiebeveiliging lijkt dit besef maar langzaam door te dringen. Heel lang is ingezet op het communiceren van de regels. Communicatiecampagnes, trainingen en e-learnings werden ingezet om medewerkers te leren wat er van ze verwacht wordt. Voor het stuk daarna was nauwelijks aandacht. Maar zoals bij alle bovenstaande voorbeelden, is het weten van de regel geen garantie voor het bijbehorend gedrag. Wéten mensen het niet, dan moeten we het ze leren. Maar als ze het wél weten en ze doen het niet, dan volstaan communicatiecampagnes en leerinitiatieven niet meer, dan moeten we aan de slag met andere acties.

Hoeveel wéten mensen eigenlijk over informatiebeveiliging?

Om inzicht te krijgen in het kennisniveau ten aanzien van informatiebeveiliging, hebben wij data van onze nulmeting van twintig organisaties in de zorgsector gecombineerd. Daarmee kwamen we op een totaal van 1155 respondenten. De meting bestond uit een online vragenlijst die was opgesplitst in verschillende delen. Voor dit artikel richten wij ons op het kennisgedeelte van de studie. Om kennis te meten, zijn door cybersecurity experts vijftien onderwerpen geselecteerd, gebaseerd op ISO, NIST en NEN-richtlijnen. Voor elk van deze onderwerpen is vervolgens een (meerkeuze-)kennisvraag ontwikkeld die door experts vanuit verschillende vakgebieden is getoetst.

Allereerst het overall resultaat. Wanneer we kijken naar het gemiddelde over de vijftien onderzochte onderwerpen, zien we dat in 38% van de gevallen, mensen het verkeerde antwoord hebben gegeven op de kennisvraag. In 62% van de gevallen wist men wel het juiste antwoord. Kennis ontbreekt dus gemiddeld in iets meer dan één derde van de gevallen.

De bovengenoemde 38% is een gemiddelde. Opvallend was een grote spreiding tussen verschillende onderwerpen: voor sommige onderwerpen is het kennisniveau aanzienlijk hoger dan op andere onderwerpen. Dit varieert zelfs van 15% van de respondenten die het goede antwoord wist tot 96%. Interessante materie om verder in te duiken, omdat hieruit blijkt dat er onderwerpen zijn waarover we mensen dus vooral niet meer hoeven 'lastig te vallen' met communicatie omdat blijkt dat ze het echt wel weten. Tevens geeft het inzicht in waar de kennishiaten nog wél zitten. Dit stelt ons in staat om mensen dus veel gerichter te voorzien van díe kennis die nu nog ontbreekt, en ook alleen maar van díe kennis.



Figuur 1 - Kennis gemiddeld over 15 onderwerpen.

Wat weet men al wel?

De resultaten in tabel 1 laten zien dat voor vijf onderwerpen het kennisniveau boven de 80% ligt. Met andere woorden: voor vijf onderwerpen kunnen we stellen dat men het over het algemeen wel weet. Voor deze onderwerpen heeft het herhalen van de regels dus niet veel toegevoegde waarde. Het betreft de onderwerpen clean desk, het vergrendelen van je computer bij het weglopen, het aanspreken van een onbekende zonder (bezoekers)pas, het gebruiken van een sterk wachtwoord en het gebruiken van veilige of goedgekeurde tools voor videoconferencing.

Onderwerp	Kennisniveau
Clean desk	96%
Computer vergrendelen	88%
Onbekende aanspreken	82%
Sterk wachtwoord	82%
Videoconferencing	80%

Figuur 2 - Tabel 1.

Opvallend is dat de meeste van deze onderwerpen gemeen hebben dat ze gaan over zaken die tegenwoordig algemene kennis betreffen. Mensen hoeven niet per se bij de onderzochte organisaties te werken om te weten wanneer zij hun computer moeten vergrendelen. Sterker nog, deze vijf onderwerpen zijn inmiddels zo bekend dat de kans groot is dat bij een straatinterview, mensen ook de goede antwoorden geven. Dit komt omdat we gelukkig steeds wijzer worden op het gebied van cybersecurity! Waar tien jaar geleden mensen nog geld overmaakten naar een zogenaamde Nigeriaanse prins om aanspraak te maken op een erfenis, is het bewustzijn over de dreigingen de afgelopen jaren sterk toegenomen. Dat zien we duidelijk terug in deze cijfers. Belangrijke bevindingen want zo weten we waar we onze kennisinspanningen níet meer op hoeven te richten!

Wat weet men nog niet?

Ondanks het toenemende cyberbewustzijn, zien we dat er ook nog onderwerpen zijn waar de respondenten veel lager scoorden op aanwezige kennis. Voor deze onderwerpen is het dus van belang om mensen wél meer te leren en instrueren, zodat hun kennisniveau stijgt. Specifiek gaat dit over het herkennen of een URL naar de correcte of veilige website verwijst en over het herkennen van phishing.

Onderwerp	Kennisniveau
Herkennen URL	15%
Herkennen phishing	23%

Figuur 3 - Tabel 2.

Opvallend is dat beide onderwerpen waar de respondenten laag op scoorden, praktisch toegepaste onderwerpen zijn met een technische component. Op basis van deze data kan gesteld worden dat dit het gebied is waar mensen nog het meest behoefte hebben aan instructie. Aan de slag dus, laten we de mensen dit gaan leren. Belangrijk hierbij is wel te begrijpen dat leren en instrueren op veel verschillende manieren kan. De meest simpele vorm van leren bestaat uit het communiceren van de regels. Dit kan kort zijn, bijvoorbeeld middels een poster met een paar regels, of uitvoeriger in bijvoorbeeld een uitgebreide instructie. Maar naast het communiceren van regels, zijn er meer vormen van leren.
Een belangrijke leervorm in dit kader is trainen: Het aanleren en oefenen van nieuw gedrag. Waar communiceren stopt bij het zenden van de regels, gaat trainen verder doordat het nieuwe gedrag meer wordt ingeslepen. Door iets meer te doen en door feedback te krijgen, worden mensen beter. Vergelijkbaar aan trainen van een bepaalde sport. Juist deze praktische onderwerpen als het goed kunnen 'lezen' van een URL en het herkennen van phishing, lenen zich uitstekend voor training. Leer mensen eerst de basis door ze de nodige kennis te geven

en laat hen daarna aan de hand van voorbeelden oefenen om deze kennis toe te passen.

En de overige onderwerpen?

Hierboven hebben we toegelicht welke onderwerpen zeer hoog en zeer laag scoren op kennisniveau. Voor de overige zeven onderwerpen uit onze meting is een gemiddelde score te zien; tussen de 45% en de 71% van de respondenten gaven het goede antwoord. Het betreft hier de onderwerpen: het melden van incidenten, het delen van informatie per e-mail, het gebruiken van een uniek wachtwoord voor je werkaccount, het kennen van je handelingsperspectief nadat je informatie naar de verkeerde persoon hebt gestuurd, het gebruik van tweefactor authenticatie, het veilig opslaan van gegevens en het delen van vertrouwelijke bestanden.

Onderwerp	Kennisniveau
Incidenten melden	45%
Informatie delen per mail	55%
Uniek wachtwoord	56%
Handelen na datalek	60%
Tweefactorauthenticatie	60%
Veilig opslaan gegevens	66%
Delen vertrouwelijke bestanden	71%

Figuur 4 - Tabel 3.

Is er een overeenkomst te zien tussen deze onderwerpen? Jazeker: het betreft hier onderwerpen die merendeels te maken hebben met het beleid van een organisatie: Dat bepaalt immers welke incidenten gemeld moeten worden en waar, welke informatie wel en niet per mail gedeeld mag worden, welke andere opties voor veilig delen er zijn, wat de regels zijn voor tweefactor authenticatie enzovoorts. We zien hier dat in de onderzochte organisaties wel degelijk aandacht is geweest voor het verhogen van bewustwording op deze beleidsonderwerpen.
Deze data laten zien dat mensen dus best wat kennis hebben van deze beleidsonderwerpen, maar dat deze kennis nog niet heel hoog is. Om het juiste gedrag te kunnen vertonen, is het wel belangrijk dat men goed weet wat er verwacht wordt. Dat pleit ervoor dat ook deze onderwerpen nog wat aandacht mogen krijgen op het kennisvlak, zij het minder dan de operationele onderwerpen die we hierboven beschreven.

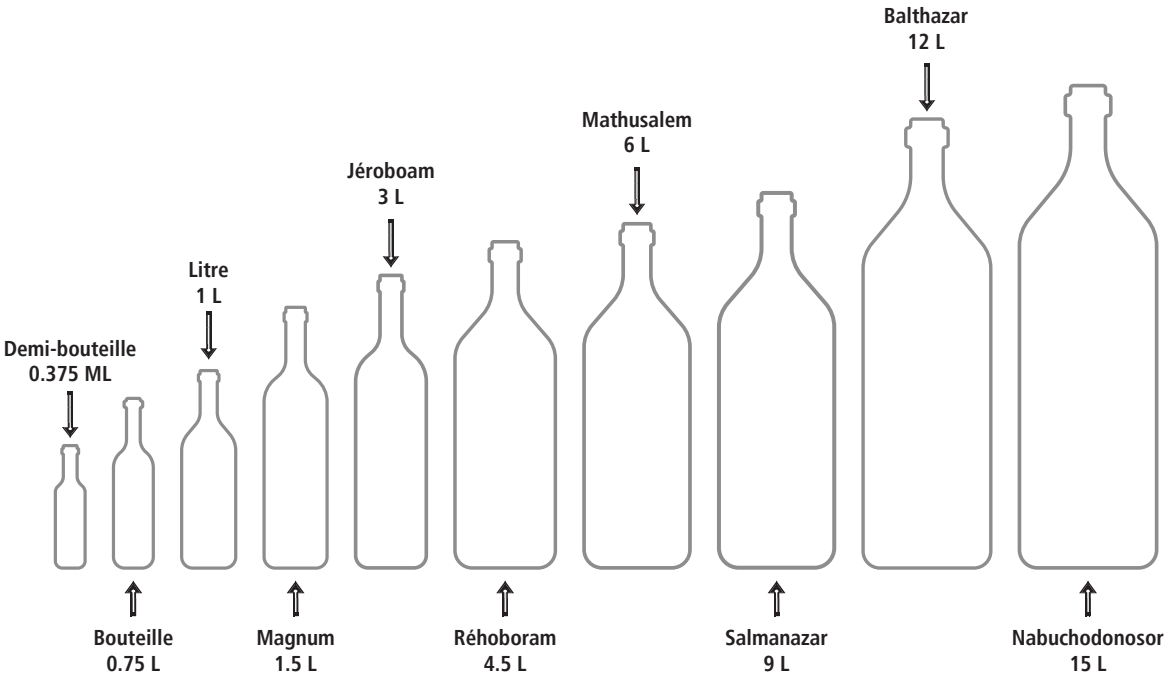
Wat kan ik met deze data?

De resultaten die in dit artikel beschreven worden, geven inzicht in het huidige kennisniveau op vijftien verschillende onderwerpen in informatiebeveiliging. Daarmee geven deze data richting aan de stappen die genomen kunnen worden om medewerkers verder cyberweerbaar te maken. Zo maakt het duidelijk welke onderwerpen nu nog kennisaanbod behoeven. Ook maakt het duidelijk op welke onderwerpen de kennisinitiatieven zich juist minder hoeven te richten.
Een kanttekening bij deze data is dat ze verzameld zijn bij twintig organisaties in de zorgsector. Uiteraard geven deze resultaten geen uitsluitsel dat het beeld bij organisaties in andere sectoren, of zelfs bij andere organisaties binnen de zorg, precies gelijk is. Om voor een specifieke organisatie aan de slag te gaan, is het dus interessant om te starten met een dergelijke meting. Dit voorkomt namelijk dat medewerkers lastig worden gevallen met e-learnings over zaken die zij al lang weten, wat zelfs tot weerstand kan leiden. Tevens zorgt het ervoor dat er wel gericht kennis kan worden aangeboden specifiek op díe gebieden waar kennis nog mist. Dat is dus veel efficiënter.

Betekent weten ook doen?

De resultaten van dit onderzoek geven dus een duidelijk beeld van het huidige kennisniveau op het gebied van informatiebeveiliging, uitgesplitst naar verschillende onderwerpen. Van hieruit is duidelijk welke onderwerpen nog aandacht behoeven op het vlak van kennisverhoging. Maar hoe zit het met de mensen die deze dingen al wél wisten? Dóen zij ook het juiste? Dus voor die onderwerpen waar het kennisniveau boven de 80% is? Zijn we daar dan klaar, zien we dat ook terug in gedrag? Het tweede deel van dit drieluik beschrijft onderzoek naar de kloof tussen kennis en gedrag in informatiebeveiliging: betekent weten ook dat mensen het doen, of zitten daar nog andere factoren tussen?

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



BLOG

Wat ik weet uit de wijnkelder

Ik leerde van mijn militaire dienstmaat Dick drie dingen over wijn, die verrassend bruikbaar zijn voor een security officer.

1. Wat ruik je in Rioja?

2. Zijn beste klant betaalde nooit zelf voor wijn

3. Ziekenhuisflesjes

Na werktijd ging ik uit kantoor regelmatig naar de wijnwinkel van Dick in Apeldoorn. Dick had sinds de zomervakantie in onze diensttijd een Italiaanse vriendin, verhuisde later naar Italië en trouwde daar met haar. In Nederland had hij zelf een ERP-systeem voor kerstpakketten gebouwd. Samenstellen van pakketten, inkopen van ingrediënten, bijhouden van voorraad, bijhouden van bestellingen voor pakketten, plannen van het inpakken, versturen van facturen en aanmaningen en exporteren van data naar het boekhoudpakket. Alles zat erin en het was, eind jaren tachtig, geschreven in Turbo Pascal op een IBM-compatible personal computer. Daar spraken we over, en over haar (Claudia), films, muziek, belasting betalen, onze collega's en wijn. Want Dick had altijd wel iets 'open' dat ik zeker even moest proeven voordat we samen naar de Italiaan (Roma), de Chinees (Fong Sheng) en/of de bioscoop (1) gingen.

Wat ruik je in deze Rioja?

Ik dacht dat die Rioja naar lavendel of vanille zou ruiken of dat je goed kon proeven dat hij in oude sherryvaten opgeslagen was geweest. Of was gemaakt van druiven die aan de westkant (dus zeekant) van de heuvel groeiden, zodat er een zweem van zilte doorheen sluimerde. Neen, zei Dick, je doet te moeilijk, je ruikt poep, koeienmest, de boerderij! En daarom is het zo lekker bij rood vlees. Soms (of: heel vaak) is het antwoord op een vraag simpel en ligt de oplossing van je probleem voor de hand.
Komt de leverancier zelf met een gratis patch voor zijn pakket? Installeren die handel en wel zo vlug mogelijk. Zelf heb je voor je bankzaken allicht een smartphone waarop ook veel dierbare foto's zijn opgeslagen. Die telefoon staat op automatisch bijwerken van patches, je hebt er geen omkijken naar. Je desktopcomputer waarmee je regelmatig (nou ja, drie tot vier keer per jaar) podcasts maakt, staat op automatisch downloaden van patches en handmatig installeren. Dat doe je ook bijna elk kwartaal. En de oude laptop, die je alleen gebruikt voor je belastingaangifte omdat je daar de eerdere aangiftes, aanslagen en bewijzen van insturen op bewaart? Die is altijd uit en hangt niet eens aan het internet! Dus die wordt één keer per jaar (eind april...) bijgewerkt.

Van die gekozen updatefrequenties kun je iets vinden: die nauwkeurig ingesproken podcast verliezen is vervelender dan één van vele digitale foto's. En de opgelegde belastingaanslag op basis van je eigen aangifte is weer belangrijker dan die podcast. Maar je hebt tenminste een plan met motivatie hoe je met software-patching omgaat. Dat moet je als organisatie ook hebben. Maak het schema niet ingewikkelder dan nodig.

Ruilhandel

Dick kocht regelmatig een complete wijnkelder uit een erfenis. Ik vroeg dan of er bijzonder en duur 'spul' bij zat. Dick vertrok zijn gezicht en leerde me dat ik tegen klanten 'kostbaar' moest zeggen. Wie kocht nou zo'n fles van 300 gulden (2), die in een restaurant vier keer over de kop ging en daar 'niet goedkoop, maar erg, erg lekker' zou zijn, wilde ik weten. Dick onthulde dat (eind jaren tachtig!) een Apeldoornse tandarts aan ruilhandel deed. Voor inlays, kronen en bruggen liet hij zich betalen in veel en exclusieve wijn. Hij bestelde het zelf, maar de rekening ging naar de patiënt, die bij Dick zijn kerstpakketten kocht. Die tandarts kreeg dus ook een 'kerstpakket', dat dan wel in april of augustus en zonder doosje crackers of tosti apparaat bij hem werd afgeleverd. Destijds hadden tankstations een 'verdiesel'-knop op de kassa. Truckchauffeurs konden daarmee de prijs van een slof sigaretten of geïllustreerd tijdschrift laten omrekenen naar liters diesel. Die dan samen met de echte tankinhoud als totaalbedrag op de bon kwamen en dus door de opdrachtgever of de baas betaald werden. Niet zwart, niet zoals bedoeld, niet helemaal ethisch, maar wel echt eighties. Voor mij als software-ontwikkelaar was zoiets toen een grappige feature van het pakket. Voor de registeraccountant in opleiding die ik ook was een gruwel, vanwege het verschuivingsgevaar in de opbrengsten en de bedreiging van de rechtmatigheid van kosten. Later als security officer kon ik deze voorbeelden echter goed gebruiken als motivatie voor 'negatief testen'. Namelijk expliciet vaststellen dat het te testen systeem, behalve de gewenste functionaliteit, géén dingen doet die juist niet de bedoeling zijn (zoals export naar Excel van alle persoonsgegevens in de totale GGD-database). Als positief voorbeeld van ruilhandel heb ik ervaren dat het 'om niet' uitwisselen van security intelligence (lees: informatie, ideeën, inlichtingen en innovatie) tussen branchegenoten voor alle partijen nuttig en positief kan zijn.

Ziekenhuisflesjes

Een grote eettafel in de wijnwinkel stond vol met een recent gearriveerde wijncollectie. Ik vroeg Dick of er een klein, betaalbaar flesje bij was dat ik dan wilde kopen, als aspirant bon vivant. "Ah", zei hij, "zo'n ziekenhuisflesje?" Een wijnfles van 37,5 cl bevat genoeg voor twee ruim gevulde glazen en een 'demi' is daarmee inderdaad een mooie hoeveelheid bij een ziekenhuismaal.

In mijn beperkte levenservaring destijds lagen familieleden in het ziekenhuis voor iets ernstigs en gold er altijd een streng dieet. Ik had er daarom tot dan toe nooit aan gedacht dat je in een dergelijke ernstige situatie, toch kunt proberen er maar het beste van te maken. En dus kunt kiezen om grote inspanning gepland af te wisselen met (grote) ontspanning. Zoals dat je bij bestrijden van een grote besmetting met ransomware, toch nog wel een grapje kunt maken om de spanning te breken en de teamgeest te versterken. En dat je – wanneer het hele weekend doorgewerkt moet worden om het probleem op te lossen – het eigen slaapmanagement op orde moet houden. Zeker wanneer er ogenschijnlijk geen tijd beschikbaar is om te slapen.

Van zijn drie security-lessen zijn die ziekenhuisflesjes misschien wel de nuttigste tip. Grazie Dick! Saluti.

Auteur: Renco Schoemaker is senior adviseur informatiebeveiliging & privacy en mede-eigenaar bij IB&P. Hij is werkzaam bij een G4 gemeente als senior information security officer en waar hij de ENSIA verantwoording coördineert. Eerder was hij adviseur en CISO (a.i.) bij diverse gemeenten. Renco is bereikbaar via r.schoemaker@ib-p.nl.

Het NIST CyberSecurity Framework als kans?

Het CyberSecurity Framework (CSF) is ontwikkeld door het NIST, ofwel het National Institute of Standards and Technology. Onder Obama werd in 2013 aan het NIST de opdracht gegeven een cybersecurity framework te ontwikkelen. En onlangs door Biden opnieuw. Maar wat kan je er als Nederlandse, overheidsorganisatie mee en hoe verhoudt het zich tot de BIO en de ISO27000 reeks?

Allereerst het verschil tussen een framework en een standaard. Een framework is een conceptuele structuur die inzicht geeft in hoe de onderlinge componenten zich tot elkaar verhouden. Vaak krijg je dit inzicht doordat een framework een visuele weergave bevat. Je kunt de vergelijking met de fysieke wereld maken: in de bouw houdt een framework het gebouw overeind doordat individuele componenten zich tot elkaar verhouden. Maar aan de hand van een framework kun je nog weinig zeggen over het eindresultaat. Frameworks vertellen je iets over de grote lijnen, de context en vooral: samenhang. Enkele voorbeelden van security gerelateerde frameworks: NIST CSF, COBIT en COSO.

Standaarden dienen een geheel ander doel, namelijk standaardisatie van best practices. In standaarden vind je dus concreet beheersmaatregelen waaraan je kunt of wilt voldoen. Vanzelfsprekend zijn deze logisch geordend in hoofdstukken, maar verder bevatten ze weinig context. Standaarden vertellen je iets over het wát, alhoewel het 'wat' nog uit te splitsen valt. Enerzijds gaat het over de feitelijk te nemen beveiligingsmaatregelen en anderzijds over het managementsysteem waarbinnen je deze beveiligingsmaatregelen neemt. Enkele voorbeelden van security standaarden voor beveiligingsmaatregelen: ISO270002/BIO, CIS Controls en NIST SP 800-53. Enkele voorbeelden van standaarden voor een managementsysteem: ISO27001 (ISMS), ISO27701 (PIMS) en meer voorbeelden zijn te vinden op de website van het ISO.

Standaarden zijn dus veel voorschrijvender dan frameworks en dat is tevens de reden dat je je wél kunt laten certificeren tegen enkele standaarden, maar niet tegen een framework. Bij overheidsorganisaties gaat het hoofdzakelijk over de BIO - ofwel ISO27002 - maar in toenemende mate ook over het ISMS (ISO27001). Wel is het ISMS lastig 'te pakken' voor velen. Maar je hoort bijna niemand over frameworks, waarom niet?

Kans of afleidingsmaneuver?

De cynicus (in mij) kan stellen dat een framework vooral de aandacht afleidt. Het is informatiebeveiliging in een ander verpakking die afleidt van achterblijvende implementatie van beveiligingsmaatregelen en/of een gebrekkig functionerend ISMS-proces. Van een framework wordt een organisatie niet veiliger, maar beveiligingsmaatregelen wél. Alhoewel in het slechtste geval niet onwaar, valt er meer over te zeggen. Informatiebeveiliging aanvliegen vanuit primair, of zelfs uitsluitend compliance is een 'dead end' wat mij betreft. Je schuift de BIO of ISO27002 nu eenmaal niet via de achterdeur naar binnen. Informatiebeveiliging aanvliegen vanuit primair, of zelfs uitsluitend risicomanagement wordt vooral een heel láng verhaal. En deels onzinnig ook: je hebt al een best practice qua maatregelen, maar gaat die toch steeds identificeren via tijdrovende risicoanalyses. Maar hoe dan wél?

Allereerst door de risicoanalyses zo gestructureerd en afgebakend te houden als mogelijk en qua maatregelen uitsluitend te putten uit wat er al is. Wat dat betreft is de Informatiebeveiligingsdienst (IBD) als CERT van de lokale overheden in Nederland je beste vriend; zij voorstaan mijns inziens deze werkwijze. Maar ook degene die deze werkwijze al jaren volgt heeft het niet makkelijk. Immers, hoe krijg je dat verrekte management en bestuur écht aangehaakt? Talloze beveiligingsincidenten en datalekken ten spijt, lukt het vaak niet. En dat moeten we vooral onszelf aanrekenen, meen ik.

En precies dáár biedt een framework een kans. Ik bezie het als het pragmatische midden tussen de lange, tijdrovende route van het managementsysteem en de kille, weinig tot de verbeelding sprekende route van compliance. Een framework biedt je de kans om op een geheel andere wijze het verhaal en belang van informatiebeveiliging over te brengen. Maar eerst iets meer over het NIST Cyber Security Framework.

CSF: core, tiers & profiles

Het CSF bestaat uit drie componenten: de core, tiers en profiles. Laten we starten bij het belangrijkste: de kern (core) van het framework. Die bestaat uit functies en (sub)categorieën. Er zijn vijf functies: Identify, Protect, Detect, Respons en Recover. Die termen moet je als lezer toch aardig kunnen plaatsen in de wereld van informatiebeveiliging. En niet onaardig: in de nieuwe, komende ISO27002 norm zal er ook een referentie terug zijn naar deze vijf CSF functies.

Afbeelding 1 – De vijf functies van het CSF.

Alle functies zijn onder te verdelen in categorieën: zo valt Identify uiteen in Asset Management, Business Evironment, Governance, Risk Assessment, Risk Management Strategy en Supply Chain Risk Management. Elk van deze categorieën bevat subcategorieën en daar wordt het redelijk concreet. Zo heeft de functie Identify (ID) de categorie Asset Management (AM) een subcategorie ID.AM-1 die als volgt luidt (vrij vertaald): Fysieke apparaten en systemen binnen de organisatie worden geïnventariseerd. Iedere subcategorie heeft referenties naar o.a. ISO27001, Bijlage A en via deze bijlage dus naar ISO27002/BIO. Het CSF bevat naast de 'core' ook nog 'implementation tiers'. Alhoewel er steeds wordt gesteld dat dit géén volwassenheidsniveaus zijn, bezie ik ze toch als zodanig. Om dit artikel 'on topic' te houden ga ik hier nu verder niet op in, evenmin op de profiles – wat toepassingen van het CSF zijn in specifieke sectoren.

Reframe het frame

Wat mij betreft kan het NIST CSF je helpen het 'grote verhaal' over informatiebeveiliging richting het (hoger) management en het bestuur opnieuw en beter te framen. Blijf weg uit de compliancehoek en mijd het lastige, ongrijpbare managementsysteem. Het CSF vervangt geenszins je managementsysteem of de BIO – deze standaarden zijn er niet voor niets – maar het framework helpt je dit alles beter uit te leggen. De vijf CSF functies vragen nauwelijks voorkennis en de eenvoud van volwassenheidsniveaus spreekt doorgaans aan. Dus het NIST CSF is wat mij betreft zeker een kans. Maar je zal je wel goed moeten inlezen om alle ingrediënten van het verhaal overtuigend te kunnen brengen. Ik hoop dat dit artikel daar positief aan heeft bijgedragen. IB&P heeft ruime ervaring met het implementeren van standaarden, managementsystemen en frameworks op het gebied van informatiebeveiliging en privacy, specifiek bij overheidsorganisaties.

Auteur: Chris de Vries is redacteur van iB-magazine. Hij werkt als zelfstandige professional werkzaam onder de naam De Vries Impuls Management. Chris is bereikbaar via e-mail: impuls@euronet.nl. Het artikel is op persoonlijke titel geschreven.

Afbeelding 1 - De setting van de cyberoefening.

Overheidsbrede cyberoefening

Het is 1 november, het weer is redelijk en de A1 weer jammer genoeg vertrouwd druk. Het zou een dag als zoveel andere kunnen zijn, ware het niet dat het fictieve Sociaal Werkbedrijf Bison juist vandaag erachter komt dat zij gehackt zijn. Bison vertegenwoordigt zeven gemeenten met 300.000 inwoners en draagt o.a. de verantwoordelijkheid voor 4.500 uitkeringen en de salarisadministratie rondom detacheringen. Een crisis van de eerste orde dus.

Met deze uitdaging wordt een crisisteam geconfronteerd bestaande uit de bekende C-managers, nu voor deze gelegenheid gerekruteerd uit het Nederlandse bedrijfsleven, de overheid en security-specialisten. Ze zijn allen naar Amersfoort gekomen om dit avontuur voor de camera te spelen. Thuis of op het werk zitten ruim 320 publieksdeelnemers en in de zaal circa 40 genodigden. Ikzelf observeer de oefening om van te leren en om een verslag met de lezers van dit magazine te delen.

De casus is realistisch. Het werkbedrijf zit midden in een transitieperiode waarbij de 'switch' naar de cloud wordt gemaakt, maar men is nog niet klaar (50% gereed) en ook zijn net niet alle kwetsbaarheden op tijd gepatcht. De eerste stap was van de CISO dan ook om alle systemen uit te zetten. Dat brengt mij meteen tot dilemma 1 in een dergelijke situatie: 'zet je de systemen uit of houd je ze actief?'. De overwegingen: moet je als CISO dat besluit zelfstandig nemen of overleg je daarover? Verder, is het belang van een justitieel opsporingsapparaat hoger dan het belang van het werkbedrijf om verdere hack-activiteiten te blokkeren?
Het crisisteam begint vervolgens met een inventarisatie van de risico's. In dit scenario moet men ervan uitgaan dat persoonlijke data (BSN) is buitgemaakt, dat uitkeringen geblokkeerd zijn (net de dag voor de uitkeringsdatum), dat ook de gedetacheerden de hack zullen ervaren en erger nog dat men niet meer beschikt over actuele data! Ook wordt meteen aangekaart dat er een 'ransomware note' met de eis van € 300.000,00 is gevonden en of men in onderhandeling met de dader(s) moet treden. De crisisteamleider sprak daarbij de verschillende teamleden afzonderlijk aan en vroeg elk van hen dienaangaande te adviseren. Het gesprek verliep daardoor civiel en geordend. Opvallend was ook dat de crisisteam spelers een goede balans wisten te vinden in de interne en externe communicatie. Wat ik wel miste was het fictief op tafel leggen van een crisisplan en het werken vanuit een dergelijk plan. In de spelpraktijk leek men een

dergelijke route wel te volgen.
In een verdere fase van het spel kwam de keten aan bod. Er werd bediscussieerd de ketenpartners te informeren, na te gaan in hoeverre zij getroffen waren door deze hack en af te stemmen of een gezamenlijke actie nodig c.q. mogelijk is.
Aardig feitje tussendoor; het PvIB is enige jaren terug intensief bezig geweest de ketenrisico's in beeld te brengen en te zien of er coördinatie mogelijk zou zijn tussen de diverse 'stakeholders'. De noodzaak wordt alom onderkend, maar de uitvoering is een zaak apart. Benieuwd hoe de stand van zaken nu is. Een ludieke reactie vanuit de toeschouwers thuis was, om maar alvast Chinese maaltijden te bestellen, want het zal nog wel even duren. Na de pauze ging de casus verder. Nu was bekend dat zeker van 1.000 inwoners data was gestolen, waaronder naam, geboortedatum en BSN. De 'deadline' van de melding aan de Autoriteit Persoonsgegevens (AP) kwam aan de orde alsook dat men onderhandelde met de aanvaller en het losgeld had weten terug te dringen tot € 200.000,00 De vraag werd door de spelers gesteld of de gemeenten zouden instemmen met betaling. Hier komt voor mij dilemma 2 aan de orde. De politie dringt bij bedrijven erop aan nooit losgeld te betalen. Binnen de overheid wordt er verder over nagedacht om betaling van losgeld vanuit verzekeringsmaatschappijen (verzekerde gebeurtenissen) te verbieden. Consequentie: bedrijven dragen alle kosten en de reputatieschade; zij kunnen die niet verhalen. Wat nu bij overheidsinstellingen? Als zij zouden betalen dan zou voor de overheid blijkbaar andere regels gelden en alle schade die zij oplopen (behalve de reputatieschade) verrekenen zij via belastingen, retributies en toeslagen aan de burger door. Dit lijkt mij zeer onredelijk en dus een moreel dilemma.

Persoonlijke mening: conform het principe van 'gelijke monniken, gelijke kappen' zou ook de overheid de pijn zelf echt moeten voelen en dat zou alleen zo zijn als de getroffen overheden gekort worden op hun budgetten zonder het recht tot herbestemming van budgetten of het aanvullen uit andere bronnen. Dit zou dan door de Rekenkamer gecontroleerd moeten worden.
Voordeel: de overheid voelt de pijn en zal alles op alles zetten om de keten te versterken en dus professionele steun te gaan bieden aan de zwaksten in de keten, t.w.: slecht functionerende overheden, maar ook hun toeleveranciers zoals het Midden- en Kleinbedrijf, die te klein zijn of niet beschikken over de professionaliteit om zich te wapenen tegen superieure hackers (waaronder statelijke actoren) met grote buidels.

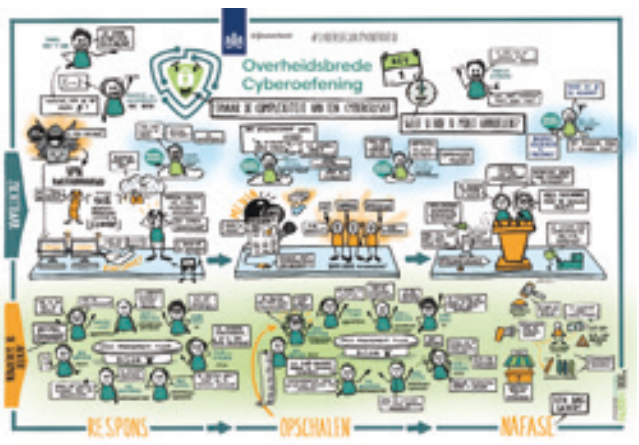
Boeiend was dat tijdens een pauze in het spel de heer Dennis Lacroix van de gemeente Hof van Twente openhartig verhaalt van zijn ervaringen met de hack bij hen. Zij hebben niet onderhandeld met de aanvaller en zij hebben bedrijfsmatige – en risico afwegingen gemaakt. Hun uitgangspunten: 1. wat zijn de belangrijkste pijnpunten; 2. wees transparant en 3. werk in scenario's en volg ze (ijk ze meteen). Inschakeling van de politie zagen zij als een moreel besluit. In deze spelcasus kwamen ook de gemeenten tot het besluit om niet te betalen. Gezien de diefstal van persoonlijke gegevens moest men de burger daarop attenderen en zeker de kwetsbare mensen daaronder. Vandaar dat besloten werd tot een getrapte aanpak en het rechtstreeks bereikbaar zijn voor deze burgers. Men formuleerden toen samen op welke wijze men naar buiten zouden treden – door middel van een persconferentie – en wat men zou mededelen. Ook dat het gebrek aan actuele data ertoe zou kunnen leiden dat uitgevoerde betalingen onjuist zouden zijn. Zo dat het geval dan zou laagdrempelig en opgeschaalde toegang tot gemeente en werkbedrijf geborgd zijn.

Aan het einde van deze oefening werden de deelnemers naar hun bevindingen gevraagd. De belangrijkste constateringen:

- Houd elkaar vast/ steun elkaar;
- Oefen het teamwerk;
- Zorg dat er ook van buiten naar binnen wordt gekeken;
- Focus op alle burgers, persoonlijke focus daar waar het verkeerd gaat;
- Luister naar de experts en
- Oefen, oefen en oefen.

Alles bij elkaar een leuke en leerzame middag en in vergelijking met andere oefeningen (vanuit het bedrijfsleven en de beveiligingssector) een verrijkende blik in de keuken van onze overheid. Goed om het denken ook van die kant te leren kennen.

Voor een visuele notulering zie navolgende tekening:



Afbeelding 2 - Visuele notulering Overheidsbrede Cyberoefening.

Laatste weetjes:

-de vierde Overheidsbrede Cyberoefening vindt plaats op 31.10.2022
-voor wie de training wil terugzien:
https://www.weerbaredigitaleoverheid.nl/inloggen/ (wachtwoord vereist!)

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.

Artificial Intelligence een nieuwe bedreiging?

Kunstmatige intelligentie, algoritmen en andere manieren om van ruwe data nuttige informatie te maken, winnen steeds meer terrein. Menig organisatie werkt met Business Intelligence afdelingen en/of werkt steeds meer data gedreven. Dat geldt niet alleen voor organisaties, maar ook voor (digitale) criminelen. Moeten wij als informatiebeveiligers ons zorgen maken? Een reflectie van een deel van de redactie.

In oktober 2021 was in het nieuws dat bij een bankroof in de Verenigde Arabische Emiraten gebruik gemaakt is van AI om de stem van de bankdirecteur na te maken (1). In de basis is dit voorbeeld natuurlijk een vorm van CEO-fraude, maar er zijn natuurlijk andere dreigingen die voortkomen uit meer en meer AI. Zo kunnen algoritmes kritisch worden voor de bedrijfsvoering (beschikbaarheid) of is de gewenste werking van algoritmen of termijn niet meer te achterhalen (integriteit).

Samen slimmer - Lilian Knippenberg

Digitalisering gaat harder dan ooit en onze organisaties werken meer en meer op data of zelfs alleen maar op data. In de basis


Chris de Vries


Fook Hwa Tan


Lilian Knippenberg

denk ik dat alle digitale ontwikkelingen steeds terug te voeren zijn op bekende dreigingen, zoals de genoemde CEO-fraude. Het probleem met de snelle doorontwikkeling van technieken is alleen dat de digitale producten die je onder ogen krijgt voor gemiddelde mensen niet meer van echt te onderscheiden zijn. We moeten dus gezamenlijk toe naar meer bewustzijn en veiligheidsprocedures: MFA in techniek én in procedures. Spreek af dat je die CEO terugbelt op het jouw bekende nummer in plaats van het nummer waar hij je belde. Zorg voor het 'meer ogen'-principe. Daarnaast zijn algoritmen natuurlijk net zo goed 'systemen' die een classificatie moeten krijgen op B, I en V. Qua integriteit hoop ik eigenlijk op een soortgelijke actie als bij de ontwikkeling van aparte ontwikkeling (Dev) en operatie (Ops) van systemen naar één team dat beiden doet (DevOps) en daarna naar een veilige variant daarvan (DevSecOps) waar de ontwikkelaars en beheerders samen invulling geven aan security by design en by default. Ik introduceer dus alvast bij deze de Artificial Secure Intelligence (Asecl). Met het ontzettend wijdverbreide gebruik van AI worden we daar allemaal slimmer van!

Menselijke toets achteraf - Chris de Vries

Artifical Intelligence (AI) oftewel in goed Nederlands 'Kunstmatige Intelligentie' is "de natuurlijk domme poging van slimme wetenschappers om menselijke intelligentie in een computer na te bootsen." (2) Ik voel wel wat voor deze definitie, want er zijn heel wat slimme mensen die ooit eens over Frederick Winslow Taylor's wetenschappelijke bedrijfsvoering hebben gelezen en daarbij de 'time & motion studies' als basis voor efficiëntie hebben leren kennen. De mens is altijd bezig om iets uit te vinden dat efficiënter is en minder werk van hemzelf vergt.

Et voila, de geboorte van de 'black box'. In een set van programmatuur wordt het besluitvormingsproces vormgegeven en vervolgens hoeft de mens zelf niet meer te beslissen. Voorbeelden uit de praktijk: 'De Bazel I t/m 3' besluiten (bankwezen) en de toeslagenaffaire (de belastingdienst c.q. de overheid).

In het eerste geval is voorgeschreven hoe banken hun vermogen op peil moeten houden en hoe risico's onderkend, geanalyseerd en beheerst worden. Op zich een lovenswaardig streven, maar in ons land leidde het er wel toe dat het MKB niet financierbaar is geworden. De toeslagenaffaire: een affreus gebeuren dat met de dag meer schandalige gevolgen laat zien en nog steeds niet goed opgepakt wordt. Laat staan dat de verantwoordelijkheid wordt genomen.
Beide zaken zijn 'black boxes' gebaseerd op efficiëntie, perfect werkende computers en verworpen menselijkheid. Artificial Intelligence heeft de toekomst, maar ik vrees bij blinde toepassing voor de mensheid.Ik onderschrijf dus de stelling van mijn mede-redactielid Lilian dat, Artificial Secure Intelligence een moeten is, maar dan moet Secure ook neerkomen op de altijd noodzakelijke menselijke toets achteraf of in het voorkomende geval het mogelijk maken van aantekening geen bezwaar.

Ingehaald door technologie - Fook Hwa Tan

We zien in ons dagelijks leven steeds meer gebruik van AI, ML en in het algemeen algoritmen, zoals in wasmachines, waterkokers of rijstkokers. Maar het geldt natuurlijk ook voor het laten zien van advertenties of ander personaliseringssoftware. Het begon met regels die werden geautomatiseerd, inmiddels heb je beslisbomen die een computer kunnen volgen om tot beslissingen te komen. En natuurlijk heb je de getrainde neurale netwerken die uit data gedrag kunnen destilleren om deze vervolgens te emuleren. Met de nieuwe generatie AI kunnen steeds complexere acties en besluiten worden genomen.
Computers voeren steeds snellere calculaties uit. Hierdoor kunnen steeds kleinere apparaten steeds meer besluiten van mensen overnemen. Met kwantumtechnologie en meer nieuwe technologieën zijn er nóg meer mogelijkheden beschikbaar voor ons om in te zetten.

We zien dus, dat technologie zorgt voor complexiteit en snelheid in nog meer toepassingen. Het gaat inmiddels zo snel, dat wij als mensen niet meer begrijpen wat onze machines doen. We zien dit al bij algoritmes die door onze overheid gebruikt worden om fraude op te sporen of verdachte gevallen te identificeren. Hoe kunnen we bijblijven met technologie als informatiebeveiligers? Het lijkt soms alsof we worden ingehaald door technologie. We moeten dus zorgen dat we qua kennis bijblijven en op de hoogte zijn van alle ontwikkelingen. Als wij de kennis niet najagen, zullen criminelen het wel doen!

(1) https://tweakers.net/nieuws/188220/criminelen-gebruiken-ai-namaakstem-bij-bankroof-van-ruim-30-miljoen-euro.html
(2) Computable, ICT Woordenboek 2003.

Jaaroverzicht

Achter het Nieuws

Wat maakt het BSN-nummer zo bijzonder?	iB2:40
AP: Google Workspace Education voldoet niet aan AVG-regels. Wat nu?	iB4:34
'Wat heeft de invoering van de AVG ons gebracht of gekost?'	iB5:48
Artificial Intelligence (AI) een nieuwe bedreiging?	iB6:36

Boekreviews

Gedoe komt er toch. Zin en onzin over organisatieverandering	iB3:34
Organisatie van de informatiebeveiliging en vertrouwelijkheid van informatie	iB4:18

Column Berry

De meeste dromen zijn bedrog!	iB1:43
Weg, die telefoon	iB2:27
Ik heb niets te verbergen	iB3:29

Column Inge

Thuiswerken	iB1:11
Nooit te oud om te leren	iB2:17
IoT: voor alles een ander wachtwoord	iB3:19
Arwarenesstest: kennis of gedragsmeting?	iB4:23
Klosje tussen de deur	iB5:19

Column Privacy

Safe seks	iB1:07
Een kind mag zich verstoppen	iB2:07
SyRi dood? Welnee het heet nu alleen anders	iB4:07
Stuur eens een brief	iB5:07
Regeldrift en de zucht naar ethiek	iB6:07

Voorwoord

Huis-tuin-en-keukenwerken	iB1:03
Speurtocht	iB2:03
Geheimen	iB3:03
In de prijzen	iB4:03
Drie jaar AVG heeft ons niet onberoerd gelaten	iB5:03
Humor	iB6:03

Artikel van het jaar iB4:32

Het bestuur in beeld

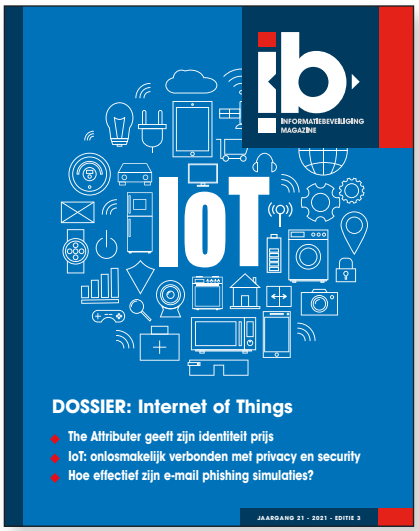
Wij doen ut soamen!	iB1:15
2021	iB2:23

Artikelen

(a) Adriaansen, Beaubine	Internet of Things, onlosmakelijk verbonden met privacy en security	iB3:26
(i) Bakker, Tom, Kagie, Sandra	Co-auteur Data Breach Investigations voor holistische aanpak cybercrime	iB5:04
(i) Bakker, Tom, Kagie, Sandra	'We hoeven niet alles te doen zoals Silicon Valley het voorschrijft'	iB6:04
(a) Bergh, Geoffrey van den, Bruin, Marloes de	Méér met data. Maar wát eigenlijk?	iB5:16
(a) Breuer, William	Voorkom Java-Scriptaanvallen via derden	iB4:08
(a) Cheney, James	Geëmuleerde honeypots in de strijd tegen hackers	iB6:18
(a) Derogee, Maurice	Thuiswerken in (post)coronatijd	iB1:16
(a) Deursen, Nicole van	Hoe effectief zijn phishing e-mail simulaties?	iB3:04
(a) Deursen, Nicole van, Tan, Fook Hwa	De onmeetbare impact van ransomware	iB6:08
(a) Dijk, Rik van	Wat te doen aan kwetsbaarheden in TCP/IP-Stacks?	iB3:23
(a) Genova, Maria	Hoe gevaarlijk is de 'smart' trend?	iB3:20
(a) Gijsen, Bart e.a.	ICT herstelvermogen: de stand van zaken	iB1:26
(a) Jans, Stijn	De voordelen van crowdsourced security	iB1:22
(i) Kagie, Sandra	CISO Dré Lemeir: 'Business as usual, anders klopt er iets niet'	iB1:04
(i) Kagie, Sandra, Bakker, Tom	Gabriel Leperlier: 'Verontrustend, zeker in coronatijd	iB1:19
(i) Kagie, Sandra	Nationaal Cyber Security Centrum: ook voor niet-vitale organisaties?	iB4:04
(a) Kleij, Rick van der, Hof, Tineke	Het is niet mijn verantwoordelijkheid	iB6:12
(a) Knippenberg, Lilian	Privacy podcasts	iB5:24
(a) Knippenberg, Lilian	Security podcasts	iB6:10
(a) Kogenhop, Gert	Bedrijfsimpactanalyse	iB3:08
(a) Laar, Enrico van de	Zie databescherming als kans in plaats van verplichting	iB4:16
(a) Lameir, Dré	Lekker foppen	iB5:31
(a) Maurer, Andres, Metsemakers, Robert	Best practices in access management (part 1 of 2)	iB4:12
(a) Maurer, Andres, Metsemakers, Robert	Best practices in access management (part 2 of 2)	iB5:32
(b) Metsemakers, Robert	Wat spionnen je leren over threat intel analyseren	iB1:32
(b) Metsemakers, Robert	Sinterklaas, verlanglijstjes en de security threat heatmap	iB2:30
(b) Metsemakers, Robert	Security sneltest	iB3:36
(b) Metsemakers, Robert	Misplaatste metaforen van security managers	iB4:24
(b) Metsemakers, Robert	Overtuigingskracht voor security officers	iB5:28
(b) Metsemakers, Robert	Wat ik weet uit de wijnkelder	iB6:30
(a) Mookhoek, Nico	Wat heeft AVG ons gebracht	iB5:20
(a) Os, Rob van	OODA-looping your security incident response	iB1:22
(a) Pitt, Laurence	Een (thuis)werkbare oplossing	iB1:08
(i) Pras, Alko, Vries, Chris de	Nieuw onderzoekscentrum TUCCR	iB3:38

(a) artikel (i) interview (b) blog (c) column

Jaaroverzicht



(a) Rahmani, Arash	Organisatiecultuur is essentieel voor informatiebeveiliging	iB2:32
(a) Rahmani, Arash	De menselijke factor in informatiebeveiliging	iB4:20
(a) Ruiter, Ard	Security overwegingen bij hybride werken	iB2:18
(a) Schelven, Peter van	Adequate gegevensbescherming werkt alleen als informatiebeveiliging op orde is	iB5:26
(a) Schoemaker, Renco	Met de BIO bezig blijven: hoe lang?	iB2:35
(a) Schoemaker, Renco	Het NIST CyberSecurity Framework als kans?	iB6:32
(a) Stein, Dave van	Krijg je organisatie mee door de business te begrijpen en te sturen op waarde	iB2:04
(a) Stuijt, Aaf	Van BIO naar boa (en weer terug)	iB5:08
(a) Teuben, Dennis	Horizontaal toezicht privacy by design	iB2:24
(b) Tissink, Mark	Anders kijken… naar informatiebeveiliging	iB2:38
(a) Verkerk, Remon	Menselijk schild: gebruikers als frontlinie van de organisatie	iB2:08
(a) Vlugt, Jurgen van der	Goto Human Driver Considered Dangerous (deel 1 van 3)	iB3:14
(a) Vlugt, Jurgen van der	Aangestuurd autorijden (deel 2 van 3)	iB5:37
(a) Vlugt, Jurgen van der	AI, Max! (deel 3 van 3)	iB6:21
(a) Vries, Chris de	Thuiswerken en Productiviteit	iB2:12
(i) Vries, Chris de	A secret revealed	iB3:10
(a) Vries, Chris de	Overheidsbrede cyberoefening	iB6:34
(a) Vries, Laura de	Handig is geen grondslag	iB5:14
(a) Wessels, Jan	Werken voor een financiële instelling vanuit huis	iB1:12
(a) Wetzer, Inge	Het begint met bewustwording	iB6:26
(a) Willemsen, Jeroen e.a.	Dear CISO: row your organization. Don't be just the gatekeeper, be an accelerator	iB3:31
(a) Wolthuis, Reinder	SOCRATES – security automation in SOC & CSIRT environments	iB4:26
(a) Wolthuis, Reinder	SOCRATES – real time threat, impact analysis and response …	iB5:42
(a) Zeegers, Ruben	BIO, een worsteling of geschenk?	iB2:29

(a) artikel (i) interview (b) blog (c) column

COLOFON

iB is het huisorgaan van het Platform voor 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
Chris de Vries

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

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

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

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

ABONNEMENTEN
De abonnementsprijs in 2021 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

YOUR CLOUDS. YOUR DATA. YOUR KEYS.

OUR DATA PRIVACY SOLUTION.

Maintain the privacy, security, and integrity of sensitive data, systems, and encryption keys across your cloud platforms with Enturst nShield as a Service. Whether you use Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), or Salesforce, you can rely on nShield as a Service to provide complete cryptographic capabilities from FIPS- and Common Criteria-certified hardware security modules, without the need for on-prem maintenance:

- Key generation and protection
- Compliance with industry and regulatory mandates
- Containerized application development

NEW INTEGRATION: Keep your most sensitive data private in Microsoft Azure Information Protection with Entrust Double Key Encryption.

LEARN MORE AT ENTRUST.COM/HSM

ENTRUST

SECURING A WORLD IN MOTION

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