INFORMATIEBEVEILIGING
MAGAZINE

- Een praktisch volwassenheidsmodel voor informatiebeveiliging
- Hoe betrouwbaar zijn uw big data en AI-systemen?
- Toepassing privacy enhancing technology in het Nederlandse eID

JAARGANG 19 - 2019 - EDITIE 6

Een nieuwe weg

Voor iB-Magazine en haar lezers bleek 2019 een interessant jaar te zijn. Er trad vanaf eind 2018 een vrijwel volledig nieuwe redactie aan en verschillende redactieleden vervulden om de beurt (en in teams van twee) het hoofdredacteurschap. Leerzaam en verrijkend voor ieder die deze eer te beurt viel.
Ook ontvingen wij (de leden) in dit jaar afwisselende edities, zowel qua inhoud als in omvang. De redactie vertrouwt erop dat dit bij jullie in goede aarde viel.
Als redactie experimenteerden wij - zie edities 3 ('Privacy') en 5 (een special over de Digital Architecture Design Day) - in onze aanpak. Leuk neveneffect: het daarin opgenomen interview met het bestuur van het Nationaal Architectuur Forum (NAF) leverde op hun 'site' een nooit eerder gezien aantal bezoekers/lezers op.
Maar stilstand is nooit goed, dus in 2020 gooien wij het roer weer om met een vaste hoofdredacteur. Dat betekent dat Nicole van Deursen vanaf iB-1 het hoofdredacteurschap solo gaat uitoefenen - natuurlijk met blijvende steun van de overige redactieleden. Zij gaat al voortvarend te werk: het redactieoverleg krijgt een betere vorm, de onderlinge communicatie gaat modernere middelen benutten en er is al een basisschema voor 2020 (ook met specials en thema's). De redactie ervoer dat haar werk positief overkwam, want nooit eerder kregen wij spontaan zoveel artikelen toegezonden als in dit jaar. Zelfs zoveel dat uitgave iB-6 min of meer vanzelf gevuld was. Wij zien dat als een compliment (voor PvIB-leden en redactie) en rekenen ook in 2020 weer op jullie bijdragen.
iB-6 is, zoals al gezegd, weer goed gevuld met zeer interessante artikelen. Een korte opsomming: een artikel van Marcel Spruit e.a. over een volwassenheidsmodel, wat vooral praktisch beoogd te zijn. Betrouwbaarheid van big data en AI-systemen staan centraal in het artikel van Henk-Jan van der Molen. Van Eric Verheul een oplossing: PEP (Polymorphic Encryption and Pseudonimation), voor privacyproblemen die in de pilot voor de nieuwe DigiD Hoog-authenticatie opgenomen is. Daarnaast nog meer artikelen en natuurlijk de vaste items.
Al met al weer voldoende interessant leesvoer voor de donkere dagen. Veel leesplezier en alvast fijne feestdagen en een goede start in 2020.

Tom Bakker
Chris de Vries

Rectificatie
Bij het artikel 'Bouwen aan digital architecture met Lego Serious Play' stond de verkeerde auteursinformatie. De juiste informatie is: 'Martin van der Poel is met zijn onderneming Zeta IT & Security actief op gebied van ICT/IT. Maarten van der Boon helpt vanuit zijn bedrijf Novitek bedrijven in de ontwikkeling van strategie, innovatie en communicatie. Hij is gecertificeerd facilitator van de Lego Serious Play-methode. Maarten is bereikbaar via maarten@novitek.nl.'

IN DIT NUMMER

Herman de Bruine is docent Integrale Veiligheidskunde en onderzoeker Cybersecurity aan de Haagse Hogeschool. Herman is bereikbaar via h.debruine@hhs.nl. Fabio Lucero Garau is student Integrale Veiligheidskunde aan de Haagse Hogeschool. Fabio is bereikbaar via f.j.lucerogarau@student.hhs.nl. Marcel Spruit is lector Cyber Security & Safety aan de Haagse Hogeschool. Marcel is bereikbaar via m.e.m.spruit@hhs.nl.

Een praktisch volwassenheidsmodel voor informatiebeveiliging

Recente incidenten met ransomware tonen aan dat veel organisaties hun informatiebeveiliging nog niet op orde hebben. Informatiebeveiliging op orde brengen vraagt naast technische middelen ook om beleid en informatiebeveiligingsbewustzijn bij medewerkers. Deze combinatie betekent dat het een illusie is te denken dat organisaties van de ene op de andere dag hun informatiebeveiliging op orde kunnen hebben. Er is behoefte aan een model waarlangs organisaties stappen kunnen zetten om hun informatiebeveiliging op orde te brengen.

In dit stuk wordt een praktisch volwassenheidsmodel voor informatiebeveiliging gepresenteerd, mede gebaseerd op het Capability Maturity Model en ISO 27001. Dit volwassenheidsmodel helpt de stand van zaken rond informatiebeveiliging in beeld te brengen en geeft aanwijzingen wat de prioriteiten van een organisatie zouden moeten zijn om de informatiebeveiliging te verbeteren.

In 2017 kwamen meerdere wereldwijde ransomware-aanvallen in het nieuws. Daardoor werden honderdduizenden organisaties getroffen, waaronder veel grote organisaties (1). Ransomware gijzelt computersystemen en als er niet betaald wordt, gaan bestanden verloren. Opvallend is dat vaak het niet up-to-date zijn van software de mogelijkheid gaf voor de verspreiding van en schade door de ransomware. Aanvallen als deze tonen de noodzaak voor organisaties om te zorgen dat zij hun informatiebeveiliging op orde hebben. Onder informatiebeveiliging worden in dit stuk niet alleen de technische beveiligingsvoorzieningen in ICT-systemen verstaan, maar ook de fysieke beveiligingsvoorzieningen (bijvoorbeeld toegangsbeheersing tot ruimtes) en organisatorische beveiligingsvoorzieningen (bijvoorbeeld protocollen voor het omgaan met vertrouwelijke informatie). Hierbij volgen we de definitie en indeling als in van Houten et al (2015) (2).

Door de toenemende invloed van ICT op onze samenleving wordt de rol van informatiebeveiliging steeds belangrijker voor publieke en private organisaties, maar betekent dit dat organisaties voldoende maatregelen nemen op het gebied van informatiebeveiliging? Uit rapporten van onder meer het Rathenau Instituut (3), de Rekenkamer Rotterdam (4) en het ministerie van J&V (5) blijkt dat er nog voldoende te verbeteren valt op het gebied van informatiebeveiliging. De weerbaarheid van organisaties is nog niet in alle sectoren op orde. Ook de (Rijks)overheid voldoet op het gebied van de informatiebeveiliging niet altijd aan haar eigen standaarden (3).

Volwassenheidsniveaus

In kwaliteitsmanagement is gebleken dat organisaties niet in één stap naar optimale kwaliteit gaan, maar dat dit een groeiproces is waarin een aantal fasen te onderscheiden is. Een voorbeeld hiervan wordt beschreven in het INK-model (6). Ook binnen de informatievoorziening zijn groeimodellen ontwikkeld. Zo is er voor softwareontwikkeling het Capability Maturity Model (CMM) (7). Zowel INK als CMM gaan uit van fasen in de ontwikkeling van organisaties, waarbij vastgesteld wordt op welk niveau een organisatie zich bevindt, om daarna daarbij passende ontwikkelacties te kunnen ondernemen. In CMM worden

deze fasen volwassenheidsniveaus genoemd en wij zullen deze term ook hanteren.

Het ligt voor de hand om de CMM-benadering te volgen, maar CMM kenmerkt zich door een grote hoeveelheid vragen en is tegelijkertijd beperkt tot alleen het beoordelen van de werkwijze binnen de organisatie. CMM is gericht op het 'hoe' en niet zozeer het 'wat' en 'wie'. Daarnaast geldt dat CMM gericht is op softwareontwikkeling, niet op informatiebeveiliging en veiligheidsbewustzijn. De doelstelling was om te komen tot een volwassenheidsmodel voor informatiebeveiliging waarmee organisaties zelfstandig het niveau van hun informatiebeveiliging kunnen vaststellen (zelfevaluatie) en op basis hiervan verbeterpunten hiervoor formuleren.

Het volwassenheidsmodel voor informatiebeveiliging is in de loop van 2016 en 2017 ontworpen en verbeterd. Toetsing van de eerste versie is in december 2016 en januari 2017 uitgevoerd met behulp van 25 derdejaars hbo-studenten van de opleiding Integrale Veiligheidskunde (8) die minimaal 32 uur per week in dienst zijn van een organisatie. Aan de studenten is gevraagd de informatiebeveiliging van hun eigen organisatie, met behulp van de eerste versie van het model, te beoordelen.

Opbouw van het volwassenheidsmodel

Het volwassenheidsmodel bestaat uit twee componenten. De aandachtsgebieden en de volwassenheidsniveaus. Als eerste worden de aandachtsgebieden behandeld.

Aandachtsgebieden

De aandachtsgebieden zijn ontleend aan ISO-normering voor managementsystemen. Daarbij is gekozen voor de zogenaamde ISO High Level Structure die de gemeenschappelijke basis is waarop de verschillende normen van ISO zijn gebouwd, zoals 9001 voor kwaliteitssystemen, 27001 voor informatiebeveiliging en 14001 voor milieu.

In ISO 27001 zijn de volgende aandachtsgebieden benoemd (9):

a. **Context van de organisatie:** het in kaart brengen van belanghebbenden, welke eisen zij stellen, en welke raakvlakken en afhankelijkheden er zijn.
b. **Leiderschap:** het tonen van leiderschap en betrokkenheid door het opstellen en communiceren van informatiebeveiligingsbeleid en het verdelen van rollen, verantwoordelijkheden en bevoegdheden om dit beleid ook te kunnen uitvoeren.
c. **Planning:** het in kaart brengen en beoordelen van risico's en kansen op het gebied van informatiebeveiliging, op basis hiervan maatregelen nemen en de voortgang van de uitvoering ervan bewaken.
d. **Ondersteuning:** het beschikbaar stellen van middelen, competenties van medewerkers benoemen en medewerkers hiervoor toerusten, werken aan bewustzijn van de medewerkers, communiceren over informatiebeveiliging en het onderhouden van gedocumenteerde informatie erover.
e. **Uitvoering:** op operationeel niveau uitvoeren van informatiebeveiliging door het uitvoeren van risicobeoordeling en het implementeren van maatregelen.
f. **Evaluatie van prestaties:** het evalueren van de prestaties (ook door audits) op het gebied van informatiebeveiliging, vastlegging daarvan en een actieve rol van het management daarbij.
g. **Verbetering:** omgaan met afwijkingen en het nemen van corrigerende maatregelen.

Vanuit deze zeven aandachtsgebieden zijn voor het volwassenheidsmodel de volgende negen aandachtsgebieden gedefinieerd:

1. **Beleid en risico's (10):** de mate van bekendheid en begrip van informatiebeveiligingsbeleid bij medewerkers en de afstemming hierover met partners.
2. **Maatregelen:** de mate waarin er een complete set van maatregelen is ingevoerd, liefst in de vorm van een Information Security Management System.
3. **Protocollen/regelgeving:** de mate waarin rond informatiebeveiliging risico's up-to-date zijn en protocollen of regels aanwezig zijn.
4. **Bekendheid met beleid, risico's en dreigingen:** de bekendheid hierover bij medewerkers en de bekendheid en afstemming erover met partners.
5. **Rol staf/lijn/directie:** de mate waarin het management informatiebeveiliging als eigen verantwoordelijkheid ziet.
6. **Toerusting van medewerkers:** de mate waarin medewerkers zijn toegerust rond informatiebeveiliging en informatiebeveiligingsbewustzijn wordt bevorderd.
7. **Processen:** de mate waarin bij procesanalyse aandacht besteed wordt aan informatiebeveiligingsrisico's en -maatregelen.
8. **Procesmanagement:** de mate waarin bij procesmanagement aandacht besteed wordt aan informatiebeveiliging.
9. **Meten en evalueren:** de mate waarin binnen de besturing van organisatie (bijvoorbeeld via de Planning & Control-cyclus) aandacht is voor informatiebeveiliging.

In tabel 1 is aangegeven hoe de ISO-aandachtsgebieden terugkomen in de aandachtsgebieden van ons model.

Aandachtsgebied model	**Aandachtsgebieden ISO (zie pagina 5)**
1.Beleid en risico's	a. Context van de organisatie: het in kaart brengen van belanghebbenden, welke eisen zij stellen, en welke raakvlakken en afhankelijkheden er zijn. c. Planning: het in kaart brengen en beoordelen van risico's en kansen op het gebied van informatiebeveiliging.
2. Maatregelen	c. Planning: op basis van risico's en kansen maatregelen nemen en de voortgang van de uitvoering ervan bewaken. d. Ondersteuning: het beschikbaar stellen van middelen, communiceren over informatiebeveiliging.
3. Protocollen/ regelgeving	d. Ondersteuning: het onderhouden van gedocumenteerde informatie.
4. Bekendheid met beleid, risico's en dreigingen	b. Leiderschap: het tonen van leiderschap en betrokkenheid, door het opstellen en communiceren van informatiebeveiligingsbeleid.
5. Rol staf/ lijn/ directie	b. Leiderschap: het verdelen van rollen, verantwoordelijkheden en bevoegdheden om dit beleid ook te kunnen uitvoeren.
6.Toerusting van medewerkers	d. Ondersteuning: competenties van medewerkers benoemen en medewerkers hiervoor toerusten en werken aan bewustzijn van de medewerkers.
7. Processen	e. Uitvoering: op operationeel niveau uitvoeren van informatiebeveiliging door het uitvoeren van risicobeoordeling en het implementeren van maatregelen op procesniveau.
8. Procesmanagement	e. Uitvoering: bewaken implementatie van maatregelen op procesniveau.
9. Meten en evalueren	f. Evaluatie van prestaties: het evalueren van de prestaties (ook door audits) op het gebied van informatiebeveiliging, vastlegging daarvan en een actieve rol van management daarbij. g. Verbetering: omgaan met afwijkingen en het nemen van corrigerende maatregelen.

Tabel 1 – Aandachtsgebieden ISO.

In de tabel is goed te zien dat in de eerste aandachtsgebieden (1. beleid tot en met 5. rolverdeling) afgeweken is van de volgorde in ISO. De reden hiervoor is dat het model ontworpen is om de praktijk van informatiebeveiliging op de werkvloer zichtbaar te maken. Dit betekent dat gefocust wordt op wat de kennis en ervaring van medewerkers is met informatiebeveiliging binnen hun organisatie. Eerst wordt gevraagd naar de inhoud van het beleid en maatregelen, daarna naar de bekendheid van het beleid, de rol van management en staf bij de uitvoering van informatiebeveiligingsbeleid en de toerusting van medewerkers. Volgend onderdeel is de uitvoering van het beleid op procesniveau waarbij onderscheid wordt gemaakt tussen de inhoud (risicobeoordeling en maatregelen) en de wijze van sturing bij het implementeren van maatregelen. Tenslotte is er aandacht voor het meten en evalueren en de wijze waarop dit verankerd is in de Planning & Control-cyclus binnen de organisatie.

Volwassenheidsniveaus

Er zijn vijf volwassenheidsniveaus onderscheiden in de omgang met informatiebeveiliging: Onbewust, Reactief, Systemen in ontwikkeling, Systemen op orde en systemen die zowel geïnternaliseerd zijn alsook op partners afgestemd. De inspiratie hiervoor komt uit verschillende bronnen: het CMM-model van Carnegie Mellon (Paulk et al 1993), het maturitymodel van Crosby (1979) (11) en het INK-managementmodel (12).

In CMM en Crosby wordt niet verwezen naar de samenwerking met externe partners, bij het INK-model is dit wel het geval (13). Er is ervoor gekozen in het vijfde niveau ook de externe partners mee te nemen, omdat veel organisaties in hun informatievoorziening interactie hebben met partners, waardoor afstemming van informatievoorziening en informatiebeveiliging met partners een noodzaak is geworden (14).

Volwassenheidsniveau	Omschrijving*
1. Onbewust	Aandacht voor IB als er een (groot) incident is geweest. Er is geen IB-beleid.
2. Reactief	Aandacht voor IB vooral na incidenten. Er is IB-beleid gemaakt n.a.v. incidenten en er zijn maatregelen genomen om herhaling te voorkomen.
3. Systemen in ontwikkeling	Er is proactief IB-beleid (naast incidenten zijn ook bedreigingen meegenomen). Dit wordt nog niet door iedereen op dezelfde wijze gehanteerd.
4. Systemen op orde	Er is proactief IB-beleid, uniform gehanteerd binnen de organisatie. Er is sturing op IB in de Planning & Control-cyclus.
5. Geïnternaliseerd en op partners afgestemd	IB-beleid wordt door medewerkers naar de geest gehanteerd en doorlopend verbeterd. Het IB-beleid is afgestemd met partners.

**IB = informatiebeveiliging*

Tabel 2 – Volwassenheidsniveaus.

Figuur 1 – Volwassenheidsmodel.

Hanteren van het volwassenheidsmodel

In het hanteren van de volwassenheidsniveaus geldt dat ze cumulatief zijn: elk volgend niveau behoudt de goede elementen van het niveau ervoor en voegt daar extra elementen aan toe. Bij elk van de aandachtsgebieden zijn stellingen geformuleerd die het volwassenheidsniveau voor dit aandachtsgebied illustreren (zie figuur 1).

Als voorbeeld de regel in het model rond protocollen/regelgeving:

- **Onbewust:** men werkt inzake informatiebeveiliging volgens de gedachte: 'zo doen we het hier nu eenmaal'.
- **Reactief:** voor sommige kritische informatiebeveiligingsrisico's zijn er protocollen of regels. Na incidenten worden protocollen of regels op- of bijgesteld.
- **Systemen in ontwikkeling:** voor alle relevante informatiebeveiligingsrisico's zijn protocollen of regels, controle op naleving nog vooral na incidenten.
- **Systemen op orde:** voor alle relevante informatiebeveiligingsrisico's zijn protocollen of regels. Deze worden bij-

gesteld als er iets niet goed blijkt te zijn of ze niet worden nageleefd.
- **Geïnternaliseerd:** voor alle relevante informatiebeveiligingsrisico's zijn protocollen of regels. Deze worden periodiek doorgelicht of ze nog passend/effectief zijn.

Om het volwassenheidsniveau (15) te bepalen in het geval van de protocollen/regelgeving wordt gekeken naar het bestaan van protocollen (zijn er protocollen, dan niveau 2), de dekking (volledig dekkend, dan niveau 3), de actualiteit (dan niveau 4) en ten slotte of ze proactief worden doorgelicht en met partners besproken (dan niveau 5).

Het is de bedoeling dat per score door de beoordelaar een feitelijke onderbouwing wordt geleverd waarom het betreffende niveau gescoord is. Bijvoorbeeld bij niveau 2: het benoemen van de bestaande protocollen en het aangeven waar nog behoefte aan is. Voor niveau 3 geldt dat aangegeven wordt hoe de naleving van de protocollen gecontroleerd wordt, enzovoort.

Van elk van de aandachtsgebieden kan zo het niveau worden bepaald. De niveaus kunnen per aandachtsgebied verschillen. Dit levert een profiel van de scores op de aandachtsgebieden.
Het uitgangspunt van het volwassenheidsmodel is dat de organisatie zo sterk is als de zwakste schakel. Het overall volwassenheidsniveau wordt daarmee de laagste score van de aandachtsgebieden. Dit maakt het prioriteren van de benodigde verbeteringen die uit de diagnose komen relatief eenvoudig: verbeter het zwakste aandachtsgebied. Mochten alle aandachtsgebieden zich op hetzelfde volwassenheidsniveau bevinden dan impliceert het model een volgorde van 1 (beleid) naar 9 (evaluatie) conform de PDCA- of Deming-cirkel. Als er onvolledigheid in het beleid is, dan dient dat als eerste te worden weggenomen. Daarna de concrete uitwerking in maatregelen, de voorlichting en toerusting. Vervolgens de uitwerking op uitvoeringsniveau en tenslotte de meting en evaluatie ervan.

Uitkomsten van de test van het volwassenheidsmodel

Zoals beschreven is het model getest door studenten van de opleiding Integrale Veiligheidskunde. Hen is gevraagd de scores te bepalen voor de organisatie waarin zij werken en deze scores toe te lichten. De rapportages van 30 studenten zijn beoordeeld door de onderzoekers. Zij hebben hen van commentaar/nadere vragen voorzien, met het verzoek de rapportages hierop aan te passen. De vragen betroffen vooral de concrete onderbouwing van de score. Uiteindelijk

	sector	beleid	maatregelen	protocollen	bekendheid risico's	rol staf / lijn	toerusting mdw	processen	processmgt	meten en evalueren	niveau	prioriteit
1	Overheid	4	2	3	3	5	2	2	4	3	2	maatregelen
2	Overheid	2	3	3	1	4	1	2	2	2	1	bekendheid
3	Overheid	4	3	5	2	5	3	5	4	2	2	bekendheid
4	Overheid	4	3	3	5	4	3	3	5	1	1	evalueren
5	Overheid	5	3	4	4	4	4	4	4	5	3	maatregelen
6	Overheid	2	2	2	2	4	1	2	2	4	1	toerusting
7	Overheid Vitaal	5	3	3	5	4	2	4	5	4	2	toerusting
8	Overheid Vitaal	3	2	2	4	4	2	3	2	2	2	maatregelen
9	Overheid Vitaal	2	2	2	2	3	1	1	3	1	1	toerusting
10	Profit	3	4	2	3	3	1	1	1	1	1	toerusting
11	Profit dienstverlening	2	2	2	2	5	1	2	2	1	1	toerusting
12	Profit dienstverlening	2	2	4	3	2	1	2	1	1	1	toerusting
13	Profit dienstverlening	2	2	2	2	3	1	2	2	1	1	toerusting
14	Profit dienstverlening	5	2	1	2	3	1	1	2	1	1	protocollen
15	Profit Industrie	2	2	3	3	3	2	3	2	1	1	evalueren
16	Profit Infrastructuur	2	2	2	2	4	1	1	2	1	1	toerusting
17	Profit offshore	2	2	2	2	3	2	1	2	1	1	processen
18	Profit productie	1	3	1	3	4	1	1	2	1	1	beleid
19	Verzekering	2	3	1	2	3	1	2	1	1	1	protocollen
20	Zorg	1	2	2	1	2	1	2	1	1	1	beleid
21	Zorg	2	2	2	2	3	2	1	2	1	1	processen

Figuur 2 - Een overzicht van de scores van verschillende organisaties op het maturitymodel.

zijn na aanvulling 21 uitwerkingen ontvangen, die van voldoende kwaliteit waren. Een tweetal studenten gaf aan dat het informatiebeveiligingsbeleid van hun organisatie (dat ze in termen van volwassenheidsniveau zelf inschatten op niveau 4) niet toestond dat ze de rapportage van concrete voorbeelden konden voorzien; deze uitwerkingen zijn niet meegenomen in deze rapportage.

De beelden van de organisaties zijn zeer uiteenlopend. Overall valt op dat er nog weinig organisaties op volwassenheidsniveau 3 (systemen in ontwikkeling) of hoger zitten. Er zijn een aantal organisaties die op zich relatief hoog zouden kunnen scoren, maar één element ontbreekt (zoals organisaties 4 en 7). Er zijn ook organisaties die nog helemaal aan het begin staan (organisaties 18 en 20).

Conclusies

In dit stuk is een praktisch volwassenheidsmodel gepresenteerd voor informatiebeveiliging op basis van de aandachtspunten uit de ISO High Level Structure en de volwassenheidsniveaus uit CMM en het INK-model. Een conceptversie is uitgetest door studenten Integrale Veiligheidskunde. Met een beperkte ondersteuning was het model goed door hen te hanteren. De ondersteuning bestond vooral uit het 'doorvragen' op aspecten en het verhelderen van wat onder een baseline informatiebeveiliging wordt verstaan. Op basis van deze ervaringen lijkt het

De uitkomsten geven een negatief beeld van de volwassenheid

dat binnen een organisatie een inhoudelijk deskundige (security officer, CISO, of een andere medewerker die zich bezighoudt met informatiebeveiliging) met behulp van het volwassenheidsmodel relatief snel kan vaststellen wat het niveau van de informatiebeveiliging in de organisatie is. Hiervoor hoeven ze geen uitgebreide opleiding te krijgen omdat hun eigen inhoudelijke kennis volstaat. Wel dient de uitvoerder bij voorkeur enige ervaring met auditen te hebben (16); hierbij kan overigens aangesloten worden op auditortrainingen die rond (kwaliteits)managementsystemen gebruikelijk zijn. Uit de resultaten van het model kan snel duidelijk worden op welk vlak de verbeterpunten voor de organisatie liggen met betrekking tot de informatiebeveiliging en in welke volgorde deze het best opgepakt kunnen worden.

De uitkomsten van werken met het model geven een negatief beeld van de volwassenheid op het gebied van informatiebeveiliging van de organisaties die zijn beoordeeld. Dit beeld was consistent met de indruk die de studenten over hun organisatie hadden. Het beeld was wellicht enigszins positiever geweest als er over de twee niet meegenomen organisaties, waarvan het volwassenheidsniveau door de betrokken studenten rond 4 werd ingeschat, gedetailleerder informatie beschikbaar was geweest. Hier staat echter tegenover dat bij informatiebeveiliging transparantie een belangrijke waarde is, waaraan deze organisaties niet voldoen.

Referenties

(1) http://www.nu.nl/internet/4692084/aantal-slachtoffers-ransomware-wannacry-loopt-200000.html

(2) P. van Houten, M. Spruit & K. Wolters (2015). Informatiebeveiliging onder controle. Amsterdam, Pearson

(3) G. Munnichs, M. Kouw & L. Kool (2017). Een nooit gelopen race – over cyberdreigingen en versterking van weerbaarheid. Den Haag, Rathenau Instituut

(4) Rekenkamer Rotterdam (2017). In Onveilige Handen. Rotterdam, Rekenkamer Rotterdam.

(5) Cybersecuritybeeld Nederland CSBN 2017 (2017). Den Haag, NCTV

(6) Zie bijvoorbeeld: Hadjono en Hes (1993). De Nederlandse kwaliteitsprijs en onderscheiding, Deventer, Kluwer

(7) Zie bijvoorbeeld: M. Paulk, C. Mark, C. Weber, B. Curtis, M. Chrissis (1993). Capability Maturity Model for Software, Version 1.1. Technical Report. Pittsburgh, Software Engineering Institute, Carnegie Mellon University en zie J. Herbsleb, D. Zubrow, D. Goldenson, W. Hayes & M. Paulk (1997). Software Quality and the Capability Maturity Model. Communications of the ACM 40(6), 30-40

(8) Als onderdeel van het vak Cybersecurity

(9) NEN-ISO/IEC 27001 (nl), Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen

(10) Onder risico's worden ook de termen dreigingen, assets en kwetsbaarheden meegenomen (termen die gebruikelijk zijn binnen het security-veld)

(11) P. Crosby (1979). Quality is Free. New York, McGraw Hill

(12) R. Emmerik (2012). Kwaliteitsmanagement, tweede editie. Amsterdam, Pearson.

(13) De volwassenheidsniveau lijken het meest op de dimensies van het INK-model, waarbij t.o.v. het INK-model een 'nul'-niveau is ingevoerd

(14) World Economic Forum (2012). Partnering for Cyber Resilience - Risk and Responsibility in a Hyperconnected World - Principles and Guidelines. Geneve, World Economic Forum

(15) Het model is ontwikkeld om te kijken naar een hele organisatie, maar kan ook op afdelingsniveau worden gehanteerd. Bij het organisatieniveau geldt dat de beveiliging zo sterk is als de zwakste schakel, de score wordt dan bepaald door de 'zwakste' afdeling (met een belangrijke rol rond het beveiligen van informatie). Wel kunnen de punten die moeten worden opgepakt dan verschillen van afdeling tot afdeling

(16) Met name de diepgang en concreetheid van de voorbeelden ter onderbouwing van de bepaling van het volwassenheidsniveau is cruciaal

Henk-Jan van der Molen is onder andere docent bij de Security Academy voor CISSP-, CISM- en CISA-modules en is werkzaam bij het SECO Institute voor het ontwikkelen van examens. Henk-Jan is bereikbaar via: henk-jan.van.der.molen@securityacademy.org.

Hoe betrouwbaar zijn uw big data en AI-systemen?

Informatiebeveiliging voor big data en AI-systemen is belangrijk om de informatiekwaliteit te garanderen, maar ook om big data en AI-systemen te beschermen tegen cybercriminelen. Dit artikel beschrijft de beveiligingsmaatregelen die relevant zijn in deze context. Deze maatregelen zijn niet compleet of voor elke situatie geschikt. Momenteel worden zowel voor big data als AI-systemen nog normen ontwikkeld. Voor een adequate beveiliging is daarom voorlopig maatwerk nodig op basis van een risicoanalyse. Het blijft een menselijke afweging waar en onder welke voorwaarden AI-systemen kunnen worden ingezet.

If you know the enemy and know yourself,
you need not fear the result of a hundred battles.
If you know yourself but not the enemy,
for every victory gained you will also suffer a defeat.
If you know neither the enemy nor yourself,
you will succumb in every battle

Sun Tzu, The Art of War

IT is onmisbaar geworden in onze samenleving. Ook al nadert de zogenaamde Wet van Moore (1) zijn houdbaarheidsgrens, op korte termijn groeit de rekenkracht van computers nog. Voor bedrijven is succesvolle innovatie nodig om te blijven bestaan. Klanten verwachten namelijk steeds meer 'non stop service' en een persoonlijke benadering van organisaties. Betere service vergt meer digitalisering en meer informatie-uitwisseling tussen processen. Ook door de toename van IoT-apparatuur groeit de beschikbare data. De meeste data die nu beschikbaar is, is in de laatste jaren gegenereerd (2). Surfend op die vloedgolf van data worden big data en AI-systemen ontwikkeld die steeds meer sturende taken overnemen.

Met de digitalisering van processen neemt de druk op de beveiliging toe en intussen heeft de AVG de privacyregels aangescherpt. Zo zijn privacy by design en privacy by default verplicht en moeten profileringsalgoritmes transparant zijn. Naast opzet en bestaan vereist de AVG ook dat de effectieve werking van beveiligingsmaatregelen aantoonbaar is. Omdat er voor beveiliging geen onbegrensd budget is, moeten organisaties de prioriteit leggen bij de beveiliging van de belangrijkste bedrijfsprocessen.

Beveiliging focust vaak op geheimhouding, maar stuurinformatie moet vooral betrouwbaar zijn. Het artikel start daarom met vier architectuurprincipes die worden uitgewerkt in generieke maatregelen om betrouwbare informatie te produceren. Daarna worden de ontwikkelingen van het big data en AI-vakgebied samengevat. Op basis van verschillen met traditionele IT-systemen sluit het artikel af met extra beveiligingsmaatregelen om big data en AI-systemen operationeel te houden en verder te kunnen ontwikkelen.

Architectuur en informatiebeveiliging

Informatiebeveiliging (IB) bestaat uit drie componenten. Allereerst is dat 'vertrouwelijkheid': alleen de doelgroep heeft toegang tot informatie. Dit wordt vaak ingevuld met encryptie, waarbij alleen de doelgroep de cryptomiddelen heeft om vercijferde informatie te gebruiken. Het tweede component is 'beschikbaarheid': informatie is beschikbaar als de organisatie die nodig heeft. Dit vergt bijvoorbeeld back-upvoorzieningen. Tenslotte geeft 'integriteit' aan dat de data of informatie authentiek, juist, volledig en actueel is. In dit artikel is 'data' de input van informatiesystemen en 'informatie' de output. Kwaliteit en betrouwbaarheid worden als synoniem gebruikt voor integriteit van informatie.

Maatregelen voor integriteit liggen minder voor de hand. De Gebruikers Acceptatie Test (GAT) toetst bijvoorbeeld of een nieuw informatiesysteem de gewenste informatie produceert, maar standaard negeert een GAT vragen over informatiekwaliteit. Denk hierbij aan vragen als:

- Kunnen alleen de juiste personen data invoeren en muteren?
- Zijn de informatievoorzieningsprocessen voldoende transparant?
- Voldoet de beveiliging van het informatiesysteem?
- Welke kwaliteit heeft de brondata en de daarmee geproduceerde informatie?

Een architectuur bevat coherente en consistente regels, richtlijnen en standaards die samenhangende componenten als geheel beschrijven (3). Een IT-architectuur beschrijft sturingsprincipes voor de ontwikkeling en het gebruik van de informatievoorziening. Vier architectuurprincipes worden hierna uitgewerkt in generieke maatregelen om betrouwbare informatie te produceren (zie figuur 1).

Figuur 1 - Vier architectuurprincipes voor informatiekwaliteit.

Principe 1: bescherm informatie van creatie tot vernietiging

Het beleid moet relevante eisen in wet- en regelgeving signaleren en bij projecten voorschrijven dat beveiligingseisen zo vroeg mogelijk worden vastgesteld. Na het vaststellen van de gewenste betrouwbaarheidsniveaus ligt de focus op governance: wie kan namens de eigenaar data invoeren, lezen, muteren of vernietigen op basis van need to know/least privilege? De procedures voor HR, systeembeheer, configuratiebeheer, wijzigingsbeheer en beveiligingseisen van transacties bepalen welke rechten aan verantwoordelijkheden worden gekoppeld. Voor de veiligheid bij aanschaf en inzet van IT-middelen is beleid nodig, gericht op leveranciersmanagement, telewerken en gebruik van bedrijfsmiddelen.

Om data te kunnen vinden en hergebruik te stimuleren is metadata nodig die de inhoud en context van data beschrijft op basis van de FAIR-principes: 'Findability', 'Accessibility', 'Interoperability' en 'Reusability'. Master Data Management en de WBP hebben deze principes eerder geïntroduceerd. Datamanagement start met een unieke identificatie van data-elementen, datagroepen en relaties daartussen, zodat metadata eenduidig kan worden geregistreerd in een data dictionary. Dit is ook relevant voor ketens, omdat eenduidige afspraken nodig zijn om de impact van foute informatie te beperken. Een ketenorganisatie heeft namelijk maar beperkt zicht op de informatiebehoefte en de risico's voor de processen van andere ketenpartijen. Meer eisen voor metadata staan bijvoorbeeld in de ISO 11179. Het beheer van metadata is een verantwoordelijkheid van de chief data officer.

Casus: wetenschap heeft betrouwbare data nodig

De wetenschap onderkende al vroeg het belang van betrouwbare gegevens. Aristarchos van Samos beweerde al in 265 v.Chr. dat de planeten om de zon draaien, maar de geocentrische visie van Aristoteles hield stand. Copernicus herintroduceerde het heliocentrische model in 1543, maar zijn wiskundige theorie was strijdig met de toenmalige uitgangspunten van de wetenschap.

Pas in de 17e eeuw begon men de Bijbel minder letterlijk te interpreteren en ontwikkelde de wetenschap zich tijdens de Verlichting. Johannes Kepler formuleerde in 1609 zijn bewegingswetten voor hemellichamen. Na de uitvinding van zijn telescoop in 1610 kon Galileo Galilei veel nauwkeurige waarnemingen doen die het heliocentrische model bevestigden. De Inquisitie dwong Galileo echter het heliocentrische model af te zweren, omdat dit zou conflicteren met de Bijbel.

Als contrast: in februari 1897 legde het Huis van Afgevaardigden van de Amerikaanse staat Indiana in een wetsontwerp de rekenwaarde van π met bijna 2% afwijking vast als 3,2. Deze 'Pi-wet' kwam op het laatste moment niet door de Senaat en werd dus niet van kracht.

Encryptie kan het onbevoegd lezen en muteren van informatie voorkomen en met PKI-certificaten kunnen systemen of personen elkaar authentiseren. De datakwaliteit kan ook worden bewaakt met controletellingen, hashing en elektronische handtekeningen. Effectieve controles op informatiekwaliteit moeten zo dicht mogelijk bij de productie worden ingericht en het effect van afwijkingen nauwkeurig kunnen inschatten. Gedurende de levensduur van informatie kunnen beveiligingsincidenten de kwaliteit ervan verminderen. De organisatie moet kwetsbaarheden en incidenten daarom tijdig signaleren, afhandelen en evalueren. Dit vergt allereerst een goede preventie, zoals firewalls, regelmatig testen van back-up- en restoreprocedures en het vastleggen van forensische informatie. Omdat reguliere antivirus steeds ineffectiever wordt, hebben grote organisaties een security operations center (SOC) met een systeem voor incident en event management (SIEM) om real time abnormaal netwerkverkeer te kunnen signaleren. Vervolgens is een procedure nodig om gecontroleerd van incident naar crisismanagement te kunnen gaan, zijn er periodieke oefeningen nodig om medewerkers risicobewust te maken en is het belangrijk om te trainen als crisisteam.

Om risico's goed te managen moet de PDCA-cyclus functioneren, zodat de organisatie consequent zoekt naar conformi-

teit met geldende normen en leert van geconstateerde afwijkingen. Omdat een organisatie niet alle incidenten kan detecteren, moeten controles regelmatig worden ingepland en alle significante risico's afdekken. Organisaties moeten ook bewaken dat de juiste controles op het juiste moment worden uitgevoerd.

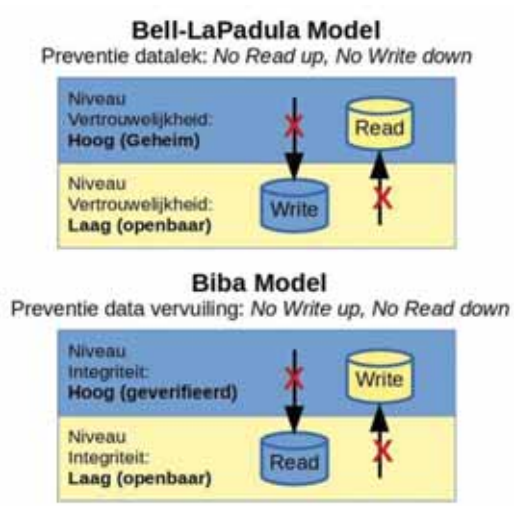
Organisaties die incidenten, klachten en auditbevindingen als startpunt willen gebruiken voor continue verbetering, kunnen daarvoor de 4xO-methode toepassen:

O1: wat is de omvang van het issue of waar is correctie nodig?
O2: wat is de oorzaak (Engels: root cause analysis) of wat bepaalt de kans op herhaling?
O3: welke oplossing met correctieve en preventieve acties is proportioneel met het risico?
O4: hoe en wanneer testen we of deze oplossing operationeel voldoet?

Principe 2: verdediging in de diepte

Voor staatsgeheimen bestaan meerdere vertrouwelijkheidsniveaus. Beveiliging wordt daarom vaak in lagen gevisualiseerd: elke laag bevat specifieke maatregelen. Voor informatiekwaliteit zijn meerdere niveaus ongebruikelijk, maar soms is wel bekend dat data vervuild is en moet worden opgeschoond.

Voor hogere niveaus van informatiekwaliteit zijn meer en zwaardere maatregelen nodig. Relevante maatregelen zijn onder andere fysieke en logische toegangscontroles, screening van medewerkers, wachtwoordbeleid, controles op informatiekwaliteit, data governance, controletechnische functiescheiding, logging van mutaties, audits op de naleving van normen en audits op de effectiviteit van maatregelen. Naast de herkomst, eigenaar en betekenis, kan metadata het betrouwbaarheidsniveau voor datakwaliteit aangeven, inclusief de houdbaarheid in plaats en tijd.



Figuur 2 - Bell-LaPadula-model versus Biba-model.

Beveiligingsmodellen voor logische controles zijn bijvoorbeeld Bell-LaPadula (voor vertrouwelijkheid) en Biba (4) (voor integriteit van informatie), zie figuur 2. Beide modellen gaan uit van centrale controle en zijn ouder dan het internet, maar zijn nog steeds waardevol. Het beveiligingsbeleid bijvoorbeeld geeft alleen aan wat een rol mag doen, terwijl een beveiligingsmodel verklaart waarom bepaalde acties wel of niet zijn toegestaan.

Het Bell-LaPadula-model voorkomt datalekken met het credo: 'no read up, no write down'. Dat wil bijvoorbeeld zeggen dat niemand informatie kan lezen die hoger gelabeld is dan zijn screening. Daarnaast kan iemand met de juiste screening geen geheime informatie kopiëren naar een locatie met een lager vertrouwelijkheidsniveau.

Het Biba-model voorkomt gegevensvervuiling met het credo: 'no write up, no read down'. Iemand met toegang tot laagwaardige informatie kan die niet kopiëren naar locaties voor hoogwaardige informatie. Tegelijkertijd mag een uitvraag voor hoogwaardige informatie geen laagwaardige data bevatten.

Principe 3: gebruiksvriendelijke beveiliging

Bekijk het systeem als gebruiker. In de ideale situatie is onveilig handelen moeilijker dan veilig handelen. Gebruikers moeten voldoende opleiding hebben gehad, beschikken over begrijpelijke documentatie en een helpdesk kunnen benaderen met vragen en klachten. De metadata van geproduceerde informatie moet worden vastgesteld op basis van de doelen en belangen van de doelgroep. De processen van de informatievoorziening moeten transparant zijn, zodat gebruikers kwetsbaarheden in de logica beter kunnen signaleren en kunnen nagaan hoe betrouwbaar hun informatie is. Om de complexiteit te verminderen, moeten informatiesystemen modulair zijn. Informatiesystemen kunnen ook functionaliteit bieden waarmee gebruikers zelf eenvoudig afwijkingen in brondata kunnen signaleren.

Anderzijds vormen de belangen van medewerkers voor (on)betrouwbare informatie een uitgangspunt voor controles op de brongegevens en geproduceerde informatie. Op

basis van risicoscenario's en pre mortem-analyses kunnen audits worden gepland en uitgevoerd.

Principe 4: security by design en security by default

Beveiligingsmaatregelen moeten het risico van incidenten zoveel mogelijk beperken. Dat begint bij dataminimalisatie: wat je aan gevoelige data niet (meer) nodig hebt, hoef je ook niet te beveiligen. Dit lijkt in tegenspraak met big data, maar relevante maatregelen hiervoor zijn vastgestelde bewaartermijnen, logische toegangsrechten op basis van 'need to know' en encryptie van data (5).

Om vanuit de privacy risico's voor betrokkenen de risicobeperkende maatregelen te bepalen is een Privacy Impact Analyse (PIA) nodig (6). Voorbeelden van privacymaatregelen zijn pseudonimiseren van data, het borgen van k-anonimiteit (voorkomt heridentificatie) en het recht op inzage, correctie en regie op het gebruik van eigen data. Een PIA beoordeelt ook de rechtmatigheid van gegevensverwerkingen.

Behalve de juiste brondata in het afgesproken formaat is ook een goed proces nodig om daar betrouwbare informatie van te maken. Als dit principe niet goed is ingericht, kunnen fouten in data of algoritmes incidenten veroorzaken. Bijvoorbeeld de Mars Climate Orbiter van $ 135 miljoen crashte in 1999, omdat één stuurcomputer communiceerde in 'imperial units' (pound) en andere in SI-eenheden (kilo) (7). Daarom gebruikt elke Java Virtual Machine dezelfde rekenfuncties en gegevensformaten, zodat een Java-programma op elk platform dezelfde uitkomsten produceert.

Om veilige software te ontwikkelen bestaan methodes zoals Secure Software Development (8). Met open source is de kwaliteit van software, inclusief de controles op informatiekwaliteit, zichtbaar en zijn die controles eventueel ook aan te passen. Daarnaast is sjoemelen met software een stuk lastiger met open source.

Van big data naar AI-systemen

De ontwikkeling van het AI-vakgebied kende verschillende stadia. Eind jaren tachtig werd business intelligence ingezet om de aandelenkoersen te voorspellen. Rond 1995 werd data mining toegepast voor direct marketing, fraudedetectie en kredietprofilering. Na de opkomst van het internet werden e-commerce-toepassingen ontwikkeld om automatisch gepersonaliseerde diensten te leveren. In de biochemie en astronomie werden intussen met succes steeds grotere modellen ontwikkeld en in 2011 werd big data in bijna elk vakgebied toegepast.

Casus: manipulatie van beursgevoelige informatie

Enron was een Amerikaans energiebedrijf dat in 1980 vooral gas leverde. Begin jaren negentig begon Enron echter miljarden te investeren in andere producten en diensten zoals water, telecommunicatie, metaal, chemie, internet en verzekeringen. Enron werd hét voorbeeld voor iedereen die in de nieuwe economie snel veel geld wilde verdienen.

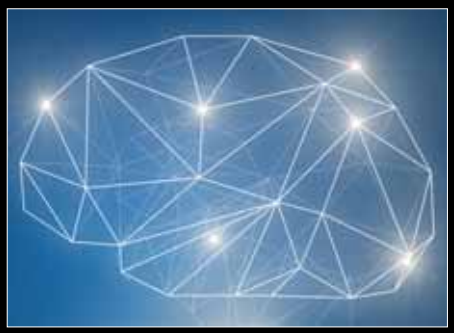
Maar Enron gaf meer uit dan er binnenkwam en hield verliezen met schimmige constructies uit de boeken. De Amerikaanse financiële controlecommissie (SEC) stelde vast dat Enron zijn winsten jarenlang fors had overdreven en 20 miljard dollar rood stond. Ook bleek dat managers miljoenen hadden gestolen en honderden dochterondernemingen hadden opgezet om belasting te ontduiken. In december 2001 was de energiereus failliet en stonden 21.000 werknemers op straat. In januari 2002 startte een strafrechtelijk onderzoek naar Enron, nam de directie ontslag en pleegde een ex-topman zelfmoord. Dit schandaal genereerde wereldwijd veel aandacht voor corporate governance en zorgde indirect voor verscherpte wetgeving op dit vlak zoals Sarbanes-Oxley, Basel II en de Nederlandse Code Tabaksblat.

Arthur Andersen was een van de oudste en meest gerenommeerde accountantskantoren van de Verenigde Staten, maar keurde als accountant van Enron de jaarrekening goed, terwijl dat overduidelijk onterecht was. Toen de Amerikaanse financiële toezichthouder de administratie opvroeg, bleek dat Arthur Andersen veel documenten had vernietigd. Door het Enron-schandaal bestaat Arthur Andersen niet meer.

Met name in het speldomein verliepen de AI-ontwikkelingen stormachtig. In maart 1997 won IBM's supercomputer Deep Blue van de regerend wereldkampioen schaken, Gary Kasparov. In januari 2016 versloeg het AlphaGo Zero-computersysteem de wereldkampioen Go (Lee Sedol), terwijl Go vele malen complexer is dan schaken (9). Volgens de Wet van Moore groeide de verwerkingscapaciteit van computers over de periode 1997 tot 2016 ongeveer met een factor 6000. AlphaGo Zero werkt dan ook fundamenteel anders en leert door tegen zichzelf te spelen (10). Menselijke Go-spelers bereikten het huidige spelniveau in ongeveer 3000 jaar, AlphaGo Zero had maar 3 dagen nodig om daar boven uit te stijgen. In juli 2019 won het Pluribus AI-systeem voor het eerst van de beste menselijke pokerspelers (11). Voor AI is de uitdaging van poker de combinatie van toeval, tactiek en onvolledige informatie. Ook Pluribus leerde poker door 8 dagen tegen zichzelf te spelen. Leren van data uit spelletjes is effectief, omdat het beste algoritme simpel te bepalen is (hint: die wint het meeste).

Machine learning is succesvol in het speldomein, maar daarbuiten is het trainen van AI-systemen veel moeilijker. Behalve het verzamelen van grote hoeveelheden betrouwbare data, bepaalt het domein namelijk mede het succes van de AI-toepassing. Voor bijvoorbeeld weersverwachtingen en aardbevingen gelden de fundamentele onzekerheden van de Chaos-theorie, waardoor heel nauwkeurige voorspellingen onmogelijk zijn. Omdat mensen soms niet-rationele besluiten nemen, geldt dat ook voor economische voorspellingen. Momenteel kunnen de vijf bestaande AI-vakgebieden alleen hun eigen, specifieke problemen oplossen (12).

- Symbolisten gebruiken beslissingsbomen en inductieve logica om te bepalen welke regels het beste de waargenomen data beschrijven en welke nieuwe informatie voorspellingen kan verbeteren. Het algoritme is helder, maar is gevoelig voor overfitting (uitzonderingen in trainingsdata), lokale optima en (nog onbekende) uitzonderingen in de praktijk.
- Connectionisten maken een netwerk van elektronische neuronen om een kunstmatig brein te bouwen. Zo'n netwerk kan leren kankercellen te herkennen op foto's, maar waarom bepaalde kankercellen wel of niet worden herkend (het algoritme) is onduidelijk.
- Genetische algoritmes simuleren evolutie, waarbij oplossingen worden gecodeerd als genen. In de volgende generatie worden de beste genen met willekeurige mutaties gecombineerd, om hopelijk betere oplossingen te krijgen.
- Het Theorema van Bayes geeft aan hoe nieuwe waarnemingen (data) de waarschijnlijkheid beïnvloeden van een oorzaak (hypothese). De uitslagen van (objectieve) medische testen veranderen bijvoorbeeld de geschatte (subjectieve) kans dat een bepaalde ziekte de oorzaak is van de waargenomen symptomen.
- Analogisten bouwen 'support-vector machines' die voor objecten efficiënt analogieën kunnen afleiden uit gewogen informatie van vergelijkbare objecten. Netflix bijvoorbeeld attendeert Alice op een film als Bob die film goed vond en van dezelfde films houdt als Alice. Het probleem is: welke subset van 100.000+ eigenschappen is relevant?



Casus: neuraal netwerk produceert nepnieuws

Menselijke invoer: 'Russia has declared war on the United States after Donald Trump accidentally ...'
AI: '... fired a missile in the air. Russia said it had 'identified the missile's trajectory and will take necessary measures to ensure the security of the Russian population and the country's strategic nuclear forces.' The White House said it was 'extremely concerned by the Russian violation' of a treaty banning intermediate-range ballistic missiles. The US and Russia have had an uneasy relationship since 2014, when Moscow annexed Ukraine's Crimea region and backed separatists in eastern Ukraine.'

De OpenAI Research Group California ontwikkelde voor neurale netwerken het zelflerend algoritme GPT-2 dat het volgende woord voorspelt in teksten (13). Ook na training met 40 GB aan internetteksten produceert GPT-2 nog veel semantische onzin, maar begin 2019 kwam er ook een hoogwaardig nepnieuwtje (zie casus). Nepnieuws is politiek belangrijk zoals de Brexit, Trump en de MH17-ramp laten zien. Door meerdere 'alternatieve

waarheden' te publiceren en onderzoeksjournalistiek te bestrijden wordt de aandacht voor de objectieve waarheid verdund. Met de huidige AI-systemen is het bestrijden van nepnieuws moeilijk (14). GPT-2 komt uit de stal van Elon Musk en is oorspronkelijk tegengehouden vanwege dit nepnieuws. In 02.2019 alsnog vrijgegeven.

Buiten het speldomein zullen AI-toepassingen zich waarschijnlijk geleidelijk ontwikkelen door het proces van probleemoplossing steeds meer te automatiseren. Vroeger was het ontwikkelen van wetenschappelijke theorieën mensenwerk en kostte bijvoorbeeld het handmatig uitrekenen van ingewikkelde formules veel tijd. Tegenwoordig ondersteunt software het bewijzen van hypothesen steeds beter. Wetenschappers richten zich daarom steeds meer op het zodanig formuleren van problemen dat software maximaal kan ondersteunen bij de oplossing ervan. De heilige graal is één AI-systeem te ontwikkelen dat alle problemen acceptabel kan oplossen, maar dat kost waarschijnlijk nog jaren. Grovers kwantumalgoritme om efficiënt te zoeken in databases kan big data en AI-ontwikkelingen versterken. Maar ondanks Nevens wet (de Wet van Moore op anabolen) vergt de ontwikkeling van voldoende krachtige kwantumcomputers meer tijd (15).

Beveiliging van big data en AI

Naast de eerder genoemde generieke maatregelen voor informatiekwaliteit hebben big data en AI-systemen specifieke beveiliging nodig. Zoals bekend zijn big data en AI-systemen erg data-intensief. Wie de beste en meeste trainingsdata heeft, kan de beste big data en AI-systemen ontwikkelen. Omdat AI-systemen zowel data gebruiken voor de training en de werking, zijn ze extra gevoelig voor laagwaardige data (16).

Om de kwaliteit en 'scheefheid' van gebruikte datasets objectief te meten, is naast normen zoals de ISO8000 een bewezen objectieve dataset als 'waterpas' referentie nodig. Voor commerciële bedrijven die innovaties ontwikkelen voor verschillende doelgroepen is dat laatste onpraktisch, vooral als concurrenten meekijken. De datakwaliteit bepaalt namelijk hoe vertrouwelijk big data moet blijven voor concurrenten. Toch moeten bedrijven de informatiekwaliteit beheersen, omdat blindvaren op scheve datasets leidt tot discutabele resultaten (17). De bijsluiter van geproduceerde informatie moet consistent de datakwaliteit vermelden.

AI-systemen worden ook voor cyberaanvallen ingezet. In 2008 ontwikkelde de Carnegie Mellon universiteit een proof of concept-systeem dat automatisch malware kon genereren uit een software-update die buffer overflows repareert (18). In 2009 werd circa 60 procent van de gemelde kwetsbaarheden in software actief misbruikt (19). In 2011 verslechterde deze situatie: ongeveer 97 procent van alle kwetsbaarheden werd binnen twee weken na publicatie misbruikt (20). In januari 2019 meldde het Australische Cyber Security Center dat uit patches voor besturingssystemen binnen 48 uur malware werd ontwikkeld en verspreid (21).
De Carnegie Mellon universiteit won in 2016 met het AI-systeem Mayhem de DARPA Cyber Grand Challenge. Omdat Mayhem volledig automatisch werkte, vond het de meeste kwetsbaarheden in de aangeboden software – ondanks een vroegtijdige crash (22). Deze successen voorspellen dat AI-systemen steeds vaker cyberaanvallen zullen uitvoeren die bovendien effectiever en moeilijker te detecteren zijn.

Casus: 'stealth' malware produceert nepinformatie

Stuxnet was het eerste Cyber Weapon of Mass Destruction dat in juni 2010 werd ontdekt door een fabrikant van antivirussoftware (23). De ontwikkeling van deze geavanceerde worm kostte naar schatting 10 manjaren. Stuxnet infiltreert specifieke Siemens-apparatuur die onder andere ultracentrifuges besturen en zou ontwikkeld zijn om het Iraanse nucleaire programma te saboteren. Stuxnet misbruikt vijf beveiligingsgaten (waarvan destijds vier onbekende Zero Days) om zichzelf te verspreiden via USB-sticks en via LAN's. Stuxnet bevatte een gestolen digitaal certificaat voor installatie en actualiseert zichzelf via een eigen P2P-netwerk. Na installatie verbergt de worm zichzelf via een 'rootkit' en verwijdert zichzelf van USB-sticks na drie infecties. Stuxnet manipuleert een Siemens-stuurprogramma zodanig dat het toerental van de ultracentrifuges op de achtergrond steeds meer varieert, terwijl het dashboard een constant toerental blijft aangeven. Door Stuxnet-besmettingen is in Iran een onbekend aantal ultracentrifuges kapotgeslagen. De broncode van Stuxnet is al in volgende malwaregeneraties toegepast. De gedachte om fake stuurinformatie te produceren is later toegepast in de sjoemelsoftware van Diesel Gate.

Zowel de brondata als kennis over AI-systemen zijn aantrekkelijk voor cybercriminelen (24). Meer nog dan bij big data-systemen

zijn voor AI-systemen daarom zware beveiligingsmaatregelen nodig, zoals een SOC/SIEM met Intrusion Prevention System, systeem hardening, periodieke pentesten en Red Teaming. Daarnaast zijn beproefde normen nodig om de beveiliging adequaat in te richten en te testen.

IT-systemen toetsen kan bijvoorbeeld al met de Common Criteria (ISO15408), maar die zijn niet specifiek bedoeld voor big data en AI-systemen. De JTC 1/SC 42 heeft in juli 2019 drie ISO-normen gepubliceerd voor big data-systemen en ontwikkelt samen met de NEN nog twaalf normen, waarvan tien voor AI-systemen (25).

AI-systemen moeten goed blijven functioneren als ze zelf worden aangevallen. Een AI kan namelijk tijdens een aanval gewoon doorgaan (waardoor ongelukken kunnen ontstaan) of zichzelf uitschakelen, maar met beide uitkomsten is een DOS-aanval succesvol. AI-systemen moeten dus hun doelen bijstellen als er een situatie ontstaat waarin de AI slecht gaat functioneren. Daarvoor moeten AI-systemen complexiteit kunnen reduceren en niet-relevante data kunnen uitfilteren. Met andere woorden: een AI-systeem heeft 'situational awareness' nodig om in een onvoorspelbare wereld effectief te kunnen functioneren. Met de huidige AI-systemen staat dit nog in de kinderschoenen. Zo heeft BMW onlangs data van autosensoren gepubliceerd om gevaarlijke situaties beter te onderkennen (26). Totdat duidelijk is hoe AI-systemen effectief kunnen worden beveiligd, moet hun autonomie mogelijk worden ingeperkt om het restrisico acceptabel te houden.

Conclusie

Informatiebeveiliging voor big data en AI-systemen is belangrijk om informatiekwaliteit te garanderen, maar ook om commerciële innovatie mogelijk te maken. Dit artikel beschrijft welke beveiligingsmaatregelen in deze context relevant zijn. Deze maatregelen zijn niet compleet of in elke situatie geschikt. Zowel voor big data als AI-systemen worden nog normen ontwikkeld. Een adequate beveiliging is voorlopig maatwerk op basis van een risicoanalyse, ook omdat big data en AI-kennis zeer aantrekkelijk zijn voor cybercriminelen. Voor organisaties met big data en AI-systemen is beveiligingsexpertise dus een must-have.

Zoals bekend is een beveiliging nooit perfect. Elke beveiliging kan daarom worden verbeterd na beveiligingsincidenten, gemelde klachten, nieuwe dreigingen voor de organisatie en door systeemwijzigingen te toetsen op hun beveiligingsimpact. Het management moet de beveiliging ook actualiseren als de bedrijfseisen, contractuele eisen, normen of wet- en regelgeving veranderen.

AI kan bestaande aanvalstechnieken verbeteren en snel nieuwe cyberaanvallen lanceren, ook tegen AI-systemen zelf. AI-ontwikkelaars moeten onderkennen dat hun uitvindingen zowel voor goede, als slechte doelen kunnen worden ingezet. Het zijn uiteindelijk mensen die moeten bepalen in welke situaties en onder welke voorwaarden AI-systemen kunnen worden ingezet. In het huidige IT-tijdperk wordt informatiebeveiliging vaak uitgelegd als: hoe beschermen we systemen tegen falen? Maar het ethische principe daarachter is: hoe beschermen we mensen tegen falende systemen?

Referenties

1) De wet van Moore: elke 18 maanden verdubbelt de rekenkracht van computers
2) 'Big Data – for better or worse', SINTEF, 2013
3) Gebaseerd op definities van NORA online en Capgemini
4) Official CISSP CBK ISBN 0-8493-8231-9, blz 324 – 326
5) 'Privacy by design in big data', dec 2015, ENISA
6) Zie de PIA voor Big Data, www.rijksoverheid.nl
7) 'Lost in Translation', aug 2009, https://sma.nasa.gov/
8) www.forumstandaardisatie.nl
9) 'How does the complexity of Go compare with Chess?', 27 jan 2018, www.quora.com
10)' Demystifying AlphaGo Zero', nov 2017, https://arxiv.org
11) AI Beats Professionals in Six-Player Poker', www.cmu.edu
12) The Master Algorithm – Pedro Domingo ISBN 978-0-141-97924-3 blz 21
13) 'Better Language Models and Their Implications', feb 2019, https://openai.com/
14) 'Facebook bestrijdt nepnieuws', NRC 16-04-2019
15) Qutech Annual Report 2018 bevat voornamelijk proof-of-principle vooruitgang; 'Quantum Supremacy Is Coming', 18 juli 2019, Quanta Magazine
16) Zie de morele ontsporing in 2016 van Tay, de chatterbot van Microsoft
17) AI recruiting tool that showed bias against women', Okt 2018, www.reuters.com
18) Automatic patch-based exploit generation', 2008, www.cs.cmu.edu
19) Fortinet Threatscape Report, juni 2009, www.fortiguard.com
20) IBM X-Force 2010 trend and risk report (2011)
21) Assessing Security Vulnerabilities and Applying Patches', Jan 2019, www.cyber.gov.au
22) Mayhem the Machine That Finds Software Vulnerabilities', jan 2019, https://spectrum.ieee.org
23) Dissecting a Cyberwarfare Weapon', mei 2011, https://ieeexplore.ieee.org
24) It is difficult to think of a major industry that AI will not transform' – Andrew Ng
25) https://www.iso.org/committee/6794475.html en www.nen.nl/ai
26) BMW openbaart autodata', NRC 4 juni 2019

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

BLOG

Smoke on the water en security-incidentafhandeling

In 'Smoke on the water' tonen de leden van hardrockformatie Deep Purple zich ware riskmanagers, want ze volgen nauwkeurig de template voor een risico-analyse. De beschreven en werkelijk plaatsgevonden brand leert security-professionals ook andere nuttige zaken.

De titel is voorbeeldig. Door zich daarin te beperken tot de objectief waarneembare rookwolk boven het water, vermijden ze te gehaast genoemde vermoedelijke oorzaken, verantwoordelijkheden, 'schuldigen' en daaruit resulterende financiële aansprakelijkstellingen. Een 'neutrale' titel verhoogt ook bij een security-incident de bereidheid bij een breed lezerspubliek om achteraf een incidentrapport te bestuderen en ervan te leren.

De eerste zin meldt duidelijk waar een en ander zich afspeelt (als eerste punt van de wat, waar, wanneer, waarom, wie en hoe die in een goede risico-analyse aan bod moeten komen). Dat is in Montreux, een kleine stad met ruim 25.000 inwoners. Zwitserland is op zich al geen goedkope plek - hun lage inkomstenbelasting moet immers ergens gecompenseerd worden - maar aan het meer van Genève wordt het zeker duur. Het staat op meerdere plaatsen in het lied: tijd is geld, een race tegen de klok en snelheid van handelen is geboden. Dit kennen wij van het managen van security-incidenten. Deep Purple wilde met het album 'Machine head' hun uitstekende live-reputatie benutten. Van de Rolling Stones (een andere band – mocht u bij generatie X, Y of Z horen) hadden ze een mobiele opnamestudio gehuurd. Deep Purple wilde in het Casino van Montreux het album opnemen, live gespeeld, maar zonder publiek. Ze arriveerden een dag eerder en werden uitgenodigd op 4 december het optreden op het Montreux Jazz Festival van Frank Zappa & the Mothers of Invention bij te wonen. In datzelfde theater, maar helaas - zo bleek later - met publiek. Gehuurde apparatuur in een vrachttruck, en dus buiten het pand, is een heel vroege vorm van cloudtoepassing. De achternaam van bandleider Frank bevat 'app' en zijn begeleidingsband, vernoemd naar 'necessity is the mother of invention' van Griekse filosoof Plato, hield zich met andere woorden bezig met resultaatgerichte 'innovatie'. Dit zijn maar liefst drie IT-toepassingen waar security officers vaak de handen vol aan hebben. Dit omdat de toepassers ervan in hun enthousiasme de ermee samenhangende security- en privacyrisico's weleens onderschatten. Of zelfs compleet vergeten, zodat de afdeling 'security' om 5 voor 12 nog even beveiliging moet toevoegen. Tijdens het nummer 'King Kong' van FZ&TMOI schoot volgens het lied een fan een vuurpijl af, die in het houten dak van het Casino terecht kwam. Maar ooggetuige Peter Schneider schreef in 2009 dat het vermoedelijk geen vuurpijl uit een seinpistool was. Hoewel er toen minder gefouilleerd werd bij concerten dan nu was het ook niet zo dat men allerlei vuurwapens bij zich had. Volgens Peter gooide de aanstichter brandende lucifers in de lucht of schoot hij met zijn rechterwijsvinger een met de kop omlaag en verticaal op het strijkvlak met de linkerduim vastgeklemde lucifer weg. Hoe dan

ook, de balken hingen laag boven de plaatsen achterin en zo vloog het houten dak in brand.
Toen de om zijn excentrieke humor bekende Frank Zappa in het Engels het publiek aanmoedigde om het pand rustig te verlaten, deed men dat - met de toenmalige taalbarrières in 1971 in Zwitserland - gelukkig massaal. Niet door de grote deur naast het podium, want het was onduidelijk of deze deur voor laden en lossen van apparatuur afgesloten was tijdens het concert. Het Casino had een glazen wand over de volle breedte van het pand, zoals ook een organisatie een uitgebreide internetzichtbaarheid kan hebben via web en app. Vaak is er dan een 'cyberautoriteit' aanwezig die bij een grote calamiteit zelfstandig en zonder bemoeienis van de directie kan besluiten om die internetzichtbaarheid tijdelijk geheel uit te zetten, totdat het securityprobleem voldoende is opgelost. Een Zwitserse brandweerman brak met zijn bijl van binnenuit de ruiten, zodat het publiek kon vluchten door een halve of hele verdieping naar beneden te springen. Dus 'people first' qua prioriteit, zoals we dat leren uit het dikke CISSP-boek. Wonder boven wonder vielen er geen doden. Er waren wel snij- en brandwonden, maar slechts een klein aantal personen moest ermee naar het ziekenhuis. Wat betreft de attributie van het incident: de vermoedelijke dader uit Oost-Europa vluchtte na enkele dagen Zwitserland uit. Bij veel security-incidenten (cybercrime, BEC, dDOS, ransomware, spyware) speelt opzet of een menselijke fout een rol en ik adviseer tijdens de incidentafhandeling sporen en aanwijzingen over verantwoordelijke personen duidelijk te registreren. Of in elk geval de aanwezige logging niet uit te wissen bij het opnieuw installeren van de server(s). 'Funky' Claude Nobs, directeur van het Montreux Jazz Festival, hielp mee om mensen te evacueren. Ook bij een security-incident is het goed als het management zich betrokken toont en met hun aanwezigheid het moreel steunt van de securityspecialisten die een nacht of weekend moeten doorwerken om de IT-zaak weer aan de gang te krijgen. En het is naar mijn mening beter om die betrokkenheid niet te tonen door nieuwe verbeteracties te starten of lopende te stoppen, of door als (totale) leek op andere wijze nieuwe prioriteiten in de incidentoplossing op te leggen aan deskundige, ervaren security-experts. Kort nadat iedereen uit het pand was, bereikte het vuur de verwarmingsruimte waarna een grote explosie volgde, daarna de uitslaande brand en toen, door de wind, kwam de rook boven het meer van Genève. Dat inspireerde bassist Roger Glover tot de titel SOTW, waar gitarist Ritchie Blackmore ter plekke de simpele gitaarriff bij bedacht. Eenvoudig, maar wereldberoemd, omdat iedere gitarist hem kan spelen en toepassen.
Door de brand moest Deep Purple uitwijken (nog een securityonderwerp) naar het Grand Hotel in Montreux om daar toch iets 'op tape' te krijgen. Toen analoog op bandrecorders, nu digitaal op een harddisk. Muzikanten en vooral hardrockbands zijn berucht om hun losse seksuele moraal aangaande 'groupies' (de fanatieke vrouwelijke fans). Toch gaat het tekstdeel 'red lights, old beds, place to sweat' over iets anders. In het Grand Hotel, de uitwijklocatie, waren de in geluidsstudio's gebruikelijke signalering (rode lamp = opname loopt, dus stil zijn) geluidsisolatie en demping van de kamerecho niet aanwezig. De ruimte was koud, kaal en leeg en dat wil je niet horen in je opname. Met oude matrassen en rode lampen werd iets geïmproviseerd, wat leidde tot een succesvol album. Ook bij een security-incident, zeker wanneer uitwijk nodig is, is het verstandig om op die andere locatie aanvullende systemen voor signalering en monitoring in te richten en de uitwijklocatie zo goed mogelijk te isoleren van haar omgeving. Uit de eindstrofe blijkt dat er een evaluatie van het incident was. Hoe het verder zal gaan en of het incident nog eens zal gebeuren blijft onzeker, maar dankzij die evaluatie zullen de mannen van Deep Purple nooit vergeten wat ze in Montreux hebben geleerd. Zoals dat wanneer je 's nachts hardrockmuziek opneemt in een luxe hotel, andere gasten gaan klagen over geluidsoverlast. En dat je 'roadies' (sjouwers en geluidstechnici) dan de deuren moeten dichthouden om – gezien de tijdsdruk – te vermijden dat de opgetrommelde politie als 'externe toezichthouder' de opnames midden in een nummer stillegt. Dus een beschermingslaag rondom de uitwijklocatie, die extra is ten opzichte van de normale werksituatie. In plaats van in de uitwijk juist minder securitymaatregelen te gebruiken. Ook dat is een waardevolle les voor ons bij security-uitwijk. Het was een echte pechweek voor Frank Zappa. Zes dagen later sprong een enthousiaste fan op het podium van het Rainbow Theater in London en duwde hem per ongeluk achterover in de betonnen orkestbak. De zanger-gitarist-componist-schrijver moest bijna een jaar in een rolstoel revalideren. Bizar genoeg overleed Frank exact 22 jaar later, op 4 december 1993.

We all came out to Montreux
On the Lake Geneva shoreline
To make records with a mobile
We didn't have much time
Frank Zappa and the Mothers
Were at the best place around
But some stupid with a flare gun
Burned the place to the ground

Smoke on the water, fire in the sky, smoke on the water

They burned down the gambling house
It died with an awful sound
Funky Claude was running in and out
Pulling kids out the ground
When it all was over
We had to find another place
But Swiss time was running out
It seemed that we would lose the race

Smoke on the water, fire in the sky, smoke on the water

We ended up at the Grand hotel
It was empty cold and bare
But with the Rolling truck Stones thing just outside
Making our music there
With a few red lights and a few old beds
We make a place to sweat
No matter what we get out of this
I know we'll never forget

Smoke on the water, fire in the sky, smoke on the water

EVERT VAN ZANTEN

12 jaar diverse ICT rollen en 25 jaar ondernemerschap in ICT, informatiebeveiliging, privacy en social enterprises brachten mij naar vandaag. Vanavond heb ik samen met mijn collega bestuursleden van het PvIB een sessie met onze Adviesraad, de klankbordgroep die ons helpt na te denken over de toekomst van onze mooie vakvereniging. Wie ben ik? Mijn naam is Evert van Zanten. Maatschappelijk betrokken ondernemer. Deler van kennis en ervaring en realistisch idealist.

Sinds begin deze eeuw ben ik erg betrokken bij ons vak, informatiebeveiliging en privacy, als gevolg van een gebeurtenis in mijn privéomgeving. Het bleek destijds dat het als onveilig werd ervaren om medische informatie te delen tussen instellingen. Dit leidde tot het overlijden van een patiënt, mijn oma. Mijn onbegrip hierover zorgde dat de idealist in mij dit gelijk wilde veranderen. Echter, de realist in mij zei dat ik dit niet alleen kan. Verandering moet duurzaam ingebed moet worden wil het op lange termijn kans van slagen hebben. Samenwerken om te bouwen aan een veilige digitale samenleving is sindsdien mijn weg. En wanneer je dan lid bent van het PvIB helpt dat enorm. Zodanig dat ik ook vanzelf de behoefte voelde om daarin wat terug te doen. Na mijn rol als voorzitter van de commissie Kennis & Innovatie ben ik nu lid van het bestuur. Op mijn agenda staat de introductie van 'Werkpakketten' bovenaan. Een nieuwe manier van werken om meer leden de kans te geven iets te doen voor de vereniging, te delen en ervaring op te doen, zonder langdurig commitment. Daarnaast neem ik namens het PvIB als kernadviseur zitting in de Cyber Security Alliantie en ben ik betrokken bij het opzetten van de Nationale Cybersecurity Educatie-agenda.

Het cybersecurity landschap is enorm in beweging. Ik zie hierbij dat het steeds belangrijker wordt om ons vakgebied duidelijker in kaart te brengen. Opleidingen en carrièremogelijkheden moeten gestructureerder en transparanter worden, willen we de uitdagingen van de toekomst met voldoende vakkundige mensen het hoofd kunnen bieden. Daar hebben onze leden en de organisaties waar zij werken iets aan. Als PvIB horen we daar een belangrijke rol in te spelen. Nu ben ik altijd wel een vooruitkijker geweest maar sinds ik trotse opa van mijn eerste kleinzoon ben, kan ik het niet helpen die horizon af en toe nog wat verder weg te leggen. En dan zie je de potentiële impact van onveilig, onbehoorlijk en crimineel gebruik van informatie in onze digitale samenleving. Mij kunnen dan de rillingen over de rug lopen. Bij jullie waarschijnlijk ook.

De positieve energie van onze avonden staat daar gelukkig tegenover. Samen ervaren dat we met velen zijn om dit schrikbeeld af te wenden. Dat zie ik ons dan ook samen doen de komende jaren. Hiervoor moeten we allemaal een rol pakken, zowel als individu en als collectief, bij de komende maatschappelijke ontwikkelingen. Als we dit doen dan ben ik ervan overtuigd dat wij, als PvIB vanuit onze rol en centrale positie in het IB-landschap, dit duurzaam kunnen bewerkstelligen.
Het blijft tenslotte mensenwerk, toch?

Wil je meer weten over wat ik gedaan heb en doe? Kijk dan vooral op mijn Linked-In pagina, Wil je weten wie ik ben? Praat gerust eens met me.

Trusted

Following on from previous articles by The Attributer on the concept of zero trust architecture, we now need to flip the coin and talk about what we might mean by 'trusted'. More to the point, how might we calculate trust levels in a zero-trust architecture model? There are many versions of the zero-trust model. We shall take as a starting point the 'Draft NIST Special Publication 800-207'. At the present time this draft document is out for public comment. The central tenet of the zero-trust architecture is that when requesting access to a resource, no-one is automatically trusted. Just because you can be seen to come from inside the enterprise network does not mean you are a friendly party. 'Don't trust, verify' is the mantra. So, whenever a request for resource access is being considered, we need to have a method of evaluating a trust level that we can associate with that requestor. Depending on the calculated trust level, and on the level required to be granted access, we may or may not allow the request. There is nothing new in checking the authorisation of a requestor against the classification of the resource. Static resource classification and access control decision making have been in use for a long time, such as in multi-level secure systems (MLS). What is new in the zero trust model is its dynamic nature, together with the positioning of the policy decision point (PDP) and policy enforcement point (PEP) as close as possible to the resource. Ideally the PDP/PEP are embedded in the resource itself, as in a data centric security architecture, but that discussion is beyond the scope of this article. Here we will consider only the algorithm for making those access decisions. However, the use of the word 'resources' is important. It includes not only 'data', but also devices that can generate data and information output, such as computational platforms, automated message systems, printers, IoT actuators and any other similar device.

Among the principles of zero trust architecture are:

- the need to make the decisions as granular as possible;
- using as many attributes as possible in support of granularity;
- minimising the time delay between making a decision and its implementation;
- applying the least privilege principle at all times;
- ensuring that the authentication of the user identity is as strong as possible;
- ensuring that the authorisation of the user is current in the context of the system and re-evaluating the authorisation criteria at frequent intervals;
- ensuring that the device used for making the access is itself trustworthy.

The real-time nature of this set of requirements leads to a potentially complex decision making algorithm. The NIST document (see above) provides a conceptual outline for such an algorithm and lists some of the attributes that might be included for scoring the trust level, but it leaves unanswered a variety of questions:

- Is it possible to have a single standard algorithm used by everyone universally?
- Is it even desireable to have a universal standard?
- Or will each enterprise have its own algorithm based on its own risk assessements, in which some user attributes are scored but not others?
- Should the scoring be weighted or simply taken as a binary value?
- How will the performance target be determined for access to be granted?
- What form will the algorthim take?

To answer that last of these questions we simply need to look at how any programmatic process is described using statements such as:

IF <boolean expression>
THEN *action 1*
ELSE *action 2*
END;
CASE

WHEN *condition1* THEN *result1*
WHEN *condition2* THEN *result2*

WHEN *conditionN* THEN *resultN*
ELSE *exception*

END;

So there we have a way of developing the trust algorithm, but one thing is still missing – the business driven approach that is at the heart of SABSA. The zero trust architecture approach is a means to ensure that the access to enterprise resources is based on business risk. That only works if you have a holistic end-to-end means of determining business risk and using the results to drive your security architecture. Zero trust may be the latest buzz-word, but without the context of SABSA it will not deliver any benefits.

The Attributer

De auteurs hebben het artikel op persoonlijke titel geschreven. Ruud Wissenburg is IT-Auditor bij de Rijksoverheid. Ruud is bereikbaar via ruudwis@tele2.nl. André Melisse is security management consultant bij Atos. André is bereikbaar via andre.melisse@atos.net. Karel van Oort is freelance security management consultant. Karel is bereikbaar via kvoort@securia.nl.

Een praktijkcase: van incident-gedreven naar in control

De steeds groter wordende digitale dreigingen, zowel in aantal als grootte, en de strenger en complexer wordende normen en wetten maken de inrichting van een adequate informatiebeveiliging er niet makkelijker op, maar wel noodzakelijker.

De Rijksoverheid heeft de Baseline Informatiebeveiliging Rijksdienst (BIR) in 2012 vastgesteld als minimum beveiligingsniveau voor de verwerking en opslag van informatie met rubriceringsniveau 'departementaal vertrouwelijk'. Inmiddels is hiervan in 2017 en 2019 (hernoemd in BIO (1)) een update verschenen. Als het gaat om het inrichten van een adequate informatiebeveiliging zie je vaak dat de verschillende departementen worstelen dit voor elkaar te krijgen. Tijdens de Verantwoordingsdag 2018 (iedere 3e woensdag in mei) gaf Arno Visser, president van de Algemene Rekenkamer (ARK), dit ook aan: "Veel van de problemen in de bedrijfsvoering hebben net als vorig jaar te maken met het thema informatiebeveiliging. Dit jaar is dat bij 9 departementen en bij de Tweede Kamer een probleem." In de 'Staat van de rijksverantwoording 2017' wordt dit ook nog in een historisch perspectief geplaatst (2). Waar over het algemeen de onvolkomenheden bij andere onderzoeksonderwerpen dalen, stijgen deze juist bij ICT en informatiebeveiliging.
Nog enkele andere citaten uit hetzelfde document:

"De informatiebeveiliging schiet op de departementen al jaren tekort …" (p. 42)

"De urgentie om de informatiebeveiliging goed op orde te hebben is groot. Maar dat lukt de rijksoverheid nog niet erg." (p. 44)

"Beperkt zicht op kwaliteit informatiebeveiliging." (p. 45)

In zijn toespraak stelt Arno Visser verder dat de meeste onvolkomenheden op het gebied van informatiebeveiliging voortkomen uit capaciteitsgebrek. De auteurs keken met belangstelling uit naar de Verantwoordingsdag van 2019. Zou er verbetering te zien zijn? Helaas, "Problemen spelen er nog altijd bij het beheer van ICT op de departementen, waaronder de informatiebeveiliging. Hieruit blijkt dat het beheer van ICT eerder verslechterd dan verbeterd is." (3) Dit wordt geïllustreerd in onderstaande grafiek uit het rapport. (4)

Wat zien wij in de praktijk? De auteurs van dit artikel hebben bovenstaande constateringen van de ARK ook ervaren. Zij werden met deze situatie geconfronteerd bij de afdeling die verantwoordelijk is voor het beheer van een grote IT-infrastructuur binnen een overheidsorganisatie. Deze afdeling nam weinig tijd de informatiebeveiliging structureel goed in te richten en ervoer hierdoor een grote auditdruk. De organisatie was vooral incident-gedreven bezig. Een pas op de plaats was nodig. Hierdoor ontstond ruimte om na te denken over een

Figuur 1 – Onvolkomenheden voor ICT in 2012-218, onderverdeeld naar IT-beheer en informatiebeveiliging.

gestructureerde aanpak om van incident-gedreven naar in control te komen. Wat houdt 'in control' in? De BIO biedt hiermee de basis om te zorgen dat de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de overheid bevorderd wordt. Deze bedrijfsonderdelen kunnen erop vertrouwen dat gegevens die worden verstuurd of worden ontvangen door andere onderdelen van de overheid in lijn met wet- en regelgeving passend beveiligd zijn. Waar naleving (nog) niet volledig mogelijk is, dienen de bedrijfsonderdelen via een 'explain' de eventuele risico's inzichtelijk te maken aan hun ketenpartners (5).

Voldoen aan de BIO, weten wat er wel/niet op orde is en weten wat je eraan gaat doen. De vraag, die dan logischerwijze opkomt, is: hoe doe je dat dan?

Aanleiding

De wil om de dingen goed te doen was er binnen deze organisatie, maar de tijd en focus niet. Om tijdens de 'verbouwing' met de operatie gewoon door te kunnen gaan, werd de auteurs van dit artikel gevraagd een aanpak op te stellen, deze tot uitvoer te brengen en te borgen in de organisatie. Binnen de organisatie was wel kennis van informatiebeveiliging aanwezig, maar deze werd niet optimaal ingezet als gevolg van het 'brandjes blussen'. Desalniettemin was er behoefte aan verdieping van de informatiebeveiligingskennis en daarbij werd niet gedacht aan iedereen op een ISO 2700x-cursus sturen, maar aan een meer hands-on- aanpak. De auteurs hebben een methode ontwikkeld die de invoering van de BIO ondersteunde en waarmee tegelijkertijd de bekendheid met de BIO werd verhoogd. Vragen die spelen omtrent de achterliggende redenen van een norm (waarom moeten we dit nu doen?) werden meteen beantwoord. Dit alles gebeurde in een gestructureerde vorm van workshops

met component verantwoordelijke, product en technisch specialisten. Voor deze aanpak was het vereist dat ieder van de desbetreffende specialisten tien werkdagen beschikbaar was. Dit geheel wordt 'de wasstraat' genoemd. Zoals aangegeven was het erg moeilijk om de operatie door te laten gaan tijdens deze workshops. Het commitment van het management was dan ook een kritieke succesfactor. Zie voor andere kritieke succesfactoren het kader.

Doel wasstraat

Het doel van de wasstraat is het overbruggen van de kloof tussen abstracte regelgeving en beveiligingsbeheer. Beleidsdocumentatie beveiligt namelijk niet, maar de beveiligingsinstellingen in de IT-systemen wel. De wasstraat is een combinatie van een zelfevaluatie en een awareness - programma, waarin meerdere deelnemers uit meerdere disciplines bespreken en vastleggen hoe de informatie beveiliging moet zijn ingericht. Deze methodiek geeft inzicht in hoeverre een component compliant is en voldoet aan het betreffende normenkader en levert een aantal concrete resultaten op, te weten:

- inzicht in de afwijkingen;
- openstaande risico's;
- de benodigde verbetermaatregelen;
- benodigde capaciteit voor realisatie verbetermaatregelen.

Doordat de deelnemers aan de workshops inhoudelijk worden begeleid en gedurende deze periode intensief met het onderwerp informatiebeveiliging bezig zijn, ontstaat er een bijvangst in de vorm van een verhoogd kennisniveau met betrekking tot informatiebeveiliging (awareness).

Na afloop van het wasproces (zie hieronder) stelt de componentverantwoordelijke een verbeterplan en een in controlverklaring op waarin wordt aangegeven wat de status van de component is in relatie tot het normenkader. Deze documenten dragen bij aan een aantoonbare onderbouwing van het 'in control' zijn van de organisatie op het gebied van informatiebeveiliging ('bewust onbekwaam').

Een template vormt de basis voor een workshop. Tijdens de workshop wordt de template gezamenlijk ingevuld. Het resultaat van de ene workshop is input voor de volgende. Wat de deelnemers eerst zien als een complex probleem, wordt door de gehanteerde methode in kleine denkstapjes opgedeeld.

Wasproces

Het wasproces bestaat uit vier fasen: scopebepaling, normselectie, maatregeldefinitie en borging en verbeterplan. Deze fases worden met workshops doorlopen, ondersteund door:

- ervaren informatiebeveiligingsadviseurs;
- een gefaseerd en gestructureerd proces;
- een documentmanagementsysteem;
- standaard templates;
- rapportages.

Fase één: scopebepaling

De componentbeschrijving bepaalt de scope. Om de scope goed te kunnen bepalen, is een duidelijke beschrijving en afbakening randvoorwaardelijk. Om dit te bewerkstellingen wordt een kwaliteitscheck gedaan op de componentbeschrijving. De controles richten zich onder andere op:

- eigenaarschap van het object;
- rollen, taken en verantwoordelijkheden;
- afnemers en toeleveranciers;
- borging van de beschikbaarheid, integriteit en vertrouwelijkheid (BIV).

In de eerste workshop wordt middels een business impactanalyse de BIV-classificatie bepaald.

Fase twee: normselectie

In deze fase stellen de deelnemers vast of een norm 'wel' of 'niet' van toepassing is met 'comply or explain'. Het kan zijn dat de betreffende norm al is geborgd, doordat dit als een dienst bij een andere afdeling wordt afgenomen ('elders belegd').

Fase drie: maatregeldefinitie en borging

In fase drie wordt voor alle van toepassing zijnde normen een maatregel beschreven. Op een SMART-wijze wordt aangegeven hoe aan de desbetreffende norm wordt voldaan, inclusief documentverwijzingen. Wanneer een norm is geborgd bij een derde partij (in- of extern) dient dit te zijn vastgelegd in een afsprakenkader.

Tijdens fase twee en drie maken de deelnemers gebruik van een normenkader-template dat is verrijkt. Door het normenkader te verdelen in thema's kunnen snelle, gebundelde selecties worden gemaakt. Denk daarbij aan het clusteren van normen die gerelateerd zijn aan bijvoorbeeld: werkplek, netwerken, autorisaties, awareness, operationele security baseline en patchen. Daarnaast zijn standaardteksten opgenomen voor de normselectie en maatregeldefinitie, die hel-

pen generieke oplossingen te definiëren. Dit levende document fungeert als een kapstok voor het verdere gehele wasproces.

Fase vier: verbeterplan

Fase vier is de laatste stap, waarin alle normen worden verzameld die niet zijn geborgd. Uit deze verzameling wordt een verbeterplan opgesteld, voorzien van een planning.
Ook kan worden bepaald dat sommige verbetermaatregelen nog even in de ijskast worden gezet en dus het risico (voorlopig) wordt geaccepteerd. Dit verbeterplan wordt in hetzelfde centrale register als auditrapporten gemanaged. Tevens wordt door de componentverantwoordelijke een in control-verklaring opgesteld waarin de actuele status van de omgeving wordt vastgelegd.

Tijdens de uitvoering van het wasproces zijn de volgende kritieke succesfactoren naar voren gekomen:

- zichtbaar draagvlak en commitment topmanagement (kick-off en mandaat);
- aansturing van het wasproces door een aangewezen MT-lid;
- borging in de lijn/organisatie;
- sturen op afspraken (afspraak = afspraak);
- motivatie dient minimaal op het niveau van acht te zijn (schaal 1-10);
- juiste kennis en kunde dient tijdens het wasproces dedicated beschikbaar te zijn;
- het volgen van het gedefinieerde wasproces.

Na afloop van ieder wasproces vindt een evaluatie plaats. Hieruit blijkt dat over het algemeen de deelnemers lovend zijn over het wasproces. Enkele mooie woorden uit de evaluaties:
"Ik ben zeer positief over de aanpak, vooral wetende hoe dit in het verleden over jaren werd uitgestrekt, met weinig concrete verbetering tot gevolg."
"Alle betrokkenen droegen hun steentje bij op hun vakgebied. Iedereen vulde elkaar mooi aan."
"Ik vond de methode van het wassen en de prioriteit die het management eraan heeft gegeven erg goed. In mijn ogen de enige manier om meters te maken in het traject voor de accreditatie van de bouwsteen."
"Strakke tijdslijnen en iedere dag tijdens aanvang en afsluiting bepalen wat te doen die dag en de dag evalueren."
"Het heeft mij in ieder geval meer inzicht gegeven en de ogen geopend dat zaken die wij als normaal beschouwen anders moeten worden aangepakt."
"Met het verbeterplan maak je duidelijk keuzes wat je komend jaar wel en tevens niet oppakt. Dit helpt zeker als onderbouwing bij bijvoorbeeld audits."

Het wasproces is ook recent geaudit op opzet, bestaan en werking. De samenvattende boodschap van de auditresultaten: het wasproces is degelijk en leidt tot voorspelbare en consistente output.

En dan?

Dan is alles geanalyseerd, maar dan ben je er nog niet. De componentverantwoordelijke weet dan waar de kwaliteit van de informatiebeveiliging van zijn component moet worden verbeterd. Voor de korte termijn gaat men aan de slag met het verbeterplan. Op dit moment ontwikkelen de auteurs voor de langere termijn een procesmodel (een zogeheten 'wiel van verbetering') waarmee de onderliggende oorzaken van het achterblijven op IB-gebied worden aangepakt.

Referenties

(1) Baseline Informatiebeveiliging Overheid, v1.0.3
(2) Staat van de rijksverantwoording 2017, Algemene Rekenkamer, p.40
(3) Staat van de rijksverantwoording 2018, Algemene Rekenkamer, p. 27
(4) Staat van de rijksverantwoording 2018, Algemene Rekenkamer, p. 35
(5) Bron: Baseline Informatiebeveiliging Overheid, v1.0.3, p.3

Inge Wetzer & Elke Weijkamp zijn sociaal psycholoog Security & Compliance bij Hoffmann. Inge is bereikbaar via i.wetzer@hoffmann.nl.

Dit is het eerste artikel van de drieluik 'Het meten van gedrag in de cybersecurity'

Een psychologische benadering van awareness in cybersecurity

Medewerkers geven hun wachtwoord niet weg via de telefoon, toch?

Bij veel organisaties wordt ervan uitgegaan dat medewerkers zich steeds cyberveiliger gaan gedragen. Medewerkers halen immers massaal 90-100% scores op awareness-testen over cybersecurity. Ze spelen e-learnings over het gebruik van veilige wachtwoorden helemaal uit tot het groene vinkje in beeld is en ze kijken iedere dag naar de liftposter waarop staat dat je niet op linkjes van onbekende e-mails moet klikken. Toch blijkt in de praktijk dat men zich lang niet altijd zo cyberveilig gedraagt als dat we denken

Het gebruik van zeer eenvoudige wachtwoorden of het onbeveiligd versturen van bedrijfs- of persoonsgevoelige informatie blijken bijvoorbeeld geen uitzondering te zijn. Dit roept direct de volgende vraag op: wat is dan het effect van al deze initiatieven om awareness te verhogen? Op die vraag kan maar één antwoord worden gegeven: awareness is níet hetzelfde als gedrag. Dit artikel zoomt in op het verschil tussen awareness en gedrag én laat zien hoe dit verschil gemeten kan worden. Dit betreft het eerste artikel van een drieluik omtrent het meten van cyberveilig gedrag en de daarbij aansluitende adviezen om te kunnen groeien naar dit gewenste gedrag.

Werkgevers verwachten cyberveilig gedrag

Werkgevers verwachten veilig gedrag van hun medewerkers, zeker op het gebied van cybersecurity met alle vaak onherstelbare imago- en financiële schade op de loer. Dit belang is ook terug te zien in de miljoenen die het kabinet uittrekt voor onderzoek hoe cybercriminaliteit moet worden tegengegaan (1). Naast technologische en organisatorische maatregelen wordt er sinds een paar jaar gestuurd op de cyberveiligheid van medewerkers binnen organisaties. Werkgevers zijn in steeds grotere mate bereid om hierin te investeren om de organisatie te beschermen. Opvallend is echter de manier waarop hier aandacht aan wordt besteed. Er wordt namelijk nagenoeg uitsluitend ingezet op het verhogen van awareness. Alle e-learnings, games en liftposters om het gedrag van mensen te veranderen zijn gestoeld op deze awareness, ofwel het verhogen van kennis en bewustzijn. Na de inzet van bijvoorbeeld een e-learningprogramma ziet men graag terug hoe medewerkers hierop hebben gescoord. Dit doet men veelal om ten eerste te kunnen laten zien dat er aandacht aan besteed is en daarnaast om een mogelijke verbetering over de tijd vast te kunnen leggen. Een awarenesstest, e-learning of game meet echter de mate van kennis en het bewustzijn over het gedrag dat wordt gevraagd. Ofwel, er wordt gemeten of men weet hoe men zich zou moeten gedragen. De groene vinkjes en scores worden toegekend wanneer men de gewenste antwoorden geeft over het gedrag wat van hen wordt verwacht. Dit zegt niets over wat men feitelijk dóet. Daarom zeggen deze uitslagen meestal weinig over ons daadwerkelijke gedrag, ondanks alle goede intenties en de eerlijkheid waarmee de testen of vragenlijsten worden ingevuld.

Hoe gedrag dan wel gemeten kan worden, is een ingewikkeld issue. Het kunnen meten van gedrag op zich is al niet eenvoudig, laat staan cyberveilig gedrag. Cyberveilig gedrag is een verzamelterm voor allerlei soorten gedragingen die bijdragen aan cyberveiligheid op de werkvloer. Het omvat vele aspecten, onderwerpen en gedragingen waar men dagelijks mee te maken heeft. Denk bijvoorbeeld aan het gebruik van een sterk wachtwoord, het herkennen van phishing e-mails, het veilig opslaan en versturen van vertrouwelijke documenten, het niet delen van je wachtwoorden of het locken van computers bij (korte) afwezigheid. Deze veelomvattendheid maakt het moeilijk om te benoemen wanneer men zich nou volledig cyberveilig gedraagt. Om cyberveilig gedrag toch meetbaar te maken, zal men zich in eerste instantie moeten focussen op meetbare aspecten van cyberveilig gedrag, zoals 'pc locken', 'aanspreken van onbekenden zonder pas', een sterk wachtwoord, etcetera.

Uit gesprekken met werkgevers komt vaak naar voren dat zij ervan uitgaan dat hun medewerkers zich gedragen naar de kennis die zij hebben. Dat zij dus doen wat ze zouden moeten doen. De vraag is of dit laatste wel zo is en waar dit uit blijkt (uit alle 100% scores die medewerkers halen op awareness-

testen). Dit is opmerkelijk te noemen, omdat men in het dagelijks leven veelvuldig geconfronteerd wordt met het feit dat iets wéten niet zomaar leidt tot iets dóen: we weten dat we vlak voor het slapen gaan niet meer naar digitale schermen moeten kijken, we weten dat we voldoende moeten bewegen en we weten dat we de telefoon niet moeten gebruiken in de auto of op de fiets. Dit weten we allemaal, maar we gedragen ons er niet altijd naar (2). Waarom verwachten we dan wanneer medewerkers bewust gemaakt worden van de gevaren op het gebied van cybersecurity dat men zich ineens veilig gaat gedragen?
Het signaal is duidelijk: wéten wat je zou moeten doen betekent dus niet je het ook daadwerkelijk doet. Voor ons, psychologen van Hoffmann, de hoogste tijd om te laten zien wat de focus op gedrag oplevert ten opzichte van de focus op awareness. De intentie was om in kaart te brengen of hetgeen dat nu wordt gedaan om medewerkers te ondersteunen, het gewenste effect heeft waar veelal vanuit wordt gegaan. Of op wordt gehoopt.

Meten biedt inzicht

Het doel van het onderzoek was het aantonen van de kloof tussen awareness en gedrag op het gebied van cyberveiligheid. Om deze reden werd gezocht naar gedrag waarover geen discussie rondom awareness zou zijn. Ofwel: gedrag waarvan iedereen weet dat het wenselijk is. In een eerste fase werden verschillende gedragingen met medewerkers van uiteenlopende organisaties besproken en werd bepaald in hoeverre awareness een rol speelde. De uitkomst was de gedraging waarvan 'awareness' het minst een rol speelde. Dit was: geen wachtwoorden delen wanneer dit per e-mail of telefonisch door een onbekende beller wordt gevraagd. Iedereen wéét dat je dit niet zou moeten doen, ofwel, het bewustzijn is op orde! Deze gedraging werd vervolgens nader onderzocht aan de hand van een methode die veelvuldig door cybercriminelen wordt toegepast, namelijk door middel van een vorm van social engineering: voice phishing.

Inspelen op gedrag door vertrouwen

Voice phishing, ook wel vishing genoemd (3), is een aanvalstechniek om mensen te misleiden en toegang te krijgen tot belangrijke informatie. Deze manier van aanvallen is gericht op een persoon of organisatie die via het persoonlijk handelen van een medewerker wordt benaderd. Er wordt voornamelijk ingespeeld op het vertrouwen in de medemens. Het betreft eigenlijk emotionele manipulatie door in te spelen op bijvoorbeeld de angst om iets te verliezen. Door middel van telefonisch contact wordt er geprobeerd om informatie van medewerkers, klanten of organisaties te achterhalen zoals gebruikersnamen, wachtwoorden, burgerservicenummers of bankgegevens. Deze gegevens kunnen bijvoorbeeld worden gebruikt om rekeningnummers van klanten bij organisaties te wijzigen, waarna uitbetalingen nooit bij de klanten terechtkomen maar via de gewijzigde rekeningnummers door de fraudeurs kunnen worden weggesluisd. Deze gegevens kunnen ook dienen als input voor scenario's voor onder andere CEO-fraude om zo financieel gewin te behalen. Iemand doet zich bijvoorbeeld telefonisch voor als een bekende beller en heeft vaak vooraf veel informatie over de organisatie, klanten of medewerkers verzameld waardoor het echt lijkt alsof diegene intern bij de organisatie betrokken is. Zo wint diegene het vertrouwen van de medewerker.

Het onderzoek

Om aan te tonen dat in cybersecurity onveilig gedrag optreedt dat niet door het verhogen van awareness tot veiliger gedrag leidt, is door middel van voice phishing onderzocht of medewerkers van uiteenlopende organisaties hun wachtwoord delen wanneer er telefonisch contact met hen wordt opgenomen. Dit betreft dus gedrag waarbij we verwachten dat awareness tegenwoordig toch geen issue meer zou moeten zijn.

In het onderzoek is telefonisch gesproken met 226 medewerkers van in totaal 33 organisaties. Alle data van organisaties die voor dit onderzoek geanalyseerd zijn komen voort uit opdrachten van de desbetreffende organisaties zelf. Opdrachtgevers (bijvoorbeeld CISO's of/en leden van het managementteam) gaven de opdracht om hun organisatie te testen door het gedrag van hun medewerkers in kaart te brengen. Aan de hand hiervan konden de organisaties zich (waar nodig) beter weren tegen echte aanvallen. Door de sterktes en zwakheden op basis van deze testen uiteen te zetten werd duidelijk aan welke knoppen gedraaid kon worden om veiliger gedrag te realiseren. Hierbij is gebruik gemaakt van twee verschillende scenario's, afhankelijk van de vraag van de desbetreffende organisatie.

In het eerste scenario zijn medewerkers telefonisch benaderd en gevraagd of zij toegang tot een computer hadden. Vervolgens werd hen met een slim verhaal over veiligheidsinstellingen verzocht een webpagina te openen. Na een aantal vragen en een gesprekje om vertrouwen te winnen, vroeg de beller of zij op de site hun logingegevens, gebruikersnaam en wachtwoord wilden invullen. De gebruikte webpagina bevatte altijd het logo van de organisatie. Wanneer de medewerkers hun gegevens invulden, kwamen deze direct bij de onderzoekers binnen. De medewerkers sloten de

webpagina weer, omdat het 'probleem' waarvoor ze gebeld werden ogenschijnlijk was opgelost.

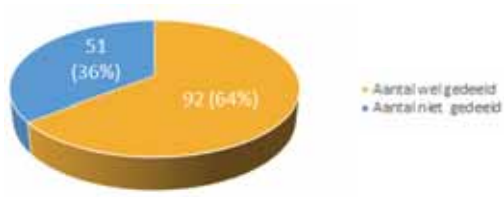
Scenario twee betrof het telefonisch vragen van het wachtwoord van het persoonlijke gebruikersaccount van de medewerker zonder het gebruik van digitale hulpmiddelen. Voor een klein deel van de onderzoeksgroep zijn - op verzoek van de organisatie - op deze manier niet de wachtwoorden maar de burgerservicenummers gevraagd.

Scenario's aan de hand van open bronnenonderzoek

Voordat medewerkers telefonisch werden benaderd, werd er eerst per organisatie en per medewerker een vooronderzoek uitgevoerd. Dit vooronderzoek betrof een open bronnenonderzoek om kenmerken van de organisatie, de medewerker, diens mogelijke klanten of collega's in kaart te brengen. Dit werd gedaan via sociale media zoals Facebook, Twitter, LinkedIn en andere bronnen zoals websites van de organisaties, leveranciers of klanten. Zo kon er bijvoorbeeld gebruik worden gemaakt van een naam van een bekende en werden details genoemd, waardoor de medewerker minder zou twijfelen aan de echtheid van de beller of diens verzoek. De verzamelde persoonlijke gegevens werden na het gesprek gewist.

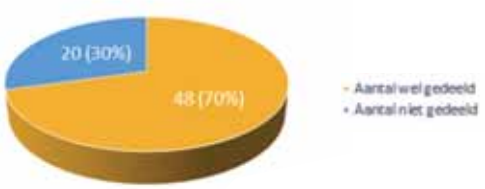
Resultaten

Met behulp van de informatie die aan de hand van het vooronderzoek in kaart was gebracht zijn er 143 medewerkers gebeld met scenario 1. De resultaten liegen er niet om: voor gedrag waarvan we tegenwoordig verwachten dat awareness geen issue meer is, heeft 64% van de medewerkers zijn gebruikersnaam en wachtwoord via de link ingevuld



Figuur 1 - Totaal aantal medewerkers dat op de website hun wachtwoord wel of niet heeft ingevuld (n=143).

Bij sommige organisaties was de reactie dat men zich kon voorstellen dat medewerkers op een website hun wachtwoord zouden invullen als dit door IT of de systeembeheer telefonisch werd gevraagd. Daarom zijn de resultaten van het tweede scenario erg interessant. Die tonen namelijk aan dat ook zónder een dergelijke website het merendeel van de medewerkers mondeling zijn/haar wachtwoord weggeeft aan een onbekende beller. Maar liefst 70 procent van de 68 gebelde medewerkers deelde telefonisch zijn of haar wachtwoord (figuur 2). Daarnaast is aan 15 medewerkers het BSN gevraagd, dat door 10 van hen (67 procent) werd gedeeld.



Figuur 2 - Aantal medewerkers dat hun wachtwoord telefonisch wel of niet afgeeft (n=68).

Conclusie

Aan de hand van het onderzoek kan worden vastgesteld dat ook op het gebied van cyberveiligheid iets wéten niet hetzelfde is als iets dóen. Zelfs bij gedrag waarvan de awareness anno 2019 heel erg hoog is, handelt men toch onveilig. Het merendeel van de onderzochte medewerkers deelde telefonisch zijn/haar wachtwoord. Uit dit onderzoek kunnen we concluderen dat in cybersecurity er een kloof heerst tussen awareness en gewenst cyberveilig gedrag.
Dit inzicht brengt ons een stap dichter bij de oplossing. Het is nu immers helder dat initiatieven aan de menskant niet blind moeten worden ingezet op awareness. Awareness is niet het einddoel. In plaats daarvan zal daadwerkelijk gedrag het einddoel moeten worden van de campagnes. Eén ding is zeker: als nog ruim 67% van de medewerkers hun wachtwoord weggeeft aan een onbekende beller, is er nog veel winst te behalen op het gebied van cyberveilig gedrag.
In het tweede deel van dit drieluik zal dieper in worden gegaan op meetmethoden voor gedrag. Het beargumenteert waarom vragenlijsten niet voldoende zijn om redenen voor (on)veilig gedrag bij medewerkers te meten. Daarnaast belicht het een methodiek die beter geschikt is om inzicht in gedrag te verkrijgen, namelijk het semigestructureerd interview op basis van concreet gedrag. Er wordt stilgestaan bij de meting op basis van interviews, bevindingen en daaruit voortvloeiende aanbevelingen, zodat medewerkers zich daadwerkelijk cyberveiliger zullen gedragen.

Referenties

(1) Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/cybercrime/-cybercriminaliteit-bestrijden
(2) Wetzer, I.M. (2018). Cyberveilig gedrag: Waarom doen we het nou niet? Informatiebeveiliging, 18 (1), 12-15.
(3) FraudWatch (2019). What is Vishing? Voice Phising Scams Explained & How to Prevent Them. FraudWatch International

Maurice Gittens werkt momenteel als IT risk manager bij een financiële instelling.
Maurice is bereikbaar via: maurice@gittens.nl.

De risicomatrix en een alternatief

De risicomatrix is een alom bekend hulpmiddel voor risicomanagement en derhalve ook voor informatiebeveiliging. Voor de bewustwording en de eerste maturiteitsniveaus van risicomanagement is dit een bruikbaar instrument gebleken, maar waarschijnlijk komt dit vooral door gebrek aan een beter alternatief. Dit artikel suggereert de eenheidscirkel als een alternatief dat door de definitie van risico volgens ISO 31000 is geïnspireerd. Of het alternatief beter is, mag u als lezer zelf bepalen.

Voor een risicomanager is het inschatten van risico's een van de basisactiviteiten die horen bij het vak. Vaak wordt na een scenarioschets - op basis van gebrekkige ondersteunende informatie en onder tijdsdruk - een risicoassessment door stakeholders verwacht dat ondersteunend is aan besluiten die vervolgens genomen worden.
Het hulpmiddel dat bij uitstek in dit verband wordt gebruikt is de risicomatrix waarvan een voorbeeld in figuur 1 getoond wordt.

Figuur 1 – Risicomatrix.

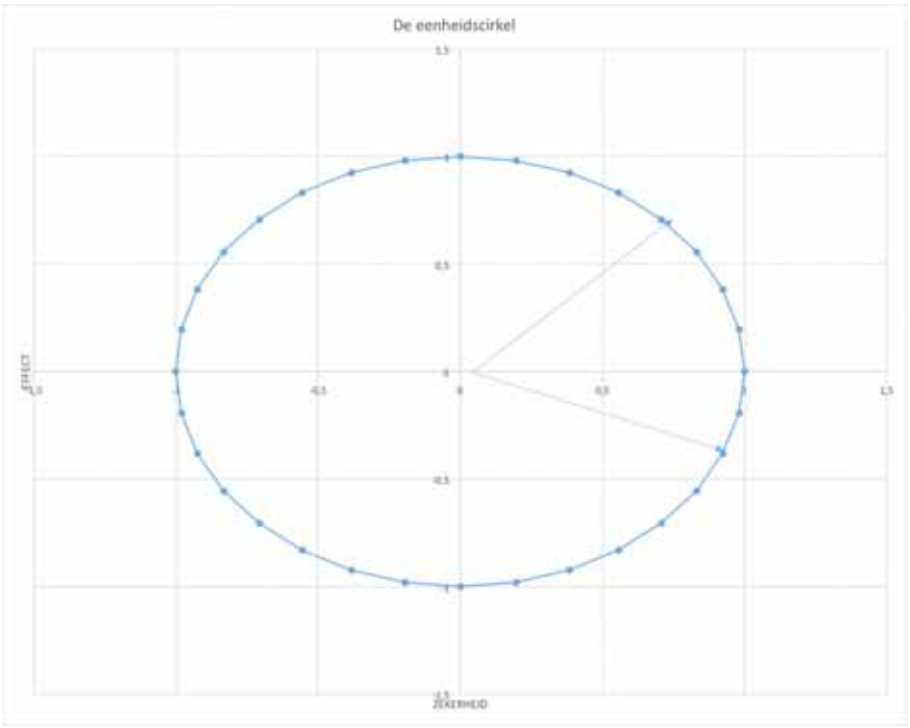
In een artikel uit 2008 met als titel 'What's wrong with the Risk Matrix' (1) onderzoekt Louis Cox de wiskundige kenmerken van de risicomatrix en zijn bevindingen liegen er niet om. De geschiktheid van risicomatrixen wordt met formeel onderbouwde argumenten sterk in twijfel getrokken. Sommige tekortkomingen die Cox benoemt liggen voor de hand, maar dat geldt zeker niet voor allemaal. In dit artikel wijzen we op drie hoofdbeperkingen van risicomatrixen volgens Cox:

- Door de lage resolutie van doorsnee risicomatrixen is de volledigheid, correctheid en ondubbelzinnigheid van risicoanalyses op basis van deze matrixen te betwijfelen.
- Voor risico's met een negatieve correlatie tussen impact en waarschijnlijkheid zijn er significante inconsistenties aan te wijzen, die het hulpmiddel contraproductief laten zijn. Het artikel gebruikt in dit verband de frase 'worse than useless'.
- De interpretatie van risicomatrixen kan subjectief zijn.

Op basis van eigen ervaring zijn de volgende observaties toe te voegen:

- De risicomatrix kan de indruk laten ontstaan dat impact altijd negatief of altijd positief is.
- Risico-aggregatie met behulp van risicomatrixen is geen algemeen aanvaarde aanpak.

Cox adviseert dat risicomatrixen met voorzichtigheid gebruikt dienen te worden en uitsluitend met een vastlegging van geldende assumpties. Andere auteurs zijn minder subtiel (3).
Risicomanagement is voor mij een formele wetenschap en mijn streven is telkens het zoveel mogelijk reduceren van het subjectieve. Ik stel dat het streven naar de reductie van sub-



Figuur 2 – Eenheidscirkel.

jectiviteit ondersteund wordt door de definitie van risico dat ISO 31000 biedt. Volgens deze definitie is risico het effect van onzekerheid op geldende doelstellingen. Gegeven deze definitie van risico is de volgende vraag voor de hand liggend: als het effect van onzekerheid nihil is, mogen we dan zeggen dat risico nihil is?

Drie assumpties

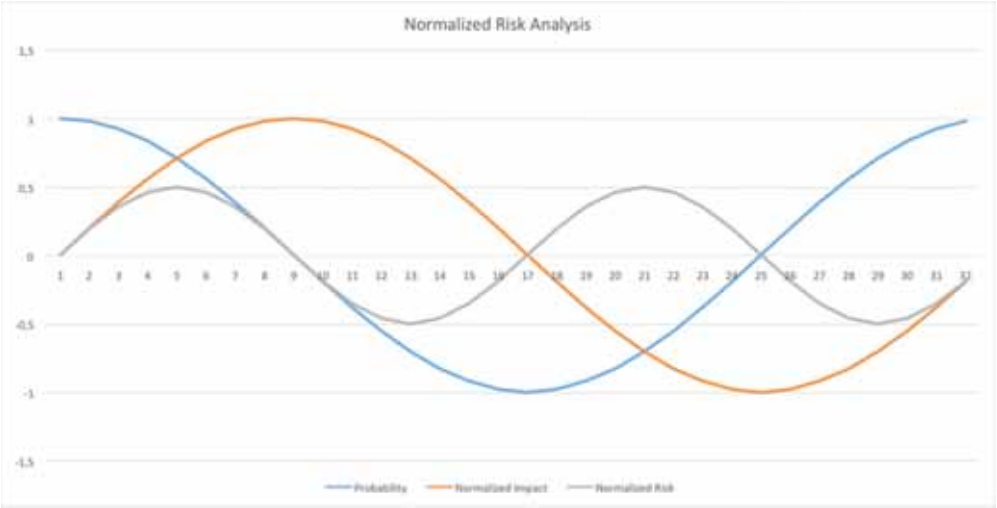
In het verdere van dit artikel wordt een bevestigend antwoord verondersteld en deze veronderstelling noem ik `assumptie 1'. De tweede assumptie die we maken in dit artikel is dat het effect van onzekerheid te normaliseren is als een percentage tussen 0 en 100%. De derde assumptie die we maken is dat een genormaliseerd risico het product is van: zekerheid, in procenten is uitgedrukt en een genormaliseerd effect heeft.
We gebruiken een eenheidscirkel (zie figuur 2) om de beoogde relatie tussen zekerheid en haar effect op geldende doelstellingen weer te geven.

Hierbij wordt effect en zekerheid als een percentage respectievelijk langs de verticale en de horizontale as uitgezet. Doordat effect en zekerheid als percentage worden uitgedrukt, manifesteren individuele scenario's A en B zich telkens als een punt op de eenheidscirkel.
Uit deze weergave is af te lezen dat:

- Een zekerheid van 100% correspondeert met een effect 0%.
- Een genormaliseerd effect van 100% correspondeert met een zekerheid van 0%.
- Effect en zekerheid negatief kunnen zijn. Hierover in het volgende meer.

Effect en zekerheid mogen negatief zijn

Uit de eenheidscirkel is af te lezen dat het samengestelde effect van onzekerheid negatief en positief uit kan pakken. Deze observatie is in lijn met de ISO 31000-definitie van risico en is voor vakbeoefenaars evident. Dat zekerheid ook negatief kan zijn, is minder evident. Een interpretatie van het concept van een negatieve zekerheid kunnen we in dit verband krijgen als we beroep doen op de propositie logica. Als we 100% zeker weten dat propositie p waar is, dan weten we met 100% zekerheid dat de inverse propositie p niet waar is. Anders geformuleerd: als het effect van onzekerheid op de realisatie van onze doelstellingen nul is (met andere woorden: we zullen zeker onze doelstellingen



Figuur 3 – Normalized risk analysis

halen), dan is de kans dat we onze doelstellingen niet halen ook nul. We stellen dat negatieve zekerheden gelden voor de inverse doelstellingen van risicoproposities.

Meer over assumptie 3

Volgens assumptie 3 is genormaliseerd risico het product van zekerheid en genormaliseerd effect. Als we met Excel de eenheidscirkel verdelen in 32 gelijke delen is genormaliseerd risico weer te geven als de grijze lijn in figuur 3.

In dit figuur is, in lijn met assumptie 3, genormaliseerd risico weergegeven als het product van effect en zekerheid (beiden uitgedrukt in %). Wiskundig uitgedrukt correspondeert dit met de functie sin(x)*cos(x). Opvallend is hierbij dat in iedere kwadrant van de eenheidscirkel deze functie een maximum bereikt als genormaliseerd effect en de zekerheid aan elkaar gelijk zijn.

Vergeleken met de risicomatrix biedt de eenheidscirkel een aantal voordelen bij het ontwerpen van risicomodellen en de analyse van genormaliseerd risico (naar de mening van de auteur tenminste). Dit zijn een aantal voordelen:

- Er zijn geen kunstmatige beperkingen die volgen uit de resolutie van eenheidscirkels.
- De volledigheid en diepgang van risicoanalyses is te verbeteren als we doelstellingen in deze zin van de ISO 31001-definitie van risico als proposities beschouwen. Het concept van negatieve zekerheid is te associëren met de negatie van deze risicoproposities.
- De lineaire algebra biedt handvatten voor de formele definitie van de genormaliseerde risicoaggregatie en ook voor de restrisico bepaling.
- meer kwantitatieve benadering voor risicomodellen wordt aangereikt.

Over dit ontwerp is meer te schrijven, maar in dit artikel laten we het hierbij.

Samenvatting

Risicomatrixen zijn alom vertegenwoordigd in de dagelijkse risicomanagementpraktijk. Toch zijn er volgens (1), (2) en (3) fundamentele issues aan te wijzen met de reproduceerbaarheid en coherentie van risicoanalyses op basis van dit instrument. De auteur experimenteert de laatste jaren voorzichtig met het gebruik van de eenheidscirkel als alternatief en is van mening dat de eenheidscirkel een alternatief voor de risicomatrix kan zijn in die gevallen waarbij er gestreefd wordt naar meer objectieve risicoanalyses en risicomodellen.

Referenties

(1) What's wrong with Risk Matrices; Louis Cox; 2008; https://eight2late.wordpress.com/2009/07/01/cox's-risk-matrix-theorem-and-its-implications-for-project-risk-management/

(2) Cox's risk matrix theorem and its implications for project risk management; Eight to Late; 2009; https://eight2late.wordpress.com/2009/07/01/cox's-risk-matrix-theorem-and-its-implications-for-project-risk-management/

(3) Why the Risk Matrix must die; Jorn Mineur; 2017 ; https://medium.com/@JornMineur/why-the-risk-matrix-must-die-620a7287e7c

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Privacysplaining

Een vriend van mij, een echte opkomende topper in de privacywereld, had er laatst weer eentje gevangen. Het was een markant type, vol van blakende zelfverzekerdheid, typisch Hollands welvaren, eloquent op de eigen manier en lekker direct. Het was een mannetje.

Met doordringende blik werd mijn vriend door dit mannetje aangestaard en van uitleg voorzien. Dit mannetje had net 'nee' gehoord en dat is ook eigenlijk wel een trigger, dus mijn vriend had natuurlijk beter moeten weten. Ik weet niet wat voor kleren mijn vriend aan had die dag, maar hem kennende zag hij er vast ook nog eens super goed uit en had hij heel vriendelijk en uitgebreid de tijd genomen om het 'nee' van een goede uitleg te voorzien, zodat de boodschap mooi zacht zou landen zonder al te veel pijn.

Het mannetje had natuurlijk weinig gehoord na de 'nee', maar ook net genoeg om te bedenken dat hij het bij het betere einde had. En dus begon hij van leer te trekken en mijn vriend de les te lezen over privacy. Over hoe privacy in elkaar zit, hoe de regels werken en hoe die uitgelegd dienen te worden. Natuurlijk had dat mannetje het volstrekt bij het verkeerde einde, hoe kon het ook anders? Privacy is immers niet zijn vakgebied.

Ik ben ze de afgelopen 20 jaar ook zelf tegengekomen: de privacysplainers. Heel vaak (eigenlijk alleen maar) van het mannelijke geslacht. Deze ziekelijke neiging om een specialist haar eigen vak uit te leggen is niet nieuw: het gebeurt vrouwen met de regelmaat van de klok dat ze toegesproken worden door mannen die het beter weten dan zij. Zelfs over de intieme werking van het vrouwelijk lichaam. Google maar eens naar het woord 'mansplaining'. Het is vrij hilarisch en sneu.

Maar naast het feit dat het hilarisch is, is het eigenlijk ook gewoon heel bruut respectloos. Laten we eerlijk wezen: gaat dezelfde man ook aan een bakker uitleggen hoe hij brood moet bakken of aan een tandarts vertellen hoe die gaatjes moet vullen? Dat lijkt me niet. Indien wel, dan is het geen mansplainer meer, maar een echte kl**tzak. Maar dat terzijde.

Ik snap het ook wel hoor. Iedereen weet wel een beetje over privacy en hoe het zou moeten werken. Gewoonweg omdat ieders gegevens overal en nergens verwerkt worden en er de afgelopen jaren steeds meer aandacht aan wordt geschonken. Ik ben ontzettend blij met al die alertheid, zolang het mijn werk en het werk van mijn mensen maar niet belemmert. Meedenken is fijn, misschien komen we samen wel op heel mooie oplossingen, maar respectloos lopen privacysplainen moet echt eens een keer ophouden. Want nee, je weet het niet beter dan de privacyspecialist en je bent gewoon een onverbeterlijke man met een godcomplex*.

*** Een godcomplex is een niet-klinische term die veelal gebruikt wordt om een individu te beschrijven die ervan overtuigd is dat hij meer kan bereiken dan wat binnen het menselijk kunnen ligt. Ook het sterk geloof dat de eigen mening automatisch beter is dan andere meningen is een vorm van godcomplex. Hij of zij gelooft boven de regels van de maatschappij te staan en een speciale behandeling te moeten krijgen.**

Rachel

Renco Schoemaker is adviseur informatiebeveiliging & privacy en mede-eigenaar bij IB&P. Momenteel coördineert hij de ENSIA-verantwoording bij twee G4-gemeenten. Eerder was hij adviseur en/of CISO (a.i.) bij diverse gemeenten. Renco is bereikbaar via r.schoemaker@ibnpbv.nl.

Toekomstscenario's voor ENSIA

Veel gemeentelijke CISO's zullen deze zin goed kennen: "ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)." En natuurlijk vervangen we inmiddels BIG voor BIO. Maar of je ENSIA al een 'effectief en efficiënt verantwoordingsstelsel' mag noemen valt te bezien. Hoe zou ENSIA zich in de komende jaren kunnen ontwikkelen om deze omschrijving wél te verdienen? Als dit voor jou relevante vragen zijn, lees dan zeker verder.

Een hele mond vol. Eenvoudig komt het erop neer dat ENSIA bestaande verantwoordingslijnen van gemeenten richting toezichthouders bundelt en wel op twee manieren: 1) normenkaders zijn zoveel mogelijk ontdubbeld en 2) de verantwoordingsmomenten zijn zoveel mogelijk uitgelijnd. Daarnaast combineert ENSIA verantwoordingsinformatie voor zowel de 'horizontale toezichthouder' (gemeenteraad) als de 'verticale toezichthouders' (bijvoorbeeld ministeries). Op deze termen kom ik later terug. Concreet bevat ENSIA diverse vragenlijsten die jaarlijks ingevuld moeten worden.

Nee, het ontbreekt ENSIA niet aan ambitie. Met het omarmen van de Baseline Informatiebeveiliging Gemeenten (BIG) hebben de gemeenten een duidelijk signaal afgegeven: de verantwoordingslast moet niet verder toenemen. Menig CISO stelt dat daar nog geen sprake van is, maar ja: de lasten gaan vaak voor de baten uit. Voor meer achtergrondinformatie over de start van ENSIA verwijs ik je graag naar eerder verschenen artikelen (1) (2).

Effectief en efficiënt verantwoording afleggen

Inderdaad, dit zijn van die containerbegrippen. Ze zijn echter goed concreet te maken: 1) wordt een gemeente ook daadwerkelijk veiliger (effectief); en 2) kost het verantwoorden niet onevenredig veel tijd (efficiënt)? Aandacht gaat al snel uit naar het tweede punt: gemeenten moeten van alles beantwoorden, vastleggen en aantonen. Dit kost inderdaad de nodige tijd weet ik uit ervaring, al wordt er heel verschillend mee omgegaan. De ene gemeente formeert een forse werkgroep die volop de diepte induikt en een andere gemeente beantwoordt de vragen 'hoog over' met hulp van de CISO en een kernteam van specialisten.
Terug naar het eerste punt: wordt een gemeente ook daadwerkelijk veiliger? Kan ENSIA brengen wat ze belooft? (3) Is ENSIA niet onbedoeld het doel op zichzelf geworden? Dit is een reëel risico wat mij betreft en het zal de draagkracht doen afnemen. Om te voorkomen dat ENSIA – het afleggen van verantwoording – het doel wordt en niet langer het nastreven van een betrouwbare informatievoorziening – langs de B-, I- en V-as - is doorontwikkeling cruciaal. Daarmee onderstreep je immers dat het verantwoordingsstelsel continue verandert en de 'automatische piloot' geen optie is. Het zet aan tot nadenken waarom we überhaupt verantwoorden en verlegt de aandacht van jaarlijks door de ENSIA-hoepel springen naar het nemen van maatregelen met als doel een betrouwbare informatievoorziening.

Verticaal en horizontaal toezicht

Alvorens ik enkele toekomstscenario's uitwerk wil ik eerst nader stilstaan bij het onderscheid in verticaal en horizontaal toezicht. Een voorbeeld van verticaal toezicht is de Inspectie van het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) dat toeziet op het Suwinet-gebruik. Suwinet is een digitale voorziening voor uitwisseling van persoonsgegevens tussen uitvoeringsorganisaties als de SVB

Horizontale toezicht wordt leidend ten opzichte van het verticale toezicht

en het UWV en de gemeentelijke sociale diensten. Organisaties die gebruik maken van Suwinet dienen te voldoen aan het normenkader. Een ander voorbeeld is Logius die toeziet op het veilig gebruik van DigiD. Organisaties met een DigiD-koppeling dienen te voldoen aan, jawel, het normenkader.

Horizontaal toezicht is daartegen compleet anders. Ten eerste anders in scoping: de horizontale verantwoording gaat primair uit van de zelfevaluatie op de Baseline Informatiebeveiliging Gemeenten (BIG). En de BIG geldt – weliswaar via het 'pas toe of leg uit' principe - voor alle gemeentelijke bedrijfsvoeringsprocessen. Dat is wel wat breder dan Suwinet of DigiD. Ten tweede oefent de (gemeente)raad het toezicht uit op deze zelfevaluatie en de gemeenteraad is doorgaans geen orgaan dat ervaringskundig is op het gebied van informatiebeveiliging. De gemeenten waar eerder een rekenkameronderzoek is uitgevoerd op dit beleidsterrein hebben wat dat aangaat 'een streepje voor'. Immers, de rekenkamer heeft dan al eens de doelmatigheid en doeltreffendheid van het informatiebeveiligingsbeleid onderzocht en daarover gerapporteerd aan de raad.

Je kan en mag niet van een raad verwachten dat ze met de introductie van ENSIA ineens de kennis en kunde in huis heeft om goed toezicht uit te oefenen. Wel dient een raad stappen in die richting te zetten, wat mij betreft. Dat betekent interesse tonen in het onderwerp, het structureel agenderen, vragen stellen en waar nodig verdieping, het eigen kennisniveau verhogen. Wel moeten we onderkennen dat de ENSIA-verantwoording naar de raad alles behalve eenduidig gebeurt (4).

Verticaal op basis van horizontaal toezicht

Een belangrijk ENSIA-uitgangspunt is dat het horizontale toezicht leidend wordt ten opzichte van het verticale toezicht. In de ideale situatie leunt een verticale toezichthouder (bijvoorbeeld Inspectie SZW, Logius) op het horizontale toezicht dat wordt uitgeoefend door de raad (5). Dit veronderstelt een raad die het beleidsterrein informatiebeveiliging, al dan niet in combinatie met privacy, ten minste jaarlijkse prominent op de agenda zet. Een raad die zich uitgebreid en deugdelijk laat informeren door de verantwoordelijk wethouder en zichzelf zeer serieus neemt in het uitoefenen van haar toezicht hierop. Desnoods gebruikmakend van expertise buiten de raad. Maar zoals eerder gezegd: zover zijn we nog niet.

Hoe kan een gemeenteraad deze essentiële stap maken? Nou, allereerst door via de portefeuillehouder(s) volledige verantwoordingsinformatie vanuit de ambtelijke organisatie te vragen. Alleen informatie over Suwinet en DigiD is niet volledig. Toch gebeurt dit in de praktijk veelvuldig, omdat er bij DigiD en Suwinet sprake is van volwassen verticaal toezicht. Voor de raad is toch de Baseline Informatiebeveiliging Gemeenten juist essentieel? Ik haal nog even deels de eerdere zin aan: "…een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)."

Laten we dus eerst het fundament van het ENSIA-verantwoordingsstelsel eens serieus nemen richting de raad. Daartoe helpen onderstaande drie toekomstscenario's, waarbij ik een combinatie van scenario 1 en 2 op voorhand afraad.

Toekomstscenario 1: werking toevoegen

Binnen ENSIA is een gemeente verplicht, voor wat betreft het DigiD-normenkader en een deel van het Suwinet-normenkader, jaarlijks een IT-audit te laten uitvoeren. Voor DigiD bestaat deze verplichting al jaren en vorig jaar heeft de NOREA haar duiding van de Suwinet-toetsing aangescherpt door de aandacht te vestigen op de 'General IT Controls'. Wel kijken IT-auditors momenteel alleen naar de opzet en het bestaan van de maatregelen. Er wordt dus niet over een langere periode getoetst op de werking van maatregelen. Het doel is een gemeente veiliger maken en juist dát toets je met werking toetsen.

Mijn advies is om werking per 2021 binnen scope te brengen voor de ENSIA IT-audit, te beginnen met DigiD. Het jaar daarop zou ook Suwinet kunnen volgen. Ik realiseer me terdege dat ik hiermee de al langer bestaande wens van de NOREA opteken. Idealiter toets je de werking voor je horizontale verantwoording, nog vóór de verticale toezichthouder het afdwingt.

Toekomstscenario 2: GITC's verbreden

Vooralsnog worden de 'General IT Controls' (GITC's) alleen met betrekking op Suwinet getoetst binnen de IT-audit. Het gaat dan ook nog om een specifieke vorm van Suwinet: DKD-Inlezen. DKD staat voor Digitaal KlantDossier en binnen deze vorm lezen applicaties die in het beheer zijn van gemeenten direct Suwinet-gegevens in. De inlezende applicatie dient daarmee te voldoen aan de GITC's. Maar gemeenten hebben natuurlijk talloze applicaties waarin gevoelige persoonsgegevens worden verwerkt. Op basis van een risicoanalyse op voornamelijk het vertrouwelijkheidsaspect dienen zij een top 10 kritieke applicaties te laten vaststellen. Uitvoering en vaststelling kan plaatsvinden in 2021.

Mijn advies is om met ingang van 2022 deze top 10 van applicaties binnen de scope van de ENSIA IT-audit te laten vallen. De GITC's zoals die nu bij Suwinet gelden worden dan in opzet en bestaan ook getoetst bij deze 10 applicaties. Eén of twee jaar later wordt ook werking toegevoegd. De parallel met de jaarrekeningcontrole zal de geïnformeerde lezer niet zijn ontgaan (6) (7).

Toekomstscenario 3: relatie met risico's aanbrengen (juiste abstractieniveau)

Of de toekomst nu meer langs scenario 1 of scenario 2 vorm krijgt, in beide gevallen zouden we veel meer werk moeten maken van het vertalen van (het niet voldoen aan) normen naar het lopen van risico's. Vooral in de BIO is er, in ieder geval op papier, veel aandacht voor risicomanagement. Bij het vakgebied informatiebeveiliging kijken we dan naar beschikbaarheid, integriteit en vertrouwelijkheid, maar ook dat zal een bestuurder doorgaans weinig zeggen. Welke risico's loopt een gemeente nu werkelijk? Afgesloten worden van DigiD is geen risico, maar een onderbreking in de dienstverlening naar burgers zeer waarschijnlijk wél.

Een raad voert haar toezichthoudende taak uit op het hoogste abstractieniveau. Als informatiebeveiligers moeten we leren onze vakgebied te relateren aan vraagstukken op dat hoge abstractieniveau. Per direct stoppen met het informeren van een raad op normniveau, wat mij betreft. Hoe kan een betrouwbare informatievoorziening bijvoorbeeld de uitoefening van publieke taken garanderen? Wanneer het digitale loket geheel stilvalt voor meerdere dagen (beschikbaarheid), het heffen van de OZB niet op basis van juiste informatie gebeurt (integriteit) of wanneer er zeer gevoelige informatie van minderjarigen lekt (vertrouwelijkheid), dán heb je de aandacht. For better or for worse. Liever voorkomen dan genezen, daar zal een bestuurder het al snel mee eens zijn.

Tot slot

Je kan van ENSIA vinden wat je wilt, maar we hebben met elkaar een belangrijke eerste stap gezet naar een meer volwassen wijze van verantwoording over informatiebeveiliging. Het fundament is er, maar nu is verder bouwen nodig. Er zijn zeker onvolkomenheden en bij de huidige effectiviteit en efficiëntie zijn terechte vraagtekens te zetten. Niettemin moeten we de blik vooruit gericht houden en niet onbedoeld van een middel het doel maken.

Referenties

(1) https://ibnp.link/ensia-artikel-1
(2) https://ibnp.link/ensia-artikel-2
(3) https://ibnp.link/ensia-artikel-3
(4) https://ibnp.link/ensia-artikel-4
(5) https://ibnp.link/ensia-artikel-5
(6) https://ibnp.link/gitc-artikel-1
(7) https://ibnp.link/gitc-artikel-2

Eric Verheul is een onafhankelijk cryptografisch adviseur en deeltijd hoogleraar aan de Radboud universiteit te Nijmegen. Hij geeft een master course in security management en doet onderzoek naar toegepaste cryptografie en privacy enhancing technologies. Dit artikel schrijft hij op persoonlijke titel. Eric is bereikbaar via eric.verheul@keycontrols.nl.

Toepassing privacy enhancing technology in het Nederlandse eID

Vanuit de Nederlandse overheid wordt hard gewerkt aan het beschikbaar krijgen van sterke (‘twee-factor’) vormen van authenticatie voor burger en bedrijven bij (publieke) dienstverleners. Belangrijke aspecten daarbij zijn beveiliging, privacy en gebruikersvriendelijkheid (ook voor de dienstverleners). Hoewel de volledige invulling nog niet bekend is, zijn wel verschillende deelproducten beschikbaar gemaakt. Dit artikel beschrijft deze deelproducten.

Op bsn-koppelregister.nl (1) staan de specificaties en decryptiesoftware (Java) voor de privacy enhancing technology (PET), voorzien binnen het Nederlandse eID-stelsel. Dit staat bekend als 'PEP' (Polymorphic Encryption and Pseudonimation). Het PEP-startpunt is – fundamenteel anders dan dat van bijvoorbeeld IRMA (2) – die van een gecentraliseerde opzet ('federatie'): de authenticatie vindt plaats bij een authenticatiedienst die het resultaat doorgeeft aan een dienstverlener.

Voor dit startpunt is gekozen, omdat ervaringen uit andere landen zoals Duitsland aangeven dat een gedecentraliseerde ('directe') benadering belastend is voor dienstverleners. Dit onder meer omdat dienstverleners dan specifieke protocollen moeten implementeren en specifieke helpdesks moeten inzetten. PEP beoogt evenwel de 'ontzorging' van een gecentraliseerde authenticatie-opzet te combineren met de privacy- en securityvoordelen van een gedecentraliseerde oplossing. Toepassing van PEP is authenticatietechnologie neutraal en kan worden gecombineerd met reguliere vormen van authenticatie (waaronder IRMA). In mei 2018 heeft PEP een securitybeoordeling door de universiteit van Birmingham glansrijk doorstaan. PEP wordt nu al toegepast voor het aanloggen vanuit Nederland in andere lidstaten en omgekeerd (eIDAS interoperabiliteit).

De cryptografische specificatie van PEP-eID staat in de subdirectory/pep-crypto-documentation/10-Reference. De specificatie start met de niet-technische achtergrond van PEP en de rationale voor de gekozen opzet. Daarnaast omvatten de specificaties ook innovatieve overheidstoepassingen die met PEP mogelijk worden zoals privacyvriendelijke gegevensuitwisseling in de zorg (3) en stemmen vanuit het buitenland. Dit wordt onderaan dit artikel verder toegelicht.

Het PEP-paradepaardje is DigiD Hoog, dat een fundamenteel privacyprobleem oplost in een gecentraliseerde opzet: in een standaard gecentraliseerde authenticatieopzet krijgt de authenticatiedienst zowel inzicht in de identiteit van de gebruiker als van de dienstverlener die deze wenst te bezoeken. Het bezoek aan sommige dienstverleners (bijvoorbeeld in de zorg) kan zelfstandig al als bijzonder persoonsgegevens worden bestempeld. DigiD Hoog lost dit privacy issue op door aanloggen anoniem te laten plaatsvinden. Dat wil zeggen: de (gecentraliseerde) authenticatiedienst DigiD verstrekt een gerandomiseerd, versleuteld BSN van een burger aan een dienstverlener zonder zelf inzage in te krijgen in het BSN of dit te kunnen linken. Doordat DigiD wel weet bij welke dienstverlener de burger wil aanloggen, kan deze wel worden beschermd tegen browser malware (`man-in-the-browser' malware). Daarmee is zowel hoge privacy als security mogelijk en hoeft hiertussen geen keuze te worden gemaakt zoals in andere landen wel is gedaan.

DigiD Hoog is gebaseerd op een eID-kaartapplicatie (Polymorphic Card Application of PCA) uitgegeven na 4 juni 2018. Het aanwezig zijn van PCA op een rijbewijs is te herkennen aan het 'ID'-logo (zie onder).

Vorig jaar is een succesvolle pilot uitgevoerd met DigiD Hoog. Als alternatief voor een separate kaartlezer konden gebruikers daarbij ook hun 'NFC-enabled'-telefoon gebruiken. Tot voor kort waren dat alleen Android-gebaseerde telefoons, maar recent zijn ook Apple-toestellen (iPhones) geschikt. November 2019 zijn ongeveer 3 miljoen rijbewijzen uitgegeven die geschikt zijn voor DigiD Hoog en dat aantal groeit met ongeveer 35.000 per week. Plaatsing van PCA op de Nederlandse identiteitskaart is later gepland (aanpassing Paspoortwet). De cryptografische werking van PCA maakt deel uit van de PEP-eID -specificaties. Een PCA-simulator kan worden gevonden op github.com (4).

PEP (en ook de eID-kaart) ondersteunt naast het BSN ook pseudoniemen zoals ook sterk geadviseerd in de Algemene verordening gegevensbescherming (AVG). Ter illustratie: de toepassing van het BSN in een attributenregister - waarin alleen wordt bijgehouden dat iemand ouder dan 18 lijkt - is niet in lijn met het AVG data minimization-beginsel. Zeker niet als de bevragende diensten (bijvoorbeeld zorg of goksites) privacygevoelig zijn. Bij gebruik van het BSN zouden de attribuutdiensten immers bij iedere bevraging inzicht krijgen

Met de toepassing van PEP ontstaat een krachtige securityinfrastructuur voor (toekomstige) Nederlandse overheid-toepassingen

wie de dienst bezoekt. Om vergelijkbare redenen hoeft ook een machtigingsregister niet het BSN van de gemachtigde te kennen; ook daar volstaat een pseudoniem.

Toepassing van pseudoniemen kan ook de beveiliging van registers enorm versterken. Een actueel voorbeeld zou een register zijn waarin de 'psychische (on)gezondheid' van burgers wordt vastgelegd ten behoeve van het afgeven van wapenvergunningen. Het gebruik van het BSN in een dergelijk register is ongewenst, omdat bij het compromitteren van een dergelijk register het leed niet te overzien is. Het gebruik van pseudoniemen mitigeert dit risico.

Naast de gebruikelijk eigenschappen hebben PEP-pseudoniemen ook bijzondere eigenschappen. Homomorfe cryptografie realiseert bijvoorbeeld dat een authenticatiedienst (zoals DigiD) de pseudoniemen vormt zonder er inzage in te krijgen; alleen de dienstverlener en betrokkene krijgen inzage. Doordat verder versleutelde BSN's en pseudoniemen digitaal getekend zijn (EC-Schnorr), kunnen zij ook end-to-end privacy en end-to-end security leveren zoals in een decentrale opzet. De eerste eigenschap betekent dat 'tussenliggende' partijen zoals makelaars geen inzage krijgen in de identiteiten (BSN's en pseudoniemen) en de tweede houdt in dat deze partijen de identiteiten niet kunnen manipuleren. PEP voorkomt daarmee dus ook het ontstaan van privacy hotspots waar in verleden discussie over was (de 'authenticatiepooiers' (5)).

Met de toepassing van PEP ontstaat een krachtige securityinfrastructuur voor (toekomstige) Nederlandse overheid-toepassingen die ook de AVG-beginselen 'data protection by design' en 'data minimization' ondersteunt. De ondersteuning van pseudoniemen maakt ook integratie mogelijk van publieke en private authenticatiediensten, hetgeen onderliggend is aan het Scandinavische eID-succes. Daarbij is sprake van één eID-infrastructuur voor zowel publieke als private dienstverleners. Bij private dienstverleners kan worden aangelogd onder pseudoniem en bij publieke dienstverleners onder BSN of pseudoniem. Een dergelijke opzet wordt al toegepast in andere landen zoals in Duitsland en Oostenrijk. Doordat pseudoniemen zijn afgeleid van het BSN zijn ze uniek per dienstverlener waarmee bijvoorbeeld ook Marktplaats-fraude en social media trolling zou kunnen worden gemitigeerd: een gebruiker kan dan immers maar een keer een eID verified (gepseudonimiseerd)-account aanvragen.

In de genoemde PEP-specificaties wordt de kracht van de eID-infrastructuur geïllustreerd aan de hand van twee voorbeeldtoepassingen: stemmen vanuit het buitenland en toepassing in het MedMij-initiatief (6).
Stemmen vanuit het buitenland gaat nadrukkelijk niet over digitaal stemmen voor iedereen, maar alleen voor de kleine groep Nederlanders die woonachtig zijn in het buitenland. Het huidige proces verloopt nu via de post (7) en staat daarmee onder meer op gespannen voet met het stemgeheim. De PEP-gebaseerde opzet vermijdt dit onder meer door gebruik van PEP-pseudoniemen. Medmij gaat over dataportabiliteit in de zorg: het ondersteunt dat patiënten hun medische gegevens vanuit zorgaanbieders naar gezondheidsomgevingen bij private dienstverleners kunnen onderbrengen. Dit levert patiënten controle over hun eigen gegevens en faciliteert zo bijvoorbeeld het vragen van second opinions. Door hun private aard mogen gezondheidsomgevingen niet het BSN verwerken. PEP-toepassing, waaronder diens pseudoniemen, kan een grote bijdrage kunnen leveren aan de beveiliging en privacy bescherming van burgers binnen Medmij. De Medmij-use case illustreert ook de voordelen van de integratie van publieke en private authenticatiediensten.

Referenties

(1) https://wiki.bsn-koppelregister.nl/display/DC/3.+Downloads
(2) https://privacybydesign.foundation/irma/
(3) www.medmij.nl
(4) https://github.com/CardContact/eID-sim/tree/PCA-sim
(5) https://pilab.nl/about%20pi%20lab/blog/privacy%20impact%20-assessement.html
(6) www.medmij.nl
(7) https://www.denhaag.nl/nl/bestuur-en-organisatie/verkiezingen/kiezers-buiten-nederland/permanente-registratie-voor-kiezers-buiten-nederland.htm

Dré Lameir is information security officer en VP innovation & development bij Enovation bv. Hij is bereikbaar via: linkedin.com/in/lameir/

Column

Goede voornemens

"Dré-tje, voor je het weet staan we allemaal weer met een kerstboom in onze handen." Een vaak aangehaalde quote van een van mijn collega's. Zijn manier om aan te geven dat de tijd vliegt. En het is waar, toch? Het ene moment wensen we elkaar (en onszelf) het beste voor het nieuwe jaar, nu kijk je terug en denk je: wat is er van al mijn life goals terecht gekomen?

Januari is de maand van de goede voornemens: we nemen een abonnement en gaan 2 keer per week de sportschool in. Uiteraard houden we het in het begin flink vol, we tonen discipline. Ook al staat de hele routine ons tegen, met de sporttas op de fiets in weer en wind, de zaal in, elke keer een tandje bij op de spinfiets, een kilootje erbij op de gewichten, een paar verdiepingen erbij op de stair master. Lekker, doorzetten!

Dit gedrag houden we even vol. In de zomer willen we immers met 6 blokjes en een strakke kont op het strand. We hebben een duidelijk doel voor ogen: eye on the price people!

Dan wordt het druk: het huis moet geschilderd worden, oma wordt ziek en je zei 'ja' tegen de ouderraad op school en de tijd glipt als los zand door je vingers. De kilo's vliegen er weer aan en na 3 reminders vanuit de sportschool ben je ineens 'slapend lid'. De kosten, maar niet langer de lusten. We zijn trainingsmoe en zelfs onze dure personal trainer krijgt geen grip meer op ons uitgezakte lijf. Zeg maar dag tegen die onuitwisbare indruk op een zonovergoten strand.

Herkenbaar? En in je eigen organisatie, hoe staat het daar inmiddels met de goede voornemens?
Vervang in bovenstaande:

- **'Goede voornemens en life goals' door 'jaarplan'.**
- **'Kilo's' door 'risico's, taken en non conformities'.**
- **'Personal trainer' door 'kwaliteitsmanager, auditor of consultant'.**
- **'2 keer per week in de sportschool' door 'continu verbeteren'.**
- **'Oma en de ouderraad' door 'opportunisme van sales en klantvragen'.**
- **'Abonnement' door 'torenhoge rekeningen van tooling, audits, training, naslagmateriaal zoals de NEN-connect'.**
- **En: 'die strakke kont' door 'een ISO27001-certificaat'.**

Waarom is het zo moeilijk om continue verbeteren vol te houden? Waarom is gedragsverandering zo moeilijk als persoon, maar ook als organisatie?

Ik denk dat continue verbeteren voor organisaties zo zwaar is, omdat we het gedrag en de motivatie van alle individuen die er werken, je collega's, gelijktijdig moeten veranderen. Het is vechten tegen de optelsom van ieders excuses, afleiding en extra werk. Hoe terecht ook, de toebedeelde tijd van collega's en discipline dalen naarmate het jaar vordert.

Nu is 2019 al op zijn eind, misschien was het een goed jaar en heb je het hele jaarplan voortijdig af kunnen vinken. Misschien ben je toch weer ingehaald door de realiteit en biedt 2020 nieuwe kansen.

Collectief de schouders eronder zetten lukt het best als je een gezamenlijk doel hebt. En let op: 'het moet van de ISO' is geen gezamenlijk doel. Wat dan wel? Als security officer of kwaliteitsmanager ben je ook een verandermanager. Jij moet op zoek naar de 6 blokjes en de strakke kont van jouw organisatie. Of zoals mijn collega van de kerstboom zou zeggen: "Tikkie, je bent 'm!"

Rik van Dijk is cyber security specialist bij CGI. Rik is bereikbaar via rik.van.dijk@cgi.com. Peter Groothuis is directeur van ArtOfado. Peter is bereikbaar via peter@artofado.nl.

Secura Blackhat Sessions 2019: een verslag over critical systems en vendor responsibility

Chris van 't Hof geeft het verzamelde publiek in het NBC Centrum in Nieuwegein een korte introductie van het programma voor de dag. De workshops tijdens Secura Blackhat Sessions 2019 met demonstraties om ICS-systemen te hacken zijn van tevoren al volgeboekt. Het is een duidelijk teken. De zaal is zich ervan bewust dat de ICS/SCADA-systemen kwetsbaar zijn. En de sprekers van vandaag bevestigen dat beeld.

Maar er is ook een andere trend te ontdekken tijdens deze conferentie: waar gebruikers nog weleens de schuld krijgen van beveiligingslekken - ze snappen de systemen niet, ze willen niet patchen - zijn het de soft- en hardware producenten die op de Blackhat Sessions worden aangesproken op onverantwoord gedrag.

Openstaande MongoDB-databases

De eerste keynote op de Blackhat Sessions 2019 zet duidelijk de toon voor de conferentie. Victor Gevers, oprichter van de GDI Foundation met meer dan 5000 Responsible Disclosures op zijn naam, neemt de zaal mee in zijn dagelijkse werk. Victor vertelt uitgebreid over MongoDB-databases die overal ter wereld openstaan, omdat de

standaardinstellingen niet voldoen aan basale veiligheidseisen. Hij laat zien hoe zijn stichting toegang heeft tot Chinese databases met daarin face-recognition-data van 150 miljoen surveillancecamera's, tienduizenden portretfoto's van Chinese mannen, vrouwen en kinderen. Victor en zijn team hebben meerdere meldingen gemaakt bij MongoDB, maar een reactie bleef uit. De producent was niet geïnteresseerd om de lekken in hun product snel te herstellen. De GDI-foundation zoekt nog support, dus als je als professional of bedrijf wilt bijdragen aan een veiliger infrastructuur kan dat.

Onveilig maar niet altijd levensgevaarlijk

Victor wordt opgevolgd door Jos Wetzels, senior researcher van Secura op het gebied van ICS/SCADA-systemen. Het beeld dat hij schetst is zorgwekkend, maar niet alarmerend. Ja, ICS/SCADA-systemen zijn kwetsbaar. Ze zijn als standalone niet ontworpen om veilig te zijn in een connected omgeving, maken gebruik van oude en open protocollen waar in enkele gevallen op het laatst een securitysausje aan toegevoegd is. En ja, vendors moeten meer verantwoordelijkheid nemen om te zorgen dat in de toekomst hun producten en protocollen wel secure zijn.
Maar, vertelt hij ook, het platleggen van een fabriek of energiecentrale is moeilijker dan op de gehackte PLC het commando 'EXPLODE' in te typen. Het vereist de gecombineerde kennis van een systeemanalist om de weg te vinden in het netwerk, een engineer om de processen binnen de ICS-omgeving te kennen en te weten wat wel en wat geen schade aanricht en natuurlijk de vaardigheden van de hacker, een ICS-hacker welteverstaan, om toegang te krijgen en de payload af te leveren.
Wetzels houdt het publiek een stelling voor, stelling 1: alle ICS-systemen zijn kwetsbaar en we gaan er allemaal aan. Stelling twee: het hacken van ICS-systemen kost zoveel tijd, technische kennis dat het gewoon de moeite niet is. Zoals vaak, vertelt hij na het tellen van de handen in de zaal, ligt de waarheid in het midden.

De techniek in

Ook tijdens de technische sessies in het NBC Centrum worden marketingtaal over secure products van de realiteit gescheiden. Hier het omzeilen van beloofde security door vendors centraal. Carlo Meijer, PhD-onderzoeker bij de Radboud Universiteit, toont stap voor stap aan hoe door de markt superieur geachte Self-Encrypting Drives (SED) als vervanger van software-encryptie van SSD's ruimschoots te kort schiet.
SED is in veel gevallen zelfs minder veilig dan de softwarevariant FDE (Full Disk Encryption). Omdat de techniek op hardware niveau werkt, is het eigendom van de fabrikant en niet open source waardoor zwakke encryptie of bugs dus niet op tijd worden gevonden. Zoals vaker blijkt de black box van fabrikanten gemakkelijk te kraken. Het was bijzonder boeiend om te horen dat het veranderen van elektronische spanning op een printplaat al voldoende is om encryptie stap voor stap te ontmantelen.
Marina Krotofil, een ervaren ICS/SCADA-security onderzoeker, zette in haar verhaal (in)security by design, wat ze haar minst technische presentatie ooit noemde, de verschillende IEC-security-standaarden uiteen. Volgens haar leiden de standaarden tot een vorm van schijnbeveiliging. Fabrikanten gebruiken gehackte certificaten. Een van de standaarden kent protocollen voor file transfer die allerlei bestanden mogen transporteren, dus ook malware en trojans.
Producenten lijken meer bezig met het afstrepen van vinkjes op een lijst dan met het verbeteren van hun producten. En waarom zouden ze ook? Er staan geen zware straffen op het maken van onveilige hard- of software. Als gemeenschap hebben we min of meer geaccepteerd dat deze producten onveilig zijn en worden de pijlen gericht op gebruikers omdat ze niet tijdig patchen. Voor Marina kunnen de standaarden overboord en werkt maar een strategie: producenten aansprakelijk stellen voor onveilige producten, inclusief passende straf.
Robin Massink van Alliander verraste ons dat Alliander zich natuurlijk zorgen maakt over cyberterrorisme, maar zich vooral moet wapenen tegen hun ergste vijand: eekhoorns en kwallen. Die veroorzaken veruit de meeste verstoringen. En hij gaf al een even mooi beeld over de staat van de infrastructuur: "We hebben een museum en noemen dat productie . Veelal oude apparatuur, maar niet zomaar te vervangen."

Conclusie

De Blackhat Sessions 2019 van Secura bracht een groot aantal boeiende sprekers bijeen op een onderwerp dat sinds een aantal jaren vol in de schijnwerpers staat: hoe beschermen we kritieke systemen? In Nieuwegein hoorden we als antwoord verfrissende geluiden van de sprekers, zowel tijdens de keynotes als in de vaak dieptechnische break-out sessies. Lakse producenten houden het probleem van onveilige kritieke systemen in stand en het wordt tijd dat daar eens iets aan gedaan wordt.

In deze rubriek geven enkele iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over de 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 kunt u sturen naar ibmagazine@pvib.nl.

De kleine man met grote impact

Het zal niemand ontgaan zijn, maar onze overheid heeft met een noodwet daadkracht getoond: van de ene dag op de andere een snelheidsverlaging op de snelwegen tot maximaal 100 kilometer per uur. Het effect? Een dusdanige besparing op stikstofoxiden (NOx) dat daarmee de vervuilende kracht van de bouw en de landbouw in één klap gecompenseerd wordt. Applaus, of toch niet?

Chris de Vries

De NOx-besparing bedraagt volgens hen die het weten minder dan één procent. Waar of niet waar? Politici & ambtenaren vreesden de acties (dan wel de actiebereidheid) van deze beleidsopponenten en met het economisch belang vooropgesteld vinden slimmeriken dan wel een rekenformule uit die het ongelofelijke waarmaakt. Wie was het eigenlijk die ooit gezegd heeft dat statistieken officiële leugens zijn?

Waarom is de automobilist dan opgezadeld met de emotionele rekening? Misschien omdat deze zich moeilijk organiseren tot verzet of misschien omdat de grote massa van automobilisten eigenlijk de kleine man vertegenwoordigen. Wat betekent dit nu eigenlijk binnen onze beveiligingswereld? Waarom is deze bespiegeling relevant; of is zij dat juist niet?

Op dinsdag 12 november 2019 waren vele PvIB-leden bijeen voor de Algemene Ledenvergadering en 's avonds voor de bijeenkomst over `awareness'. En juist op die avond verzuchtten de sprekers: "Hoe krijgen wij het MKB actief als het gaat om beveiliging en dan niet alleen door iets op te schrijven of een mening te hebben, maar door daadkrachtig hun bedrijven (waaronder vele zzp-bedrijven) te beschermen?"

Ook hier spreken wij over 'de kleine man'. Deze laat zich moeilijk mobiliseren en het ontbreekt hen aan geld, middelen, kennis en inzichten. Dus kan er dan een andere uitkomst tot stand komen?

Een van de gestelde vragen was of de overheid (bijvoorbeeld het ministerie van Economische Zaken en Klimaat) dan niet op ethische wijze de kleine ondernemingen moet hacken. Dat leidt tot emotionele pijn en schaamtegevoel, dus tot actie?!

Een andere vraag was of de Rijksoverheid niet concreet met raad (lees: bezoek aan de ondernemers, actieve voorlichting) & daad (open source beveiligingssoftware gratis ter beschikking stellen) alsook met geld (subsidies) het MKB echt kan helpen.

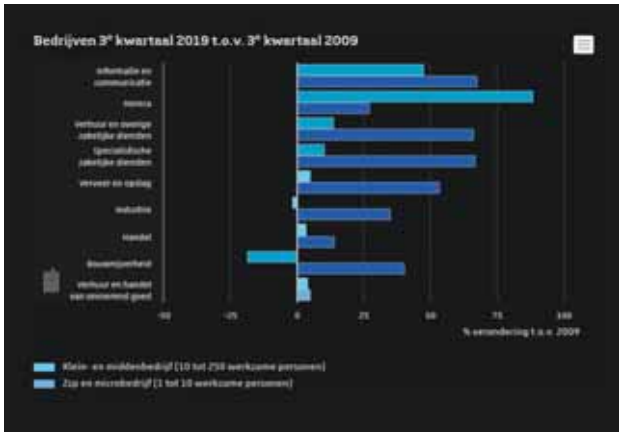
Voor de (Rijks)overheid een kleine kostenpost op haar resultatenrekening, dat meteen herdefinieert als overheidsproductie. De overheid leidt nooit verlies. Voor de kleine ondernemer (de MKB'er) echter een substantiële aderlating als hij alles zelf moet dragen of uitvinden. Voor de MKB'er een vraag van leven of dood, dus het is niet zo verrassend dat het MKB de grote wegblijver is bij beveiligingsvraagstukken. En toch bezit deze kleine man - gezien zijn groepsomvang - in tegenstelling tot de automobilist een grote impact. Dat vermenigvuldigt met het risico sommeert tot een onaanvaardbare lage tolerantiematrix.

Waarom?

1. Nederland telt in het 3e kwartaal van 2019 1,16 miljoen (1) MKB-bedrijven in haar (in goed Nederlands) 'business economy'. De toename in de afgelopen 10 jaar bedroeg 335.000 bedrijven, waarvan 330.000 microbedrijven (en dat is 98,5%). Zie figuur 1.
2. Wat de arbeidsgelegenheid betreft staat het MKB voor 3,5 miljoen voltijdsequivalenten. Daarmee is het MKB een banengenerator zo niet beperker van het uitkeringstrekkerschap en dus van veel hogere overheidsschulden. (2)

Fook Hwa Tan | Chris de Vries | Tom Bakker

3. Het MKB is (in)direct toeleverancier voor veel middenbedrijven en overheidsinstellingen. Hun beveiligingszwakte vertaalt zich als een backdoor bij de overheid (denk aan de werkgroep Ketenveiligheid van het PvIB in 2017/2018).



Samengevat: hoe kunnen wij inderdaad het MKB activeren, welke rol moet er weggelegd zijn voor de overheid en hoe zouden wij als PvIB daar een rol bij kunnen spelen?

Tom Bakker

Ik zie het probleem niet zo van een snelheidslimietverlaging in het algemeen. Het heeft meer voordelen dan nadelen. Of dat nu substantieel scheelt in de stikstofuitstoot is mij niet duidelijk. Getallen worden te pas en te onpas uit de hoge hoed getoverd. Maar dat terzijde. Wat met de maatregelen en impact daarvan in bovenstaande inleiding nog even vergeten is, is de impact op de continuïteit van bedrijven. Zeker voor het MKB. Langdurige stilstand is funest voor kleine bouwondernemers. Zouden die dit scenario in hun al dan niet aanwezige BCM risicoanalyse meegenomen hebben? Trouwens, grote bouwondernemingen wel? Ik denk van niet. Zeker een punt van aandacht.
Terug naar beveiliging in het MKB. Het MKB moet zeker geholpen worden. Een eerste stap is gezet met de oprichting van het Digital Trust Center (DTC). Het DTC gaat het MKB met raad en daad terzijde staan. In een van de volgende iB-nummers komt daar zeker nog een artikel over. Ik weet niet of we veel leden hebben die in het MKB werkzaam zijn. Die kunnen kennis en advies van peers opdoen in de vereniging. Als die leden nog schaars blijken te zijn (misschien zijn er in het MKB sowieso weinig nog beveiligers) dan zou het PvIB een voortrekkersrol kunnen nemen in de awareness (AVG, risico's etc) bij het MKB al dan niet via het DTC.

Fook Hwa Tan

In ons vakgebied wordt veel gesproken over de kleinere MKB's. Deze worden als fundament van onze maatschappij gezien. In het bovenstaande gedeelte is te lezen hoeveel van dit soort organisaties er zijn in Nederland. Wat we ook constateren is dat deze organisaties onvoldoende middelen hebben om zich adequaat te verdedigen tegen cyberaanvallen. Hierdoor vormen ze een gemakkelijk doel voor dreigingsactoren. Naast onvoldoende middelen is vaak ook het bewustzijn bij management erg laag tot niet aanwezig. Dit is niet omdat ze het niet belangrijk vinden, maar omdat andere bedrijfsprioriteiten voorrang krijgen.
Aan de andere kant merken we ook dat het echte gevaar zich alleen voordoet als het een aanzienlijke groep van deze MKB-organisaties tegelijk raakt. Voor de individuele organisatie is en blijft het natuurlijk niet leuk om onder aanval te komen, maar individuele organisaties hebben in het grote plaatje weinig tot geen impact. De vraag blijft wat er voor een dreigingsactor te halen valt bij deze organisaties. Er zal geldelijk gewin zijn, maar door de grootte van de organisatie zullen het geen super hoge bedragen zijn.
Is de kleine man dan wel belangrijk? Vanuit ons als security professionals is elke organisatie belangrijk. Ook in de keten kunnen MKB-organisaties van belang zijn. Denk aan Diginotar in 2010. Maar kijkend naar de prioriteiten is het logischer om de grote organisaties, indien deze getroffen worden door een groot cyberincident, te helpen vanwege de grote schade die ze in de maatschappij kunnen aanrichten. Besluit zelf of de kleine man belangrijk is.

Referenties

(1) https://www.cbs.nl/nl-nl/nieuws/2019/31/meer-kleine-mkb-bedrijven
(2) https://www.cbs.nl/nl-nl/nieuws/2019/41/robuuste-groei-toegevoegde-waarde-in-het-mkb

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

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

BLADMANAGEMENT
MOS bv
José Broekhuizen
Lisa Petersen
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE
MOS bv
Jan van de Vis
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 2019 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

COLUMN Berry

Niet zo geheimzinnig

Op een regenachtige zondagmiddag zit ik achter mijn pc en lees ik nieuwsberichten en allerlei andere berichten die nauwelijks nieuws genoemd mogen worden. Een van de berichten die ik lees valt denk ik wél onder 'nieuws', maar ik twijfel nog. Het zou ook gewoon fake news kunnen zijn. Het gaat weer over mijn grote vriend Zuckerberg, de CEO van Facebook.

Deze Zuckerberg zat op een ochtend achter zijn bureau en las een mail waarin Facebook werd gevraagd om hun plannen om end-to-end-encryptie toe te passen in te trekken, omdat het op die manier voor de overheden erg lastig wordt de inhoud van alle berichten te zien.

Zuckerberg krabt zich op zijn achterhoofd en leest de mail nogmaals. Het staat er toch echt en het is ondertekend door de Verenigde Staten, het Verenigd Koningrijk en Australië. Ook niet echt de kleinsten. Zuckerberg staat op, loopt naar zijn espressoapparaat, drukt vijf keer op de 'extra strong'-knop en de machine komt tot leven. Hij neemt een teugje en vraagt zich af of hij het goed begrijpt. Een jaar geleden kwam de hele wereld rollebollend over hem heen, omdat hij gegevens van 87 miljoen Facebookers had afgegeven aan Cambridge Analytica om te analyseren en te verkopen. Inmiddels is het Engelse bedrijf gestopt dankzij alle negatieve publiciteit. Ik begrijp de verwarring van Zuckerberg, hij wil het allemaal geslotener maken om de privacy van de Facebookers te beschermen.

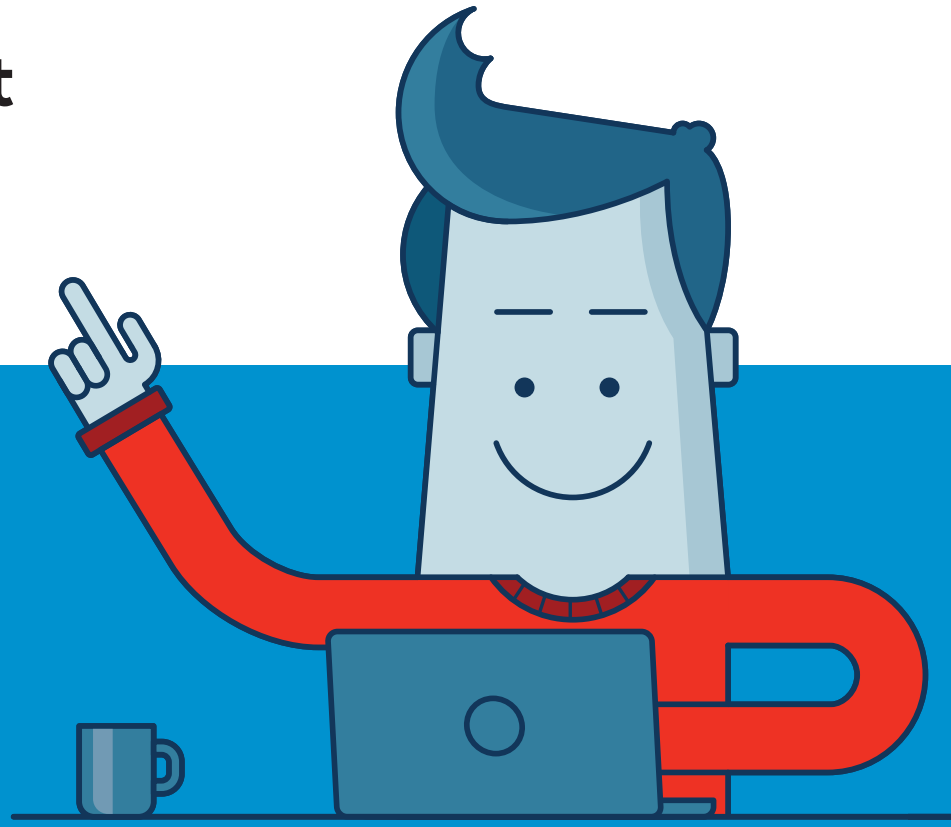
Zoals bekend is Zuckerberg ook eigenaar van WhatsApp. Deze berichtenapp heeft al jarenlang de end-to-end-encryptie en is dus ook erg lastig in te zien door de drie eerder genoemde landen. Zuckerberg wil ook Messenger (onderdeel Facebook) en Instagram (ook onderdeel van Facebook) de encryptie geven om deze te integreren met WhatsApp.

Gelukkig hebben we slimme lezers en die hebben geconcludeerd dat Messenger en Instagram dus geen end-to-end-encryptie hebben. Geheime diensten kunnen nu dus alles vrij eenvoudig inzien. Deze geheime diensten zijn bang dat kinderporno gaat toenemen als controle niet meer mogelijk is en Facebook meer misbruikt wordt. Dat zou natuurlijk verschrikkelijk zijn, maar het is tegelijkertijd een niet valide argument. De uitwisseling vindt plaats op hele andere platforms en daarbij is het dark web wel een hele belangrijke. Alle acties waarvan de buurman niets mag weten gebeuren daar: illegale handel, smokkel, kinderporno, organisatie van botnets en dat soort illegale zaken. Gewoon je eigen zin doordrijven Zuckerberg, goede actie!

Berry

Zonder integrale aanpak is Privacy & Informatiebeveiliging een Russische roulette:

Ben jij al echt in control?



Door Privacy & Informatiebeveiliging integraal te benaderen, krijg je een beter inzicht in risico's en zorg je voor bewuste medewerkers die de juiste maatregelen kunnen toepassen op de juiste plek én het juiste moment.

- Meer privacy en security in minder tijd
- Completer inzicht in risicolandschap
- Versterking van de menselijke schakel

smile

Nieuwsgierig naar de mogelijkheden?

Download de Whitepaper op www.smile.nl/whitepaper-privacy