iB
INFORMATIEBEVEILIGING
jaargang 19 - 2019
#1

Borsten hacken en ander privacyleed

Controle is goed, maar vertrouwen is beter

Risk paralysis by analysis

Datalekken

TSTC

ICT en Security Trainingen

Next Generation Cybersecurity Training

TSTC is een gerenommeerd IT opleidingsinstituut en erkend specialist in informatie beveiliging-, cybersecurity en privacy trainingen.

Top 10 Security trainingen

CEH • OSCP • CCSP • CCFP • CISSP • C|CISO • CRISC
Privacy CIPP/E-CIPM • CISM • ISO 27001/27005/31000

Nieuw in 2019

- Extreme Hacking NextGen tm
- Cybersecurity Compliance Officer
- Cybersecurity Specialist
- Certified Chief Innovation Officer
- Red team vs Blue team

Recognition for Best ATC's and CEI's

TSTC Accredited Training Center of the Year 2017

Circle of Excellence Instructor 2017

www.tstc.nl

GOEDE VOORNEMENS

Een nieuw jaar; voor velen gepaard met goede voornemens. Natuurlijk heeft u (als IB&P pro) geen information securityvoornemens meer, anders dan continue verbeteren, maar geldt dat ook voor uw management? Welke goede voornemens heeft uw bestuur? En wat te denken over de organisaties – groot en klein – waar u niet de pro bent die men in huis (nodig) heeft?

Worden er dit jaar toch echt maatregelen genomen tegen alle dreigingen die (hopelijk) al wel zijn geïnventariseerd? Dachten zij vorig jaar nog dat het wel 'los zou lopen met die AVG' en willen ze nu toch beginnen, of waren ze al overtuigd en is men al helemaal op orde met alle zaken rondom informatiebeveiliging? Hoe dan ook, het blijft een kwestie van bij blijven en zaken stap voor stap aanpakken.

Nu nog beginnen betekent: inventariseren waar de risico's liggen en daar gepaste maatregelen tegen nemen. Als u al helemaal klaar denkt te zijn, blijft het zaak om te evalueren en telkens te herijken. In beide gevallen adviseren we om klein te beginnen. Het gevaar om overweldigd te worden door alle meningen - intern en extern - is groot en voordat je het weet, weet je helemaal niet meer waar te beginnen. In deze uitgave hebben we hierover een interessant artikel: 'Risk Paralysis by Analysis'.

Nu nog beginnen is overigens wel een heel goed begin van 2019 en een goed voornemen om zeker na te streven. 2018 was een jaar met veel voorpaginaberichten. We kennen uiteraard allemaal de invoering van de AVG, de globale cyberaanvallen met ransomware, de boetes vanwege privacyschendingen en de vele voorspellingen van experts uit het veld.

Informatiebeveiliging & privacy waren 'hot' en de verwachting is dat dit in 2019 niet minder wordt. Het dringt, gelukkig, bij steeds meer mensen en organisaties door: (privacy)gevoelige gegevens zijn overal en daarmee is informatiebeveiliging voor iedereen.
De AP controleert stelselmatig op verschillende onderdelen en in diverse branches. Nu kennen wij ook de geluiden dat de AP 'het niet genoeg doet' en 'helemaal niet zichtbaar is'. Of je het daar nu mee eens of oneens bent, feit is wel dat er gehandhaafd wordt. Dit is voor veel bedrijven een welbekende stok achter de deur. Voor anderen een moment om aan te tonen dat het securitydenken al helemaal in het DNA van de organisatie zit. Een interessante inkijk daarop geeft Sjoerd Peerlkamp in zijn artikel op pagina 15.

Wat uw goede voornemens voor dit jaar ook mogen zijn, wij zijn in ieder geval van plan om u ook dit jaar weer te voorzien van een aantal uitgaven met mooie artikelen, achtergrondinformatie en relevante items. Uiteraard doen we dat samen met u; in deze uitgave vindt u artikelen welke uitnodigen tot het gezamenlijk nadenken over oplossingen (zie de 'call to action' van Bas van Gils op pagina 13).

Want, zoals Lex Dunn in zijn - voorlopig - laatste artikel in deze PvIB ook aangeeft, alleen door kennis te delen, kunnen we kwaadaardige acties voor zijn of pareren. Laten dat daarmee ons gezamenlijke, goede voornemens zijn.

Veel leesplezier en uiteraard horen we graag van u.

Tom Bakker en Bianca Brooijmans

In dit nummer

INTERVIEW

Lex Dunn neemt afscheid van PvIB en iB-magazine

UIT HET OOG, MAAR NIET UIT HET HART

Zijn laatste taak als lid van de redactie van iB-magazine heeft hij net afgerond. Het controleren van de drukproef van de laatste uitgave waaraan hij meewerkte. Niet iets wat hij zal gaan missen, geeft Lex Dunn onmiddellijk aan het begin van dit afscheidsinterview aan. "Altijd last minute, altijd een klus", blikt hij terug.

Wanneer ik hem direct daarna vraag wat hij wél gaat missen - dit nu hij inmiddels ook zijn lidmaatschap van het PvIB heeft opgezegd - hoeft hij niet lang na te denken: "De thema-bijeenkomsten. Daarvan heb ik veel geleerd. Ik heb als securityspecialist altijd aan de policy kant gezeten. Door allerhande thema-avonden van het PvIB te bezoeken, werd mijn scope echter veel breder. Zo is de eerste hackersworkshop die ik meemaakte me altijd bijgebleven. Het was voor het eerst dat ik een kijkje kreeg in het brein van een hacker. Hoe denkt hij? Waar ziet hij kansen? Zo leerzaam. Hierdoor is vervolgens mijn interesse in bijvoorbeeld Black Hat ontstaan."

Wijnstokken

Voor degenen die het nog niet weten: Lex verruilt nog dit jaar, uiterlijk per 1 juli, Almere voor een dorpje in het zuiden van Frankrijk. Een dorp met 250 inwoners in de buurt van Perpignan, waar hij al elf jaar samen met zijn vrouw komt. Ze hebben er een huis gekocht met daarbij drieduizend vierkante meter grond. "Genoeg ruimte dus om wat wijnstokken te planten", geeft Lex een inkijkje in zijn toekomstige leven. Een leven dat voor een deel ook nog steeds zal bestaan uit werken. Lex gaat zich inschrijven bij de Franse Kamer van Koophandel zodat hij in Frankrijk - of Nederland, maar dan op afstand - als freelance securityspecialist aan de slag kan. "Omdat ik het leuk vind én om de extraatjes te bekostigen die het leven daar nog net wat aangenamer maken. Dit totdat ik helemaal kan gaan genieten van mijn pensioen", legt hij uit.
En juist omdat hij dus in het vak werkzaam blijft, sluit Lex het niet uit dat hij vanuit Frankrijk 'als leverancier van bijdragen' bij het blad dat u nu leest betrokken zal blijven. "Zijdelings", benadrukt hij. "Maar wie weet wat ik allemaal bedenk wanneer ik nippend aan een glaasje Pastis uitkijk over het Franse land", mijmert hij.

Sandra Kagie is freelance tekstschrijver/journalist. Als ervaren tekstschrijver en eindredacteur verricht zij uiteenlopende werkzaamheden op het gebied van tekst & taal. In het verleden is zij als eindredacteur nauw betrokken geweest bij 'Informatiebeveiliging'. Haar website is www.sanscriptproducties.nl en op Twitter is zij actief als @SanSanscript.

Ideeën voor nieuwe artikelen heeft hij nog niet. ‘Project verhuizen naar Frankrijk’ heeft momenteel prioriteit. “Daar gaan flink wat uren per week in zitten. Maar wanneer ik er gesetteld ben, begint het vast weer te kriebelen. Bovendien zullen de contacten met mensen uit het vak blijven, bijvoorbeeld via LinkedIn. Dat zal ongetwijfeld weer inspiratie voor bijdragen opleveren.”

Nieuwe werkwijze

Lex zou dan vanuit Frankrijk de nieuwe werkwijze die het PvIB voorstaat in de praktijk brengen. “We willen als club met zo’n zestienhonderd leden namelijk meer leden actief bij het PvIB betrekken. De actieve club meer body geven. Nu zijn we veel te afhankelijk van zo’n vijftig à zestig actieve leden.” “Door mensen éénmalig verantwoordelijkheid te geven voor een bepaald ‘werkpakketje’ willen we voorkomen dat we steeds een beroep doen op diezelfde mensen. Daarom gaan we via een soort Marktplaats op de website een beroep doen op álle leden, zoals al door Evert van Santen uit de doeken gedaan in iB-magazine 6.” “De redactie kan bijvoorbeeld op de website vragen of iemand een specifiek artikel wil schrijven of een boekbespreking wil maken. Terwijl de activiteitencommissie kan vragen om hulp bij het regelen van sprekers voor een thema-avond. Degene die het werkpakketje op zich neemt, is hiervoor vervolgens verantwoordelijk. Maar hij of zij hoeft zich niet direct voor de langere termijn te committeren aan een bepaalde commissie.” En hoewel Lex dus geen lid meer is van de club, ziet hij een dergelijke ‘losse rol’ voor zichzelf zeker zitten. Uit het oog is wat hem betreft dus zeker niet uit het hart.

Historie binnen de club

Vanaf februari 2007, hij heeft het voor het interview nog even opgezocht, heeft Lex deel uitgemaakt van de redactiecommissie van het iB-magazine. Daarvoor was hij al lid van de activiteitencommissie van het toenmalige Genootschap van Informatiebeveiliging (GvIB).
Trots qua bijdrage aan het iB-magazine is hij desgevraagd op de rubriek ‘Achter het Nieuws’. Een idee uit zijn koker. In de rubriek geven iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems aangaande informatiebeveiliging. “Persoonlijke meningen die niet noodzakelijk het officiële standpunt weergeven van hun werkgever of van het PvIB”, legt Lex uit. “Maar juist daarom interessant omdat we op deze manier discussie proberen uit te lokken met leden en lezers. Interactie met onze lezers waar we als redactie behoefte aan hebben.”

Verscheidenheid

Zijn carrière in de IT begon in 1981. En sinds 1999 is hij specifiek binnen het vakgebied informatiebeveiliging actief. Wat hem als professional aanspreekt in het PvIB is de verscheidenheid aan mensen die de club herbergt. “Alles draait tegenwoordig in ons vakgebied om het uitwisselen van kennis en informatie. Alleen wanneer je kennis deelt, kun je kwaadwillenden te slim af zijn. Die kwaadwillenden worden immers steeds beter en professioneler.” Om kennis en informatie te delen, is wederzijds vertrouwen volgens Lex een absolute voorwaarde. “En ik heb het altijd als een enorm voordeel beschouwd dat ik via het PvIB al heel veel mensen kende waar ik later in de praktijk mee heb mogen samenwerken. De vertrouwensbasis voor de samenwerking was vaak al gelegd.”

Redactiepet

“Blijf om je heen kijken en praat met vakgenoten.” Dat is het advies dat Lex tot slot aan zijn voormalige collega’s binnen de redactiecommissie wil meegeven. “Een interessant artikel zit vaak in een klein hoekje, zo heb ik mogen ervaren. In een gesprek met een collega of vakgenoot zette ik daarom op zijn tijd altijd even mijn ‘redactiepet’ op. Ik zal proberen dit in Frankrijk te blijven doen.”

JESSICA CONQUET

Mijn naam is Jessica Conquet. Binnen het bestuur van het PvIB vervul ik de rol van voorzitter. Vanuit mijn voorzittersrol zit ik regelmatig met diverse partijen rond de tafel om te praten over onze vereniging.
Het valt me op dat veel bedrijven onbekend zijn met het PvIB. Ze willen graag weten hoeveel leden we hebben, in welke branche de leden werkzaam zijn en wat de doelstelling is van de vereniging. Vooral in het afgelopen jaar kreeg ik menigmaal de vraag of PvIB 'als beroepsvereniging' een mening had over een bepaald onderwerp. Ook wordt er regelmatig gevraagd of wij trainingen verzorgen. Gelet op het feit dat we gezamenlijk over zoveel kennis beschikken, is die vraag eigenlijk ook niet zo gek. De vragen die ik tijdens mijn bezoeken 'in het veld' krijg, neem ik mee en breng ik ter tafel tijdens de bestuursvergaderingen. Als voorzitter zit ik ook tweemaal per jaar de Algemene Ledenvergadering (ALV) voor.

Naast mijn rol als voorzitter van het bestuur ben ik tevens werkzaam als global IT security officer bij ABN AMRO Clearing. Ik ben zeer gepassioneerd over mijn vak en mijn functie binnen de securitypraktijk van de bank. Ik maak regelmatig buitenlandse zakenreizen naar mijn teamleden in Noord-Amerika en Azië. Ik krijg enorm veel energie van mijn werk, vanwege de dimensie in de verschillende landen/werelddelen en het feit dat het nooit saai is binnen het cybersecuritydomein. Mijn stakeholders zijn van zeer uiteenlopende pluimage. Ik moet me enerzijds inleven in de risicobeleving van de C-level topmanagement en anderzijds in het cyber- en informatiebeveiliging bewustzijn van een ontwikkelaar. Daarnaast zijn we bij de bank uiteraard ook afhankelijk van de dienstverlening van externe partijen. Ik overleg op dagelijkse basis ook met leveranciers en partners waarmee we samenwerken.

Ik verwacht dat 2019 een heel interessant jaar gaat worden voor ons vakgebied. We worden meer en meer gezien als een gesprekspartner en daarmee moeten we ook als vakbroeders en zusters andere skills aanwenden. De publieke en private sectors gaan meer aansluiting zoeken bij het PvIB en daarmee verwacht ik dat we als vereniging nog slagvaardiger kunnen gaan opereren.

Verder hoop ik nog vaker in gesprek te kunnen gaan met onze leden, zodat we ons programma nog beter kunnen laten aansluiten bij de behoefte van onze leden.

Jessica Conquet

VERMIJD EEN BLINDSPOT: RISICO'S VAN SCHADUW IT

Eind 2017 begin 2018 heb ik onderzoek gedaan naar het fenomeen 'schaduw IT' (SIT) en hoe de negatieve effecten met behulp van IT governance (ITG) kunnen worden beheerst.

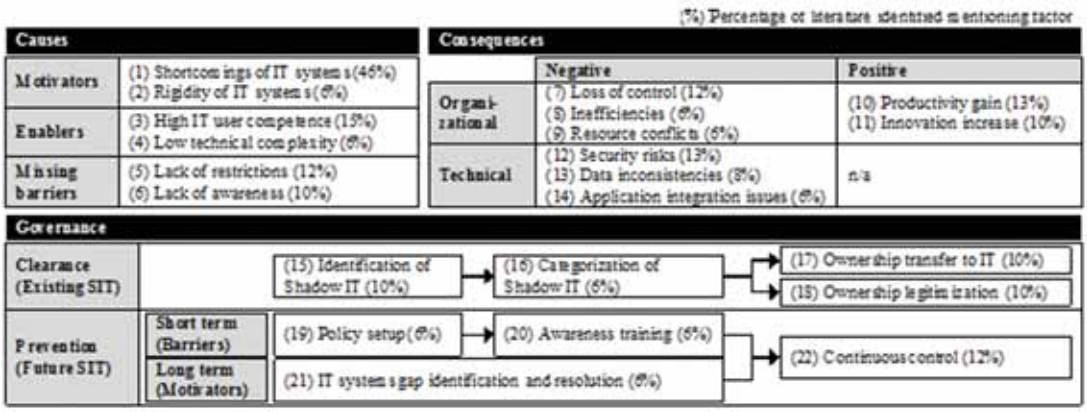
Allereerst is het van belang om een goed beeld te krijgen wat schaduw IT dan precies is: Schaduw IT (SIT) is de naam voor software en hardware die in een organisatie voorkomt zonder dat de formele IT-organisatie daarbij betrokken is (Kopper & Westner, 2016).

Er zijn grof genomen vier verschijningsvormen van SIT te vinden in de literatuur:

- Clouddiensten zoals SAAS-oplossingen; Office365, Dropbox en OneDrive.
- Zelf ontwikkelde applicaties zoals Microsoft Access databases en Excel-sheets.
- Zelf aangeschafte en vervolgens geïnstalleerde applicaties op de door IT aangeboden middelen.
- Zelf aangeschafte hardware of mobile apparatuur zoals smartphones en tablets.

Vele organisaties worstelen met het vraagstuk waarom SIT ontstaat en of SIT wel of niet leidt tot risico's. In een poging inzicht te geven in de beheersing van de risico's van SIT met behulp van het toepassen van governance, is er onderzoek uitgevoerd. De centrale onderzoeksvraag van dit onderzoek luidde als volgt: in hoeverre kan een (IT-) governance bijdragen aan het beperken van de risico's van schaduw IT?

Het fenomeen SIT is met name onderzocht bij streng gereguleerde organisaties, zoals banken- en verzekeringswezen en er is nog weinig bekend over de



Figuur 1 - Framework for causes, consequences, and governance of Shadow IT (Kopper & Westner, 2016)

toepassingen hiervan bij andere sectoren waaronder, onderzoek en onderwijs. Kopper en Westner hebben in 2016 een onderzoek uitgevoerd bij een een aantal zeer gereguleerde organisaties (zoals banken en industrie in Duitstalige landen) en hebben een framework ontwikkeld met een model voor de governance van SIT. Het framework bevat de oorzaken, gevolgen van de SIT voor een organisatie en de governance benaderingen.

In het governance model van het framework van figuur 1 worden er twee benaderingen weergegeven: de 'Clearance' (Existing SIT) en 'Prevention' (Future SIT). Bij de laatstgenoemde benadering wordt er gebruik gemaakt van het opwerpen van barrières en de motivatoren achter de keuzes voor SIT worden aangepakt. De onderzoekers gaan er ook vanuit dat het totaal uitbannen van SIT binnen een organisatie niet mogelijk is en ook niet wenselijk is. De meeste onderzoeken naar de positieve gevolgen van SIT wijzen uit dat met name de SIT wordt toegepast om te vernieuwen (innovatie) en op het vlak van productiviteit toegevoegde waarde heeft (György, Cleven, Uebernickel, & Brenner, 2012).

Risico's van SIT

Verlies van grip op IT en controle op data is een belangrijk risico voor organisaties. In de door SURF (ICT-samenwerkingsorganisatie van het onderwijs en onderzoek in Nederland) opgestelde dreigingsanalyse wordt het verlies van data aangemerkt als belangrijkste risico voor onderzoek en bedrijfsvoering (SURF, 2016). Daarnaast zijn er binnen universiteiten verschillende onderzoeksgroepen die gebruik maken van privacygevoelige gegevens. Het lekken van deze gegevens kan grote gevolgen hebben voor de subjecten en kunnen flinke boetes opleveren voor de bestuurders.

De meeste organisaties zijn ook risico-avers als het gaat om verlies van data (privacygevoelige data), omdat dit uiteindelijk zeer grote gevolgen voor het imago kan hebben van bijvoorbeeld een universiteit. Imagoschade kan invloed hebben op de toestroom van studenten en inkomsten uit researchopdrachten (valorisatie). Zeker gezien de waarde die studenten en onderzoekers hechten aan privacy en informatiebeveiliging.

Ing. Léon Wiskie MBI CISSP CCSP is een zelfstandig professional op het gebied van IT en informatiebeveiliging. Hij heeft dit artikel geschreven op basis van zijn thesis voor de masteropleiding Business Information, waar hij risicobeheersing rond schaduw IT heeft onderzocht.
Leon is te bereiken via leon.wiskie@wiskieit.nl of LinkedIn www.linkedin.com/in/leonwiskie

De grootste risico's van SIT zijn:
- verlies van grip op IT en controle op data (loss of control);
- informatiebeveiligingsrisico's (security risks).

Beheersing van SIT door governance

In dit onderzoek is IT governance gedefineerd als:
1. verzorgen van alignment IT-dienstenaanbod op de behoefte van de business;
2. effectieve en efficiënte besturing van de organisatie;
3. beperken van risico's met betrekking tot IT-investeringen: waarde creëren voor de organisatie maar ook waarde behouden voor de organisatie door controle en nemen van maatregelen.

Een belangrijke pijler is risicomanagement: het effectief toepassen ervan maakt het mogelijk doelen te realiseren en falen van IT te beperken

Om SIT onder controle te krijgen, kan men IT governance inzetten als beheersmiddel. Concreet betekent dit dat SIT onder de risicomanagement processen gecontroleerd kan worden door het overdragen naar de IT-afdeling of dat de business managers de risico's accepteren en dragen. Verder kan de organisatie korte termijn maatregelen treffen door extra barrières op te werpen om nieuwe SIT tegen te gaan en door de awareness van medewerkers vergroten. Als lange termijn oplossing kan men de motiverende factoren voor SIT wegnemen, door betere samenwerking tussen business en IT. Tenslotte is het toepassen van detectie en monitoring een belangrijk onderdeel van preventie.

Casestudy

Voor het empirisch deel van het onderzoek is er gebruik gemaakt van een casestudy, met als onderzoekseenheid een universiteit in Nederland dat bestond uit interviews met experts binnen de organisatie en bestudering van de bedrijfsdocumentatie.

In de casestudy is er gebruik gemaakt van de onderstaande empirische deelvragen:
1. Welk risicoprofiel is acceptabel en welke wet- en regelgeving is voor de universiteit relevant?
2. Wat is de beheersing van de risico's van SIT bij de universiteit?
3. Wat is de volwassenheid van de relevante ITG processen en is er een samenhang met de beheersing van SIT bij de universiteit?

Op basis hiervan kunnen de volgende uitspraken gedaan worden die tenminste geldig zijn voor de casestudy organisatie:
- Het toepassen van governance kan de risico's van de SIT beperken. Er is een blindspot ontstaan door het gebruik van SIT.
- Er wordt onvoldoende gecontroleerd op naleving van geldend beleid en toepassing van maatregelen op de niet door IT beheerde systemen.

Naar aanleiding van dit onderzoek kunnen in ieder geval de volgende aanbevelingen worden gedaan:
- vermijden van een blindspot door het toepassen van IT-assetmanagement;
- toepassen van meer interne controle en audits om compliance aan te kunnen tonen.

Naar aanleiding van het onderzoek zijn er daarnaast minimaal twee aanbevelingen die gedaan kunnen worden die in ieder geval van toepassing zijn op de case organisatie.
1. IT-assetmanagement: zeker door het toenemend gebruik van BYOD- en Cloud-toepassingen is het van belang dat er een beeld ontstaat van de het totale IT-landschap en waar bepaalde data zich bevindt.
2. Door het toepassen van risicomanagement kan er dan gekeken worden naar de bedreigingen per asset. Daarnaast is het van belang om eerdergenoemde data te classificeren en beleid op te stellen waar bepaalde data binnen of de buiten de organisatie mag worden bewerkt. Dit maakt het mogelijk om technische en organisatorische maatregelen te treffen die in overeenstemming zijn met de risicoacceptatiegraad van de organisatie.

Uiteraard is dit onderzoek toegespitst op een specifieke organisatie maar waarschijnlijk is het goed toepasbaar bij andere organisaties die met dezelfde problematiek worstelen. Het doel van de governance van SIT is het vermijden van een `blindspot': een vergeten of decentraal beheerde IT-voorziening waardoor organisaties aan meer risico worden blootgesteld dan acceptabel is.

Referenties

- Györy, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. Ecis 2012 Proceedings.
- Kopper, A., & Westner, M. (2016). Deriving a Framework for Causes, Concequences, and governance of Shadow IT form literature.
- SURF. (2016). cyberdreigingsbeeld 2016 Sector onderwijs en onderzoek.

Mr. Rachel Marbus
@rachelmarbus op Twitter

BORSTEN HACKEN EN ANDER PRIVACYLEED

Wat hebben een meisje van 11, borstimplantaten en de Museumjaarkaart met elkaar gemeen? Persoonlijk privacyleed. Deze keer eens geen start van het jaar met grootse vooruitblikkende privacyzaken of weidse vergezichten aangaande aanstaande privacyschendingen door onze overheid. Bovenstaande lijkt een enorm bizar bij elkaar geraapt rijtje zaken, maar in alle gevallen gaat het om intiem persoonlijk privacyleed wat niet de voorpagina's haalt, maar wel uitermate nare persoonlijke schade kan veroorzaken.

Het geval van de Museumjaarkaart is saillant vervelend. Een mevrouw, sinds lange tijd al gescheiden en daarna 3 maal van adres gewisseld, krijgt op een dag de Museumjaarkaart van haar ex op de mat. Ze kon er niet om lachen en vond het freaky. Ik kan me daar wat bij voorstellen. Mijn twee huwelijken zijn ook niet bepaald voor niets geëindigd. Maar erger nog, stel nu dat de twee ex-echtlieden elkaar niet meer mogen zien, omdat er bijvoorbeeld gewelddadigheden hebben plaatsgevonden in het verleden? Je moet er toch niet aan denken dat een ander dan heeft zitten blunderen met je goed geheimgehouden adresgegevens. Zo kan klein persoonlijk privacyleed snel groot worden.

In de VS zat een meisje lekker te surfen op het internet toen ze op de blog van haar moeder stuitte. Haar moeder blogt over haar moederschap en daarmee ook over het meisje. Met naam en toenaam en vele foto's. Ze vroeg haar moeder de blogs te verwijderen en ook niet meer in de toekomst over haar te schrijven. Moeder blogde vervolgens dat ze dat toch absoluut niet ging doen, waar moest ze dan immers anders over gaan schrijven? Ze was er nog trots op ook. Wat me opviel in de commentaren was dat iedereen vooral over de moeder heen buitelde (en dat kan je heel terecht vinden), maar dat niemand uiteindelijk echt opkwam voor het meisje. Maar goed, internet eigen, liever azijn schenken dan honing geven.

Nu over naar die borsten. Gezien het feit dat het over borsten gaat, zou het zomaar toch wel eens het nieuws kunnen gaan halen, maar op het moment van schrijven: geen voorpagina's. Wat blijkt? Verschillende borstprotheses (let op: niet allemaal dus) bevatten een RFID-chip. Met een uniek nummer. Wat zoals elke RFID-chip uitgelezen kan worden met de juiste apparatuur. Daarnaast waarschuwde Melanie Rieback al jaren geleden dat dergelijke chips slecht beveiligd zijn en daardoor makkelijk te hacken. Je kunt dus niet alleen naar borsten kijken, je kunt ze ook uitlezen en hacken.

Er is veel meer privacyleed dan wat de voorpagina's haalt. Daar staan toch doorgaans de grote datalekken en zeer gevoelige grote inbreuken op privacy. Misschien een schone taak voor de toezichthouder om eens wat meer te drukken op dit 'kleine' leed. Bij de toezichthouder hebben ze trouwens ook nieuws! Er zijn inmiddels, na een lang solobewind door voorzitter Wolfsen, twee nieuwe leden aan het bestuur toegevoegd. En nog wel twee vrouwen. Daarover ben ik toch wel in mijn nopjes. Erg jammer alleen dat de dames beiden geen ervaring hebben met privacy. Dat is echt een enorm gemiste kans. Maar goed, in klein leed kan iedereen zich invoelen toch? Dus hopelijk leren de dames snel veel bij over privacy in de praktijk, want daar gaat het veel vaker over dit soort zaken dan over de grote vissen.

ARCHITECTUUR ENABLER VOOR DIGITALE TRANSFORMATIE

De digitalisering van de maatschappij is een feit: praktisch alles kan vanaf de bank met een smartphone geregeld worden. Vaak (b)lijkt dit nog eenvoudiger te gaan dan in de fysieke wereld. Probeer maar eens geld over te schrijven door langs een bankkantoor te gaan. Deze digitalisering biedt organisaties kansen. Tegelijkertijd gaat er ook een serieuze dreiging vanuit: als je niet meegaat in het digitale 'spel' of als er teveel incidenten rond informatiebeveiliging plaatsvinden, dan ben je zo maar out of business.

Informatiebeveiliging en architectuur

Eén van de disciplines die essentieel is voor effectieve grootschalige transformaties van organisaties is architectuur. Er zijn veel definities van dit begrip in omloop. Kort samengevat komt het neer op het volgende:

- De architectuur van een systeem betreft twee aspecten: (1) wat is de fundamentele organisatie van het systeem en (2) wat zijn de principes die daaraan ten grondslag liggen?
- Het bedrijven van architectuur komt neer op het 'sturen op samenhang' in de context van grootschalige transformatietrajecten, waarbij de nadruk ligt op de grote lijn, wetende dat 'the devil in the details' is.
- Architecturen worden veelal vastgelegd in modellen. De taal ArchiMate is hiervoor een marktstandaard.

Informatiebeveiliging, als onderdeel van beveiliging in het algemeen, betreft het vertalen van de 'risk appetite' van de organisatie naar een concrete en consistente set aan maatregelen waarmee de informatie assets van de organisatie voldoende worden beveiligd. De sleutelwoorden hierin zijn: (1) consistent en (2) maatregelen.

Het samenspel tussen architectuur en informatiebeveiliging laat zich dan ook makkelijk duiden: voorgestelde beveiligingsmaatregelen zijn input voor het architectuurproces waarin de uitwerking ervan wordt geborgd.

Architectuurmodellen vormen bij uitstek een goed analyse- en visualisatiemechanisme om de impact van deze maatregelen te doorgronden en de organisatie daarmee het vertrouwen te geven dat de veiligheid van informatie assets geborgd is. Een

klein voorbeeld om dit te illustreren: stel je voor dat een grote internationale lease maatschap als principe 'back in the box' heeft. Daarmee wordt bedoeld: om onze dienstverlening goed op te kunnen, tuigen hebben we een aantal bedrijfsfuncties of capabilities nodig, zoals CRM, Legal, Contract Management, Sales, et cetera. Elke capability kan als een 'box' worden gezien. De bedoeling van het principe is dat elke capability zo veel mogelijk zelfstandig gerealiseerd wordt, dus met eigen processen, mensen, data en systemen. Je kan je voorstellen dat er nogal wat data flows nodig zijn tussen de verschillende capabilities en dat daar de nodige risico's aan verbonden zijn. Hoe ga je bijvoorbeeld om met afwijkende privacyrichtlijnen in verschillende landen waar het om klantdata gaat, terwijl je de CRM capability maar één keer wil inrichten?

Hoe voorkom je dat bepaalde maatregelen in elke capability apart en/of op verschillende manieren en dus dubbelop worden opgelost, terwijl een eenvoudiger maatregel op ondernemingsniveau voor de hand ligt? Anders gezegd: hoe voorkom je dat ieder zijn eigen stoepje wel schoon heeft gepoetst met beveiligingsmaatregelen, maar dat de organisatie als geheel nog uitermate kwetsbaar is met alle gevolgen voor de bedrijfscontinuïteit van dien?

Het Landelijk Architectuur Congres (LAC)

In Nederland is het NAF dé vakorganisatie op het vakgebied van architectuur in de digitale wereld. Jaarlijks wordt het Landelijk Architectuur Congres georganiseerd en sinds een aantal jaren ben ik hiervan de dagvoorzitter. Dit jaar vond het congres plaats op 15 en 16 november, en wat viel op: het thema 'informatiebeveiliging' werd veel genoemd, al was het niet als een prominent thema benoemd in het programma. Gezien de uitdaging in onze maatschappij pleit ik ervoor om hier verandering in te brengen: de thema's 'architectuur' en 'informatiebeveiliging' gaan hand in hand.
Als je door de titels van de presentaties/ sessies van dit jaar gaat dan is het niet zo gek dat het thema informatiebeveiliging zo vaak genoemd wordt. Thema's als 'gedistribueerde systemen', 'cloud & business ecosystemen' zijn onlosmakelijk verbonden met informatiebeveiliging.
Helaas lukt het niet om bij alle sessies aanwezig te zijn, al heb je als dagvoorzitter wel een goed excuus om bij meerdere sessies een kijkje te nemen. Een aantal zaken viel me wel op in de sessies die ik heb gezien:

- Steeds meer architecten lijken zich ervan bewust te zijn dat beveiliging niet iets is wat 'bovenop' een architectuur gebouwd wordt, maar juist iets is dat er een integraal onderdeel van uit maakt.
- Veel discussies gaan over de relatie tussen wetgeving (AVG), regelgeving (solvency), beveiliging, en de impact daarvan op architectuur en het informatie(systeem)landschap.
- Er worden veel kritische vragen gesteld: zijn functionele wensen/vraagstukken nog wel leidend, of zijn eisen en wensen uit wetgeving, regelgeving en beveiliging inmiddels dominant?
- Er wordt veel gesproken over de innovatie 'mind set' waarbij experimenten met data worden gedaan, vaak zonder enige vorm van toezicht. De gedachte is: eerst maar eens kijken of iets werkt, daarna zien we wel of en hoe we zaken "netjes" naar productie brengen. Wat vinden we daar eigenlijk van vanuit een beveiligingsperspectief?

Genoeg stof tot nadenken: veel vragen, en het besef dat er geen eenvoudige antwoorden zijn.

'Call to action'

Rest de vraag: 'so what'? In de praktijk zie ik architecten en informatiebeveiligingsprofessionals al nauw samenwerken. Laten we daar de volgende stap in zetten. Ik nodig alle lezers van dit blad uit om de 'call for papers' voor het komende congres (november 2019) aan te grijpen en sessies in te sturen. Laten we het congres aangrijpen om samen te bouwen aan effectieve, veilige organisaties.
(Noot van de redactie: wij overwegen om vlak voor het congres een iB-thema nummer over dit onderwerp tot stand te brengen.)

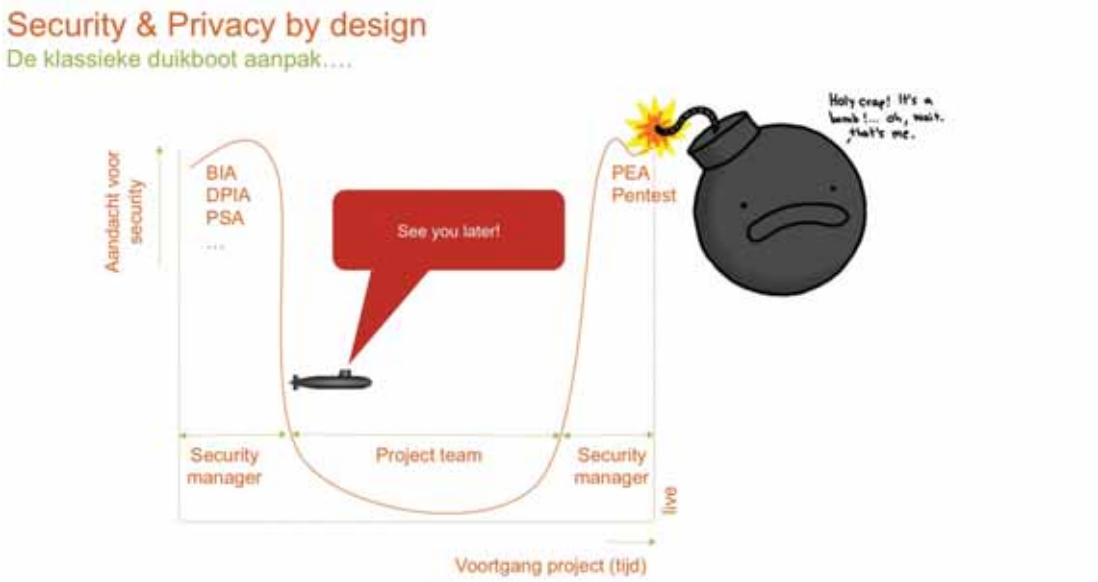
Referenties

www.naf.nl
www.laccongres.nl

Bas van Gils is managing partner en mede-oprichter bij Strategy Alliance.
Hij is bereikbaar via bas.vangils@strategy-alliance.com

SECURE BY DESIGN: CONTROLE IS GOED, MAAR VERTROUWEN IS BETER

Eind vorig jaar kreeg ik de vraag of ik een verhaal zou willen houden tijdens de CISO-25 Esmeralda lezing. Het liefst met een beetje prikkelende stelling om daarna daarover met elkaar van gedachten te wisselen. Hoe meer ik daarover nadacht, hoe meer ik uitkwam op het onderwerp `controle en vertrouwen' en hoe dat samenhangt met Secure by Design en de energietransitie waar Alliander middenin staat.



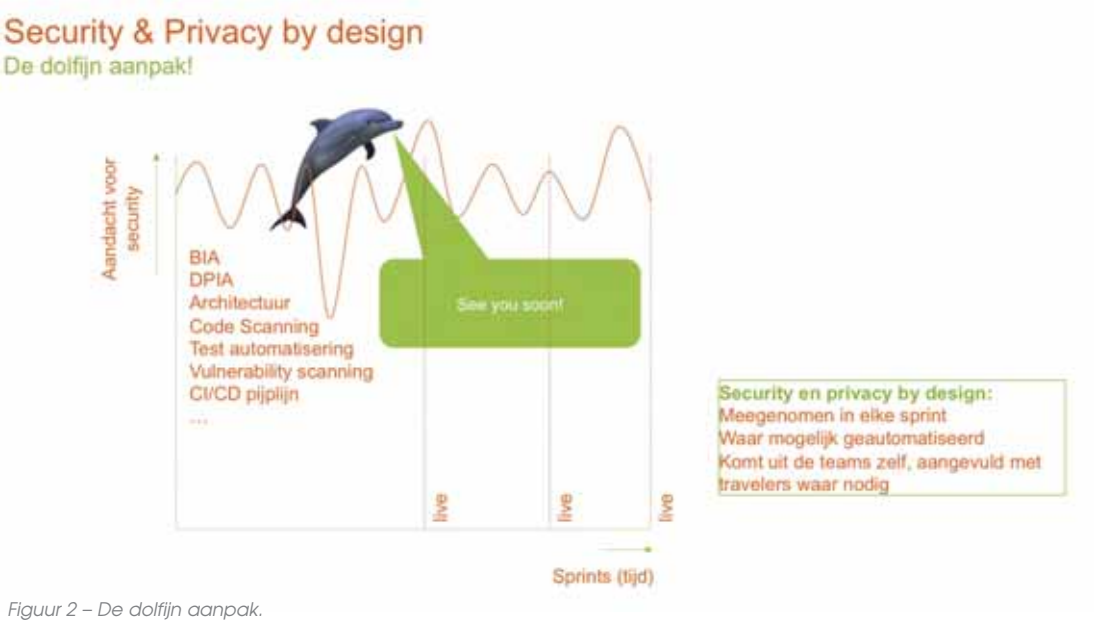
Figuur 1 - De klassieke duikboot aanpak.

Om maar even kort met het laatste te beginnen: Alliander zorgt ervoor dat het licht brandt en de huizen warm zijn, vandaag en in het duurzame morgen. Wij zorgen ervoor dat in ongeveer 1/3 van Nederland elektriciteit en gas bij jou in huis komt via onze kabels en leidingen, niet te verwarren met de rol van de energieleveranciers, die de energie leveren via ons netwerk. En die taak komt de laatste jaren met steeds meer uitdagingen. Het energiemodel verandert namelijk sterk, wat we ook wel de energietransitie noemen. Het oude model met dikke kabels vanuit centrale opwek, die steeds fijnmaziger naar alle huizen gaan, staat sterk onder druk door de snelle opkomst van decentrale opwek (zoals energie uit zon en wind), maar ook door bijvoorbeeld elektrificatie van vervoer. Daardoor wordt de piekbelasting van de kabels steeds groter. Maar alle kabels vervangen door dikkere kabels is praktisch niet haalbaar en zou de maatschappij ook onredelijk veel geld kosten. We moeten dus slimmer met onze netten omgaan en bijvoorbeeld zorgen dat we door slim om te gaan met vraag en aanbod, de piekbelasting kunnen beperken. Daarnaast gaan ook steeds meer meten in het netwerk om storingen vroegtijdig te ontdekken (of te voorspellen) en om op afstand de impact te kunnen beperken door slim te schakelen. Dit vraagt om wendbare en weerbare IT, waarbij ook informatiebeveiliging een cruciale rol speelt. Denk hierbij maar eens aan de thriller Blackout van Marc Elsberg (1) of aan de stroomstoringen in Oekraïne in december 2015 (2) en december 2016 (3).

Om tot een wendbare en weerbare IT te komen, vindt er bij ons, net als bij veel andere bedrijven, een kanteling plaats naar het 'agile werken'. In multidisciplinaire scrum teams, georganiseerd naar 'Value Streams' (4), worden die zaken opgepakt die de meeste waarde toevoegen en worden op grote snelheid kleine wijzigingen doorgevoerd. Maar hoe borg je de informatiebeveiliging binnen een dergelijke manier van werken?

Geïnspireerd door 'agile-goeroe' Rini van Solingen (5) ben ik gaan kijken hoe informatiebeveiliging in watervalprojecten verloopt en welke verschillen er zijn met agile werken. Een watervalproject lijkt namelijk sterk op een duikboot. In het begin zitten business en IT samen en komt ook vaak informatiebeveiliging eraan te pas in de vorm van Business Impact Assessments (BIA's), Data Protection Impact Assessments (DPIA's) en verplichte securitystukken in de Project Start Architectuur (PSA) die door security-architecten getoetst worden. Maar daarna duikt het project onderwater, is soms wel maanden bezig met langzaam veranderende scope of architectuur om vervolgens vlak voor de geplande livegang weer aan te

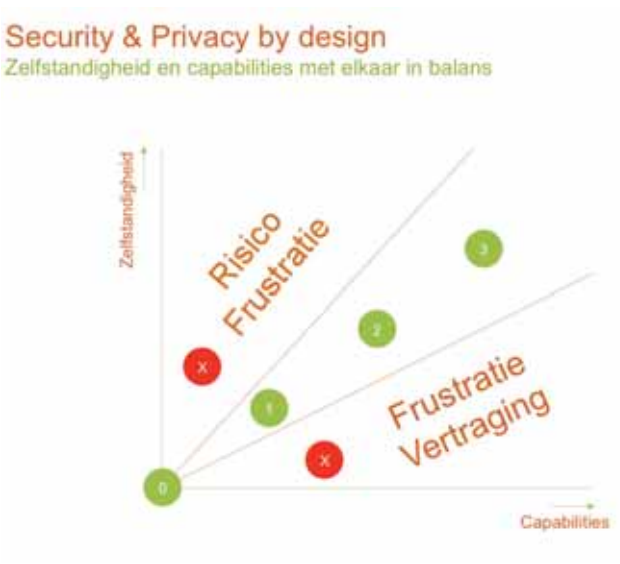
Sjoerd Peerlkamp is CISO van Alliander en is ook verantwoordelijk voor de teams met privacy- en security-experts/architecten en het cyber resilience centrum. Sjoerd is bereikbaar via sjoerd.peerlkamp@alliander.com



Figuur 2 – De dolfijn aanpak.

kloppen bij security voor akkoord op de Project Eind Architectuur (PEA) en wellicht een penetratietest, waarvan de bevindingen bijna onmogelijk nog opgelost kunnen worden voor de geplande livegang. Een zeer ontvlambare situatie, wat wordt weergegeven in figuur 1

Hoe anders is dat bij een agile manier van werken. Business en IT werken constant samen in korte sprints waarbij er steeds productdemo's worden gedaan en hoog frequent wordt bijgestuurd. Bij elke verandering een securityteam laten aanhaken voor de wijzigingen in de BIA, DPIA en (security) architectuur is dan ondoenlijk. En pas vlak voor oplevering van de definitieve 'live' producten goed naar de security (laten) kijken, is ook zeker geen optie. Daarom is er eigenlijk maar één mogelijkheid: Secure by Design. Bij alles wat we ontwerpen en ontwikkelen moeten security en privacy integraal meegenomen zijn. Eventueel kunnen concrete eisen ook in de 'Definition of Done' (6) opgenomen worden. Net als (op) tijd en (binnen) budget moet veilige producten en diensten een kwaliteitsaspect zijn dat continue meegenomen wordt. En dan verandert de duikboot opeens in een dolfijn, zoals te zien is in figuur 2.



Figuur 3 – Zelfstandigheid en capabilities met elkaar in balans.

Gedurende elke sprint is er de juiste aandacht voor security en privacy. Soms is dit wat meer, soms is dit wat minder, maar het is permanent aanwezig. En ten opzichte van het watervalmodel zijn er ook veel meer momenten dat wijzigingen live gaan. Het begint al met een minimum viable product (MVP) (7), wat daarna steeds verder verfijnd wordt in elke volgende sprint. Als security en privacy al geen onderdeel uitmaken van het MVP, wordt het lastig om dit later nog te corrigeren.
Het klinkt allemaal mooi, maar hoe zorg je er nu voor dat Secure by Design ook echt gaat werken? Daarbij is het belangrijk de balans te vinden tussen zelfstandigheid en de capaciteiten die een (scrum) team bezit op het gebied van security en privacy. Wanneer je in één keer het roer omgooit en teams 'zelfstandig' maakt zonder dat ze de juiste capabilities hebben gekregen of ontwikkeld hebben, ontstaat er veel frustratie binnen zowel de (scrum) teams als bij de security- en privacy-experts en ontstaan er ook onnodige security- en privacyrisico's. Een tegenovergestelde situatie waarin (scrum) teams wel al over de juiste capabilities beschikken, maar niet de zelfstandigheid krijgen, zorgt voor een onwenselijke situatie waarbij (scrum) teams onnodig vertraagd worden en gefrustreerd raken. Het is zaak om de balans te vinden

tussen de juiste capabilities in de (scrum) teams en de zelfstandigheid die de (scrum) teams krijgen. Dit is weergegeven in figuur 3:

Capabilities

Daarin is ook aangegeven dat je meerdere volwassenheidsniveaus kunt krijgen die de bijbehorende mate van zelfstandigheid op zouden moeten leveren. Niet elk team hoeft op hetzelfde moment niveau 3 te halen. Over welke capabilities hebben we het dan eigenlijk? Deze capabilities zijn volgens mij op te delen in vijf gebieden:

1) Beleid en kaders (of noem het de spelregels) die passen binnen de risicobereidheid van je bedrijf. Hierin zitten je technische minimale eisen voor bijvoorbeeld authenticatie of je netwerkzonering, maar ook eisen vanuit bijvoorbeeld de AVG.
2) Een juiste cultuur waarbij iedereen zich verantwoordelijk voelt voor de privacy- en security-aspecten van hun producten en waarbij collega's elkaar helpen en aanspreken op dat bijvoorbeeld kort door de bocht niet altijd de snelste route is.
3) Een juiste structuur waarbij de juiste kennis over security en privacy grotendeels in de (scrum)teams aanwezig is, maar waarbij op specialistische gebieden ook zogenaamde travelers (8) ingezet kunnen worden of op een andere manier specialisten aangehaakt kunnen worden. En ook een structuur waarbij risico's binnen de Value Streams worden bijgehouden en benodigde verbeteringen met de juiste prioriteit op de backlog belanden om daadwerkelijk opgelost te worden.
4) Beschikbaarheid van de juiste technologie. Dit gaat bijvoorbeeld over de beschikbaarheid van (security) bouwblokken, zoals identity en access management inclusief federatie zodat joiner/mover/leaver processen zonder veel inspanning automatisch goed verlopen en niet steeds opnieuw ontwikkeld hoeven te worden. En denk daarbij ook aan bijvoorbeeld (security) testautomatisering in de CI/CD (9) pijplijn. Dit kan bijvoorbeeld door automatische code scanning of vulnerability scanning waarbij een developer zelf de resultaten kan interpreteren en verbeteringen kan doorvoeren. Een ander voorbeeld is code scanning op je gehele code repository zodat je gelijk kunt zien welke modules (nieuwe) kwetsbaarheden bevatten en in welke producten deze modules gebruikt zijn;
5) Last but not least is de beschikbaarheid van het juiste talent. Je zult een actief trainingsprogramma moeten ontwikkelen om bestaande collega's in deze aanpak mee te krijgen waarbij ze op allerlei security- en privacyvlakken getraind worden, inclusief de nieuwe tooling en techniek. Dit gaat dus een stuk verder dan klassieke bewustwordingscampagnes. Ook zal nog meer dan vroeger de juiste kennis over security en privacy als noodzakelijke competentie meegenomen gaan worden bij het aantrekken van nieuw talent, zoals ontwikkelaars.

Vertrouwen

Dan kom ik op het eind toch nog even toe aan de titel van dit stuk. Of Secure by Design gaat werken, ligt volgens mij sterk aan het vertrouwen dat er is in je collega's. Als register EDP auditor (RE) heb ik geleerd dat vertrouwen goed is, maar controle beter. Als CISO kijk ik daar heel anders tegenaan: controle is goed, maar vertrouwen is beter! Als wij door de juiste capabilities (beleid, cultuur, structuur, technologie en talent) kunnen gaan vertrouwen dat al onze medewerkers de juiste dingen doen, op het gebied van security en privacy, is dat vele malen krachtiger dan dat je allerlei hoepels en blokkades moet gaan inrichten om iedereen te controleren en bij te sturen door middel van controles. En een worst case denker komt met worst case control frameworks en dat komt je wendbaarheid weer niet ten goede! Bovendien stimuleert dat mensen niet tot zelf nadenken en volgen ze dom de checklistjes zonder vanuit de bedoeling te werken en vinden ze er anders wel een weg omheen. Het kan zeker geen kwaad om aantoonbaar 'in control' te zijn en ook af en toe wat steekproeven te nemen en te analyseren waar je moet bijsturen, maar de basis moet liggen in het borgen van de juiste capabilities en daarmee het vertrouwen in de kunde van je collega's. Vandaar mijn stelling: controle is goed, maar vertrouwen is beter! En zolang je dat vertrouwen niet hebt, is er voor de CISO en de securityspecialisten werk aan de winkel om voor de juiste capabilities te zorgen zodat we wél kunnen vertrouwen op onze collega's!

Referenties

(1) 2014; ISBN: 9789022571576
(2) https://en.wikipedia.org/wiki/December_2015_Ukraine_-power_grid_cyberattack
(3) https://en.wikipedia.org/wiki/Industroyer
(4) https://www.scaledagileframework.com/value-streams/
(5) http://rinivansolingen.nl/
(6) https://agilescrumgroup.nl/wat-is-definition-of-done/
(7) https://agilescrumgroup.nl/minimum-viable-product/
(8) https://less.works/less/framework/coordination-and-integration.html#TravelerstoexploitandbreakbottlenecksandcreateskillI
(9) https://www.infoworld.com/article/3271126/ci-cd/what-is-cicd-continuous-integration-and-continuous-delivery-explained.html

CATENACCIO ALS INFORMATION SECURITYSYSTEEM

"Voetbal is een eenvoudig spel: 22 mannen rennen 90 minuten achter een bal aan en uiteindelijk winnen de Duitsers." Dat zei de Britse voetballer en commentator Gary Lineker ooit. Een lange tijd wist ik alles over voetbal, tot ik bij het bekijken van mijn eerste voetbalwedstrijd ooit in een Italiaans restaurant leerde dat de spelers zijn verdeeld in aanvallers en verdedigers. Een aanvaller kan 89 minuten van de wedstrijd ballen kwijtraken, niet op tijd zijn of bij een strafschop compleet over het doel schieten (dit gebeurt echt!), maar als hij één minuut schittert en dan een doelpunt maakt, heeft hij de partij gewonnen en in de ogen van publiek, pers en trainer een goede wedstrijd gespeeld. En een verdediger die 89 minuten piekt, alle aanvallen blokt, steeds behendig de bal afpakt, maar die ene minuut aan zijn hypotheek, zijn vriendin of een ontwerp voor een nieuwe tatoeage denkt,

kan in één minuut of met één fout de wedstrijd verliezen. En zo is het ook in securityland waar de hackers aanvallen en wij onze organisaties en (klant)data moeten verdedigen.

We weten allemaal dat het moeilijk is om aan goed securitypersoneel te komen. Maar wat je niet kwijtraakt, hoef je in elk geval niet te vervangen. Daarom adviseer ik als leidinggever je waardering uit te spreken naar de securitymedewerkers over de zaken die wèl goed gaan. De 64.000 poorten op de firewall die wel gesloten zijn. De 99% van de servers die wel zijn gepatcht op de woensdag na de maandelijkse Patch Tuesday van Microsoft. De spamberichten (98% ervan) die wel worden tegengehouden meteen aan de mailpoort en die niet in een mailbox van een medewerker terechtkomen. En dus bij het aansturen en 'motiveren' niet alleen te focussen op de keren dat het fout gaat. Als er een hacker op Lionel Messi-niveau aan komt zetten, gewapend met een SMB-exploit gemaakt door - naar verluid, er is nog niets bewezen - de Amerikaanse NSA en verder versterkt en aangepast door - ook weer naar verluid - de Russen, staan de meeste verdedigers in eerste instantie even machteloos. En je kan je nu eenmaal pas verdedigen nadat ze je hebben aangevallen.
Maar securitymedewerkers zijn professionals die gewoon graag hun werk goed doen. Een spits die een wedstrijd lang niet heeft gescoord, weet dat zelf ook wel. En een verdediger die een fout, vergissing, omissie, stommiteit (enzovoort) heeft gemaakt, weet dat zelf óók. Gun daarom securityprofessionals de tijd de 'fout' te lokaliseren, deze te verwerken, ervan en erover te leren (Google is your friend, ook in deze!) en daarna hun gedrag en werkwijze verder te optimaliseren. Daar worden we aan de verdedigende kant allemaal beter van. Want cybercriminelen zien ons van security als de Italianen in de uitspraak van Johan Cruijff: "De Italianen kunnen niet van je winnen, maar je kan wel van ze verliezen".

Italiaanse verdediging

En dat kwam, zo leerde ik in dat Italiaanse restaurant met behulp van vier flesjes Peroni-bier, doordat ze zo bedreven waren in 'catenaccio' in hun verdediging. De lege flesjes werden op een rij op tafel gezet. Dat was de Italiaanse verdediging. Dat begreep ik als leek zelfs nog wel. En als securityman herkende ik daarin natuurlijk de mij bekende functies en teams.

Integriteit

Er was een man of team voor identity & access management. De mannen en vrouwen die bepalen wie er toegang tot de systemen en applicaties krijgen en bij welke personen die rechten moeten worden ingetrokken of gewijzigd. En tot welke systemen ze precies toegang krijgen en wat ze in die systemen vervolgens mogen doen. Niet heel sexy, maar wel essentieel voor het bewaken van integriteit en vertrouwelijkheid van in die systemen opgeslagen informatie.
Daarnaast een team van testers, die alle nieuwe systemen, websites en mobiele apps stevig onder handen nemen voordat ze 'in productie' gaan. Let op: tijdens die wedstrijd was er nog geen continuous deployment. Het team van testers onderwerpen bovendien de bestaande systemen periodiek ook aan een inspectie met daarbij de testafdeling met al hun verschillende kleuren hoedjes en petjes (rood, blauw, zwart, wit, grijs), die toen nog helemaal niet bestond. Wel sexy, ook essentieel, maar helaas niet altijd in dank ontvangen door de onderzochte partij.

In het volgende flesje herkende ik het team dat compliance checks en monitoring doet, om bijvoorbeeld te zien of medewerkers toch via proxies, zoals Google Translate, verboden websites bezoeken. En dat ze geen onversleutelde USB-sticks of externe harde schijven aansluiten op het netwerk en daar bedrijfsdata op zetten, wat bij verlies of diefstal van die kleine of grote schijf tot een AVG-incident of zelfs boete kan leiden. Dit team zorgt als onderdeel van de onderling nauw samenwerkende verdediging ook voor het aanbrengen van de security patches op alle extern verworven software. Niet sexy, maar wel essentieel om onnodige securityfouten met betrekking tot beschikbaarheid, integriteit en soms vertrouwelijkheid te vermijden.

Robert Metsemakers is als ervaren IT auditor en informatiebeveiliging expert beschikbaar voor security advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.

Drie functies die elke security-afdeling wel heeft, lijkt mij. Hoeveel mensen je daarvoor nodig hebt, vraagt u dan? Nou, als je 100 personeelsleden hebt waarvan één zich fulltime bezighoudt met security, kom je uit op 1 per honderd (of 'per cent', zoals de Romeinen zeiden). Eén procent dus. Heb je bijvoorbeeld 15.000 medewerkers, waarvan er 30 werken op de afdeling security, kom je op twee per duizend. Dat is dus 0,2 procent van het totale personeelsbudget. Dertig klinkt voor mij veel, maar 0,2 procent niet.

Koffie

Als je die 15.000 medewerkers elke werkdag (225) vier koppen koffie of thee geeft (0,25 euro per stuk, dat is inclusief koffie, thee, water, elektra, het onderhoudscontract op de koffiemachine, melk, suiker, kartonnen of plastic beker), kost dat 3.375.000 euro per jaar. Als ze bekers en suiker meenemen voor gebruik tijdens hun vakantie, als er een bedrijfslogo op de bekers komt, of als medewerkers bij elke vergadering op een dag (staand) een beker pakken, dan wordt het duurder. En zeker als je als hippe startup company of Google de koffie door een echte 'barista' (Italiaans) laat bereiden. Of je telt de gederfde arbeidsuren mee voor het opnemen van de bestellingen, het tappen van alle koffie en thee, en het rondbrengen ervan op de afdeling. Ook al is het stimulerend voor de teamgeest en onderlinge collegialiteit, je hebt ook nog heb je ook nog van die dure dienbladen nodig!

In het algemeen lijkt het me in dit moderne, digitale tijdperk redelijk om het bedrag dat je aan koffie uitgeeft voor je medewerkers ook als minimumbedrag te investeren in security. Een kleine zelfstandige, zoals een schoenpoetser, paaldanseres, gaslantaarnaansteker of stadsomroeper heeft een baan met een lage informatie-intensiviteit. Er hoeft dus inderdaad minder aan informatiebeveiliging te worden uitgeven dan in een digitaal getransformeerde organisatie waar informatie zowel grondstof, halffabricaat als eindproduct is. Maar 225 euro per jaar is bijna iedereen wel kwijt. Voor een paar virusscanners op tablet, laptop en smartphone, een backup-apparaat, een USB-powerbank om ook bij een lege mobiele telefoon toch de DigiD-code als tweede factor via SMS te kunnen ontvangen en zo te kunnen aanloggen op een belangrijke website. En de uren die je jaarlijks moet besteden om de gewijzigde privacyreglementen van social media providers te bestuderen, kun je wat mij betreft ook meerekenen als 'aan security besteed'.

Juist toen ik me zat af te vragen wat het vierde flesje was, kwam de restauranteigenaar aan ons tafeltje staan. Hij transformeerde twee stukjes stokbrood in doelpalen en schoof het vierde flesje daartussen, als een keeper. Na het bekijken van de wedstrijd begreep ik dat het de Italianen er vooral om ging geen doelpunt tegen te krijgen en dat daarvoor de bal gestopt moest worden tijdens elke aanval. En wanneer dat tegenhouden niet lukte door de bal bruut (Brutus – ook een Italiaan) of listig (Machiavelli van 'De Vorst' - een van de oudste managementboeken - was behalve diplomaat, politiek filosoof, militair strateeg, historicus, dichter, toneelschrijver en humanist ook Italiaan) af te pakken, dat dan in elk geval de aanvaller gestopt moest worden. Daarbij werd een flinke overtreding niet geschuwd. Want als de afweging is: óf een tegendoelpunt krijgen en de wedstrijd verliezen en daarmee de winnaarsbonus voor alle spelers en trainer kwijtraken en op langere termijn ook reclame- en merchandisingrechten en de opbrengsten uit verkoop van losse toegangskaarten en jaarabonnementen, óf de situatie dat één verdediger één keer de volgende wedstrijd niet mee mag doen, maar daarvoor toch betaald krijgt…

DDoS-aanval

Ik kon me met die uitleg wel voorstellen dat die keuze meestal in het nadeel van de enkel- of kruisbanden van de betreffende aanvaller werd gemaakt. Of door héél hard aan zijn truitje te trekken terwijl hij probeert de bal te koppen.
Begrijp me wel: securitymedewerkers hoeven voor mij niet per se (Latijn!) zo meedogenloos op de man te spelen, maar hard ingrijpen om bijvoorbeeld een grote DDoS-aanval snel te stoppen, is soms wel noodzakelijk. De website uit de lucht halen om een essentiële patch aan te brengen, de toegang tot de centrale server die software deployed uitzetten als ransomware elders op het netwerk wordt gevonden en dat soort maatregelen. Maar hoe bekwaam je ook verdedigt, het gaat toch incidenteel weleens fout, legde de eigenaar uit. En die betreurenswaardige situaties, waar een aanvaller de eerste beveiligingslinie doorbreekt, worden dan door de doelman geblokkeerd.

Goed, dat was dus het Security Incident Response Team - om auteursrechtelijke reden ook vaak 'SOC' genoemd. Het zijn in elk geval de groep mannen en vrouwen die in actie komen bij grote security-incidenten en die daarna pas naar huis gaan om te slapen als de acute problemen in de operatie voldoende zijn opgelost.
Net toen ik dacht het hele systeem te begrijpen, plaatste

Inmiddels zijn sinds die voetbalwedstrijd vele jaren verstreken en wordt catenaccio in zijn pure vorm weinig meer toegepast

de eigenaar zijn eigen, inmiddels ook lege, flesje Birra Moretti op de tafel en bleef dat over de tafel schuiven tussen de vier Peroni-flesjes door. Hij vertelde dat het Italiaanse woord 'catenaccio' deurgrendel betekent en dat het voetbalsysteem met dezelfde naam was beïnvloed door het 'verrou' (dat is Frans voor 'deurgrendel') systeem uitgevonden door de Oostenrijkse coach Karl Rappan toen hij in de jaren '30 en '40 het, voor mij enigszins verwarrend, Zwitserse voetbalteam coachte. Hij gebruikte een extreem defensief ingestelde speler, die net voor de keeper was gepositioneerd: de verrouilleur. Ook wel 'bezem' genoemd, omdat hij de taak had om alle, toch nog door de verdediging gekomen, ballen op te vangen. In het Nederlands werd die speler ook wel laatste man genoemd, zei hij nog. Het leek mij, als voetballeek, dat juist de keeper die functie had, maar ik knikte hier instemmend. De restauranteigenaar had mij namelijk bij een eerder bezoek al gezegd: "Keepa calm? I cannota keepa calm, I am Italian!"

Deze speler werd later ook wel 'libero' genoemd en zijn rol was het oppikken van verloren ballen in de breedte van het veld en het eventueel helpen met dubbele mandekking, bij erg sterke opponenten. Een andere innovatie in de jaren '50 in het catenaccio was de snelle counteraanval, vooral door lange ballen naar voren vanuit de verdediging. Maar ik dwaal hier – voor het eerst in mijn leven – af.

Terughacken

De verdedigingslinie bestond dus uit drie man en hield zich bezig met in voetbaltermen een zeer strikte mandekking, dus elke verdediger zijn eigen aanvaller. In securitytermen is dat een strikte functionele scheiding: de testers doen geen IAM, de autorisatiebeheerders doen geen pentesting, de securitypatchers zitten niet in het redteam. Ieder team heeft zijn eigen specialisme en dat werkt door de onderlinge samenwerking. Als voetbalsysteem richt catenaccio zich vooral op een goed georganiseerde en effectieve verdediging, die de aanvallen van de opponenten moet neutraliseren en kansen bij de tegenpartij om doelpunten te maken moet voorkomen. Er is echter ook een aanvallend aspect en sommige vleugelverdedigers scoren net zoveel als een aanvaller. Maar securitymedewerkers vallen niet aan, zoals ik al aangaf. Behalve misschien als ze bij een veiligheidsdienst of law enforcement agency werken en wettelijk gezien mogen 'terughacken'.

De liberofunctie kun je op een security-afdeling invullen met een team mobiele 'probleemoplossers', die afwisselend op verschillende plaatsen waar nodig de security van een organisatie versterken. De Duitsers noemen deze speler trouwens 'Ausputzer', die rugdekking geeft aan de verdedigers (als een soort 'security van de security'). Dat klinkt voor mij beter dan 'bezem' of 'slingerback', mocht u beste lezer hiervoor nog in alle haast een nieuwe vacaturetekst gaan opstellen. Consultant dekt de lading niet helemaal, want behalve raad wordt er af en toe van de raadgever ook daad verwacht. Omdat deze personen naast hun interne samenwerking ook regelmatig extern afstemmen en verbinden met branchegenoten, overheid (NCSC), politie en securityleveranciers vind ik 'liaison officer' (verbindingsofficier) wel een mooie functienaam.

Succesvolle defensie

Inmiddels zijn sinds die voetbalwedstrijd vele jaren verstreken en wordt catenaccio in zijn pure vorm weinig meer toegepast. Buiten Italië is catenaccio een scheldwoord geworden voor saai, negatief voetbal. Wanneer een Italiaans voetbalteam echter een succesvolle defensie, met welk systeem dan ook, laat zien in een wedstrijd zijn de dames en heren van de schrijvende pers er als de kippen bij (om maar eens twee clichés in één zin te gebruiken), om te reppen van 'de terugkeer van het Italiaanse catenaccio'. Dat is dan strikt genomen onjuist geformuleerd, want het is eerder 'zona mista' - dus met zonale dekking in plaats van mandekking - of een opvolger daarvan. Maar dit taalgebruik geeft wel aan dat catenaccio een synoniem is geworden voor een succesvolle defensietactiek, die geen of slechts zeer weinig ballen doorlaat. En dat is iets waar we als securityspecialisten toch allemaal naar streven!

RISK PARALYSIS BY ANALYSIS

Onze CEO heeft mij gevraagd om, samen met een collega, de certificering volgens de normen ISO27001 & NEN7510 te realiseren voor onze organisatie. Ik werk al meer dan 11 jaar bij dit mooie bedrijf. We verbinden mensen en systemen in de zorg. Ik kijk naar het whiteboard. Het staat volgeschreven met mogelijke bedreigingen op de infrastructuur die 'Ops' in beheer heeft en het is niet het eerste bord vol. Op mijn iPhone staan nog 4 scans van volle whiteboards. Ik ken veel collega's die erg creatief zijn in het bedenken van nieuwe risico's en beren op de weg, maar Bert is een klasse apart. Bert en Jan zijn net de kamer uit, het pak koekjes is leeg.

"Zo komen we er niet", verzucht ik onhoorbaar tegen het bord. Een moment later een pingeltje. Mail van Bert:

"Dré!

Geweldig man dat iemand zich nu eens inzet om alle risico's in kaart te brengen waar we dagelijks mee worstelen hier. We zagen het eerst niet zo zitten maar Jan en ik zijn superenthousiast! We blokken voortaan elke woensdag om nieuwe risico's te bedenken. Lang leve de ISO!

Bert.

- Sent from my iPhone - "

"Aaah! Zo komen we er echt niet", roep ik nu hardop. "Bedankt voor het meedenken!"

Verwondering

Wat is het toch met mijn collega's? Niet alleen Bert en Jan zijn meesters in het bedenken van gevaren en bedreigingen. Het lijkt wel een standaardeigenschap van IT'ers. De intelligentie en creativiteit van de mensen, gecombineerd met de complexiteit van de materie, geeft een reële kans dat we meer risico's bedenken dan dat we kunnen behandelen in het certificeringstraject. Dit is de 5e sessie met steeds een andere afdeling en inmiddels staat de teller in de sheet met geïnventariseerde risico's op ruim 200. Als het aan Bert en Jan ligt, gaan we de 1.000 wel halen.

Ik denk erover mijn opdracht terug te geven aan de CEO, sluit mijn laptop en ga naar huis. Het is druk op de snelweg en ik rijd binnendoor om de file te vermijden. Ik denk: mensen zijn zo goed in het bedenken van risico's, met als gevolg dat certificeringstrajecten verlamd raken. Hoe kan dit?

Waarom een risicoanalyse?

Terug naar de basis. Waarom doen we het en hoe werkt een risicoanalyse?

Een risicoanalyse is een logisch onderdeel van informatiebeveiliging. Verplicht als je de Praktijkgids Code voor Informatiebeveiliging aanhoudt, stap 3 "U voert een risicoanalyse uit" (oud, 2002, p40). Ook paragraaf 5.4 geeft aan dat een risicoanalyse noodzakelijk is (oud, 2002, p82). De risicoanalyse valt onder het plangedeelte van de 'Plan, Do, Check, Act (PCDA)' repeat cycle van Deming (figuur 1). Als gevolg van de eisen van externe partijen en de wetgeving waaraan ons bedrijf gehouden is, dient een risicoanalyse uitgevoerd te worden (oud, 2002, p73). Ook de normen waarop we willen certificeren, vereisen dit zoals de NEN7510 (NEN, 2011) en de ISO27001 (NEN-ISO, 2013).

Figuur 1- Deming Cycle.

De risicoanalyse helpt een organisatie met focussen op datgene wat belangrijk is. De planfase gebruiken we om vast te stellen wat we gaan doen en hoe we dit gaan doen. Op basis van de literatuur, externe belangen, wet- en regelgeving en de aard van ons bedrijf, stel ik vast dat een risicoanalyse een verplicht onderdeel is.

Hoe voeren we een risicoanalyse uit?

We komen niet onder een risicoanalyse uit, maar hoe stellen we die op? In de praktijkgids lezen we een formule die in veel publicaties terugkomt: "Voor een bepaalde bedreiging geldt: risico = kans x schade" (oud, 2002, p76).

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

We hebben voor deze methode gekozen. Dit geeft geen gekwantificeerd risico zoals bij het hanteren van een 'Single Loss Expectancy' (Whitman & Mattord, 2014, p325), maar het helpt ons de risico's ten opzichte van elkaar te wegen en zo de prioriteit te bepalen.

In de praktijk hebben we sessies belegd met betrokken afdelingen en zijn we risico's gaan inventariseren. Daarna hebben we op verschillende assen de schade ingeschaald en de kans op optreden vastgesteld. Het komt uiteindelijk uit op Low, Medium, High of Extreme. Dit geeft voor de verzameling risico's een zogenaamde Risk Matrix (zie figuur 2).

Deze risk matrix is een weergave van het door ons gekozen registratietool. De risico's administreren en controleren we in JIRA van de leverancier Atlassian. Prettig is dat deze tooling dicht bij de engineers ligt en past bij onze werkprocessen.

Figuur 2 - Screenshot Risk Matrix, original exposure (Bron: ISMS) .

Wat veroorzaakt die verlamming?

Het opstellen van de risicoanalyse lijkt een prima en heldere activiteit. Mijn introductie laat zien dat de praktijk weerbarstiger is. Waar ligt dat nu aan?

Uitstelgedrag

Ik zal ongeveer 19 jaar geweest zijn en woonde in Den Haag op kamers voor mijn studie Informatica aan de Haagse Hogeschool. Gewoonlijk stond de afwas 8 hoog in de keuken (en niet alleen daar). Dit vervelende klusje had zelden prioriteit. Tot de tentamenweek! Ineens was afwassen (en stofzuigen) van wereldbelang. Alles om maar niet te hoeven leren.

Het 'vluchten' in de oplevering van een complete risicoanalyse zouden we kunnen zien als een vorm van uitstelgedrag. Immers, zolang we bezig zijn met het inventariseren van alle risico's is de uiteindelijke prioriteit nog onduidelijk en kunnen we niet gaan beginnen met het aanpakken ervan. Procrastination is "to voluntarily delay an intended course of action despite expecting to be worse off for the delay" (Steel, 2007). Let wel, het gaat hierbij niet om het uitstelgedrag van een individu maar van een complete werkgroep of afdeling.

Beloning

Het benoemen van meer of grotere risico's dan je collega heeft een zekere mate van voldoening of beloning in zich (gratification). Je moet er creatief voor zijn, kennis van zaken hebben en het benoemen ervan 'voelt' alsof je positief hebt bijgedragen aan de staat van informatiebeveiliging. Maar het benoemen, inschalen en opnemen in het risicoregister is niet hetzelfde als een afgehandeld of behandeld risico. Immers, er heeft nog geen mitigatie, acceptatie, vermijding of overdacht van het risico plaatsgevonden. Dit zijn de 4 algemeen geaccepteerde strategieën (Lacey, 2009, p125-126). Een teamlid kan fanatiek bijdragen aan de risicoanalyse en daar veel zingeving uit halen. Het is belangrijk om hem of haar ook te motiveren om eigenaarschap aan te gaan voor benoemde risico's.

Informatiebeveiliging

In de praktijkgids wordt duidelijk gesteld dat informatiebeveiliging geen project is. Het kent geen eindig karakter (oud, 2002, p37). Toch wordt een projectmatige aanpak aangeraden. De valkuil, mijns inziens, is dat een verplichte risicoanalyse als een compleet op te leveren deliverable wordt gezien zoals gebruikelijk bij een Princell aanpak ("PRINCE2 Methodology", z.j.). Er is een intrinsieke drijfveer om volledig of uitputtend te zijn bij het opstellen van een risicoanalyse. Maar de vraag is: kan je een uitputtende risicoanalyse maken?

Nee, gelet op het boogde doel van Risk Management is een uitputtende risicoanalyse onmogelijk:

"… Well, the goal of a formal risk management program is to employ a governance framework to achieve a known and consistent state – a state that can be measured, discussed and continuously improved in an organized manner over time …"
(Whitman & Mattord, 2014, p. 330)

We moeten het opstellen van een risicoprofiel meer zien als een continue activiteit. Het risicoprofiel zelf is een

momentopname. Dit wordt ook gestaafd door de stelling dat kwetsbaarheden toenemen ondanks onze inspanningen om ze te dichten (Lacey, 2009, p124).

Analysis Paralysis

Het is mijn overtuiging dat er sprake kan zijn van Risk Analysis Paralysis. Door te 'over'-analyseren ontstaat er een situatie waarbij er geen waarde meer wordt bijgedragen aan de verlaging van het totale risico. Wat verstaan we in deze context onder Analysis Paralysis?

"…Analysis Paralysis is based on the premise that by delaying decisions or committing to a particular direction, there's more time to gather new information, conduct analysis and present recommendations to the business. This premise only holds true for a while though. At some point, the law of diminishing returns sets in – the extra information collected and the extra time devoted to analysis no longer add any significant value to the project…" ("Managing Analysis Paralysis", z.j.)

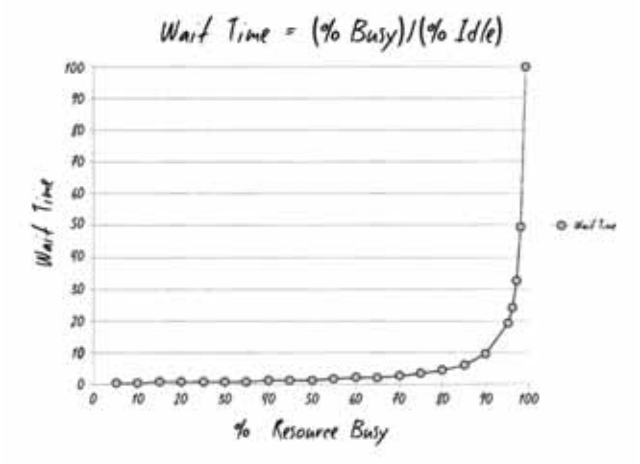
Er wordt geen begin gemaakt en we voltooien om die reden nooit de eerste slag van de PDCA-cyclus. Ik zie in de Lean en Agile wereld vaak de toepasselijke slogan "Stop starting, start finishing" terugkomen (Vashishtha, 2014).

(Personal) Politics

Het opstellen van een risicoanalyse geeft collega's ook een podium. Het kan een manier zijn om het belang van de eigen processen, code, machines of afdeling te overdrijven. Door risico's in scope van de eigen afdeling een zware impact en grote waarschijnlijkheid toe te dichten kunnen extra resources vanuit het management voor jou beschikbaar komen (Lacey, 2009, p117). Door risico's in te schalen volgens een vastgesteld principe worden onderlinge verhoudingen ineens inzichtelijk. Daar zit mogelijk een belangenverstrengeling als e om budget gevochten moet worden.

Work In Progress

Work In Progress (W.I.P.) is de hoeveelheid 'onderhanden werk'. Een gevolg van een niet te stoppen risicoanalyse is een te grote W.I.P., dit leidt tot een ogenschijnlijk niet te behappen berg aan risico's. De uiteindelijke voortgang neemt af naar 0. Met andere woorden: de wachttijd op werk dat gereed komt, loopt oneindig op (Kim, Behr & Spafford, 2013, p235).



Figuur 3 - Wachttijd loopt op naar oneindig (Kim, Behr & Spafford, 2013, p235).

Risico's staan voor werk, die risico's waren er altijd al, maar door ze te benoemen wordt het een niet te behappen hoeveelheid werk. Dat kan verlammend zijn, ook al schaal je die risico's correct in. Denk eens in, na inventarisatie heb je 15 risico's die vallen in de categorie 'high impact – high probability'. Een correcte respons vanuit de organisatie zou dan zijn: "Avoid – take immediate preventive action" (Lacey, 2009, p117). Mogelijk heeft onze organisatie de middelen helemaal niet om die stappen nu te zetten, dat kan onrust geven. Uiteraard speelt de mate van Risk Appetite hier ook een rol in (Whitman & Mattord, 2014, p. 318). Door als onderneming een bepaalde risico tolerantie te hebben kunnen we zaken (voor nu) accepteren. Vaak zien we dan een formeel getekende acceptatie door de CEO of Board.

Conclusie

Mijn verwondering waarom mensen zo goed zijn in het bedenken van risico's zodat certificeringstrajecten verlamt raken, was het vertrekpunt. Door met collega's te praten, onderzoek te doen, veel te lezen en vanuit mijn eigen ervaring met verschillende certificeringstrajecten zie ik een aantal oorzaken:

- uitstelgedrag (procrastination), zolang we nog nieuwe risico's bedenken is het aanpakken ervan nog niet aan de orde;
- beloning of voldoening, elk nieuwbenoemd risico voelt als een positieve bijdrage en als voortgang;
- informatiebeveiliging is geen project, de complete risicoanalyse wordt een 'deliverable' op zich in plaats

van een startpunt voor discussie en continue verbetering;
- (personal) politics: door het moment of je podium te pakken kunnen jouw belangen meer gewicht krijgen. De inventarisatie van risico's wordt een machtsmiddel;
- Work in Progress (W.I.P.): de aandacht van het team wordt verdeeld en doorlooptijden, voor het behandelen van de risico's, convergeren naar oneindig.

Mijn conclusie is dat het blijven hangen in een risicoanalyse, een reëel gevaar is voor een organisatie. Daardoor begint men niet met continue verbeteren. Niets menselijks is een organisatie vreemd.

Aanbeveling

Ik zie een duidelijke analogie tussen 'Work in Progress' en 'Risks in Progress'. De oplossing voor W.I.P. is: verlaag het inkomend werk, scherm je mensen die de bottleneck vormen af en zorg dat er weer een flow ontstaat waarbij werk van 'Todo' naar 'Done' gaat (Kim, Behr & Spafford, 2013).

Net zoals in een DevOps-team zal je niet alles in 1 sprint kunnen oplossen. Het team kijkt wat het aankan (sprintplanning) en de rest gaat op de backlog. Na elke sprint releasen we een nieuwe variant van de software (Schwaber & Sutherland, 2016).

Bij risico's is het net zo. Maak een sprintplanning van bijvoorbeeld 1 kwartaal. Zet de behandeling van een aantal risico's op die sprintplanning. Dat kunnen in ons geval risico's uit de categorie 'Extreme' zijn. Mogelijk zijn er ook wel een aantal quick wins in de categorie 'Medium' aan te pakken die de organisatie nu veel pijn doen. Na elk kwartaal releasen we, als het ware, een nieuwe versie van ons bedrijf. Een versie die robuuster is met een lager risicoprofiel dat beter past bij de risk appetite.

Borg dit in je ISMS! Als security officer kun je jezelf zien als de product owner van het gewenste risicoprofiel van je bedrijf. Hoe groot is de risk appetite? Met welk risidual risk kan een organisatie en haar stake holders leven? Welke risico's zien we? Welke maatregelen nemen we om het risicoprofiel te verlagen? En hoe blijven we in control van die risico's? Dat lijkt heel veel een Scrum- of Agile-werkwijze.

Plan in elke iteratie ook tijd vrij om onderhoud te plegen (interne audits en het oppakken van verbeterpunten) en voor incidenten (niet eerder beschreven risico's of plotseling optredende incidenten).

Het grootste punt is: blijf niet hangen in de perfecte risicoanalyse. Zie het als een momentopname van je risicoprofiel en zorg dat je het wiel van continue verbeteren in gang zet.

Referenties

- Deming Cycle (Illustratie). (z.j.). Geraadpleegd op 25 september 2017, van https://www.pdcacyclus.nl/william-edwards-deming/deming-cirkel/
- Kim, G., Behr, K., & Spafford, G. (2013). The Phoenix Project. Portland, Oregon, USA: IT Revolution Press.
- Lacey, D. (2009). Managing the Human Factor in Information Security. Chichester, England: Wiley.
- Managing Analysis Paralysis. (z.j.). Geraadpleegd op 25 september 2017, van https://businessanalystlearnings.com/blog/2014/2/10/managing-analysis-paralysis
- NEN-ISO. (2013). NEN-ISO/IEC 27001 (en) Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013,IDT) (2e ed.). Delft, Nederland: Nederlands Normalisatie-instituut.
- NEN. (2011). NEN 7510(nl) -- Medische informatica - Informatiebeveiliging in de zorg -- Health Informatics - Information security management in healthcare. Delft, Nederland: Nederlands Normalisatie-instituut.
- Oud, E. (2002). Praktijkgids Code voor informatiebeveiliging. Amsterdam, Nederland: Academic Service.
- PRINCE2 Methodology. (z.j.). Geraadpleegd op 25 september 2017, van https://www.prince2.com/eur/prince2-methodology
- Schwaber, K., & Sutherland, J. (2016, 1 juli). The Scrum Guide. Geraadpleegd van http://www.scrumguides.org/scrum-guide.html
  Steel, P. (2007). The Nature of Procrastination: A Meta-Analytic and Theoretical Review of Quintessential Self-Regulatory Failure.
- Psychological Bulletin, 133(1), 65-94.
- Vashishtha, S. (2014, 28 maart). Agile Thinking : Stop Starting, Start Finishing. Geraadpleegd van http://www.agilebuddha.com/agile/agile-thinking-stop-starting-start-finishing/
- Whitman, M., & Mattord, H. (2014). Management Of Information Security (4e ed.). Stamford, USA: Cengage Learning.

ZERO TRUSTED

It's the beginning of 2019 and the new buzz-ware from the security solution vendor community is 'zero trust'. What do we think that means? It must be important because they're all rushing to tell us how their products and services support this new initiative in security architecture. It's being presented as the new holy grail, something never before imagined, that will solve all your corporate security problems. Google has apparently implemented the approach in a form named BeyondCorp. This shifts the access control decisions away from the corporate perimeter and repositions them close to the resources being protected.

What? You mean you are still doing that 'perimeter security' thing? Didn't you ever come across the Jericho Forum commandments on deperimeterisation for the enterprise? And now you're buying into this latest fad which is just the same thing served up in smaller slices. The clue is in the word 'microperimeters'.

Whilst all vendors are climbing aboard this zero-trust bandwagon, the Attributer believes it is fair to single out Forrester Research as the main culprit, since they claim that one of their research analysts (John Kindevag) invented the zero-trust concept in 2010. We can assume this claim to be correct (trusted) because no-one is arguing with it.

Wow! Forrester! It must be good. Do we understand what it means? Of course we do.

It is claimed that Zero Trust is a data-centric architecture that puts micro-perimeters around specific data or resources so that more-granular access control policy rules can be enforced and implemented. This is the first problem that The Attributer has with this model of utopia. Data centric security architecture would be embedding security in the data structures. This is just another version of network-centric security architecture – one where you carve the network up into smaller segments to use it as the means to control access to your data.

This is a fundamentally flawed architectural approach. The job of the network is to provide transport services for protocol data units to be moved from one place to another, in sequence order and with certain performance targets to be met. It is NOT the job of the network to protect application data from theft, corruption, or fabrication. We are dealing with the vendor community once again trying to sell us network-embedded security products for architectural approaches that we threw out decades ago. They were trying to sell us this nonsense back in the 1990s and they are still trying to sell it now.

Let's be clear. The only thing that network security architecture should be protecting is the network itself and its ability to meet its service level agreements with users and applications that make use of its transport services.

When we dig a little deeper, we discover that the term 'zero trust' refers to 'zero trust networking', in which you never trust the network, or anything connected to the network. It takes the principle of 'trust but verify' that was popularised by President Reagan in the 1980s in his dealing with the Soviet Union over nuclear disarmament and twists it round into the phrase 'never trust, always verify'. One of the basic concepts of zero trust is that trust is binary – trusted or untrusted, black or white, and that somehow this trust is controlled by technical components in the architecture.

All of this is nonsense. Without trust, society and business could never operate. Trust is a human concept, not a technology one. We trust different people for different things and the levels of trust are measured in microlevels.

This attempt to sell us pre-packaged 'architecture' in the form of more technical products shows just how immature the security architecture industry really is. Technology, technology and more technology. If you stack your business full of technology, then you're bound to solve the problem – eventually.

Quite frankly The Attributer finds this approach to be insulting to the intelligence of the security architecture community – those who are SABSA educated and certified and who recognise that first you must model the business before you can start selecting security products. One day the vendor community will wake up to the need to supply components that really do populate a business-driven security architecture model. Until then they will continue to sell 'solutions' that have virtually no merit in solving real business problems.

How much should we trust the vendors to help us solve our security problems? Zero. They got that bit right.

The Attributer

DATALEKKEN NAAR EN VIA FACEBOOK

Facebook had het niet makkelijk het afgelopen jaar. Medio 2018 kwam de organisatie in een kwaad daglicht te staan, omdat het onterecht persoonlijke data deelt met derden. En eind 2018 waarschuwde Privacy International dat vele Android-applicaties automatisch data over hun gebruikers met Facebook delen. Facebook verrijkt met deze data vervolgens haar kennis over individuen, ongeacht of het Facebookgebruikers betreft en zonder te weten of de gebruikers hiervoor toestemming aan de eigenaar van de app hebben gegeven.

Voor velen is hier nauwelijks nog sprake van nieuws. En Facebook? Die organisatie verschuift de verantwoordelijkheid naar ons: de organisaties die hun middelen gebruiken. De organisatie verwerkt immers enkel data die wij ze aanbieden. Volgens Facebook ligt de verantwoordelijkheid daarom primair bij haar klanten en gebruikers. Maar is dat wel zo? En als dit het geval is: hoe zouden wij hier als organisaties dan mee om moeten gaan? En hoe kunnen security en privacy officers vanuit hun verantwoordelijkheid hun organisatie helpen om ook op dit onderdeel data op een passende wijze te beschermen?

Tom Bakker

Ik vond het een ingewikkeld rapport van Privacy International. Centraal in deze kwestie is 'Facebook SDK for Android'. Deze kit integreert apps met het Facebookplatform om gerichte advertenties te kunnen tonen. De SDK geeft o.a. support voor logins met Facebookauthenticatie, lezen/schrijven naar Facebooks API's. Dat persoonsgegevens dan verzameld worden was te verwachten. Maar dat deze datadeling standaard staat ingesteld, óók als de eindgebruiker niet inlogt met Facebook en/of geen Facebookaccount heeft, is een kwalijke zaak. Het is niet transparant en er wordt ook niet om toestemming gevraagd. Er blijkt wel een Opt-out mogelijkheid voor de bouwers van de app te zijn maar die blijkt moeilijk te vinden en niets voor te stellen/niet te werken. Gegevens worden dan wel aangeleverd door de gebruiker zelf, maar die weet niet wat er mee gedaan wordt. Het blijkt dat ook veel appontwikkelaars er niet van op de hoogte zijn. Volgens Facebook zijn ze echter wel primair verantwoordelijk. Het lijkt mij dat bedrijven die apps


Maarten Hartsuijker


Tom Bakker


Fook Hwa Tan

ontwikkelen, maar geen gebruik meer moeten maken van de SDK-kit. Commercieel gezien voor sommige misschien geen optie vanwege de gerichte advertenties die getoond moeten kunnen worden. Maar dat is een kwestie van keuzes en voldoen aan de wet. Daarnaast kunnen organisaties met Mobile Device Management eindgebruikers het zakelijk gebruik van gratis apps verbieden (hoewel niet duidelijk is of betaalde apps misschien ook lekken). Meer onderzoek is nodig.

Maarten Hartsuijker

Dat data het verdienmodel is van partijen als Facebook en Google weten we inmiddels allemaal. En dat deze partijen superkrachtige marketingtools hebben waar je als marketeer eigenlijk niet meer zonder wilt ook. Of het nu Customer matching of Custom Audiences heet: Facebook en Google helpen graag om te zorgen dat onze (toekomstige) klanten zo gericht mogelijk worden bereikt. En daar is data voor nodig die onder andere via SDK's als deze wordt vergaard. Zo helpen deze organisaties ons onder andere om overal op internet onze klanten en bezoekers via 'retargetting' te herinneren aan een eerdere interesse. Als ik marketeers spreek die mij advies vragen over de impact van het gebruik van een Facebookcomponent zoals Custom Audiences krijg ik steevast als eerste de opmerking: we verstrekken Facebook alleen de hashes van onze klantenlijst, dús het betreffen geen persoonsgegevens. Maar doordat Facebook van het merendeel van de hashes al weet wie het betreft, help je Facebook uiteraard met de verrijking van hun dataset. Afhankelijk van het type organisatie dat je bent (zorginstelling, kerk, homobar) zou je zelfs indirect bijzondere persoonsgegevens kunnen verstrekken. Ditzelfde is het geval op het moment dat je van SDK's of 'gratis' content delivery netwerken (CDN) gebruik maakt. Koppel je je website voor het inladen van fonts, open source libraries, of vertaaldiensten aan een CDN van Google, dan verstrek je Google informatie over elke bezoeker van jouw site. Security en privacy officers kunnen hun organisatie vanuit hun rol helpen om dit soort indirecte lekken van klant- en bezoekersdata tijdens het uitvoeren van PIA's en BIA's als risico te benoemen en bespreekbaar te maken. Zo raakt de organisatie bekend met de impact en alternatieven. Het inladen van data en scripts vanaf externe sites is bijvoorbeeld veelal niet noodzakelijk en het (over het algemeen zonder verwerkersovereenkomst) verstrekken van bezoekersgegevens is hier makkelijk te voorkomen door de betreffende scripts naar de eigen server te kopiëren. Het verstrekken van klantdata aan Google en Facebook kan voor organisaties ook minder aantrekkelijk zijn op het moment dat onduidelijk is of deze organisaties hiermee indirect ook de concurrent bedienen. Een impact analyse kan hier dan een aanleiding zijn om minder of andere data in te zetten voor een campagne of om te proberen privacy-afspraken aan te scherpen.

Fook Hwa Tan

Verantwoordelijkheid ligt bij de eigenaar, maar of het nou de AVG is of standaarden met betrekking tot informatiebeveiliging, ze wijzen erop dat verantwoordelijkheden juist belegd moeten worden. De 'eigenaar' van de data moet/mag zelf beslissen wat hij of zij vrijgeeft of geheimhoudt. Dat gezegd hebbende, merk ik in mijn jaren binnen verschillende organisaties en natuurlijk ook in mijn privéleven dat de 'eigenaar' vaak niet in staat is om zelf te beslissen. Veel mensen hebben geen of weinig kennis van informatiebeveiligings- of privacyrisico's. Met enige IT-kennis kom je er al snel achter dat er een hoop kwetsbaarheden bestaan in zaken die we dagelijks gebruiken, zoals onze mobiele telefoon, laptop, smartwatch en andere internet verbonden apparatuur. Deze kunnen mogelijk misbruikt worden, maar veel mensen zijn hier niet bekend mee en denken niets te kunnen verliezen. Binnen ons vakgebied zien we veel incidenten op cybersecurityvlak en vaak ook snel nieuwe kwetsbaarheden, maar dat geldt niet voor een groot deel van de bevolking. De groep mensen die wel meer kennis heeft van de gevaren van de digitale transformatie zijn echter vaak niet in staat om maatregelen te nemen om zichtzelf te beschermen. Hierdoor kunnen ze alleen kiezen om apparatuur of programmatuur wel of niet te gebruiken. Uiteindelijk is de gehele digitale transformatie bedoeld om ons werk en ons leven gemakkelijker te maken. Dat is vaak de reden waarom mensen technologie gebruiken. Neem ons betalingsverkeer: het kan contactloos, met mobiel of online. Het is toch erg makkelijk om dit allemaal digitaal te kunnen doen. Het is niet zoals vroeger, waar een cheque of overschrijvingskaart geschreven moest worden of alleen met contant geld een aankoop gedaan kan worden. Daarom is, ondanks het feit dat de verantwoordelijkheid bij de eigenaar (bij ons dus) ligt, het belangrijk dat overheid en organisaties deze gebruikers helpen. Deze eindgebruikers zijn immers onbekend met de risico's, onbekwaam om deze risico's te mitigeren en kiezen bewust of vaker onbewust voor gemak boven veiligheid. Het is daarom taak voor overheid en bedrijfsleven deze mensen bewuster te maken, maar nog belangrijker om een digitale omgeving te creëren, waar mensen in alle vrijheid en transparantie met elkaar om kunnen gaan! Hiertoe is in 2018 gelukkig al een begin gemaakt, waarbij meer dan 60 organisaties wereldwijd zich hebben toegewijd om gebruikers en klanten op cybersecuritygebied te beschermen. Dit is het Cybersecurity Tech Accord!

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
Patrick Dersjant
Nicole van Deursen
Rik van Dijk
Maarten Hartsuijker
Lilian Knippenberg
Hugo Leisink
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 2018 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

SAMBAL BIJ?

Voor mijn werk moet ik vaak reizen en nu de jaren meer en meer gaan tellen, neem ik vaak de luxe van een hotel. Het reizen wordt door de files en het drukke verkeer er niet leuker op en dan is het wel heel relaxed om de tijd te nemen, lekker uit te rusten en op te laden voor de volgende dag. Het is alleen jammer dat het zo gevaarlijk is. U zult dat misschien een beetje een wonderlijke opmerking vinden, maar ik denk dat mijn creditcardgegevens, mijn rekeninggegevens, adres en andere gegevens meerdere malen zijn gestolen bij het Marriott hotel. En ik ben niet de enige. Er schijnen nog 500 miljoen gasten bestolen te zijn. Ik zal het even voluit schrijven, want anders lees je er zo snel overheen: de gegevens van 500.000.000 mensen zijn gestolen. Een ongekend groot aantal en daarmee vallen de hacks waar ik in eerdere columns over schreef eigenlijk best wel mee. Ik noem de hack van het Mattiott hotel niet alleen omdat ik er persoonlijk mee te maken had, maar eigenlijk ook omdat onderzoekers hebben aangetoond dat het misschien wel Chinese hackers geweest zijn. Misschien hoor, want het zou best kunnen zijn dat andere hackers zich voordoen als Chinese hackers en dat het helemaal geen Chinezen zijn. De Chinese overheid zou er achter zitten, maar zeker weten doen we het niet. Het zou alleen best kunnen.

Het bericht van de Marriott hack komt vlak na de arrestatie van een topvrouw van het Chinese telecom bedrijf Huawei. Huawei maakt behalve smartphones ook netwerkapparatuur. Eigenlijk moeten we het omdraaien: ze maken naast netwerkapparatuur ook telefoontjes. In de netwerkapparatuur zou misschien weleens spionagesoftware kunnen zitten waarmee de Chinese overheid de hele westerse wereld kan ontwrichten, want Huawei-apparatuur staat overal in de westerse wereld. We vermoeden dat, want we hebben daar geen bewijzen voor. Er is dus niemand die het kan bewijzen en toch arresteren we de Chinese topvrouw. Een Belgische parlementariër heeft inmiddels het voorstel gedaan in het Belgische parlement om een verbod uit te vaardigen tegen de verkoop van deze apparatuur. Op grond waarvan? Omdat we vermoeden dat er weleens spionagesoftware in geplaatst zou kunnen zijn. Ben ik nou zo naïef of zijn de anderen zo dom? We moeten toch minimaal kunnen aantonen dat er foute software in zit? Dat hebben we toch ook gedaan bij de sjoemelsoftware in onze Volkswagen? Terwijl ik dit allemaal intyp, zie ik de Huawei van mijn zoon liggen en ik twijfel. Ik maak me zorgen, want hij ligt wel gewoon bij mij op het bureau. Zien ze mij aan de andere kant van de wereld nu achter een Mac zitten? Weten ze wat ik vandaag heb gedaan? Ik vermoed van niet, maar ik geef toe dat ik onzeker ben. Ik pak mijn eigen telefoon maar om even een maaltijd te bestellen bij Ni Hao, of zal ik Antonio bellen? Ik besluit het laatste te doen. Ik heb genoeg Chinees gehad vandaag.

Berry

Business Resilience Masterclass

Woerden | 21 maart, 28 maart, 4 april, 11 april, 18 april

Inclusief Master Slot Event in het Grand Kasteel Woerden

JOHAN BAKKER
CISSP - ISSAP - CPT

GERT KOGENHOP
(HON.) MBCI - FINANCE - AT

MICHIEL KUETHE
CRISISMANAGEMENT - AT

BRENNO DE WINTER
HACKER - BEVEILIGINGS- & PRIVACYEXPERT

Betrek het topmanagement bij de resilience van uw organisatie

De maatschappelijke ontwikkelingen vragen van de overheid en het bedrijfsleven een toenemende kennis op het gebied van Business Resilience.

Schrijf u nu in voor deze unieke Masterclass, waarin u in vier interactieve sessies ontdekt wat de combinatie van Information Security (IS), Business Continuity Management (BCM) en Crisis Management (CM) kan betekenen voor de resilience in uw organisatie.

Ter afsluiting vindt een Master Slot Event in het Grand Kasteel Woerden plaats, waarvoor u één of meerdere introducees mag uitnodigen.

Interesse in deze Masterclass? Neem een kijkje op onze website voor meer informatie of vraag de brochure aan.

Security Academy | www.securityacademy.nl
0348 40 80 61 | info@securityacademy.nl

SECURITY ACADEMY | SECO INSTITUTE