INFORMATIEBEVEILIGING
MAGAZINE

- Hoe je in 10 stappen een cybercrisisoefening organiseert
- Nederlandse partijen bouwen testomgeving voor Gaia-X clouddiensten
- Column: People, Process, Technology

JAARGANG 23 - 2023 - EDITIE 3

VERSTERK UW ISO/IEC 27001 MANAGEMENTSYSTEEM!

Wilt u zeker weten of uw organisatie klaar is voor certificering volgens ISO/IEC 27001? Doe de online DNV Self-Assessment en ontvang een rapportage in uw inbox. Of volg de Normkennis ISO/IEC 27001

Kent u de DNV Self-Assessment Suite al? Deze tool stelt u in staat te testen hoe goed u ISO/IEC 27001 kent en te beoordelen in hoeverre uw managementsysteem klaar is voor certificering. De evaluatie is op basis van puntenscores en laat zien waar er tekortkomingen bestaan en waar u verbeteringen kunt doorvoeren.

Stel een nulmeting op, stel kwantitatieve doelen vast voor een specifiek aandachtsgebied en meet regelmatig de geboekte vooruitgang. De Self-Assessment Suite biedt u in alle gevallen een gedetailleerd inzicht in uw kennis of prestaties en uw mate van beheersing.

Wilt u graag uw kennis vergroten over ISO/IEC ISO 27001? Volg dan de Normkennis ISO/IEC 27001 training! De trainer geeft u handige tips en voorbeelden uit de praktijk, zo leert u te kijken naar de norm, zoals een auditor dit doet.

Kijk voor meer informatie over de Self-Assessment Suite op dnv.nl/self-assessment of scan de QR-code als u wilt deelnemen aan de training.

DNV

Lessen voor de 21e eeuw

Chris de Vries

Een voordeel van het hoofredacteurschap is dat je soms een kleine voorsprong krijgt op anderen. Slimme mensen komen met slimme artikelen en voordat deze door Jan en alleman gevonden worden, zijn er auteurs die deze voor ons vinden.

Zo ook dit keer. Dimitri van Zantvliet schrijft een interessant artikel en gaat daarbij onder andere in op de paper *'Ethics of Decentralized Social Technologies (DST): lessons from …'*. De auteurs werken bij Harvard University & Microsoft Research. Dimitri adviseert ons het artikel te lezen en een snelle scan leerde mij dat hij gelijk heeft: leesbaar, toekomstgericht en op niveau. Een citaat: *'...improving coordination capacity and collective intelligence can contribute to our ability to tackle the major challenges that define not only this century, but the human condition as a whole.'* En niet alleen in dat artikel word je tot activiteit, zo niet eigen-ondernemerschap, opgeroepen. Op hogescholen en universiteiten wordt al langere tijd onderwezen medewerkers te stimuleren om in elke functie ondernemerschap te tonen. Wij kunnen de toekomst niet bouwen op basis van hiërarchie, maar eerder door een bottom-up benadering waarbij het topmanagement faciliteert in plaats van dirigeert. En dus roept André Beerten nogmaals op om op zijn artikelen te reageren, mee te denken en positief kritisch te zijn. *'Wat is dat met jullie, is de waarheid te pijnlijk of zijn jullie te lui om te reageren op mijn fouten en ongenuanceerde mening?'*, luidt zijn hartenkreet.
Meedenken en –doen wordt ook gepropageerd door ons bestuur en dat wordt uitstekend verwoord door Evert van Zanten in zijn bestuursblog in dit magazine.

Lex Borger breekt een lans voor de samenhang tussen: 'people, processes & technology' dat sterk doet denken aan de begrippen 'people, planet & profit'. Hij geeft een beeld van de versnelling in technologische ontwikkelingen op basis van geluids- & beelddragers en vat een en ander krachtig samen: *'Investeer in het gedegen bewustzijn van mensen en het implementeren van veilige processen. Maar houd ook in de gaten waar techniek zijn eigen gang lijkt te kunnen gaan, los van mensen en processen."*

Al met al een magazine vol interessante artikelen van betrokken auteurs die uitnodigen tot interactie en samenspraak. Laat deze kans niet liggen!

Chris

IN DIT NUMMER

Auteurs: Vincent van Dijk en Chris de Vries. Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Chris de Vries is redacteur van het IB Magazine en daarnaast eigenaar van De Vries *Impuls* Management, hij is bereikbaar via impuls@euronet.nl.

Hulpgids beveiliging voor het kleinbedrijf (deel 2)

In de vorige uitgave (1) hebben wij een beschrijving gegeven van het belang van het mkb en hoe deze ondernemers begeleid moeten/kunnen worden naar informatie- & ketenveiligheid. Daarbij zijn de eerste vragen en antwoorden gegeven. Ook zijn wij ingegaan op de eerste beschikbare 'tools' en bronnen van informatie.

Het eerste advies betrof de beeldvorming bij de mkb-ondernemer van wat cyberveiligheid inhoudt. Het tweede advies: inventariseer waarom hij/zij zich moet gaan bezighouden met cybersecurity, terwijl het derde advies het gebruik van beschikbare (gratis) gereedschappen aan de orde stelde, zoals onder andere de Cybersecurity Canvas, de CIS-controls en het 5-stappenplan van Patrick Bet-David.

Vincent, een vraag die vrijwel direct rijst is, zijn er ook gereedschappen die mij snel informeren over hoe de vlag bij mij als mkb'er erbij hangt, zonder dat ik eerst zelf binnen mijn bedrijf moet gaan analyseren? Per slot van rekening als mkb'er of als (z)zp 'er, heb ik al zo weinig tijd.

"Dan verwijs ik je naar de **D**igital **T**rust **C**enter (DTC) (2) website en start dan bij de vijf basisprincipes van veilig digitaal ondernemen. Onderaan die DTC-websitepagina

staat de Basisscan Cyberweerbaarheid. Duur: circa vijf minuten. Op basis van 25 stellingen over de vijf basisprincipes word je begeleid bij de status van jouw bedrijfsveiligheid. Let wel: de uitkomst is indicatief!
De vijf basisprincipes van het DTC zijn:
1. inventariseer kwetsbaarheden;
2. kies veilige instellingen;
3. voer updates uit;
4. beperk toegang en
5. voorkom virussen en andere malware.

Het is te adviseren eerst de vijf basisprincipes door te lezen alvorens de scan te starten. Je doorloopt de scan en begrijpt het eindresultaat makkelijker. Elk basisprincipe wordt helder toegelicht en via hyperlinks word je geholpen die analyse handen en voeten te geven. Een vereenvoudigd overzicht van die hyperlinks en geadviseerde stappen:

– inzake kwetsbaarheden:
  – stappenplan risicoanalyse:
    – waaronder ICT-onderdelen inventarisatie;
  – opstellen van een noodplan:
    – leg afspraken vast;
    – stel een uitwijk- en herstelplan op;
  – opstellen van een bellijst:
    – contactgegevens;
– inzake veilige instellingen:
  – IoT-apparaten beveiligen;
  – bedrijfsnetwerk beveiligen;
  – e-mail beveiligingsstandaarden controleren;
  – controleer de veiligheid van het gebruikte wachtwoord;
  – inrichten van een log-informatie systeem;
– inzake updates:
  – een voorbeeld van het opstellen van een patchmanagement-beleid;
  – maak heldere afspraken over welke patches relevant zijn;
  – de controletest of automatisch updaten iets is voor jouw bedrijfsomgeving;
– inzake toegankelijkheid:
  – een link naar een model rechtenmatrix (al of niet met gebruikersrollen);
  – een advies voor realisatie van een in- en uitdiensttredingsbeleid;
– inzake voorkomen van malware en virussen:
  – tips over medewerkersgedrag;
  – antivirusprogramma's en phisingmails.

Vanuit het DTC kun je ook terechtkomen bij hun advies 'Wat te doen bij een cyberincident?', waarom iets zelf uitvinden als het er al is? Daar ook al een overzicht bij wie je terechtkunt na het ondergaan van een cyberincident. Mocht je een IT-specialist in huis hebben of er een inhuren, maar wil je hem ook kunnen volgen/instrueren **inzake het verzamelen van informatie over de daders**, zoek dan het 'Stappenplan voor IT-specialisten' (3) op dat door de politie ter beschikking wordt gesteld."

Er is recentelijk ook vanuit de Kamer van Koophandel een e-mailserie geweest onder de titel: 'Een veiliger bedrijf in 6 stappen'. Hoe sprak je dat aan?
"Deze e-mailserie is gerealiseerd in samenwerking met het DTC en daarom van goede kwaliteit. Het mooie van deze serie is dat ook de collegae mkb-ondernemers aan het woord zijn gekomen. Zij verhaalden van hun cybersecurity-ervaringen en hoe zij geconfronteerd werden met hacks en dergelijke. Het maakt duidelijk dat in de cyberwereld van alles en nog wat kan gebeuren en dat er geen valse schaamte moet zijn om wanneer er iets gebeurd, te handelen en hulp in te roepen. Niets doen, zwijgen of ervan weglopen is geen optie."
OK, er moet gehandeld worden, maar nadat een hack heeft plaatsgevonden of ransomware is geïnstalleerd lijden wij al pijn. Natuurlijk is het beter om op voorhand te acteren. Bekend is back-ups te draaien en na te gaan of je ze ook weer terug kunt zetten. Wat zouden jouw adviezen zijn om jezelf voordien te beschermen?
"Ik wil nu niet direct op alle opties ingaan, maar twee stappen liggen wel erg voor de hand. De eerste betreft het installeren van antivirussoftware en firewalls (gratis zijn redelijke pakketten verkrijgbaar, maar met een overzienbare uitgave kom je al aardig richting semi-professionele pakketten of hardware) en het gebruik van wachtwoorden alsook het beheer daarvan in wachtwoordmanagers (4) — met een open source wachtwoordmanager zoals Bitwarden.com kun je zelfs al gratis aan de slag.

Enkele bekende antivirus- en/of firewallsoftware zijn: AVG, Avast, Avira, Bitdefender, HitmanPro Malwarebytes, Norton, Panda, TotalAV, Webroot SecureAnywhere. Ook kun je met een met advertentie blocker in de browser al tal van virussen gratis voorkomen: uBlock Origin is een gratis extensie, die voor Firefox, Chrome en tal van andere browsers beschikbaar is.

Wat firewalls betreft kan je denken aan: Zyxel, Netgate, Sophos, Cisco, Sonicwall, Fortinet of een gratis open source firewall: vyos.io en pfsense. Mijn lijstje is niet compleet en evenmin in volgorde van kracht of prijsstelling. Laat je door de eigen IT-beheerder/cybersecurity-dienstverlener en/of vertrouwde leverancier voorlichten."

Vincent licht toe:
Het is mijn ervaring dat talrijke cybersecurity-dienstverleners moeite hebben met het vinden van passende oplossingen voor het midden- en kleinbedrijf (mkb). Zelf heb ik jarenlang aan de kant van de securityproviders gewerkt. In die hoedanigheid besefte ik hoe uitdagend het kan zijn om aan te sluiten bij de behoeften van het mkb. De kern van dit probleem schuilt in het onvermogen van serviceproviders om af te stemmen op de pragmatische en zakelijke mentaliteit van mkb-bedrijven. Het is cruciaal om te begrijpen hoe cybersecurity past in zowel de zakelijke als de technische context van de klant, zonder concessies te doen aan het complete cybersecurityplaatje. Helaas slagen veel serviceproviders hier niet in.

Zakelijke context:
De zakelijke omgeving van het mkb verschilt aanzienlijk van die van grotere ondernemingen. In het mkb moet men vlot kunnen schakelen tussen strategische en tactische besluitvorming, aangezien kleinere organisaties doorgaans meer gericht zijn op pragmatisme.

Technische context:
Om succesvol aan te sluiten bij het mkb is het essentieel om snel te kunnen schakelen naar de technische aspecten. Dit is belangrijk omdat techniek in de praktijk de drijvende kracht is waar het meeste werk verzet moet worden.

Compleet cybersecuritybeeld:
Vanwege het beperkte budget en de schaarse middelen binnen het mkb zijn eenvoudige oplossingen vaak aantrekkelijk. Echter, dit kan leiden tot het verlies van het volledige cybersecuritybeeld, wat een cruciaal aspect is voor een effectieve bescherming.

Dank tot zover. Het zal de mkb'er duidelijk zijn geworden dat hij zijn huiswerk vooraf te maken heeft. Kan jij nog andere 'tools' adviseren die de ondernemer op weg naar cybersecurity skillfulness zou kunnen opppakken?
"Jazeker, host je jouw applicaties of een website dan kun je gratis achter de protectie van een Web Application Firewall (WAF) van Cloudflare. Met PingCastle.com kun je gratis jouw Windows **A**ctive **D**irectory (AD) laten scannen op issues en kom je tot praktische verbeteringen. Hardentools is een open source tool waarmee je jouw Windows laptop of PC kunt laten 'hardenen' om zo de meest gevaarlijke features van Windows uit te schakelen (5). Stronghold is een open source tool voor Apple laptops (6). Ook raad ik aan om uBlock Origin te downloaden voor je browser, veel virussen worden namelijk verspreid via advertenties.

Er zijn genoeg tools online te vinden. Toch ziet iedereen steeds vaker dat belangrijke data verstopt zit in SaaS applicaties. Daar zijn vaak geen tools voor. Daarvoor is het van belang dat je een lijstje maakt van alle SaaS applicaties en waarvoor ze gebruikt worden. Vervolgens ga je één voor één de applicaties langs en kijk je of de rechten en users goed staan ingesteld.

In het volgende deel zal ik nog een paar handige APPs aanhalen, maar ik zal ook stilstaan bij wat Windows al aanbiedt in de vorm van automatisch gegenereerde log-informatie databestanden. En dus de vraag aan de ondernemer(s): "Wie van jullie gebruikt al log-rapporten en, zo ja, welke kennen/gebruiken jullie? Laat ook eens weten welke problemen je tegen bent gekomen of welke vragen er verder nog zijn. Benut deze kans."

Referenties

(1) InformatieBeveiliging Magazine, jaargang 23 – 2023 – editie 2, pagina 4 t/m 7
(2) https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen
(3) https://www.politie.nl/binaries/content/assets/politie/algemeen/algemeen/-brochure-stappenplan-cybercrime.pdf
(4) Zie de twee artikelen in InformatieBeveiliging Magazine, jaargang 23 – 2023 – editie 2, pagina 23 ("Password mismanagement" van Lex Borger, Tesorion) en pagina 32 t/m 37 ("De werking en vele functies van wachtwoordmanagers" van Menno Vermeulen, CGI Nederland B.V.)
(5) https://github.com/securitywithoutborders/hardentools
(6) https://github.com/alichtman/stronghold

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Dan word ik wel je vriend

Van leerkrachten tot belangenorganisaties en privacy- en securityspecialisten. Al jaren wijzen zij erop dat we zuinig moeten omgaan met de privacy van onze kinderen. We moeten ze goed weerbaar maken, vertellen over de gevaren en laten weten waar je beter maar niet aan kunt beginnen. En, we hebben vooral zelf ook werk te verzetten – niet zomaar foto's van kinderen online plaatsen en respectvol omgaan met hun recht op privacy (stop met neuzen in die dagboeken en chats). Maar er is een barrière die we maar lastig kunnen nemen. Aanbieders van online diensten en apps verzinnen allerhande mogelijkheden om toch die jongeren weer te kunnen vinden. En dat zelfs zeer letterlijk.

"Mam, weet je dat Snap nu ook AI heeft en dat je dat niet eens uit kan zetten?" Zo begint een voor mij wat ontnuchterend gesprek. Ik had er al van gehoord en ik had ook wat Reels en Tiktoks voorbij zien komen waarin deze feature gebruikt wordt. Sinds kort heeft iedereen die van Snapchat gebruikmaakt er een nieuwe vriend bij: een AI robot waarmee je kunt praten en die supersnel antwoord geeft bovendien. Mijn zoon ging natuurlijk het gesprek aan, nieuwsgierigheid voorop. Maar, hij blijft een kind van zijn moeder en vroeg natuurlijk direct aan deze nieuwe vriend of die ook wist waar hij woont. De robot gaf aan dat hij het weliswaar niet exact wist, maar kwam tot de schrik van mijn zoon met een zeer nauwkeurige benadering.

De volgende vraag laat zich raden. 'Hoe weet je dat?!!!', vroeg hij geschrokken. Mijn zoon verbergt zijn locatie namelijk voor iedereen, behalve voor een aantal hechte vrienden. Als er een ding is dat jongeren heel goed begrijpen dan is het dat het echt gevaarlijk is als iedereen zomaar weet waar je te vinden bent. Klaarblijkelijk ziet de AI robot zich als een hechte vriend, zelfs als je daar niet voor gekozen hebt. En, zoals gezegd, kun je die niet-gekozen AI vriend ook niet ontvrienden of verwijderen.

Gelukkig is er al enige ophef ontstaan over deze nieuwe vriend op Snapchat, want deze robot begon ook al een heel aantal keer een seksueel getint gesprek aan te knopen met de jongeren die ertegen waren gaan kletsen. Hetgeen uiteraard tot enige bombarie heeft geleid. De techgigant heeft inmiddels aangegeven dat ze wat strenger naar de regels gaan kijken en wat beperkingen gaan opleggen aan deze AI robot. Toch jammer dat ze daar pas achteraf aan denken. Ik zou ze graag adviseren om die robot eerst even uit te zetten, dan de regels te bedenken en daarna pas weer aan te bieden. Met daarin de optie dat je actief moet kiezen om vriend te worden en dat je deze kunstmatige vriend ook weer direct kunt verwijderen. Want zoals het nu vormgegeven is, krijg ik wat kippenvel en bekruipt me een zin uit een oude horrorfilm: *'Hi my name is Chucky, wanna play?*'.*

Rachel

*Child's Play 1988

Auteur: André Beerten is sinds 2015 zelfstandig adviseur informatiebeveiliging en ook associate bij Verdonck, Klooster en Associates. Hij werkte eerder bij KPN, Getronics en het Groene Hartziekenhuis. In zes bijdragen ontvouwt hij een Meetbare Maatregelen Aanpak voor de inrichting van een ISMS. Hij is te bereiken via: andre@octopus-ib.nl of via LinkedIn (1)

Even terug

Met mijn eerste bijdrage in IB Magazine 1 van dit jaar over de rol van de CISO dacht ik wel wat reacties los te zullen maken. Ik sloeg nogal van me af en spaarde niemand, ook mijzelf niet, maar wat bleef het stil! Ik werd door niemand op de vingers getikt, maar kreeg ook maar beperkte bijval. Met de mogelijkheid om online te reageren werd bijzonder weinig gedaan. Wat is dat met jullie, is de waarheid te pijnlijk of zijn jullie te lui om te reageren op mijn fouten en ongenuanceerde mening? Spreek je uit op LinkedIn of in mijn e-mail.

MMA

In mijn bijdrage in IB Magazine 2 vertelde ik over de 'implementatiekloof' en bood ik mijn inzichten aan, met het idee dat kritiek leveren belangrijk is, maar ook wel wat gemakkelijk. Wie kritiek levert moet ook een oplossing aanbieden en dat heb ik geprobeerd. Verwacht van mij geen diepe inzichten of doorwrochte beschouwingen met verwijzingen naar grote denkers. Ik schrijf gewoon op wat ik heb geleerd. Ik heb dit allemaal niet tussen hoofdgerecht en toetje bedacht, maar er een hele tijd over gedaan: jaren van fouten maken en peinzen over wat toch het probleem is. Ik kan het namelijk niet uitstaan dat wij - zoals ik in het eerste artikel betoogde - heel druk zijn, maar intussen maar weinig tot stand brengen én daarbij ook vaak niet blij zijn in ons werk.

GEDACHTEN OVER HET ISMS:

IB-Beleid en -eigenaarschap

Vandaag wil ik het hebben over enkele aspecten van het ISMS, het InformationSecurity ManagementSystem. Je kent het wel vanuit de standaarden ISO27001, NEN7510-1. Ik heb er lang mee geworsteld. Maar door schade en schande wijs geworden, denk ik nu dat er écht wel een ambachtelijke standaardmanier bestaat om een ISMS op te zetten. Passen en meten hoort erbij omdat organisaties verschillen, vooral het vinden en binden van de juiste spelers in de organisatie is een 'ding', maar verder…

Geen 'ding'

Even een voorafje: het is af en toe gewoon gênant mensen uit het vakgebied te horen praten over het ISMS alsof het een ding is, een database of een stapeltje documenten dat je koopt en dat je beveiliging magisch dichterbij brengt.
Wat ook niet helpt is dat sommige makers van 'tooltjes' (zoals ik het dan maar noem) de zegeningen van hun systeem/dienst zo breeduit meten dat het wel een oplossing móet zijn. De waarheid is dat ze vaak niet meer bieden dan een soort 'document-ophangrekje' aangevuld met een optie voor beheer van actiepunten (en misschien een risicoregister). Heel handig maar ook niet meer dan dat en zeker geen 'oplossing'.

Schaamlappen

Ook erg vind ik de aanbieders die je aanvullend ontzorgen met standaardteksten voor alles, van beleid, strategisch en tactisch tot procesdocumenten. Daarmee komt het hoofddoel van het ISMS, *nadenken over risico's en passende beveiliging niet dichterbij.* Erger nog, het zorgt voor een jaarlijks herhalend vinkjes-circus dat veel tijd vergt en ergernis oplevert. In de gemeentelijke wereld krijg je zelfs op verzoek een jaarlijkse update, zodat je inspanning wordt gereduceerd tot een druk op de knop… waarna een ingehuurde kracht toeziet op het bijeenrapen van je verdere papieren zodat je er weer voor een jaar vanaf bent. Het moet toch niet gekker worden… we noemen het ook wel ENSIA (2).

Maar het ergste van alles vind ik toch wel de aperte misleiding door partijen die een ISO-certificatie in vier weken aanbieden en dan de *zoek en vervang* ook nog voor je komen uitvoeren. Die in een paar weken een indrukwekkende papieren façade opbouwen en je mensen interviewtraining geven. Een handelwijze waarmee je dan ook nog (echt waar!) een certificering behaalt. Welke auditor je daar dan voor moet bellen weet ik niet, ik ga dit soort misleiding uit de weg.

Zélf nadenken

Ik kan het niet laten er hier ook opnieuw op te wijzen dat de BIO geen ISMS bevat, wel veel tekst die verwijst naar noodzakelijke elementen van besturing, maar het ISMS wordt alleen genoemd in een van de overheidsmaatregelen (H18). Ik vrees dat de lopende update weer een vervolg wordt op dit jaren geleden ingezette dwaalspoor.

Het ISMS in de ISO27001 is waar het allemaal om draait. Niet de controls vormen de norm (al denkt de BIO daar anders over), maar het geheel van beleid, besturing, eigenaarschap, maatregelen, monitoring, rapportage en lering. Het gaat om het geheel, het ManagementSystem dus, dat zoveel lijkt op dat uit de ISO9001, 'the HighLevelStructure'.

Dat is noodzakelijkerwijs voor elke organisatie anders en kan dus onmogelijk helemaal uit een standaardkoker komen. Doe wat een goede auditor doet en bestudeer elk '*moetje*' dat je vindt in de 27001 en denk na over wat het voor jouw organisatie betekent, kies voor een aanpak (goed gedocumenteerd) en houd je aan je voornemen. Meer wordt er niet gevraagd.

Communicatie

Liefst 85 pagina's telde het beleid voor informatiebeveiliging dat ik kortgeleden onder ogen kreeg. Vastgesteld door het bestuur, jawel. Wie denkt dat ze het hebben gelezen moet zijn vinger opsteken. Waartoe dient een document van 85 pagina's überhaupt? Dat wordt alleen gelezen als het een boek is met een leuke omslag, een belofte van spanning of genot. Anders wordt het nooit of te nimmer gelezen. Daarvoor hebben we samenvattingen uitgevonden, liefst in drie PowerPoint-dia's.

Bezweringen

Afgezien van de omvang is er nog iets mis met dergelijk beleid: de inhoud bestaat gewoonlijk uit bezweringsformules (of erger nog: herhaalt de teksten uit de norm). We spreken niemand aan, we stellen geen eisen, geen kaders en criteria. Wat denken we daarmee te bereiken?
Beleid moet iets in beweging zetten, het moet een helder doel communiceren en de randvoorwaarden aangeven waaronder dat doel bereikt moet worden. Het bestaat uit 5 W's:

- *Waarom* – je moet vragen vóór zijn en uitleggen waarom het beleid er überhaupt is;
- *Wie* – verantwoordelijkheid/eigenaarschap is de sleutel tot alles;
- *Wat* – zonder helder doel is elke inspanning te rechtvaardigen, mét alle de gewenste;
- *Waarmee* – reik middelen aan, anders gaat veel tijd verloren met zoeken;

- *Wanneer* – geef realistische tijdslijnen, en maak het SMART.

Het '*Hoe*' moet uit de organisatie komen, bij voorkeur van de 'Wie', die jóu komt vragen om hulp, dát moet het beleid bewerkstelligen.

Strategisch en tactisch

Het beleid dat het bestuur van de organisatie vaststelt moet zich beperken tot haar niveau: het strategische dat doelen stelt, de verantwoordelijken helder benoemt, de middelen daartoe aanreikt en dan het stokje doorgeeft aan het volgende niveau. In de NEN7510 wordt dit volgende niveau IBMF (3) genoemd. Die club (met leden uit de eerste én de tweede lijn (4)) kan zich namens het bestuur buigen over het tactisch beleid, wat dé norm (ISO27001) de 'kaders' noemt waartegen de *opzet, bestaan en werking* van de IB-maatregelen getoetst moeten worden.
Alle IB-beleid moet vastgeklonken worden aan de planning- & controlcyclus (die overal weer anders is), zoals NEN en ISO van ons eisen (in norm-eis 5.1b) tegen vrijblijvendheid.

Kaders (de halve Maesbrug)

Als je spreekt over kaders dan betekent dat 'ruimte afbakenen', minimale, functionele, eisen formuleren. NIVEA (5): de omzetting van controls naar passende en effectieve maatregelen moet gedaan worden door de 'control-eigenaren, zoals ik in mijn artikel in IB Magazine 2 betoogde. Die hebben behoefte aan kaders die worden meegegeven in de implementatie-opdracht, maar willen geen gedetailleerde voorschriften, want dan stopt het nadenken en wordt implementeren een invuloefening. Ook hier geldt: kórt én krachtig, want lange verhalen worden nu eenmaal niet gelezen.

Eigenaarschap

De hoeksteen van het ISMS is eigenaarschap. Daar merk je ook het verschil tussen ondernemers en managers. De eerste voelt zich volledig verantwoordelijk voor zijn eigendom, de tweede vaak alleen als je het hem 'duidelijk uitlegt'. Informatiebeveiliging staat nu eenmaal niet bovenaan de ambitielijst van de gemiddelde manager, hij scoort er niet makkelijk mee. Managers (en allen die zij managen) voeren nu eenmaal de opdracht van het bestuur uit, meestal met beperkte ruimte voor eigen inbreng. Dus zonder expliciete opdracht van het bestuur hangt IB maar al te vaak 'aan de laatste tiet' (6), conform (ontbrekende) opdracht. Al het andere krijgt voorrang.

Soorten

Wat een eigenaar moet doen is in het algemeen wel uit te leggen: hij moet goed zorgen voor zijn eigendom. Dus ook voor de informatieveiligheid ervan. Makkelijk toch?
Maar zoals ik al schreef in mijn artikel van april ligt dat net even anders: informatiebeveiliging is voor velen geen bekend onderwerp, geen routine- of ervaringskwestie. Dus is hulp geboden met middelen en adviezen door competente mensen. Dat is ónze rol: helpen met adviezen en middelen, maar we moeten daarbij níet op de stoel van de eigenaar gaan zitten, niet zijn taak overnemen.
In het artikel van april heb ik de control-eigenaar, de leverancier van informatieveiligheid, al een rol gegeven, hier behandel ik zijn klant: de vrager van informatiebeveiliging, de 'verwerkingseigenaar'.

Verwerkingseigenaar

Er zijn mensen die vinden dat de term verwerkingseigenaar eigenlijk 'informatie-eigenaar', 'proceseigenaar' of zelfs 'systeemeigenaar' moet zijn. Informatie moet mijns inziens horen bij een bedrijfsactiviteit, dat is de basis. Een afdelingsmanager (van een of een samenhangende groep bedrijfsactiviteit(en)) is in mijn ogen voor de informatieverwerking van zijn afdeling als 'verwerkingsverantwoordelijke' de natuurlijke kandidaat. De activiteit van zijn 'afdeling' genereert & gebruikt informatie en draagt dús verantwoordelijkheid. Er zijn vaak meerdere afdelingen zowel maker & gebruiker van informatie in gemeenschappelijke systemen, dus moet uit hun midden één de eigenaarrol op zich nemen en zo de anderen vertegenwoordigen. Ik gebruik heel bewust de AVG-term 'verwerking', om de relatie met de privacycollega's te benadrukken.
Geen van ons heeft nog alle IT in eigen huis, dus alle (cloud-

)diensten zijn verwerkingen mét een eigenaar ín de afdeling waar de gegevens gemaakt en gebruikt worden. Die is immers verantwoordelijk voor de uitbesteding.

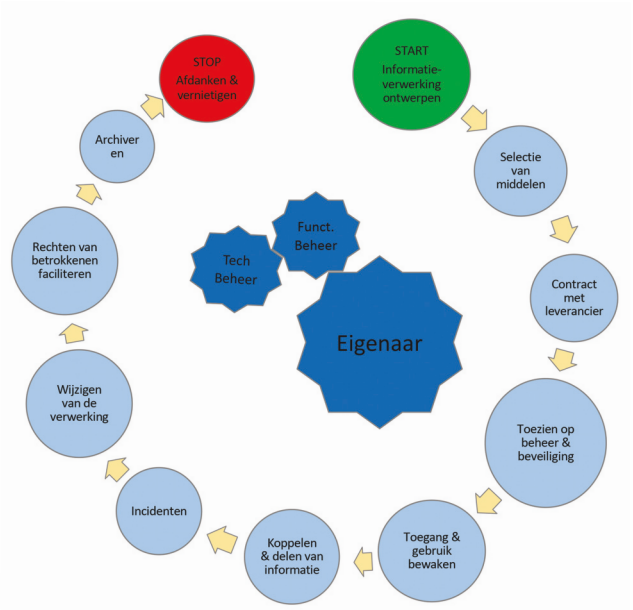
Beheersing loont

Ik heb het ook meegemaakt bij een gemeente dat output uit i-navigator (7) werd gebruikt om een verwerkingenlijst op te stellen. Die lijst telde toen 1215 regels. Dat zijn wel heel erg veel DPIA's en alleen al door de aantallen onwerkbaar voor eigenaren! Dus: beheers je, houd het werkbaar.

Beeld

Eigenaarschap gaat over de gehele periode van het bestaan van de informatieverwerking, de hele levenscyclus dus.

Om de breedte en diepte van dit eigenaarschap goed over te brengen, gebruik ik een eenvoudig beeld (zie figuur 1) dat de hele levenscyclus van een verwerking omvat, van concept tot en met afdanken. Daarbij horen ook het delen van informatie, de privacytaken en vooral: afdanken, goed opruimen, daar gaat nog wel eens wat fout.



Figuur 1: Eigenaarschap in de héle verwerkings-cyclus.

Tekst

Naast het beeld is de formele verankering van dit eigenaarschap van groot belang: het zijn immers managers, zoals eerder betoogd. Het volgende komt rechtstreeks uit beleid dat ik meestal gebruik (als toelichting op het beeld, Figuur 1).

- *Informatie*: tijdens het onderzoek naar een nieuw te starten informatieverwerking brengt hij de beveiligingseisen die aan de informatieverwerking worden gesteld in beeld middels een BIA (en soms een DPIA). Die eisen gaan over de Beschikbaarheid, Integriteit, Vertrouwelijkheid, Privacyklasse, Maximale uitvalduur, Maximaal gegevensverlies & de eisen uit de AVG (rechtmatigheid/doelbinding, proportionaliteit, subsidiariteit, dataminimalisatie);
- *Selectie*: op basis van de gevonden waarden moeten passende maatregelen worden gekozen en (bij uitvoering door derden) zekerheden dat die maatregelen ook effectief zijn. Hierbij laat de eigenaar zich adviseren door de tweede lijn (CISO/ISO).
- *Acceptatie*: bij de start van de verwerking wordt alle informatie rondom uitgevoerde BIA en DPIA, vereiste maatregelen en zekerheden gedocumenteerd en vastgelegd in het register van verwerkingen (hierna Register).
- *Overeenkomst*: alle afspraken rondom uitvoering van de beveiliging en privacy in de vorm van de overeenkomst (en eventuele verwerkersovereenkomst) worden door de **eigenaar** ondertekend en opgenomen in het Register;
- *Beheer*: de eigenaar laat zich actief informeren over beheer en beveiliging van de informatieverwerking, conform afspraken en eisen door de verantwoordelijken hiervoor.
- *Toegang en gebruik*: de eigenaar zet een autorisatiematrix op die gegevens en functionaliteit koppelt aan rollen/functies in/voor de verwerking (meest gebruikelijk in applicaties). Hierbij neemt hij 'functiescheiding' mee in de beoordeling van de rollen.
  De eigenaar verleent toestemming voor de toegang, het passende gebruik en ook beëindiging van toegang.
- *Instructie*: de eigenaar zorgt voor de nodige opleiding

Dit beleid hoort bij het algemene IB-beleid en moet door de bestuurder worden vastgesteld en gecommuniceerd naar alle verwerkingseigenaren.

en oefening voor de gebruikers om de informatieverwerking veilig te kunnen gebruiken zoals bedoeld.

- *Delen*: doorlopend bewaken en beoordelen van informatiekoppelingen en -verstrekkingen met andere verwerkingen binnen en buiten DLZ.
- *Wijzigen*: de eigenaar zorgt ervoor dat hij betrokken is bij alle wijzigingen die invloed kunnen hebben op de vereiste Beschikbaarheid, Integriteit of Vertrouwelijkheid of Privacy van zijn verwerking. Hij zorgt dat hij het laatste woord heeft bij grote wijzigingen in de informatieverwerking. Hij zorgt dan voor een (geactualiseerde) BIA en/of PIA.
- *Incidenten*: de eigenaar zorgt ervoor dat alle (vermoedens van) beveiligingsproblemen en datalekken tijdig gemeld worden. Hij zet in op beperking van de gevolgen, op onderzoek naar de oorzaken, melding bij de betrokkenen en definitief verhelpen van het lek;
- *Rechten van betrokkenen*: hij verwerkt verzoeken van betrokkenen in het kader van de AVG: informatie, inzage, rectificatie, beperking van de verwerking, overdraagbaarheid, bezwaar en vergetelheid.
- *Archiveren*: hij past de archiveringsregels en wettelijke bewaartermijnen toe.
- *Afdanken*: hij verwijdert tijdig alle informatie die niet meer nodig is voor de verwerking.

Dit beleid hoort bij het algemene IB-beleid en moet door de bestuurder worden vastgesteld en gecommuniceerd naar alle verwerkingseigenaren.
De CISO staat mijns inziens voor de taak dit beleid voor zijn organisatie aan te vullen en specifiek te maken én om optimale ondersteuning te leveren. Misschien kan hij/zij maar het beste starten met een cursus voor alle eigenaren. Hier is de eerste lijn namelijk aan zet!

Control-eigenaar

Over de control-eigenaar ga ik nu niets meer zeggen dan dat deze de leverancier van 'passende beveiliging', is, afgestemd op de eisen en wensen van de verwerkingseigenaar. Aan control-eigenaarschap en -implementatie heb ik heel mijn vorige artikel gewijd. Wat ik wel kwijt wil is dat deze eigenaar een expliciete opdracht van of namens het bestuur moet krijgen en ook de middelen nodig heeft (zoals 'gebruik de MMA') om dit realiseren. En natuurlijk ondersteuning van de CISO.

De volgende keer schrijf ik over bronnen van risico-informatie en een andere keer over het hierboven aangehaalde Register, de plek waar alle informatie te vinden is over verwerkingen, middelen, risico's, beveiliging enzovoorts.

Referenties

(1) https://www.linkedin.com/in/andrebeerten/
(2) www.ensia.nl
(3) Informatie BeveiligingsManagement Forum
(4) Bezoek www.iia.nl voor het nieuwe 3-lines model
(5) NIVEA - Niet Invullen Voor Een Ander
(6) Denk hierbij aan de big die het met de achterste en kleinste tiet van de zeug moet doen
(7) http://www.inavigator.nl/index.php/tags/gemeenten

COLUMN LEX

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

People, Process, Technology

Ik ben in een vlaag van opruimzin door oude papieren aan het gaan. Voordat het internet ons enige communicatiekanaal werd, stuurden bedrijven waar je diensten van afnam regelmatig informatiekrantjes. Zo ook OHRA. Ik had daar een paar pagina's uit bewaard en mijn oog viel op een artikel op de achterzijde ervan, met de titel 'Hoe veilig is het internet?'. Het is bedoeld om mensen comfortabel te maken met zakendoen over het internet. Veel details hebben te maken met de menselijke kant en de procesmatige aspecten: *'Beveiliging is meer dan voorkomen dat onbevoegden van buitenaf inbreken. Het heeft ook te maken met stabiliteit en betrouwbaarheid.'*

'De inspanningen om systemen te beveiligen hebben tot doel om het zo lastig mogelijk te maken hierin te breken. In vrijwel alle gevallen wordt misbruik opgemerkt voordat het daadwerkelijk plaatsvindt.' Nou, dat laatste zou ik anders verwoord hebben, toch zijn ook die misverstanden op het raakvlak van proces en techniek van alle tijden.

Maar dan: *'Voor de beveiliging van de website wordt gebruikgemaakt van zogenoemde certificaten, waarmee in Amerika goede ervaringen zijn opgedaan. De techniek hiervan laat zich moeilijk uitleggen, maar simpel gezegd komt het erop neer dat aan elk inkomend of uitgaand bericht een certificaat hangt dat bevestigt dat de informatie ook daadwerkelijk van de afzender afkomstig is én dat ervoor zorgt dat de informatie op de juiste plek terechtkomt.'* Eerst wil ik wel een compliment geven voor het vermijden van woorden als 'cryptografie'. Als je nu een korte lijst zou moeten maken welke maatregelen voor de beveiliging van een website gelden, zou een certificaat wellicht niet eens genoemd worden, omdat het geen keuze meer is. Wel staat er een hele rits aan maatregelen op.

Dan denk ik gelijk *'people, process, technology'*. En de volgorde waarin die staan, dat is niet toevallig. Technologie is de meest veranderlijke van de drie. Processen zijn al minder veranderlijk en mensen hebben echt een aversie tegen verandering. Als techniek zonder mensen kan werken, gaat ontwikkeling snel, maar als er mensen bij betrokken zijn, moet er expliciet rekening gehouden worden met het tempo. Daarom gaat AI zo snel en is uitleg van uitkomsten zo lastig. Procedures en processen zitten er tussenin. Ze moeten het mogelijk maken mensen techniek te laten gebruiken.

Techniek daarentegen ontwikkelt zich steeds sneller. Kijk bijvoorbeeld naar geluids- en beelddragers: 78 toerenplaten kwamen rond 1890 op de markt, vinylplaten in 1948, CD's in 1982 en DVD's in 1996. Toen kwam de USB-flash drive: 8MB in 2001, 64MB (equivalent van een CD in MP3) in 2003, 4GB (equivalent van een DVD) in 2005, 32 GB (een Blue-ray disk) in 2007. Geen wonder dat Blue-ray, geïntroduceerd in 2006, nooit echt doorgebroken is. En nu heeft streaming alles overgenomen, een USB-flash drive is een zeldzaamheid geworden. Maar het proces van afspelen is maar weinig gewijzigd. Geluidsafspeelprogramma's op de PC lijken op de oude hifi-apparaten.

Zo moeten we in informatiebeveiliging dus tegen *people, process, technology* aankijken: investeer in het gedegen bewustzijn van mensen en het implementeren van veilige processen. Maar houd ook in de gaten waar techniek zijn eigen gang lijkt te kunnen gaan, los van mensen en processen, zoals bij AI. Dat zijn de toepassingen die snel extra aandacht moeten krijgen, zodat we ze kunnen blijven beheersen met standaarden en technische maatregelen.

Auteurs: Pepijn van den Broek, partner bij ISR Nederland BV, Jean-Pierre van Eekelen, Corporate Business Continuity Officer ProRail, Gert Kogenhop, Operationeel Manager BCM Kader Group, Dick Hortensius, Senior-consultant managementsystemen, NEN Zorg, Consumenten en Maatschappij. Voor meer informatie over deze visie of het uitwisselen van ideeën erover neem contact op met de auteurs via pepijn.vandenbroek@isrnederland.nl.

Bescherming van vitale infrastructuur? Gebruik bestaande normen!

Bepaalde processen zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting of grote economische schade leidt en een bedreiging vormt voor onze nationale veiligheid. Elektriciteit, toegang tot internet, drinkwater en betalingsverkeer zijn voorbeelden van deze vitale processen. Deze processen en hun infrastructuur vormen de Nederlandse vitale infrastructuur. Als vitale infrastructuur uitvalt, kan dat grote maatschappelijke gevolgen hebben.

De mogelijke grote maatschappelijke gevolgen zijn de reden voor overheid, bedrijfsleven, hulpverleningsdiensten en inlichtingendiensten om nauw samen te werken om de bescherming van zulke vitale producten, diensten en processen continu te verbeteren en te borgen. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft een coördinerende rol bij de bescherming van onze vitale infrastructuur en het opstellen van beleid en wetgeving die hierbij horen. Echter, in de Nederlandse beschermingsaanpak van vitale infrastructuur, die sinds circa het jaar 2000 (als gevolg van de millenniumproblematiek) bestaat, wordt nauwelijks het gebruik van normen gestimuleerd als het gaat om hoe als vitaal aangemerkte organisaties (de vitale aanbieders) zich dienen te beschermen tegen uitval. De overheid vindt de processen die deze organisaties uitvoeren en de infrastructuur die ze daarbij gebruiken essentieel voor ons maatschappelijk functioneren, maar stelt nauwelijks eisen aan hoe risico's op uitval van hun vitale diensten beheerst dienen te worden.
Wanneer je als organisatie als vitale aanbieder bent geïdentificeerd én de essentiële processen/diensten die je levert afhankelijk zijn van ICT en dataverkeer én je bent aangewezen als Aanbieder van een Essentiele Dienst (AED) of als een Andere Aangewezen Vitale Aanbieder (AAVA), dan dien je aan specifieke eisen voor informatiebeveiliging te voldoen die gelden vanuit de Wet beveiliging Netwerk- en informatiesystemen (Wbni). Maar meer eisen gericht op instandhouding van vitale dienstverlening zijn er eigenlijk nauwelijks, zelfs niet met het actief worden van de nieuwe Europese richtlijn Critical Entities Resilience (CER).

En dat is op zijn minst best vreemd te noemen, in een tijd waarin we steeds afhankelijker worden van (ICT-)infrastructuur en we meer en meer gericht zijn op het uitbannen van risico's en het voorkomen van grote crises. Om die reden pleiten wij voor een verbeterde aanpak van de bescherming van de vitale infrastructuur, niet zozeer door meer wet- en regelgeving, maar door veel meer gebruik te maken van beschikbare internationale normen en standaarden en daarmee een betere aansluiting te realiseren bij gangbare risico- en crisisbeheersingsmethodieken binnen vitale organisaties en tevens te zorgen voor een meer uniforme, Europese aanpak.

Er wordt al jaren gewerkt aan het normaliseren en standaardiseren van processen om stabiele processen en producten te kunnen garanderen en risico's op afwijkingen te verkleinen. Onder andere de Internationale Organisatie voor Standaardisatie (ISO) werd hier in 1947 voor opgericht. De normen die door ISO worden ontwikkeld kunnen door organisaties over de gehele wereld worden gebruikt en zorgen ervoor dat processen, diensten, producten en materialen geschikt zijn voor hun doel. Ook zorgt ISO ervoor dat deze vereisten in alle aangesloten landen (167 in totaal) overeenkomen, zodat er sprake is van internationale standaardisering.

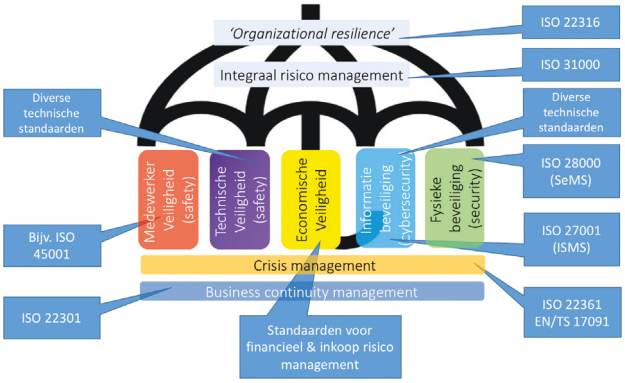
Een weerbare vitale infrastructuur door het gebruik van standaarden

Het doel van het Nederlandse programma Bescherming vitale infrastructuur onder regie van de NCTV is om de beveiliging en continuïteit van vitale processen en infrastructuur zo goed mogelijk te kunnen garanderen. Een stabiele vitale infrastructuur is dus eigenlijk niets minder dan het hebben van een stabiele en beheerste procesuitvoering met een focus op continuïteit. En dat is precies waar normen en standaarden bij kunnen helpen. Er zijn diverse standaarden gericht op risicobeheersing (ISO 31000), informatiebeveiliging/ cybersecurity (o.a. ISO 27001), crisisbeheersing (ISO 22361) en bedrijfscontinuïteit (ISO 22301) die door vitale aanbieders kunnen worden gebruikt om continuïteitsrisico's te mitigeren en effecten van verstoring sneller te verhelpen. Hiermee werken de vitale aanbieders aan risicobeheersing, weerbaarheid, continuïteit en veerkracht. In het Engels is daar een overkoepelende term voor, namelijk 'organizational resilience'.

'Organizational resilience: the ability of an organization to absorb and adapt in a changing environment'

(Bron: ISO 22316:2017 Security and resilience – Organizational resilience – Principles and attributes)

Organizational resilience gaat dus over de mate waarin een als vitale aanbieder aangemerkte organisatie in staat is zich 'te wapenen' tegen veranderingen en de risico's die daaruit kunnen ontstaan. Risico's die de bedrijfsvoering ernstig kunnen verstoren en dientengevolge de continuïteit van product- en dienstlevering kunnen bedreigen. Organizational resilience vormt als het ware de conceptuele paraplu waaronder alle aandachtsgebieden gericht op procesbeheersing en risicobeheersing zich bevinden. Ook voor organizational resilience is inmiddels een ISO-norm ontwikkeld, de standaard ISO 22316.



Figuur 1: model voor organizational resilience m.b.v. internationale standaarden – © ISR Nederland BV.

Dit model zou door vitale aanbieders, de verantwoordelijke ministeries en de toezichthouders als referentiekader gehanteerd kunnen worden om de organizational resilience van vitale aanbieders (en dus de weerbaarheid) aantoonbaar te verbeteren. Door vanuit beleid (de NCTV en de ministeries die beleidsverantwoordelijk zijn voor de aanbieders die vitale processen uitvoeren) het gebruik van standaarden meer te stimuleren en hier duidelijker op te sturen ontstaat een meer uniforme en toetsbare aanpak en risicobeheersing.

De vitale aanbieders kunnen deze internationaal geaccepteerde standaarden gebruiken om hun weerbaarheid te organiseren op een systematische en aantoonbare manier door gebruik te maken van de standaarden, de voorbeelden van beheersmaatregelen daarin en de lerende aanpak die erin is opgenomen. Daarnaast maakt het gebruik van standaarden het mogelijk voor vitale

‘Ter bevordering van de convergente uitvoering van deze richtlijn moedigen de lidstaten, waar nuttig en zonder het gebruik van een bepaald soort technologie op te leggen of te bevoorrechten, het gebruik aan van Europese en internationale normen en technische specificaties die relevant zijn voor de beveiligings- en weerbaarheidsmaatregelen die van toepassing zijn op kritieke entiteiten.’

(Artikel 16 CER-richtlijn).

aanbieders om eenvoudig en snel kennis van het toepassen van standaarden van de markt te betrekken. De toezichthouders hebben zeer waarschijnlijk ook baat bij meer gebruik van standaarden. Door een gestandaardiseerde aanpak neemt de toezichtlast waarschijnlijk af, omdat er duidelijker normen worden gehanteerd. Daarnaast is `metatoezicht’ mogelijk. Door als toezichthouder te kunnen vertrouwen op de gecertificeerde toepassing van de standaarden door de vitale aanbieders, kan efficiënter effectief toezicht plaatsvinden.
Een laatste voordeel van meer standaardisering is nog dat het eenvoudiger wordt om gestructureerd kennis op te bouwen over de beschermingsaanpak via regulier onderwijs en commercieel onderwijs. Met name omdat een aanpak via standaarden goed aansluit bij bestaande bedrijfskundige theorieën. Er zijn al tal van voorbeelden van succesvolle toepassing van normen in als vitaal aangemerkte sectoren, zoals NEN 7510 (gebaseerde op ISO 27001) voor informatiebeveiliging in de zorg en de NTA 8620 (gebaseerd op ISO 55001) voor assetmanagement bij netbeheerders. Deze normen geven praktische handvatten voor het voldoen aan algemene wettelijke zorgverplichtingen.

Ook op Europees niveau wordt het gebruik van standaarden voor de organisatie van meer weerbaarheid (resilience) gestimuleerd. De recent aangenomen nieuwe Europese richtlijn gericht op de verbetering van de weerbaarheid van kritieke/vitale sectoren, de Criticial Entities Directive (EU) 2022/2557 (hierna de CER-richtlijn) bevat ook een duidelijke eis richting de lidstaten om meer gebruik te maken van normen en standaarden.

De eisen uit de CER-richtlijn worden vanaf oktober 2024 van toepassing op alle Nederlandse vitale aanbieders. Op dit moment wordt door het ministerie van Justitie en Veiligheid de Nederlandse wet ontwikkeld die de Europese eisen verplicht zal stellen aan de Nederlandse vitale aanbieders. Daarom is volgens ons nú het moment om in de wet (of de toelichting daarop) de visie van organizational resilience te adopteren en het gebruik van standaarden als hulpmiddel voor de aantoonbare organisatie van weerbaarheid te stimuleren. Op deze manier kan gebruik worden gemaakt van normen die vaak in samenwerking met vertegenwoordigers uit vitale sectoren zijn ontwikkeld waardoor deze aanpak op draagvlak en praktische toepasbaarheid kunnen bogen en er geen nieuwe wielen hoeven te worden uitgevonden.

Referenties

(1) https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen
(2) https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Jouw BBB gevraagd

De afgelopen periode hebben we allemaal meegemaakt dat er een kleine politieke aardverschuiving ontstond tijdens de Provinciale Statenverkiezingen. Wat er gebeurde is dat mensen hun stem lieten horen. De leden van de vereniging NL lieten zich horen en vinden dat het anders moet. Dit zette mij aan tot reflectie over onze eigen mooie vereniging.

Er komen veel vakzusters en –broeders op onze evenementen en iedereen is over het algemeen erg positief. We halen nog steeds leuke artikelen op bij de leden voor ons magazine en als we een feestje hebben, zijn veel leden van de partij. Vanachter de bestuurstafel bezien lijkt het er dan op dat we de goede dingen doen en dat we een prachtige vereniging zijn met een stijgend ledenaantal. Tot zover prima. En toch…?

Om ons heen verandert de wereld in rap tempo. Ons vak verandert, opleidingsorganisaties passen hun curriculum aan, de behoefte aan specialisten met erkende kennis en vaardigheden wijzigt continu en de gereedschapskist waarover zij moeten beschikken wordt met de dag zwaarder. En onze rol verandert omdat we steeds meer moeten nadenken over de betekenis van informatiebeveiliging voor de business en de maatschappij, wat hebben zij eigenlijk echt van ons nodig? En dan wijzelf. Ook jullie en ik veranderen. Als een continu proces gaan we mee in de stroom van verandering, soms als kapitein op de boot en soms als passagier.

De *'en toch'* tijdens mijn reflectie wordt dan ook ingegeven door de vraag of dat wat wij doen als vereniging, na al die jaren nog het beste is wat wij samen kúnnen doen. Is dit de beste versie van het PvIB die er bestaat of is er ruimte voor of zelfs behoefte aan verandering, innovatie, groei en een nog mooiere bloei? We weten allemaal dat stilstand achteruitgang is en dus moeten we ons afvragen hoe we ook als bloeiende vereniging mee moeten transformeren. En als we dat samen willen, in welke richting dan?

Het antwoord op deze vragen kan natuurlijk alleen van jullie komen. De koers die we bepalen, de manier waarop we die volgen en de middelen die we daarvoor benutten worden voor een groot deel bepaald door de reden waarom wij met elkaar de belangrijkste vakvereniging zijn in het IB-domein. Dit antwoord is onze gemeenschappelijke '**Why**'.

Dus jullie mening is hierbij essentieel. En die willen we dan ook heel graag horen. Dat kan tweemaal per jaar op onze ALV waar dit op een formele manier kan. Je kunt ook meedoen aan de klankbordgroep, die ons helpt om op gerichte vragen van het bestuur antwoorden en richting van jullie te krijgen. Maar boven alles is er die vrijheid van meningsuiting. Vrijheid om altijd jouw mening, of die van een groepje gelijkgestemden, kenbaar te maken. Dit kan tijdens een evenement rechtstreeks met de bestuursleden of gewoon via mail natuurlijk. En niet alles hoeft te leiden tot een aardverschuiving, maar jouw mening telt!

Doe dus mee! Help ons en zorg voor die Belangrijke Bijdrage aan het Besturen van onze vereniging in de goede richting.

Hartelijke groet (en tot gauw),
Evert van Zanten

Auteurs: Marijke Stokkel, Strategisch adviseur cybersecurity en oefenleider OZON 2023, UvA en HvA. Roeland Reijers, Chief Information Security Officer (CISO) en (gedelegeerd) opdrachtgever OZON 2023, UvA en HvA.

Hoe je in 10 stappen een cybercrisis-oefening organiseert

Het is half maart, een week voor de oefening. Marijke, de oefenleider, wordt gebeld door een deelnemer, laten we hem Joris noemen. "Het is me toch nog niet helemaal duidelijk. Kun je vertellen wat er precies van mij wordt verwacht? Waar moet ik me melden op 23 maart? En krijg ik dan een opdracht bij de start van de oefening?"

Joris is bij de briefing geweest, heeft de uitleg en spelregels meegekregen, maar vindt het toch lastig om een voorstelling te maken van de oefening, en vooral van zijn rol hierin.

Eigenlijk niet zo vreemd. Een crisisoefening is een nabootsing van de werkelijkheid, in een min of meer gecontroleerde omgeving met beperkingen en spelregels. Het vergt verbeeldingskracht om daar direct soepel in te opereren. En dit geldt des te meer voor een *cyber*crisisoefening, omdat hier minder concrete elementen zijn waartoe je je kunt verhouden dan bij andere crisisoefeningen - denk aan terreur of brand - zoals een fysieke locatie waar de crisis plaatsvindt, materieel en (nep) slachtoffers. Cybercrisis-oefeningen zijn echter belangrijk voor de digitale weerbaarheid van organisaties (1), het is dus raadzaam om deze te houden. Vooraf zorgvuldig nadenken over de juiste opzet maakt een oefening doeltreffender.

Op 23 en 24 maart jl. werd OZON gehouden, de tweejaarlijkse sectorbrede cybercrisisoefening voor onderwijs en onderzoek. De oefening is een initiatief van SURF (2) en wordt sinds 2016 tweejaarlijks gehouden. De Universiteit van Amsterdam (UvA) en de Hogeschool van Amsterdam (HvA) hebben eerder deelgenomen en waren ook dit jaar van de partij, net als zeventig andere instellingen.

Hoe organiseer je een cybercrisisoefening? Hoe kun je die zo voorbereiden dat de deelnemers optimaal kunnen oefenen? Dit artikel beschrijft hoe de OZON oefening is voorbereid en uitgevoerd bij de UvA en HvA, vanuit het perspectief van de oefenleider en van de opdrachtgever.

Voordat we beginnen: waarom gaat dit artikel over de UvA én de HvA? Waarom samen? Dat komt omdat de instellingen een gemeenschappelijke ICT-dienst (ICT Services genaamd) en één CISO hebben. Dat zijn centrale partijen bij een cybercrisis(-oefening) en daarom was het logisch dat beide instellingen gezamenlijk deelnamen aan de oefening.

Voorbereiding

‘We denken in grote lijnen maar leven in details’ [3]

Omdat we deelnamen aan het initiatief van SURF stond de opzet van de oefening van tevoren al vast. OZON is een zogenaamde simulatie-oefening, waarbij de deelnemers een realistisch scenario naspelen in hun eigen werkomgeving. Een andere bekende variant is een tabletop-oefening. Hier wordt een crisisoverleg nagebootst en hebben de deelnemers meer gelegenheid om tijdens de oefening te reflecteren op hun eigen handelen. Deze variant duurt een stuk korter dan de simulatie-oefening (4).

De UvA en HvA namen deel aan OZON met twee crisisteams en in totaal veertig deelnemers. Dit vergde een gedegen voorbereiding. We wilden een optimale oefenomgeving creëren. We schreven een zo realistisch mogelijk scenario, informeerden de deelnemers via meerdere briefings, bootsten bestaande communicatiemiddelen na en stelden een respons cel samen. We volgden een aanpak die, achteraf gezien, in tien stappen uiteengezet kan worden. Deze aanpak werkte goed voor ons en daarom hebben we hem uitgewerkt in een apart kader.

De oefenleider bereidde zich dus minutieus voor op de oefening. Voor een deelnemer geldt dit idealiter niet. Een crisis komt in de regel onverwacht. Als een deelnemer allerlei voorbereidingen gaat treffen voor een oefening, wordt deze minder waarheidsgetrouw. Het is dus niet de bedoeling dat een deelnemer gaat werken op een andere locatie dan gebruikelijk, of samen met andere deelnemers in één overlegruimte de injects gaat afwachten. Wat een deelnemer wél kan doen, is ervoor zorgen dat er geen belangrijke afspraken in de agenda staan voor de oefendagen. Voor een crisis zeg je belangrijke afspraken af, maar voor een oefening werkt dat net iets anders.

De aanpak van de UvA en HvA in 10 stappen

1. **Zorg voor bestuurlijk commitment.** Een stevig draagvlak bij het bestuur zorgt voor meer animo voor deelname aan de oefening en vergroot de kans dat de aanbevelingen achteraf daadwerkelijk opgepakt gaan worden. Dit draagvlak was bij ons ruim aanwezig. Sterker nog, terwijl het CISO-team en ICT Services overwogen om vanwege meerdere lopende audits en verbetertrajecten dit jaar niet deel te nemen aan OZON, was het bestuur resoluut. Het oefenen gaat door. Dit bestuurlijke draagvlak is heel prettig, want er gaat veel tijd zitten in de voorbereidingen en het is vervelend als er over elk extra uurtje inzet een discussie gevoerd moet worden.

2. **Maak iemand verantwoordelijk.** Stel iemand aan als oefenleider. Bij de UvA en HvA is vanwege de grootte en complexiteit van de oefening gekozen voor twee oefenleiders. Zij hadden elk een eigen aandachtsgebied. De oefenleiders bereidden de oefening voor en leidden de oefendagen.

3. **Denk ook alvast aan de waarnemers.** Waarnemers hebben als taak om de oefening te observeren en achteraf om de evaluatie te leiden. Wij hebben gekozen voor drie waarnemers: één voor het bestuurlijke crisisteam en twee voor ICT Services, waaronder het operationele crisisteam en de incidentresponsteams CERT en SOC. Zorg ervoor dat er qua profiel voldoende aansluiting is met de teams die worden waargenomen.

4. **De oefendoelstellingen zijn het fundament.** Oefendoelstellingen geven gedurende het hele traject focus: bij het opstellen van het scenario en het samenstellen van het deelnemersteam en tijdens de evaluatie. Bedenk in een vroeg stadium wat je wilt bereiken en leg dit voor aan de opdrachtgever of het bestuur. Een cybercrisisoefening is in eerste instantie bedoeld om in de volle breedte een crisis na te bootsen, met alle betrokkenen van de organisatie. De oefendoelen gaan idealiter over de processen en procedures. Werkt men volgens het crisishandboek? Worden de juiste stakeholders betrokken? Hoe verloopt de opschaling naar een crisis? Voor het toetsen van technisch-inhoudelijke vaardigheden is een oefening minder passend, dan volstaat een training of Capture-the-Flag (5) ook.

5. **Stel een team van deelnemers samen.** Op basis van de oefendoelstellingen kun je grotendeels al bepalen wie er deel moeten nemen. Wil je de opschaling naar een crisissituatie oefenen? Zorg er dan voor dat er zowel leden van de operationele uitvoering als van het crisismanagementteam op de deelnemerslijst staan. Wil je de samenwerking oefenen tussen twee afdelingen? Dan doen er afgevaardigden van beide afdelingen mee. Wees flexibel bij het samenstellen van het team. Mensen kunnen afzeggen of uitvallen. Zorg indien mogelijk voor een back-up van sleutelfiguren. Met de uitwerking van het scenario kan ook duidelijk worden dat meer mensen nodig zijn.

6. **Creëer een realistisch scenario van een uitzonderlijke situatie.** Stel een achtergrondverhaal op dat beschrijft hoe de cybercrisis ontstaat. Richt je op een ongewone situatie die veel vergt van de organisatie om aan te pakken en die de organisatie zeer kwetsbaar kan maken. SURF leverde een fraai basisscenario aan. Een van de verhaallijnen was een hackerscollectief dat veel 0-day kwetsbaarheden verzamelde en deze tijdens de oefendag in korte tijd achter elkaar op hun website publiceerde. Voor de UvA en HvA hebben we daarnaast een instellingsspecifiek scenario opgesteld, dat kortgezegd neerkwam op een datalek van zeer vertrouwelijke onderzoeksdata.
   Het was een tijdrovende klus, want we wilden zeker weten dat alle verhaallijnen realistisch waren. We hebben tijdens het opstellen advies ingewonnen van een aantal experts bij de UvA en HvA.

7. **Ontwikkel scenario-injects.** Stel een draaiboek op met berichten (ook wel injects genoemd) die deelnemers ontvangen tijdens de oefening. Een inject is bijvoorbeeld een bericht over inlogproblemen aan de servicedesk van medewerkers. Bedenk hoe de servicedesk hier waarschijnlijk op reageert (ook wel 'expected player action' genoemd). Gaat de medewerker eerst zelf onderzoek doen? Neemt hij of zij contact op met andere afdelingen? Schrijf uit hoe het proces zal lopen. Zorg ervoor dat je voldoende injects achter de hand hebt om de vaart in de oefening te houden. Stel dat er niet geëscaleerd wordt naar het bestuur terwijl dat volgens het scenario wel zou moeten,

dan kun je als responsecel het bestuur op de hoogte brengen. Hiervoor dien je een andere partij te simuleren. Je benadert bijvoorbeeld het bestuur als hoofd van een afdeling - kies iemand die niet deelneemt aan de oefening - met het bericht dat veel van je medewerkers inlogproblemen hebben, dat dat nog niet is opgelost en dat je snel actie van het bestuur vraagt. Beschrijf per inject hoe laat deze ingezet wordt, met welk doel en wat de 'expected player action' is.

8. **Stel een responsecel samen.** Met een responsecel simuleer je de wereld buiten de deelnemers. De deelnemers kunnen niet zomaar met iedereen gaan bellen tijdens de oefening. Als zij contact met iemand willen opnemen die niet in de deelnemerslijst staat, dienen zij dat via de respons cel te doen. Onze responsecel bestond uit zeven mensen: twee security architecten, twee servicemanagers, een communicatieadviseur, een bestuursondersteuner en een functioneel beheerder. In de voorbereiding hielpen deze mensen mee met het realistisch maken van het scenario en tijdens de oefening fungeerden zij als de hele buitenwereld. Voor de communicatie met de spelers gebruikten we een gedeelde mailbox.

9. **Boots communicatiemiddelen na.** Om realistisch te kunnen oefenen, moeten deelnemers gebruik kunnen maken van communicatiemiddelen die normaal ook tot hun beschikking staan. Denk aan een Signal-groepen, maillijsten, intranetpagina's en webpagina's. We wilden niet de echte kanalen gebruiken omdat dat voor verwarring kan zorgen en omdat dat het exporteren van data voor evaluatie-doeleinden in de weg staat. We kozen ervoor om Teams-kanalen en gesimuleerde Signal-groepen in te zetten. Elke bestaande Signal-groep kreeg een OZON-imitatieversie en de andere communicatiemiddelen kregen elk een eigen Teams-kanaal. Dit werkte prima. De kanalen behoefden vooraf weinig uitleg en tijdens de oefening werd er volop gebruik van gemaakt.

10. **Besteed aandacht aan de briefing van deelnemers.** We organiseerden meerdere bijeenkomsten voor de deelnemers. Hierin kwamen de opzet van de oefening, de spelregels en het simuleren van de communicatiemiddelen aan de orde. Uiteraard deelden we niet het inhoudelijke scenario, dat diende geheim te blijven. Voor sommige deelnemers was de materie, zoals het concept van een respons cel, lastig om direct te bevatten. We namen extra tijd om hen goed te informeren.

De uitvoering

Chaos is a friend of mine [6]

Een crisis verloopt niet ordentelijk - als dat wel zo was zou het geen crisis zijn - en dat gold ook voor de crisis in de oefening. Op de oefendag zaten de oefenleiders om negen uur 's ochtends samen met de respons cel als gezamenlijk oefenteam in één ruimte. Draaiboek bij de hand, de visuele weergave van het scenario vergroot uitgeprint aan de muur. Toen de oefening startte, kwam er direct een grote stroom berichten op gang. Vanwege het sectorale karakter van de oefening hadden we hier slechts beperkt invloed op.

Na al het gepuzzel en geverifieer van de voorgaande periode, moest het oefenteam de controle loslaten. De

chaos omarmen. Inspelen op wat er gebeurde. We vonden die omschakeling aanvankelijk best lastig, maar uiteindelijk lukte het aardig.

Over het optreden van de deelnemers kunnen we niet te veel uitweiden, de evaluatie is momenteel in volle gang. Vooral de operationele teams waren druk met het verweer tegen de continue stroom kwetsbaarheden. Er werd redelijk snel opgeschaald, wat te maken had met de talloze alarmerende berichten die binnenkwamen vanuit de sector. De crisisoverleggen verliepen in de regel doelmatig. De crisisteams pasten het BOB-model toe, zoals ook wordt voorgeschreven in de UvA en HvA crisishandboeken. Het BOB-model is het bekendste model voor crisisbeheersing en staat voor *beeldvorming*, *oordeelsvorming* en *besluitvorming*. Het geeft structuur aan crisisoverleggen en draagt bij aan heldere besluitvorming. (7)

In het algemeen kunnen we zeggen dat de crisisteams goed op elkaar ingespeeld waren. De deelnemers overlegden constructief en bewaarden de rust.

De nabeschouwing

Kostbaar is de wijsheid die door ervaring wordt verkregen [8]

De evaluatie is misschien wel de belangrijkste fase. Na het precisiewerk van de voorbereiding en het tumult van de oefendagen, gaat deze fase over lering trekken uit de oefening. Wij hebben in totaal drie evaluatiebijeenkomsten gehouden: twee voor ICT Services en één voor het bestuurlijke crisisteam. Dat deden we direct na de oefening (ook wel 'hotwash' genoemd). Het waren constructieve sessies waarbij de deelnemers stoom konden afblazen, hun enthousiasme deelden en hun grieven konden uiten. De boventoon was positief. We hebben ook een evaluatieformulier gestuurd naar alle deelnemers.

De waarnemers en oefenleider zijn nu bezig om alle observaties en input van deelnemer te verwerken in een evaluatierapport. De UvA en HvA crisishandboeken en de oefendoelstellingen worden hierbij gebruikt als leidraad. Daarna is het zaak om de positieve punten te koesteren en de leerpunten op te pakken ter verbetering.

De OZON 2023 oefening bleek weer een goed leerinstrument. De deelnemers gingen uiterst serieus aan de slag. Het scenario en de oefenomgeving waren een goede benadering van de realiteit. We hebben de doelstellingen uitgebreid kunnen oefenen.
Kortom, we kijken positief terug op de oefening en zijn blij dat we hiermee kunnen bijdragen aan een cyberweerbare organisatie.

Referenties

1. De Nederlandsche Bank ziet het oefenen van een cyberaanval als een van de drie basismaatregelen die aandacht behoeven bij organisaties om zich te beschermen tegen cyberdreigingen: https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/
2. SURF is de ict-coöperatie van de sector onderwijs en onderzoek. Meer informatie: https://www.surf.nl
3. Dit citaat wordt toegeschreven aan de negentiende-eeuwse filosoof en wiskundige Alfred North Whitehead
4. Deze en andere oefenvarianten worden beschreven in de whitepaper van SURF over oefeningen. whitepaper-cybercrisisoefening-ozon-een-gap-bridging-exercise.pdf (surf.nl) p18-20
5. Capture the flag (cybersecurity) - Wikipedia
6. Dit citaat wordt toegeschreven aan Bob Dylan
7. Meer informatie over het BOB-model: Waar komt 'ons' BOB model voor besluitvorming in crisisteams vandaan? - Zaak voor Crisiskunde
8. Dit citaat wordt toegeschreven aan de zestiende eeuwse Britse auteur Robert Ascham

Dimitri van Zantvliet is Directeur Cybersecurity bij de Nederlandse Spoorwegen

COLUMN DIMITRI

Open the pod bay doors, HAL

Waar zal ik eens beginnen? Misschien door te vermelden dat ik dit schrijf een dag nadat een duizendtal 'technology bigwigs' de A.I. ontwikkeling in de pauzestand wilden zetten. Dit magazine komt pas veel later uit waardoor de wereld, wanneer je dit leest, zomaar eens in een GPT5 of -6 chaos kan verkeren. Misschien zitten we wel in een soort dystopisch Cyber Wuhan scenario: een A.I. ontsnapt aan zijn ethische 'guardrails', automuteert naar een polymorfe worm, propageert zich per milliseconde en valt het hele internet aan waardoor de (digitale) wereld tot een stilstand komt totdat een slimme student de CAPTCHA killswitch weet te vinden: **'Open the pod bay doors, HAL'.**

Het Collingridge dilemma is een bekend vraagstuk binnen de technologie-ethiek. Het dilemma stelt dat het erg moeilijk is om in een vroeg stadium te bepalen welke gevolgen een technologie zal hebben, en dat het juist als deze gevolgen duidelijk zijn, het vaak te laat is om er nog iets aan te veranderen.

Dit dilemma wordt alleen maar actueler (en groter) wanneer we kijken naar de snel evoluerende Decentrale Sociale Technologieën (DST's) zoals, het metaverse, web3, activitypub, e-ID's en de Fediverse. Maar ook cryptografie, artificial intelligence en quantum computing trekken een exponentiële sprint. Het grote geld moet natuurlijk wel snel terugverdiend worden en de doorontwikkeling lijkt dus vaak op een race waarbij bedrijven proberen om zo snel mogelijk nieuwe producten op de markt te brengen, zonder zich al te veel zorgen te maken over de potentiële cybersecurity- en privacyrisico's. Sterker nog, vele organisaties spenderen miljarden om endorfine genererende algoritmes te bedenken om massa's gebruikers verslaafd te maken aan hun apps en content. Ik verzin het helaas niet!

Een van de betere papers die ik recent las is *Ethics of Decentralized Social Technologies: Lessons from Web3, the Fediverse, and Beyond*. De paper is geschreven door Danielle Allen, Glen Weyl et al. (echt even lezen). Het beschrijft de radicale technologische versnelling waarin we terecht zijn gekomen en de uitdaging die dat voor de samenleving betekent. 'Too Long; Didn't Read (TL; DR)': we hebben een nieuwe vorm van beleid en toezicht hierop nodig om de pluraliteit en democratie van de samenleving te bewaken. Analoog aan het Collingridge dilemma kunnen we niet altijd wachten tot we precies snappen wat de transformatieve technologie gaat betekenen voor de maatschappij en zullen we richting moeten geven aan zaken die we niet altijd helemaal begrijpen. De schrijvers noemen dit 'Experimental Governance'. Ik vertaal het even naar experimenteel beleid.

Het houdt in dat we proberen risico's te duiden vóórdat we precies weten wat de exacte consequenties zijn. Het kan dus ook betekenen dat we er wel eens naast kunnen zitten. Binnen NS Cybersecurity zijn we dit 'hot topics' gaan noemen en helpen we de bedrijfsonderdelen de risicoscenario's te schetsen zonder ze per se te weerhouden van het gebruik ervan. Ik vermoed dat we de komende jaren meer en meer gebruik gaan maken van 'digital twins', 'testbeds' en 'cyberranges' om de risico's op- en van nieuwe technologie te verminderen. Wél zullen we hierin een zekere mate van transparantie moeten gaan betrachten richting onze klanten. Experimenteren met experimenteel beleid zal één van onze dagelijkse cybersecurity-activiteiten moeten worden. Een stuk interessanter dan die vermaledijde basis securitymaatregelen. Dat dan weer wel :-)

Auteurs: Erik Langius en Edwin Harmsma. Beiden werkzaam bij TNO ICT, Strategy & Policy. Erik is te bereiken via: erik.langius@tno.nl en Edwin via edwin.harmsma@tno.nl.

Nederlandse partijen bouwen testomgeving voor Gaia-X clouddiensten

Gaia-X is een Europees initiatief om een federatieve data- en cloudinfrastructuur te ontwikkelen en is sinds 2020 operationeel in de vorm van een Europese stichting. Inmiddels heeft de stichting meer dan 350 leden verspreid over de hele wereld. Door de start van het cloudinfrastructuur-project Structura-X en de recente lancering van het Gaia-X Digital Clearing House (GXDCH) (1) ontstaat er ook voor Nederlandse cloudaanbieders momentum om actief aan te sluiten.

Niet-Europese partijen beheren momenteel grotendeels de Europese digitale infrastructuur en data. Partijen uit de VS hosten inmiddels zelfs al meer dan negentig procent van de westerse data. Om die afhankelijkheid tegen te gaan hebben marktpartijen en onderzoeksinstituten de krachten gebundeld in Gaia-X.

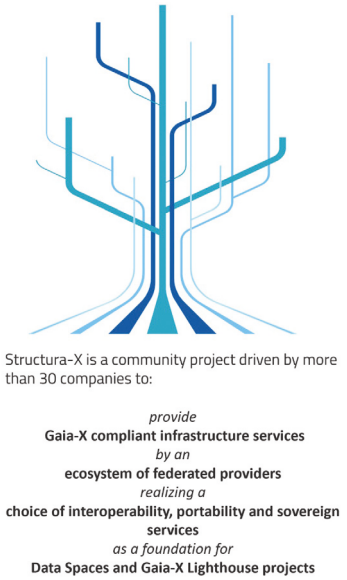
Het Gaia-X framework

Het initiatief ontwikkelt het Gaia-X framework (2) dat bestaat uit specificaties en software om gefedereerde data-ecosystemen op te zetten en te beheren. De federaties die het framework gebruiken kunnen het zowel inzetten ten behoeve van het uitwisselen van vertrouwde data als het aanbieden van vertrouwde clouddiensten. In beide situaties maakt de software van het framework het mogelijk om vertrouwd met elkaar samen te werken en ook uitspraken over onder meer veiligheid en compliance automatisch te verifiëren. Gaia-X is daarnaast bezig met het ontwikkelen van verschillende complianceniveaus voor diensten die onder de regels van een ecosysteem aangeboden worden.

Digitale soevereiniteit in cloudlandschap via Structura-X

Op dit moment zijn er binnen Gaia-X tien lighthouse projecten actief. Deze projecten hebben als doel om Gaia-X daadwerkelijk in een operationele setting te gaan toepassen. Waar negen van de tien projecten zich richten op toepassing ten behoeve van data-uitwisseling in specifieke sectoren, richt het Structura-X project zich op de ontwikkeling van federaties van cloudinfrastructuur-aanbieders. In Structura-X werken inmiddels meer dan dertig organisaties in Europa samen om in volledige overeenstemming met de Gaia-X richtlijnen een federatief clouddienstaanbod op te zetten. Daarnaast wil het project de interoperabiliteit, portabiliteit en uitwisselbaarheid van clouddiensten sterk verbeteren.

Voor afnemers van infrastructuur en platformdiensten zal hierdoor meer keuzevrijheid ontstaan en wordt daarmee een belangrijke stap gezet naar meer digitale soevereiniteit. Daarnaast concludeert de ACM in zijn recente marktstudie (3) dat lock-in effecten grote invloed hebben op de concurrentiedynamiek. Om concurrentie tussen cloudaanbieders te verbeteren is uitwisselbaarheid van clouddiensten een noodzakelijke voorwaarde.



Structura-X marks an important milestone in the evolution of Gaia-X, aiming to realise the first example of Federation of Infrastructures.

Francesco Bonfiglio, CEO, Gaia-X

Realisatie van een nationale testomgeving

Met steun van de Nederlandse Gaia-X hub, mogelijk gemaakt door het ministerie van Economische Zaken en Klimaat, realiseren TNO, BIT, Intermax, Info Support, SURF en AMS-IX een nationale testomgeving. Deze testomgeving wordt in eerste instantie opgezet op basis van de open-source technologie Kubernetes. BIT, Intermax en SURF koppelen hun onafhankelijk beheerde Kubernetes-clusters in combinatie met het open-source project Liqo (4) met elkaar via private VLAN van de Amsterdam Internet exchange (AMS-IX). Info Support verzorgt de health monitoring in de gefedereerde testomgeving en TNO verzorgt de technische integratie en validatie van een aantal technische use cases. In latere fases zullen ook andere technische- en organisatorische federatievormen aan de testomgeving worden toegevoegd, waarin nieuwe deelnemers ook welkom zijn om aan te sluiten. Uiteindelijk moet de mogelijkheid om aan te sluiten met de ontwikkelingen voor Gaia-X voor elk bedrijf openstaan.

Gefaseerde uitrol: van nationale testopstelling naar Europese testinfrastructuur

De betrokken partijen beproeven in de eerste fase of data en berekeningen technisch van cloudprovider naar cloudprovider kunnen verhuizen. Daarnaast test men in hoeverre capaciteiten van verschillende cloudproviders met elkaar te combineren zijn (‘scale out scenario’). Het doel is om in volgende fases de Nederlandse omgeving te koppelen aan Italiaanse, Duitse en Belgische testomgevingen om de verschillende federatievormen ook over de landsgrenzen heen te bewerkstelligen.

Met het opzetten van deze Europese testinfrastructuur kunnen cloudproviders de benodigde ervaring opdoen om uiteindelijk tot een commercieel afgestemd dienstaanbod te komen in een open ecosysteem. Interoperabiliteit van het dienstenaanbod is hierbij een speerpunt van het Structura-X project. Het verkrijgen van een gevalideerd Gaia-X label is echter geen onderdeel van deze eerste fase; daar is nog verdere ontwikkeling voor nodig. Het is dus goed om de ontwikkelingen te blijven volgen.

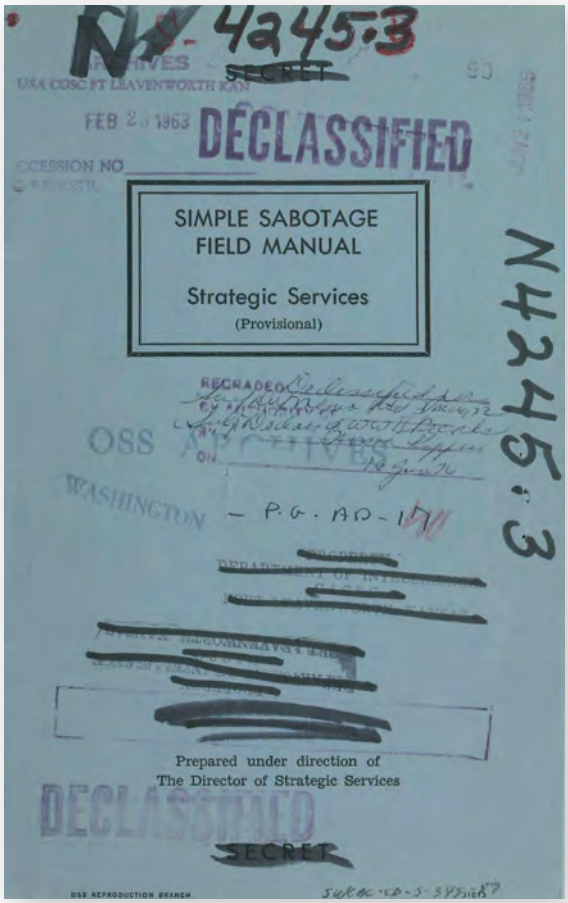
Centre of Excellence for Data Sharing and Cloud

De Nederlandse Gaia-X Hub is sinds 1 januari 2023 onderdeel van het nieuw opgerichte Centre of Excellence for Data Sharing & Cloud (CoE-DSC) (5). Is jouw organisatie geïnteresseerd om aan te sluiten bij deze ontwikkelingen? Neem dan contact op via hub@gaia-x.nl.

Referenties

(1) Market-X Conference & Expo: Gaia-X Digital Clearing House (GXDCH) a success for the industry, https://gaia-x.eu/news/latest-news/market-x-conference-expo-gaia-x-digital-clearing-house-gxdch-a-success-for-the-industry/
(2) Gaia-X framework, https://docs.gaia-x.eu/framework/
(3) ACM Marktstudie clouddiensten, https://www.acm.nl/nl/publicaties/marktstudie-cloud-diensten
(4) Computing Without Borders: The Way Towards Liquid Computing, https://liqo.io/
(5) Centre of Excellence for Data Sharing and Cloud van start https://www.tno.nl/nl/newsroom/2023/03/start-centre-excellence-for-data-sharing/

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



Bron afbeelding:
https://www.amazon.nl/s?k=simple+sabotage+manual&__mk_nl_NL=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=3PFR3WTQXY0JI&sprefix=simple+sabotage+manual%2Caps%2C81&ref=nb_sb_noss

BLOG

Saboteren van vergaderingen en productiviteit dankzij de CIA

In 1944 bracht het Office of Strategic Services (OSS), voorloper van de CIA, het 'Simple Sabotage Field Manual' uit, met daarin tactieken om de vijand te demoraliseren. Waaronder acht ongelooflijk subtiele en verwoestende tactieken om besluitvormingsprocessen van organisaties te verzieken.

De handleiding is tientallen jaren oud, maar deze sabotagetactieken liggen nog steeds op de loer in organisaties. Komen ze je bekend voor? Draai je eigen gedrag dan voortaan om.

Voorzitters van overleggen, boards en tafels:

1. Dring erop aan om alles via (de juiste) 'kanalen' te doen. Noem dit 'langs de as van …'. Sta nooit 'shortcuts' toe om beslissingen te versnellen.
2. Houd 'toespraken'. Praat zo vaak en zo lang mogelijk. Maak je punt duidelijk via lange anekdotes en impressies van je persoonlijke ervaringen. Benadruk steeds 'dat we het samen moeten doen'.
3. Laat zo veel mogelijk onderwerpen door commissies uitzoeken en uitwerken. Maak die commissies zo groot mogelijk (minimaal vijf personen).
4. Breng zo vaak mogelijk irrelevante kwesties ter sprake.
5. Kibbel over precieze bewoordingen van communicatie-uitingen, notulen en voorstellen. Stel de 'toon van het debat' ter discussie.
6. Verwijs naar zaken die eerder zijn besloten en probeer deze beslissingen opnieuw ter discussie te stellen.
7. Bepleit 'voorzichtigheid'. Wees 'redelijk' en dring erop aan dat de andere deelnemers ook 'redelijk' zijn. Vermijd haast, die later tot verlegenheid of problemen kan leiden.
8. Wees bezorgd over de gepastheid van een beslissing - stel de vraag of de overwogen actie wel binnen de jurisdictie van de vergaderende groep valt of dat deze in strijd zou kunnen zijn met het beleid van een hoger echelon.

De OSS geeft ook tips aan managers en (kantoor)medewerkers, zie hierna. In 1944 was er nog geen e-mail en werd nauwelijks software ontwikkeld. In de vertaling heb ik dat aangepast naar 2023.

Managers en toezichthouders (1):

1. Vraag altijd om schriftelijke opdrachten, om 'het voor iedereen, ook de werkvloer, duidelijk te maken'.
2. Begrijp opdrachten 'verkeerd'. Stel eindeloos vragen of voer lange correspondenties over die opdrachten. Blijf volhouden dat het eerst onduidelijk was: 'hoe kan ik nou weten dat een dienstwagen alleen voor *dienstreizen* is?'.
3. Doe al het mogelijke om levering van gevraagde diensten of producten (nu: 'deliverables') te vertragen. Ook al zijn delen van een bestelling eerder gereed, lever hem pas af als deze volledig klaar is. Dit advies is nog van vóór uitvinding van de waterval-ontwikkelmethode, maar ook een (kleinere) sprint-oplevering kun je zo saboteren.
4. Bestel nieuw werkmateriaal (zoals nu ook laptops, telefoons, toegangspasjes, leaseauto's, parkeervergunningen) pas wanneer uw voorraad vrijwel is uitgeput. Dan blokkeert reeds de kleinste vertraging bij het uitvoeren van uw bestelling het complete primaire proces.
5. Bestel uitsluitend hoogwaardige materialen ('zware laptops' en 'senior scrummasters met tien jaar ervaring van maximaal 23 jaar') die moeilijk te krijgen zijn. Als je ze niet krijgt, maak er dan ruzie over, bijvoorbeeld met interne recruiters. Waarschuw luid dat inferieure materialen inferieur werk betekenen.
6. Schrijf bij het maken van werkopdrachten eerst de *onbelangrijke* taken uit. Wijs de belangrijke opdrachten toe aan inefficiënte medewerkers. Geef hen te lichte computerkracht of te weinig (cloud)servers.
7. Dring aan op perfectie in relatief onbelangrijke producten (zoals urenverantwoordingen bij een niet-doorbelaste afdeling of onkostendeclaraties voor wekelijks dezelfde dienstreis). Stuur een auto terug voor het overspuiten van de kleinste lakfout. Keur een complete security awareness campagne een dag voor de uitrol af omdat op één poster 'die hele securityshit' staat. Keur andere defecte onderdelen, waarvan de gebreken niet meteen met het blote oog zichtbaar zijn, juist goed zodat ze verderop in het proces problemen geven: 'ja, het is niet perfect ik weet het, maar ik heb de directie beloofd dat we morgen live gaan'.
8. Maak fouten in het doorsturen van onderdelen, materiaal en informatie, zodat ze naar de verkeerde plaats in de fabriek of organisatie worden gestuurd. En dus niet arriveren waar ze werkelijk nodig zijn.
9. Geef bij het opleiden van nieuwe werknemers onvolledige of misleidende instructies.
10. Wees, om het moreel en de productie te verlagen, heel vriendelijk voor inefficiënte werknemers; geef hen onverdiende promoties. Discrimineer efficiënte harde werkers en klaag onterecht over hun werk: 'zij brengt véél te veel securityrisico's voor dit project in kaart'.
11. Houd conferenties (heel groot, op een plaats waar *alle* deelnemers veel reistijd hebben) wanneer er meer belangrijk werk te doen is.
12. Vermenigvuldig papierwerk op ogenschijnlijk geloofwaardige manieren. Maak een schaduw-administratie en bewaar dubbele bestanden.
13. Vermenigvuldig procedures en toestemmingen die nodig zijn voor het geven van instructies, uitbetalen van declaraties, enzovoort. Zorg dat drie mensen (van steeds hogere managementlagen-) alles moeten goedkeuren waar één persoon voldoende zou zijn.
14. Pas alle voorschriften toe tot op de laatste letter.

Komen deze sabotagetactieken je bekend voor? Draai je eigen gedrag dan voortaan om.

Kantoorklerken (2):

1. Maak fouten in de hoeveelheden materiaal (opslagruimte, uitzendkrachten, cloudcapaciteit) bij het doorsturen van bestellingen. Verwar vergelijkbare persoonsnamen: 'oh, die *andere* Steef Jansen, die echter niet in de directie zit?'. Gebruik verkeerde (mail)adressen.
2. Verleng de (meestal toch al lange) correspondentie met overheidsinstellingen.
3. Berg essentiële documenten verkeerd op: verkeerde afdelingsschijf of map. Gebruik een onduidelijke filenaam.
4. Maak van doorslagen (carbonpapier, wie kent het nog!) van brieven er één te weinig, zodat een extra kopieeropdracht moet worden uitgevoerd. Dit kan nu ook met afdrukken van vergaderstukken en iemand 'vergeten' in de adresregel van e-mails.
5. Vertel belangrijke bellers dat de baas bezet is of 'in een call zit' (terwijl dat toevallig een keer *niet* zo is).
6. Post ophouden tot de volgende ophaalronde. Nu kan dit nog door alleen het eerste halfuur van de werkdag je e-mails te lezen en erop te reageren. Of: 'ja, ik zit wel in die whatsapp-groep, maar ik lees het eigenlijk nooit'.
7. Verspreid verontrustende geruchten die klinken als insiderinfo. Laat dergelijk 'fake news' per ongeluk op de afdelingsprinter liggen.

Productiemedewerkers

1. Werk langzaam. Vergroot het aantal bewegingen dat nodig is voor je werk: gebruik een lichte hamer en geen zware, een kleine moersleutel in plaats van een grote, gebruik weinig (denk) kracht waar veel kracht nodig is.
2. Laat je werk zoveel mogelijk onderbreken: neem bij veranderen van materiaal waarop je werkt (zoals op draaibank of pons), onnodig de tijd om dit te doen. Als je snijdt, vormgeeft of ander 'gemeten werk' doet, meet dan afmetingen - twee keer zo vaak als nodig is. Blijf langer op het toilet dan nodig is. Vergeet gereedschap (zoals vergaderstukken) zodat je het moet gaan halen.
3. Doe alsof je instructies in een vreemde taal niet snapt, zelfs als je die taal (Engels) wel begrijpt.
4. Doe net alsof instructies moeilijk te begrijpen zijn en vraag om ze meer dan eens te herhalen. Of zeg dat je graag je werk heel goed wilt doen en val de chef lastig met onnodige vragen: 'was Sigma er nou eerst of juist Lean?'.
5. Voer je werk slecht uit en geef slecht gereedschap de schuld. Klaag dat dit je belemmert je werk goed te doen. Dit is nog te versterken door over collega's te klagen.
6. Geef je vaardigheden en ervaring nooit door aan een nieuwe of minder bekwame werker.
7. Vertraag administratie op alle mogelijke manieren. Papieren formulieren onleesbaar invullen, zodat ze overgedaan moeten worden. Fouten maken of gevraagde informatie weglaten in digitale formulieren.
8. Indien mogelijk, sluit je aan bij of help bij het organiseren van een groep om problemen van werknemers aan het management voor te leggen. Zorg dat de gekozen procedures zo onhandig mogelijk zijn voor het management: laat een groot aantal werknemers bij elke presentatie aanwezig zijn, organiseer meer dan één bijeenkomst voor elke klacht, stel problemen aan de orde die grotendeels denkbeeldig zijn, enzovoort.

Voetnoten

(1) Nu: leidinggevenden, maar soms zien ze alleen toe op wat toch al gebeurt of wat 'hun' medewerkers uit zichzelf reeds doen.

(2) Nu: staf- of beleidsmedewerkers, als een andere groep kantoorwerkers dan productiemedewerkers in bijvoorbeeld een verzekeringsbedrijf.

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

COLUMN MARTIJN

Voor de afwisseling op mensen jagen

Eens per jaar mag ik mijn digitale skills inzetten om op mensen te jagen. Dit in het tv-programma Hunted waarin ik de rol van digitaal rechercheur binnen een team van specialisten op het gebied van opsporing vervul. Het is weer bijna zover en in mijn hoofd ben ik al druk bezig met de voorbereidingen. Op welke fouten die ik de voortvluchtigen vorig jaar zag maken, wil ik dit jaar inspelen? Hoe zijn cloudaccounts en digitale sporen veranderd het afgelopen jaar? Is er iets veranderd in de bevoegdheden van de politie en inlichtingendiensten of in de toepassing daarvan?

Mocht je het programma niet kennen: twaalf normale burgers zijn drie weken op de vlucht voor een opsporingsteam. In die tijd proberen de 'voortvluchtigen' informatie te verkrijgen over het extractiepunt waar ze, als ze daar op de laatste dag aankomen, het land kunnen verlaten om zo het programma te winnen. Voor mij betekent het programma drie weken lang op het hoofdkwartier zitten. Daar voegen we alle informatiebronnen over de voortvluchtigen samen om vervolgens op basis van die informatie opsporingsteams in het land aan te sturen zodat zij de deelnemers op kunnen pakken. Naast dat het een entertaining programma is, proberen we het onderwerp privacy in Hunted sterk te belichten. Zo willen we bijvoorbeeld laten zien wat er in Nederland en daarbuiten allemaal over je wordt opgeslagen.

Ik zal dus binnenkort weer drie weken lang in een hok, zonder ramen, zitten. Doorwerkend in het weekend met een continu gevoel van stress over loslopende 'voortvluchtigen'. Toch vind ik het heerlijk! In mijn dagelijkse werk kom ik gigantisch veel bedrijven tegen die getroffen zijn door cybercriminelen. We doen altijd (uitgebreid) digitaal onderzoek, maar helaas worden ze niet vaak gepakt. Tijdens Hunted krijg ik die voldoening vaak wel en hoewel het geen echte criminelen zijn, voelt het goed om in rap tempo een bijdrage te kunnen leveren met de digitale middelen die we tot onze beschikking hebben. Daarnaast is het stiekem ook hartstikke leuk om het team weer te zien en samen te werken. Een beetje alsof je teruggaat naar je kindertijd en je je vriendjes van zomerkamp weer ziet!

Een leuke actie tijdens Hunted waren twee voortvluchtigen die hun Google Assistant gebruikten om een wekker te zetten. Ze waren zich er totaal niet van bewust dat ze hiermee op de achtergrond hun Google-account gebruikten. Het was zelfs een account waarbij ze het vinkje voor spraakverbetering aan hadden gezet. Hierdoor kon ik niet alleen de activiteit zien, maar zelfs het audioclipje downloaden. Het clipje even uitluisteren gaf de bevestiging dat het om de voortvluchtigen ging: de opsporingsteams doken er meteen op.

Destijds kreeg ik zelfs van de productiemedewerkers van het programma verbaasde reacties over wat er allemaal wordt opgeslagen in een Google-account. Een andere keer stuurden we 'phishingmails' naar e-mailaccounts waarvan we wisten dat deze gebruikt gingen worden door voortvluchtigen. Twee deelnemers klikten op de link en een kwartiertje later waren ze in de boeien geslagen.

Ik ben weer benieuwd wat het nieuwe seizoen gaat brengen. En hopelijk kunnen we Nederland weer wat wijzer maken op het gebied van (digitale) privacy!

Auteurs: Saman Tamo en Miguel Chehin. Saman Tamo is sinds 2015 docent-onderzoeker cybersecurity aan de Haagse Hogeschool. Hij is sinds 2022 ook actief als ondernemer bij CTRL Disrupt, waar hij met zijn collega's een bijdrage wil leveren aan een digitaal veilige samenleving en kennisdeling op het gebied van cybersecurity. Hij is te bereiken via: Saman@ctrl-disrupt.nl. Miguel Chehin is werkzaam als security consultant bij CTRL Disrupt. Hij is te bereiken via: Miguel.chehin@ctrl-disrupt.nl.

Context Driven Data Gathering Framework

Data Gathering is an often overlooked step in the process of improving data analysis. Data analysts go through countless data streams whilst trying to filter relevant from irrelevant data. This data analysis process is time consuming and costly, often resulting in analysts spending the majority of their time on filtering out irrelevant data instead of focusing on analysing the data that is important to their organisation. In this framework we aim to provide structure to the process that foregoes data analysis, namely *data gathering*. To improve the quality and relevancy of the data you collect and thereby minimize the strain on data analysts.

When analysts are exposed to a huge amount of irrelevant material, analyst fatigue can develop. This condition may lead to fatigue, burnout, and decreased productivity, which could have detrimental effects on businesses (1). Organisations may suffer major repercussions because of analyst fatigue brought on by irrelevant data. It may result in lost opportunities, incorrect data interpretation, and subpar decision-making. Thus, it is crucial that businesses take action to reduce this issue (2).

There are several areas where you can find sources of unrelated data. Open-source intelligence (OSINT) feeds, for instance, might contain a lot of noise and misleading information when used for intelligence analysis. Users may upload inaccurate or irrelevant information on social media platforms, which can be another source of irrelevant data. Furthermore, a study from Oxford University shows that false positive triggers in event management systems such as SOCs and SIEMs could be responsible to false positive rates of up to 99%, thereby severly increasing the incoming amount of raw irrelevant data (3).

Whilst the focus on reduction in false positive rates and filtering of (ir)relevance in data has primarily been done on the data analysis side, using methods such as, but not limited by:

- data clustering
- pattern tracking
- regressions
- predictions

We find that organisations should spend more effort on the step that priors' data analysis, therefore trying to up the quality and relevance of the data before any data analysis is applied.

Mapping your organisational context involves applying three levels of situational awareness in dynamic environments where decisions must be made frequently.

It should be noted that Context Driven Data Gathering does not eliminate or replace the need of further data analysis and filtering, but should be used to complement the analysis part and assist the analyst in working more efficient and effective.

By establishing and defining the context of your organisation, a well-designed method for gathering data can help your organisation to reduce irrelevant data. Establishing specific goals will help to focus data collection efforts on the most important information and lessen over-saturating analysts with unnecessary data (4).

This strategy should prioritize data sources based on your organisational needs, that are most likely to have pertinent information. Thus, this prioritization is likely to reduce the volume of irrelevant data that analysts must filter through, which would lead to reduced time spend on analysing what is not relevant to your organisational needs (5).
In order to define data as pertinent or irrelevant it is important to lay the grounds on what data could be seen as important in the first place. This framework will focus on assisting you in mapping the organisational context and possible relevance of data based on the importance it has for the enterprise levels within your organisation. This Framework distinguishes 3 enterprise levels into Strategic, Tactical and **O**perational (**STO**).

Step1 Requirements

The requirements stage is critical to a successful Context Driven Data Gathering process. During this phase, the team determines the intelligence program's objectives and operating procedures based on stakeholder requirements. Organisational context and situational awareness are essential to proper data gathering. Mapping your organisational context involves applying three levels of situational awareness in dynamic environments where decisions must be made frequently. A proposed way to map your organisational context is to apply three levels of **S**ituational **A**wareness (**SA**) (6)(7).

Level 1 SA: Perception of the Elements in the Environment

It is important to be aware of what is needed and present within your organisation to perform (daily) tasks and determine what key infrastructures one is dependent on.

To map the elements within your organisation you can start by logging:

- what kind of software is our organisation using, such as applications and operating systems;
- what types of hardware is the organisation using;
- which of those elements are locally managed versus outsourced and
- what could be the possible attack surface of your organisation.

The Importance of the perception of these environmental elements became clear when the renowned log4shell zero day was used to execute arbitrary code in Apache's log4j, with countless organisations not being aware of the fact that they were making use of Apache's log4j in the first place, thus being vulnerable to the exploit (8)(9).

Level 2 SA: Comprehension of the Current Situation

After your organisational perception of elements are consciously mapped and documented, it becomes of importance to comprehend and understand your organisational needs. This way, you are able to change the perimeters of data you are willing to find and focus on what is relevant and important to your organisation.
One way to do that, is to break the organisation down into 3 enterprise layers (**STO**): **S**trategic **- T**actical – **O**perational. The concept behind this approach is to acquire data more consciously, it is crucial to be aware of the needs and desires of your company at several levels (strategic, operational, and tactical).

Efficiency: you can concentrate on gathering data that is pertinent and practical when you have a clear understanding of the data requirements for your firm. By preventing the collecting of unnecessary data, you can save time and money. Accuracy: being aware of the precise information that is wanted at various levels, helps you gather the proper data to satisfy those needs. This implies that the data you gather will be more relevant and beneficial for making decisions and conduct analyses on. Relevance: as each level of the organisation has different information needs, it is crucial to gather information that is pertinent to that level.

Level 3 SA: Projection of Future Status

Level 3 situational awareness involves predicting how the environment will behave and impact your organisation in the near future. Understanding the dynamics and status of the elements at Levels 1 and 2 is necessary for this. For example, if your organisation uses a certain Linux Distribution, you can search for vulnerabilities or news relevant to it. Also, if the strategic layer of your organisation plans to do business with foreign countries, you should monitor for possible conflicts that could affect the mission and vision of your organisation. Without situational awareness, crucial data could be missed.

Step 2 Data Collection

Finding the right data collection tools based on your organisational context is important, because it allows an organisation to tailor its data collection process to its specific needs and goals. Different tools are used to collect different types of data from different sources, while the list of possible data collection methods and tools is very large, we would

like to give you a few tooling suggestions to cater your data gathering needs. It is important to understand that tools can be used to gather data on all enterprise levels and are not limited to a single **STO** enterprise level.

We recommend looking at the GitHub Repository listed at (10), containing a curated list of various tools, to be used for data gathering. However, this list is finite and various other tools, that are preferred within your organisation, naturally can be used as well.
Depending on the needs and wants of your organisation there are specific sources that focus on certain types of news, for example: Where the RSS feeds of the National Cyber Security Centre (NCSC) excels in providing well-structured and documented data relevant to imminent or potential (operational) cyber threats, such as the announcement of a vulnerability in software, it will most likely lack in notifying you when there are geopolitical conflicts unfolding between the countries you might be dependent on, or operating in.
Combining the right sources and tooling (11) is of crucial importance to organisational data needs, with proper mapping of the Situational Awareness levels.

Step 3 Data processing & post analysis

Raw data needs to be processed before analysis. This involves tasks such as putting data into spreadsheets, decrypting files, translating foreign language data, and assessing data reliability. Pre-processing improves the value of data analysis by cleaning, normalising, and transforming the data, making it consistent and usable. This saves time and allows for structured, automated, and manual analysis of the most relevant data.

Finally, the data review is a critical component of Context Driven Data Gathering. After processing the data, a thorough analysis is needed to answer the questions mapped during the requirements phase. The team works to translate the dataset into useful recommendations for stakeholders. This iterative process requires constant maintenance and adjustments to stay aligned with the organisation's mission and vision across enterprise levels. Staying up-to-date with relevant data gathering is crucial.

Conclusion

The Context Driven Data Gathering Framework aims to reduce the amount of irrelevant data that analysts have to filter through, thereby reducing analyst fatigue and improving decision-making. By establishing and defining the context of the organisation and prioritizing data sources based on organisational needs, the framework can help organisations to collect higher quality and more relevant data, ultimately leading to more efficient and effective data analysis.

References

(1) Pherson, R.H. and Heuer, R.J. (2021) Structured Analytic Techniques for intelligence analysis. Thousand Oaks, CA: CQ Press.
(2) "Closing the Data Decision Gap" (2022), March. Available at: https://web-assets.domo.com/blog/wp-content/uploads/2022/03/Domo-The-DDG-Paper.pdf.
(3) Alahmadi, B.A., Axon, L. and Martinovic, I. (no date) 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms. Oxford University. Available at: https://www.usenix.org/system/files/sec22summer_alahmadi.pdf
(4) Kabir, S. M. S. (2016). Methods Of Data Collection Basic Guidelines for Research: An Introductory Approach for All Disciplines (first ed., pp. 201-275).
(5) Schönberger, M. and Cukier, K. (2013) Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt.
(6) Endsley, M.R. (no date) Designing for Situation Awareness in Complex System. SA Technologies, Inc. Available at: https://www.researchgate.net/profile/Mica-Endsley/publication/238653506_Designing_for_situation_awareness_in_complex_system/links/542b1ada0cf29bbc126a7f35/Designing-for-situation-awareness-in-complex-system.pdf
(7) Jakalan, A. H. M. A. D. (2013). Network security situational awareness. The Int. J. of Comp. Sci. and Commun. Secur. (IJCSCS), 3, 61-67
(8) Vijayan, J. (2022) DHS Review Board deems Log4j an 'endemic' cyber threat, Dark Reading. Available at: https://www.darkreading.com/application-security/dhs-review-board-deems-log4j-an-endemic-cyber-threat (Accessed: March 24, 2023).
(9) Inc., S. (no date) LOG4J updates and vulnerability resources, Sonatype. Available at: https://www.sonatype.com/resources/log4j-vulnerability-resource-center (Accessed: March 24, 2023).
(10) https://github.com/hslatman/awesome-threat-intelligence#tools
(11) https://github.com/hslatman/awesome-threat-intelligence#frameworks-and-platforms

Ruimte voor een brede juridische blik binnen onze redactie

Informatiebeveiliging kent naast organisatorische en technische aspecten nog vele andere raakvlakken. Het juridische raakvlak is er daar één van en de ontwikkelingen op dit vlak zijn talrijk en gaan snel. ICTRecht is daarom verheugd om voor de toekomstige edities van het IB Magazine op regelmatige basis een bijdrage te leveren om lezers van het magazine op de hoogte te houden.

ICTRecht is in 2004 door Steven Ras opgericht. In de beginfase bestonden de werkzaamheden vooral uit het geven van juridisch advies aan hostingproviders en webwinkels. Al snel volgden het opstellen van ICT-contracten, het oplossen van domeinnaamgeschillen en het adviseren over aansprakelijkheidsvraagstukken. Met de komst van Arnoud Engelfriet in 2008 groeide het kantoor uit tot een compleet adviesbureau voor ICT, privacy en internet in het algemeen. De afgelopen jaren is er daarnaast een sterke focus ontstaan op informatiebeveiliging en legal tech, met twee nieuwe businessunits als gevolg. Op dit moment adviseren wij met meer dan 180 specialisten over zaken op het snijvlak van recht, security en tech vanuit zes locaties: Amsterdam, Groningen, Maastricht, Eindhoven, Enschede en Brussel. ICTRecht bedient hierbij een klantenbestand van start-up tot multinational en van overheidsinstantie tot zorginstelling.

Onze visie op informatiebeveiliging

Door technologische ontwikkelingen en de toename van data nemen zowel de mogelijkheden als de risico's toe. Organisaties zijn voor hun bedrijfsvoering in grote mate afhankelijk van hun informatie en informatiesystemen: als informatie niet beschikbaar is, niet correct is of in verkeerde handen valt, kan aanzienlijke schade ontstaan en kan de continuïteit van de bedrijfsvoering in gevaar komen. Het is dan ook niet verwonderlijk dat de maatschappij, maar ook wetgevers, toezichthouders en andere stakeholders, steeds hogere eisen stellen als het aankomt op de beveiliging van (al dan niet privacygevoelige) informatie. Informatiebeveiliging is wat ons betreft geen doel op zich – het staat ten dienste van de organisatie en haar bedrijfsvoering. Het is onmogelijk om alle informatiebeveiligingsrisico's tot nul te beperken. Waar het, wat ons betreft, om draait, is dat organisaties in control zijn over hun data en IT-landschap, dat er bewuste en weloverwogen keuzes worden gemaakt als het gaat om de beveiliging daarvan. Hierover moet ook verantwoording kunnen worden afgelegd. Dat kan door informatiebeveiliging niet alleen technisch, maar ook organisatorisch en procesmatig goed in te richten. Dat is geen eenmalige oefening, maar een continu proces waarbij de gehele organisatie zoveel mogelijk betrokken dient te worden.

Onze bijdragen

Voor toekomstige edities van het IB Magazine zullen verschillende auteurs van ICTRecht een bijdrage leveren. Naast onderwerpen die informatiebeveiliging raken, zullen wij ons ook toeleggen op ontwikkelingen en onderwerpen die in de belangstelling staan, zoals: kunstmatige intelligentie, privacy, leveranciersmanagement en nieuwe wet- en regelgeving zoals de Medical Device Regulation (MDR) en de Wet elektronische gegevensuitwisseling in de zorg (Wegiz).

Naschrift redactie:
Het is voor informatiebeveiligers een goede zaak om op hoogte te blijven van de ontwikkelingen binnen en rond ons vakgebied. Gewoontegetrouw gaan wij al diep in op de (ICT-)technische en organisatorische aspecten. Om onze kwaliteit als magazine en de brede kennis van onze leden/lezers verder te ondersteunen meenden wij dat het juridische vlak niet mag ontbreken. Vandaar dat wij ICTRecht hebben benaderd. Wanneer je deze eerste kennismaking wil verdiepen, bezoek dan: https://blog.iusmentis.com/

In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

'Onze' GAIA-X omgeving

Zeven Nederlandse partijen vangen aan met de bouw van 'onze' GAIA-X omgeving. Deze omgeving zal naar verwachting medio mei gereed zijn om te kunnen testen en onderzoeken of en hoe cloudaanbieders voldoen aan de regels van het Europese platform. De Duitsers, Italianen en Belgen gingen ons voor. Het uiteindelijk doel is uiteraard om een alternatief te kunnen bieden voor de Amerikaanse cloudgiganten die de markt momenteel domineren. Afgelopen februari zei staatssecretaris Van Huffelen nog dat GAIA-X nog niet groot genoeg was om een alternatief te bieden. Zou het nu dan toch echt gaan gebeuren? Aan het woord onze redactieleden.

Leo van Koppen - 'Beter ten halve gekeerd dan ten hele gedwaald'

GAIA-X, het Europese antwoord op de cloudoverheersing van de Amerikaanse techreuzen. Althans of het echt een antwoord gaat zijn, zal de tijd moeten leren. Mijn eerste reactie is wel enigszins cynisch: 'nu al?'. Op het moment dat alle grote en inmiddels ook kleinere bedrijven en overheden de overstap naar de cloud hebben gemaakt, wordt een Europees antwoord gegeven op de dominantie van Google, Microsoft en Amazon.

Voor GAIA-X worden partners uitgenodigd, iedereen kan deelnemen aan dit project waarvoor alvast tien miljoen euro in de eerste fase beschikbaar is gesteld. Hebben ze in Brussel al die tijd zitten slapen en zijn ze nu eindelijk als *gevolg van een boze droom ontwaakt? Welke enge droom is dat dan geweest? En waarom niet veel eerder gestart met een dergelijke strategie?*

Het antwoord op de eerste vraag ligt voor de hand. Het gaat natuurlijk om de Europese 'kroonjuwelen': kunnen we de BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid) van deze kroonjuwelen waarborgen? Op dit moment is het antwoord 'NEE', want Amerikaanse wetgeving kan de garanties van Microsoft e.a. overrulen. Nu is de VS onze bondgenoot en loopt het misschien zo'n vaart niet, maar dan nog: de CIA is per definitie nieuwsgierig en daarbij, wie garandeert dat onze relatie met de VS zo blijft? Wie weet, verandert dat na de Amerikaanse verkiezingen in rap tempo. Kortom: het antwoord op deze vraag levert een rechtvaardiging op voor het vinden van een veilige haven. GAIA-X zou dat kunnen zijn of beter gezegd: zou het kunnen worden.

Blijft over de tweede vraag. *Waarom nu pas?* Het antwoord op die vraag is niet zo eenvoudig te geven, maar ik denk dat ik het antwoord wel kan raden. Het zal wel te maken hebben met het trage Europese overheidsapparaat. Voordat politici vinden dat er iets moet gebeuren, is er al veel tijd verloren gegaan. Die technologielobby werkt blijkbaar nog niet zo goed daar in Brussel.
Voordat het Europees Parlement heeft beslist, een plan klaar


Leo van Koppen | Maarten Hartsuijker | Fook Hwa Tan

heeft en er geld voor heeft vrijgemaakt, zijn we zomaar vijf jaar verder. Immers de eerste ideeën werden al in 2018 vastgelegd en in 2020 werd het besluit genomen. Daarmee is nog maar een eerste begin gemaakt, want in een publiek-private samenwerking moet het geld voor realisatie óók vanuit de markt komen. Iets waar nu met belangstelling naar wordt uitgekeken.

Kortom: het gaat nog even duren voordat de 'Europese kroonjuwelen' veilig in de eigen omgeving kunnen worden opgeslagen. *Te laat* neig ik te denken, nu we ons hart al hebben verpand aan Azure, AWS of Google. Hoezo geen 'vendor lock-in'? Ga het allemaal maar weer eens opnieuw inrichten in die nieuwe veilige omgeving. Terwijl de overstap naar de cloud nog nauwelijks is afgerond. Dat brengt ook risico's en kosten met zich mee.
Wellicht is het dan toch de samenkomst van een aantal zaken die dit project zal laten slagen:

1. het gevoel van urgentie, ingegeven door een snel veranderende wereld als gevolg van de Russische inval in Oekraïne,
2. het verworven inzicht in de risico's die gepaard gaan met de nieuwe cloudstrategieën van de verschillende overheden en
3. het nieuwe elan om zaken die we 'hier in eigen huis' in technologische zin ook wel kunnen realiseren ook in 'eigen huis' te behouden.

Het initiatief komt naar mijn idee veel te laat (zoals zo veel zaken uit Brussel veel te laat komen) en kost daardoor onnodig veel extra inspanningen en geld. Maar ja, 'beter ten halve gekeerd dan ten hele gedwaald'. Het zal zijn beslag wel krijgen op termijn, maar het verdient zeker geen schoonheidsprijs wat mij betreft.

Maarten Hartsuijker - We maken het veel te moeilijk

Wanneer ik de afgelopen jaren klanten sprak over de beveiligings- en privacy impact van het wel of niet gebruiken van de Amerikaanse cloud, twijfelde men vaak om dezelfde reden: we weten dat er meer met onze data gebeurt dan we eigenlijk willen. Maar ze gingen (zeker tijdens COVID) vaak toch overstag om dezelfde redenen: we kunnen niet zonder, we willen dit niet meer zelf doen, er zijn geen Europese alternatieven die zo goed werken, de overheid gebruikt het zelf ook en er is toch geen handhaving op Schrems.
Als je hier als Europese samenleving iets aan wil doen, helpt een complex theoretisch model niet. Van drie jaar praten over specificaties, compliance labels en data ecosystemen worden alleen de gesubsidieerde praatclubs beter.
Wil je de bedrijven bereiken die nu massaal voor Azure en AWS kiezen, dan zul je supersterke concurrentie in de markt moeten zetten die IT-ontwikkeling en beheer tegen een scherpe prijs zo gemakkelijk maakt dat niemand nog zonder wil. Stop met ingewikkelde kaders, stelsels en interfaces en vraag 'gewone' klanten wat een Europese cloud moet bieden om hen als klant te kunnen verwelkomen. Het antwoord op die vraag is vermoedelijk makkelijker te begrijpen (én te realiseren) dan Gaia-X.

Fook Hwa Tan - Probeer kansen te zien!

Project Gaia-X is een veelbelovend project binnen de EU met zowel publieke als private partijen die deelnemen. Het ideaal om binnen de EU een eigen infrastructuur te creëren die aan Europese wet- en regelgeving voldoet, is iets waar organisaties naar op zoek zijn. Het is gebaseerd op een decentraal model dat veiligheid, betrouwbaarheid, interoperabiliteit en data portabiliteit moet waarborgen, binnen de grenzen van EU-wetgeving.

Zowel de VS als China beschikken echter al over grote cloudinfrastructuren die al veelvuldig worden gebruikt binnen de EU. Om nu een infrastructuur te ontwikkelen die moet concurreren met al volwassen buitenlandse partijen, is een zeer grote uitdaging.
Het is überhaupt de vraag of er iets opgezet kan worden dat kan concurreren met deze buitenlandse partijen. Worden door alle wensen en eisen de kosten niet te hoog voor Gaia-X partijen ten opzichte van de huidige partijen? Het is een publiek-private samenwerking, maar de EU kan hier in het kader van gelijke concurrentie niet te veel geld in steken. Het kan dan immers als staatssteun worden gezien.
Dit project is voornamelijk een samenwerking en afsprakenstelsel met betrekking tot de *software layer.* De vraag blijft natuurlijk nog bestaan hoe het zit met de onderliggende *hardware layer.* Moet die dan ook niet binnen de EU geproduceerd zijn om daadwerkelijk de gewenste beveiliging te behalen?
Kortom, dit project heeft tal van uitdagingen. Maar het moet ook gezegd: nu is er momentum. En gezien de geopolitieke sfeer zijn er mogelijk ook de financiële middelen om dit binnen de EU voor elkaar te krijgen. Laten we het daarom een kans geven om te bloeien!

PvIB Platform voor InformatieBeveiliging

COLOFON

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

HOOFDREDACTEUR
Chris de Vries

REDACTIE
Leo van Koppen
Bianca Brooijmans
Maarten Hartsuijker
Lilian Knippenberg
Rachel Marbus
Fook Hwa Tan
Chris de Vries

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

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

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
Veldhuis Media, Meppel

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

ABONNEMENTEN
De abonnementsprijs in 2023 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

TSTC

ICT en Security Trainingen

Ransomware? Log4j?

ADVANCE YOUR CAREER WITH SECURITY IN 2023

WR - Workshop Ransomware
EHE - Ethical Hacking Essentials
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v12
OSCP - Offensive Security PEN-200

GET SKILLED
WWW.TSTC.NL

Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

CEH - Certified Ethical Hacker
CHFI - Computer Hacking Forensic Investigator
CPENT - Certified Penetration Testing Professional
SSCP - Systems Security Certified Professional
OSCP - Offensive Security Certified Professional

SECURITY MANAGEMENT TRAININGEN

CISSP - Certified Information Systems Security Professional
CISM - Certified Information Security Manager
CISA - Certified Information Systems Auditor
CRISC - Certified In Risk And Information Systems Control
C|CISO - Certified Chief Information Security Officer

PRIVACY TRAININGEN

CIPP/E - Certified Information Privacy Professional / Europe
CIPM - Certified Information Privacy Manager
CIPT - Certified Information Privacy Technologist
CDPO - Certified Data Protection Officer

CLOUD SECURITY TRAININGEN

CCSP - Certified Cloud Security Professional

ISO TRAININGEN

ISO 27001 - Foundation
ISO 27001 - Lead Implementer
ISO 27001 - Lead Auditor
ISO 27005 - Risk Manager
ISO 27701 - Privacy Management

www.tstc.nl

Onze trainingen zijn weer klassikaal of Live Online te volgen