PvIB 15 reconnect in cyber security

ib

INFORMATIEBEVEILIGING MAGAZINE

- Interview met drs. Johan van den Bosch (MCM CISA agentschap Telecom projectleider CSA en NCCA): 'Securitycertificering steeds meer een Eurpese aangelegenheid'
- (Cyber)spieken mag gewoon!
- Column: Metaverse en het volgende virtuele hoofdpijndossier

JAARGANG 22 - 2022 - EDITIE 5

Verbinding door de verschillen

Nicole van Deursen

Een van de leukste dingen van het voorwoord schrijven is het vinden van de samenhang tussen de ogenschijnlijk uiteenlopende artikelen die we elke keer weer aangeleverd krijgen. Synoniemen voor samenhang zijn context en kader. Met alle verschillende perspectieven op ons vak en vaak uiteenlopende terminologie zijn het uiteindelijk de verschillen die ons verbinden. Redactielid Lilian schrijft in deze uitgave een ode aan de context. Een deel van de context in ieders werk zijn de normen en kaders die wij als mensen aan elkaar stellen, waardoor wij samen de sterke schakels vormen. Daarover schrijft Lex Borger in zijn blog en wij als redactie in Achter het Nieuws. Het derde artikel van TNO in de winnende iB-Magazine-artikel-van-het-jaar-2021-serie over SOC/CSIRT capabilities geeft weer meer inzicht in versterkende schakels. Een ander deel van onze context zit in de normen en kaders vanuit de Rijksoverheid. In deze uitgave maken we kennis met twee organisaties die een belangrijke rol spelen: Agentschap Telecom en ICTU. Vakgenoten helpen onze overheid ook waar ze kunnen. Jeroen Gaiser schreef een artikel over hoe het kwam dat hij de cyberspiekbriefjes kon aanbieden aan de Tweede Kamer. Zo dragen we allemaal op onze eigen wijze bij aan het versterken van onze samenhang. Blijf vooral zo doorgaan iedereen: vier de verschillende perspectieven en zoek juist daarop de verbinding. We hebben elkaar allemaal nodig.

Nicole

IN DIT NUMMER

Auteur: Lilian Knippenberg is senior information security officer en schrijft op persoonlijke titel. Ze is te bereiken via LinkedIn.

Ode aan de context

De context en omgeving van de organisatie waar je werkt zijn erg belangrijk. Niet alleen voor het type gegevens, maar ook omdat de mensen die er werken, de doelen die de organisatie nastreeft en de wensen van de directie allemaal specifiek voor die organisatie zijn. Hierbij een ode aan de context als startpunt, plus manieren om dit praktisch toepasbaar te maken.

Voordat ik een tweetal best practices bespreek, nodig ik je uit om even stil te staan bij wat jouw organisatie voor jou betekent. Waarom werk je waar je werkt? Wellicht heb je gekozen voor een bepaalde branche, zoals de gezondheidszorg of de overheid, of kies je voor IT-dienstverlening, een internationaal opererende organisatie of advocatenkantoor. Heb je specifiek gekozen voor deze werkgever? Waarom? Misschien sprak de filosofie of de culturele of religieuze achtergrond je aan. Misschien heb je zelf wel positieve ervaring bij de organisatie of was het zo simpel als nu eenmaal moeten werken voor je geld en maakt de context je niets uit. Ben je trots of blij met je werkgever? Zou je nog kunnen overstappen naar de directe concurrent of naastgelegen instelling? Die subtiele verschillen zijn belangrijk voor de cultuur van de organisatie en de mensen die er werken. En die verschillen maken de context! Sluit je met het informatiebeveiligingsprogramma daarbij aan, dan ben ik ervan overtuigd dat het programma meer succes heeft. Omdat jij voelt – en dus ook de medewerkers en andere stakeholders voelen – dat we informatieveiligheid samen nastreven voor hetzelfde doel.

De context in best practices: ISO en NIST

Goed, genoeg zachte overtuigingen, tijd voor de industry standards. Ik zoom in op ISO27001 en het NIST Cybersecurity Framework (CSF). Beide normen besteden aandacht aan de context van de organisatie. Ook deze normen kennen een context die interessant is om in het achterhoofd te houden. ISO is een onafhankelijke niet-overheidsinstantie waar 167 landen lid van zijn. Het instituut brengt de leden bij elkaar om middels consensus relevante standaarden voor de markt vast te stellen. De ISO-normeringen staan achter een betaalmuur. Vanuit Nederland is het NEN (Stichting Koninklijk Nederlands Normalisatie Instituut) lid van ISO. Het NIST CSF is gemaakt door het National Institute of Standards and Technology (NIST), dat onderdeel is van het U.S. Department of Commerce. De missie van het NIST is om Amerikaanse innovatie en industriële concurrentievermogen te stimuleren door het bevorderen van meetmethoden, standaarden en technologie op manieren die de economische zekerheid vergroten en onze kwaliteit van leven verbeteren. Het NIST CSF is verplicht gesteld in de Verenigde Staten voor alle federale overheidsinstellingen in het land en is gratis beschikbaar. Beide kaders hebben dus een andere insteek, die je terugziet in het concreet maken van de business context.

1. ISO 27001: Context of the organization

De ISO27001:2017 heeft de context beschreven in hoofdstuk 4. De context wordt als volgt concreet gemaakt:

- Understanding the organization and its context;
- Understanding the needs and expectations of interested parties;
- Determining the scope of the information security management system.

Hierin is ook direct de volgorde duidelijk: start met de organisatie zelf en haar omgeving, kijk daarna naar belanghebbenden en tot slot naar de omvang van het Information Management System (ISMS).

2. NIST Cybersecurity Framework: Business Environment

Naast de ISO 27001 wordt het CSF van het NIST steeds populairder om te gebruiken als standaard. Ook hier vind je de context terug: binnen de functie Identify (ID) staat de categorie Business Environment (BE) als tweede. Het doel van Identify.Business Environment (ID.BE) is: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. En ook in het NIST CSF is dat verder uitgesplitst in subcategorieën:

- ID.BE-1: The organization's role in the supply chain is identified and communicated;
- ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated;
- ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated;
- ID.BE-4: Dependencies and critical functions for delivery of critical services are established;
- ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).

Het NIST CSF geeft redelijk praktische invulling. Denk weer even terug aan de context van de norm: verplicht voor de Amerikaanse federale overheden. De vraag is natuurlijk hoe deze context passend te maken is voor ons in Nederland. Die vraag is aan eenieder om zelf voor jouw organisatie te beantwoorden. De invulling van ID.BE is in elk geval een stuk concreter en specifieker dan in de ISO27001. Het gaat hier om de keten, infrastructuur, missie, afhankelijkheden en weerbaarheid van de organisatie.

Overzicht geeft inzicht: geschreven en ongeschreven regels

Zowel de zachte als de hardere kanten van de context zijn van belang. De normen vragen vooral om overzicht over de meetbare en concrete punten, die ik de geschreven regels noem. Dat gaat onder meer over wetgeving, branchenormen, gedragscodes. De ongeschreven regels gaan over de belanghebbenden, de (onuitgesproken) verwachtingen, de concurrentie en ongrijpbare dingen als de historie en de toekomst. Als je op beide punten overzicht hebt, zorgt dat voor inzicht. Zorg er dus eerst voor dat je overzicht hebt door op te schrijven wat je weet. Maak een documentje aan en ga schrijven. Eerst voor de gehele organisatie, daarna per business unit, daarna per afdeling. Juist die specificering is belangrijk, want dan gaan mensen het voelen. Dat is dan weer basis voor risicomanagement en informatieveilig gedrag.

Hieronder mijn checklist, gebaseerd op ISO, CSF en eigen ervaring.

De geschreven regels

- Wat is de rol van de organisatie in Nederland? En in de wereld?
- Wat is de missie en visie (waarom bestaat deze organisatie/business unit/afdeling)?
- Wat levert de organisatie?
- In welke branche acteert de organisatie?
- Welke rol heeft de organisatie in de keten? Wat komt ervoor of erna vanuit het perspectief van de klant/cliënt? Met andere woorden: welke afhankelijkheden zijn er?
- Welke wetgeving, normen en gedragsregels zijn van toepassing?
- Welke eisen zijn er aan continuïteit?

De ongeschreven regels

- Welke stakeholders zijn er?
- Met awareness (de doelgroep) in het achterhoofd: welke functies hebben medewerkers?
- Zijn er leveranciers belangrijker dan andere?
- Wie zijn de vaste contactpersonen? Welke (formele) functie hebben zij?
- Welke reguliere overlegstructuren zijn er?
- Welke primaire processen zijn cruciaal?
- Welke vragen aan de ISO zijn als laatst gesteld? Of welke worden het meest gesteld?
- Welke vragen aan IT zijn als laatst gesteld? Of welke worden het meest gesteld?
- Wat waren de laatste incidenten en/of events?

Met overzicht over bovenstaande onderwerpen krijg je inzicht in de patronen en factoren die de context van jouw organisatie maken. Met deze context kun je vorm gaan geven aan je communicatie over informatieveiligheid en je invulling van het informatieveiligheidsprogramma/roadmap.

Communicatie met de stakeholders

Nu we de omgeving en de patronen van de organisatie in de basis helder hebben, kunnen we aan de slag met communicatie. Niet meteen een heel communicatieplan, dat komt bij de specifieke onderwerpen in het programma. Als onderdeel van de context ben ik op zoek naar verwachtingen, vragen en antwoorden. In de ongeschreven regels zit al een deel van de vragen die aan informatieveiligheid en IT gesteld worden. Hoe wordt daarop antwoord gegeven? Is de toon van communicatie zakelijk of juist persoonlijk? Door dit onderwerp specifiek te bekijken, kom je te weten hoe de organisatie impliciet functioneert. Ga dat ook na bij de afdeling communicatie (en marketing). Zij kunnen je helpen. Door de communicatie af te stemmen op de verschillende doelgroepen, sluit je goed aan bij de verwachtingen die zij hebben en word je een voorspelbare partner. Dat is natuurlijk een beetje kort door de bocht, maar de toon van de antwoorden én je vragen aanpassen aan de stakeholder helpt zeker. Ook een goede vraag die expliciet terugkomt in de ISO27001 is wat de stakeholders van jou nodig hebben. Ook daarop kun je aansluiten in de manier waarop je communiceert.

Tot slot: met de context geef je je programma vorm

Met inzicht in alle omgevingsfactoren kun je jouw informatiebeveiligingsprogramma vormgeven. Wat mij betreft geeft het NIST hier de duidelijkste richting aan door middel van Special publication 800-53. Hierin worden de Security and Privacy Controls for Information Systems and Organizations beschreven. In de familie Planning wordt invulling gegeven aan de controls die je nodig hebt om je informatieveiligheidsplan of programma vorm te geven. Dit zijn:

- Policy & procedures
- System security & privacy plans
- Rules of behavior
- Concept of operations
- Security and privacy architectures
- Central management
- Baseline selection
- Baseline tailoring

Door de context als eerste mee te wegen, ontstaan op deze cruciale onderwerpen de maatregelen en het plan dat bij jouw organisatie het best past. Neem de punten mee waar jouw organisatie iets aan heeft en vergeet de rest. Deze ode aan de context is dus met name een oproep om niet direct de maatregelen in te duiken, maar eerst aandacht te geven aan de omgeving. Zo maken we met het hele vakgebied de stap van beveiliging naar veiligheid en weerbaarheid!

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Hoe onaantastbaar is het lichaam van personen met een baarmoeder?

Met vlaggen staan ze voor de supermarkt waar ik langs loop. Het evangelie te verkondigen en daarbij leugens scanderend over abortus. Een paar honderd meter verderop is namelijk een abortuskliniek – maar daar mogen ze van de rechter niet meer bij in de buurt komen.

De beschikking van personen met een baarmoeder over hun eigen lichaam staat momenteel weer volop in de belangstelling. Het recht op lichamelijke integriteit, is net als alle andere aspecten van het grondrecht op privacy, niet absoluut. In de praktijk betekent dit dat onze wetgever uitzonderingen mag bedenken die je hebt te dulden als persoon. Zo mag de politie je fouilleren als ze bijvoorbeeld denken dat je een wapen draagt en dit gevaar kan opleveren voor anderen. En als iemand een medische handeling op, aan of in jouw lichaam wil verrichten, moet je daar eerst toestemming voor geven. Echter, niet elke wettelijke beperking op onze lichamelijke integriteit is altijd te billijken, laat staan dat deze als ethisch verantwoord kan worden gezien.

Een discussie over privacy in relatie tot abortus is ook in Nederland ontzettend hard nodig. Want, wie denkt dat het hier allemaal zo goed geregeld is, komt van een koude kermis thuis. Er bestaat namelijk geen recht op abortus in onze wetgeving. Sterker nog, abortus is nodeloos gecriminaliseerd door opname in het Wetboek van Strafrecht:

"Hij die een vrouw een behandeling geeft, terwijl hij weet of redelijkerwijs moet vermoeden dat daardoor zwangerschap kan worden afgebroken, wordt gestraft met gevangenisstraf van ten hoogste vier jaar en zes maanden of geldboete van de vierde categorie."

Alleen al het woordgebruik is verouderd en onnodig gegenderd. Daarnaast voelt het pijnlijk patriarchaal dat 'hij' een zwangerschap afbreekt bij een 'vrouw', en daarmee komen we direct aan bij een cruciaal punt van kritiek. Het verankeren in het strafrecht zendt het signaal dat een persoon met een baarmoeder onvoldoende handelingsbekwaam zou zijn over diens eigen lichaam en dat de Staat dat dan maar dient 'te beschermen'. In Nederland hebben wij voor de gevallen dat die handelingsonbekwame zwangere persoon een abortus wil, daarnaast een speciale wet: Wet afbreking zwangerschap. Als alle betrokkenen aan de eisen daarin voldoen, dan zullen zij niet gestraft c.q. strafrechtelijk vervolgd worden. Overigens blinkt ook die Wet afbreking zwangerschap niet uit in respect voor personen die zwanger zijn, alleen al de plicht die het artsen oplegt om uitgebreid te vertellen dat er ook middelen zijn die de zwangerschap had kunnen voorkomen, illustreert dat zeer pijnlijk.

Voorstanders van deze strafbaarstelling zeggen dat het zwangere personen moet beschermen tegen een gedwongen abortus. Dat deze argumentatie uitermate zwak is, blijkt alleen al uit onze Wet op de geneeskundige behandelingsovereenkomst. Deze regelt namelijk dat je niet zomaar aan een medische behandeling onderworpen kunt worden, daarvoor moet je namelijk zelf toestemming geven. Daarnaast bevat onze strafwetgeving allerhande mogelijkheden om personen te vervolgen die zonder toestemming iets op, in of aan iemands anders lijf doen. Hoog tijd om deze vreemde inperking op het recht op privacy van personen met een baarmoeder voorgoed gedag te zeggen, de strafbaarstelling te schrappen en een recht op abortus op te nemen in onze wetgeving.

Mr Rachel – baas in eigen buik – Marbus

Rachel

Auteur: Jeroen Gaiser is adviseur cybersecurity. Hij is te bereiken via: jeroen.cissp@gmail.com

(Cyber)spieken mag gewoon!

Als professionals hebben we te maken met het omslagpunt waar je de inhoud moet vertalen naar bestuurlijke taal. Bestuurders en andere beslissers zijn geen inhoudelijke experts en hebben een andere context waarin ze besluiten nemen. In deze context zijn cybersecurityrisico's één van de wegingsfactoren. Willen we veilig kunnen digitaliseren, dan moeten wij als experts de aansluiting vinden met collega's van buiten ons vakgebied. Met mijn ervaringen hoop ik jullie te inspireren om deze uitdaging aan te gaan!

Op Valentijnsdag 2021 werd in het televisieprogramma *Zondag met Lubach* (1) een onderwerp aangesneden waar ik zelf veel van merkte, Digibetocratie. Het ging over de verkiezingen van 2021 en Arjen Lubach kaartte aan dat onze volksvertegenwoordiging nogal weinig af wist van iets wat zo belangrijk is. "We worden bestuurd door mensen die geen reet snappen van computers en digitale veiligheid", aldus Lubach.
Nou, dat signaal was regelmatig in mijn LinkedInfeed terug te zien. Niet alleen Kamerleden, maar bestuurders in algemene zin kregen er regelmatig van langs over het kennisniveau van digitalisering en de daarbij horende cybersecurityrisico's.
In alle discussies op LinkedIn vroeg ik me steeds vaker af wat ik als inhoudelijk expert aan informatiebeveiliging had gedaan om dit te verbeteren. Klagen is makkelijk, maar ik kan ook wat gaan doen vond ik. In een van de discussies vroeg ik me af of het niet handiger was om deze mensen spiekbriefjes te geven.

De reden dat ik aan een spiekbrief dacht was dat ik van mening ben dat je niet alle kennis paraat hoeft te hebben. Daarnaast blijft de term goed 'plakken'. Kamerleden krijgen enorme hoeveelheden informatie te verwerken over zeer diverse onderwerpen. Ja, ze hebben een belangrijke rol in de digitale veiligheid van Nederland, maar nee, het is niet nodig alle inhoudelijke expertise paraat te hebben zoals degenen voor wie het dagelijks werk is. Voor een debat kunnen zij dus even snel spieken om zeker te weten dat het onderwerp scherp op het netvlies staat. Dit ondersteunt een kwalitatief goede inhoudelijke behandeling.

Aan de slag!

En zo was het cyberspiekbriefjesidee geboren en ging ik op persoonlijke titel aan de slag. Uiteraard registreerde ik eerst het domein cyberspiekbrief.nl; ik wist niet hoeveel aandacht er zou komen. Daarna was de uitdaging tweeledig. Ten eerste: wat is de juiste kennis in de juiste vorm voor de doelgroep? Ten tweede was het de uitdaging voor ons als experts om zonder jargon, kort en krachtig de essentiële boodschap op te schrijven?

Om beeld te krijgen van de informatievorm en behoefte van een Kamerlid, kon ik te rade gaan bij enkele mensen zoals Fred Streefland (2) die vanuit hun cybersecurityachtergrond al vaker Kamerleden hadden geïnformeerd. Zijn boodschap was helder: kort, krachtig en het moet snel lezen ondersteunen.
En dan de inhoud. In een LinkedInpost vroeg ik aan mijn netwerk welke onderwerpen zij dachten in Kamerdebatten te verwachten en waarvan men vond dat deze bekend moeten zijn. Uit deze discussie kwamen 17 onderwerpen. In mijn netwerk vond ik medeexperts die hielpen met de inhoud. Het template had ik zelf gemaakt, dit borgt de uniformiteit en gaf de spelregels om de inhoud te gaan vullen.

Zoeken naar een landingspagina

In de loop van 2021 waren de spiekbriefjes af, maar wat doe je dan? Stuur je ze zo naar alle fracties? Naar info@tweedekamer.nl? Taggen op LinkedIn/Instagram/Facebook/etc.? Het toeval was dat ik medio 2021 ook in gesprek kwam met het ECP, die contact hadden met het platform veiliginternetten.nl. Na een eerste gesprek werd duidelijk dat er een goede match was tussen de doelen van dit platform en wat ik voor ogen had. De maanden daarna is er hard gewerkt om de site te maken en te vullen.

Begin maart 2022 was het zo ver, de site www.cyberspiekbriefje.nl was online. Trots kon ik het op LinkedIn laten zien en kreeg ik vele goeie reacties en de onvermijdelijke correcties op spelfouten en typo's. Ook werd de lancering opgepikt door media als BinnenlandsBestuur en Security.nl. Op een event begin april jl. sprak ik Queeny Rajkowski, lid van de commissie Digitale Zaken van de Tweede Kamer. Zij vond het een erg leuk initiatief en droeg me voor om de spiekbriefjes aan te mogen bieden aan deze commissie. Op 14 juni stond ik op de agenda en heb samen met Sophieke Thurmer en Marjolijn Bonthuis van veiliginternetten.nl de cyberspiekbriefjes mogen overhandigen aan voorzitster Roelien Kamminga.

Zoek elkaar op

Aan de commissieleden legde ik kort uit dat ze een belangrijke rol hebben. Niet alleen in digitalisering, maar vooral ook veilige digitalisering. Wij als experts willen hen daarbij helpen en de spiekbriefjes zijn daar een voorbeeld van. Ook legde ik uit dat wij als experts moeten beseffen hoe de wereld van een parlementariër eruit ziet en onze communicatie aanpassen op deze wereld. De commissieleden waardeerden het zeer dat ik ook belicht heb dat experts de toenadering moeten zoeken door meer in de taal en context van de commissieleden te communiceren.

De opbouw van een cyberspiekbriefje

Om een spiekbriefje snel leesbaar en herkenbaar te maken, had ik een vaste indeling gemaakt met gescheiden blokken. Het begint met een uitleg wat de term betekent. In enkele bullets wordt de kern van het onderwerp toegelicht. Vervolgens wordt het belang voor Nederland geschetst. Dit helpt politici om het onderwerp te plaatsen qua impact op de maatschappij en helpt dus het nut te begrijpen.

In het volgende blok wordt beschreven wat de impact op de maatschappij is als het niet goed gaat door misbruik. Dit helpt een politicus om de voor- én nadelen in te zien. Door in het volgende blok toe te lichten of misbruik al voor is gekomen en op welke manier, worden voorbeelden gegeven of dit risico reëel/actueel is, maar het helpt ook om de impact nog beter te begrijpen.

Bij enkele grote organisaties is er ook interesse om de spiekbriefjes op maat te maken voor de eigen organisatie.

Roelien Kamminga en Jeroen Gaiser met het cyberspiekbriefje.

Ten slotte wordt er kort inzicht gegeven in een blok of er al specifieke wetgeving is op dit onderwerp. Wetgeving is een belangrijk middel wat vaak in debatten genoemd wordt om in te grijpen en informatie over bestaande wetgeving is daarom belangrijk om mee te geven.

Op de achterkant van het spiekbriefje staat een link en QR-code naar bestaande video's om net een slag beter het onderwerp te leren kennen als hier tijd voor is.

Belangrijkste lessons learned

Na ruim een jaar bezig te zijn met dit (iets) uit de hand gelopen project, zijn mijn belangrijkste leerpunten:

- Probeer bij elk probleem te bedenken wat je rol is in het ontstaan en oplossen ervan
- Probeer voordat je advies uitbrengt, eerst de context en het probleem van je gesprekspartner te begrijpen
- Let op gebruik van jargon
- Praten met je doelgroep is essentieel om begrip en wederzijds vertrouwen op te bouwen
- Heb je een idee, ga er mee aan de slag ook al weet je niet hoe het uit gaat pakken. Spring in het diepe!
- Durf hulp te vragen als je ergens heel zeker van bent
- Verzamel mensen om je heen die meehelpen, maar niet klakkeloos meepraten. Organiseer tegengeluid

Hoe nu verder met de cyberspiekbriefjes?

Mijn horizon lag bij het aanbieden bij de commissie Digitale Zaken en ik heb nog niet verder gedacht. Sowieso ga ik het domein nog overdragen aan het platform. Daarnaast is er bij enkele grote organisaties ook interesse om de spiekbriefjes op maat te maken voor de eigen organisatie. Dit was ook altijd een mogelijkheid, daarom staat het lege Wordtemplate ook op de site. Door het blok 'Belang voor…' aan te passen naar de eigen context, kan een spiekbrief snel aangepast worden voor de eigen organisatie.
Wie weet kunnen we naast de landelijke politiek nog een set maken voor de lokale overheden. Dit zou ik niet zozeer zelf doen, het idee moet door iedereen opgepakt kunnen worden. Ik wil dan ook iedereen uitnodigen een set spiekbriefjes te maken voor de eigen bestuurders.

Voor nu ben ik trots op het resultaat, de inspanning van de mede-experts en samenwerking met het platform. Wie weet wat hierna op mijn pad komt!

Referenties

(1) Zondag met Lubach, seizoen 13, aflevering 2, 14 februari 2021

(2) www.linkedin.com/in/fredstreefland/

COLUMN LEX

De mens als sterkste schakel

In bijna elk gesprek over cybersecurity komt het ter sprake: 'De mens is de zwakste schakel'. Dit is een makkelijke uitspraak, maar het zet wel een toon die maakt dat de mens als weerloos wordt weggezet. Dit kan ook anders.

Vaak hebben we het over security in de context van maatregelen en kosten. We focussen ons daardoor snel op de meest efficiënte manier om de maatregel te implementeren en uit te voeren. We vergeten dat ze veilig gebruikt en beheerd moeten kunnen worden door mensen. Als een systeem lastig te gebruiken of te beheren is, wordt dit afgewenteld op 'de zwakste schakel'. Fout geklikt op een link? Menselijke dwaling. Waar we op deze manier aan voorbij gaan is hoe krachtig die mens is. En wat zij of hij allemaal wél bijdraagt aan de beveiliging. Mensen kunnen veel meer bereiken dan systemen want, anders dan systemen, zijn mensen intelligent en ervaren zij emoties.

Intelligentie

Systemen werken op basis van programma's en data. Ook voor AI (artificial intelligence) geldt dat. En dat heeft voordelen: ze werken secuurder dan mensen en ze hebben meer verwerkingscapaciteit. In de basis zijn systemen oerdom. Een systeem kan de mens helpen, maar een systeem kan ze niet analyseren. Omgekeerd kan wel, systeemanalist is een normale, goed beschreven functie. Mensen werken met de kennis en vaardigheden die ze hebben. Daarmee zijn ze weerbaarder, hebben ze meer flexibiliteit, en zijn ze bovenal creatiever. Een mens kan buiten gebaande paden denken en handelen. Verwacht dat alsjeblieft niet van systemen. Die worden ontworpen, gebouwd, gebruikt en misbruikt door mensen – want criminelen zijn ook maar mensen. Pas als systemen zo slim zijn als mensen zullen systemen slimmere systemen kunnen ontwerpen dan de mens dit kan doen. Dit noemen we de singulariteit. Zover zijn we nog lang niet, sommigen twijfelen of we daar ooit kunnen komen. Tot die tijd moeten we letten op de goede geschiktheid van systemen om gebruikt te worden door mensen.

Emotie

Emotie is iets wat systemen niet ervaren. Heel voorzichtig zijn er pogingen om emoties bij mensen te kunnen herkennen met AI, maar succesvol kun je het niet noemen. Bij cybersecurity benoemen we het risico dat emoties juist misbruikt worden om een aanval te doen, dat weer bijdraagt tot het idee dat emoties maar een teken van zwakte zijn. Het tegendeel is waar: door emoties staan we sterker. We gebruiken empathie om emoties bij anderen los te maken. Zodat ze ons sympathiek vinden, bijvoorbeeld. Dat helpt om begrijpelijk te communiceren en samen in actie te kunnen komen. Systemen hebben dit niet nodig, wie aan de knoppen zit heeft control en weet je niet hoe de knoppen werken, dan heb je pech. Emoties zetten mensen aan tot actie. Emoties beleven leidt tot productiviteit en stuurt veranderingen. Je ziet al snel dat je in een omgeving waar een grote verandering moet plaatsvinden dit beter lukt met een inspirerend leider dan met een strakke, zakelijke, directieve aansturing.

Emoties helpen mensen beslissingen nemen. Hoe vaak hebben we het niet over ons onderbuikgevoel? Als dat goed is, zijn we veel meer gemotiveerd om te beslissen voor een bepaald alternatief. De mens kan focussen op wat belangrijk is in het moment en met een beperkt overzicht. Systemen kunnen die focus alleen verleggen binnen geprogrammeerde paden. Ze kunnen niet werken met incomplete informatie. Wanneer systemen falen moeten mensen in actie komen om te handelen. Emotie helpt mensen gevaar zien. Zo heeft de evolutie ons gemaakt. We vermijden grote gevaren, omdat de angst gaat overheersen. Zo blijven we ongedeerd. Dit is allemaal heel nuttig in de oerwereld, maar de laatste paar duizend jaar staat dit aspect ons ook soms in de weg. Een aanvaller die onze sympathie kan winnen, die ons angstgevoel en/of onze perceptie van succes kan beïnvloeden, kan ons handelen sturen. Dan kunnen we onder druk verkeerde beslissingen gaan nemen.

Door de mens hierbij weg te zetten als zwakste schakel, sta je beïnvloeding toe. Door alternatief de mens intelligent en emotioneel in zijn kracht te zetten, creëren we een schakel die sterker is dan alle beveiligingssystemen. Hierbij helpt het hebben van bewustzijn van die kracht, en daar kunnen we mensen bij helpen. Zie dat als een versterking en niet als het tegengaan van een zwakte.

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

Authors: Reinder Wolthuis, senior consultant/project manager cybersecurity at TNO. Can be reached at reinder.wolthuis@tno.nl. Frank Fransen, senior scientist cybersecurity at TNO. Can be reached at frank.fransen@tno.nl.

SOCCRATES - Vision & Roadmap for SOC & CSIRTs

SOCCRATES (SOC & CSIRT Response to Attacks & Threats, based on attack defence graphs Evaluation Systems) is a European innovation project, co-funded by the Horizon2020 program and led by TNO. It brings together some of the best European expertise in the field to develop, implement and evaluate an automated security platform to support SOC analysts. This third article on the project provides a summary of the 'vision, roadmap and guidance for SOC' booklet that was recently published by SOCCRATES.

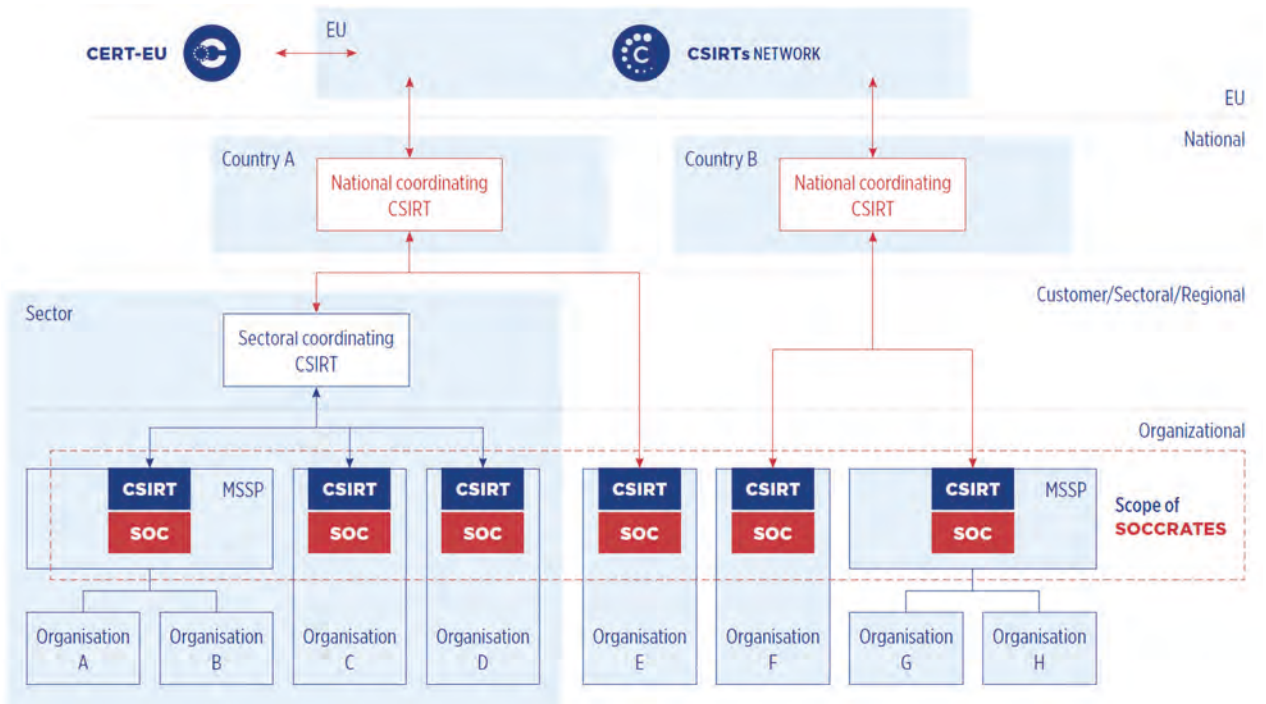


Figure 1 - SOC and CSIRT clustering and layering.

The SOCCRATES project was introduced in two previous articles (iB-Magazine 4 and iB-Magazine 5 2021). The first article gave an overview of the challenges that Security Operations Centers (SOCs) and Computer Security Incident Response Teams (CSIRTs) face, and how the SOCCRATES project addresses these challenges by developing a security automation and decision support platform, 'the SOCCRATES platform'. The second article described in more detail how the SOCCRATES platform is providing security automation for SOC and CSIRT processes. How it provides situational awareness and option awareness to the SOC analyst and enables (semi) automated response execution. This third article elaborates on the SOC and CSIRT capabilities, and the vision of the SOCCRATES project on the future needs for SOCs and CSIRTs.

SOC & CSIRT

The increasing dependency of organisations, and society as a whole, on IT systems and networks as well as the increase of cyber security incidents with major impact, has led to organisations (and governments) increasing their spending on cyber security. Many organisations have established a Security Operations Centre (SOC) and Computer Security Incident Response Team (CSIRT) to protect the organisation against cyber-attacks, or they contracted a Managed Security Service Provider (MSSP) to perform these operational cyber security services for them. Both a SOC and a CSIRT are thus expert teams (often also formally embedded in an organisational unit), that provide operational security services. It is quite common to use alternative names for similar types of such organisational units, such as Cyber Defence Centre (CDC) for SOC, and Computer Emergency Response Team (CERT) for CSIRT. Moreover, the terms SOC and CSIRT are also applied at different levels, as can be seen in figure 1.

In the lowest layer of the picture we see the organisations that have their own SOC and organisations that make use of SOC and/or CSIRT services provided by commercial MSSPs. These actually are the core focus of the SOCCRATES project, i.e. SOCCRATES enhances the SOC/CSIRT capabilities of SOCs and CSIRTs that are run by organisations and MSSPs.

In the higher layers, we mainly see so called coordinating CSIRTs that provide services to a set of organizations known as the constituency (e.g. organisations in a sector, region, country, etc.). These services include typically coordination of security incidents that affect several organisations within the constituency, acting as a single point of contact for the sector/region/country, distribution of cyber threat intelligence and providing security incident analysis and forensic services.

Note that coordinating CSIRTs sometimes operate at a same level

	SOC	CSIRT
Current Capabilities	• Monitoring and detection • Event analysis • Information security incidents analysis (triage) • Vulnerability analysis • Security Awareness Creation	• Information security incidents analysis (incl. event correlation) • Threat analysis (incl. collection, sharing and processing of CTI) • Artefact and forensic evidence analysis • Information security incident coordination • Vulnerability coordination • Awareness Building
	• Event detection (through alerting and/or hunting) / threat hunting • SOC tool life-cycle support (incl. operations and maintenance, tuning tools (e.g. detection sensors), engineering and deployment, and R&D)	
New Capabilities	• Security Orchestration, Automation and Response (SOAR) • Automated security reasoning (real-time threat & impact assessment) • Automated generation and assessment of response actions (both pro-active & reactive) • Automated response execution	

Figure 2 - Current & needed SOC / CSIRT capabilities.

as the Information Sharing and Analysis Centres (ISACs), not shown in the figure, which facilitate gathering and sharing of information on cyber threats while CSIRT activities may go beyond the ISAC activities, e.g. through security incident coordination.
In figure 1 the following coordinating CSIRTs are depicted:

- Sectoral or Regional CSIRTs - Dedicated CSIRTs that collect and analyse threat intel, translate this to the specific context of the sector or region and distribute it within the sector/region organizations. Examples of sectoral CSIRTs in the Dutch context are Z-Cert (healthcare) and IBD (Informatie Beveiligings Dienst, municipalities).
- National CSIRTS – These CSIRTs have the task to enhance a nation's resilience in the digital domain, prevent or limit the failure of the availability or the loss of integrity of information systems of vital operators and central government, and to handle severe computer attacks against critical infrastructure and information within the nation. On Dutch national level we of course have the Dutch National Cyber Security Centre (NCSC).
- CERT-EU - This is a specific CSIRT on EU level and is the Computer Emergency Response Team for the EU Institutions, bodies and agencies

Additionally, a community initiative across coordinating CSIRTs has been started, the 'CSIRT network', which provides a forum where members can cooperate, exchange information and build trust. Although not really common, some of these coordinating CSIRTs maintain monitoring and detection capabilities on a regional or national level.
Of course the different layers are not independent. Especially during serious security incidents, there will be heavy exchange of information between the CSIRTS on the different layers and between CSIRTs on the same layer.

Current SOC / CSIRT capabilities

In ENISA's "How to setup up CSIRT and SOC", from December 2020 (1), a set of services has been identified that are typically provided by a SOC and CSIRT. These typical services are a subset of the CSIRT services framework compiled by the Forum of Incident Response and Security Teams (FIRST) (4). The main difference between the SOC and CSIRT (in practice this separation of duties usually is not quite as strict) is that the SOC provides a real-time monitoring and incident detection service, whereas the CSIRT further analyses an event they receive from the SOC and can coordinate mitigating actions in case the event turns out to be an actual security incident.

New SOC / CSIRT capabilities

Most SOCs and CSIRTs have a good set of capabilities (see also the top of Table 1), but present day SOC and CSIRT capabilities simply do not suffice to deal with the persistence and sophistication of professional threat actors also considering the increasing complexity of ICT infrastructures and shortage of skilled staff.

Therefore we need to increase the speed and effectiveness of detection of and response to ongoing attacks, and the scope, effectiveness and efficiency of proactive analysis of threats to the ICT infrastructure to enhance its cyber resilience.

To achieve this we need to introduce so called Security Orchestration, Automation and Response (SOAR) capabilities. Also we have to introduce automated security reasoning capabilities on the vulnerability, resilience and potential impact of an organisation's ICT infrastructure and automatically generate and assess response actions to ongoing attacks and emerging threats. Furthermore, in order to increase the speed of responding to ongoing attacks and emerging threats, the ICT infrastructure has to be adapted, so it can support automatic instantiating and/or reconfiguring of security controls. Such automated response execution capability will in many environments include a human-in-the-loop, but in modern ICT environments (e.g. programmable infrastructure, cloud-native technology) this may even be fully autonomous response systems. The new SOC / CSIRT capabilities are listed at the bottom of Table 1.

To establish the capabilities that the SOCCRATES project envisions for the future, a variety of technical challenges will need to be overcome:

- Actual machine-readable model of the infrastructure
- Improvement of detection capability and coverage
- Advanced use of Cyber Threat Intelligence
- Real-time Business Impact Assessment
- Recommend Course of Action (CoA) generation
- Automation and orchestration to improve SOC response

In the following sections these challenges are elaborated on by describing the current state and future needs.

Actual machine-readable model of the infrastructure

Although inventory and control of hardware and software assets are essential elements in many cyber security frameworks (e.g. NIST Cyber Security Framework (3), CIS Critical Security Controls for Effective Cyber Defense (2)), many organizations still struggle with keeping their asset inventory up to date. As our IT environments are getting more dynamic, it is becoming an even more challenging task. SOC analysts, however, need to interpret and understand security events in the context of the continuously evolving ICT networks and systems of an organisation. The SOC and CSIRT analysts also need to understand the critical attack surfaces, the attack paths that may lead to a compromise of assets, as well as defence mechanisms present and/or can be enforced to counter an attack. For a human analysts the infrastructure information has to be visualized in a comprehensive manner such that it is easy to understand and security events can be projected on top of the infrastructure to create real cyber situational awareness. Moreover, for automated security reasoning and decision support capabilities, such as automated threat modelling and simulation and real-time business impact assessment, the infrastructure information has to be current, accurate and machine-readable and made available via Open APIs in a standardized format.

There are promising developments (e.g. Software Bill of Materials (SBoM) (5)) and new products entering the market that enable access information on assets (incl. installed software), network topology and vulnerabilities in the infrastructure. But these products do not often provide an API for third party tools to collect a machine-readable standardised model of the infrastructure for (third party) security analysis tools.

The SOCCRATES project foresees the following needs for the near future:

- Improve asset discovery and change detection. There is a need for better asset discovery of a wide range of asset types, both from an internal and external viewpoint, in near real-time, going beyond just IP/port/service detection and into fingerprinting of the make-and-model of all assets. Moreover, uniquely mapping of information about the same asset from different data sources (e.g. Network MAPper (nmap), vulnerability scanner, AD, netflow) to a single object in the data model is challenging.
- Improve access to asset management systems. Access to asset management systems is needed to provide accurate up to date infrastructure information at different levels of detail or granularity (such as the make and model of assets).
- Better visualisation of ICT infrastructures. Visualization is needed with the capability to overlay security status and event information.

- Create the ability to provide historical infrastructure model information. This might be limited to a certain point in time and with gradually decreasing level of detail, but will help understanding historical log events during threat hunting.
- More standardisation of data models. Standardisation of the data models describing the ICT infrastructure in a machine readable manner.
- Improve automatic discovery of security functions in a machine readable manner. This should include information on scope (i.e. what security functions do they provide for which assets?), whether these functions are configurable, via what API, etc.

Improvement of detection capability and coverage

A major activity of a SOC is to respond to the alerts that are generated by detection systems. Approaches to detecting cyber-attacks can be broadly placed into two categories: those that use signatures that describe adversarial behaviour, versus those that aim to detect anomalies that manifest in collected data and could indicate a cyber-attack. For the latter approach, there is increasing interest in applying machine learning algorithms to learn a model of normal behaviour and use this as a basis for detection. The advantage of anomaly-based detection approaches is that novel – previously unseen – attacks can be detected, if the manifestation of their behaviour deviates from a learned norm.

The SOCCRATES project foresees the following needs for the near future:

- Improve detection capability across IT and OT systems. Whilst advancements are being made, OT systems have traditionally not been monitored for adversarial behaviour to the same extent as their IT counterparts. With the integration of these systems, increased attention has been paid to this issue. Although detection systems for deep-packet inspection of industrial protocols (e.g. Modbus, DNP3, OPC UA, etc.) exist, endpoint monitoring and detection on OT devices and infrastructure is still relatively immature or absent. The result is that OT visibility is limited.
- Improve detection of prevailing adversary techniques and procedures. A major challenge for a SOC, is to determine whether a deployed detection posture is able to effectively identify techniques and procedures that are of concern. Knowledge-bases, such as the MITRE ATT&CK Framework, provide insights into the data sources that could be used to detect specific techniques but there is a gap between this information and that needed to determine whether specific procedures that an adversary is using can be detected. This problem is exacerbated by adversaries adjusting their procedures to avoid detection.
- Increase effectiveness of detection of security events in large data sets. The amount of data that can be used to detect security events is growing tremendously. One apparent challenge here is to determine which of all this data is worthwhile paying attention and applying resources to in order to gain useful insights. Put simply, where should one start to detect an attack?
- Decrease number of false positives. Large volumes of data also exacerbate a well-understood problem that is associated with anomaly-based detection systems: false positives, i.e. alerts that indicate malicious behaviour when none exists. The job of the cybersecurity data scientist is to improve detection performance, as much as possible, using techniques such as feature engineering or tuning the hyper-parameters of deep learning models. The goal is to reduce the false positive rate so that SOC analysists do not waste time fielding unwarranted alerts.
- Improve response on detected incident. The obvious advantage of anomaly detection techniques is that one does not need to prescribe the adversarial behaviour to be detected – the norm is learned by a machine learning algorithm and if a sample deviates from this norm, an alert is generated. However, there is arguably a (semantic) gap between what an anomaly detection system generates and insights that can lead to steps to mitigate an attack (i.e. the invocation of a playbook that is related to a specific class of attack). For example, it is not immediately apparent whether a detected anomaly relates to a ransomware attack or perhaps data exfiltration – two types of attack that require distinct responses. Automated support for this activity should help to improve the effectiveness of a SOC, as it aims to realize its KPIs.
- Increase resilience against Adversarial Machine Learning. Machine learning (ML) and artificial intelligence (AI) are finding increasing utility in SOC operations. However, also attackers are exploring the benefits of AI and ML. So-called adversarial machine learning can take many forms. An attacker's goal can

The key to detecting adversary behaviour is procedures.

include model theft and poisoning, for example, and subverting a model's output, in order to cause misclassification. Because machine learning is applied to ever-increasing mission critical applications and adversaries explore this new form of attack, it could become a major future challenge.

Advanced use of Cyber Threat Intelligence

Apart from knowing what you are defending, you also need to know the enemies and their capabilities against which you are defending. This is the goal of Cyber Threat Intelligence (CTI). CTI is evidence-based knowledge about threats that provides situational awareness and actionable decision support. CTI can be further divided into subtypes: strategic, operational, tactical and technical (6). The tactical and technical subtypes are the most relevant for SOC and CSIRT needs. Tactical CTI is knowledge about adversary behaviour, and is referred to as the Tactics, Techniques and Procedures (TTPs) of the adversary. Technical CTI is knowledge about specific malware, tools or infrastructure. Examples are file hashes, IP addresses and domain names observed in an incident and shared as Indicator of Compromise (IoC).

Although IoCs can directly be used to detect or hunt for malicious behaviour, the volume of shared IoCs is very large and they changes quickly. More quickly than the associated TTPs. Detecting adversary behaviour based on the TTPs lets defenders therefore stay ahead of the attackers. Another advantage of tactical CTI is that TTPs can be used for adversary emulation, as is done in Threat Intelligence Based Ethical Red-teaming (TIBER) (7).

Nowadays, IoCs are extensively used by SOCs and CSIRTs in an automated fashion. Threat feeds are downloaded and used to compile a signature for attack detection. Additionally, CSIRTs automate IoC sweeps on logs to find historical intrusion activity that was not detected when the activity took place. The application of tactical CTI is, however, largely a manual process. The underlying reason for this is lack of machine readable standards. MITRE ATT&CK is first and foremost a knowledge base of techniques, linked to adversary groups and software. The tactics in ATT&CK are tactical objectives, not actually tactics. But more importantly, the procedures in ATT&CK are human readable examples, not suitable for processing by a computer.

The key to detecting adversary behaviour is procedures. ATT&CK provides no guidance on how to define procedures in a machine readable format, and the same applies to the standards for sharing CTI (e.g. Structured Threat Information Expression (STIX) and Malware Information Sharing Platform (MISP) formats).
The SOCCRATES project foresees the following needs for the near future:

- Improve quality, relevance and timeliness of technical CTI (i.e. IoCs) to reduce false positive alerts and exhausting limited resources of the SOC and CSIRT chasing non-incidents. New methods are needed to contextualise IoCs to help defenders with prioritisation.
- Increase level of automation for collection, sharing and processing of tactical CTI to enable adversary behaviour detection and assessing the infrastructure with adversary emulation. This includes describing adversary behaviour in a machine readable format, and developing methods and tools for automatically process and use this information for detection and attribution.

Real-time Business Impact Assessment

The impact of attacks on an infrastructure is usually analysed from a technical point of view: the logs and the alerts raised by intrusion detection systems allow a SOC analyst to identify the assets targeted by the attacks and, with the help of attack graphs based tools, predict the potential attack path among the other assets of the infrastructure. This approach is essential, as it greatly facilitates the deployment of courses of action that will both mitigate the attack and correct vulnerabilities. However, this technical analysis does not take into account the operational impact, i.e. to which extent the attack will disrupt the organisation of the company departments. Therefore, in addition to understanding the ICT infrastructure, the SOC analyst needs to be able to assess the potential impact on the business of an ongoing attack or emerging threat. To do so, it is necessary to not only develop a model of the business processes, but also be able to process this model and obtain computable metrics.
In the context of SOC/CSIRT environments, impact analysis on business processes is not usually done. Typically SOC and CSIRTs use predefined lists containing the Business Impact Assessment scores per host, in terms of Confidentiality, Integrity and Availability. More specific analysis of business impact is done manually and in collaboration with the business owner of the particular system., which is time consuming and does not allow the courses of action selection to match the business priorities during an ongoing attack on the infrastructure. Moreover, it does not allow for an assessment of the negative consequences to the business by deploying one or more courses of action. In order for such types of business impact assessments to be performed, a model of the business processes and functions is necessary. Business processes need to be mapped on the ICT infrastructure components, and insight in the consequences of a breach of confidentiality, integrity and/or availability of system resources or information assets needs to be (near real-time) available.

The SOCCRATES project foresees the following needs for the near future

- Improve (automatic) identification of business functions and -processes. It would be extremely useful to at least partially automate the identification of the company's business functions & - processes, as well as their dependencies. Including the dependencies with the assets from the infrastructure that directly support business functions. The main challenge to overcome is the lack of automation solutions in the state of the art. Methodologies to elaborate Business Process Model and Notation (BPMN) models are well known, but usually rely on manual work done beforehand, involving discussions and interviews with various services in the company. However, BPMN almost entirely decorrelates the business view from the technical view, which means that the link between the business entities and the assets must also be defined manually, though without any established methodology.
- Computation of relevant metrics to perform the business impact analysis. The challenge is to design a scalable mathematical model that is able to compute various metrics in real time, all while taking into account things such as asset redundancy and interdependencies and the specificities of the attack. To do so, well known graphical models, such as Bayesian networks, can be exploited, but will often require specific adaptations to match real life situations. Moreover, a

realistic model will need frequent data updates to match the dynamic nature of the business impact. Also, business impact is temporal by nature, the impact would typically be different during business hours compared to weekends, or may depend on seasonal aspects (e.g. point of sale system during the weeks before Christmas), or may depend on particular production orders.

Recommend CoA generation

To be able to automatically suggest optimal courses of actions (CoAs) for improving security in ICT infrastructures we can analyse cause and effect of various possible defence actions related to the infrastructure in a model (in popular terms; a digital twin), before getting into action with implementation. In general, the more detailed this analytic model will be, the better the suggested actions can be. And the model quality depends both on how much "raw data" from the ICT infrastructure is available and how well the model language captures the facts about what actions indeed are efficient security improvements, given different states of the infrastructure. With the model, we can examine the preventive measure optimization, in which we have to weigh and aggregate multiple assumptions made in various scenarios. One thing to assess is the expected shortest time it would take for a simulated attacker to traverse the attack graph connecting the starting and target points. And, with added defensive actions and enabled security controls we expect the estimated time to compromise (TTC) of the selected target(s) to increase, which improves security. By enabling or disabling defences time estimates for different attack vectors varies, and the defender can elaborate on good ways to increase the TTC for the attacker. The challenge we face here though is that the potential action space for the defender is very large, even for just a moderately sized ICT infrastructure. The CoA generator is thus tasked with finding highly effective defense action combinations, sparing the defender the work of trial-and-error simulations of testing different defense strategy hypotheses.

The SOCCRATES project foresees the following needs for the near future

- Improve asset management. As already mentioned, one of the biggest challenges for building an Infrastructure model is the challenge of discovering all the components in an ICT infrastructure. Even though we believe that this will remain a challenge for quite some time we can note that this situation is improving significantly with numerous new tools and tool capabilities. Also, we can note that the challenge is significantly smaller for cloud environments where the infrastructure is deployed from code and does not have to be discovered.
- Improve mapping of the detection space and the security analysis space. If we know that some particular asset has been compromised, an attack simulation with some assumed attacker starting point (such as the internet) will give the easiest attack vector to reach the compromised node. Looking for additional traces of breach along this vector is probably a good starting point to learn more about the incident. In principle we would like to be able to generate attack graphs that also include information on which attack steps can be detected, including the quality of detection.
- Improve visualization and contextualization of CoAs. A great support for a SOC analyst would be the capability to visualize and contextualize the CoAs depending on different threat scenarios and use cases.

Automation and orchestration to improve SOC response

Around 2015 technology started to emerge that we now call Security Orchestration, Automation and Response (SOAR) solutions. Initially these solutions were developed out of convergence from three different technologies: a) security incident case management platform with structured incident response workflows or playbooks, b) threat intelligence platforms that integrate automation for CTI processes, and c) tools for integration of different security tools/technologies in a coordinated way (playbooks). The combination of orchestration and automation for security operations refers to the tasks perform by a SOC analysist collecting information from multiple systems to support the decision-making process. The tools that entered the market could perform mundane repetitive tasks and thereby speed up incident investigations.

Also standardisation to support automation and orchestration of security operations has started. In particularly,

- Open Command and Control (OpenC2) (8), specifications to

enable machine-to-machine communications for purposes of CoAs execution
- Collaborative Automated Course of Action Operations (CACAO) (9), specifications for documenting playbooks for cybersecurity operations and sharing these across organisational boundaries.

The current state of security tools at many organisations can best be described as a plethora of disparate products from different vendors or sources. SOAR solutions can help with the integration and aggregation of the information from the diverse multi-vendor security products and tools, but the diversity and lack of standardised data formats is challenging.

Another challenge when deploying a SOAR solution is the fact that these tools require a significant amount of manual tuning and playbook definition. In addition, it remains to be seen how effective current SOAR solutions are with the increasing number of security events and alerts an organization has to cope with. Note that many of the simultaneous triggers may be related to the same security event. Handling of multiple simultaneous triggers and running different playbooks for related security events needs to be studied further.

The following future needs has among others been identified:

- Increase support for deployment of SOAR tools in SOC and CSIRTs, including integration of diverse security products and tools and sharing of playbooks that can easily be tuned and adopted.
- Improve how to deal with number of playbooks triggered and simultaneously handle potentially on related or even the same security incident.
- Automate playbook generation for execution of dynamically generate response actions. This includes translation from abstract response actions into specific reconfiguration commands for one or more security functions.
- Improve the interaction of the human analysist with SOAR, or security automation in general, will be a topic of concern for the coming years. Since there is a shortage of skilled cybersecurity staff there is much focus on training and education of cyber security personnel. But how will the role of the SOC and CSIRT analyst change in the coming years due to the introduction of security automation?

Concluding remarks

It is clear that SOC and CSIRTS need to transform. The SOC/CSIRT capabilities need to be strengthened and expanded, new capabilities are necessary to be able to handle future threats. Building and implementing these capabilities will have impact on all aspects of the SOC/CSIRT operations, including the interaction with the outside world.

Lookout to next articles

In the coming articles (next editions of the PvIB magazine) we will zoom in on the Orchestration and Integration Engine of the SOCCRATES platform and on the pilot evaluation. More info and the vision, roadmap and guidance for SOC booklet are available at www.soccrates.eu. More detailed information regarding this article can be found in the SOCCRATES vision paper:
https://www.soccrates.eu/wp-content/uploads/2022/05/soccrates_vision_paper_downloadable.pdf

SOCCRATES has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No. 833481.

References

(1) Edgars Taurins, How to setup up CSIRT and SOC - good practice guide. ENISA. 2020. (https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc)
(2) Klaus-Peter Kossakowski, Computer Security Incident Response Team (CSIRT) Services Framework, version 2.1. November 2019. Forum of Incident Response and Security Teams, Inc. (FIRST.Org). (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1)
(3) Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. NIST. 2018 (https://www.nist.gov/cyberframework)
(4) CIS Controls. Version 8. Center for Internet Security, Inc. (CIS). 2021 (https://www.cisecurity.org/controls)
(5) https://www.ntia.gov/sbom
(6) https://nsarchive.gwu.edu/document/17212-united-kingdom-government-threat-intelligence
(7) https://www.dnb.nl/voor-de-sector/betalingsverkeer/tiber-nl
(8) https://www.oasis-open.org/committees/openc2
(9) https://www.oasis-open.org/committees/cacao

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

COLUMN MARTIJN

Cybercriminelen hebben ook vakantie

De cybersecuritywereld draait meer en meer om externe aanvallers. Vroeger ging cybercriminaliteit vooral alleen om het geld, maar de belangen worden steeds complexer. Waardevolle data stelen, zelfs in opdracht van een overheid, of bepaalde landen of organisaties als doelwit uitkiezen vanuit ideologisch standpunt, alles zit erbij. Bij fysieke beveiliging kan je je nog voorstellen wie je tegenstander kan zijn, online blijft het een schim van een IP-adres en een vermoeden van het land waar criminelen zich verschuilen. Maar, we komen steeds meer te weten.

Lang geleden deed ik onderzoek naar een gehackt e-mailaccount waarbij geld was gestolen. Bij het analyseren van de acties van de criminelen werden er twee dingen duidelijk. Eén: ze waren verschrikkelijk goed in het nabootsen van echte e-mails. Ze deden uitvoerig onderzoek naar gesprekshistorie en zorgden dat er op eenzelfde manier werd gecommuniceerd. Twee: ze lieten soms per ongeluk sporen achter die wezen naar waar ze vandaan kwamen! In dit geval voegde het mailprogramma van de crimineel netjes een regel toe aan de e-mail: 'Piet schreef op 30 Februari 2028 om 15:40…'. Maar Piet had de mail om 10:10 (UTC) gestuurd. Ik zal toegeven, even dacht ik dat de tijd op de mailserver niet correct was. Aannames! Het mailprogramma van de crimineel staat natuurlijk netjes ingesteld op zijn tijdzone, wat in dit geval +5:30 is. Een hele kleine tijdzone voor alleen India en Sri Lanka.

Dit is maar een van vele voorbeelden van hoe we steeds beter beeld krijgen van criminele groeperingen (en niet alleen die met ransomware bezig zijn), hoe ze opereren, en waar ze zitten. Het geeft ons handvatten om belangrijke vragen te beantwoorden zoals: welke sancties zijn van toepassing op deze groep? Welke instanties kunnen helpen om ze op te sporen? Welke technieken gebruiken ze en hoe kunnen we ons daar het beste tegen verdedigen?

Maar ook mijn allerbelangrijkste vraag: hebben deze gasten nooit vakantie ofzo?! Ik krijg bijvoorbeeld notificaties bij elke nieuwe 'leak' van een ransomwaregroep. Dat zijn er veel, veel te veel. Als je in cybersecurity werkt lijkt het nieuws over ransomware-aanvallen nooit op te houden. Als het niet in Nederland is, dan wel in de EU, of een groot bedrijf in Amerika waar we over horen. Een recent rapport van ENISA over ransomware geeft waardevolle inzichten hierover. Op basis van meer dan 600 verschillende ransomware-incidenten in het afgelopen jaar geven ze antwoord op vragen over ransomware.

Zijn er sectoren die vaker als doelwit worden gekozen? Het lijkt er niet op. Aanvallen zijn ongericht, of je klein of groot bent, of je een transportbedrijf of professional services bent, het maakt niet uit.
In hoeveel cases wordt er losgeld betaald? Dat wil nog steeds niemand zeggen, daar moeten we naar gissen. Meerdere onderzoeken, waaronder deze, geven een percentage van rond de 60% aan.
Gaan ransomwarecriminelen met vakantie? Ja!

Oké, dat is mijn interpretatie van de data die bewijst dat er in de zomer beduidend minder gerapporteerde incidenten zijn. Ransomwarecriminelen hebben ook kinderen met zomervakantie, en nu de coronarestricties voorbij zijn, gaan ze er lekker op uit. Het is wellicht ook waarom we altijd in januari wat minder incidenten zien; daarin valt immers orthodoxe kerstmis, dat in Rusland wordt gevierd. (In het algemeen wordt Rusland het meest geassocieerd met ransomwaregroeperingen). Nu weet je voor de toekomst wanneer je je vakantie kan plannen: simpelweg even de schoolvakanties erbij pakken van het land waar de relevante boefjes zitten.

Auteur: Chris de Vries is redacteur van iB-Magazine en werkt als consultant onder de naam De Vries Impuls Management. Hij is bereikbaar via impuls@euronet.nl.

Hoe ICTU werkt aan een betere digitale overheid

Ken jij ICTU? Nee? Oké, daar uit de overheidshoek worden antwoorden geroepen. Zo zou het kunnen gaan in een grote zaal waar het plenaire deel van de conferentie plaatsvindt. ICTU (b)lijkt een vreemde eend in de bijt te zijn en toch vervult zij al lang een belangrijke rol in onze samenleving. ICTU acteert onder meer op het snijvlak van overheid en uitvoering. Op het terrein van informatiebeveiliging organiseert zij bijvoorbeeld jaarlijks de Overheidsbrede Cyberoefening voor het Ministerie van Buitenlandse Zaken.

ICTU is een overheidsstichting zonder winstdoel, opgericht in 2001. De volledige naam luidt: ICT-implementatie-organisatie Stichting ICTU, waarbij ICTU staat voor ICT-Uitvoerings-organisatie. Nu wordt enkel de naam ICTU gebruikt. Zie onder andere de brief van de minister voor grote steden- en integratie-beleid, R.H.L.M. van Boxtel, aan de voorzitters van de Eerste en Tweede Kamer. Oprichters van ICTU zijn de Staat en de Vereniging Nederlandse Gemeenten (VNG).

De oprichting was een antwoord op de behoefte om niet alleen beleidsvoorbereidend, maar ook bij de implementatie van ICT-programma's gericht op de overheid in projectvorm samen te werken. Daarbij wordt het bedrijfsleven waar mogelijk ingeschakeld. ICTU werkt zonder winstoogmerk in opdracht van verschillende overheden. ICTU zet beleid van overheden om in concrete projecten, diensten en producten. Alle overheden (ministeries, provincies, VNG) kunnen projecten door ICTU laten uitvoeren.

De programma's

ICTU houdt zich bezig met:

- advies
- realisatie van projecten en programma's en
- ontwikkeling van maatwerksoftware

1. Overheidsbrede cyberoefeningen

Een van de grotere projecten waarmee ICTU zich jaarlijks bezighoudt is de overheidsbrede cyberoefening waaruit diverse producten/diensten voortkomen, zoals:

1. De podcastserie 'Let's talk about hacks' (2)
2. Het cybermagazine (3)
3. De handreiking redteaming (4)
4. Het scenario van de Overheidsbrede Cyberoefening (5)
5. De masterclass ransomware (6)

2a. Digitale overheid

Via de website van ICTU, www.ictu.nl, is meer te lezen over de Overheidsbrede Cyberoefening die jaarlijks wordt georganiseerd. Een ander groot project is de website www.digitaleoverheid.nl die in opdracht van het Ministerie van BZK wordt beheerd. Een redactieteam binnen ICTU deelt informatie over de verschillende projecten met de professionals. De site www.digitaleoverheid.nl slaat een brug tussen het beleid en de professionals die werken aan digitalisering van de overheid. Je vindt er een schat aan informatie en praktische voorbeelden die helpen bij het verbeteren van de digitale dienstverlening van de overheid.

Figuur 1 - Infographic NH-SV.

2b. Desinformatie tegengaan

Via de website www.digitaleoverheid.nl verschenen onlangs berichten over projecten van andere overheidsorganisaties. Zo bracht ICTU voor Noord Holland Samen Veilig (NH-SV) aan het begin van dit jaar een infographic onder de aandacht met betrekking tot de 'aanpak online aangejaagde openbare ordeverstoringen'.

Op heldere wijze wordt een gemeente begeleid om 'online' aangejaagde openbare ordeverstoringen systematisch aan te pakken. De interventiekaart – waarbij opgemerkt dat deze niet statisch is – vormt daarbij een leesbare en goed op te volgen leidraad. Onderwerpen:

1. Doe niets.
2. Wees zichtbaar op social media en de-escaleer.
3. Zoek verbinding.
4. Burgerparticipatie.
5. Verwijder online uitingen 'Notice & Take Down (NTD).
6. Bestuurlijke bevoegdheden.

Op 6 februari 2022 verscheen via digitaleoverheid.nl een bericht van de VNG waarbij het onderwerp 'desinformatie' in samenhang met de gemeenteraadsverkiezingen aan de orde werd gesteld (7), aangevuld met onder meer een handreiking van de rijksoverheid (8). Daarnaast werd in opdracht van het Ministerie van BZK een serious game ontwikkeld door DROG. DROG doet onderzoek naar de effecten van nepnieuws en desinformatie. De game heeft als doel om politieke ambtsdragers bewust te maken van nepnieuws en de effecten daarvan (9). De game is door iedereen die daar interesse in heeft te spelen. De game staat niet op zichzelf, maar maakt onderdeel uit van het 'Leeraanbod Maatschappelijke Stabiliteit' (10). De game zelf, als originele bron, vind je terug op de website 'desinformatie in je gemeente' (11). Het leeraanbod Maatschappelijke Stabiliteit en de verschillende thema's (12), is een initiatief van 15 (rijks)partners, een imposant samenwerkingsverband (13). Definitie van NHL Stenden & Rijksuniversiteit Groningen: 'Online monitoring als praktijk omvat het anticiperen op veiligheidsrisico's, het opsporen van vragen en opmerkingen over de gemeente en het analyseren van opkomende issues van reputatie-uitingen over de gemeente' (14).

De vraag wat al het voorgaande opwerpt is of gemeenten mogen monitoren als een dergelijke dreiging wordt onderkend en aan welke voorwaarden dient te zijn voldaan. Een vraag die relevant is indien in ogenschouw wordt genomen dat: 'Uit onderzoek van NHL Stenden & Rijksuniversiteit Groningen is gebleken dat 75% van de gemeenten online monitoring tools gebruikt' (15).

Het onderzoek leidde tot een handreiking waarbinnen de volgende punten onder de aandacht werd gebracht:

1. Let op: er is in feite geen wettelijke basis.
2. Aangrenzende wetgeving (geen wettelijke basis, maar wel een handvat).
3. Juridische overwegingen (op basis van aangrenzende

Figuur 2 - Gesprekscanon Digitale Veiligheid.

wetgeving): de do & don't gekoppeld aan punten om op te nemen in een schriftelijk protocol.

4. Overleg & afstemming binnen de driehoek: burgemeester, de officier van justitie en de politie, maar daarnaast ook het overleg tussen de OOV'er (Openbare Orde en Veiligheid medewerker/monitorende ambtenaar) en de burgemeester.

En zo komt het VNG ook tot een 'Gesprekscanon Digitale Veiligheid' (16) zijnde bestuurlijke gesprekken tussen gemeentebestuurders en hun collegae en dat alles in een interactieve spelvorm. Via de website digitaleoverheid.nl en via verschillende andere kanalen werd de gesprekscanon onder de verschillende doelgroepen verspreid.

Via de website digitaleoverheid.nl werden meer relevante berichten verspreid rondom het thema informatiebeveiliging. Een greep uit recente berichten: Kwetsbaarheden in Log4j: geleerde lessen; Oefen een cyberincident met de serious game 'Alisson' met drie scenario's: het Zontach-, Castra- en Citrix-scenario en last but not least het Overheidsbrede Cyberprogramma 2022:

Activiteiten	Wanneer
Cyberwebinars	Juni en oktober 2022
Kick off Cybersecurity Maand	03 oktober 2022
Bestuurlijke cyberspecial	Oktober 2022
Overheidsbrede Cyberoefening	31 oktober 2022
Cybermasterclass	29 november 2022

Figuur 3 - Overheidsbrede Cyberprogramma 2022.

Al met al een organisatie om nauwgezet te volgen, of minstens om op de hoogte te blijven van de actualiteit bij de overheid. Voor de website van ICTU's zie (17).

Referenties

(1) zoek.officielebekendmakingen.nl/kst-27510-1.html
(2) open.spotify.com/episode/15m1NYuy2ZNhwIU7iRC5vB
(3) cyber-magazine.nl/
(4) www.digitaleoverheid.nl/nieuws/red-teaming-oefen-met-een-realistische-digitale-aanval/
(5) www.digitaleoverheid.nl/document/zelf-aan-de-slag-met-scenario-cyberoefening/
(6) player.vimeo.com/video/654055662?h=c7d1f1cace
(7) vng.nl/nieuws/hoe-te-handelen-bij-online-aangejaagde-ordeverstoringen
(8) www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2022/02/09/handreiking-omgaan-met-desinformatie/BZK+-+Handreiking+omgaan+met+desinformatie.pdf
(9) www.digitaleoverheid.nl/nieuws/game-om-bewust-te-worden-van-nepnieuws/
(10) maatschappelijkestabiliteit.nl/bronnen/desinformatie_game
(11) www.desinformatieinjegemeente.nl/#intro
(12) maatschappelijkestabiliteit.nl/
(13) maatschappelijkestabiliteit.nl/partners/
(14) nh-sv.nl/action/?action=download&id=143
(15) ibid
(16) vng.nl/nieuws/bestuurlijke-gesprekken-over-digitale-veiligheid-van-start
(17) www.ictu.nl/

Even voorstellen

Weer een bestuurscolumn van een nieuw bestuurslid en dit keer vanuit de activiteitencommissie. Ik ben Stefan Veenendaal (31) en heb begin van dit jaar het stokje overgenomen van Kelvin Rorive. Hij heeft zich afgelopen tien jaar volledig ingezet voor het PvIB, waaronder als voorzitter van onze commissie, en blijft gelukkig nog steeds actief als lid van de activiteitencommissie. We bestaan nu uit dertien vrijwilligers en blijven relevante, inhoudelijke en sociale evenementen voor jullie organiseren.

Op de middelbare school bouwde ik weleens een website in HTML en kwam ik in aanraking met de eerste Trojans. Die kon je toen nog (dacht ik) vrij onschuldig via MSN versturen om iemands cd-romspeler te openen. Ik vond dit iets magisch hebben en besloot na mijn middelbare school te kiezen voor de mbo-opleiding Particulier Digitaal Onderzoeker in Utrecht. Hier werd ons al vrij snel wat bijgebracht over ethiek, techniek en digitale veiligheid.

Het vakgebied grijpt mij aan en ik besloot mijn studie te vervolgen in Zoetermeer op de Haagse Hogeschool. De opleiding Information Security Management (nu HBO-ICT) ging niet alleen in op de techniek maar ook de menselijke en beleids/procesmatige kant van Informatiebeveiliging. Ik begeef me nog steeds in het midden van die driehoek en heb besloten geen partij te kiezen: People -> Process -> Technology.

Tijdens de studie was het de bedoeling om onze opdrachten zoveel mogelijk uit te voeren voor 'echte opdrachtgevers'. Hierdoor leer je direct hoe het er in de praktijk aan toe gaat! Een plek om deze opdrachtgevers te leren kennen is het PvIB. Onze docent Leo van Koppen nam ons mee naar een eerste thema-avond. Dit was spannend, je loopt tussen mensen die al veel ervaring hebben in het vakgebied terwijl je zelf net start. We vielen op als jong publiek wat voor de nodige aanspraak zorgde en de eerste opdracht was gescoord.

Elke sessie een ander thema, de verschillende mensen die samenkomen en de openheid van het PvIB zorgen ervoor dat ik zeven jaar later nog steeds lid ben van het PvIB. Deze eigenschappen kenmerken het PvIB en blijf ik waarborgen zolang ik voorzitter ben van de activiteitencommissie. We willen en blijven sessies organiseren waar je vakgenoten kan ontmoeten (jong en oud), je kennis kan verbreden of verdiepen en zelf een actieve bijdrage kan leveren.

Heb je ideeën voor een sessie, lijkt het je leuk om mee te werken in de activiteitencommissie of heb je een andere vraag? Spreek mij dan vooral aan tijdens een van onze activiteiten. Ik hoop je daar snel te ontmoeten!

Stefan Veenendaal

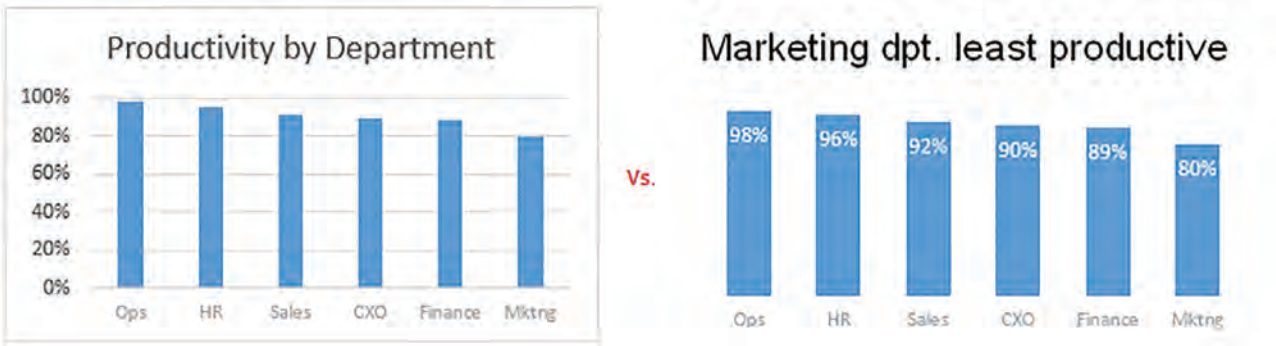
Auteur: Robert Metsemakers is als ervaren IT-auditor en informatiebeveiligingsexpert beschikbaar voor security-advies via: robert.metsemakers@gmail.com. Zie voor andere artikelen www.linkedin.com/in/robert-metsemakers, 'publicaties'.

BLOG

Meer impact met minimalisme, data looks better naked

Let hierop als je in een vergadering een grafiek presenteert:

1. Laat overbodige of dubbele gegevens weg;
2. Geef minder belangrijke gegevens minder aandacht;
3. Leg nadruk op de belangrijke zaken (met GROTE letters, **vetgedrukt**, in kleur).



Figuur 1 - Bron: https://chandoo.org/wp/rules-for-making-awesome-column-charts.

Soms heeft het publiek extra uitleg nodig. Een grafiek helpt dan om onderliggende gegevens te tonen

Minimalistische slide

Bij een interne presentatie weet je publiek echt wel waar ze werken en welke dag het is. Het gaat ze meer om de presentatie-inhoud dan om de titel of jouw naam. Die gegevens hoef je dus niet allemaal op elke slide te herhalen. Ook bij externe presentaties hoeft dat niet per se.
Laat, als onderaan elke slide onder een horizontale lijn alleen een paginanummer staat, beide items weg. Je toeschouwers kunnen immers maximaal zeven visuele items tegelijk verwerken. Als die lijn toch moet van de huisstijl, maak hem dan niet rood of lichtblauw. Dat trekt de aandacht en leidt af van je echte boodschap. Grijs? Prima, maar niet vijftig verschillende tinten op één slide. Bedenk eerst een inhoudelijke titel. Wat wil je zeggen met de slide? Dus waarom bestaat hij? Kun je dat niet in één korte zin formuleren, laat hem dan weg uit je presentatie. Vaak past deze verzonnen zin bij wat het publiek toch al verwacht of meteen als logisch van je accepteert. Als men instemmend knikt na het lezen van de titel, kun je meteen naar de volgende slide in je presentatie.

De grote, vette letters (zie krantenkoppen) wordt door McKinsey' een 'so what' regel genoemd. Ervaren krantenlezers weten: het antwoord op de vraag in een kop is altijd 'neen'. Gebruik dus geen vraag, maar zeg wat je bedoelt. Dus in het voorbeeld hierboven niet 'Productiviteit per afdeling', maar eerder 'Marketing is de minst productieve afdeling in ons bedrijf'. Soms heeft het publiek extra uitleg nodig. Een grafiek helpt dan om onderliggende gegevens te tonen, zeker als je hun ontwikkeling in de tijd of hun onderlinge relatie zichtbaar wilt maken.

Minimalistische grafiek

Leg in een grafiek de nadruk op de data en niet op versiersels. Effen wit is een betere achtergrond dan bont gekleurd. Wit vormt een 'passe-partout' om de grafiek, dus aparte kaderlijnen zijn overbodig. Als je met labels in een kolom (verticaal) of balk (horizontaal) grafiek exact de afgebeelde waardes toont, kun je de Y-as of X-as weglaten, net als horizontale en verticale hulplijnen richting die assen. Door labels te plaatsen bij de lijnen in een lijngrafiek, in/naast een balk of in/onder een kolom ziet je publiek ondubbelzinnig welke gegevens worden getoond. Maar het gaat in de grafiek om het vergelijkende gevoel: welke staaf is de grootste, welke is de kortste? Je kunt natuurlijk afspreken in je organisatie dat je de kolommen of balken altijd oplopend (of aflopend) sorteert, dan weet je waar je moet kijken.
Excel-gebruikers weten dat je die ene kolom afwijkend kunt kleuren, als je in de grafiek twee dataranges tegelijk toont. In de oorspronkelijke datarange zet je die ene kolom op nul. Die tweede datarange bevat alleen die apart te kleuren waarde en verder allemaal nullen. Heel makkelijk, de tweede keer dat je het doet.

Maar eigenlijk zijn door gebruik van labels in een kolom of balk grafiek aparte kleuren per rechthoek overbodig. Alles in een kleur is minder druk en goedkoper af te drukken. En ook de legenda (een aparte box bij de grafiek, normaliter met een eigen kader en achtergrond, die de betekenis van de gebruikte kleuren toelicht) kan vervallen.

Vermeld de bron van de getoonde data onderaan wel, maar in grijze, kleinere letters. Dan leidt het de reeds overtuigde luisteraars niet af en de muggenzifters zijn ook tevreden.
Darkhorse Analytics heeft een animatie "data looks better naked" over het met impact presenteren van een kolom grafiek.

Zie ook: https://www.darkhorseanalytics.com/portfolio/data-looks-better-naked-bar-charts

Auteurs: Chris de Vries is redacteur van iB-Magazine en werkt als consultant onder de naam De Vries Impuls Management. Chris is bereikbaar via impuls@euronet.nl. Mr. A.IJ. Ard Ruiter is bestuurslid van PvIB en werkt als privacy- en beveiligingsfunctionaris/senior inspecteur bij de ILT Inlichtingen en Opsporingsdienst (ILTIOD). Ard is bereikbaar via LinkedIn.

INTERVIEW

Drs. Johan van den Bosch MCM CISA (agentschap Telecom) projectleider CSA en NCCA:

‘Securitycertificering steeds meer een Europese aangelegenheid’

Sinds april van dit jaar heeft het Agentschap Telecom er een nieuwe taak bij: de Nationale Cybersecuritycertificeringsautoriteit (NCCA). Een interessant onderwerp waar we meer van willen weten. Johan van den Bosch, projectleider NCCA bij het AT, stond ons welwillend en geëngageerd te woord.

In onze samenleving is de beschikbaarheid en betrouwbaarheid van de digitale infrastructuur enorm belangrijk. Agentschap Telecom (AT) voert de wet- en regelgeving uit op dit gebied en houdt er toezicht op dat iedereen zich aan de regels, eisen en voorwaarden houdt. Het AT is een overheidsorganisatie en is ondergebracht bij het ministerie van Economische Zaken en Klimaat (EZK) en heeft zowel uitvoerende als toezichthoudende taken voor de digitale infrastructuur. Het agentschap doet dat ook op andere terreinen, zoals bijvoorbeeld de wet die toeziet op veilig graven (Wibon), weegschalen, goud, zilver of platina en ruimtevaartactiviteiten. De taken van het AT omvatten het werkgebied Nederland, waaronder ook Caribisch Nederland. Daarnaast doet het AT onderzoek en brengt ze trends op het gebied van technologie, media en digitale infrastructuur in beeld. De AT is de Nationale Cybersecuritycertificeringsautoriteit (NCCA) voor Nederland geworden.

Het AT gaat als NCCA de certificerings- en toezichtstaken uit CSA uitvoeren. Wat kunnen we verstaan onder de certificerings- en toezichtstaken uit CSA? Wat gaat u precies doen en wat merken we daarvan?
Van den Bosch: "De Wet beveiliging netwerk- en informatiebeveiliging (Wbni) is op 9 november 2018 ingevoerd. De Wbni volgt op de NIS-directive (in het Nederlands NIB-richtlijn) van de Europese Unie, die moet zorgen voor meer eenheid in beleid over netwerk- en informatiebeveiliging. Dit is de Nederlandse implementatie van de Directive on security of Network and Information Systems (NIS-directive). De Wbni dicteert onder meer dat organisaties passende technische en organisatorische maatregelen op het gebied van cybersecurity moeten nemen. Op de NIS komt een opvolger: NIS2. NIS2 moet de cybersecurity-eisen in Europa verhogen en meer organisaties aanmerken als essentieel bedrijf. Het gaat om zo'n 160.000 organisaties door heel Europa. Deze bedrijven moeten gaan voldoen aan hogere eisen."

Met enthousiasme vertelt Johan van den Bosch over de vier taken van de NCCA: "Twee taken gaan over de voorafgaande goedkeuring; de andere twee over het behoud en de handhaving van goede certificering. De eerste betreft de CSA-taak. Certificering gebeurt dan volgens de CSA-zekerheidsniveaus, te weten: 'basis', 'substantieel' en 'hoog risico'. Dat laatste, meest intensieve niveau, gaat om producten of diensten die een grotere impact op de samenleving hebben als het misgaat. Nederland kiest uitdrukkelijk voor het systeem van 'prior approval'. De certificering van de producten op het CSA niveau 'hoog' worden door NCCA voorafgaand aan de uitreiking van het certificaat extra gecontroleerd en goedgekeurd. Pas daarna mag door de certificerende instelling het certificaat aan haar klant, die een product of dienst heeft laten certificeren, worden uitgegeven. In Duitsland, Frankrijk, Italië en Spanje geeft de overheid zelf certificaten uit om diezelfde mate van controle te bereiken. De kracht van ons land: er zijn goede Nederlandse partijen in de markt voor conformiteitsbeoordeling. In Europa is Nederland één van de meest actieve landen en wij zijn één van de leidende inbrengers binnen het Europese samenwerkingsverband."

Waar staat CSA voor?
CSA staat voor Cyber Security Act, de Europese wetgeving voor cyberbeveiliging die sinds 2019 van kracht is en aansluit op de Wbni. Europese lidstaten hebben de laatste jaren, ieder voor zich, verschillende certificeringsverplichtingen ingevoerd. De CSA moet zorgen voor regels die voor alle lidstaten hetzelfde zijn. Fabrikanten en dienstverleners behalen straks niet meer in elk lidstaat afzonderlijk een certificaat. De Europese regeling vervangt dus vergelijkbare nationale certificeringen.

"De tweede taak van de NCCA heeft betrekking op de toelating van CBI's (Conformiteitsbeoordelingsinstanties) (1) tot het Europese certificeringsstelsel. De CBI's moeten CSA geaccrediteerd zijn gebaseerd op de ISO17065-norm. Dat is de ISO-norm die de vereisten vaststelt voor organisaties die producten, processen en/of diensten mogen certificeren. Deze vereisten omvatten de competentienormen vanuit de opgestelde certificeringsschema's. De NCCA toetst of CB's en CAB's voldoen aan de additionele eisen in het certificeringsschema (dus eisen bovenop de ISO17065). Monitoring van certificeringstrajecten op het CSA Assurance Level Hoog betekent dat bij een positief oordeel, een goedkeuring verleend wordt aan de CB voor uitreiking van het certificaat aan de klant van de CB die een product of dienst heeft laten certificeren.

In het geval van additionele eisen is dan verificatie nodig, zonder additionele eisen is enkel certificatie vereist. Is het niveau substantieel, dan zorgen Notified Bodies (NB) voor productcertificering. Dit gaat als proces verder omdat er hogere eisen worden gesteld dan bij de competentienormen. Die eisen zijn transparanter – want opgenomen in schema's –, in vergelijking met product-NB's. Certificatieclaims (QR-codes) worden gepubliceerd en zijn dus te controleren door de gebruiker (2)."

De derde taak van het NCCA is het toezicht dat achteraf plaatsvindt. Projectleider Van den Bosch vertelt dat het ook gaat om het controleren of gecertificeerde producten en diensten nog steeds voldoen aan de vereisten uit het certificeringsschema. "De eerste stap is dan controle van het certificatiedossier van de certificerende instelling. De tweede stap kan dan zijn verdere controles of hertesten van product of dienst bij de fabrikant of provider, de houder van het certificaat. Dit gebeurt zowel gedurende de levenscyclus van het product, de dienst en het proces als de geldigheidsduur van het certificaat. Opgave voor de fabrikant en dienstverlener zal het proces 'vulnerability handling' zijn: 'hoe behandel ik de kwetsbaarheden?' Kwetsbaarheden kunnen zich immers ook voordoen als het gecertificeerde product al in de markt is. Het resultaat van een certificatie in het verleden, is niet per se een garantie voor de toekomst. Dat proces kan leiden tot de noodzaak van hercertificatie, ook bij wijzigingen van of in het product. Uitgangspunt is dat er veel meer beheersing wordt gevraagd met betrekking tot de kwetsbaarheden, risico's en/of wijzigingen. Dit stelt dus specifiek eisen aan het management, de ontwikkeling, de productie en het beheer van IT-producten, -diensten en -processen."

Certificering in Europa

Wil een certificerende instelling (Certification Body (CB)) actief zijn onder een Europees CSA-schema, dan moet het door de Raad voor Accreditatie worden geaccrediteerd per CSA-certificeringsschema. Het eerste certificeringsschema zal zijn de 'Common Criteria based European Union Cybersecurity Certification scheme (EUCC)'. Dat schema vervangt het SOG-IS (basisschema in verschillende landen). Het EUCC-schema is bedoeld voor certificering van IT-producten, ook wel beveiligingsproducten genoemd. ENISA heeft het kandidaatschema opgeleverd aan de Europese commissie die de tekst verwerkt in een Europese regeling onder de CSA. Na de publicatie van de regeling zal Nederland de deelname aan het Nederlands Schema voor de Certificatie op het gebied van IT-Beveiliging (NSCIB) gaan beëindigen.

Wens EU om te harmoniseren

De EU wil harmoniseren, hetgeen een direct gevolg is van de Digital Single Market Strategy (DSMS). Het Europese Common Criteria certificeringsschema (EUCC) bevordert harmonisatie van nationale - met internationale normen en is een multilaterale overeenkomst onder deelnemende landen en certificatie-instanties. Meer dan 50 landen nemen momenteel deel aan de regeling, met inbegrip van de belangrijkste, industriële naties. Een tweede reden voor de wens om te harmoniseren is de verhoging van de cyberweerbaarheid, de digitale autonomie en datasoevereiniteit. Het wordt ook telkenmale in de Europese State of the Union geplaatst.

De vierde taak van het NCCA omvat het toezicht op CBI's en testlaboratoria. Dat toezicht bestaat uit: toetsing van de naleving door de CB van de verplichtingen die opgenomen zijn in de CSA- en EU- certificeringsschema's en de toetsing van de competenties van de CB. Passen zij certificeringseisen uit de EU certificeringsschema's op een juiste wijze toe? Johan van den Bosch beoordeelt of een Conformiteitsbeoordelingsinstantie Europese CSA-certificeringen kan en mag uitvoeren (toelating). Verder beoordeelt hij op het CSA-zekerheidsniveau 'hoog' of een CBI aan het einde van het certificeringstraject een Europees certificaat mag uitreiken (voorafgaande goedkeuring) en ten slotte of een geaccrediteerde CBI toestemming mag geven aan de fabrikant om het Common Criteria Recognition Arrangement-logo (CCRA) te gebruiken bij communicatie over een gecertificeerd product. Wat toezicht betreft, let het NCCA op de naleving van de certificeringsvereisten door fabrikanten en aanbieders die een IT-product, - dienst of –proces hebben laten certificeren alsook op de naleving van de certificeringsvereisten door de toegelaten CBI's.

Welk advies zou het Agentschap Telecom/de NCCA de lezers van iB-Magazine geven ten aanzien van scholing en uw certificatiebeleid?

Van den Bosch: "Na- of bijscholing is niet aan het NCCA. Het is verstandig dat leveranciers, afnemers en adviseurs de ontwikkelingen volgen en dan onder meer aandacht hebben voor de schema's die in ontwikkeling zijn en verplichtingen tot certificering die mogelijk in de nabije toekomst gaan gelden. Voor de lezer zal wel van belang zijn, de vraag: 'Wat betekent certificatie voor onze marktbenadering? Welke wensen kunnen klanten met betrekking tot die eisen naar voren brengen?' Uiteindelijk kunnen klanten bij de inkoop van producten en/of diensten CSA-certificeringen gaan eisen dan wel een voorkeur voor uitspreken. Onder de NIS2 zullen in Nederland circa 5.000 partijen vallen. Ook voor kleine bedrijven kan NIS2 spelen. Ga zo nodig – inzake de certificering – ook in gesprek met AT. Wacht niet totdat NIS2 actief wordt, dan ben je te laat! Cybersecurity wordt steeds meer een EU aangelegenheid, kijk dus naar de EU-ontwikkelingen en regelgeving. Let daarbij op de Data resilience act dat omvat alle data veiligheidseisen gekoppeld aan alle IT-producten."

Moeten onze lezers een kennis- en vaardigheidscertificaat bij de AT/NCCA binnenhalen?

"Kennis en vaardigheden over het thema certificering en marktsegmentatie (bijvoorbeeld inzake 'main archetypes suppliers/competitive dynamics IoT-market' (3)) zullen nodig zijn om een relatie tussen een schema en producten en diensten te kunnen leggen. Scholing is geen kerntaak van de NCCA, het advies is om de ontwikkelingen op de voet te volgen, zodat bedrijven er goed en tijdig op in kunnen spelen."

Ziet u hier knelpunten, zijn er voldoende gekwalificeerde CBI's en leeft de NIS-directive voldoende bij uw doelgroepen?

"Nederland heeft een sterke markt voor conformiteitsbeoordeling. Agentschap Telecom doet wat in haar vermogen ligt om bij de doelgroepen van regelgeving onder de aandacht te brengen. In het kader van de CSA is de doelgroep fabrikanten en providers lastig te benaderen, omdat deze groep heel groot is en zich over de hele wereld kan bevinden. Voor certificerende instellingen en testlaboratoria ligt dat anders, de groep die in Nederland actief is kennen we en daar zitten we al twee jaar mee om tafel. Het gaat in hier om IT-producten, -diensten en -processen."

Wat denkt u als u de zeer krappe, professionele markt in ogenschouw neemt en bedrijven een NCCA-certificaat willen behalen?

"Groot aandachtspunt. Ook het Agentschap Telecom zoekt mensen, en zeker bij de operationalisering van de eerste schema's met name dus vanaf het einde van dit jaar en 2023 en verder. Bel ons dus gerust. Het werk moet je natuurlijk wel liggen, het gaat om monitoren en toezichthouden; dat is werk met een grote maatschappelijke impact. Om- en bijscholing is wellicht een oplossing voor tekorten. Efficiënte combinaties van werk kunnen bijdragen daar waar het toezicht op de CSA en het toezicht op andere AT-toezichtsdomeinen elkaar raken."

"Effectiviteit aan het voorgaande is daarbij essentieel. Het AT streeft ernaar om haar toezichtstaken in samenhang op te pakken. Dit vanuit de doelstelling om de toezichtslast voor ondernemingen te beperken. Bij de toelating (de autorisatie): het werk van de NCCA voor de toelating invoegen in het werk van de RvA met betrekking tot de accreditatie. De NCCA vervult dan de rol van expert in het accreditatietraject om additionele schema-eisen zoals competenties te toetsen. Dat betekent dat wanneer een partij is geaccrediteerd, de toelating een formaliteit kan zijn."

Fabrikanten en dienstverleners hebben een beperkte ruimte om certificeringseisen te interpreteren en te implementeren.

Hoe beoordeelt het AT wat precies CSA-gecertificeerde producten-, diensten- en processen zouden moeten zijn? Welke kaders hanteert de NCCA?

"De NCCA heeft niet zelfstandig de mogelijkheid om eenzijdig Europese regels aan te passen. De certificeringschema's schrijven de eisen voor, waarop de NCCA toetst. Andere EU-regelgeving (zoals de NIS en CRA) zal verplichtingen tot certificering of tot gebruik van gecertificeerde producten en diensten gaan bevatten. Het AT/NCCA is deelnemer in de Europese Cybersecurity Certification Group (ECCG), die zorgt voor de ontwikkeling en beheer van de schema's. Het ECCG is in de CSA genoemd als officieel adviesorgaan van de Europese Commissie, het dagelijks bestuur van de Europese Unie op het gebied van cybersecurity. Het Europees Agentschap voor netwerk- en informatiebeveiliging ENISA krijgt opdracht van de EC tot ontwikkeling van een schema en betrekt dan externe experts en de ECCG-leden, de lidstaten, bij de ontwikkeling in een Ad Hoc Working Group (AHWG)."

Bezitten de ondernemingen die een certificaat aanvragen eigen beoordelingsruimte?

"Nee. In beginsel zijn certificeringseisen zeer concreet, de certificerende instelling interpreteert voor zover er ruimte is. Op de achtergrond kijkt de NCCA mee. Als gebreken blijven, zal het AT in haar rol als NCCA actie ondernemen met als doel het herstel van de veiligheid van een product of dienst. Ultimo kan dat leiden tot boetes, maar voordat daartoe wordt overgegaan is er al veel met elkaar gesproken. Er wordt eerst onderzoek gedaan en daarna volgt overleg en het geven van aanwijzingen. De CSA verplicht de betrokken organisaties de instantie volledige en juiste informatie aan te leveren, zo niet, dan kan het AT het certificaat in laten trekken en de Europese registratie schorsen."

"Fabrikanten en dienstverleners hebben een beperkte ruimte om certificeringseisen te interpreteren en te implementeren. Die ruimte zit voornamelijk in de keuze voor gebruikte technologie of wijze waarop een proces is ingericht. Dat is de aard van certificering. Indien een certificaathouder niet voldoet aan de eisen dan zal deze in veel gevallen de gelegenheid krijgen om dit binnen redelijke termijn te herstellen, maar het is ook mogelijk dat het certificeringsschema voorschrijft dat bij bepaald type non-conformiteit het certificaat direct moet worden ingetrokken en dat na herstel hercertificering nodig is. Ik verwacht dat in de meeste gevallen de mogelijkheid van verlies van het certificaat voorkomt dat er boetes moeten worden opgelegd."

Welke zorgen en aandachtspunten ziet het AT nu op de markten?

"Neem de certificatie-eisen op in de eigen inkoopvoorwaarden. Certificering kost tijd en is niet meer vrijblijvend. De Network & Information Security-2 directive zal verwijzen naar CSA-schema's. Dat betekent de mogelijkheid van het ontstaan van verplichtingen voor de vitale partijen."
De boodschap van Van den Bosch, als projectleider NCCA, aan de afnemers: "Kijk eens waar je zelf aan moet voldoen. Analyseer de eigen inkoopvoorwaarden daarop. Wordt actief. De hyperscalers vind je nu al actief in overleg, ook al moeten zij het nodige nog uitvinden."

Kunnen het AT, de NCCA en de informatiebeveiligers elkaar helpen? Zo ja, hoe ziet u dat?

"Allereerst kan uw lezer aandacht vragen voor deze ontwikkeling bij zijn of haar relaties en daar waar nodig de relatie en/of organisatie van advies dienen. Komt men in de markt fouten of gebreken tegen, meldt deze onregelmatigheden dan aan ons."

Drs. Johan van den Bosch MCM CISA werkt bij het Agentschap Telecom en is projectleider CSA en NCCA. Hij is bereikbaar via ncca@agentschaptelecom.nl.

Referenties

(1) ec.europa.eu/growth/single-market/goods/building-blocks/accreditation-conformity-assessment-bodies_en
(2) ITSEF: IT Security Evaluation Facility
(3) Zie ook: www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid

De Nederlandse NCCA

Agentschap Telecom bereidt zich al vanaf 2019 voor op de certificerende NCCA-taken en de NCCA-toezichthoudende taken. Nederland heeft gekozen om certificerende taken volgens de CSA-optie van 'prior approval' uit te voeren, de 'voorafgaande goedkeuring'.

Agentschap Telecom als Nationale Cybersecuritycertificeringsautoriteit (NCCA)

De Nederlandse Nationale Cybersecuritycertificeringsautoriteit (NCCA) heeft een rol bij het certificeren van IT-producten, -diensten en -processen en het toezicht daarop. De Nederlandse NCCA wordt ingesteld op grond van de CSA-uitvoeringswet. De CSA-uitvoeringswet ligt bij het parlement ter behandeling. In de Memorie van Toelichting spreekt de regering het voornemen uit om de NCCA-taken bij Agentschap Telecom te beleggen.

NCCA-certificering:

- Beoordeelt of een conformiteitsbeoordelende instantie (CBI) Europese CSA-certificeringen kan en mag uitvoeren (toelating);
- Beoordeelt op het CSA-zekerheidsniveau 'hoog' of een CBI aan het einde van het certificeringstraject een Europees certificaat mag uitreiken (voorafgaande goedkeuring);
- Beoordeelt of een geaccrediteerde CBI toestemming mag geven aan de fabrikant om het 'Common Criteria Recognition Arrangement' (CCRA) logo te gebruiken bij communicatie over een gecertificeerd product.

NCCA-toezicht:

- Houdt toezicht op de naleving van de certificeringsvereisten door fabrikanten en aanbieders die een IT-product, -dienst of -proces hebben laten certificeren;
- Houdt toezicht op de naleving van de certificeringsvereisten door de toegelaten CBI's.

De Europese certificeringregelingen zijn nog in ontwikkeling. De opbouw van de NCCA-taken bij Agentschap Telecom strekt zich daarom over meerdere jaren uit. Met elk nieuwe Europees certificeringsschema (1(groeit de omvang van de NCCA-taken van Agentschap Telecom. Het eerste certificeringsschema is het EUCC-schema voor certificering van IT-producten. ENISA heeft het kandidaatschema opgeleverd aan de Europese commissie die de tekst verwerkt in een Europese regeling onder de CSA. De verwachting is dat de regeling begin 2022 wordt gepubliceerd.

Context CSA

In juni 2019 is de Europese 'Cybersecurity Act' (CSA) van kracht geworden. De CSA is een verordening waarmee de Europese Unie grensoverschrijdende cyberaanvallen beter het hoofd wil bieden. Onder de CSA-certificeringsschema's kunnen IT-producten, -diensten en -processen gecertificeerd worden op het gebied van cybersecurity. De rol van Nederlandse Nationale Cybersecuritycertificeringsautoriteit (NCCA) is ondergebracht bij Agentschap Telecom. Agentschap Telecom geeft hiermee invulling aan de certificerings- en toezichtstaken uit CSA.

Europese CSA-certificaten

Afnemers van CSA-gecertificeerde producten, -diensten en processen krijgen de zekerheid dat deze voldoen aan de cybersecurity-eisen uit de certificeringsregeling. Het is voor de aanbieders, fabrikanten en dienstverleners daarom interessant om gecertificeerde producten, diensten of processen op de markt te brengen. Europese CSA-certificaten voor IT-producten, -diensten en -processen worden erkend in elke EU-lidstaat. Hierdoor maakt een fabrikant geen kosten voor certificering in elke afzonderlijke lidstaat. Momenteel is CSA-certificering nog vrijwillig, maar op termijn verandert dat waarschijnlijk. In sommige gevallen zullen afnemers door andere nationale of Europese regelgeving verplicht worden om CSA-gecertificeerde producten-, diensten- en processen af te nemen.

Referentie

(1) www.agentschaptelecom.nl/onderwerpen/cybersecurity-certificering

Achter Het Nieuws

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

De mens wel/niet de zwakste schakel in informatiebeveiliging

Zodra we het hebben over informatiebeveiliging, gaat het over houding en gedrag van mensen. Dat is logisch, want vaak komen de grootste fouten in onze digitale wereld voort uit onachtzaamheid en nonchalance. En wat definieert dan een fout? Eigenlijk altijd, enkel en alleen, het resultaat. Of dit nu 'positief' is (gezien vanuit de hacker: doorbreking van een beveiliging) of 'negatief' (gezien vanuit ons als slachtoffer: de ongeoorloofde overboeking van een bedrag, wat direct een verlies betekent!).

Chris de Vries | Fook Hwa Tan | Nicole van Deursen | Tom Bakker

Praat erover en leer van elke fout van jezelf en die van een ander.

De keten is zo sterk als haar zwakste schakel en in elke digitale keten is dat altijd de mens! Natuurlijk moeten wij het in de informatiebeveiliging dus hebben over dat falend wezen, die domoor/sufferd/…, wiens catastrofale handeling iedereen natuurlijk voorzien had (vanuit het standpunt dat je altijd 'achteraf de koe in de kont kijkt'). Of niet soms? Wij hebben onze redactieleden gevraagd wat zij vinden van deze automatische reactie. Hoe staan zij tegenover deze onachtzame en nonchalante 'dader'? Hebben zij weleens in diens schoenen gestaan? Zo niet, wat zien zij als reden dat zij het goed hebben gedaan. Daarom een reflectie uit de zielen van de redactie.

Chris de Vries - Geluk, geluk, geluk en bedachtzaamheid

De enige keer dat ik ooit waargenomen heb dat mijn computer besmet was geraakt, betrof een eenvoudig macrovirus in een Wordperfectprogramma (voorloper van MS Word) en dat moet ergens midden de jaren 80 geweest zijn. Waargenomen, want hoe vaak ben ik niet besmet geweest, terwijl ik onwetend bleef? Dat dank ik, vermoed ik, aan drie factoren: geluk was aan mijn zijde, mijn bankiersachtergrond en mijzelf opgelegde vertragingen.

Geluk is het belangrijkste, maar dat kan bevorderd worden door discipline. Discipline die in mijn eerste arbeidsjaren als bankier werd gevoed door de noodzaak van vertrouwelijkheid, zorgvuldigheid en bedachtzaamheid. Als faillissementenbeheerder ga je om met het leven van anderen. Dat heb ik altijd als een grote verantwoordelijkheid ervaren en dus legde ik mij op vele acties vertraagd door te voeren; lees: te overdenken en de reflex te beheersen! Dat is weleens fout gegaan, ik bleek mens te zijn….

Daarnaast mijn filosofische aanleg en herkenning van veel in de deugden van de Stoïcijnen. Dat zijn er vier: moed, matigheid, rechtvaardigheid en wijsheid. Met deze beschikbare werktuigen benader ik mijn handelingen, mijn werk, mijn leven. Daar komt mijn begrip voor de mens als 'zwakste' schakel uit voort en voorkwam ik de grootste fouten in informatiebeveiliging.

Nicole van Deursen - Mensen zijn sterke schakels

Ik zal niet snel zeggen dat mensen zwakke schakels zijn. Ik hou niet van negatief geformuleerde boodschappen in ons vak. Mensen zijn niet altijd zwak, een hacker is niet per definitie een crimineel en techniek is niet per se moeilijk. We maken allemaal weleens een fout of we zien iets over het hoofd. Waar het om gaat is hoe je daarna handelt: ga je het herstellen en ervan leren, of geef je een ander de schuld? Veel fouten komen voort door gebrek aan digitale geletterdheid, werkdruk of interesse. Als je niet goed weet hoe iets werkt, als je onder te veel stress moet werken (lichte stress schijnt juist weer goed te zijn), of je vindt het niet echt interessant, dan kan het zijn dat je op een verkeerd linkje klikt of een instelling over het hoofd ziet. Meestal blijven mensen wel weg van zaken waar ze geen verstand van hebben. Maar er is bijna geen beroep meer waar je om computers heen kunt. Je moet dus wel gaan bijleren en 'zin maken'. Digitale geletterdheid begint al op school en ik hoop dat de volgende generaties van hun (beroeps)opleidingen komen met betere digitale vaardigheden dan mijn generatie. Werkgevers hebben ook een verantwoordelijkheid naar (nieuwe) medewerkers. Die weten niet vanzelfsprekend alles van de systemen waarmee je ze laat werken en vinden het ook niet altijd leuk om zich daar in te verdiepen. Train ze goed in de basis van het gebruik van een systeem voordat je veilig gedrag verwacht. En zorg dat ze zich veilig voelen om te rapporteren wanneer ze toch de mist in zijn gegaan. Praat erover en leer van elke fout van jezelf en die van een ander. Zo maken we onszelf weerbaar.

Fook Hwa - Mensen zijn je belangrijkste verdediging

Binnen informatiebeveiliging bouwen en beschermen we een organisatie door verschillende lagen van beveiliging op te richten. Dit betekent, dat we door maatregelen te nemen in processen en technologie en mensen daarover te leren, we het moeilijker maken voor criminelen om een organisatie binnen te komen om iets mee te nemen of schade aan te richten.

De mens wordt vaak gezien als de zwakste schakel. Maar is dit wel zo? Processen worden ingericht om te zorgen dat er geen ongeautoriseerde activiteiten worden uitgevoerd. De wereld is echter erg veranderlijk en vergt een hoge mate van flexibiliteit. Dit betekent dat ongeacht hoe goed een proces is bedacht er altijd situaties zijn waarbij je zou willen afwijken omdat de situatie dit noodzaakt. Technologie vindt men sterk, omdat het geen 'menselijke fouten' kan maken. Het is echter door mensen gemaakt en bevat vaak kwetsbaarheden. We zijn bezig met zelfhelende systemen, maar op dit moment zijn we nog

Fouten maken is zo menselijk. Er is geen training opgewassen tegen per ongeluk het verkeerde doen.

niet zover en kunnen we niet alleen op systemen vertrouwen. Dan krijg je nog de menselijke barrière die je kunt opwerpen. Dit doen we door training en bewustwording om te zorgen, dat personen binnen en buiten de organisatie geen rare dingen doen om de organisatie open te stellen voor onnodige inbreuken. Het is natuurlijk wel zo dat een fout heel menselijk is.
Organisaties werken hard om mensen niet op linkjes te laten klikken, bijlagen te openen en geen inloggegevens achter te laten. Dit doen we door e-learning, trainingen en andere gedrag beïnvloedende maatregelen. We komen er echter achter, dat we het vaak niet tot nul kunnen brengen. Fouten maken is zo menselijk. Wanneer iemand emotioneel is, haast heeft of anderszins is afgeleid dan is er geen training opgewassen tegen per ongeluk het verkeerde doen. Maar ik geloof dat wanneer we alle drie lagen van proces, technologie en mens op een hoger niveau krijgen, het mogelijk is een mix te creëren waarbij de verdediging van de organisatie optimaal is, oftewel: Intelligent Security Operation.

Tom Bakker - De mens als de sterkere schakel

De mens zou de sterkste schakel moeten zijn maar helaas in de praktijk blijkt het tegendeel. Er zijn allerlei redenen waarom de mens de zwakste blijkt. Naast de 'domme' fouten (vergissingen) die men soms maakt, is het zo dat criminelen steeds doortastender worden om mensen te verleiden ongewenste en verkeerde dingen te laten doen. Blijkbaar vinden zij ook dat de mens de zwakste schakel is. Daartoe gebruiken ze allerlei middelen om hun doel te bereiken.
Hoogleraar psychologie en marketing Robert Cialdini ontwikkelde zes principes om mensen te beïnvloeden en te manipuleren (Schaarste, Social Proof, Autoriteit, Sympathie, Wederkerigheid, Consistentie) (1). Later is daar Eenheid (groepsgedrag/-gevoel) als zevende aan toegevoegd. Het zijn eigenlijk marketingprincipes maar ook prima te gebruiken voor social engineering. De CEO-fraude is een voorbeeld van het autoriteit-principe. Wederkerigheid: ik heb iets voor jou gedaan en nu moet je iets voor mij doen. Relatiegeschenken zouden hier ook onder kunnen vallen. Zo zie je die principes terugkomen in allerlei ellende.

In 2010 verscheen in iB-Magazine (voorheen InformatieBeveiliging) acht artikelen van auteur Jan de Boer over deze principes toegepast op Social Engineering testen (o.a. Mystery Guest) (ze staan nog in het archief op de PvIB-website (2)). Wellicht een idee om deze principes in awarenessprogramma's op te nemen zodat men 'bewust bekwaam' wordt en verandert van de zwakste in een sterkere schakel. Iedereen kan het overkomen in die principes te trappen. Los van hacking en hackers. Alleen al in de supermarkt trap je er telkens weer in met die 'speciale aanbiedingen die je snel vandaag moet kopen'. Want op=op (schaarste).

(1) https://en.wikipedia.org/wiki/Robert_Cialdini
(2) https://www.pvib.nl/actueel/ib-magazines/archief?pagina=11

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

COLUMN DIMITRI

Metaverse en het volgende virtuele hoofdpijndossier

Men neme een internet, een vleugje augmented/virtual/extended reality, een snufje blockchain, een eetlepel artificial intelligence/deep fakes, wat cloud computing en 100 gram IoT wearables. Men voegt daar twee NFTapen, een duizendtal API's, wat cryptocurrencies in mobiele wallets plus een paar digitale identiteiten aan toe en je hebt de perfecte metaverse cocktail te pakken. Shaken, not stirred welteverstaan. De hamvraag is hoe we dat nieuwe Web3.0 een beetje veilig gaan houden.

Ik schreef hier al eerder over de basissecuritymaatregelen en dat de maatschappij nogal moeite heeft om de kinderlijk lage cybersecurity-lat een niveautje hoger te tillen. Het valt ons allemaal erg zwaar om digitaal, by design en default, veilig te werken want het moet snel en het moet renderen dus mag het niet te veel kosten. Bij gratis diensten is de gebruiker zelf het verdienmodel en privacyrechten zijn hier dan regelmatig aan ondergeschikt. Wetgeving hobbelt hier dan weer decennialang achteraan. Het zal met de metaverse niet veel anders gaan, schat ik in. Overigens ben ik echt wel een geek en al lang met crypto bezig, dus ik ben er in principe allemaal niet op tegen en vind het superinteressant. Mijn voordeel is echter dat ik behoorlijk beroep gedeformeerd ben en enigszins paranoïde op cybergebied. Het gros van de gebruikers is dat natuurlijk niet en daarmee uitermate kwetsbaar voor allerlei nieuwe risico's.

Want fraude met NFT's en valse identiteiten zal flink toenemen. Er zullen meer en meer nep-tokens en avatarattributen in omloop komen met piramidespelachtige constructies waar mensen met een beetje FOMO toch weer blind zullen instappen. Wallets zullen gehackt worden en financiële transacties zullen in een sinkhole uitkomen. Mensen zullen rare (seks?)dingen gaan doen met zo'n hololens op en een haptisch pak aan waar je ze vast wel weer mee kunt bedreigen. Gelukkig is digitaal gokken wel helemaal anoniem, toch? Allerlei metaserviceproviders zullen data heen en weer sturen tussen mobiele apps, clouds en edges. Metadata zal in megabuckets opgeslagen worden die vervolgens weer gehackt, gelekt en verhandeld gaan worden. Door al die zaken aan elkaar te koppelen zal ons persoonlijk aanvalsoppervlak exponentieel groter worden. Maar dan echt!

En over wetgeving gesproken, in 2021 reeds kocht een investeerder via 792 NFT's 2000 hectare grond in een metaverse die The Sandbox heet. Als het op de immutable blockchain staat dan zal het eigenaarschap wel geborgd zijn en te gebruiken in verschillende werelden dacht men. Nou mooi niet want als men zich aanmeldt op een virtuele wereld kunnen de kleine lettertjes (die nooit gelezen worden) het eigendom claimen en is er van portabiliteit geen sprake meer. Je avatar, je tokens, je property, ja zelfs je identiteit; alles is op een of andere manier toch gebonden aan de technology stack die het allemaal mogelijk maakt en daarmee is er van de bejubelde decentralisatie van macht via de blockchain helemaal geen sprake meer. Sterker nog, ik vrees dat een beperkt aantal metaverse unicorns zoals Twitter en Facebook nu, ook hier de macht in handen gaat krijgen en een verder loopje gaat nemen met onze fundamentele mensenrechten.

Enfin, ik had willen afsluiten met een mooie, hoopvolle en positieve paragraaf maar het wordt een lelijke. Kijkend naar ons huidige gedrag dan vrees ik dat slechts een enkeling nadenkt over Morpheus' rode of blauwe pil. Het gros zal weer als lemmingen het metaverse inspringen en zichzelf laten compromitteren en de monopolisten komen er via machtige lobby's weer mee weg. En de schaarste op de cyber- en privacymarkt zal nog verder toenemen.

15 PvIB reconnect in cyber security

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
Nicole van Deursen

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

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

ABONNEMENTEN
De abonnementsprijs in 2022 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

TSTC

ICT en Security Trainingen

ADVANCE YOUR CAREER WITH SECURITY IN 2022

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

Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

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

SECURITY MANAGEMENT TRAININGEN

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

PRIVACY TRAININGEN

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

CLOUD SECURITY TRAININGEN

CCSP - Certified Cloud Security Professional

ISO TRAININGEN

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

www.tstc.nl

Onze trainingen zijn weer klassikaal of Live Online te volgen