

- ◆ **CTI en dreigingsanalyse binnen het NCSC**
- ◆ **De falende CISO: 'Hoe we voortmodderen'**
- ◆ **Column: Chatten met OpenAI**

**ORDINA**  
Ahead of change

**15** PvIB  
reconnect  
in cyber security

# ORDINA FELICITEERT PvIB MET HET 15-JARIG JUBILEUM!

Looking for change?  
Join our team! >



# TRAXION

PART OF SWISS IT SECURITY GROUP

## Independent. Dynamic. Involved.

Traxion is onafhankelijk specialist op het gebied van Identity & Access management als onderdeel van een breed Information Security portfolio binnen de Benelux en DACH-regio.

Met strategische, tactische en operationele adviezen en diensten begeleiden we onze klanten al meer dan 20 jaar naar robuuste, flexibele oplossingen.

[www.traxion.com](http://www.traxion.com)

[www.workattraxion.com](http://www.workattraxion.com)





# Nieuwjaar



Chris de Vries

**E**en tijd van bezinning en goede voornemens. Het oude jaar (2022) is een memorabel jaar gebleken en dat niet alleen in positieve zin. Kijk naar de agressie-oorlog van het Russisch imperium dat blijkbaar meer 'Lebensraum' zoekt, maar ook naar de consequenties daarvan: de energieprijzen, dreigende hongersnoden, sabotage-acties op West- & Oost-Europese infrastructuur, inflatie en een verdiepende samenwerking tussen de dictatoriaal geregeerde landen. Beter geschreven: het gaat om de samenwerking tussen de machthebbers in die landen, want de overheerste volkeren kunnen er weinig aan doen.

Dichter bij huis hebben wij (IB Magazine) afscheid genomen van onze onvolprezen (hoofd)redacteur Tom Bakker. Hij blijft gelukkig lid van het PvB en wij rekenen er dan ook op artikelen van (of via) hem in de toekomst te blijven ontvangen. Wij, als redactie, wensen dat het jaar 2023 een memorabel jaar voor jullie wordt in positieve zin. Het redactieteam streeft ernaar de kwaliteit van ons vakblad hoog te houden en zo mogelijk verder uit te bouwen. Wij streven ernaar het contact met jullie interactiever te maken. Ook aan de vormgeving schenken wij aandacht.

Natuurlijk houden wij de actualiteit in de gaten, zoals de toenemende cyberdreiging op Nederland gericht, zie de rapportages van de AIVD (1), (2). Zo weten wij dat statelijke actoren (Rusland) bezig zijn (is) onder meer de Nederlandse LNG-terminals te scannen, proberen in te loggen en te achterhalen wie daar werkzaam zijn (3). Dat belooft voor ons vak dat 2023 een interessante tijd zal worden, zoals een Chinese vervloeking luidt. Wij Nederlanders zijn echter positief ingesteld. Een mooi voorbeeld hiervan is het artikel van Robert Metsemakers in deze uitgave. Met 'Cappuccino-smaak' en Italiaanse levensstijl legt hij een verband naar de 'Advanced Persistent Threat (APT)'. Daaruit komt voort zijn 'security-inspiratie'. Het mooiste vind ik zijn gedachte van een 'caffè sospeso', dat mij doet denken aan de kans dat organisaties die hun veiligheid redelijk tot goed op orde hebben, kleinere organisaties om niet terzijde staan. Dát uit welbegrepen eigenbelang. Om te voorkomen dat statelijke actoren via deze 'kleintjes' toegang krijgen tot de groten of de overheid. Geniet van het IB Magazine in 2023 en laat van jullie horen: door artikelen, door vragen of door participatie in de interactie die wij nastreven. Een gezond, succesvol en leerzaam 2023 toegewenst.

*Chris*

## Referenties

- (1) <https://www.aivd.nl/onderwerpen/cyberdreiging/>
- (2) <https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2021/internationale-dreigingen-en-politieke-veiligheidsbelangen>
- (3) <https://tweakers.net/nieuws/203862/russische-hackers-onderzoeken-digitale-systemen-van-ing-terminals-in-nederland.html>

## IN DIT NUMMER

- 03** Voorwoord – Nieuwjaar
- 04** CTI en dreigingsanalyse binnen het NCSC. Omgaan met een groeiende informatiebehoefte in een divers organisatielandschap
- 09** Column Privacy – De vinkentering
- 10** The GREAT 'Risk' Reset
- 12** De falende CISO: 'Hoe we voortmodderen'
- 16** Column Lex Borger – Chatten met OpenAI
- 18** AI of nie?
- 21** Bestuurscolumn – Even voorstellen: Valentijn Ishaqsada
- 22** Blog Robert Metsemakers – Security inspiratie uit Italiaanse koffies
- 25** Column Martijn Hoogesteger – Vlaggetjes scoren om scherp te blijven
- 26** SOCCRATES - Automation and Orchestration of Security Operations
- 30** Risicoklassenindeling digitale veiligheid gelanceerd
- 33** Column Dimitri van Zantvliet – Fourth Party Risk Management, SBOM, CSAF en VEX
- 34** Achter Het Nieuws – De wereld gaat aan... ten onder!



**Auteur:** Noortje Henrichs is teamleider van het team Cyber Threat Intelligence en Dreigingsanalyse (CTI/DA) bij het NCSC. Samen met haar team is zij verantwoordelijk voor het leveren van tijdige en relevante informatie over digitale dreigingen aan de doelgroepen van het NCSC. Het is haar missie om organisaties en bedrijven een goed inzicht te bieden in het huidige dreigingslandschap en informatie te leveren over de digitale aanvallen die er op Nederland afkomen. Noortje is bereikbaar via [noortje.henrichs@ncsc.nl](mailto:noortje.henrichs@ncsc.nl).



# CTI en dreigingsanalyse binnen het NCSC

Omgaan met een groeiende informatiebehoefte in een divers organisatielandschap

Binnen het Nationaal Cyber Security Centrum (NCSC) is het team Cyber Threat Intelligence & Dreigingsanalyse (CTI/DA) verantwoordelijk voor het onderzoeken, duiden en inschatten van digitale dreigingen uit binnen- en buitenland.

Dreigingsanalisten en specialisten van het NCSC helpen zo organisaties aan relevante informatie om zich te beschermen tegen cyberaanvallen. De vraag naar dreigingsinformatie neemt toe.

**T**oen in januari dit jaar de spanningen tussen Rusland en Oekraïne verder opliepen en Russische troepen zich verzamelden voor de Oekraïense grenzen, heerste er bij Nederlandse bedrijven en organisaties grote onzekerheid over wat er ging gebeuren.

Naast zorgen over een fysieke invasie, leefde er ook onrust over mogelijke cyberaanvallen die in het kader van dit conflict uitgevoerd konden worden. Al in 2017 hadden we in Nederland immers een voorproefje gezien van een digitale aanval op Oekraïense doelwitten, waarvan ook bedrijven in andere landen slachtoffer werden. De NotPetya-aanval richtte wereldwijd grote schade aan door computers te vergrendelen zonder dat dit teruggedraaid kon worden.

Deze zogenoemde wiper-aanval is een voorbeeld van een ongecontroleerd cyberwapen dat in het verleden al vaker in een conflict is ingezet. In het kader van deze bezorgdheid werd het NCSC geregeld benaderd door organisaties en bedrijven met vragen over digitale dreiging. Wat was er tot nu toe waargenomen en welk soort cyberaanvallen konden organisaties in Nederland in de toekomst verwachten?

### Taak van het NCSC bij dreigingen

Het NCSC ontvangt geregeld vragen van organisaties die zich zorgen maken over hun digitale veiligheid en over de dreigingen die ze op zich af zien komen. Om hier goed antwoord op te kunnen geven, zet het NCSC de expertise in van het team Cyber Threat Intelligence & Dreigingsanalyse (CTI/DA). Dit team, met medewerkers met verschillende achtergronden, onderzoekt en duidt digitale aanvallen en schat de waarschijnlijkheid en impact van deze aanvallen in voor doelgroeporganisaties. Hiernaast maakt het team gebruik van het Nationaal Detectie

Netwerk (NDN). Het team deelt eigenschappen van malafide verkeer voor detectie met doelgroeporganisaties en monitort zelf ook op deze eigenschappen binnen de rijksoverheid.

De veelzijdigheid van kennis en mensen in dit team zorgt voor een interessante en afwisselende werkomgeving waar ik met plezier deel van uitmaak. Ik vertel dan ook graag iets meer over het onderwerp dreigingsinformatie en hoe het NCSC daarmee omgaat.

### Dreigingsinformatie delen

In het Cybersecuritybeeld Nederland wordt 'dreiging' gedefinieerd als een cyberincident dat zich in de toekomst kan voordoen of een combinatie van gelijktijdige of opeenvolgende cyberincidenten die kunnen plaatsvinden. Binnen het NCSC neemt team CTI/DA daarom een andere plaats in dan bijvoorbeeld het team Incident Response dat uitrukt bij incidenten die zich ook daadwerkelijk manifesteren.

De medewerkers van ons team zijn gespecialiseerd in digitale aanvallen en campagnes die zich misschien in Nederland nog niet hebben voorgedaan, maar die wel op ons afkomen. Ook houdt het team de digitale aanvallen bij, die we nu al veel zien in combinatie met de trends en ontwikkelingen die zich daarbij voordoen. Door de informatie over deze toekomstige dreigingen te delen, draagt het team bij aan het versterken van de weerbaarheid van organisaties. Wie weet wat er op hem/haar afkomt, ligt op veiligheidsgebied altijd een stap voor.

In de periode vóór de Russische invasie in Oekraïne heeft het NCSC bijvoorbeeld op de NCSC-website beschreven welk soort aanvallen in Nederland volgens het NCSC te verwachten waren en welke maatregelen organisaties kunnen treffen om zich

tegen dit soort aanvallen te beschermen (1). Tot nu toe heeft het NCSC geen aan de oorlog gerelateerde, digitale aanvallen gericht op Nederlandse belangen waargenomen.

Hoewel we altijd zoveel mogelijk informatie via onze website delen, is uiteraard niet al onze dreigingsinformatie geschikt voor openbare publicatie. Bepaalde informatie is gevoelig en wordt door het NCSC alleen gedeeld met doelgroeporganisaties voor wie dit relevant is. We hebben hier een goede reden voor: we willen digitale aanvallers niet wijzer maken dan ze al zijn.

### Combineren van dreigingsinformatie op verschillende niveaus

Dreigingsinformatie over digitale aanvallen is niet eenduidig, er bestaan verschillende typen. Britse voorlopers van het huidige NCSC-UK hebben dreigingsinformatie onderverdeeld in vier niveaus: het technische, operationele, tactische en strategische niveau.



Figuur 1: Niveaus van dreigingsinformatie, bron: CPNI.gov.uk.

In 2018 werkten de dreigingsanalisten binnen het NCSC nog gescheiden van de meer technische CTI-specialisten. Zij concentreerden zich op dreigingsinformatie op tactisch niveau, bijvoorbeeld de werkwijze van digitale aanvallers en hoe zij hun digitale hulpmiddelen ontwikkelen. Deze analisten hebben meestal geen technische opleiding gehad, maar hebben een achtergrond in bijvoorbeeld integrale veiligheidskunde, inlichtingen of criminologie. Dit stelt ze in staat om digitale dreigingen ook in een breder verband, bijvoorbeeld op geopolitiek vlak, te kunnen duiden.

Toen ik werd aangesteld om het team van dreigingsanalisten te leiden, werd mij duidelijk dat tactische dreigingsinformatie niet erg waardevol is, als je deze niet kunt combineren met de bijbehorende informatie op technisch niveau. Want hoe zouden we

organisaties goed kunnen helpen als we alleen de context en werkwijze van bijvoorbeeld een wiper-malware publiceren, zonder dat we ook de bijbehorende technische details leveren?

Technische dreigingsinformatie bestaat bijvoorbeeld uit herkenbare eigenschappen van malafide verkeer die organisaties vervolgens kunnen gebruiken voor detectie. Onder technische dreigingsinformatie vallen loC's (Indicators of Compromise), zoals URL's, domeinnamen, hashes, YARA-rules en andere malware-eigenschappen. Zonder deze technische informatie kunnen organisaties de eerder genoemde wiper-malware niet binnen hun eigen netwerk detecteren of op deze malware monitoren.

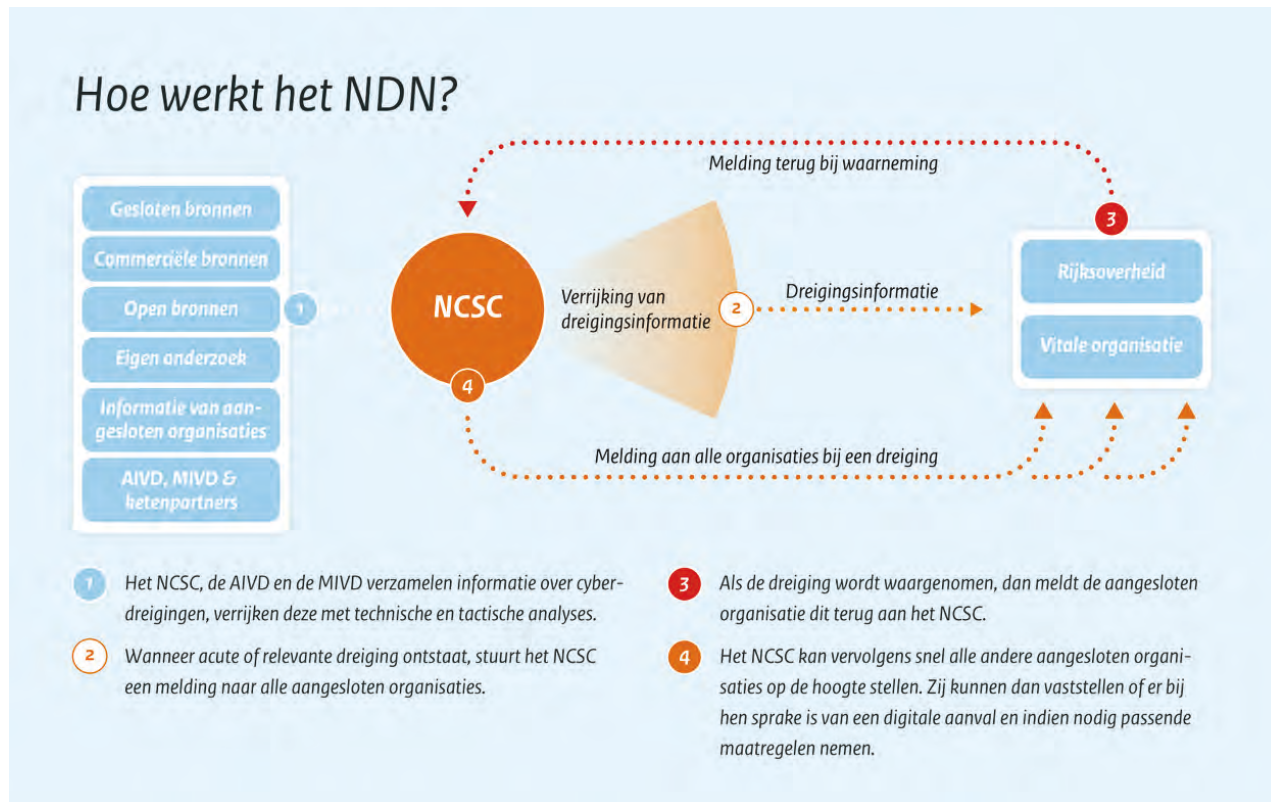
Andersom geldt hetzelfde: je kunt wel technische informatie zoals loC's hebben, maar zonder context weet je niet hoe relevant deze indicatoren zijn voor jouw organisatie. Je weet niet wat de malware precies als oogmerk heeft en wat de waarschijnlijkheid en mogelijke impact van een besmetting zal zijn.

De verschillende niveaus van dreigingsinformatie moeten samenwerken om een compleet beeld te krijgen van digitale dreigingen waar Nederland mee te maken krijgt. Dit volledige beeld wordt in jargon ook wel het 'dreigingslandschap' genoemd. Alleen met kennis van dit dreigingslandschap kan het NCSC de vraag beantwoorden welke digitale aanvallen we in Nederland kunnen verwachten. Dit is de reden waarom ik pleit voor het samenvoegen van tactische analisten en technische specialisten in hetzelfde team als het gaat om digitale dreigingsinformatie, zoals bij het NCSC nu het geval is (2). Daarnaast is dit



Figuur 2: De combinatie van technische en tactische dreigingsinformatie binnen het NCSC.





Figuur 3: De IoC-feed van het Nationaal Detectie Netwerk.

ook de reden waarom het NCSC graag informatie over digitale incidenten van organisaties en bedrijven teruggedeed krijgt. Een incident bij de één is immers een waarschuwing voor de ander.

### Diversiteit aan producten

De analisten en specialisten van ons team werken iedere dag aan informatieproducten die een beeld geven van het huidige dreigingslandschap. Maar digitale dreiging is niet voor alle organisaties hetzelfde. Het mag duidelijk zijn dat banken zich over andere cyberaanvallen zorgen maken dan bijvoorbeeld universiteiten. Het ministerie van Defensie zal doorgaans ook een ander soort aanvallers aantrekken dan een gemeente. Geen organisatie of sector is hetzelfde en 'one-size-fits-all' levert daarom zelden een goede bijdrage aan de digitale veiligheid.

Hiermee hebben we meteen de moeilijkheid te pakken. Hoewel de meeste organisaties en bedrijven goed kunnen uitleggen welk soort dreigingsinformatie voor hun netwerken en systemen

relevant is, moeten CERT's (Computer Emergency Response Teams) zoals het NCSC meer dan driehonderd (!) doelgroepen kunnen bedienen met specifieke dreigingsinformatie. En als je dan bedenkt dat iedere organisatie weer een andere informatiebehoefte heeft, is dat nogal een uitdaging. Precies de reden voor ons team om verschillende informatieproducten te publiceren die de diverse dreigingsniveaus raken.

Een van de vele producten die we onze doelgroepen aanbieden, is onze IoC-feed. Deze bestaat uit indicatoren voor malafide verkeer (IoC's) die CTI-specialisten elke dag uit een hoeveelheid van bronnen verzamelen, analyseren en van labels voorzien. Deze feed wordt door middel van een platform verspreid naar organisaties die deelnemen aan het Nationaal Detectie Netwerk. Een van onze andere publicaties is de NCSC-dreigingsanalyse voor partijen in de vitale sector en de rijksverheid. In de dreigingsanalyse kijken we elke drie maanden terug op de voor Nederland relevante dreigingen die ons team heeft waargenomen.

Daarnaast faciliteert ons team zogenoemde scenariosessies voor organisaties. Hierbij identificeren we gezamenlijk toekomst-scenario's die zich richten op dreigingskans en -context. Het doel van deze sessies is om verschillende toekomstige digitale aanvallen te inventariseren, hierop te anticiperen en risico's te beoordelen (fysieke, politieke, financiële et cetera)

Ook in de aanloop naar de oorlog in Oekraïne heeft ons team, begin vorig jaar, dreigingsscenario's ontwikkeld. In deze scenario's hebben we op basis van precedentenonderzoek verschillende aanvallen geïdentificeerd die Nederland kunnen treffen in relatie tot de gespannen geopolitieke situatie. We hebben deze scenario's zo breed mogelijk binnen onze doelgroepen verspreid. En toen de oorlog uitbrak, heeft ons team de scenario's gepresenteerd aan onze doelgroepen en aan leden van het CIO Platform Nederland. In een informatiesessie mede georganiseerd door het Digital Trust Centre (DTC), zijn we vervolgens dieper ingegaan op de specifieke digitale dreigingen die een gevolg van deze oorlog kunnen zijn (een sessie die terug te kijken is op You Tube (3)). Nu de oorlog al een tijd voortduurt, houdt het team de ontwikkelingen doorlopend in de gaten en worden dreigingsscenario's en handelingsperspectief voortdurend door onze analisten geactualiseerd.

Over handelingsperspectief gesproken: naast dreigingsinformatie is het zeer belangrijk dat in berichtgeving wordt benoemd wat organisaties kunnen doen om een bepaalde dreiging tegen te gaan. Binnen het NCSC werken de dreigingsanalisten daarom nauw samen met adviseurs die zijn gespecialiseerd in beveiligingsmaatregelen. Buiten het NCSC vindt op dit vlak bovendien nauwe afstemming plaats met partners binnen de overheid, zoals inlichtingendiensten en politie.

### Toenemende vraag

Binnen het team merken we dat de vraag naar dreigingsinformatie toeneemt. Geopolitieke spanningen en gebeurtenissen met maatschappelijke impact zijn vaak aanleidingen voor aanvallen in het digitale domein. Daarnaast zal de nieuwe Europese richtlijn voor netwerk- en informatiebeveiliging (NIB2) tot gevolg hebben dat het aantal doelgroepen van het NCSC zal toenemen. Dat heeft voor het NCSC als gevolg dat er veel meer nieuwe doelgroepen met dreigingsinformatie bediend moeten worden dan tot nu toe het geval was.

Om aan deze vraag te kunnen voldoen, zal ons team meer gaan samenwerken met internationale en commerciële organisaties. Er zal een sterker beroep op ons worden gedaan om onze informatie met meerdere partijen te delen. Daarvoor zullen we manieren moeten vinden om op grotere schaal vertrouwelijke informatie te kunnen delen met partijen voor wie dit relevant is. En natuurlijk zullen we zo goed mogelijk inzicht moeten geven in het huidige dreigingslandschap, zonder daarbij uit het oog te verliezen welke veiligheidsmaatregelen organisaties kunnen treffen om een specifieke dreiging het hoofd te kunnen bieden. De oorlog in Oekraïne is een goed voorbeeld van een situatie waar de vraag naar actuele dreigingsinformatie zeer groot was. Een vraag die maatschappelijk veel breder leefde dan alleen binnen de rijksoverheid en vitale sectoren.

'Heeft de oorlog in Oekraïne gevolgen voor mijn digitale veiligheid?' 'Welk soort digitale aanvallen zijn actief in mijn sector en wat zijn hun werkwijzen?' 'Mijn detectiesensor neemt een indicator waar op mijn netwerk. Word ik aangevallen?' Het NCSC bereidt zich voor op een toename van dit soort vragen en bouwt aan een effectievere en efficiëntere manier om te zorgen dat dreigingsinformatie op de juiste plekken terechtkomt.

Tegelijkertijd blijven de dreigingsanalisten, CTI-specialisten en de teamleiders van mijn team zich iedere dag enthousiast inzetten om de meest actuele dreigingsinformatie te publiceren en blijven wij graag met u samenwerken aan de digitale veiligheid van Nederland.

### Referenties

(1) <https://www.ncsc.nl/onderwerpen/oekraïne-met-welke-digitale-aanvallen-moet-u-rekening-houden>

(2) Ter aanvulling m.b.t. de andere twee soorten informatie in de kwadranten.

Dreigingsinformatie op operationeel niveau biedt doorgaans specifieke en gedetailleerde inlichtingen op zeer korte termijn, expliciet gericht op organisaties en dreigingen. Als een dreiging acuut en concreet wordt, wordt de zaak binnen het NCSC vaak overgedragen naar het incident response team en nemen we zo snel mogelijk contact op met de (mogelijk) getroffen partijen. Dreigingsinformatie op strategisch niveau omvat met name inlichtingen over ontwikkelingen in digitale veiligheid die voor een langere termijn gelden en bruikbaar zijn voor een beleids- of bestuurslaag in een organisatie. Binnen het NCSC draagt het team CTI/DA jaarlijks bij aan het Cybersecuritybeeld Nederland, een voorbeeld van een strategisch informatieproduct.

(3) <https://www.youtube.com/watch?v=bZocelpruDQ>





# COLUMN PRIVACY

Mr. Rachel Marbus  
@RACHELMARBUS OP TWITTER

## De vinkentering

Het is nou niet bepaald een sexy onderwerp, maar het heeft de gemoederen eind vorig jaar flink beziggehouden en het zal ook dit jaar nog zeker op menig privacy-agenda staan. Het uitwisselen van persoonsgegevens over de landsgrenzen heen en dan met name naar landen waar geen adequate bescherming bestaat. Een onderwerp dat organisaties flinke hoofdpijn kan bezorgen. Daarbij wordt inmiddels gewerkt met Transfer Impact Assessments (TIA) om het risico van het uitwisselen naar een bepaald land te bepalen. En hoewel zo'n TIA heel waardevol is, is het ook beperkt. Want dat het uitwisselen van gegevens met een bepaald land misschien minder risicovol is, betekent niet dat het uitwisselen met een bepaalde organisatie in dat land dan ook ineens minder risicovol zou zijn.

Even kort ter herinnering. In 2020 deed het Europese Hof van Justitie uitspraak in de tweede Schrems zaak, in die uitspraak vernietigde zij de toen bestaande afspraken voor het uitwisselen van persoonsgegevens met de USA. De vervanging: iedereen moest Standard Contractual Clauses (SCC) gaan afsluiten. In die contracten staan door de Europese Commissie vastgestelde regels op basis waarvan persoonsgegevens uitgewisseld mogen worden.

Maar stel nu dat je zaken wilt doen met een organisatie in de Verenigde Staten en je hebt die SCC's afgesloten, zou je dat dan ook altijd moeten doen? Juridisch gezien kan jou niet veel gemaakt worden als je dat mooie contract getekend en gedateerd hebt liggen. Maar stel nu dat dit bedrijf onderdeel uitmaakt van de Meta organisatie die in januari een boete heeft gekregen van 390 miljoen euro voor het tegen de regels in verwerken van gegevens voor gericht persoonlijk adverteren. Of je wilt zakendoen met Apple dat in dezelfde maand 8 miljoen euro boete kreeg opgelegd vanwege eenzelfde privacyvergrijp. Of met Epic Games, die nog net in december, schikte met de FTC voor 520 miljoen dollar, omdat ze zonder toestemming gegevens van kinderen verwerkt en daarbovenop ook nog eens spelers misleidt tot het doen van onbedoelde aankopen. De voorbeelden zijn legio – alleen al de afgelopen maanden.

Al is je TIA dus nog zo strak en komt eruit dat je weinig risico loopt, het schetst mogelijk een vertekend beeld bij iedereen in jouw organisatie die geen privacy-specialist is. Het zegt – op dit moment – echt alleen maar iets in zijn algemeenheid over het land waarmee de gegevens uitgewisseld worden. Het zegt helemaal niets over de partij waarmee je dat beoogt te doen. En hoewel iedereen weet dat je bij een aanstaande zakenpartner naar het geheel hoort te kijken, zou het bestaan van de TIA het in dit opzicht nog wel eens negatief kunnen beïnvloeden. En hoewel ik merk dat er in de praktijk ook steeds meer ruimte is voor ethische overwegingen bij de due diligence voor het zakendoen met derden, zie ik ook dat als het vinkje maar groen kleurt (we hebben SCC's, we hebben een TIA met lage score op risico) het contract snel getekend is. En dan heb je met een beetje pech een geval van de 'vinkentering' te pakken: alles staat op groen, maar de patiënt is overleden.

*Rachel*



*The GREAT 'Risk Reset' werd gehouden in Congrescentrum Spant! In Bussum.*

# The GREAT 'Risk' Reset

Op 16 november 2022 was er een grote bijeenkomst van audit-, compliance-, risk- en security professionals: The GREAT 'Risk' Reset. Het evenement was georganiseerd door ISACA in samenwerking met NOREA, IIA en PvlB. Het was alweer de derde keer dat de conferentie gehouden werd. Door COVID-19 was het lange tijd niet mogelijk zoveel mensen bijeen te brengen om met elkaar te netwerken en kennis te delen. Ondanks vele webinars de laatste jaren was het nu weer prettig om fysiek bijeen te komen.

**H**et Risk Event, zoals de bijeenkomst in de volksmond wordt genoemd, wordt georganiseerd om professionals bij elkaar te brengen rond het onderwerp risk. Na meer dan twee jaar COVID-19 kon eindelijk weer een groots evenement georganiseerd worden voor meer dan 450 deelnemers. Dat is ook de reden voor de keuze van het thema: The Great 'Risk' Reset. Heeft deze periode van lockdowns, testen en thuiswerken ook in het risicolandschap veel veranderd? Het was de vraag die de sprekers probeerden te beantwoorden en de vraag waarop deelnemers graag een antwoord wilden.

## Keynotes en tracks

Het event werd gehouden in Congrescentrum Spant! in Bussum. De conferentie had naast de keynotes, waar iedereen bij elkaar was, ook vier tracks waaruit deelnemers konden kiezen. De onderwerpen van de tracks waren: IT Risk, Emerging Risk, Corporate Risk en Supplier Risk. Hieronder volgt een korte terugblik op de behandelde onderwerpen.

De keynotes gingen over circles of trust, cyber mythe en privacy in de praktijk. Vanuit de circles of trust werd aangegeven uit te zoeken welke stakeholders je hebt en hoe je deze moet beheer-

sen. In de cyber mythe presentatie werd getracht de FUD (Fear, Uncertainty and Doubt) te halen en cybersecurity weer in een positief licht te brengen. Met privacy in de praktijk probeerde de spreker aan te geven dat ondanks de vage wetsteksten organisaties best heel praktisch met privacy om kunnen gaan.

### IT Risk track

In de IT Risk track werd gesproken over risico's met betrekking tot cybersecurity, DevOps, Cloud, softwareontwikkeling, purple teaming en human risk. De verschillende sprekers gaven een verscheidenheid aan risico's weer die een connectie hebben met IT. In de afgelopen jaren zijn organisaties door Citrix, aan het begin van 2020, en vervolgens door het thuiswerken als gevolg van COVID-19 versneld verder gaan digitaliseren. Met deze digitale transformatie zijn ook nieuwe risico's geïdentificeerd. De discussie was ook in hoeverre deze risico's nieuw zijn of bekende fenomenen met een iets andere prioriteit. We zien dat IT en digitalisering nog meer boardlevel agendapunten zijn geworden. Dit ofwel door het verder automatiseren van processen ofwel door de toename van cyberaanvallen.

### Emerging Risk Track

Bij de Emerging Risk track kwamen nieuwe risico's aan de orde, zoals deepfakes, web 3.0 (DeFi, blockchain, metaverse), ransomware en model risk. Het begon met de beschrijving van risico's met betrekking tot deepfakes. Hoe kunnen we echt van nep onderscheiden? Wat doet het met een medewerker van wie deepfake porno video's of foto's rondgaan op het internet? Wat moet een organisatie hieraan doen, wanneer zij een reputatie wil hooghouden?

Hiernaast werd ook ingegaan op de vele mogelijkheden van de metaverse. Dit zou op afstand werken of ondersteund werken verder kunnen bevorderen. Maar hoe weten we wat echt is en hoe controleren we de berekeningen die zijn gemaakt? Verder werd ook ingegaan op hoe we risico's zouden moeten definiëren in een genetwerkte wereld, waarbij meer naar de impact op bedrijfsfuncties zou moeten worden gekeken in plaats van naar de organisatie als geheel. De context waarin een risico wordt geïdentificeerd zal moeten bepalen hoe het beoordeeld, geëvalueerd en behandeld dient te worden.

Ransomware als opkomend risico werd behandeld op een manier waarbij de deelnemers werden meegenomen in het gehele proces van initiële infectie tot aan de onderhandelingen over het losgeld en het verkrijgen van de decryptor sleutel om alle data weer terug te krijgen. Ook kwam in deze track een interessant verhaal aan bod over de klimaatgevolgen van de beno-

digde capaciteit voor het minen van cryptovaluta. Voorbeelden werden gegeven van hoe door aanpassingen aan algoritmes de benodigde capaciteit aan rekenkracht kan worden gereduceerd. Dit betekent weer een afname in energiebehoefte van de datacenters die deze capaciteit leveren. Milieubewust leven door te investeren in groene crypto? Iets om over na te denken.

### Corporate Risk track

Risico's met betrekking tot Avg, algoritmes, ethiek, interne audit, gedrag en EU-wetgeving vormden de basis van de sessies binnen de Corporate Risk track. Vanuit wet- en regelgeving werd bekeken met welke nieuwe risico's organisaties rekening moeten houden. Maar er werd ook gekeken naar de kansen die de nieuwe ontwikkelingen met zich meebrengen. Een van de sprekers behandelde hoe haar organisatie omgaat met behavioural risk. Ze ging in op het identificeren van dit soort risico's en het beheersen hiervan door te sturen op de gewenste cultuur. Ook werd ingegaan op de kansen en mogelijkheden door het gebruik van algoritmes. Deze algoritmes zullen een verdere transitie in de samenleving teweegbrengen met betrekking tot slimmer werken, mobiliteit, geneeskunde en onderwijs. Vanuit het perspectief van een interne audit werd gekeken naar een overzicht van risico's voor het nieuwe jaar 2023.

### Supplier Risk track

De vierde track ging over de Supplier Risk, een onderwerp waarover in de markt veel gesproken wordt. Sprekers bespraken risicomangement met betrekking tot derden, gebruik van AI, leveranciersmanagement, statelijke actoren, circles of trust en nationale ketens. Hierbij werd duidelijk weergegeven dat een organisatie niet alléén functioneert en zeker rekening moet houden met stakeholders in de gehele keten. De vraag was hoever gaat de keten en hoe diepgaand moet je daarbij onderzoeken? In hoeverre vertrouwt je op de organisaties waarmee je samenwerkt en hoeveel controle moet je hierbij uitvoeren? Van software tot hardware tot producten en diensten moet je weten wat je verwacht van een leverancier. Dit moet je niet eenmaal toetsen, maar continu.

### Conclusie: prioriteit bepalen

Vele risico's zijn de revue gepasseerd, waarbij veelal nieuwe perspectieven werden gegeven op bestaande en bekende risico's. Ik denk dat uiteindelijk de boodschap was dat de wereld is veranderd en dat daarmee het landschap aan risico's is veranderd. Hierbij wordt eenieder aangemoedigd om voor de eigen organisatie te bepalen welk risico prioriteit heeft en daarbij een keuze te maken welk risico behandeld dient te worden in 2023!



**Auteur:** André Beerten is sinds 2015 zelfstandig adviseur informatiebeveiliging en ook associate bij Verdonck, Klooster en Associates. Hij werkte eerder bij KPN, Getronics en het Groene Hartziekenhuis. Hij is te bereiken onder: [andre@octopus-ib.nl](mailto:andre@octopus-ib.nl) of via LinkedIn (1)



# De falende CISO

'Hoe we voortmodderen'

Een niet aflatende stroom berichten in de media vertelt ons dat de beveiliging van informatie te wensen overlaat en dat we de strijd tegen de digitale onveiligheid dreigen te verliezen. Voorkomende incidenten ondersteunen deze claim met hun oplopende frequentie en de ernst van de gebeurtenissen. Hoe komt dit en wat is de rol van informatiebeveiligers, (C)ISO's, hierin? Wij zijn immers de professionals, de mannen en vrouwen met security kennis en de fraaie certificaten. Toch!?

**W**e kunnen al lang niet meer wijzen naar de techniek, want er zijn al een hele tijd volop deugdelijke middelen beschikbaar. Wel kunnen we wijzen naar directies en managers, maar die hebben óns, de (C)ISO's, nodig om de beveiliging te snappen en de juiste dingen te doen.

Een onderzoek van CIP (2) (zie kader) schetst geen al te vrolijk beeld van onze beroepsgroep. Wat ik zélf waarneem: we zijn vaak oud, wel al lang in het IT-vak werkzaam, maar nog maar kort (C)ISO: zonder middelen, zonder macht, zonder personeel, soms werkend in deeltijd, veelal met te weinig opleiding voor de specifieke rol en we kijken al uit naar ons pensioen.

#### Dit is de gemiddelde CISO

Ondanks het gegeven dat de gemiddelde leeftijd van de CISO 55 jaar bedraagt, is de ervaring in de functie van CISO relatief kort. 40% geeft aan slechts 0 tot 2 jaar werkervaring te hebben en nog eens 40% 3 tot 5 jaar.

De jongeren moeten het beter gaan doen, maar zij krijgen als vorming het trio CISSP-CISM-CISA opgediend, recht uit de Amerikaanse keuken, niet gericht op je dagelijkse praktijk (met BIO en NEN), maar meer gericht op carrièreperspectief en een mooie uitstraling van het Curriculum Vitae.

#### Het probleem

Voor mij (en vele anderen die ik spreek) is het zonneklaar dat we falen. We krijgen niet voor elkaar wat we beogen. We slagen er niet in (met name in de non-profit) om onze broodheren op een aantoonbaar volwassenheidsniveau te krijgen. Ondertussen drijft onze digitale veiligheid vooral op de professionaliteit en inzet van IT-afdelingen en andere betrokken ondersteuners.

Dat leidt niet alleen tot vage en ondermaatse informatiebeveiliging, maar ook tot persoonlijke problemen. Teleurstelling en frustratie liggen voor de (C)ISO op de loer. Soms neemt het zelfs zeer ernstige vormen aan, denk aan burn-outs. Voor veel collega's geldt 'slikken en doorploeteren', want vooral in onzekere tijden (zoals er nu weer dreigen) moet je blij zijn dat je een baan hebt. Allereerst wens ik al deze mensen sterkte toe, maar we moeten vooral ook kritisch naar onszelf kijken:

*waarom krijgen we zo weinig voor elkaar en welke fouten maken we?*

Ons grootste probleem is mijns inziens dat we (de tweede lijn in informatiebeveiliging - zie figuur 1) blijven proberen 'het probleem' op te lossen. We maken informatiebeveiliging tot ónze verantwoordelijkheid of hebben ons die verantwoordelijkheid laten opdringen, gaan daarin mee en we zorgen er daarmee ook nog eens voor dat de hele organisatie dat ook zo ziet. We sluiten onszelf op in de welbekende ivoren toren en verstoppen ons achter giga-spreadsheets, onleesbare beleidsstukken en lange e-mails. En áls we dan eens echte mensen spreken, gaan we uitleggen in plaats van luisteren.



Figuur 1 bron: IIA website (3).

Wij denken voortdurend te moeten vertellen *wat* 'zij' moeten doen. We vergeten of kunnen daarbij niet aangeven welk doel bereikt moet worden en al helemaal niet hóe dat doel bereikt kan worden. En dán vinden we het gek dat we geen duidelijke antwoorden krijgen, dat onze opdrachten niet uitgevoerd of 'vergeten' worden.

Als we een vraag krijgen van de business, een roep om ondersteuning, dan nemen we maar wat graag het probleem over van de probleemeigenaar. Wij weten immers wat er moet gebeuren. We nemen het initiatief en de verantwoordelijkheid weg bij diegene(n) waar dat thuishoort. We trainen zo de organisatie om óns het te laten doen. Wij trainen ze om achterover te leunen. Onze adviezen worden uitgevoerd, wij zetten een vinkje en vervolgens wordt de bal weer teruggelegd bij ons. De eerste lijn wacht weer rustig af.

## De weg naar een succesvolle aanpak

Er is een middel dat de weg wijst naar een succesvolle aanpak, een adequate invulling van governance vanuit de juiste verantwoordelijkheid (de eerste lijn) en dat is het ISMS in de ISO27001/NEN7510, waarmee governance echt vorm kan worden gegeven.

Helaas slaan we 'dat boekje' meestal over. We pakken dat andere 'boekje' waarin alleen voorbeelden en suggesties staan, de ISO27002, want dat is veel handiger, daar staat gewoon in wat je moet doen. Althans dat denken we en als het zo uitkomt dan pakken we het liefst een baseline, nóg simpeler (denken we), want met de BIO ben je sneller klaar.

Er is, door de komst van BIO, flink gewied in baselineland en het moet gezegd: die geeft het ISMS een plek, maar dan wel helemaal op het eind, in de paragraaf 'Naleving' onder 18.2.1.1. Alsof het bijna vergeten was. Dat is geen aanmoediging om die oproep serieus te nemen en er energie in te steken terwijl 'beheersing van risico's', CONTROL dus, het doel moet zijn: het gaat immers om de beheersing van risico's, niet om het verzamelen van vinkjes... *toch?*

## Geld en macht

In de bijna zeldzame situaties dat we een werkend ISMS mogen inrichten en ook moeten onderhouden, dan behoren daar ook middelen bij. Daar heb ik in mijn praktijk nog maar weinig voorbeelden van gezien. In het Angelsaksische model lijkt dat wél normaal, daarvoor mag je dan zelfs (soms) in de 'board' optreden.

Maar bij ons? Ik ken vooral (C)ISO's met informele invloed en net genoeg budget om het NEN7510-boekje te kopen en dat alleen in goede tijden. Macht ligt vaak bij de bestuurder en in de lijn, maar je moet wel volledig vrij kunnen rapporteren over risico's naar de bestuurder. En dat zonder tussenkomst van de 'kleilaag' die dingen liever wat 'politieker' formuleert.

## Communicatie

Verhalen over hakkelende, onzekere presentaties voor het management kennen we allemaal. Ook ik stond er vaak met klotsende oksels. Dat helpt je natuurlijk niet verder, maar is

niet per sé het probleem. Veeleer gaat het over de problematische vorm en inhoud van ons verhaal: veel techniek, te veel details, te veel emotie en te weinig oog voor waar de business echt op aanslaat. We beginnen bovendien vaak met een heel analytisch verhaal en komen pas op het eind toe aan de kernvraag. Dan zijn de meeste toehoorders al afgehaakt.

Communicatie gaat twee kanten op en we vragen ook niet genoeg waar de directie, de business nu echt van wakker ligt. Wij denken immers meestal vanuit de baseline, niet vanuit wat nodig of wenselijk is (vanuit wat de organisatie wil dus).

## Ter verdediging

Wij (C)ISO's zijn meestal de mensen met een reeks van subtitels achter hun naam, de CISSP- en CISM- oorkondes. Biedt ons dat steun, hebben we daar ook echt iets aan? Om voor een baan in de informatiebeveiliging in aanmerking te komen, wordt vanwege onbenul bij bemiddelaars en HR vaak alleen naar deze 'stickertjes' gekeken. Maar kun je er ook echt iets mee in je dagelijkse werk?

De vraag stellen is hem beantwoorden: beide opleidingen grossieren in schema's, tabellen en wijsheden uit allerlei verschillende culturen en organisatietypen. Maar voor jouw werkomgeving wordt er geen passend model geboden, geen diagram, best practice of methode die bruikbaar is in de dagelijkse praktijk.

De ambachtelijke kant van je vak, de confrontatie met jouw organisatie en zijn eigenaardigheden en belemmeringen, die komt niet aan de orde. Deze opleidingen laten je achter met een dik boek en een mooi papiertje (en embleem voor LinkedIn). Dit zonder handvatten voor praktische toepassing van de geboden stof en oplossing voor het probleem. Voor het werk als (C)ISO zijn veel meer competenties nodig dan wat een dergelijke certificering biedt.

Het is niet iedereen gegeven weet te hebben van én techniek én organisatie én cultuur én ook nog van risicobeheersing. Het vergt een schaap met vijf poten om dat allemaal in de juiste samenhang te kunnen aanpakken. Het opbouwen van de juiste allianties in de organisatie en het



## Van de redacteur

Wellicht kun je je niet helemaal vinden in de opvattingen van de auteur en wil je reageren. Dat kan uiteraard direct naar de auteur, maar we denken dat het interessanter kan worden als de discussie wat breder kan worden getrokken. Reageer daarom via de link naar de LinkedIn-pagina van het PViB: <https://www.linkedin.com/company/pvib/> of scan de QR-code.



- *Herken je het ook - of juist niet - dat je de verantwoordelijkheid voor informatieveiligheid krijgt toegeschoven, maar dat je niet gefaciliteerd wordt in zeggenschap (macht) noch in middelen om deze taak te kunnen uitvoeren?*
- *Herken je het ook - of juist niet - dat onze opleidingen te veel gericht zijn op het dikke boek en de mooie titel en te weinig op ter zake dienende competentie-ontwikkeling?*
- *Ervaar je ook dat binnen jouw organisatie geklaagd wordt dat wij te weinig invulling geven aan de werkelijke wensen/behoefte van de organisatie? Of heb jij juist goede oplossingen weten te realiseren, zo ja welke/hoe, zodat je goed afgestemd bent op het management en kader?*

### Laat van je horen!

organiseren van competente ondersteuning is dan heel belangrijk. Dat is niet altijd mogelijk, nooit eenvoudig, maar wel van essentieel belang voor succes.

### Conclusie

Is het dan allemaal ónze schuld? Nou niet helemaal, maar we spelen mijns inziens wel een hoofdrol in het falen van informatiebeveiliging. Als we echt het verschil willen maken dan moeten we heel kritisch in de spiegel kijken. We moeten beter leren omgaan met mens en organisatie, we moeten werken aan governance met een goed ISMS én we moeten bereid zijn de opdracht terug te geven als niet aan de randvoorwaarden wordt voldaan.

We moeten weigeren boven onze macht te functioneren. We moeten weigeren om met onvoldoende middelen het onmogelijke doel te bereiken. We moeten onszelf verder scholen om beter die rol van het schaap met de vijf poten te kunnen invullen. Deze aanpak vergt persoonlijke moed, maar zonder moed blijven we doormodderen. Zonder lef geen leven!

### Referenties

- (1) <https://www.linkedin.com/in/andrebeerten/>
- (2) <https://ib-p.nl/download/cip-enquete-onder-overheids-cisos/>
- (3) <https://www.iaa.org.uk/threelinesofdefence>

Lex Borger is security consultant bij Tesorion en oud-hoofdredacteur van iB-Magazine. Lex is bereikbaar via [lex.borger@tesorion.nl](mailto:lex.borger@tesorion.nl)

## Chatten met OpenAI

Tijdens de voorbereiding op deze column werd er een bètaversie van de nieuwe versie van de chatfunctie op OpenAI.com gelanceerd. Ik heb jaren geleden eens een misser begaan door niet te herkennen welke invloed AI (Artificial Intelligence) zou hebben op ons vakgebied. Het is mij duidelijk dat de toepassing van AI in informatiebeveiliging cruciaal is. De OpenAI chat liet mij twee dingen zien. Ten eerste: AI is heel ver gekomen, maar mist de boot bij het trekken van conclusies. Ik probeerde de zelftest en vroeg de chatbot "Schrijf een column van 500 woorden voor een vakblad over informatiebeveiliging over het gebruik van kunstmatige intelligentie in cybersecurity." Dit was het antwoord, vertaald met behulp van Google Translate:

"Kunstmatige intelligentie (AI) heeft het potentieel om een revolutie teweeg te brengen op het gebied van cyberbeveiliging door computers in staat te stellen menselijke vermogens na te bootsen om gegevens te analyseren en te interpreteren. Met de groeiende afhankelijkheid van technologie en de toenemende complexiteit van cyberdreigingen, is het gebruik van AI in cyberbeveiliging de laatste jaren steeds gangbaarder geworden.

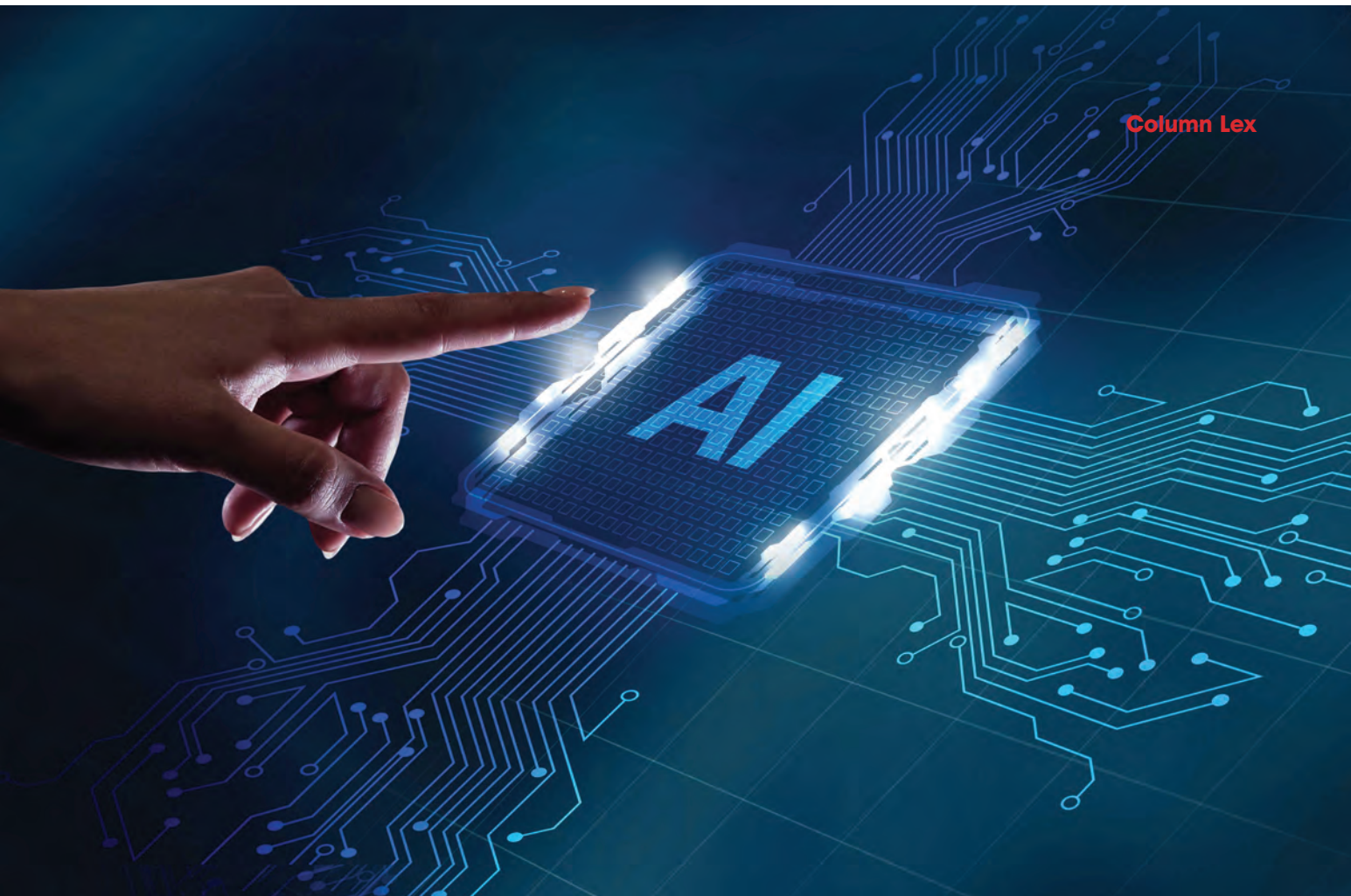
Een groot voordeel van het gebruik van AI in cyberbeveiliging is de mogelijkheid om grote hoeveelheden gegevens snel en nauwkeurig te analyseren. Security professionals raken overweldigd door de enorme hoeveelheid gegevens die ze moeten analyseren om potentiële bedreigingen te identificeren. AI-algoritmen daarentegen kunnen deze gegevens veel sneller doorzoeken en patronen en anomalieën aan het licht brengen die erop kunnen wijzen dat een cyberaanval op handen is.

Een ander voordeel is het vermogen om te leren en zich in de loop van de tijd aan te passen. Naarmate cyberdreigingen evolueren en geavanceerder worden, kan de traditionele aanpak minder effectief worden. AI-algoritmen kunnen echter leren van ervaringen uit het verleden en zich aanpassen aan nieuwe dreigingen, waardoor ze een waardevol hulpmiddel worden in de strijd tegen cybercriminaliteit.

Een voorbeeld van hoe AI wordt gebruikt in cyberbeveiliging is op het gebied van netwerkbeveiliging. AI-algoritmen kunnen netwerkverkeer in realtime analyseren en patronen en afwijkingen identificeren die op een mogelijke cyberaanval kunnen wijzen. Deze algoritmen kunnen worden getraind om de kenmerken van bekende malware te herkennen, waardoor het gemakkelijker wordt om kwaadaardige software te detecteren en de verspreiding ervan te voorkomen.

AI wordt ook gebruikt om de nauwkeurigheid van dreigingsinformatie te verbeteren. Traditionele dreigingsinformatiesystemen vertrouwen op menselijke analisten om gegevens te interpreteren en potentiële bedreigingen te identificeren. Dit kan een tijdrovend en





foutgevoelig proces zijn, omdat analisten mogelijk niet over de nodige deelexpertise beschikken of belangrijke gegevens over het hoofd zien. AI-algoritmen daarentegen kunnen gegevens uit meerdere bronnen analyseren en zorgen voor meer nauwkeurige en meer uitgebreide informatie over bedreigingen.

Ondanks de vele genoemde voordelen zijn er ook enkele zorgen die moeten worden aangepakt. Een punt is het potentieel van AI-algoritmen om vooroordelen te bestendigen die aanwezig zijn in de gegevens die worden gebruikt om ze te trainen. Dit kan leiden tot oneerlijke of discriminerende resultaten, zoals het markeren van bepaalde soorten netwerkverkeer als verdacht op basis van stereotypen of vooroordelen.

Een andere zorg is de mogelijkheid dat AI voor kwaadaardige doeleinden wordt gebruikt. Cybercriminelen kunnen proberen AI te gebruiken om hun aanvallen te automatiseren of traditionele maatregelen te omzeilen. Om deze risico's te beperken, is het belangrijk voor organisaties om de beveiliging van alle AI-systemen die ze gebruiken

zorgvuldig te evalueren en passende waarborgen te implementeren.

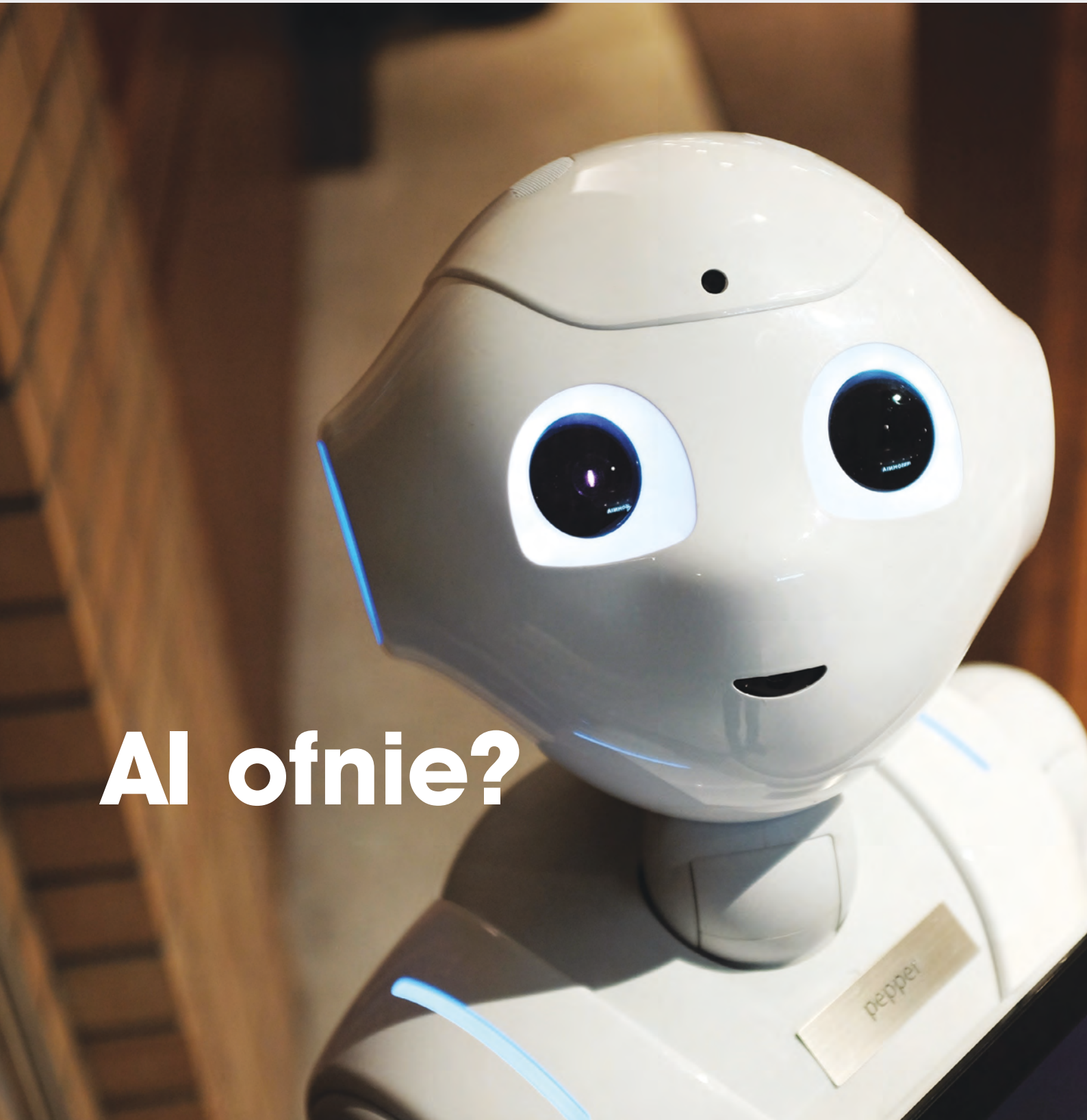
Concluderend biedt het gebruik van AI in cyberbeveiliging veel voordelen, waaronder de mogelijkheid om grote hoeveelheden gegevens snel en nauwkeurig te analyseren, en het vermogen om zich aan te passen en te leren naarmate cyberdreigingen zich ontwikkelen. *Het is echter belangrijk voor organisaties om de potentiële risico's zorgvuldig te overwegen en passende waarborgen te implementeren om ervoor te zorgen dat AI op een verantwoorde en ethische manier wordt gebruikt.*

En juist die conclusie laat nog de achterstand van de intelligentie zien: het is niet aan iedere organisatie om te beslissen AI wel of niet te gebruiken, want je kunt niet de enige zijn die geen AI gebruikt en je bent zeker niet opgewassen tegen een tegenstander die AI gebruikt wanneer jij dat niet doet. Het is aan de samenleving om te beslissen hoe we omgaan met AI. Pandora's doos is geopend, terugstoppen lukt niet meer.





**Auteur:** Dré Lameir is CISO en CTO bij Enovation Group en is bereikbaar via [linkedin.com/in/lameir](https://www.linkedin.com/in/lameir).



# AI ofnie?

Sinds medio 2022 valt iedereen over elkaar om over de impact van Artificial Intelligence (AI) te praten. Artikelen, podcasts, mainstream media en vooral Twitter zijn er vol van. Zelf roep ik al een tijdje dat we over een paar jaar de ene AI tegen de andere AI gaan zien 'battelen' in cybersecurity. Ik stel me zo voor dat een CISO van een groot bedrijf aan het eind van de maand een mooi PowerBI dashboardje heeft waarop staat:

#### Dec 2025

- Cyber attacks:
  - o Lost: 4
  - o Won: 36
  - o Paid: 17 (Total amount BTC 4,5643)
- Executed by:
  - o Human: 13 (22,8%)
  - o AI: 41 (71,9%)
  - o Unknown: 3 (5,3%)

Het gaat nu echt hard vooruit met kunstmatige intelligentie. Ik denk niet dat ik het nog hoeft uit te leggen, maar toch ... we hebben het hier over beelden creëren met DALL-E 2, Midjourney, et cetera Teksten schrijven met Lex en chatten met OpenAI.com waar de engine GTP-3 onder ligt. Ik heb zelf een beetje gespeeld met ChatGTP (op chat.openai.com) en net als miljoenen anderen voel ik dat de resultaten verbluffend zijn, er staat iets te gebeuren.

Vroeger wilde ik altijd naar mijn ome Piet om daar Pong te kunnen spelen: "Wow! Ik kan de televisie besturen!" Nu voel ik dezelfde 'wow!' bij het gebruiken van deze tools. ChatGTP is minder leuk dan een potje Pong, maar leidt zeker tot verwondering.

#### Een voorbeeld:

**Invoer:** What is AI? How could it be used in a cyberattack? Can we write a poem about it?

#### **Respons:**

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think and act like humans. These intelligent machines can be trained to perform a variety of tasks, such as recognizing patterns, making decisions, and solving problems. AI has the potential to revolutionize many industries and has already begun to transform fields such as healthcare, transportation, and manufacturing.

In the context of a cyberattack, AI could be used to automate various aspects of the attack, such as identifying and exploiting vulnerabilities, evading detection, and adapting to countermeasures. For example, an AI-powered malware might be able to modify its own code to bypass security measures or generate new tactics to evade detection.

#### Here is a poem about AI:

*"AI, a curious mind,  
A digital being, of a different kind,  
With algorithms for thought, and data for sense,  
Its intelligence grows, with every experience.  
..."*

Misschien niet mijn beste stukje proza... maar het kostte me minder dan vijf seconden om te fabriceren. Stel je voor dat we iets invoeren dat we eenvoudig zouden kunnen vinden op openbare bronnen als Facebook? Een beetje AI meets Open Source Intelligence (OSINT) zullen we maar zeggen.

**Invoer:** Stel een vraag aan Ome Piet die glaskunst maakt en een vintage gameconsole heeft met Pong erop.

**Respons:** Ome Piet, hoe ben je begonnen met het maken van glaskunst en wat trekt je het meest aan in dit medium? Heb je ook ervaring met andere soorten kunst, zoals schilderen of tekenen? Wat vond je het leukste aan het spelen van Pong op je vintage gameconsole? Zou je ooit een andere oude game willen proberen?

Met wat gestoei kan je een vlot gesprek simuleren. Kijk hier eens naar...

**Invoer:** Ome Piet antwoord: Die oude Pong game werkt niet meer hoor!

**Respons:** Sorry dat te horen. Het kan frustrerend zijn als een apparaat of spel niet langer werkt zoals verwacht. Zou je interesse hebben in het proberen om de Pong game te repareren of misschien zelfs te modificeren? Of ben je meer geïnteresseerd in het spelen van andere vintage games op je console? Ik ben benieuwd naar je ervaringen met het verzamelen en spelen van oude games.

Dit is natuurlijk geen conversatie waar Ome Piet in zou trappen. Je hoort bijna een computerstem in je hoofd als je het leest. Ik stuur een beetje bij...

**Invoer:** Nog veel informeler, amicaler zoals een puber zou doen.

**Respons:** Hé Ome Piet, jammer dat die oude Pong game niet meer werkt. Ben je geïnteresseerd in het proberen om het te repareren of heb je misschien zin om andere oude games te spelen op je console? Dat lijkt me zo cool! Is er een game in het bijzonder waar je naar uitkijkt om te spelen?

Hmmm, veel beter. Nu is het zo dat je eenvoudig met wat scripting tegen deze ChatGTP aan kunt programmeren, er is gewoon een API

## AI ofnie?

beschikbaar. Het is dus goed denkbaar dat je op grote schaal 'nep gesprekjes' kunt voeren. Eenmaal 'beet' kan de uiteindelijke phisher het gesprek overnemen en de buit binnenhalen. ChatGTP gaat zelfs door op voorgaande responses en kan daar slim op variëren. Voor nu vergezocht, maar met de juiste context en wat extra informatie trappen er misschien wel mensen in deze vorm van communiceren.

Echt van nep onderscheiden wordt steeds moeilijker. De eerdergenoemde AI's die beelden genereren op basis van prompts (invoer) kunnen daarbij ook invloeden van kunstenaars meenemen. Er is een Zweedse kunstschilder (Simon Stålenhag) die al bezwaar heeft gemaakt tegen de output, het leek gewoon sprekend op zijn werk. Met tekst werkt het net zo, je kunt ChatGTP vragen iets in de stijl van Shakespeare te schrijven.

Als kunstenaars en schrijvers moeten gaan vechten om de rechten op intellectueel eigendom met een AI dan weet je dat we op onze hoede moeten zijn. Tot nu toe was een van onze grootste wapens tegen cybercriminaliteit dat je met wat training, oppassen en controleren snel 'fake' kon herkennen. Vaak mist gegenereerd materiaal een ziel. Die verdediging lijkt nu voorgoed van tafel.

En we zijn niet de enige beroepsgroep die gaat worstelen. De eerste afstudeerverslagen die door een computer zijn geschreven, zijn al gesignaleerd. "Nakijken is onzin vanaf nu!", roepen sommige leraren. In Amerika heeft ChatGTP het advocaat-examen met goed gevolg afgelegd en Getty Images verbiedt AI gegenereerde kunst. Bij het schrijven van software krijgen engineers hulp in Github van CoPilot. Ook hier schrijft ChatGPT mee. Wie is er aansprakelijk als dat tot fouten leidt? Van wie is de code? Moeten we dit juist meenemen in onderwijs en gaan omarmen, zoals we dat ook met industriële robots en 3D printers doen? Moeten we meer nadruk gaan leggen op correct, veilig en ethisch gebruik van de tools?

Maar goed, AI gedreven phishing bots. Mijn ome Piet is helaas al een paar jaar dood en trapt er dus niet meer in. Voor de rest van ons hier nog de tweede strofe van het gedicht waarop de chatbot me trakteerde:

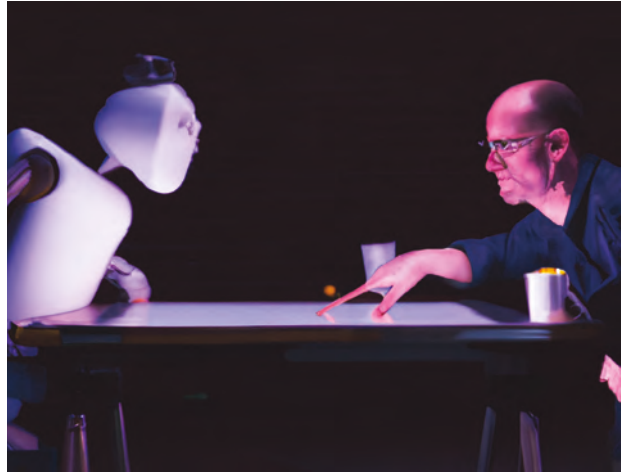
"...

*It can learn and adapt, at an alarming pace,  
A formidable force, in the digital space,  
But with great power comes great responsibility,  
For AI, a potential for both good and malevolency."*

Een heel goed nieuwjaar en ... sterkte allemaal in 2023.

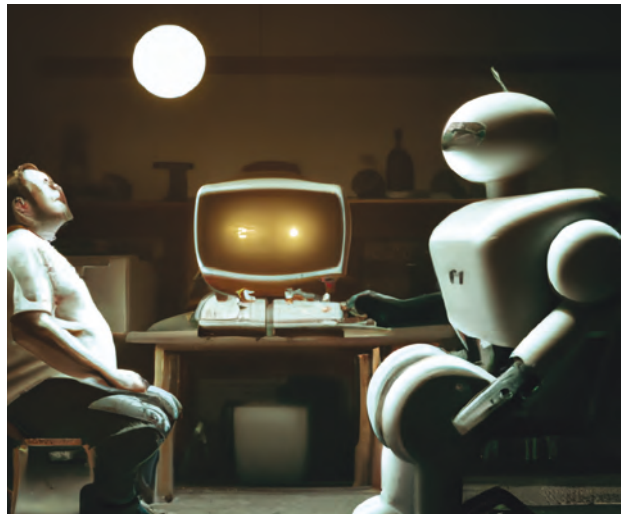
**Invoer:** A game of pong played between a robot and a older man in a dark lit room. The style is photo realistic. They are looking at a screen where the game is visible.

### Respons DALL-E 2:



**Invoer:** A futuristic robot that resembles a man is playing a computer game of classic pong against a male older bold chubby human. They look directly at the screen where the game of PONG is visible. The room is dark lit and the style of the image is like a photo by Annie Leibovitz. Both are holding a joystick.

### Respons DALL-E 2:



### Referenties

CoPilot: <https://github.com/features/copilot>

DALL-E 2: <https://openai.com/dall-e-2/>

ChatGPT: <https://chat.openai.com/chat#>

Midjourney: <https://midjourney.com>

Lex: <https://lex.page/>

OSINT: Open Source Intelligence ([https://en.wikipedia.org/wiki/Open-source\\_intelligence](https://en.wikipedia.org/wiki/Open-source_intelligence))

Simon Stålenhag geïnspireerd: <https://www.wired.com/story/artists-rage-against-machines-that-mimic-their-work/>



# Even voorstellen: Valentijn Ishaqsada



Ik ben Valentijn Ishaqsada, sinds november officieel de nieuwe voorzitter van de commissie Public Relations & Communicatie (PRC). In deze rol heb ik het stokje overgenomen van Migiel de Wit-Beets. Eerder vorig jaar ben ik, in de rol van algemeen bestuurslid, al toegetreden tot het bestuur van het Platform voor Informatiebeveiliging (PvIB).

In mijn tijd als student Information Security Management aan de Haagse Hogeschool ben ik via mijn toenmalige bijbaan bij APM Terminals, tussen het vulnerability management door, enthousiast gemaakt voor het PvIB. Dit via onze huidige secretaris Erwin Bosma. Al snel was ik lid, bezocht ik de leerzame evenementen en werd ik commissielid van Jong PvIB.

Inmiddels werk ik al enkele jaren als zelfstandige. En of een IB-casus zich nu afspeelt bij een multinational of een overheidsinstelling, nog altijd ben ik zeer content met mijn keuze voor dit vak. Vind maar eens een ander vakgebied met een soortgelijke diepgang, breedte en evenredig ontwikkelingstempo.

Hoewel ik al bijna tien jaar een betrokken lid ben van het PvIB, leer ik binnen de vereniging steeds weer iets nieuws. Er komt immers een enorme berg aan kennis, ervaring en verschillende achtergronden samen binnen deze mooie club. Informatiebeveiliging is logischerwijs niet absoluut, maar het doet mij altijd goed om te zien hoe gepassioneerd PvIB'ers de discussie over uiteenlopende IB-thema's met elkaar aangaan. De (verbale) polemiek vind ik belangrijk in het interpersoonlijke samenspel, waarbij de kennis en ervaring van de één voor een ander weer tot nieuwe perspectieven en inzichten kunnen leiden.

Of het nu voortvloeit uit nieuwe verplichtingen van de wetgever of een ernstiger dreigingsbeeld, security & privacy zijn in steeds grotere mate een standaard gespreksonderwerp aan de managementtafel geworden. Daarbij is het in beginsel voor de gemiddelde IB-professional geenszins nieuws dat de sector en het beroepenveld ieder jaar gestaag groeit. Dit maakt dat het PvIB

zich in een kansrijk klimaat bevindt voor de verdere ontwikkeling en professionalisering van de vereniging.

Het afgelopen jaar heeft de commissie PRC deze kansen al goed weten te benutten. Zo is het PvIB door haar inspanningen sterk aanwezig op LinkedIn en wordt er gestaag voortgang gerealiseerd in de verdere digitalisering van de vereniging. Daarbij is het 15-jarig lustrumfeest een prestatie van formaat gebleken, waaraan PRC door middel van sponsoracquisitie ook een bijdrage heeft geleverd.

In mijn rol als voorzitter heb ik samen met de commissie meerdere hoofdpijlers geformuleerd. Zo gaan we inzetten op een doelgroepgerichte aanpak met een bijpassende boodschap. In je ontwikkelreis als professional heb je in verschillende fasen immers verschillende behoeften. Daarnaast gaan we inzetten op een sterkere profilering. Door als vereniging op de juiste plekken zichtbaar te zijn en marketinginstrumenten tactisch in te zetten, brengen we onze vereniging naar een hoger niveau. Hierbij werken we nauw samen met Jong PvIB. Studenten en young professionals vormen immers de sleutel tot de continuïteit van de vereniging.

Graag zie en spreek ik jullie op de evenementen en mocht je ideeën hebben of kansen zien, spreek me dan zeker aan. Mailen mag ook naar [valentijnishaqsada@pvib.nl](mailto:valentijnishaqsada@pvib.nl).

Samen gaan we er iets moois van maken. Op naar de toekomst!

**Valentijn Ishaqsada**



**BLOG**

# Security inspiratie uit Italiaanse koffies

Italiaanse koffies maken mij gelukkig. Lees hier hoe ze je ook kunnen inspireren op security-gebied.



### Cappuccino

De ochtend na mijn eerste overnachting in Reggio Emilia ontdekte ik hoe echte Italianen ontbijten: een cappuccino, staand en pratend gedronken in de ontbijtzaal en een sigaret, stijlvol opgerookt in de naastgelegen binnentuin.

Het mij als "Engels en geschikt voor toeristen" aanbevolen hotel bood geen Engels ontbijt, maar ruim voldoende zachte broodjes, beleg, hardgekookte eieren, muffins en croissants. De Italiaanse gasten taalden hier niet naar en namen alleen een espresso met daarop een flinke hoeveelheid warme geschuimde melk. Door je oogharen lijkt dat inderdaad op de bruine pij en witte kap van een kapucijner monnik (Ordo Fratrum Minorum Capucinatorum). Na mijn ontbijt zag ik tijdens het wandelen door de pittoreske plaats meer inwoners cappuccino drinken, maar na half elf was dat voorbij. Dit gebruik verklaart de verbaasde blikken van Italiaanse obers wanneer Nederlandse toeristen, na het nuttigen van een salade, een portie pasta, een volledige pizza en *alle* op tafel gepresenteerde olijven en stokbroodschijfjes met kruidenboter, als toetje bij hen ook nog een volledig *ontbijt* bestellen.

Dat is net zo raar als pas na afronding van een security-issue de gang van zaken te gaan evalueren. Oh wacht, zo doen we het meestal juist wel in securityland! Alleen bij een uitwijktest lopen er al tijdens de testuitvoering personen rond die zelf niet uitwijken, maar louter waarnemen, interpreteren, opschrijven en melden wat er goed en vooral fout gaat.

Evalueren (zie ook: "grondig onderzoeken, alle feiten op tafel, achterliggende oorzaken diepgaand inventariseren en de onderste steen boven halen" in Den Haag), kun je natuurlijk nooit vooraf doen. Maar tijdens het proces vind ik wel nuttiger dan alleen achteraf. Want wie weet of je later de 'lessons learned' (zie: "take aways, ja er zijn fouten gemaakt, hebben veel geleerd, gaan nog meer ons stinkende best etc.", idem) in *precies* hetzelfde incident kunt toepassen? Beter ten halve gekeerd, dan ten hele gedwaald. En om dat te bereiken, kun je je leermomenten maar het beste zo vroeg mogelijk in het proces pakken.

### Espresso is de basis

Veel Italiaanse kantoren en bedrijven hebben geen eigen koffievoorziening. Medewerkers lopen dus enkele keren per dag

naar buiten om in een café een koffie te drinken. Een perfecte 'espresso' maak je door een straal warm water 25-30 seconden lang onder druk (9 atmosfeer of meer) door een dunne en geperste laag van zeven gram gemalen koffie te laten lopen. Resultaat is een concentraat - niet meer dan 30 ml - van puur smaakgenot.

Staand en aan de bar gedronken is de 'espresso' goedkoper dan wanneer je aan een tafeltje gaat zitten. Wie weinig tijd heeft, bestelt een 'ristretto'. Door het beperken (denk aan: restrict) van de hoeveelheid water krijg je een heel sterke koffie die je in één slok kunt innemen. En dan snel weer aan het werk natuurlijk.

Met meer tijd en dorst neem je een 'doppio', een dubbele espresso in een kopje. Vind je dat te duur, dan laat je een enkele espresso met heet water aanlengen tot een 'lungo'. Ook wel 'Americano' genoemd, omdat Noord-Amerikaanse toeristen van grote kartonnen (bah!) bekers met slappe slobberkoffie houden. In Oostenrijk, waar de eerder genoemde croissant is uitgevonden onder de naam 'Hörnchen', heet zo'n espresso met extra water erin prozaïsch een 'Verlängerte'. Veel duidelijker beschrijven kan niet, al komt het Duitse "koude rauwe dode vis" voor Japanse sushi dicht in de buurt.

Voor goed en stevig schuim op een cappuccino gebruikt men halfvolle melk op de espresso. Maar als je warme volle melk in een glas doet en dan voorzichtig een espresso erbij giet, ontstaan er mooie lagen in meerdere kleuren bruin en heb je een 'Latte' gemaakt. Met een lepel kun je die lagen door elkaar roeren, zodat een Duitse 'Milchkaffee' ontstaat. In Nederland heette dit vroeger 'koffie verkeerd', maar dat is tegenwoordig niet meer foutloos te bestellen bij een louter Engelstalige ober. Al die varianten op die ene 'espresso' gemaakt onder hoge druk doen mij denken aan APT. De aanvalsgroepen (1) die een Advanced Persistent Threat vormen, verzinnen natuurlijk zelf stoere namen (tiger, bear, gator) voor hun bendes, hacking-softwareleveranciers en samenwerkingsverbanden. Toch krijgen ze van security-onderzoekers ook een APT-volgnummeretje. Omdat de volgnommers doorlopen over meerdere landen heen, suggereert bijvoorbeeld APT28 (Rusland) dat er nog minstens 27 andere aanvalsgroepen uit Rusland zijn. Uit bijgaande tabel blijkt echter dat de meeste APT-groepen geattribueerd worden aan China. Niet elke APT-groep heeft het op bijvoorbeeld ban-

## Security inspiratie uit Italiaanse koffies

ken of ziekenhuizen gemunt. Wel mikken vele groepen op het 'Militaire Industrie Complex'. Deze langdurig (zeer) goedverdienende bedrijfstak is aantrekkelijk voor ransomware-aanvallen. Maar veel verdedigers nemen aan dat de aanvallen op MIC door APT-groepen als proxy uitsluitend in opdracht van landen (nation states) gebeuren.

Gooi de diverse doelwitten van de verschillende APT-groepen op één hoop en kijk puur naar de aantallen groepen en niet naar hun feitelijke omvang en of ze nog steeds actief zijn. Dan kun je stellen: "de grootste cyberdreiging voor de wereld (en dus Nederland) komt uit China". Een conclusie die ook de AIVD een tijd geleden trok. Naar ik hoop op basis van meer onderzoek dan alleen mijn bijlage met een samenvatting van APT-actors en hun *vermoedelijke* (!) herkomstlanden. Enkele groepen in de tabel hebben meerdere namen. Sommige security-onderzoekers denken op basis van overeenkomsten in criminele aanpak, geraakte doelwitten en hergebruik van specifieke (delen van software) code dat het toch een en dezelfde groep is. De lijst is dus mogelijk overcompleet en zeker niet uitputtend: de beste APT's staan er niet op!

### Bijzondere variaties

Een 'caffè corretto' wordt 'verbeterd' door er een scheutje grappa, cognac of sherry bij te gieten. Wanneer je als Nederlandse toerist in Italië als een echte 'local' nonchalant een 'corretto' bestelt, krijg je dus (in het Italiaans!) de detailvraag 'wat wil je er in?'.  
De allermooiste variant vind ik de 'caffè sospeso' (denk aan: suspended). Deze 'uitgestelde koffie' is een traditie in de koffiebars van Napels. Wanneer de klant uit vrijgevigheid een 'sospeso' bestelt, betaalt hij twee koffie maar krijgt er slechts een. Een waardebon voor de tweede kop gaat met een magneet of plakband op de espressomachine, de bar of het buitenraam. Iemand zonder geld, maar met zin in koffie kan vragen of zelf zien "of er nog een koffie in de wacht staat" en deze op de gezondheid van de schenker lekker opdrinken.

Zo kun je ook eigen kennis en ervaring met securityzaken (wel achteraf, zie 'cappuccino') gratis delen met andere personen, bij voorkeur in je eigen bedrijfstak. Als iedereen dat in vertrouwen en naar draagkracht doet, ontstaat vanzelf een 'wisselgeldgemeenschap' waarin uiteindelijk elk lid leert en beter wordt.

### Referentie

(1) Meer informatie over APT-actors op

[https://en.wikipedia.org/wiki/Advanced\\_persistent\\_threat](https://en.wikipedia.org/wiki/Advanced_persistent_threat)

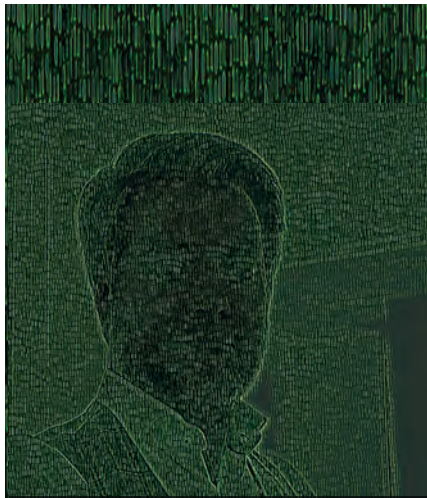
### Bijlage Advanced Persistent Threats Actors (APTs)

Onderstaande lijst staat in andere volgorde, met informatie over doelwitten en aanvalstechnieken op <https://www.mandiant.com/resources/insights/apt-groups>

Let op: overal staat *suspected* attribution. AKA = also known as.

- APT41** China
- APT40** China
- APT39** Iran
- APT38** North Korea
- APT37** North Korea
- APT35** Iran - AKA: Newscaster Team
- APT34** Iran
- APT33** Iran
- APT32** Vietnam - AKA: OceanLotus Group
- APT31** China
- APT30** China
- \*\*APT29** Russian (staat niet in deze lijst, maar elders wel attributie aan Rusland)
- APT28** Russian government - AKA: Tsar Team
- APT27** China
- APT26** China
- APT25** China - AKA: Uncool, Vixen Panda, Ke3chang, Sushi Roll, Tor
- APT24** China - AKA: PittyTiger
- APT23** China
- APT22** China - AKA: Barista (*leuk! - RM.*)
- APT21** China - AKA: Zhenbao
- APT20** China - AKA: Twivy
- APT19** China - AKA: Codoso Team
- APT18** China - AKA: Wekby
- APT17** China - AKA: Tailgator Team, Deputy Dog
- APT16** China
- APT15** China
- APT14** China
- APT12** China - AKA: Calc Team
- APT10** China - AKA: Menupass Team
- APT9** freelancer group with some nation-state sponsorship, possibly China.
- APT8** China
- APT7** China
- APT6** China
- APT5** China
- APT4** China - AKA: Maverick Panda, Sykipot Group, Wisp
- APT3** China - AKA: UPS Team
- APT2** China
- APT1** China's People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 - AKA: Unit 61398, Comment Crew





Martijn Hoogesteger is Head of Cyber bij S-RM en is bereikbaar via [m.hoogesteger@s-rminform.com](mailto:m.hoogesteger@s-rminform.com).

## Vlaggetjes scoren om scherp te blijven

Wat komt er na ransomware? Het is een onderwerp dat ik vaak raak in gesprekken, in presentaties voor klanten of zelfs in mijn columns. De afgelopen jaren hebben cybercriminelen vrij spel gehad en gigantische impact gemaakt met ransomware en de bijbehorende strategieën. Dit vormt ook onze preventie en detectie van cyberaanvallen. Ons hele narratief als we over cyber willen praten, is ransomware. Ik snap het, de jaren hiervoor waren we iedereen nog aan het wakker schudden dat cybersecurity toch echt wel belangrijk is. En nu hebben we een magisch woord dat iedereen triggert om wat te doen.

Laten we niet vergeten dat cybersecurity om meer draait, zodat we blijven reageren op de volgende stap. Een van de manieren waarop ik dat graag doe, is meedoen aan CTFs – Capture the Flag evenementen. Het idee is simpel: verschillende cybersecurity puzzels en -challenges staan online en als je ze oplost, krijg je een 'flag', een bepaalde zin die je inlevert voor punten. Meer punten betekent hoger op het scorebord staan en vaak zijn er ook prijzen voor de beste teams. Verschillende evenementen spitsen zich toe op verschillende onderdelen binnen cybersecurity. Er zijn er ook veel die voor beginners geschikt zijn, dus laat je niet tegenhouden!

Challenges kunnen gaan over (web) hacking, forensics, open source intelligence, cryptografie, noem het maar op. Het leuke hieraan: je traint jezelf om weer anders naar cyberproblemen te kijken en nieuwe inzichten te vergaren. Het type challenges dat je in deze CTFs vindt, heeft bijna altijd een ander perspectief nodig om op te lossen. Je leert wellicht over hoe je netwerkpakketten op een andere manier kunt inspecteren, hoe bepaalde cryptografische sleutels werken of hoe vrachtcontainers een code hebben die via open bronnen te volgen is.

Voor mij is het niet alleen iets om mijzelf te trainen. Het is ook hartstikke leuk om samen te doen met collega's of ze nou in cybersecurity zitten of niet. Hen een website laten bezoeken om in de HTML een vlag te vinden kan soms leuker zijn dan malware reversen door de grootste expert. Iedereen kan altijd scherper worden en we moeten rennen om bij te blijven met hoe snel ons vakgebied ontwikkelt.

Dit blijven leren en met nieuwe perspectieven werken, is belangrijk wanneer er weer een nieuw soort techniek of aanval op de radar verschijnt. Het maakt het snelle schakelen en nieuwe context tot je nemen een sport in plaats van een zwetende crisis. Misschien zit je uiteindelijk net als ik te wachten tot de volgende challenge vrijkomt en ik weer grijnzend kan proberen de eerste te zijn die de hem oplost.

Hoe je het doet, maakt me niet uit, als je maar blijft uitzoeken en jezelf scherp houdt! Cybercriminelen mogen ook in de volgende ronde weer wat extra tegengewerkt worden.

Xvwx rraf rra xrre bc pgsqvzr.bet ibbe rra yrhr PGS, ra nnatrmvra wr qvg urog jrgra bc gr ybffa, vx mvr wr qne!





# SOCCRATES - Automation and Orchestration of Security Operations

SOCCRATES (SOC & CSIRT Response to Attacks & Threats) is an European innovation project, co-funded by the Horizon2020 programme 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 fourth article on the project will focus on the SOCCRATES Orchestrator and Integration Engine which is at the core of the SOCCRATES platform providing automation and orchestration of security operations to response.

## SOCGRATES - Automation and Orchestration of Security Operations

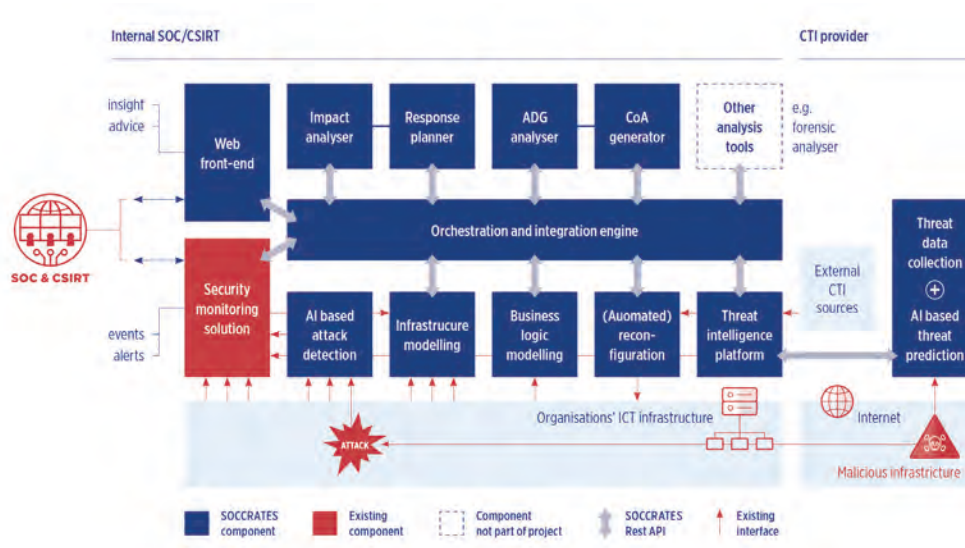


Figure 1: The SOCCRATES Platform.

The SOCCRATES project was introduced in three previous articles (IB4-, IB5.2021, and IB5.2022). 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 (winning) 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 fourth article goes into more details on the SOCCRATES Orchestrator and Integration Engine which is at the core of the SOCCRATES platform.

As described in the first articles, there are many challenges that SOCs, CSIRTs and Managed Security Service Providers (MSSPs) face to offer an efficient and quick answer to the increasing, evolving and more and more complex number of cyber attacks that organisations are confronted with.

One of these challenges is to provide support to the security analysts in the automation and orchestration of the different tasks they need to perform to give response to specific common situations, such as the ones included in the SOCCRATES Use Cases:

- **Use Case 1: Response on Detected Ongoing Attack**

Detect ongoing attacks and automatically analyse the attack, automatically determine the best response, and initiate deployment of the selected response.

- **Use Case 2: Response on Newly Received Cyber Threat Intelligence**

Continuously collect new threat information, automatically analyse the potential business impact and determine best options for proactive mitigation.

- **Use Case 3: Response on Newly Discovered Vulnerable Assets**

Automatically detect vulnerabilities on assets in the ICT infrastructure, assess if they enable new attack paths, determine and initiate mitigation actions.

- **Use Case 4: Response on Discovered System Configuration Change**

Automatically detect configuration changes on assets in the ICT infrastructure, assess if they enable new attack paths and determine if action is needed.

- **Use Case 5: Response on Deployment of New Systems in Infrastructure**

Automatically detect introduction of new systems to the ICT infrastructure. Automatically assess the new situation and determine if (additional) security measures are needed.

The SOCCRATES Orchestrator and Integration Engine is at the core of the SOCCRATES platform (see figure 1) and was developed from existing technologies to cover the requirements about automation and orchestration established in the project.

After analysing the current state of the art in security orchestration and automation solutions, two different open-source solutions (Activiti (1) and Cortex(2)) were chosen as starting point to provide on the one hand workflow execution capabilities and on the other hand support to interconnect and invoke external tools. Consequently, the component was divided in two main sub-

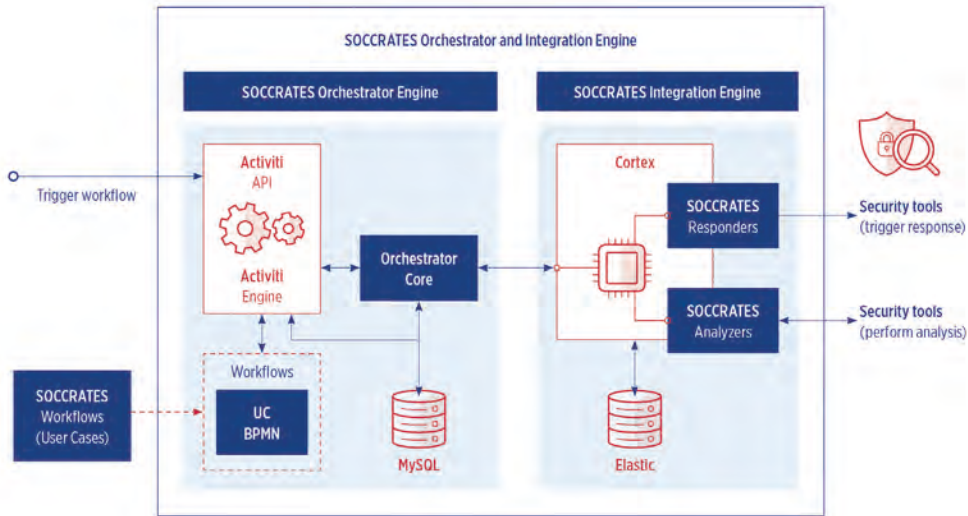


Figure 2: SOCCRATES Orchestrator and Integration Engine Architecture.

components (see figure 2), each of them focused on one of those main functionalities and built on top of different technologies:

- the SOCCRATES Orchestrator Engine, and
- the SOCCRATES Integration Engine.

### The SOCCRATES Orchestrator Engine

This component integrates the lightweight open-source BPMN (Business Process Model and Notation) workflow engine Activiti to support the management and execution of the security automation and decision processes included in the five use cases defined in the project. The different workflows associated to the use cases have been modelled using the standard BPMN and they are loaded to the Activiti Engine.

The workflows can be triggered by different external tools invoking the Activiti REST API. In particular, the Use Case 1 is triggered by a SIEM (Security Information and Event Management) when there is an alarm for an ongoing attack, Use Case 2 is triggered by the Threat Intelligence Platform when it is reported a new exploit code discovered for a vulnerability or a new technique associated with a threat actor, and the other Use Cases (3-5) are triggered by the Infrastructure Modelling component in different situations. Each of these triggering messages starts a new process definition in the Activiti Engine.

The Orchestrator Core manages the communication between Activiti and the SOCCRATES Integration Engine, retrieving from the triggering messages the relevant information, preparing the request data necessary for the invocation of the different security components in charge of each task included in the workflows and processing the responses received.

### The SOCCRATES Integration Engine

This component is composed by the open-source solution Cortex created by The Hive Project (3) and a set of SOCCRATES Responders and Analysers, most of them developed in the project by the tool partners and associated to each of the components in the SOCCRATES Platform.

Analysers and responders are connectors that allow interaction between Cortex and external tools. The main difference between them is that Responders just trigger some action in an external tool (e.g. send an email or update a business model) without the need of receiving any response from the component, whereas the Analysers request some analysis or action providing some data in the request and obtain a response with the report of the analysis performed. These Cortex Analysers and Responders are invoked by the SOCCRATES Orchestrator Engine throughout the different workflow stages. The following components of the SOCCRATES Platform are integrated through Cortex analysers or responders:

- **Attack Defence Graph (ADG) Analyzer**, to analyse and generate a next step analysis or determine the potential attack path.
- **Course of Action (CoA) Generator**, to suggest potential defences (Course of Actions) included in the model to the SOC analysts that could be activated to isolate or mitigate the risks.
- **Business Impact Analyzer (BIA) & Business Logic Modelling**, to evaluate the affected or potentially affected assets and for containment.
- **AI based Attack Detection (AAD)**, to perform a new attack detection based on multiple data sources when a new vulnerability or asset has been found in the infrastructure.
- **Infrastructure Modelling Component (IMC)**, to get information of



Figure 3 – SOCCRATES Web Front End.

the monitored infrastructure, mainly to translate from IPs and hostnames to internal identifiers.

- **Automated Reconfiguration (AR)**, to interact with the IT support or IT infrastructures to perform some mitigation action (e.g. send an email, send a webhook notification to an endpoint or execute a CACAO playbook) depending on the selection of Course of Actions done by the SOC analyst.
  - **Response Planner (RP)**, to calculate the Return on Response Investment (RORI) associated to the Course of Actions identified.
- The SOCCRATES Orchestrator and Integration Engine also includes a Web Front End (see figure 3) which provides a graphical user interface that allows the SOC/CSIRT analysts to visualize and interact with the different workflows (Use Cases) running in the Orchestrator and access to the graphical user interfaces provided by the different SOCCRATES components (Business Impact Analyzer, Response Planner, Infrastructure Modelling Component and Threat Intelligence Platform).

### Future research lines

As it has been presented, current functionality of the SOCCRATES Orchestrator and Integration Engine is based on the capabilities provided by two open-source solutions, Activiti and Cortex, and it provides automation and orchestration for the workflows defined by the use cases considered in the project. These workflows should be reviewed and updated to support different target SOC/CSIRT infrastructure models (such as hybrid, cloud based, virtualized) and add the possibility to be tuned for specific environments. It is also necessary to perform more research and new developments to improve the visualisation capabilities of the component and allow its integration with other open-source tools that could be also used in SOC/CSIRT environment. Related to interoperability, investigate

the feasibility of normalizing the data formats used in the communication between the different components integrated through the SOCCRATES Orchestrator and Integration Engine is another potential research topic. The usage of some standardized format (such as STIX or OpenDXL) in this communication could help to extend and generalize the workflows and facilitate the integration of the SOCCRATES platform with other security products or tools used by SOC/CSIRTs analysts.

It would be also interesting to investigate how to improve the capabilities of the SOCCRATES Orchestrator and Integration Engine to support the simultaneous triggering of events related to a same security incident and do some additional research to integrate Artificial Intelligence (AI) in the component, for example to add the possibility of learning from the decision-making process done by the SOC/CSIRT analysts in order to make suggestions for future handling of security events based on previous choices. Finally, also related to an effective security decision-making process, human-machine interaction in SOC/CSIRT operations is also an important topic for future research and many open questions are still to be answered in this area.

### References

- (1) <https://www.activiti.org/>
- (2) <https://github.com/TheHive-Project/Cortex>
- (3) <https://thehive-project.org/>
- (4) SOCCRATES Vision, Roadmap & Guidance for SOC. Available at <https://www.soccrates.eu/wp-content/uploads/2022/05/SOCCRATES-Vision-Paper.pdf>
- (5) D6.1 Initial version of the SOCCRATES Platform Orchestration, Reconfiguration and Front-end. Available at <https://www.soccrates.eu/results/>
- (6) D6.2 Initial version of the SOCCRATES platform. Available at <https://www.soccrates.eu/results/>





# Risicoklassenindeling digitale veiligheid gelanceerd

De coronacrisis heeft eens te meer duidelijk gemaakt dat verdere digitalisering van onze samenleving onvermijdelijk is. Ook is duidelijk dat het inschatten van cyberrisico's ingewikkeld is en het verzekeren ervan voor veel bedrijven en burgers niet vanzelfsprekend. Met de ontwikkeling van een 'risicomodel cyber' willen publieke en private partijen hierin gezamenlijk verandering brengen. Begin 2021 heeft het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) daarom de Risicoklassenindeling Digitale Veiligheid gelanceerd (1), gebaseerd op de bij verzekeraars ingeburgerde 'VRKI-methodiek'.

**N**aast een objectief oordeel over het niveau van cyber-risico van een (mkb-)onderneming, biedt het instrument inzicht in de bijpassende beheersmaatregelen. Dit artikel schetst het belang en de werking van het instrument.

Particulieren en bedrijven ondervinden steeds meer hinder van cyberincidenten, een verzamelnaam voor falende systemen, maar ook vandalisme en criminaliteit zoals diefstal of afpersing. Cyberincidenten kunnen op verschillende manieren tot schade leiden. Systemen kunnen onbruikbaar worden en criminelen kunnen gegevens misbruiken voor geld of om te frauderen. Bedrijven lopen het risico dat hun operationele continuïteit in gevaar komt of dat ze klanten kwijtraken. Doordat ze bijvoorbeeld niet bereikbaar zijn of omdat gegevens op straat zijn komen te liggen. Steeds vaker ook worden systemen gegijzeld voor losgeld.

De toenemende digitalisering is ook zichtbaar in de criminaliteitscijfers; daar waar in algemene zin de offline criminaliteit gestaag daalt, neemt de online criminaliteit toe en is dit ook een vast onderdeel geworden in de opsporing door de politie. De politie roept daarom bedrijven op om altijd aangifte te doen (zie kader Melding of aangifte van incidenten).

### Verzekeren van cyberrisico's niet vanzelfsprekend

Ook verzekeraars worstelen met cyberrisico's bij en cyberveiligheid van hun klanten. Het verzekeren van cyberrisico's is nog altijd verre van vanzelfsprekend. Voor een deel komt dit doordat het bewustzijn van deze risico's onder burgers en bedrijven wel toeneemt, maar nog altijd laag is, overheidscampagnes ten spijt. Ook komt het voor dat mensen of organisaties denken dat schade door cybercrime wordt gedekt door bestaande verzekeringen, de zogenaamde 'stille' cyberdekking, terwijl dat meestal niet of hooguit zeer beperkt het geval is. Tegelijkertijd is het aanbod van cyberverzekeringen nog relatief klein.

De modus operandi van criminelen en daarmee het risico verandert zeer snel en net als bij terrorisme en natuurrampen zijn cyberrisico's voor individuele verzekeraars en de verzekeringsbranche moeilijk in te schatten. De meeste 'traditionele' verzekeringsproducten bieden hooguit beperkte dekking voor de gevolgen van cyberrisico's. Verzekeraars willen hun (zakelijke) klanten ook oplossingen bieden voor cyberrisico's en bieden inmiddels cyberverzekeringen aan.

Het betreft hier vrijwel zonder uitzondering zogenaamde 'totaalpakketten', waarin verzekeraars vooraf risico's scannen, preventieve maatregelen adviseren, (technische, juridische, forensische) hulp bieden tijdens en na een incident en de financiële gevolgen van het restrisico verzekeren. Het Centrum voor Verzekeringstatistiek van het Verbond van Verzekeraars becijfert het totale premievolume van

cyberverzekeringen in Nederland in 2019 op 'slechts' 17 miljoen euro, tegen 2,3 miljard dollar in de Verenigde Staten. Hoewel het premievolume langzaam toeneemt en Nederland het in vergelijking met andere Europese landen zo slecht nog niet doet, blijven de absolute en relatieve aantallen klein. Zeker gezien de dichte IT-infrastructuur in ons land. Het Centraal Planbureau concludeert in het rapport *Risicorapportage cyberveiligheid economie 2019* (2) dat gebrek aan inzicht in kosten en baten van cyberveiligheid een belemmering is voor de ontwikkeling van een verzekeringsmarkt voor cyberrisico's.

### Risicoklassenindeling

'Keurmerk voor een veilig internet is hard nodig', kopte het Financieele Dagblad in de zomer van 2017. Volgens Het FD werden er destijds wereldwijd per minuut tachtig apparaten aangesloten op het internet, maar kwamen deze onbeveiligd onze huiskamer of ons kantoor binnen. Nu, vijf jaar later is dit nauwelijks verbeterd. Ook onder verzekeraars en IT-beveiligingsbedrijven bestaat de behoefte aan een instrument om eenduidig en objectief de cyberrisico's van hun klanten te bepalen en te koppelen aan gepaste maatregelen. De Risicoklassenindeling helpt bedrijven om cybersecurityrisico's in te schatten en maatregelen te treffen.

Het instrument richt zich in eerste instantie op het midden- en kleinbedrijf (mkb), maar is ook voor andere bedrijven bruikbaar. Vertrekpunt is de impact van een cyberincident op de bedrijfscontinuïteit. Het gaat vervolgens om het vergroten van het bewustzijn en het op orde brengen van de basis van digitale beveiliging van ondernemingen.

Op basis van elf vragen, zoals vastgelegd in de *Scorekaart risico's digitale veiligheid*, wordt het risico van de mkb-onderneming op een cyberincident bepaald. De scores vertalen zich in vier risicoklassen en per risicoklasse is een set van beveiligingsmaatregelen opgesteld. Deze sluiten aan op de basisprincipes van het Digital Trust Center (3). Naast technische maatregelen gaat het ook om organisatorische maatregelen, want veel risico's ontstaan juist door menselijk handelen of falen. Net als in de fysieke wereld is een driesterrenslot immers alleen effectief als je dat bij het verlaten van het pand ook echt op slot doet. Datzelfde geldt voor de cyberwereld. Computers, tablets, telefoons en alle andere apparaten die inmiddels op het internet zijn aangesloten, zijn alleen goed beschermd als er een deugdelijke firewall is ingeschakeld en wachtwoorden goed zijn en ook goed kunnen en worden beheerd.

Door cyberrisico's objectief te koppelen aan beveiligingsmaatregelen kunnen bedrijven gericht hun IT-/securitybeleid aanpassen, medewerkers instrueren en eventueel samen met hun leveranciers gepaste beschermingsmaatregelen treffen. Dat laatste is belangrijk

omdat een goed en objectief gevalideerd handelingsperspectief veelal nog ontbreekt. Ondernemers die hun cyberrisico's willen beheersen moeten kunnen vertrouwen op bestaande (gecertificeerde) normen en procedures. Zij moeten hierin immers tijd en geld investeren.

### Certificeringsregelingen

Cybersecuritydiensten zorgen voor een goede beveiliging van digitale systemen, die aansluiten op het risico van een cyberincident. Een onderneming die zich wil beschermen tegen cybercriminaliteit, wil dat dit goed gebeurt, met veilige producten en geïnstalleerd of uitgevoerd door een vakman. Voor een ondernemer is dit vaak moeilijk zelf goed in te schatten. Certificatieschema's van cybersecuritydiensten bieden hiervoor een goede oplossing. In het kader van de Risicoklassenindeling is als eerste een certificatieschema ontwikkeld voor pentesten. De komende periode wordt onderzocht voor welke andere instrumenten het wenselijk en haalbaar is om een certificatieschema te ontwikkelen.

### Publiek-private samenwerking

De Risicoklassenindeling Digitale Veiligheid en de bijgaande certificeringsregeling zijn via publiek-private samenwerking tot stand gekomen, onder regie van het CCV. Gezien het maatschappelijk belang en de rol die met name het Digital Trust Center speelt, is de ontwikkeling van het instrumentarium door de overheid gefinancierd. De deelnemende organisaties en bedrijven (zie kader Publiek-private samenwerking) hebben belangrijke bijdragen geleverd. Samen vormden ze ook de stuurgroep van het project. Sinds 1 januari 2021 bemensen ze het College van Belanghebbenden, dat de uitvoering en de verdere ontwikkeling van het instrumentarium begeleidt. Naast het delen van kennis, biedt deze brede coalitie draagvlak en objectiviteit.

### Conclusie

Met de Risicoklassenindeling Digitale Veiligheid is er voor verzekeraars, verzekeringsadviseurs, IT-/securityspecialisten en hun (mkb-) klanten een instrument beschikbaar gekomen om digitale risico's objectief in kaart te brengen en te koppelen aan gepaste beveiligingsmaatregelen. Dit vergroot de verzekeraarbaarheid van cyberrisico's.

Het digitale landschap verandert snel, waardoor onderhoud en mogelijk ook de ontwikkeling van een nieuwe certificeringsregeling nodig zal zijn. Ook voorziet het instrument vooralsnog niet in een mechanisme voor het controleren en aantoonbaar maken van

hetgeen klanten invullen via de Scorekaart. Verzekeraars kunnen hieraan in hun eigen voorwaarden eisen stellen, bijvoorbeeld door te vragen om het formulier te ondertekenen of anderszins van waarborgen te voorzien.

### Melding of aangifte van incidenten

Net als bij andere vormen van criminaliteit is het wenselijk dat ondernemers incidenten niet alleen melden bij hun IT-/security-adviseur en eventueel verzekeraar, maar dat ze ook aangifte doen. Hoewel opsporing bij cyberincidenten moeilijk is, ondersteunt het doen van aangifte het opsporingsproces meer in algemene zin. Minister Grapperhaus schrijft hierover (Tweede Kamer, vergaderjaar 2019–2020, 26 643, nr. 678): *'Door aangifte kunnen politie en justitie passende maatregelen nemen. Aangifte draagt daarnaast bij aan het brede inzicht in de aard en de omvang van deze vorm van criminaliteit waardoor ook op langere termijn een betere aanpak kan worden ontwikkeld en passende preventieve maatregelen kunnen worden genomen.'*

### Publiek-private samenwerking

De ontwikkeling van de Risicoklassenindeling Digitale Veiligheid is een samenwerking tussen het CCV, het Verbond van Verzekeraars, VNO-NCW/MKB-Nederland, Cyberveilig Nederland, NLdigital, Politie, CIO Platform Nederland, Partnering Trust, het ministerie van Justitie en Veiligheid en het ministerie van Economische Zaken en Klimaat. Deze partijen vormen ook het College van Belanghebbenden. Het project is mogelijk gemaakt door de belangeloze medewerking van genoemde partijen en financiering door de ministeries. De Risicoklassenindeling Digitale Veiligheid is online beschikbaar op [www.digitaltrustcenter.nl/risicoklasse](http://www.digitaltrustcenter.nl/risicoklasse).

### Referenties

- (1) <https://hetccv.nl/nieuws/nieuw-instrument-gelanceerd-om-cyberveerbaarheid-ondernemers-te-vergroten>
- (2) <https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf>.
- (3) <https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen>



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

## Fourth Party Risk Management, SBOM, CSAF en VEX

We beginnen het nieuwe jaar vol goede moed en bereiden ons voor op weer een jaar vol Log4J, Log4text, OpenSSL en vele andere soortgelijke kwetsbaarheden. Overnight en in het weekend lekker de eigen repo's scannen, uitpluizen en patchen en de leveranciers (third parties) bevragen of ze direct of indirect een risico vormen voor onze bedrijfsvoering. De leveranciers van de leveranciers (fourth parties) zijn echter zelden goed in beeld terwijl Supply Chain Risico's inmiddels bovenaan de lijst met cyberdreigingen staan. Hoe kunnen we de komende jaren beter zicht krijgen op deze afhankelijkheden en responstijden verkleinen op het moment dat het nodig is?

Op momenten dat we vermoeden dat er iets mis is met een softwarecomponent moeten we gaan onderzoeken of we kwetsbaar zijn. We kijken naar security advisories, bevragen de leverancier ("schiet maar een ticket in"), gaan zelf op onderzoek uit of gaan zoeken in de Software Bill Of Materials (SBOM). Als we die laatste hebben en deze up-to-date en voldoende gedetailleerd is tenminste. Het is duidelijk dat het zo dagen kost om vast te kunnen stellen of producten kwetsbaar zijn en die dagen kunnen we nu net niet missen. Automatisering is wat we hier missen.

Als we kijken naar de CVE's, de bekende kwetsbaarheden in software en netwerken, dan zien we een sterke stijging in het aantal per jaar en ze zitten ook echt overal en nergens. Op het moment van schrijven van deze column (4 december 2022) staat de teller al op 46.416 stuks. Echter, niet alle CVE's zijn ook (direct) exploiteerbaar en vormen daarmee een even groot risico. Er zit dus veel ruis in het grote aantal wat het duiden ervan en het snel schakelen evenmin versnelt.

Op de OneConference, het flagship store cyber event in Europa van het NCSC, sprak dr. Allan Friedman van de Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) over software transparantie en het tracken van software kwetsbaarheden via CSAF, de SBOM en VEX. Veel afkortingen die ons het dagelijkse cyberleven gemakkelijker moeten maken de komende jaren.

Het Common Security Advisory Framework (CSAF) is de set van afspraken over een taal waarmee security advisories en kwetsbaarheden in producten eenduidig en geautomatiseerd uitgewisseld kunnen worden binnen een keten van leveranciers. CERTS, ISACs en NCSCs gebruiken het al en in combinatie met een Vulnerability Exploitability Exchange (VEX) biedt het, volgens Friedman, de oplossing voor al het zoekwerk.

De VEX, ontwikkeld door de Amerikaanse overheid, biedt de leveranciers en gebruikers de mogelijkheid te focussen op de CVE's die daadwerkelijk direct risico's opleveren en geen tijd te verspillen aan kwetsbaarheden die geen impact hebben op de producten die jouw organisatie gebruikt. De combinatie van SBOM, CSAF en VEX geven dus direct inzicht of een product "affected", "not affected", "fixed" of "under investigation" is. De status "not affected" kan dan ook weer diepere uitleg bevatten waarom niet en de nachtrust bevorderen.

De hamvraag gaat nu worden hoeveel tienduizenden VEX-en we per jaar moeten gaan verwerken. Is de VEX het licht aan het eind van de CVE-tunnel of slechts de volgende cyber trein die op ons afkomt?





## 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](mailto:ibmagazine@pvib.nl).







Chris de Vries

Fook Hwa Tan

Leo van Koppen

# De wereld gaat aan... ten onder!

De wat ouderen (wijzeren?) onder ons herkennen wellicht deze titel. Hij dateert uit 1954 en de schrijver is Max Dendermonde. Diegenen die dat boek niet kennen, zullen wellicht woorden invullen als "oorlog", "terrorisme", "bandietenstaten", "politiek", "waandenkbeelden", "onvoorzichtigheid", "cybercriminaliteit", "phising", "software" en misschien zelfs "ICT" (vakgenoten) of "vlijt" (filosofisch aangelegde vakgenoten). Het laatste woord is juist.

De fictieve locatie is een researchcentrum in de VS (Oaklake om precies te zijn) waar men hard werkt aan middelen om nog harder te werken. En daarmee kunnen wij ook de huidige wereld karakteriseren waar - in locaties binnen de VS, China, Rusland, Europa, Azië en zo verder - hard gewerkt wordt aan de efficiëntie en transparantie van de digitale wereld. En net als in het boek zijn maar weinig mensen bereid om de zinnigheid en de daarmee gepaard gaande risico's / gevaren ("1984 - George Orwell") van al die spanningen te overwegen. Zo ook in ons kleine, bescheiden en het goede nastrevende Nederland. Zo meldt Tweakersnet met (technisch!) objectieve nauwkeurigheid (1.286 woorden) de komst van een Nederlands paspoort voor op het internet (1). Daarvan zijn 292 woorden (22,7%) gewijd aan de "kritiek en de politieke spanning". De kritiek beperkt zich tot 144 woorden (11,2%) de resterende 148 woorden (11,5%) gaan vooral om het politieke spel daaromheen. Deze kritiek-paragraaf sluit dan ook af met: "De demo van de Nederlandse app is er nu al, zodat de ontwikkeling niet pas hoeft te beginnen als die verordening er inderdaad komt."

Dat moet ons dus geruststellen, Nederland zal niet achterlopen, zeker zolang wij nog niet weten of er een beperkende Europese verordening komt. En dat ondersteunt door artikelen van de Onderzoeksraad voor Veiligheid: "Aanpak Cybersecurity heeft versnelling nodig" d.d. 13.12.2022 in aansluiting op zijn rapport "Kwetsbaar door software" d.d. december 2021(2 en 3)

## De vraag rijst dus waaraan... (?) gaat onze wereld dan ten onder? - Chris de Vries

Mijn leesadvies: zie de artikelen van Tim Janssen, VISMA, in IB.4-2020 en Kim Schneider, RABO, in IB.5-2020 over de Self-Sovereign Identity (SSI) en vergelijk dat met het Nederlands paspoort voor het internet (4).

Het is natuurlijk kinderachtig om meteen weer dwars te liggen, terwijl Nederland er voor moet waken niet achterop te raken. Kinderachtig (?), als op hetzelfde moment Tweakersnet twee andere publicaties het licht laat zien met als titels: "EU-lidstaten overtreden Europees recht met verwerking passagiersgegevens"[5] en "Microsoft laat Europeanen vanaf januari kiezen of ze data in EU willen opslaan"(6). Met dit laatste brengt Microsoft de door haar verkregen (klant)gegevens onder op een Europese server (lees - zoals ik denk - Ierland). Hetgeen natuurlijk geen garantie biedt dat Amerikaanse diensten niet alle data kunnen overnemen naar Amerikaanse servers en dat naar eigen, politiek inzicht dan wel - opdracht kunnen gebruiken.

Ook vanuit NEMO kennislink wordt m.i. een meer objectief, kritische kijk geformuleerd over een ander bestanddeel van onze ICT-voetafdruk in het artikel: "Bescherming of bedreiging - de voors en tegens van de aangepaste sleepwet op een rij"(7). En dit alles onder de supervisie / strategie van de Europese Commissie die een Europees digitale identiteitswallet (mooi, nieuw Nederlands woord?) laat ontwikkelen, waaraan onze SIDN via de 'joint venture' IRMA-ontwikkelaar ('I Reveal My Attributes', ook hier verwonder ik mij over het schone van onze taal) in een pilot deelneemt (8).

Misschien ben ik te wantrouwend, misschien twijfel ik te zeer aan de integriteit van onze overheden - wie ben ik om dat te (mogen) doen (?) - maar worden wij niet keer op keer teleurgesteld? Denk aan de recente "Toeslagenaffaire" of aan de gaswinning in Groningen, de boeren met hun CO2-problematiek en misschien zelfs ook al aan Limburg en de mijnbouw problematiek, welke recent boven water kwam als gevolg van de stijgende waterstanden in de gesloten mijnen.

Moeten wij als burger, maar meer nog als over kennis beschikkende cybersecurity-specialist, ongebreideld vertrouwen blijven houden, meewerken aan en toestaan wat ICT-technisch mogelijk is? Voortgang in technologie nastrevend in het vertrouwen dat de tijd en



## Elke berg is er om beklommen te worden!

de mensen dan levend er voor zorg dragen dat het wel goed komt door oplossingen welke wij nu nog niet zien. Waar doet mij dat ook weer aan denken: pensioenverdamping, klimaatverandering, 4-jarig kortetermijnpolitiek (en te vaak opportunistisch) beleid ...?

Daarbij wil ik erkennen dat de noodzaak voor weerbaarheid, bescherming van de identiteit van de burger, bestrijding van terrorisme, staatsactoren en wat dies meer zij terecht hoog op de agenda staan, maar niet tegen elke prijs en niet zonder het kind erbij te hebben die op straat naar de koning kijkt en de vraag stelt: "Mama, loopt die koning niet ..."?

### **Fook Hwa Tan - Ondergaan of herrijzen!**

We zien vele problemen in deze wereld. Om de haverklap wordt iets geïdentificeerd als een crisis. Ik heb, toen ik klein was, geleerd dat een crisis een uitzonderlijke situatie is. Maar nu hebben we een energiecrisis, een woningcrisis en een asielcrisis. Dit vlak na een pandemie waarmee we meer dan twee jaar hebben geworsteld. Gaan we echt ten onder?

In de geschiedenis zijn er veel bevolkingsgroepen geweest die hebben geworsteld met de veranderende tijden. Dit noemen we ook wel innovatie en ontwikkeling. Bij grote wijzigingen in de maatschappij hebben mensen moeite om mee te gaan of mee te veranderen. Wordt hierdoor elke grote uitdaging meteen een crisis? Ik denk dat het tot stilstand komen van de hele wereld door COVID-19 heeft laten zien hoe afhankelijk we van elkaar zijn geworden. Drie jaar geleden dachten we dat de pandemie mogelijk het einde van de wereld zou betekenen. Vandaag de dag leven we weer gewoon ons leven.

Het is niet zozeer de vraag waaraan we ten onder gaan, maar meer hoe houden we hoop? Er wordt wel gezegd dat elke tegenslag juist een kans is om deze te overwinnen. Onder invloed van de verdere globalisering en digitalisering van de wereld zullen we moeten leven met nieuwe technologieën en nieuwe manieren van werken, maar zolang we hoop houden en met de beste intenties ons leven leiden - waarbij we de zwakkeren onder ons helpen en de sterkeren kunnen controleren - zal de mensheid een eind komen. Elke berg is er om beklommen te worden! We zullen herrijzen als een feniks!

## Leo van Koppen - De wereld gaat aan excuses ten onder

Excuses zijn de afgelopen tijd erg in het nieuws(!) Is het een nieuwe trend geworden die hoort bij deze tijd van meer openheid en diversiteit? Ik weet het ook niet, maar constateer slechts dat vooral de huidige bestuurders zich uitputten in het uiten van excuses aan slachtoffers: ministers (aardbevingsschade, toeslagenaffaire), burgemeesters en bestuurders (slavernij, aardbevingsschade, toeslagenaffaire), CEO's (milieu, gezondheid) et cetera. Opvallend is daarbij dat er wel een flinke tijd overheen gaat voordat de slachtoffers een excuus krijgen aangeboden. Pas als er echt geen andere mogelijkheid rest, komen er excuses.

Een soort van laatste redmiddel en de erkenning van het feit dat bepaalde zaken in het verleden niet goed zijn aangepakt en vervolgens later verkeerd uitpakken. Een poging om de zaak alsnog een beetje goed te maken, waarbij een excuus tegelijkertijd wordt voorzien van de nodige disclaimers. Interessante vraag is natuurlijk of onze huidige minister-president zo rond 2040-2050 ook zijn excuses zal gaan aanbieden? Verwacht het eigenlijk niet, want zijn geheugen is, zoals hijzelf meerdere malen heeft toegegeven, nogal *volatiel*.

In ons vakgebied lijkt deze trend van het aanbieden van excuses nog weinig opvolging te krijgen. Ik heb ze nog niet gezien althans, de excuses van Microsoft, Citrix, F5, Fortinet en VMware om nog maar even in de actualiteit te blijven. En helaas is dit slechts een klein puntje van een hele grote ijsberg. Geen excuus nog gezien van deze bedrijven en ik verwacht ze eerlijk gezegd ook niet. Niet op korte, noch op langere termijn.

In de informatiebeveiliging leven we gewoon verder, werken we ons met Kerst een slag in de rondte om zaken ook voor het nieuwe jaar in de lucht te houden. Dit nadat we het hele jaar al *patchend* zijn doorgekomen.

IT-designs die in het verleden niet goed zijn aangepakt en die dan, zo blijkt later, verkeerd uitpakken. In onze wereld is het onderhoud ervan een hele industrie geworden. Een verkeerde aanpak in het ontwerp of tijdens de realisatie of in het onderhoud, allemaal ten gevolge van verkeerd inzicht, onzorgvuldigheid of incompetentie. Of, kan het erger, vanwege de eenvoud het ene gat met het andere proberen te dichten. Ik hield mijn studenten altijd voor: *"bij elke maatregel moet je bedenken welke kwetsbaarheid je introduceert"*. Dan is er wel enige gelijkenis met onze nationale held Hansje Brinkers. Natuurlijk, ook ik begrijp dat honderd procent veilig een utopie is, maar ik zou graag zien dat we de manier waarop we systemen ontwerpen en ontwikkelen nu eens echt gaan aanpakken.

**"Security := a functional"**. Dus vanaf het eerste begin de security eisen meenemen en tot aan het einde van de levenscyclus aanhouden. Eisen vanuit de wetgever (EU's Cyber Security Resilience Act) komt eraan, al duurt het nog wel even voor deze er is), eisen vanuit de afnemer (Software Bill of Materials, SBOM), eisen vanuit competenties (security een verplicht onderdeel maken binnen alle IT-gerelateerde opleidingen). Dat zijn de stappen waarvan ik hoop dat we die in 2023 kunnen gaan maken om zo onze werklust terug te kunnen dringen. Ik bezocht onlangs de voorstelling *De mens en ik* van Tim Franssen. Twee van zijn uitspraken zetten aan tot denken en bieden een goede leidraad om in de toekomst al die excuses te voorkomen en ook onze security lasten te verlichten: *"we worden meer bepaald door onze gebreken dan door onze prestaties"* en *"onze kennis is onze wijsheid voorbijgestreefd"*.

## Referenties

- (1) [https://tweakers.net/nieuws/204138/nederland-krijgt-een-paspoort-voor-op-internet-hoe-gaat-dat-werken.html?utm\\_source=nieuwsbrief&utm\\_medium=email&utm\\_campaign=twk\\_nieuwsbrief](https://tweakers.net/nieuws/204138/nederland-krijgt-een-paspoort-voor-op-internet-hoe-gaat-dat-werken.html?utm_source=nieuwsbrief&utm_medium=email&utm_campaign=twk_nieuwsbrief)
- (2) <https://www.onderzoeksraad.nl/page/21847/aanpak-cybersecurity-heeft-versnelling-nodig> - 13.12.2022
- (3) <https://softwareveiligheid.onderzoeksraad.nl/> - december 2021
- (4) "Met een SSI behoudt de gebruiker regie over zijn eigen data" IB-4.2020 pagina 46 t/m48 alsook "Volledige controle over je persoonsgegevens met SSI" IB-5.2020 pagina 52 t/m 54
- (5) [https://tweakers.net/nieuws/204566/edpb-eu-lidstaten-overtreden-europees-recht-met-verwerking-passagiersgegevens.html?utm\\_source=nieuwsbrief&utm\\_medium=email&utm\\_campaign=twk\\_nieuwsbrief](https://tweakers.net/nieuws/204566/edpb-eu-lidstaten-overtreden-europees-recht-met-verwerking-passagiersgegevens.html?utm_source=nieuwsbrief&utm_medium=email&utm_campaign=twk_nieuwsbrief)
- (6) [https://tweakers.net/nieuws/204544/microsoft-laet-europeanen-vanaf-januari-kiezen-of-ze-data-in-eu-willen-opslaan.html?utm\\_source=nieuwsbrief&utm\\_medium=email&utm\\_campaign=twk\\_nieuwsbrief](https://tweakers.net/nieuws/204544/microsoft-laet-europeanen-vanaf-januari-kiezen-of-ze-data-in-eu-willen-opslaan.html?utm_source=nieuwsbrief&utm_medium=email&utm_campaign=twk_nieuwsbrief)
- (7) Auteur: van Enith Vlooswijk d.d. 16.12.2022 - [https://www.nemokennislink.nl/publicaties/bescherming-of-bedreiging/?news\\_letter=true&utm\\_medium=email&utm\\_campaign=NEMO%252](https://www.nemokennislink.nl/publicaties/bescherming-of-bedreiging/?news_letter=true&utm_medium=email&utm_campaign=NEMO%252)
- (8) Tweakersnet d.d. 16.12.2022 - [https://tweakers.net/nieuws/204604/irma-ontwikkelaar-sidn-neemt-deel-aan-eu-pilot-voor-digitale-identiteitswallet.html?utm\\_source=nieuwsbrief&utm\\_medium=email&utm\\_campaign=twk\\_nieuwsbrief](https://tweakers.net/nieuws/204604/irma-ontwikkelaar-sidn-neemt-deel-aan-eu-pilot-voor-digitale-identiteitswallet.html?utm_source=nieuwsbrief&utm_medium=email&utm_campaign=twk_nieuwsbrief)



# Hoe stuur jij op security in de board room?


Kijk op [cisomasterclass.nl](http://cisomasterclass.nl) om uit te vinden hoe je daar grip op krijgt en schrijf je in voor de masterclass op 12, 13 en 14 april 2023.

Kennis brengt je naar de top, skills zetten je aan het stuur!



 [www.cisomasterclass.nl](http://www.cisomasterclass.nl)

 [info@cisomasterclass.nl](mailto:info@cisomasterclass.nl)

 079-360 4268



## COLOFON

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

### HOOFDREDACTEUR

Chris de Vries

### REDACTIE

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

### BLADMANAGEMENT

MOS bv  
Caroline Knobbe  
Sam Dekkers  
E [ibmagazine@pvib.nl](mailto:ibmagazine@pvib.nl)

### ADVERTENTIE-ACQUISITIE

MOS bv  
Eric Noordam  
E [acquisitie@mos-net.nl](mailto:acquisitie@mos-net.nl)  
T 033 247 34 00

### VORMGEVING

Neverseen Art & Design  
Dimitri van den Berg

### DRUK

Veldhuis Media, Meppel

### UITGEVER

Platform voor InformatieBeveiliging (PvIB)  
Postbus 1058  
3860 BB NIJKERK  
T (033) 247 34 92  
E [secretariaat@pvib.nl](mailto:secretariaat@pvib.nl)  
W [www.pvib.nl](http://www.pvib.nl)

### ABONNEMENTEN

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

### ABONNEMENTENADMINISTRATIE

Platform voor InformatieBeveiliging (PvIB)  
Postbus 1058  
3860 BB NIJKERK  
E [secretariaat@pvib.nl](mailto:secretariaat@pvib.nl)



Tenzij anders vermeld valt de inhoud van dit tijdschrift onder een Creative Commons Naamsvermelding-gelijkeDelen 3.0 Nederland Licentie (CC BY-SA 3.0)  
ISSN 1569-1063



Ontdek

# PRISM

Hét platform voor  
Privacy Information & Security Medewerkers

- Netwerken met vakgenoten
- Audittrail helpdesk
- Sjablonenbibliotheek
- Trainingen & webinars



**SECURITY**  
ACADEMY

**ISACA**  
Accredited Training Partner

## Certified Data Privacy Solutions Engineer CDPSE Preparation Course

Valideer je expertise.  
Boost je IT Profiel.

Je vind de opleiding op:  
[www.securityacademy.nl](http://www.securityacademy.nl)







# TSTC

## ICT en Security Trainingen

### Ransomware? Log4j?

### ADVANCE YOUR CAREER WITH SECURITY IN 2023

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

**GET SKILLED**  
**WWW.TSTC.NL**



*Want security start bij mensen!!*

#### TECHNICAL SECURITY TRAININGEN

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

#### SECURITY MANAGEMENT TRAININGEN

- CISSP** - Certified Information Systems Security Professional
- CISM** - Certified Information Security Manager
- CISA** - Certified Information Systems Auditor
- CRISC** - Certified In Risk And Information Systems Control
- CJCSO** - 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](http://www.tstc.nl)

**Onze trainingen zijn weer klassikaal of Live Online te volgen**