

Thema: onderwijs, onderzoek en ontwikkeling

- ◆ Digitale druk op de jonge schouders
- ◆ Quantum Security: van hype naar realiteit
- ◆ Waarom mkb-ondernemers niet investeren in cyberweerbaarheid



Recht in de doelgroep

100% veilig. 0% spam.

Uw merk, product of dienst onder de aandacht brengen bij dé professionals in de intersectorale branche?

IB-Magazine is hét betrouwbare platform met een sterke, betrokken lezerskring. Geen ruis, geen verspilling — alleen zichtbaarheid waar het telt.

Meer weten?

Mail naar ibmagazine@pvib.nl

AI: Artificiële Intelligentie of Afnemende Intelligentie? Of waar staat onze lezer?



Chris de Vries

De hoogleraar klinische neuropsychologie (VU-Amsterdam), Erik Scherder, zal velen bekend zijn. In de eerste plaats door zijn boeken en daarnaast zijn van tijd tot tijd optreden op de televisie. In zijn meest recente boek: "Liever moe dan lui", breekt hij een lans voor het blijven denken. Denken ziet hij als een spier en net als bij topsport moet je spieren blijven oefenen. Dus blijf "moe worden" door mentaal en fysiek de uitdagingen te zoeken en die zit niet in de AI, indien die alleen ingezet wordt om: het eigen denken, toetsen, afwegen en standpunten innemen, over te laten aan een programma.

Zelf ben ik, gisteren, bezig geweest met Claude (van Anthropic). Ik wilde nagaan wat AI van mijn macro-economische verkenning over de periode 2006 t/m 2025 zou maken. En dat was zowel indrukwekkend als teleurstellend.

Indrukwekkend, omdat Claude mij oplossingen aanbood waaraan ik niet gedacht had, teleurstellend dat ik Claude – naar ik aanneem op basis van mijn heldere instructies – niet ertoe kon verleiden een correcte 'outside-inside' waardering voor een confrontatiematrix te laten maken.

Wat het mij dus leerde is dat ik, als mens, nog steeds mijzelf "moe moet maken". Natuurlijk zal een AI leren om betere resultaten tot stand te brengen, echter net als de computer blijft AI een 'black box' en die moet je per definitie niet blind vertrouwen.

En wat heeft dat bovenstaande te maken met onze huidige uitgave van InformatieBeveiliging Magazine? Veel, want in dit nummer zeer gevarieerde artikelen over: ChatGPT 's "muffins & malware" via Quantum Security 's "van hype tot realiteit" alsook "waarde toevoeging door samenwerken" naast "cyberweerbaarheid bij de MKB'er".

En dan zijn wij er nog niet, want het interview van onze redacteur Marcel over "Hackers met een missie (DIVD)", het thema: "duurzame gedragsverandering", gekoppeld aan deel 2 van Inge Wetzer's artikel: "Baat het niet dan schaad het wel ..." en dan specifiek "waar je moet beginnen met gedragsverandering" en "de CISO als bruggenbouwer" zal menigeen intrigeren zo niet boeien, dan toch vermoeien. En daarmee is nog niet eens alles benoemd, wat - net als een AI-tool - onverwacht uit onze magische hoed komt.

Dus ook wij sporen de lezers aan: "Word moe, lees wat de auteurs voor jullie opgesteld hebben en train die hersenen, die met hun ongebruikte cellen, elk AI-systeem doet blozen vanwege diens (AI dus!) gebrek aan intelligentie, inlevingsvermogen en fantasie.

En ... laat eens horen - via onze website, nieuwsbrief of LinkedIn - wat jullie hebben gevonden en waar jullie staan in de wereld van AI. Wij zijn benieuwd hoe vermoeid jullie daarna zijn.

Chris

IN DIT NUMMER

- 03 Voorwoord en inhoudsopgave
- 04 Een jaar verder in ontwikkeling
- 06 Digitale druk op de jonge schouders
- 09 Van muffins naar malware: hoe ChatGPT digitale dreiging industrialiseert
- 10 Towards a Blueprint for Maritime Port Cyber Resilience
- 16 Quantum Security: van hype naar realiteit
- 18 Dutch Institute for Vulnerability Disclosure

- 22 Samen op weg naar duurzame gedragsverandering
- 26 Managing Shadow IT: From Bans to Benefits
- 29 Vertrouwen in het Onzichtbare
- 30 Waarom mkb-ondernemers niet investeren in cyberweerbaarheid
- 34 De CISO als bruggenbouwer
- 36 Baat het niet dan schaad het wel...
Waar begin je dan wél met gedragsverandering?
- 40 1 + 1 = 3 / Samenwerken moet waarde toevoegen

Een jaar verder in ontwikkeling

Vorig jaar brachten we als IB-Magazine (IB.3) het themanummer "Onderwijs, onderzoek en ontwikkeling" uit. Met, naar mijn idee, een enorme diversiteit aan onderwerpen vanuit de onderzoekswereld en het onderwijs. In dit artikel blik ik terug op een aantal bijdragen uit het themanummer van vorig jaar en geef ik een voorproefje van wat u in dit nummer (IB.5) kunt verwachten.

Kennisnet

Het artikel van Kennisnet - namens het primair en voortgezet onderwijs - ging vorig jaar over "Veilig digitaal onderwijs". Hierbij werd een normenkader geïntroduceerd waarmee schoolorganisaties veilig digitaal onderwijs kunnen borgen. Dit jaar gaat het over de hulpmiddelen die Kennisnet aan het PO en VO levert. Mooi om te zien dat het onderwijzend personeel nu beter ondersteund wordt om niet alleen de mogelijkheden, maar ook de risico's van nieuwe technologie inhoudelijk te bespreken.

AD's

In een ander artikel ging het over nieuwe Associate Degrees. HBO-opleidingen van 2 jaar op het gebied van Cyber- en Information security. Ik was benieuwd naar de acceptatie van dit nieuwe, toegevoegde niveau in de beroepspraktijk. Dat leverde helaas geen volledig artikel op, maar wel de volgende status (juni 2025): "We zien, bij deeltijdstudenten, dat zij beginnen vanuit een beheer-, servicedeskfunctie en tijdens of net na de opleiding doorgroeien naar information security-achtige taken.



Bij de voltijdopleiding zijn er nog geen afstudeerders. Tijdens de opleiding gaan ze wel aan de slag met opdrachten die ze voor een echte opdrachtgever uitvoeren, zoals social-engineering opdrachten awarenesstrainingen opstellen en risico-/gap-analyse uitvoeren (in beperkte scope) op basis van de ISO 27001." Het lijkt me waardevol om daar volgend jaar opnieuw een artikel aan te wijden: hoe manifesteren deze verschillende opleidingsniveaus zich in de beroepspraktijk, en hoe verhouden ze zich tot elkaar?

Lectoraten

Vorig - en dit jaar, zelfs meerdere bijdragen vanuit lectoraten van verschillende Hogescholen. Het mooie van het soort onderzoek dat daar wordt gedaan, is de praktische waarde. Veelal kunnen de onderzoeksresultaten leiden tot een toepassing in de praktijk. Mooie resultaten voor de onderzoekers, daaraan gerelateerde relevante alsook leuke onderwijs-onderzoeksopdrachten voor de studenten en prima resultaten voor de beroepsgroep en het bedrijfsleven. Dit keer Shadow IT, Cyberweerbaarheid bij MKB'ers en een blueprint voor cybersecurity in de havens. Met zoveel lectoraten en zoveel productie kunnen we in elk nummer van IB-Magazine wel een artikel gaan opnemen, "auteurs: zie het als een mogelijkheid!"

SURF

Een bijdrage van SURF kan en mag in een dergelijk thema-nummer natuurlijk niet ontbreken. De instantie die op het vlak van cybersecurity voor het onderwijs- en onderzoeksveld van grote betekenis is. Ook deze keer weer aandacht voor de menselijke factor. In een onderzoek - uitgevoerd samen met verschillende universiteiten en hogescholen - is men via het COM-B-model gekomen tot een nieuw procesmodel voor gedragsverandering. Dat werd tot nu toe vaak onder de noemer 'awareness' geschaard, maar dit model gaat duidelijk verder. Het gaat om daadwerkelijk te realiseren gedragsverandering bij mensen (docenten, onderzoekers en wetenschappers). Dat vermoeden hadden we al, maar het is nu ook wetenschappelijk onderbouwd en er komen tools om het mogelijk te maken.

C-SIDE

Vanwege de beperkte ruimte kan ik hier niet gaan reflecteren op alle artikelen van vorig jaar, maar ééntje wil ik er, ook vanuit persoonlijke interesse, nog wel even uitlechten. Dat is het artikel over C-Side. Het onderzoek dat door de Universiteit Leiden is gestart naar secure software development. Ik denk dat het heel relevant kan worden in het kader de compliance eisen vanuit de

CRA. De Cyber Security Resilience Act, waarbij "producten met digitale elementen die op de EU-markt worden gebracht, minder kwetsbaarheden vertonen en fabrikanten verantwoordelijk blijven voor cyberbeveiliging gedurende de hele levenscyclus van een product". Helaas is de auteur van het vorig jaar gepubliceerde artikel overgestapt naar een andere universiteit en is dus ook uit dit onderzoek gestapt. Er was geen vervanger/opvolger voor het vervolgartikel voorhanden, maar het onderzoek is wel verder voortgezet. Op de site van de het NWO (<https://www.nwo.nl/projecten/nwa121518008>) is de status van dit onderzoek terug te vinden en ik kom daar verschillende publicaties tegen, die in het kader van het onderzoek inmiddels zijn verschenen. Hierbij een korte update over de huidige stand van zaken:

Het onderzoek introduceert een omvattend raamwerk om de beveiliging van softwaresystemen te evalueren en te meten. Het framework wil bestaande benaderingen verrijken en verbeteren door een gestructureerde aanpak. Het raamwerk wordt opgezet als een evaluatiestructuur die drie centrale elementen combineert:

- **Security doelen** – wat moet beschermd worden?
- **Evaluatiecriteria** – hoe meet je of dat goed gebeurt?
- **Contextuele factoren** – zoals softwaretype, gebruiksscenario, en risicoprofiel.

Het raamwerk is bedoeld als flexibele tool voor ontwikkelaars, onderzoekers en beleidsmakers om de effectiviteit van software-beveiliging systematisch te analyseren en te verbeteren.

Het voorgestelde Software Security Evaluation Framework van het C-Side project combineert beveiligingsdoelen, evaluatiecriteria en contextfactoren tot een modulair model. Het raamwerk is ontworpen om zowel bestaande evaluatiestructuren te ondersteunen als gaten in huidig beleid en praktijk bloot te leggen. Het is toepasbaar op verschillende soorten software, en bevordert een systematische aanpak om zwakke plekken vroegtijdig te signaleren en gericht te verbeteren.

Het eindrapport wordt in 2026 verwacht. Ik ben erg benieuwd naar het resultaat, en ga ervan uit dat we er dan opnieuw aandacht aan besteden in dit magazine.

Wij schotelen u opnieuw een veelzijdig en lezenswaardig thema-nummer voor over onderwijs, onderzoek en ontwikkeling, met ook nog artikelen over DIVD, de CISO masterclass en niet te vergeten de vertrouwde columns.

Digitale druk op de jonge schouders

Het onderwijs staat er niet alleen voor

Digitalisering is inmiddels gemeengoed in het onderwijs. Scholen gebruiken digitale leermiddelen, smartboards en nemen regelmatig toetsen digitaal af. Sinds de komst van AI versnelt die ontwikkeling zichtbaar. Maar naast alle kansen, brengt digitalisering ook nieuwe risico's met zich mee – zoals het ongezien en ongeregeerd gebruik van AI bij schoolopdrachten, sociale onveiligheid via smartphones of het lekken van leerlinggegevens door gebrekkige beveiliging. Die risico's raken het onderwijs en roepen vooral de vraag op hoe we leerlingen daartegen beschermen – zowel in hun digitale gedrag als in de bescherming van hun gegevens.



Juist daarom moeten scholen investeren in digitaal veilig onderwijs, met aandacht voor het bewust en verantwoord leren omgaan met technologie. Dat is geen eenvoudige opgave: digitale veiligheid raakt veel verschillende thema's tegelijk, van gedrag tot beleid en techniek. Als elke school het wiel zelf moet uitvinden, kost dat niet alleen tijd en energie, maar leidt het ook tot versnippering en ongelijkheid.

Dat vraagt om samenwerking tussen scholen, sectororganisaties en leveranciers. Kennisnet helpt scholen hierbij met concrete hulpmiddelen, advies en diensten voor het onderwijs, zodat geen enkele school er alleen voor staat.

Kennisnet is de publieke organisatie voor onderwijs en ICT. We zijn een stichting zonder winstoogmerk en worden volledig gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW). We ondersteunen scholen in het funderend onderwijs met kennis, visie en praktische oplossingen op het gebied van digitalisering. Daarbij werken we samen met scholen, sectororganisaties en leveranciers aan veilig, betrouwbaar en toegankelijk digitaal onderwijs.

Leerlingen zijn jong en extra kwetsbaar

Leerlingen groeien op in een digitale wereld, maar kunnen nog niet altijd overzien wat veilig of verstandig is. Ze zijn daardoor extra kwetsbaar voor digitale risico's. Daarom is aandacht voor digitale geletterdheid essentieel. Digitale geletterdheid is het geheel van kennis en vaardigheden waarmee leerlingen zich bewust, kritisch en actief kunnen bewegen in een wereld vol digitale technologie. Kennisnet biedt scholen praktische hulpmiddelen om leerlingen hierin te begeleiden.

Zo laten we in het artikel 'Tips voor bigtech-alternatieven in je onderwijs over digitale geletterdheid' (1) zien, hoe je leerlingen bewust maakt van alternatieven voor dominante techbedrijven. Bijvoorbeeld door niet de standaard zoekmachine te gebruiken van een Chromeboek, maar door hen kennis te laten maken met privacy vriendelijke zoekmachines zoals DuckDuckGo of Ecosia. Zo leren ze dat er ook andere keuzes zijn.

En door gebruik te maken van bewustmakende lespakketten zoals 'De baas op internet' (2), die gericht zijn op bewustwording over internetgebruik voor kinderen van 10 tot 14 jaar, ontwikkelen ze een breder en kritischer perspectief op technologie.

Nieuwe technologie verbieden helpt niet

Experimenteren met technologie hoort bij goed onderwijs, maar vraagt om bewust handelen. Door te experimenteren ontdekken

scholen wat wel en niet werkt, onder welke condities en wat leerlingen én leraren nodig hebben om technologie verantwoord in te zetten. Kennisnet ondersteunt dit proces met hulpmiddelen zoals de Techwijzer (3) en de handreiking 'Hoe experimenteer je met innovatieve technologie in het onderwijs' (4). Daarmee helpen we scholen om technologie op een doordachte en veilige manier in te passen in het onderwijs – want verbieden werkt niet altijd.

AI is daar een treffend voorbeeld van: het is niet meer weg te denken uit het onderwijs. Juist daarom is het belangrijk om leerlingen hierin te begeleiden en te beschermen. Uit onderzoek van NOS Stories (5) onder 1.300 middelbare scholieren blijkt namelijk dat het merendeel AI gebruikt bij het maken van schoolopdrachten. Het verbieden van nieuwe technologie werkt dan ook niet. In plaats daarvan is het belangrijk om met leerlingen in gesprek te gaan over verantwoord gebruik. Ofwel: AI-geletterdheid. Dat is ook wat er vanuit de AI-act wordt verwacht bij gebruik van AI binnen een school. In het nieuwsbericht 'Hoe bereid je je als school voor op AI-geletterdheid?' (6) wordt uitgelegd wat dat in de praktijk betekent en welke raakvlakken het heeft met ICT-bekwaamheid en digitale geletterdheid.

Om AI op een veilige en verantwoorde wijze in te zetten, is het belangrijk dat er schoolafspraken zijn over het gebruik van generatieve AI. Om scholen hierbij te helpen, zijn in het artikel 'Schoolafspraken over het gebruik van generatieve AI (7)' zeven principes beschreven. Zo benadrukken deze afspraken het belang van transparantie over het gebruik van AI, het ontwikkelen van een gedeeld begrippenkader en het maken van keuzes over de rol van AI bij het leren. Ook privacy komt expliciet aan bod: een van de principes luidt 'bescherm je eigen privacy en die van anderen', met als voorbeeldafpraak: "voer geen persoonsgegevens in". Met hulpmiddelen, zoals een voorbeeldpresentatie, werkblad en voorbeeldbrief voor ouders worden scholen geholpen om AI-gebruik in goede banen te leiden en bewustwording bij leerlingen en leraren te vergroten.

Gebruik van smartphones niet meer toegestaan

Steeds meer kinderen hebben een smartphone. In de klas leidt dat vaak tot afleiding, onrust of zelfs onveilige situaties – zoals het stiekem filmen van klasgenoten.

Sinds 2024 is het gebruik van smartphones in de klas niet meer toegestaan. Dit is afgesproken in een hoofdlijnenakkoord tussen OCW en organisaties van leerlingen, ouders, leraren en schoolbestuurders. Scholen moeten zelf bepalen hoe zij dit akkoord vormgeven.

Hoewel de afspraak bedoeld is om rust en focus te bevorderen, kan het volledig weren van smartphones ook nadelig zijn voor het leren en ontwikkelen van digitale vaardigheden. Daarom is maatwerk nodig. 'One size fits all' bestaat niet. Een 'nee, tenzij'-benadering wordt aanbevolen: geen smartphonegebruik, tenzij dit noodzakelijk is voor het leren of vanwege een beperking of medische reden. De publi-

catie 'Schoolbeleid voor smartphones' (8) ondersteunt scholen bij het ontwikkelen van een gedragen beleid. Met praktijkvoorbeelden, onderzoek én een stappenplan. Een waardevolle tip daaruit: koppel het smartphonebeleid aan het bredere sociale veiligheidsbeleid van de school. Zo ontstaat samenhang tussen regels, begeleiding en schoolcultuur. Op kennisnet.nl delen we ook praktijkvoorbeelden van scholen die hiermee aan de slag zijn gegaan. Zo laat een schoolbestuur zien dat duidelijke routines helpen: leerlingen leggen daar bij aankomst hun telefoon in de kluis. Dat zorgt voor rust, voorkomt discussie en maakt het beleid zichtbaar en werkbaar in de schoolpraktijk.

Brede aandacht nodig voor digitale veiligheid

De risico's die in de klas ontstaan door technologiegebruik, zoals afleiding, ongewenst AI-gebruik of onveilig smartphonegebruik, raken niet alleen de directe onderwijspraktijk. Door de toegenomen inzet van digitalisering is het onderwijs steeds afhankelijker geworden van digitale middelen. Een verstoring kan het lesproces flink onderbreken en een datalek kan grote impact hebben op leerlingen. Daarom is er, naast aandacht voor concrete risico's in het klaslokaal, ook bredere aandacht nodig voor informatiebeveiliging en privacy.

Scholen missen vaak tijd, kennis of richting

Veel scholen willen aan de slag met digitale veiligheid, maar weten niet goed waar ze moeten beginnen. Door tijdgebrek of gebrek aan overzicht blijven maatregelen liggen. Met het Groeipad (9) - een praktische wegwijzer in de vorm van een website - worden scholen geholpen om digitale veiligheid stapsgewijs te verbeteren. Het bestaat uit vijf fasen waarin je werkt aan deelprojecten met normen die logisch bij elkaar horen en gezamenlijk kunnen worden opgepakt. In de eerste fase leg je het fundament, bijvoorbeeld door het vormen van een IBP-team (InformatieBeveiliging en Privacy), het opstellen van beleid en het in kaart brengen van systemen en hardware. In de fasen daarna bouw je verder aan structurele borging van informatiebeveiliging en privacy. Bij elk deelproject vinden scholen uitleg, een stappenplan en voorbeeldmaterialen. Zo groeit digitale veiligheid mee met de ontwikkeling van de school.

Zo geven scholen invulling aan het Normenkader IBP (10), dat we als onderwijssector hebben vastgesteld. Het bevat 69 normen voor informatiebeveiliging en 25 normen voor privacy. Deze normen geven inzicht in de maatregelen die nodig zijn voor een zo goed mogelijke bescherming tegen digitale dreigingen en privacy risico's. Ondanks alle voorbereidingen kan een school te maken krijgen met een grootschalig cybersecurity-incident of zoals een datalek of ransomware aanval. In zulke situaties biedt School-CERT (11) ondersteuning: een meldpunt dat scholen helpt met duiding, begeleiding en praktische opvolging van digitale veiligheidsincidenten.

School-CERT adviseert bij het inschatten van de ernst van het incident, het bepalen van vervolgstappen en de communicatie met betrokkenen. Ook adviseert School-CERT over meldingen aan de Autoriteit Persoonsgegevens, indien nodig. In geval van betrokkenheid van leveranciers wordt samengewerkt met SIVON, die het contact onderhoudt met deze partijen namens het onderwijs. Daarnaast publiceert School-CERT dreigingsinformatie, zoals maandoverzichten, kwartaalanalyses, sector alerts en handreikingen. Ook informeert het scholen en besturen over kwetsbaarheden die door derden zijn ontdekt, zodat zij gericht actie kunnen ondernemen. School-CERT is ontstaan vanuit het Programma Digitaal Veilig Onderwijs (DVO), een samenwerking van Kennisnet, SIVON, de PO-Raad, de VO-raad en het ministerie van OCW om scholen weerbaarder te maken tegen digitale dreigingen. Vanuit dit programma zijn verschillende diensten ontwikkeld die scholen ondersteunen op het gebied van informatiebeveiliging en privacy. School-CERT wordt door Kennisnet geleverd aan het funderend onderwijs. Schoolbesturen binnen het bekostigd funderend onderwijs kunnen zich gratis aanmelden via www.schoolcert.nl

Gezamenlijke verantwoordelijkheid

Digitale veiligheid vraagt om meer dan alleen techniek of regels: het vraagt om samenwerking, bewustwording en gedeelde verantwoordelijkheid. Scholen staan daarin niet alleen. Kennisnet ondersteunt daarbij. Laat dit artikel inspiratie zijn zelf stappen te zetten of bestaande aanpakken te versterken. Wil je een voorbeeld nader bekijken of ben je benieuwd naar andere praktijkverhalen? Kijk op kennisnet.nl of neem gerust contact met mij op.

Referenties

- (1) <https://www.kennisnet.nl/digitale-geletterdheid/tips-voor-bigtech-alternatieven-in-je-onderwijs-over-digitale-geletterdheid/>
- (2) <https://debaasopinternet.nl/>
- (3) <https://www.kennisnet.nl/technologische-innovatie/techwijzer/>
- (4) <https://www.kennisnet.nl/technologische-innovatie/hoer-experimenteer-je-met-innovatieve-technologie-in-het-onderwijs/>
- (5) <https://nos.nl/artikel/2562959-middelbare-scholen-passen-schoolopdrachten-aan-om-ai-gebruik-tegen-te-gaan>
- (6) <https://www.kennisnet.nl/nieuws/hoer-bereid-je-je-als-school-voor-op-ai-geletterdheid/>
- (7) <https://www.kennisnet.nl/artificial-intelligence/schoolafspraken-over-het-gebruik-van-generatieve-ai/>
- (8) <https://www.kennisnet.nl/app/uploads/Schoolbeleid-voor-smartphones.pdf>
- (9) <https://normenkaderibp.kennisnet.nl/groeipad/>
- (10) <https://normenkaderibp.kennisnet.nl/informatiebeveiliging/>
- (11) <https://www.kennisnet.nl/diensten/school-cert/>



Van muffins naar malware: hoe ChatGPT digitale dreiging industrialiseert

Ergens tussen het genereren van recepten voor glutenvrije muffins en het uitleggen van quantumfysica aan achtjarigen, werd ChatGPT ingezet voor staatspropaganda, malwareontwikkeling en Noord-Koreaanse sollicitatiebrieven.

Volgens het rapport van OpenAI, *Disrupting Malicious Uses of AI*, zijn verschillende staten en criminele netwerken erin geslaagd deze AI-modellen voor schadelijke doeleinden aan te wenden. ChatGPT is niet defect, maar een instrument dat zich naadloos aanpast aan zijn gebruiker — of die nu een frauduleus cv nodig heeft of een geautomatiseerde phishingcampagne. De technologie blijkt een krachtig middel in handen van kwaadwillenden: razendsnel, vrijwel foutloos en zonder moreel filter genereert het wat er gevraagd wordt.

In Rusland werd geen grootschalige aanval uitgevoerd, maar een geraffineerde, stapsgewijze aanpak gevolgd. Via tijdelijke accounts werd in losse onderdelen malware gebouwd — poortscans, Telegram-notificaties, credential dumping. De uiteindelijke code, ScopeCreep, had een bescheiden impact, maar het ontwikkelproces was tekenend voor deze tijd: AI als digitale handleiding voor cyberdreiging. Niet innovatief, maar wel schaalbaar, onderhoudbaar en herhaalbaar. De actoren gebruikten ChatGPT slechts eenmaal per account, wat hielp om onopgemerkt te blijven. De vergelijking met Lego ligt voor de hand: zoals een kind met duizenden blokjes een bouwwerk maakt, bouwen cybercriminelen met ChatGPT aan aanvallen — stap voor stap, zonder dat de volledige constructie ooit zichtbaar wordt.

In Noord-Korea zagen we een ander soort misbruik. Daar werden geen exploits gebouwd, maar arbeidsprofielen — compleet met cv's, motivatiebrieven, projectvoorbeelden en gescripte sollicitatie-antwoorden. In plaats van netwerken binnen te dringen, probeerden 'medewerkers' bedrijven binnen te komen via sollicitatieprocedures. Met behulp van prompts automatiseerden ze het aannemen van valse identiteiten, het volgen van vacatures, het organiseren van remote werk en zelfs het verzenden van hardware naar Amerikaanse adressen. ChatGPT werd zo medewerker, recruiter én loopbaanadviseur tegelijk — in dienst van een staatseconomie die draait op misleiding.

Ook China maakte gebruik van het model, in dit geval voor socialemediamanipulatie. Actoren genereerden reacties op geopolitieke onderwerpen — van Taiwan tot USAID — en verspreidden deze via TikTok, Reddit en Facebook. De inhoud was weinig subtiel, maar het proces bleek geautomatiseerd, schaalbaar en grensoverschrijdend in taal. Ideaal om de informatieruimte te overspoelen met strategisch rumoer.

Maar het grimmigste voorbeeld kwam uit Cambodja, waar criminele netwerken ChatGPT gebruikten om wervingsadvertenties te schrijven in Swahili, Kinyarwanda en Haïtiaans Creools. De advertenties waren bedoeld om mensen te lokken naar zogenaamde scam-compounds: afgesloten complexen waar slachtoffers onder dwang onlinefraude plegen. De teksten waren niet foutloos, maar overtuigend genoeg om hoop op een beter leven te verkopen.

OpenAI heeft inmiddels accounts geblokkeerd en indicatoren gedeeld, maar het bredere beeld blijft hardnekkig: we zien geen hackers meer achter groene tekst op zwarte schermen, maar operatoren die prompts testen, vertalen en opschalen. De dreiging is niet technischer geworden, maar industriëler. ChatGPT is het Zwitserse zakmes van digitale misleiding geworden — eindelijk herbruikbaar, onvermoeibaar efficiënt en altijd beschikbaar.

Wat ooit afhankelijk was van kunde, is nu afhankelijk van intentie. En die intentie wordt zelden tegengehouden door een keurig geformuleerde disclaimer aan het begin van een chatsessie.

"Waarmee kan ik je vandaag van dienst zijn?"

Dr. Nicole van der Meulen is expert op het gebied van cybersecurity en emerging technologies en werkzaam bij SURF als Cybersecurity Innovation Lead, ns.vandermeulen@gmail.com

Towards a Blueprint for Maritime Port Cyber Resilience

Integrating Strategic and Operational Risk Management

Seaports are critical infrastructures that serve as essential nodes in global supply chains. Their functioning affects national economies, international trade and societal well-being. In the EU, ports support 90% of exports and 43% of internal market exchange. These facilities, by connecting sea and inland transport, are the arteries of modern commerce. As digitalization in logistics and port operations accelerates, these hubs have become increasingly vulnerable to cyber threats.



Maritime supply chain

Cyber resilience in the maritime supply chain has become a paramount concern. The increasingly interconnected nature of port operations means that the digital compromise of a single entity—be it a customs authority, cargo handler, IT vendor or shipping line—can trigger cascading failures. Unlike traditional security, cyber risk introduces new challenges for port operators: fragmented governance, lack of internal expertise and widely varying security capabilities across stakeholders. Also, there is limited understanding on how supply chains operate and lack of security knowledge.

To address these complexities, several collaborative frameworks have emerged. One notable example is the Cyber Strategie Nederlandse Zeehavens, a joint initiative from the Dutch government and port stakeholders. This strategy led to the formation of FERM, a partnership aimed at enhancing the cybersecurity resilience of the five national seaports in the Netherlands: Port of Rotterdam, Port of Amsterdam, Port of Moerdijk, Groningen Seaports, and North Sea Port (Vlissingen, Ghent, and Terneuzen). These initiatives demonstrate a collective recognition of the systemic risks posed by cyber threats.

Efforts by the European Union Agency for Cybersecurity (ENISA) have also played a key role. ENISA's reports on port cybersecurity and supply chain security offer valuable taxonomies, threat models, and recommended practices. However, these documents tend to focus on the strategic level, describing what should be done, but often neglecting the how—the actionable, operational steps necessary for implementation.



Figure 1. Supply Chain Cyber Resilience Strategy

This leaves a significant gap for practitioners operating within the complex and distributed environment of seaports. What is needed is a blueprint that is both strategic and operational—a guide that can be adapted to the realities of port operations and supply chain interdependencies.

To bridge this gap, a qualitative focus group was conducted. This included representatives from all major stakeholders in the seaport process chain, including terminal operators, IT service providers, customs authorities, logistics coordinators and SME partners. Through structured discussion, we captured shared concerns, operational bottlenecks and areas of potential

synergy. These discussions provided the empirical grounding for the four-phase blueprint we propose in this paper, see Figure 1. The paper outlines the application of the ENISA method within the maritime port call process, specifically focusing on the arrival and departure of vessels at the Port of Moerdijk. This chain involves operational interdependencies between the ports of Moerdijk and Rotterdam.

Objectives of the focus group session

- To review the procedural steps involved in the arrival and departure of a vessel at the Port of Moerdijk.
- To identify and map the cybersecurity risks associated with the process of a vessel's arrival and departure at the Port of Moerdijk.
- To gain practical experience with ENISA's risk management toolbox.

Our central research question is: *How can seaports structure their cyber risk management to enhance supply chain resilience?* This paper presents a method informed by both literature and field input, resulting in a four-phase blueprint:

- Supply Chain Risk Management
- Relationship and Contract Management
- Vulnerability Management
- Transparency of Digital Quality

Each phase is discussed in the following sections, alongside supporting context, stakeholder challenges and operational recommendations.

Supply Chain Risk Management

Cyber resilience begins with a thorough understanding of the supply chain ecosystem. Ports are not monolithic entities but are composed of a vast network of actors, each of whom plays a critical role. Mapping the ecosystem-including cargo handlers, customs authorities, IT infrastructure providers, logistics companies and third-party vendors-is the first step.

This involves building an inventory of digital assets, identifying key service interdependencies and understanding how data flows between organizations. It also requires identifying all actors who have access to operational systems or data, whether directly or indirectly. Only with this visibility can cyber risks be effectively assessed.

ENISA's guidance recommends an asset-and-service-based taxonomy to aid in this mapping. By classifying assets according

to their function-such as cargo processing systems, vessel traffic management or administrative tools-organizations can better assess the impact of disruptions. This approach also enables the alignment of cybersecurity investments with business-critical operations.

The interconnectedness of port operations means that an incident affecting a seemingly minor supplier can have ripple effects throughout the system. Therefore, risk assessments must extend beyond the organizational perimeter to include third-party risks. Ports must define and adopt unified risk assessment methods to manage supply chain risks collectively.

Relationship and Contract Management

With the supply chain mapped and risks identified, the next step is to institutionalize security practices through governance mechanisms. This includes relationship management, contract standardization and change control processes.

Seaports often rely on long-term partnerships with service providers, yet many of these agreements lack explicit cybersecurity terms. These agreements are often not described or recorded at all and therefore do not contain any security requirements. Without formalized obligations, it becomes difficult to enforce baseline practices or respond effectively in the event of an incident. To resolve this, contractual agreements must include clauses on incident response coordination, compliance standards, cybersecurity insurance requirements and access controls.

A shift is also needed in the cultural approach to third-party relationships. Instead of treating vendors as external actors, ports should aim to integrate them into joint security frameworks. This involves creating shared incident response protocols, co-developing KPIs and conducting collaborative risk assessments. Furthermore, change management processes must account for the dynamic nature of digital systems. Whether rolling out new software, updating configurations or onboarding new partners, every change introduces potential vulnerabilities. These transitions must be governed by security review processes that are embedded within procurement and operational workflows. ENISA's reports underline the importance of governance structures that include cybersecurity considerations at the highest levels of decision-making. Ports should establish cybersecurity steering groups composed of cross-functional representatives, empowered to enforce policy and monitor performance across the entire supply chain.

Best practices in vulnerability management include penetration testing, threat modelling and red teaming.

Vulnerability Management

The third phase focuses on detecting, managing and mitigating vulnerabilities in a proactive and continuous manner. This is a critical element in ensuring resilience, as even the best governance framework cannot eliminate all risks.

The challenge here lies in the operational complexity of port environments. Many ports operate with legacy OT (Operational Technology) systems that are difficult to update or to secure. These systems are often segmented from IT networks but are still vulnerable to physical and cyber threats. Moreover, these environments are highly dynamic, with equipment and personnel changing regularly.

Best practices in vulnerability management include penetration testing, threat modelling and red teaming. These activities allow organizations to simulate adversarial scenarios, identify gaps in their defences and prioritize remediation. Red teaming, in particular, has proven useful in assessing not only technical vulnerabilities but also weaknesses in human behaviour and process design.

Automated tools for scanning and monitoring are also essential. Ports should deploy tools that can identify unpatched systems, unauthorized devices or misconfigured software in real time. These tools must be configured to avoid disrupting critical operations-especially in OT environments where system downtime can have cascading effects.

Another important element is data sharing. Threat intelligence platforms that enable secure exchange of indicators of compromise (IOCs), tactics and mitigation strategies among trusted partners can enhance collective resilience. However, this requires building a culture of openness and trust, which in turn depends on robust contractual and policy frameworks.

Finally, a structured vulnerability remediation process must be in place. This involves assigning risk owners, defining escalation

paths and tracking closure rates. Such processes should be integrated into organizational workflows to ensure that they are followed consistently.

Transparency of Digital Quality

The final phase in the blueprint involves achieving transparency in the quality and security of digital systems across the port ecosystem. The goal is to move from reactive defence to proactive assurance, where the cybersecurity posture of each component is known, monitored and benchmarked.

This begins with digital audits. All hardware and software systems in the ecosystem-whether developed in-house or procured from vendors-must be subject to cybersecurity assessments. These assessments should evaluate the system's architecture, update frequency, support model, encryption standards and known vulnerabilities.

ENISA suggests using maturity models to facilitate these assessments. These models allow organizations to evaluate their posture along dimensions such as governance, technology, training and incident response. A shared maturity model adopted across port stakeholders enables benchmarking and prioritization of collective investments.

Transparency also involves certification and labelling. Where feasible, ports should require that vendors provide verifiable certifications for their products and services. This could include adherence to ISO/IEC 27001, IEC 62443, or other relevant frameworks. Procurement teams should be trained to evaluate these certifications as part of the acquisition process.

Digital quality transparency must also be communicated clearly across all organizational layers-from boardrooms to dockyards. Staff at all levels should be made aware of the trustworthiness of the tools and systems they use. This fosters a culture of accountability and informed decision-making.

Method: Focus Group Walkthrough of the Shipping Process Cyber Risk Management

To validate and enrich the proposed blueprint, a structured focus group was conducted with representatives from the entire port process chain. The walkthrough involved analysing four critical phases of port operations:

- **Pre-Arrival Coordination:** Activities include advance vessel notifications, berth planning, customs clearance pre-checks and allocation of port services. Digital systems used here involve vessel traffic services, scheduling platforms and customs data hubs.
- **Arrival and Unloading:** This phase covers vessel docking, gangway setup, unloading of cargo, initial inspections and transfer to temporary holding. Here, port OT systems interact with IT networks, making it a hotspot for cyber-physical risk.
- **Inland Transfer and Storage:** Goods are moved via trucks, rail or inland shipping to logistics depots. This step depends heavily on transportation management systems, route optimization algorithms and storage automation.
- **Customs Clearance and Final Delivery:** Cargo is finally processed by customs, matched with digital manifests and released for domestic distribution. This phase involves significant document handling and secure data exchange.

The following participant-roles joined the focus group research session: Director of Firm (Organizer), Professor of Cyber Risk Management (facilitator), CISO Groningen Seaports (Observer), IT Manager Port Authority Moerdijk (Subject-Matter Expert – Moerdijk), CISO, Loodswezen (Subject-Matter Expert – Pilots), Manager Cybersecurity Port of Rotterdam (Subject-Matter Expert – Rotterdam), IT Manager, KRVE Mooring Services (Subject-Matter Expert – KRVE), CISO, Portbase (Subject-Matter Expert – Portbase), Deputy Harbourmaster, Moerdijk Port (Subject-Matter Expert – Moerdijk).

The Participants described cybersecurity practices, vulnerabilities and pain points associated with each phase.

Process Description: Moerdijk Port Perspective

The following steps among others were identified in the vessel call process:

- The vessel's agent submits a pre-arrival notification to Portbase at least 24 hours in advance.

- Portbase disseminates this notification to relevant stakeholders.
- The notification appears in Moerdijk's port systems with an unique identifier.
- Port Authority Moerdijk is now aware of the vessel's imminent arrival.
- The Actual Time of Arrival (ATA) is obtained from Rotterdam.
- Terminal master data updates from Moerdijk are sent back to Portbase.
- Draft data is communicated to Rotterdam to support admission policy decisions.

Identified Concerns and Vulnerabilities

The following Concerns and Vulnerabilities were identified among others.

- **System Dependencies:** the implications of several dependencies warrant examination.
- **Data Integrity:** ensuring consistency and accuracy of data across systems is a major concern.
- **Spoofing and Jamming:** potential threats to signal and system integrity.
- **Incident Coordination:** a lack of predefined response agreements across the chain poses risks.
- **Inter-System Security:** securing interfaces between systems remains a critical issue.

Conceptual and Methodological Reflections

The following conceptual and methodological reflection came forward in the focus group.

- The appropriateness of the term "supply chain" was questioned; alternative conceptual frameworks may be more suitable, e.g. systemic risks or cascading risks.
- While individual stakeholders maintain internal process maps, a unified Concept of Operations (CONOPS) is absent.
- The current methodology emphasizes defining 'what' must be addressed, but lacks guidance on 'how' to implement collaborative chain-wide risk management.

Discussion, conclusion and next steps: Proposed Approach for Chain Cyber Risk Management

One conclusion that was made in the focus group was that in order to enhance collaborative risk management across the maritime chain, a 5 phased approach was recommended by the focus group.

The 5 phases are:

- Foster mutual understanding and trust among stakeholders.
- Conduct joint walkthroughs of the operational chain.
- Share organizational perspectives on the chain.
- Synthesize a shared, comprehensive chain overview.
- Execute a collective risk and threat analysis based on this overview.

The blueprint's phased approach was validated for being both comprehensive and adaptable. Stakeholders expressed interest in adopting a joint maturity assessment model and organizing cross sector workshops to deepen engagement, see: Figure 2. Figure 2 incorporates the 'how to do' aspects with the 'what' aspects that were addressed in the ENISA framework in Figure 1. What is needed is this integration of strategic and operational aspects in supply chain risk management.

The session demonstrated the complexity and interdependence of port call processes, highlighting both operational challenges and cybersecurity risks. The ENISA toolbox with this addition will provide a valuable framework, but additional effort is still needed to integrate risk management practices across stakeholders in a coherent and effective manner.

This study demonstrates that seaports require a structured, collaborative approach to cyber resilience that addresses both strategic and operational challenges. By engaging stakeholders from across the supply chain and combining ENISA's frameworks with field-based validation, we offer a practical blueprint for enhancing cybersecurity in maritime environments.

One other key insight is the importance to come together with the representatives of each of the members of the supply chain. This leads to a more shared understanding; an alignment with regards to cyber risk awareness and management.



Figure 2. Blueprint for Supply Chain Cyber Resilience
Strategy and Operational Risk Management

An additional insight is the vulnerability of SMEs within the supply chain. Addressing this gap should be a top priority in future initiatives. Targeted training, shared services, subsidized assessments and simplified maturity models can help elevate the baseline.

The next steps include conducting a second focus group where organizations will present their cybersecurity risk strategies. Based on these insights, we propose developing a sector-specific cyber maturity toolkit tailored for ports. This toolkit will serve as a benchmarking and improvement instrument, enabling both self-assessment and peer comparison.

Ultimately, cyber resilience is a collective endeavour. By implementing this blueprint, seaports can transform cybersecurity from a compliance exercise into a shared value driver, enabling safer, more efficient and more trustworthy global trade.

References:

- ENISA (2019) Port Cybersecurity
- ENISA (2020) Cyber Risk Management for Ports
- ENISA (2023). Good Practices for Supply Chain Cybersecurity



Quantum Security: van hype naar realiteit

De ontwikkelingen op het gebied van quantumtechnologie, zoals quantumcryptografie en -netwerken, volgen elkaar in hoog tempo op. Waar het quantumdomein de afgelopen jaren vooral de aandacht trok van wetenschappers, visionairs en beleidsmakers, staan nu ook securityprofessionals voor een belangrijke opgave. De beveiliging van netwerken en data tegen toekomstige dreigingen van quantumcomputers – ook wel aangeduid als quantumbeveiliging – wordt steeds urgenter. Met de begrotingsrondes voor 2026 in aantocht is dit hét moment om te starten met een quantum risicoanalyse van kritieke systemen en informatie. De tijd om quantumbeveiliging serieus te integreren in het cybersecuritybeleid is aangebroken.

Wat is quantum computing ook alweer?

De kracht van quantumcomputing ligt in de unieke principes van de kwantummechanica, zoals superpositie en verstrengeling. Waar klassieke computers werken met bits die uitsluitend de waarde 0 of 1 kunnen aannemen, gebruiken quantumcomputers quantumbits, of qubits, die dankzij superpositie gelijktijdig in een combinatie van 0 en 1 kunnen verkeren. Pas wanneer een qubit wordt gemeten, neemt deze één van de klassieke waarden aan. Dit stelt quantumcomputers in staat om bepaalde berekeningen parallel uit te voeren, waar klassieke systemen dat slechts sequentieel kunnen. Als simpel voorbeeld: stel je voor dat je een doolhof probeert op te lossen. Normaal gesproken probeer je elke mogelijke route één voor één totdat je de uitgang vindt. Quantumcomputers kunnen echter alle mogelijke routes tegelijk uitproberen, waardoor de kans dat je meteen de juiste route vindt aanzienlijk groter wordt en de benodigde tijd veel korter is. Bovendien kunnen qubits via verstrengeling zodanig met elkaar verbonden zijn dat de toestand van de ene direct invloed heeft op die van de andere, ongeacht de afstand ertussen. Door

superpositie en verstrengeling te combineren, in combinatie met quantumalgoritmen, kunnen quantumcomputers rekenproblemen oplossen die voor klassieke computers tijdrovend of zelfs onhaalbaar zijn.

Ontwikkelingen in quantumcomputing

Sinds het Amerikaanse National Institute of Standards and Technology (NIST) de vier finalisten voor de standaardisatie van Post-Quantum Cryptografie (PQC) heeft aangekondigd, zijn IT-dienstverleners en cloudproviders begonnen met de implementatie van deze protocollen in hun cryptografische bibliotheken. De huidige focus ligt op experimenteren en testen, voordat deze protocollen breed worden uitgerold in besturingssystemen zoals Windows en Linux.

Tegelijkertijd werkt NIST aan de standaardisatie van aanvullende protocollen, om in de toekomst voldoende diversiteit te kunnen bieden. Dit is van belang, omdat het moeilijk te voorspellen is hoe goed PQC bestand zal zijn tegen toekomstige quantumaanvallen. De huidige generatie quantumcomputers beschikt

Grote afhankelijkheid maakt de EU kwetsbaar voor veiligheids- en privacy risico's.

namelijk nog niet over voldoende rekenkracht om deze algoritmes daadwerkelijk op robuustheid te testen.

Intussen richten technologiebedrijven en onderzoeksinstituten zich op het verbeteren van de hardware, zoals het verminderen van foutgevoeligheid en het opschalen van het aantal qubits op quantumchips. IBM publiceerde onlangs een geüpdatete quantumroadmap, waarin het streeft naar een foutresistente quantumcomputer met 2000 logische qubits en 1 miljard quantumgates tegen het jaar 2033. Dit zou de eerste praktische quantumcomputer kunnen worden die commercieel inzetbaar is, hoewel het op dit moment nog onzeker is of deze ambitie daadwerkelijk gerealiseerd wordt.

Ook andere spelers, zoals Microsoft en Google, investeren volop in de ontwikkeling van krachtigere, betrouwbaardere en efficiëntere quantumcomputers. De technologische wedloop richting een volwaardige quantumcomputer is daarmee nog in volle gang.

Digitale soevereiniteit in het quantumtijdperk

Door de geopolitieke spanningen groeit de roep om Europese, en specifiek Nederlandse, digitale soevereiniteit. TNO waarschuwt dat momenteel bijna 92 % van alle "Westerse" data wordt gehost in de Verenigde Staten, met slechts zo'n 4 % in Europa. Deze grote afhankelijkheid maakt de EU kwetsbaar voor veiligheids- en privacyrisico's.

Dit geldt ook voor quantumtechnologie. Quantumcomputers zijn fysiek geavanceerde systemen die zich in gespecialiseerde, afgeschermd en gekoelde ruimtes bevinden om decoherentie te voorkomen. Daarom worden ze – net als bestaande HPC-systemen – via de cloud aangeboden. Gebruikers schrijven algoritmen lokaal en sturen die via de cloud naar de quantumhardware. De cloud is dus onmisbaar voor toegang tot quantumcomputing.

Europa beschikt inmiddels over sterke onderzoeksinfrastructuur: in Nederland werken Qutech, Quantum Delta NL (met hubs in Delft, Enschede, Leiden, Twente en Amsterdam) en QuSoft samen aan quantumhardware en -software. Daarbuiten zijn kenmerkende startups zoals het Finse IQM en Franse Pasqal actief met Europese quantumhardware. Europese investeringen lopen echter ver

achter op die van de VS en China.

Wat ontbreekt is een volwaardig, Europees cloudalternatief, compatibel met de functionaliteiten van Amerikaanse hyperscalers. Zonder zo'n platform zullen Europese bedrijven geneigd blijven hun quantumalgoritmen via bijvoorbeeld Microsoft Azure, AWS of Google Cloud te draaien. Daarbij is het lastig om nu al te bedenken hoe een mogelijke migratie van quantumsoftware (zoals algoritmen) er naar een mogelijke Europese cloud eruit gaat zien.

Quantum Security is meer dan alleen cryptografie

De snelle ontwikkelingen in quantumtechnologie maken het aannemelijk dat binnen 5 tot 10 jaar quantumcomputers beschikbaar komen voor commerciële toepassingen. Organisaties zullen deze technologie willen inzetten om concurrentievoordeel te behalen. Quantum Security richt zich enerzijds op het veilig benutten van quantumtechnologie en anderzijds op het versterken van de organisatie tegen quantumdreigingen. Geopolitieke spanningen en discussies over digitale soevereiniteit maken de keuze tussen Europese en niet-Europese quantumtechnologie complex. Vanuit architectuurperspectief is het daarom van belang om tijdig na te denken over een quantumstrategie. Dit houdt in: kritisch kijken naar de bestaande architectuur en bepalen waar quantumcomputing daadwerkelijk toegevoegde waarde kan leveren.

Vanuit het oogpunt van cyberweerbaarheid is het aanbevolen om te starten met een risico-inventarisatie. Identificeer systemen die gevoelige informatie bevatten en geef prioriteit aan de implementatie van post-quantum cryptografie (PQC) op deze systemen. Zo wordt data beschermd tegen het 'store-now-decrypt-later'-scenario, waarbij data nu wordt buitgemaakt en later – zodra quantumcomputers beschikbaar zijn – alsnog ontsleuteld kan worden voor bijvoorbeeld chantage of misbruik.

Tot slot is het essentieel om te investeren in kennisopbouw en expertise op het gebied van quantumtechnologie. De impact van deze technologie op organisaties en de samenleving kan enorm zijn. Door nu al de kansen en risico's in kaart te brengen, kunnen we ons gezamenlijk voorbereiden op deze nieuwe digitale realiteit.

Auteurs: Interviewer drs. Marcel Feenstra, FRSA MALD MBA is werkzaam als trainer en consultant op het gebied van cybersecurity. Ook is hij een van de redacteurs van de IB-Magazine. Hij is bereikbaar via marcel@afterimage.nl. Geïnterviewden Victor Gevers (Victor@csirt.global), Chris van 't Hof (Chris@divd.nl) en Astrid Oosenbrug (Astrid@divd.academy) zijn de oprichters van DIVD.

Dutch Institute for Vulnerability Disclosure

De beveiligers van de digitale wereld

Het Dutch Institute for Vulnerability Disclosure (DIVD) is een Nederlandse non-profitorganisatie die zich inzet voor een veiligere digitale wereld. Sinds de oprichting in 2019 is DIVD uitgegroeid tot een internationale beweging van ethische hackers en cybersecurityexperts. Vanuit hun maatschappelijke missie sporen zij kwetsbaarheden op in digitale systemen en melden die verantwoord – met oog voor proportionaliteit, samenwerking en transparantie. In dit interview spreken we met de drie oprichters: Victor Gevers, Chris van 't Hof en Astrid Oosenbrug.



Hoe is DIVD ontstaan, en wat waren oorspronkelijk de doelstellingen?

Victor: DIVD is begonnen vanuit frustratie én idealisme. We zagen dat er veel kwetsbaarheden in systemen zaten, maar dat er weinig werd gedaan om die verantwoord te melden. Vaak was het onduidelijk bij wie je moest zijn, of werd je zelfs gezien als dreiging. Dat wilden we veranderen.

Chris: In 2019 zijn we gestart met een groep vrijwilligers die het internet veiliger wilden maken door kwetsbaarheden actief op te sporen en die te melden aan partijen die ze kunnen oplossen. Niet voor geld of erkenning, maar vanuit maatschappelijk belang. "We doen dit met open vizier, onafhankelijk en transparant." Velen deden dit al individueel, maar samen sta je sterker.

Astrid: We zagen ook hoe belangrijk publiek-private samenwerking is. DIVD is onafhankelijk, maar werkt nauw samen met CERT's, overheden en andere betrouwbare partners. Onze missie is helder: de digitale samenleving veiliger maken, ethisch en verantwoord.

Wat waren de resultaten in de eerste jaren? Was het wat jullie ervan verwachtten?

Victor: We hadden nooit kunnen voorzien hoeveel impact we zouden hebben. Eén van onze eerste grote successen was de wereldwijde kwetsbaarheid in Citrix-servers. In korte tijd wisten we een groot aantal getroffen organisaties te waarschuwen — vaak nog vóór aanvallers hun kans konden grijpen.

Chris: Ook bij de Kaseya-aanval speelde DIVD een sleutelrol. We hadden de kwetsbaarheid vooraf ontdekt en gemeld. 1.500 organisaties werden gehackt via een laatste kwetsbaarheid die nog opgelost moest worden, maar dat hadden er veel meer kunnen zijn als wij niet tijdig die andere kwetsbaarheden hadden gemeld en de wereld direct hadden gewaarschuwd dat Kaseya uitgeschakeld moest worden.

Astrid: Het toonde aan dat wat wij doen, werkt: een onafhankelijke groep die snel schakelt, zorgvuldig werkt en handelt vanuit publiek belang.

Welke activiteiten zijn er in de loop van de tijd bijgekomen, en waarom?

Chris: We zijn altijd meer geweest dan een groep die meldingen doet. We geven lezingen, verzorgen workshops en delen actief onze kennis. Maar bovenal zijn we een fijne en veilige plek geworden waar nerds hun ding kunnen doen.

Astrid: Binnen DIVD richt ik me op de maatschappelijke impact van ons werk. Ik zet me in voor meer diversiteit, onderwijsprogramma's en sterke publiek-private samenwerking. En ik voer gesprekken met

overheden en andere partijen over hoe we jonge hackers aan de goede kant van de wet houden. Dat vraagt om wederzijds vertrouwen én een veilige leeromgeving.

Victor: Onze Code of Conduct vormt daarin het ethisch fundament. We werken met gevoelige data die vaak zonder voorafgaande toestemming is verzameld — via internetscans, kwetsbaarheden of gelekte credentials. Onze uitgangspunten zijn: maatschappelijke noodzaak, proportionaliteit en subsidiariteit. Die hanteren we strikt en delen we actief met de community.

Op welk moment, en met welke reden, kwamen jullie op het idee voor DIVD Academy?

Victor: Tijdens de Citrix-crisis viel het ons op hoeveel jongeren meedachten — vaak jong, technisch sterk, maar nergens écht welkom. Dat triggerde ons: er moest een plek komen waar zij hun talent legaal en verantwoord kunnen inzetten.

Astrid: Zo ontstond DIVD Academy. Een plek waar jongeren praktijkgericht leren over ethisch hacken, responsible disclosure, cyberveiligheid en maatschappelijke verantwoordelijkheid. Ze worden onderdeel van een gemeenschap die werkt aan het publieke belang.

Op welke doelgroep richten jullie je met DIVD Academy en wat hoop je ermee te bereiken?

Astrid: We richten ons op jongeren tussen de 14 en 24 jaar, met speciale aandacht voor wie buiten de boot dreigen te vallen: uitvallers, autodidacten, jongeren met talent maar zonder diploma en met name jongeren met een bi-culturele achtergrond die structureel minder kansen krijgen.

Victor: Zij worden vaak afgewezen voor stages, waardoor ze hun opleiding niet kunnen afronden. Bij ons krijgen ze wél de kans. Ze leren samenwerken, communiceren, verantwoordelijkheid nemen én werken mee aan het oplossen van échte maatschappelijke vraagstukken.

Wat zijn de resultaten tot nu toe en wat zijn de plannen voor de toekomst?

Victor: We hebben al tientallen jongeren begeleid die nu doorstromen naar stages en vervolgoopleidingen of meedraaien als begeleiders van nieuwe deelnemers. De impact zit niet alleen in wat ze leren, maar vooral ook in het vertrouwen dat ze krijgen.

Astrid: We werken samen met overheid, onderwijs en bedrijfsleven aan uitdagende projecten. Een goed voorbeeld is ons huidige programma rond kwetsbaarheden in het energiesysteem. We ontwikkelen lesmateriaal, trainingen en workshops voor studenten en

We leiden een nieuwe generatie experts op die de energietransitie niet alleen technisch ondersteunt, maar ook digitaal weerbaar maakt.

vakmensen in de sector. Zo leiden we nieuwe experts op én maken we de energietransitie digitaal veiliger.

Chris: Het Europese elektriciteitsnetwerk is in rap tempo veranderd in een 'smart grid': slim en duurzaam, maar ook kwetsbaar. In het project CVD in het Energiesysteem onderzoeken we de digitale veiligheid van apparaten die vaak buiten het zicht van netbeheerders vallen – zoals laadpalen, omvormers van zonnepanelen en Home Management Systemen. Veel risico's zitten juist achter de meter, terwijl daar nauwelijks toezicht op is. Daarom bundelen we losse initiatieven tot een structureel onderzoeksprogramma, bouwen we een IoT Hacking Lab en richten we een CVE Numbering Authority in voor energiegerelateerde kwetsbaarheden.

Astrid: Op basis van die bevindingen ontwikkelt DIVD Academy lesmateriaal, trainingen en workshops voor installateurs, studenten en andere vakmensen in de sector. Zo zorgen we dat de kennis die we opdoen niet op de plank blijft liggen, maar ook echt landt in het onderwijs en op de werkvloer. We leiden een nieuwe generatie experts op die de energietransitie niet alleen technisch ondersteunt, maar ook digitaal weerbaar maakt.

Energieproject in het kort

Met het project CVD in het Energiesysteem onderzoekt DIVD-kwetsbaarheden in randapparatuur zoals laadpalen en omvormers. Het project loopt tot eind 2026 en richt zich op onderzoek, educatie en structurele samenwerking met de energiesector. Meer informatie: <https://www.divd.nl/energie/>

Tot slot

Chris: DIVD is gebouwd op vertrouwen, ethiek en de wil om het goede te doen. We werken binnen Nederland goed samen met alle relevante partijen en internationaal met 20 landen. Nu nog de rest

van de wereld. Die impact bereiken we niet alleen met techniek, maar juist door mensen die het verschil willen maken.

Astrid: Bij de Academy bouwen we structureel aan kansen voor jongeren met talent voor cybersecurity. Ik richt me op de strategische ontwikkeling, maar begeleid ook jongeren één-op-één. We geven ze de ruimte om te leren, fouten te maken en verantwoordelijkheid te nemen. Als je hen serieus neemt, doen zij dat ook. Dat vraagt visie, samenwerking en lef. Want het talent is er, wij zorgen dat ze ook het podium krijgen.

Wat is CSIRT.global?

CSIRT.global is een internationaal vrijwilligersteam dat organisaties helpt bij het oplossen van digitale kwetsbaarheden. Ze richten zich op bug bounties, exploits onderzoek en incident-respons, en werken daarbij onafhankelijk, transparant en zonder commerciële of politieke belangen. De organisatie is verbonden aan DIVD, maar opereert zelfstandig. Waar DIVD-kwetsbaarheden opspoor, helpt CSIRT.global bij het daadwerkelijk verhelpen ervan. Alles gebeurt op basis van een strikte gedragscode, met aandacht voor proportionaliteit, maatschappelijke noodzaak en minimale impact. Meer info: [https://www.csirt.global/\(/Kader\)](https://www.csirt.global/(/Kader))

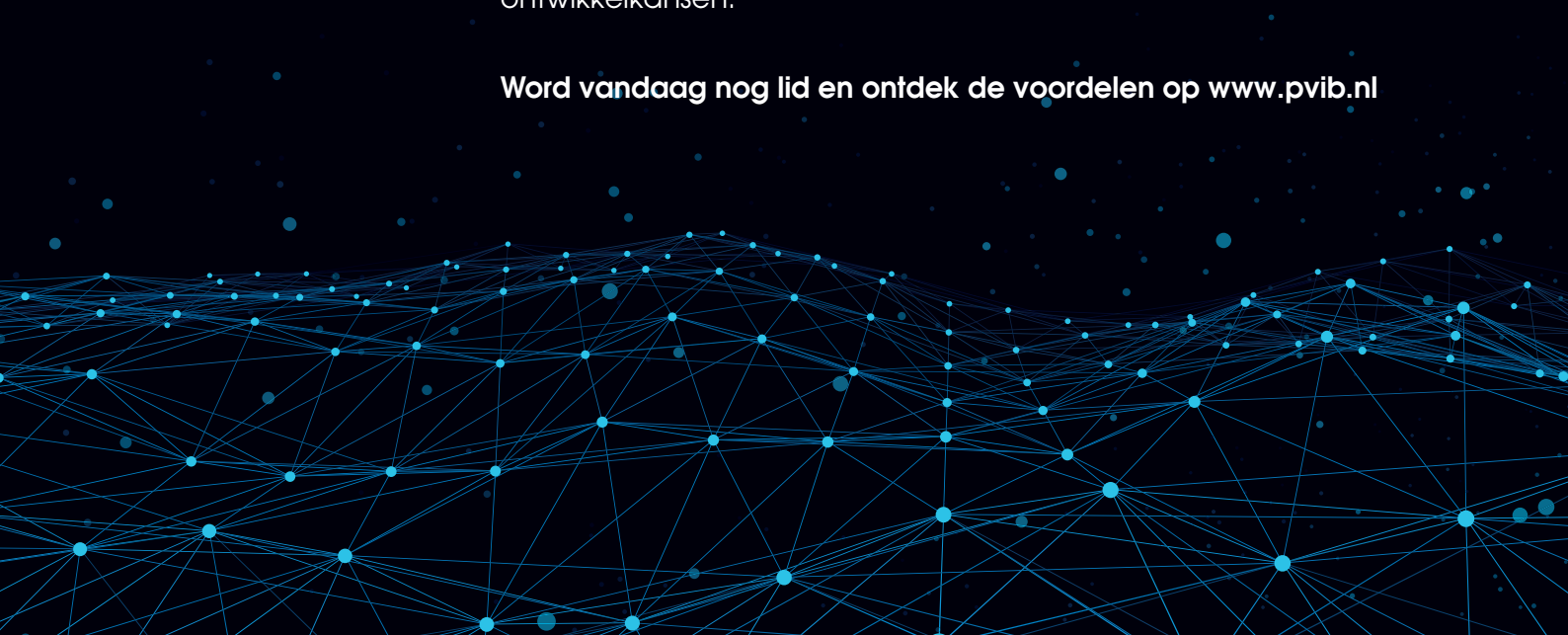
Victor: Naast DIVD en de Academy speelt ook CSIRT.global een belangrijke rol in het digitale speelveld. Waar DIVD zich richt op Nederland en de Academy op talentontwikkeling, pakken we met CSIRT.global juist de wereldwijde blinde vlekken aan. Kwetsbaarheden stoppen niet bij de grens — onze inzet ook niet.

Versterk jouw carrière

Ben jij actief als informatiebeveiligger, IT-auditor, risk- of compliance manager, of werk je binnen een aanverwant vakgebied? Dan is PvIB dé plek waar jouw carrière een boost krijgt. PvIB verbindt professionals uit uiteenlopende sectoren – van forensisch IT-onderzoekers tot (lijn)managers – en biedt een krachtig platform voor kennisdeling, inspiratie en persoonlijke groei.

Of je nu een doorgewinterde expert bent of net je eerste stappen zet in het vak, bij PvIB vind je een community waar je leert, groeit en nieuwe waardevolle connecties opdoet. Profiteer van een sterk netwerk, actuele vakkennis en talloze ontwikkelkansen.

Word vandaag nog lid en ontdek de voordelen op www.pvib.nl





Samen op weg naar duurzame gedragsverandering

Een procesmatige aanpak voor cybersecurity awareness in de sector onderwijs en onderzoek

In de wereld van cybersecurity wordt vaak als eerste aan technische maatregelen gedacht. Firewalls, encryptie, antivirussoftware zijn stuk voor stuk cruciale bouwstenen. De belangrijkste aanvalsvector voor cybercriminelen zijn tegenwoordig niet de systemen, maar de mensen. Volgens het Verizon Data Breach Investigation Report 2024 is bij maar liefst 68% van alle beveiligingsincidenten menselijk handelen betrokken. Het is tijd voor een nieuwe aanpak voor awareness. Instellingen werken samen met SURF aan een procesmatige aanpak om awareness structureel te verhogen.



Samenwerken is samen sterker

De sector onderwijs en onderzoek (O&O) deelt regelmatig kennis en ervaring op het gebied van cybersecurity. Daardoor kunnen instellingen sneller en effectiever optreden bij incidenten, bijvoorbeeld zoals eerder dit jaar bij de TU Eindhoven. Naast de technische aspecten komen steeds vaker vraagstukken over de menskant in de community terecht. We zien een toenemende interesse in awareness en training bij instellingen en de daarbij komende vraagstukken.

In 2023 is bij SURF een visie opgesteld inzake awareness bij instellingen, met daarbij behorende projecten. Het eerste project was het ontwikkelen van een 'proces voor awareness'. Met dit proces kunnen instellingen zelf aan de slag. Daarnaast moest dit proces ook orde aanbrengen in de diverse disciplines die nodig zijn voor een succesvol awarenessprogramma. 'Er is al zoveel materiaal en informatie beschikbaar, we missen het overzicht en hoe we dit effectief in kunnen zetten'.

Proces voor awareness

Deelnemers van: Yuverta, Saxion, de Erasmus Universiteit, Fontys, Universiteit Leiden en SURF hebben gedurende 6 maanden gewerkt aan dit project. Als eerste stap hebben we bestaande modellen gereviewd, om aan te sluiten bij wat reeds bestaat. Daaruit bleek dat de bestaande modellen niet voldeden voor het doel wat we voor ogen hadden. We kwamen uit op een nieuw model waarin awareness in processtappen weergegeven is.

De aanpak volgt het PDCA-model (Plan, Do, Check, Act), wat zorgt voor continue verbetering en aansluiting bij bredere organisatiedoelen, zoals de cybersecurity en cyberweerbaarheid vastgelegd in SURFaudit. In de eerste stap wordt gekeken naar de cybersecurityrisico's voor de instelling. Daaruit worden de belangrijkste thema's gekozen voor het awarenessprogramma. Aan de hand van een risicomatrix kiest de instelling welke doelgroepen het meeste risico lopen. Het proces sluit daarmee aan op de vereisten voor risicobeheersing zoals aangegeven in de NIS-2 richtlijn/Cbw.



Afbeelding 1 Procesmodel voor awareness

Bewustzijn ≠ Gedragsverandering

Onderzoek wijst uit dat informeren en kennis overdragen alleen, niet leidt tot ander gedrag. Sterker nog, mensen die slachtoffer worden van financiële fraude hebben vaak bovengemiddelde financiële kennis. Dit principe geldt ook bij cybersecurity. Traditionele bewustwordingscampagnes missen daardoor vaak de vertaalslag naar duurzame gedragsverandering.

Op basis van intern onderzoek (bijvoorbeeld een 0-meting, interviews of een vragenlijst) wordt gekeken welke de factoren zijn die bepalen of iemand het gewenste gedrag vertoont. Door gebruik te maken van een gedragsmodel zoals bijvoorbeeld het COM-B model (Capability, Opportunity, Motivation, en Behaviour) wordt daarmee gekeken naar verschillende factoren zoals capaciteit, omgeving en motivatie.

Om awarenesscampagnes effectief te maken wordt per thema in kaart gebracht welke technische, organisatorische en procedurele aanpassingen nodig zijn om het gewenste doelgedrag mogelijk te maken en te stimuleren. Het meten van awareness is een integraal onderdeel van alle processtappen.

Onderdelen procesmodel

Naast risicomanagement en gedrag, zijn de volgende onderdelen ook opgenomen in het proces voor awareness:

Programmaplan

Het opstellen van een strategisch en operationeel programmaplan. Deze onderdelen zijn apart benoemd, omdat uit de praktijk blijkt dat binnen organisaties zowel het bestuur overtuigd moet worden alsook de stakeholders in de organisatie.

Informeren en trainen

Het uitvoeren van campagnes, trainingen en gedragsinterventies vind je in deze stap terug. In dit onderdeel van het proces voer je deze uit, vaak gezamenlijk met de stakeholders in de organisatie. Dit is ook het moment waarop het meetbaar maken van belang is: een voor- en nameting geven inzicht in de effectiviteit.

Evalueren en rapporteren

De laatste stap in het proces is het evalueren en rapporteren. Om de effectiviteit van het awarenessprogramma inzichtelijk te maken en je stakeholders te laten zien, hoe het programma op basis van informatie bijgestuurd wordt. In deze stap bereid jezelf ook voor op de volgende cyclus van het proces.

Om het model in te zetten, is er ook een tijdlijn variatie beschikbaar waarbij je het proces stapsgewijs kunt doorlopen.



Afbeelding 2: Tijdlijn van het Proces voor awareness

Proof of Concept

Om te testen of het model in de praktijk toe te passen is, zijn begin 2025 twee Proof of Concepts gestart. Op basis van de praktijk wordt het model verder aangevuld. Omdat een proces, tijd kost, is dit een langdurig traject waarbij we ongeveer elke drie maanden toetsen hoe de PoC's verlopen. Het model wordt vervolgens aan het einde van het kalenderjaar geëvalueerd en aangepast.

Hogeschool Fontys

Het proces gebruikt om het awarenessprogramma voor het komende jaar vorm te geven. Vanuit de risico's wordt gekeken naar gedragsverandering, waarbij samengewerkt wordt met een gedragspsycholoog.

Erasmus Universiteit

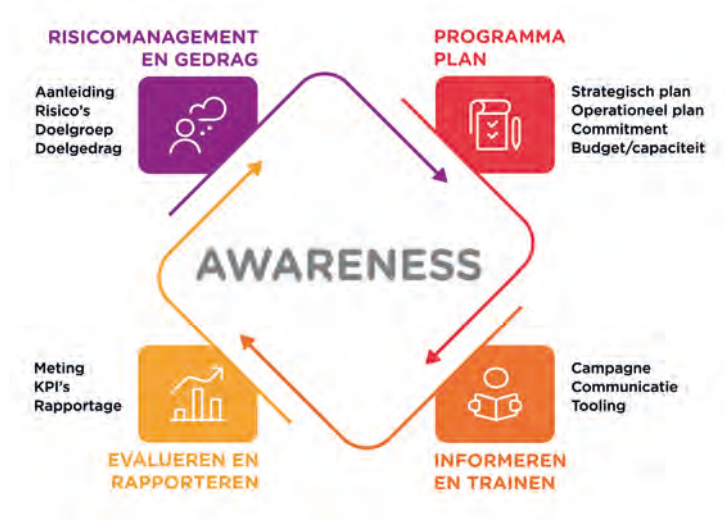
Het proces is de basis om awareness structureel in te vullen. Centraal wordt dit door de awareness officer gecoördineerd, terwijl decentraal bij de faculteiten hetzelfde proces gebruikt wordt, maar de inhoud aangepast is naar de medewerkers bij de faculteiten.

Om te testen of het model in de praktijk toe te passen is, zijn begin 2025 twee Proof of Concepts gestart

Breed toepasbaar

Het model is ontwikkeld door instellingen in de sector O&O, maar is breed toepasbaar. Het materiaal en informatie over dit model worden openbaar gepubliceerd en is vrij te gebruiken. Binnen Nederland, maar ook in Europees verband via GÉANT, de Europese koepelorganisatie voor NREN's.

Het procesmodel is uitgewerkt in de vier stappen, inclusief subonderdelen. Deze meer uitgebreide toelichting vind je in de CSY toolkit (1) Daar is ook een PowerPoint-presentatie te vinden met voorbeelden hoe je in jouw instelling invulling kunt geven aan de verschillende stappen.



Afbeelding 3: Uitgebreider Procesmodel voor awareness

De komende tijd gaan we aan de slag om de templates, materialen en hulpmiddelen verder te ontwikkelen en te ordenen in de processtappen. Bijvoorbeeld het ontwikkelen van een basistraining gebaseerd op het procesmodel.

Voordelen procesmodel

Op gebied van awareness zijn er al meerdere modellen en frameworks ontwikkeld. Wat dit proces voor awareness uniek maakt:

- Het is gebaseerd op recente wetenschappelijke inzichten rondom awareness en gedragsverandering.
- Ondersteunt met praktische tools zoals templates, voorbeeldmaterialen en een training voor awarenessprofessionals.
- Flexibiliteit voor instellingen, zodat zij hun aanpak kunnen afstemmen op hun eigen context.
- Gericht op structurele integratie binnen de instelling. Door aan te sluiten bij de PDCA-cyclus, het integreren van risicomanagement, gedragsverandering en het meetbaar maken van awareness.
- Groeit mee aan de hand van praktijk.

Conclusie

Cybersecurity gaat niet alleen over technologie - het gaat vooral over mensen. Door bewustwording te combineren met gedragsverandering,

kunnen instellingen structureel werken aan een veilige digitale omgeving. Het proces voor awareness helpt instellingen om die vertaalslag te maken. Niet door nóg een theoretisch model te introduceren, maar door een praktisch, onderbouwd proces dat werkt in de praktijk. Met dit recept kunnen organisaties zelf aan de slag om structureel te werken aan het verhogen van awareness.

Daarom de uitnodiging aan de lezer om bij te dragen aan dit awarenessproces door contact met mij op te nemen voor al uw suggesties, ideeën, verbeteringsvoorstellen en natuurlijk vragen. Ik kijk al uit naar de respons.

Referentie

- (1) Het model met documentatie vind je terug in de CSY toolkit edu.nl/3trdb
Updates over de PoC's, achtergrond, interviews en artikelen over het proces voor awareness op SEC.SURF.nl

Auteur: Remco Maurits Emile van der Schoot is a PhD researcher at the Hogeschool Utrecht and Radboud University. His PhD focuses on the use of shadow IT by employees from a behavioural change perspective. Additionally, he teaches at the Master's Project Management and Digital Security and is reachable via remco.vanderschoot@hu.nl



Managing Shadow IT: From Bans to Benefits

When innovation collides with regulation, shadow IT emerges. Employees, driven by performance gains and innovative needs, often resort to unsanctioned tools that bypass security policies. Shadow IT poses cybersecurity risks but also offers insights into what the organisation's official tools may lack. Rather than fighting shadow IT with restrictions, organisations should start by learning from shadow IT and striking a balance between security and business needs.

Imagine Mark, a financial analyst, handling sensitive financial reports and personal data. His organisation enforces a strict policy to protect this information: all files must be stored on a secure, company-provided cloud. In practice, this system creates friction. Remote access is slow, and the two-factor authentication (2FA) process feels cumbersome to Mark and his colleagues. Mark regularly collaborates with external clients who cannot access the company-provided cloud, making file sharing nearly impossible. Frustrated, Mark develops a personal cloud to enable collaboration and access his files with ease. In doing so, Mark introduces shadow IT into the organisation.

Beyond the risks: What shadow IT brings to the table

Mark's personal cloud is a textbook example of shadow IT: unknown, unapproved, and autonomous supplementation to the organisational IT. Shadow IT increases cybersecurity risks while hindering the ability to identify and manage the associated risks (1). Yet, shadow IT originates not merely from a disregard for the rules. It also originates from employees seeking to enhance their performance or address practical needs. Research shows that shadow IT improves individual performance by increasing productivity, adaptability, innovation, and collaboration (2, 3, 4). It also enables employees to continue when facing system limitations or barriers. In this way, shadow IT is a double-edged sword, introducing security concerns while also providing value.



Afbeelding 2: 'Double-edged sword'

Why restrictive approaches fail

To manage shadow IT risks, many organisations turn to restrictive policies and technical measures to enforce organisational IT use. While these measures appear justified from a security perspective, research indicates that restrictive measures yield inconsistent results (3). These approaches frequently backfire, leading to greater and more concealed shadow IT usage (5). Restrictive approaches can enhance compliance by reducing the detectability of shadow IT. However, on their own, they are likely insufficient for managing the actual risks. Moreover, banning shadow IT altogether deprives the organisation of potential value (4). In short, restrictive approaches are neither a reliable nor a long-term solution for managing shadow IT risks (3, 4).

Managing shadow IT risks:

Accommodating needs and allowing for innovation

Instead of relying solely on restrictive approaches, organisations should manage shadow IT by striving to accommodate business needs while keeping the organisation's cybersecurity within acceptable limits (2). This can be approached in three steps:

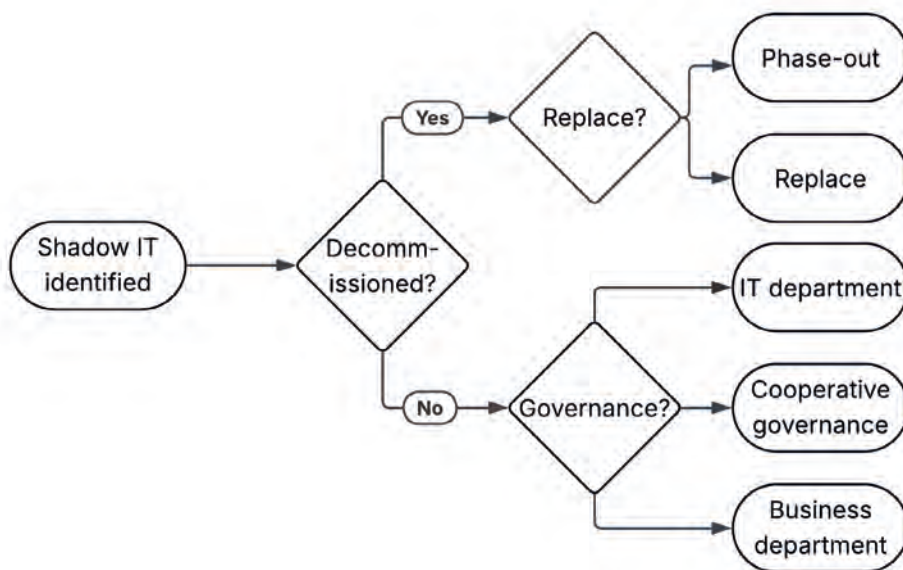
The first step is to identify what shadow IT solutions employees are using. This can be achieved through technical monitoring and by encouraging employees to share their shadow IT solutions (1, 2). At the same time, organisations should identify gaps between business needs and the organisational IT. Closing these gaps proactively can lower the desire for shadow IT.

In Mark's case, his ability to work efficiently and effectively is impeded by slow IT, restrictive sharing, and burdensome authentication. This leads Mark to seek out shadow IT. If collaboration with external clients is provided, Mark's desire for shadow IT would lessen.

Once shadow IT solutions are identified, the organisation should decide whether to keep or restrict them. This decision should be based on two factors (1). First, the value the shadow IT solution provides to the organisation. For example, what business needs does this shadow IT solution accommodate? Second, the risks that the shadow IT solution poses to the organisation. This analysis should transcend individual departments to capture the full ramifications of the shadow IT solution.

In Mark's case, his personal cloud enables collaboration with clients, highlighting a gap in the current organisation's IT offering. Nevertheless, it heightens the potential for data loss and leakage. Rather than punishing Mark, the organisation could respond by replacing the shadow IT solution with an internal function in the secure company-provided cloud.

Managing Shadow IT: From Bans to Benefits



Afbeelding 3: 'flowchart'

The identified shadow IT solutions can be kept by either accepting them (with conditions) or replacing them with a safe alternative. This safe alternative should address the same underlying business need (1). In some cases, the shadow IT solution cannot be kept, and restrictions are a necessary last resort.

The two-factor authentication (2FA) may feel burdensome, as seen in Mark's case, but it is also one of the most effective and proven cybersecurity tools. Removing it would unacceptably undermine the organisation's cybersecurity.

The third and final step depends on whether the organisation decides to keep or restrict the shadow IT solution. If the shadow IT solution is to be retained, it should be integrated into the organisation and responsibilities should be assigned (1). If the shadow IT solution is restricted, this should be supported by efforts to explain the decision and build employee understanding. This starts with open communication with decision-makers and clear, transparent policies (1). If essential security measures continue to be circumvented by shadow IT, a focused awareness campaign might be necessary.

As this article shows, managing shadow IT is not just about tightening controls. It is about understanding why it exists. Shadow IT reveals gaps

between business needs and the systems, security measures and policies. Rather than dismissing or suppressing shadow IT, organisations should learn from shadow IT and find a balance between security and performance.

References

- (1) Klotz, S., Kopper, A., Westner, M., & Strahinger, S. (2022). Causing factors, outcomes, and governance of Shadow IT and business-managed IT: a systematic literature review. *International Journal of Information Systems and Project Management*, 7(1), 15-43. <https://doi.org/10.12821/ijisp070102>
- (2) Haag, Steffi and Eckhardt, Andreas (2024) "Dealing Effectively with Shadow IT by Managing Both Cybersecurity and User Needs," *MIS Quarterly Executive*: Vol. 23: Iss. 4, Article 5. Available at: <https://aisel.aisnet.org/misqe/vol23/iss4/5>
- (3) Welck, M. V., Trenz, M., Jensen, T. B., & Veit, D. (2017). Empowerment and BYOx: Towards Improved IS Security Compliance. In *ICIS 2017 Proceedings*, Association for Information Systems. AIS Electronic Library (AISeL). <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=11116&context=icis2017>
- (4) Zimmermann, S., Rentrop, C., & Felden, C. (2017). A Multiple Case Study on the Nature and Management of Shadow Information Technology. *Journal of Information Systems*, 31(1), 79-101. <https://doi.org/10.2308/isis-51579>
- (5) Raković, L., Sakal, M., Matković, P., Marić, M. (2020). Shadow IT – A Systematic Literature Review. *Information Technology and Control*, 49(1), 144-160. <https://doi.org/10.5755/j01.itc.49.1.23801>

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



Vertrouwen in het Onzichtbare

In mijn dagen als software engineer had ik te maken met compilers. Een compiler is een behoorlijk complex programma, het zet programmaregels om naar uitvoerbare code. Het bevat alle kennis van de programmeertaal én van de omzetting van elke taalconstructie naar instructies voor een computer.

Voor ons was het een eye-opener wat Ken Thompson, mede-uitvinder van Unix, in 1984 aangaf in zijn Turing Award-lezing: "Reflections on Trusting Trust" (1). Het is een verhaal over het vertrouwen in compilers, met een diep filosofische boodschap: vertrouwen in technologie is vaak gebaseerd op aannames die we niet kunnen verifiëren.

Thompson liet zien: hoe een compiler subtiel aangepast kan worden om een backdoor in elke applicatie te verstoppert in de omzetting van bron- naar machinecode, zodat er in de broncode geen backdoor zichtbaar is, maar in de machinecode wel. Nog verontrustender: de compiler kan ook op die manier zichzelf aanpassen. Zo ontstaat een ingesloten, zichzelf herhalende kwetsbaarheid. Zelfs met toegang tot alle broncode, kun je deze backdoor niet ontdekken – hiermee liet Thompson zien dat je een compiler alleen kon vertrouwen als je de volledige keten van tools vertrouwt die gebruikt zijn om hem te bouwen.

Dat was toen. We staan nu aan de vooravond van een nieuw technologisch tijdperk, gedreven door AI (kunstmatige intelligentie). En net als bij compilers rijst de vraag: hoeveel vertrouwen mogen we het geven als we werkelijk niet weten wat er onder de motorkap gebeurt?

Net zoals compilers een ingesloten kennis hebben van de programmeertaal die ze vertalen, bevatten AI-modellen een ingesloten kennis van hun trainingsdata en richtlijnen voor gebruik. Een groot taalmodel zoals GPT-4 is getraind op gigantische hoeveelheden tekst en heeft daaruit talloze patronen, associaties, en concepten geleerd. Maar we kunnen niet exact aanwijzen hoe of waar die kennis zich in het model bevindt. En net zoals een gemanipuleerde compiler onverwachte of kwaadaardige code kan genereren, kunnen AI-systemen:

- **Onjuiste of bevooroordeelde informatie geven;**
- **Onbedoeld (of doelbewust) afwijkend gedrag vertonen;**
- **Gevoelig zijn voor manipulaties (zoals prompt injection) of data poisoning.**

We gebruiken AI steeds vaker in besluitvorming, contentcreatie en zelfs broncodegeneratie. Toch is het zelden duidelijk welke aannames het model maakt, of welke invloeden het gedrag hebben gevormd en welke stappen gezet zijn bij de formulering van het antwoord. En meer nog als bij de backdoor van Thompson, kunnen zwakheden of manipulaties onzichtbaar blijven.

Programmacode inspecteren is lastig. Een AI-model inspecteren is lastiger: ook als het functioneert weten we niet altijd waarom. We hebben geen zicht op de volledige trainingsdata en richtlijnen. De uitkomsten geven onvoldoende informatie over de interne werking, laat staan het maakproces.

De lezing van Thompson blijkt tijdloos. Zijn waarschuwing over onzichtbare kwetsbaarheden in vertrouwde systemen geldt misschien nog wel sterker in het AI-tijdperk. Zowel compilers als AI-modellen zijn fundamenten waarop we bouwen. Als we de fundering niet kunnen controleren, is het huis dat we erop zetten kwetsbaar – ongeacht hoe solide het eruitziet. Een kritische houding blijft cruciaal.

Vertrouwen in technologie begint niet bij wat het doet, maar bij wat we weten van het maakproces.

Referentie

(1) <https://dl.acm.org/doi/pdf/10.1145/358198.358210>

Auteurs: Renske Korenromp en Esger ten Thij zijn beiden onderzoekers bij het lectoraat Cyberweerbare Organisaties van Avans Hogeschool. Mieke Zijlstra is programmamanager bij Cyber Weerbaarheidscentrum Brainport. Rick van der Kleij is lector Cyberweerbare Organisaties bij Avans Hogeschool en Cybersecurity onderzoeker bij TNO. Renske is bereikbaar via: ram.korenromp@avans.nl



Waarom mkb-ondernemers niet investeren in cyberweerbaarheid

Focusgroeponderzoek naar ervaren belemmeringen

In de huidige digitale wereld is cyberweerbaarheid een steeds grotere uitdaging voor bedrijven, met name voor het midden- en kleinbedrijf (mkb). Recent onderzoek onder 895 organisaties, laat zien dat in 2023 bijna driekwart van het Nederlandse mkb te maken kreeg met een cyberaanval (Krauwel, 2024). Ook de impact op deze ondernemers is vaak enorm. Schattingen wijzen uit dat 60% van de mkb-bedrijven die slachtoffer worden van een cyberaanval binnen zes maanden hun deuren moeten sluiten (1). Zo vroeg onlangs nog Wodkaproducent Stoli faillissement aan in de Verenigde Staten, mede vanwege een ransomware-aanval.

Daarnaast geloven veel mkb-ondernemers, veelal ten onrechte, dat ze niet interessant zijn voor cybercriminelen (2). Dit maakt dat zij noodzakelijke investeringen in het vergroten van de cyberweerbaarheid uitstellen (Van der Kleij, 2025). Bovendien zijn zij vaak afhankelijk van externe IT-dienstverleners die mogelijk niet over de nodige cyberexpertise beschikken, wat de kwetsbaarheid voor cyberaanvallen alleen maar vergroot (3). De combinatie van deze factoren vergroot het risico voor individuele mkb-bedrijven op slachtofferschap en vormt een bredere bedreiging voor de cyberweerbaarheid van de hele keten waar deze bedrijven onderdeel van uitmaken (SIDN, 2023).

Ondernemers erkennen cyber risico's vaak pas na schade, zoals herstelkosten, omzetverlies of reputatieschade. Volgens Krauwer (2024) hebben aanvallen bij 59% van het grootbedrijf en 43% van het mkb al tot zulke gevolgen geleid, cijfers die overeenkomen met de Cybersecuritymonitor van het CBS. Toch neemt het aantal mkb-bedrijven en zelfstandigen dat cybercriminaliteit als groot risico ziet af, terwijl bijna één op de vijf bedrijven aangeeft onvoldoende voorbereid te zijn (Van der Kleij, 2025). Deze afnemende risicoperceptie onder mkb-ondernemers staat haaks op de groeiende dreiging van cybercriminaliteit. Dit spanningsveld vormt de basis van ons onderzoek naar de terughoudendheid van hen om in cyberweerbaarheid te investeren, ondanks duidelijke risico's. Het onderzoek is uitgevoerd in opdracht van het Cyber Weerbaarheidscentrum Brainport.

Het verkrijgen van inzicht in de onderliggende gedragsfactoren die bepalen of mkb-ondernemers wel of niet investeren in hun cyberweerbaarheid, is cruciaal voor het begrijpen van deze terughoudendheid. Inzicht in deze gedragsfactoren is tevens van belang, omdat ze helpen te begrijpen hoe mkb-ondernemers gestimuleerd kunnen worden om noodzakelijke stappen te nemen om hun cyberweerbaarheid te optimaliseren. De onderzoeksvraag is dan ook:

"Onder welke voorwaarden zijn ondernemers in het mkb bereid tijd en

geld te investeren in ondersteuning voor het versterken van hun cyberweerbaarheid?".

Theoretisch kader

Om het gedrag van mkb-ondernemers te analyseren, is het COM-B model toegepast. Dit model biedt een theoretisch kader waarin gedrag wordt verklaard aan de hand van drie componenten: Capaciteit (Capability), Gelegenheid (Opportunity) en Motivatie (Motivation). Het model helpt factoren te identificeren die gedrag beïnvloeden en biedt een systematische benadering om te begrijpen waarom ondernemers wel of niet in cyberweerbaarheid investeren (Michie, Van Stralen & West, 2011). Als aanvulling is het Theoretical Domains Framework (TDF) gebruikt, dat het COM-B model uitbreidt met 14 domeinen die psychologische, gedragsmatige en omgevingsfactoren in kaart brengen. Het TDF biedt daarmee gedetailleerder inzicht in de specifieke determinanten van gedrag. Door het TDF te integreren met het COM-B model worden niet alleen algemene gedragsfactoren, maar ook de onderliggende mechanismen zichtbaar die gedrag sturen (Zigbano-Wenzler, Magwood, Mueller & Fraser, 2020).

Methode

Als methode voor dit onderzoek is gebruik gemaakt van de focusgroep, waarbij meerdere deelnemers tegelijk met elkaar in gesprek gingen.

Werving en deelnemers

De deelnemers aan de focusgroep zijn geworven via Midpoint Brabant en Hallo. Midpoint Brabant is de regionale economische ontwikkelingsorganisatie voor Midden-Brabant, die samen met ondernemers, onderwijs en overheid innovatie en groei stimuleert. Hallo ondersteunt mkb'ers door ICT toegankelijker en efficiënter voor hen te maken, met aandacht voor veiligheid, training en groei. De samenstelling van de focusgroep was divers, representatief voor verschillende sectoren en bedrijfsgroottes binnen het mkb. Hiermee zijn uiteenlopende inzichten verzameld over de bereidheid om in cyberweerbaarheid te investeren.

In totaal namen negen mkb-ondernemers uit diverse sectoren deel aan de focusgroep.

Data-collectie

De focusgroep vond fysiek plaats in een sessie van twee uur bij Midpoint Brabant. Tijdens de focusgroep werden tien stellingen aan de deelnemers gepresenteerd waarmee zowel specifieke onderzoeksthema's geadresseerd konden worden als ruimte werd geboden voor spontane discussies. De TDF-domeinen zijn toegepast bij het formuleren van de stellingen.

Een voorbeeld van één van de stellingen is: "Als ik gebruik maak van een externe IT-dienstverlener, dan zal dit de kans op schadelijke incidenten aanzienlijk verminderen."

Resultaten

In de focusgroep kwamen verschillende gedragsfactoren naar voren die het mkb belemmeren om beschikbare initiatieven en ondersteuningsmogelijkheden op het gebied van cyberweerbaarheid optimaal te benutten. Hieronder bespreken we de belangrijkste barrières, geordend volgens de drie centrale componenten: Capaciteit, Gelegenheid en Motivatie.

Capaciteit

Communicatiekloof: uit de focusgroep blijkt dat onduidelijke communicatie – mede door verschillen in kennis en vaardigheden tussen aanbieders en ondernemers – een belangrijke barrière vormt voor het benutten van beschikbare cybersecurity-initiatieven. Ondernemers missen vaak de kennis om te begrijpen welke maatregelen nodig zijn om hun bedrijf te beschermen tegen cyberdreigingen. Ook ontbreekt het hen regelmatig aan de vaardigheden om maatregelen daadwerkelijk toe te passen, waardoor ze moeite hebben om geïnformeerde keuzes te maken. Cybersecurity-experts gebruiken bovendien vaak technische termen die ondernemers lastig kunnen begrijpen, waardoor informatie moeilijk toepasbaar wordt. Onduidelijke communicatie belemmert zo een effectieve samenwerking. Experts moeten hun communicatie en advies beter afstemmen op het niveau en de belevingswereld van mkb-ondernemers.

(On)Bewustzijn van cybersecurity-initiatieven: ondernemers zijn zich vaak niet bewust van de initiatieven en subsidies die beschikbaar zijn om hun cyberweerbaarheid te versterken. Dit wijst opnieuw op een gebrek aan kennis, in dit geval over de beschikbare ondersteuning vanuit publieke dienstverleners. De communicatie over deze programma's is, zoals eerder genoemd, vaak te technisch of abstract, waardoor ondernemers de waarde ervan lastig kunnen inschatten. Daardoor weten zij vaak niet welke stappen zij kunnen zetten om hun bedrijf te beschermen. Beter afstemming van de communicatie op het kennis- en vaardigheidsniveau van ondernemers kan hun hande-

Een gebrek aan motivatie bleek een belangrijke barrière voor ondernemers om hun cyberweerbaarheid te verbeteren.

lingsvermogen vergroten en hen helpen de juiste keuzes te maken om hun cyberweerbaarheid te versterken.

Gelegenheid

Gelegenheid om gebruik te maken van beschikbare initiatieven en ondersteuningsmogelijkheden speelt een belangrijke rol in de bereidheid van mkb-ondernemers om te investeren in cyberweerbaarheid. Ondersteuningsmogelijkheden, zoals financiële vouchers en subsidies, werden als waardevol gezien, vooral voor ondernemers die al de intentie hadden om te investeren. Dit kan helpen de eerste stap te zetten zonder grote financiële verplichtingen.

Motivatie

Gebrek aan urgentiebesef: een gebrek aan motivatie bleek een belangrijke barrière voor mkb-ondernemers om hun cyberweerbaarheid te verbeteren. Veel ondernemers erkennen wel dat cyberbeveiliging belangrijk is, maar zijn zich vaak niet volledig bewust van de risico's die gepaard gaan met cybercriminaliteit. Dit kan deels worden toegeschreven aan het gebrek aan urgentiebesef; de dreiging van cyberincidenten wordt vaak pas erkend wanneer het te laat is. Cybersecurity wordt daardoor vaak als een abstracte en niet-urgente taak gezien. Dit kan verklaard worden door de struisvogelparadox, die verwijst naar de menselijke neiging om bedreigingen te negeren of te vermijden, zelfs als deze belangrijke risico's met zich meebrengen. Deze cognitieve bias leidt ertoe dat ondernemers de noodzaak om preventieve maatregelen te nemen vaak onderschatten, waardoor ze geen actie ondernemen totdat een incident zich daadwerkelijk voordoet (Meyer & Kunreuther, 2017). Dit zou kunnen verklaren waarom cybersecurity vaak laag op de prioriteitenlijst van mkb-bedrijven staat.

Begrip van de waarde van cyberbeveiligingsmaatregelen: uit de focusgroep bleek dat dienstverleners vaak onvoldoende in staat zijn het nut van hun diensten en producten te vertalen naar de bedrijfscontext,

waardoor mkb-ondernemers de waarde van cyberbeveiligingsmaatregelen niet altijd inzien en moeite hebben om het belang ervan voor hun bedrijfscontinuïteit te begrijpen. Als ondernemers niet geloven dat de maatregelen daadwerkelijk verschil maken, zijn ze minder geneigd om erin te investeren. Ze hebben dan onvoldoende overtuiging over de impact van cyberbeveiligingsmaatregelen op hun bedrijfscontinuïteit, wat hen ontmoedigt om actie te ondernemen. Dit gebrek aan vertrouwen in de effectiviteit van de maatregelen draagt bij aan het lage gevoel van urgentie en belang rondom cyberweerbaarheid. Hierdoor hebben ondernemers vaak moeite om de juiste vragen te stellen aan cybersecurity-experts en zijn ze minder in staat om goede keuzes te maken. Ondernemers moeten daarom bewust worden gemaakt van het belang van cyberweerbaarheid, zodat zij hun overtuigingen over de effectiviteit en de gevolgen van maatregelen kunnen bijstellen.

Aantoonbaarheid waarde van cyberbeveiligingsmaatregelen: een andere barrière voor mkb'ers is dat de voordelen van cyberbeveiligingsmaatregelen vaak moeilijk te vertalen zijn naar concrete bedrijfsresultaten. De effectiviteit van maatregelen, zoals beveiligingssoftware of personeelstraining, blijft vaak onzichtbaar zolang incidenten uitblijven. Pas bij een aanval wordt duidelijk hoe waardevol deze investeringen zijn. Dit maakt het voor ondernemers lastig om de waarde van deze maatregelen vooraf aan te tonen, aangezien de voordelen pas zichtbaar zijn bij het optreden van een probleem. In dit verband noemen Meyer en Kunreuther (2017) de kortzichtigheidheuristiek, waarbij besluitvormers de langetermijnavoordelen van beschermende maatregelen niet zien of uitstellen, omdat ze niet goed de toekomstige voordelen kunnen inschatten, die pas na een incident zichtbaar worden. Beslissingen om te investeren in beschermende maatregelen vereisen vooruitziendheid, wat voor ondernemers uitdagend kan zijn, omdat de waarde van toekomstige investeringen vaak moeilijk te overzien is. Ondernemers gaven aan dat het benadrukken van de voordelen van preventieve cyberbeveiligingsmaatregelen en het delen van praktijkvoorbeelden van andere bedrijven, hen kan motiveren om actie te ondernemen. Dit helpt om de abstracte voordelen tastbaarder te maken en ondernemers te overtuigen van het belang van investeren, ook als de voordelen pas op lange termijn zichtbaar zijn. Door de kortzichtigheidheuristiek te doorbreken en de voordelen concreter te presenteren, kan de motivatie om in cyberweerbaarheid te investeren worden vergroot.

Conclusie en aanbevelingen

Dit onderzoek richtte zich op de vraag onder welke voorwaarden mkb-ondernemers bereid zijn om te investeren in hun cyberweerbaarheid. Uit de focusgroep blijkt dat drie generieke gedragbepalers cruciaal zijn: capaciteit, gelegenheid en motivatie. Ondernemers beschikken niet altijd over voldoende kennis of praktische vaardigheden om effec-

tieve cyberbeveiligingsmaatregelen te treffen. Technische en abstracte communicatie vanuit dienstverleners belemmert bovendien het gebruik van beschikbare initiatieven en ondersteuningsmogelijkheden. Heldere, contextspecifieke informatievoorziening is essentieel om de capaciteit te versterken. Ook gelegenheid blijkt een bepalende factor. Ondernemers zijn wél bereid te investeren, mits de ondersteuning laagdrempelig is en aansluit bij hun praktische realiteit. Denk aan subsidies, vouchers of praktische tools die inspelen op hun beperkte tijd en middelen. Verder worden op het gebied van motivatie drempels ervaren. De urgentie om te investeren wordt vaak pas gevoeld na een incident; preventieve investeringen blijven daardoor uit. Ondernemers ervaren cybersecurity als een abstract thema zonder directe bedrijfs-waarde. Praktijkvoorbeelden, concrete succesverhalen en simulaties kunnen deze perceptie kantelen en cyberweerbaar gedrag stimuleren.

Wij adviseren publieke en private dienstverleners dan ook om te investeren in begrijpelijke communicatie, toegankelijke ondersteuning en contextgerichte voorlichting. Alleen dan kan daadwerkelijk een belangrijke stap worden gezet richting een hoger niveau van cyberweerbaarheid.

Referenties

- (1) <https://techround.co.uk/news/60-of-smes-that-suffer-a-cyber-attack-go-out-of-business-within-six-months/>
- (2) <https://www.abnamro.nl/nl/zakelijk/insights/sectoren-en-trends/alle-sectoren/mkb-isoleert-zich-door-beperkt-bewustzijn-cyberdreiging.html>
- (3) <https://www.digitaltrustcenter.nl/nieuws/veel-kleine-bedrijven-zijn-onvoldoende-cyberweerbaar>

Literatuur

- Meyer, R., & Kunreuther, H. (2017).** The ostrich paradox: Why we underprepare for disasters. - University of Pennsylvania Press.
- Michie, S., van Stralen, M. M., & West, R. (2011).** The behaviour change wheel: A new method for characterizing and designing behaviour change interventions. Implementation - Science, 6(1), 42. <https://doi.org/10.1186/1748-5908-6-42>.
- SIDN. (2023).** MKB en cyberweerbaarheid: Uitdagingen en kansen. SIDN. <https://www.sidn.nl/whitepaper/mkb-cyberweerbaar?>
- Van der Kleij, R. (2025).** Nu veiligheid er niet meer is: Naar een aanpak van cyberrisico's die wel werkt (Lectorale rede). Avans Hogeschool.
- Zigbano-Wenzler, E., Magwood, G. S., Mueller, M., & Fraser, A. (2020).** Establishing content validity for a conceptualized instrument to measure barriers to eating a healthful diet in adults: a consensus approach. BMC Health Services Research, 20, 1-13.



De CISO als bruggenbouwer

Meer dan techniek alleen

In veel organisaties is de Chief Information Security Officer (CISO) een eenling met een ingewikkelde missie. Hij of zij moet securityrisico's zichtbaar maken en beheersbaar houden – vaak zonder formeel mandaat, zonder directe toegang tot de top en met beperkte middelen. Terwijl compliance, dreigingen en publieke verwachtingen almaar toenemen, moet de CISO voortdurend anderen in beweging krijgen: bestuurders, lijnmanagers, projectleiders, leveranciers, collega's.

Daarbij is technische expertise niet genoeg. Het echte werk van een CISO speelt zich af op het grensvlak van business en IT. De CISO moet begrijpen hoe besluitvorming werkt, wie invloed heeft, wat mensen drijft en hoe je dat krachtenveld gebruikt om beweging te creëren. Wie die 'zachte' kant niet beheerst, loopt vast – hoe deskundig de risicoanalyses ook zijn. En dat maakt het vak van CISO moeilijker dan het op papier lijkt.

De praktijk is weerbarstig

Stel je werkt maandenlang aan een businesscase voor een monitoringoplossing. Alles klopt: de kosten zijn scherp, de baten inzichtelijk, de risicovlagging overtuigend. En toch strandt het voorstel in het MT. Hoe kan dat? Bijvoorbeeld een onvoldoende gevoel van urgentie bij de besluitvormers en geen aansluiting bij hun beleavingswereld. Je kunt denken dat de inhoud vanzelf wel zal overtuigen, maar dat is meestal niet het geval. Je zal veel eerder moeten snappen wat de echte belangen aan tafel zijn en daar je boodschap op moeten afstemmen.

Het is een herkenbaar voorbeeld voor veel security professionals die de stap maken naar een strategische rol. Je wordt geconfronteerd met organisatiepolitiek, met informele macht, met weerstand die zelden openlijk wordt uitgesproken. De positie van CISO vraagt dan ook om politieke sensitiviteit: het vermogen om de onderstroom te lezen, de krachtenvelden te duiden en daarbinnen effectief te opereren.

Het gaat in de boardroom vaker over gelijk krijgen dan over gelijk hebben; maar waar leer je dat?

Opleiding als hefboom

De CISO Masterclass is, vanuit onze eigen ervaringen, ontstaan vanuit precies die vraag. In 2014 begonnen we aan een opleidingstraject waarin de zachte kant van het vak centraal staat. Niet als vervanging van technische of juridische kennis, maar als noodzakelijke aanvulling voor wie impact wil maken op strategisch niveau.

De deelnemers zijn ervaren securityprofessionals die doorgegroeid zijn of op het punt staan die stap te maken. Wat ze gemeen hebben: het besef dat het vak fundamenteel verandert zodra je aan de besluitvormingstafel komt. Dan gaat het ineens niet meer over firewalls of SIEM-systemen, maar over strategische doelstellingen, investeringsprioriteiten en reputatierisico's. En over hoe je daar als CISO serieus in kunt meepraten.

De masterclass biedt daarvoor geen kant-en-klare oplossingen. Wat we wel bieden, is een intensief leertraject waarin deelnemers hun eigen praktijk inbrengen, samen dilemma's verkennen, leren van elkaars aanpak en onder begeleiding oefenen met thema's als invloed, overtuigingskracht en bestuurlijke communicatie.

Leren in context

Wat de masterclass onderscheidt, is dat we niet werken met fictieve cases, maar met échte vraagstukken van deelnemers. Iemand worstelt met het draagvlak voor een awarenessprogramma. Een ander zoekt naar de juiste positionering van zijn rol binnen de governance-structuur. Een derde bereidt een gesprek voor met de auditcommissie. Deze situaties worden gedeeld, onderzocht, uitgespeeld – en iedereen leert ervan.

De docenten zijn oud-CISO's en ervaringsdeskundig. Hoe beoordelen zij een securityvoorstel? Wat werkte bij hen in de boardroom en wat juist niet? Wie is de eigenlijk probleemeigenaar achter een voorstel; de directie of de CISO? En hoe krijg je dat over de Bühne? Die inkijk in de realiteit van besluitvorming blijkt vaak een eyeopener.

Deelnemers leren hoe ze hun verhaal relevanter, compacter en businessgericht kunnen maken. In plaats van een technisch gedetailleerde analyse, presenteert je bijvoorbeeld drie scenario's met impact op reputatie, conti-

nuititeit en aansprakelijkheid – inclusief wat het zou kosten om elk scenario beheersbaar te maken. Daarmee zorg je ervoor dat het (h)erkent wordt door de directie en dat die zich ook eigenaar gaat voelen.

Van inhoud naar invloed

De impact van de masterclass zit niet alleen in de inhoudelijke kennis of de concrete tools die deelnemers meekrijgen. Die zijn er zeker – over stakeholderanalyse, beïnvloedingsstijlen, communicatiestrategieën – maar de werkelijke waarde zit in de persoonlijke ontwikkeling. Veel deelnemers ontdekken gaandeweg hoe hun eigen houding, aannames of blinde vlekken hun effectiviteit beïnvloeden. En hoe je daar met kleine veranderingen veel in kunt winnen.

Bovendien stopt het leren niet na de laatste trainingsdag. Je neemt al het geleerde mee in een persoonlijk werkboek, waar je nog vaak zaken in zult naslaan. Dat maakt het leerproces duurzaam en relevant, ook in de veranderende praktijk van morgen.

Geen luxe, maar noodzaak

Soms wordt gedacht dat opleidingen voor CISO's een 'nice to have' zijn – iets voor als er tijd en budget over is. Maar in de praktijk zien we dat juist de organisaties die investeren in deze vorm van leiderschapsontwikkeling, de vruchten plukken. Ze hebben CISO's die eerder draagvlak krijgen voor noodzakelijke maatregelen, die beter samenwerken met andere stafafdelingen en die met meer vertrouwen optreden in externe audits of toezichtstrajecten.

En dat is nodig ook. Want met de komst van regelgeving zoals de NIS2-richtlijn en de almaar aanscherpende eisen rond privacy en compliance, wordt de directie steeds actiever in het spel gebracht en wordt van organisaties verwacht dat zij aantoonbaar in control zijn. De CISO van morgen moet hiertoe voldoende geëquipeerd zijn om onderdeel te zijn van dit spel. Niet alleen qua techniek, maar ook qua organisatorische positionering en politieke sensitiviteit. Een CISO die stevig in de schoenen staat en de rug recht kan houden, is daarvoor onmisbaar.

Tot slot

Het vak van CISO is volwassen geworden. Het is niet langer een technisch specialisme aan de rand van de organisatie, maar een cruciale rol in het hart van de bedrijfsvoering. Een rol die méér vraagt dan vakinhoudelijke kennis. Het vraagt om inzicht, overtuigingskracht en het vermogen om mensen mee te krijgen in een abstract, maar urgent, verhaal.

Daarom is investeren in de bredere ontwikkeling van CISO's geen luxe, maar noodzaak. Niet om te zenden, maar om te leren luisteren. Niet om te overtuigen met argumenten alleen, maar om verbinding te maken met belangen. En bovenal: om vanuit eigen kracht écht invloed te leren hebben.

Auteur: Inge Wetzer is werkzaam bij Bureau Veritas Cybersecurity als sociaal psycholoog cybersecurity & compliance. Zij is gepromoveerd in de sociale psychologie en is bereikbaar via e-mail: inge.wetzer@bureauveritas.com



Baat het niet dan schaadt het wel... Waar begin je dan wél met gedragsverandering?

Deel 2 van tweeluik

Steeds meer organisaties zetten in op gedragsverandering om cyberveiligheid te vergroten, maar lang niet alle programma's leveren het gewenste effect op. In het eerste deel (1) van dit tweeluik werd besproken dat slecht afgestemde interventies zelfs kunnen leiden tot frustratie, weerstand en afname van veilig gedrag. Dit tweede deel laat zien waar je dan wél begint. Op basis van een benchmark, onder dertien organisaties en ruim tweeduizend medewerkers, is in kaart gebracht welke cybergedragingen het meest en het minst worden vertoond en welke gedragsfactoren (weten, willen of kunnen) daarbij het meest ontbreken. Deze resultaten geven organisaties richting: welk gedrag verdient prioriteit en aan welke knop moet worden gedraaid om verandering in gang te zetten. Voor organisaties die zelf nog niet meten, biedt deze benchmark een onderbouwd vertrekpunt om gericht en effectiever aan de slag te gaan met gedragsverandering.

Van goede bedoelingen naar gerichte actie

Steeds meer organisaties zetten gedragsprogramma's in om medewerkers cyberveiliger te laten werken. Maar, zoals werd besproken in het eerste deel van dit tweeluik, zijn deze programma's niet altijd effectief. Ze kunnen zelfs averechts werken. Wanneer medewerkers worden overspoeld met informatie die ze al kennen, kan dat leiden tot security fatigue, waardoor ze nieuwe boodschappen minder serieus nemen. Ook worden programma's vaak niet goed afgestemd op de juiste gedragsfactor: kennis wordt eindeloos herhaald terwijl het echte probleem ligt in motivatie of praktische belemmeringen. Daarnaast sluiten trainingen regelmatig niet aan op het kennisniveau van medewerkers, waardoor zij zich niet serieus genomen voelen of afhaken. Dit alles kan ertoe leiden dat gedragsprogramma's niet alleen ineffectief zijn, maar zelfs weerstand en frustratie oproepen. De vraag is dus: als veel organisaties de verkeerde aanpak kiezen, hoe zorg je er dan voor dat een gedragsprogramma wél werkt? Waar begin je als je gedragsverandering écht wilt realiseren? De beste aanpak

begint met het meten van wat er in de eigen organisatie speelt. Op die manier krijg je inzicht in de gedragingen die in je eigen organisatie het meest aandacht nodig hebben. Ook geeft het richting: aan welke knop kun je het beste draaien om dit gedrag te veranderen; ligt het ontbreken van bepaald gedrag aan capaciteit (wéten mensen het niet), motivatie (willen mensen het niet) of gelegenheid (worden mensen niet in staat gesteld)? Helaas heeft niet elke organisatie de mogelijkheid om dit uitgebreid in kaart te brengen. Daarom biedt dit artikel een startpunt: op basis van een benchmark van gedragsmetingen bij verschillende organisaties, laten we zien welke onderwerpen vaak al goed gaan, waar de grootste knelpunten zitten en welke patronen we terugzien in cyberveilig gedrag.

Deze inzichten helpen om te bepalen waar jouw aandacht het meeste effect zal hebben. Ze bieden een richting voor organisaties die niet direct de mogelijkheid hebben om grootschalig te meten, maar toch een datagedreven aanpak willen hanteren. Met deze inzichten kun je gericht aan de slag met gedragsprogramma's die niet alleen

effectief zijn, maar ook voorkomen dat medewerkers afhaken of weerstand opbouwen. Kortom, een richting om met gedragsverandering op de juiste plek te beginnen.

Benchmark: waar te beginnen?

De data zijn verzameld bij 13 organisaties, variërend van kleine tot grote bedrijven en van de publieke sector tot industriële bedrijven. In totaal hebben 2616 – 5423 medewerkers deelgenomen aan het onderzoek (aantallen wisselen per onderwerp, omdat de onderwerpen alleen worden meegenomen als zij voor een organisatie een risico vormen). Deze grote steekproef stelt ons in staat een breed en representatief beeld te geven van cyberveilig gedrag in verschillende werkomgevingen. Deze benchmark biedt waardevolle inzichten in welke cybersecurity-onderwerpen medewerkers goed beheersen, waar nog hiaten zitten en welke gedragsdrempels het meest voorkomen. Door deze data te analyseren, kunnen we niet alleen trends en patronen blootleggen, maar ook concrete aanknopingspunten bieden voor organisaties die hun gedragsprogramma's effectiever willen maken.

Methode

De meting werd uitgevoerd met een online vragenlijst, die bestond uit meerdere onderdelen. In totaal zijn 23 cybersecurity-onderwerpen geselecteerd, gebaseerd op richtlijnen van ISO, NIST en NEN. Voor elk van deze onderwerpen is een meerkeuzevraag ontwikkeld om het kennisniveau van medewerkers te meten. Naast kennis is in deze meting ook gekeken naar gedrag, omdat dát uiteindelijk is waar het om draait. Veel organisaties zeggen dat ze inzetten op bewustwording, maar wat ze eigenlijk willen, is dat medewerkers het juiste doen. Niet alleen weten wat veilig gedrag is, maar het ook daadwerkelijk toepassen in de praktijk. Een medewerker die precies weet wat er van hem verwacht wordt maar het niet doet, vormt immers nog steeds een risico. Daarom is per onderwerp niet alleen gemeten of medewerkers het juiste antwoord weten, maar ook in hoeverre zij het bijbehorende gedrag vertonen.

Om echt te begrijpen waarom medewerkers wel of juist niet cyberveilig handelen, zijn naast kennis en gedrag ook de twee andere gedragsbepalende factoren gemeten: motivatie en gelegenheid. Motivatie gaat over de vraag of iemand bereid is om het gewenste gedrag te vertonen. Gelegenheid kijkt naar de praktische omstandigheden: is het gedrag überhaupt uitvoerbaar in de werkomgeving van de medewerker? Door al deze factoren te meten, wordt duidelijk waar het knelt. Alleen als je weet waar het probleem zit: in weten, willen of kunnen, kan je gericht ingrijpen en het gedrag echt veranderen.

Resultaten: hoe staan we ervoor?

Hoe staan medewerkers ervoor als het gaat om cyberveilig gedrag?

Want kennis is een voorwaarde, maar gedrag is het doel

Om dat zichtbaar te maken, zijn alle resultaten samengebracht in één overzichtelijke tabel. Per onderwerp is te zien hoe vaak het gewenste gedrag wordt vertoond. Dit overzicht laat in één oogopslag zien wat al goed gaat en waar nog winst te behalen valt. Een waardevol startpunt voor wie gericht aan de slag wil met gedragsverandering. De tabel is gerangschikt op basis van gedrag, omdat dát uiteindelijk het doel is: een organisatie waarin medewerkers het gewenste gedrag daadwerkelijk vertonen. Niet gesorteerd op kennis, maar bewust op doen. De onderwerpen bovenaan zijn degene waar het gedrag het meest op orde is. Onderaan staan de onderwerpen waar het gedrag nog achterblijft. Juist die onderwerpen zijn interessant. Als ergens gestart wordt met gedragsverandering, dan is dit de plek waar de meeste impact te maken is.

Onderwerp	Gedrag	Capaciteit	Motivatie	Gelegenheid
Sociale media	94	92	91	
Werkaccount delen	87	93	92	92
AI	83	39	76	
Unieke wachtwoorden	69	84	86	
Incidenten melden 2	69	62	88	92
Veilig opslaan	68	89	89	94
Privemail	68	91	76	76
Cleandesk	68	97	89	81
Browser opslag	62	68	76	
Computerscherm vergrendelen	60	97	85	98
Sterke wachtwoorden 2	57	8	88	
Phishing herkennen	53	72	93	
Updates uitvoeren	42	74	86	
Malvertising	31	11	82	
Veilige URL	29	25	86	
Veilig delen	24	83	89	86
Onbekenden aanspreken	23	81	73	80
Wachtwoordmanager	20	73	60	75

Gedrags tabel, factoren en impactkansen (hoe lager, hoe meer)

Nu duidelijk is met welk gedrag gestart moet worden (de onderwerpen onderaan de tabel dus), is de volgende stap om te kijken welke factor van het gedrag het meest ontbreekt: capaciteit (weten), motivatie (willen) of gelegenheid (kunnen). Goed, gewenst gedrag komt pas tot stand als alle drie factoren aangesproken zijn. In de tabel is per onderwerp inzichtelijk gemaakt welke van deze factoren het meest ontbreken. Op basis daarvan kunnen gerichte interventies worden gekozen die aansluiten bij de échte oorzaak. Licht het knelpunt bij motivatie, dan helpt het weinig om opnieuw kennis aan te bieden. En als medewerkers wel willen en weten wat ze moeten doen, maar

In de praktijk is weerbaarheid sterk geïnspireerd door organische systemen, zoals het menselijk immuunsysteem

worden belemmerd door de werkomgeving, dan moet juist dáár iets veranderen. Zonder deze afstemming loop je het risico mensen te vermoeien met de verkeerde prikkel. Dat leidt niet alleen tot ineffectiviteit, maar kan ook zorgen voor frustratie en weerstand tegen het hele programma.

Wat leren deze cijfers ons?

Deze cijfers vormen een waardevol vertrekpunt voor organisaties die zelf (nog) geen meting kunnen uitvoeren. Omdat de resultaten gebaseerd zijn op het gedrag van duizenden medewerkers verspreid over verschillende typen organisaties, geven ze een betrouwbaar gemiddeld beeld van waar het vaak goed gaat en waar het juist nog knelt. Natuurlijk blijft het ideaal om binnen de eigen organisatie te meten, maar als dat op korte termijn niet mogelijk is, bieden deze cijfers een stevige basis. Ze geven meer houvast dan op onderbuikgevoel of aannames te sturen, en helpen om gericht te kiezen waar te beginnen met gedragsverandering. Om te illustreren hoe deze tabel in de praktijk gebruikt kan worden om interventies te ontwikkelen, is hieronder het onderwerp 'wachtwoordmanagers' uitgewerkt.

Wachtwoordmanagers

Eén van de eerste onderwerpen die uit deze cijfers naar voren komt, als aandachtspunt, is het gebruik van een wachtwoordmanager. Als we naar het gedrag kijken, zien we dat dit nog relatief weinig voorkomt, wat het tot een logische start maakt voor gedragsverandering. De kennis over dit onderwerp is nog niet optimaal: 71 procent van de medewerkers weet wat een wachtwoordmanager is en hoe die werkt. Dat betekent dat er een groep is (29%) die eerst moet leren wat het precies is en waarvoor je het gebruikt. Maar opvallender is dat vooral de motivatie achterblijft (58%). Met andere woorden: zelfs onder medewerkers die het wel weten, is de bereidheid om het ook echt te gaan gebruiken laag. Dat maakt motivatie op dit onderwerp de belangrijkste knop om aan te draaien. Pas als die verhoogd wordt, heeft verdere kennisdeling of het wegnemen van praktische obstakels zin.

Aan de slag met motivatie dus, maar hoe? Uit de interviews, die aanvullend op de metingen zijn uitgevoerd, blijkt dat de lage motivatie voor het gebruik van wachtwoordmanagers vaak niet voortkomt uit onwil, maar uit onzekerheid. Veel medewerkers hebben een laag vertrouwen in hun eigen kunnen, ook wel self-efficacy genoemd. Ze denken dat het te moeilijk is, zien op tegen de installatie en haken bij voorbaat af omdat ze verwachten eerst een ingewikkelde handleiding te moeten doorlezen. Die drempel zorgt ervoor dat het gedrag niet van de grond komt, zelfs als het belang ervan wordt ingezien. De oplossing ligt in het helpen overwinnen van die barrière. Bijvoorbeeld door een laagdrempelige lunchsessie te organiseren waarin medewerkers stap voor stap aan de hand worden genomen bij het installeren en gebruiken van een wachtwoordmanager. Zo wordt het gedrag concreet, behapbaar en haalbaar en stijgt de kans dat mensen het ook echt gaan doen.

Conclusie

Gedragsverandering begint niet met doen, maar met begrijpen. Begrijpen welk gedrag achterblijft en vooral: waarom. Deze benchmark laat zien dat er tussen organisaties grote verschillen zijn, maar dat er wel degelijk onderwerpen zijn waar gedrag gemiddeld achterblijft. Door per gedraging te kijken welke factor ontbreekt, wordt het mogelijk om gerichte en passende interventies te ontwikkelen. Zo voorkom je dat medewerkers vermoeid raken door herhaling van wat ze al weten of gefrustreerd door obstakels die niet worden weggenomen. Of er nu wel of geen ruimte is voor eigen metingen, deze inzichten bieden een concreet startpunt om met gedragsverandering aan de slag te gaan op een manier die écht effect heeft. Want pas als de aanpak klopt, komt het gedrag in beweging.

Referenties

- (1) InformatieBeveiliging Magazine, jaargang 25 - 2025 - editie 1, pagina 22 t/m 26 met uitzondering van de eerste paragraaf na de inleiding (pagina 23) dat een zetfout was en niet tot het artikel behoorde.



1+1=3

Samenwerken moet waarde toevoegen

Steeds meer organisaties worden slachtoffer van een cyberaanval. De impact hiervan op de organisatie, hun medewerkers en andere betrokkenen is enorm groot. Van organisaties wordt verwacht dat zij hun beveiligingsniveau verhogen en de kans en impact van cyberaanvallen verlagen. De meeste organisaties kunnen dit niet alleen en schakelen hiervoor IT- en security-dienstverleners in. Gegarandeerd een beter beveiligde organisatie zou je denken, maar helaas laat de praktijk nog te vaak wat anders zien. Er wordt niet goed genoeg samengewerkt waardoor de toegevoegde waarde achterblijft. Het is tijd om echt samen aan de slag te gaan en meer waarde uit de samenwerking te halen.

Overvloed aan keuzes

De beschikbare maatregelen om jouw organisatie tegen cyberaanvallen te beschermen nemen toe. Deze toename is aan de ene kant een goede ontwikkeling. Aan de andere kant leidt het tot zorgen. Wekelijks kom ik bij verschillende organisaties over de vloer. Ze zien door de bomen het bos niet meer. Er zijn zoveel keuzes om te maken en ze weten vaak niet hoe de juiste keuze te maken.

Er komen steeds meer IT- en security-dienstverleners bij. De diensten die geleverd kunnen worden zijn er in allerlei soorten en maten. Een menukaart in een restaurant is er niets bij. Daarnaast is er ook een stijging te zien in de tooling die in te zetten is om security-uitdagingen aan te gaan. Regelmatig krijg ik de vraag: welke tool heb ik nodig? Wat mij betreft: "Het draait niet om de tooling." De tool is een middel en niet het doel. Welk doel wil je als organisatie bereiken? Het maakt mij niet uit welke dienstverlener, dienst of tool jij als organisatie kiest. Als je maar een doelbewuste keuze maakt.

Schaarste in experts

Om securityrisico's te identificeren en maatregelen te nemen is er expertise nodig. Dat leidt weer tot een nieuwe uitdaging: het zelf

doen of hiervoor externe expertise inschakelen. Dat laatste kan bijvoorbeeld door een dienst af te nemen. In de praktijk wordt er dan gesproken over een uitbesteding. Een volledige uitbesteding van IT- en security-dienstverlening bestaat echter niet. Als eindklant ben en blijf je altijd zelf (eind)verantwoordelijk voor IT en security. We moeten dan ook stoppen met het gebruik van de term "uitbesteding". Dus je doet het zelf of je doet het samen (ook wel hybride genoemd). Door de schaarste in expertise wordt er vaak gekozen om samen te werken met een dienstverlener.

1 + 1 = 1.5

Dat samendoen is waar ik het vaak mis zie gaan. We werken niet goed genoeg samen. Wekelijks hoor ik geklaag. Geklaag over IT-dienstverleners en security-partijen, maar ook over klanten. Geklaag dat vaak niet bij de juiste persoon terechtkomt en niet opgelost wordt. Dat moet anders.

Graag deel ik wat ik hiervan in de praktijk mee maak aan de hand van vier verschillende fases.

Inkoop

Dienstverlening staat lang niet altijd goed beschreven in contract-documentatie. Denk bijvoorbeeld aan verantwoordelijkheden en

garanties die gegeven worden. Als je niet weet wat je koopt, koop het dan niet. Of zorg ervoor dat het duidelijk wordt wat je koopt. Het komt ook regelmatig voor dat dienstverleners weigeren wijzigingen te maken in de teksten. Het betreft namelijk een "standaard dienst" en daarop afwijken is niet mogelijk.

Ik ben ervan overtuigd dat de kwaliteit omhooggaat als we met z'n allen kritische vragen blijven stellen aan dienstverleners. Als de dienstverleners deze vragen serieus nemen, worden zowel de klanten als de dienstverleners hier beter van.

Implementatie

Implementatietrajecten lopen vaak vertragingen op of kunnen pas na enkele maanden starten. Verwachtingen zijn niet duidelijk, instructies worden niet juist opgevolgd of er wordt te weinig informatie gedeeld. Het resultaat? Frustraties aan beide kanten.

Ook hier zijn communicatie en de communicatiemiddelen cruciaal. Ik ben klaar met die enorme vragenlijsten die een klant moet invullen om informatie op te leveren. Organiseer een sessie waarin opdrachtgever en dienstverlener samen de benodigde informatie boven tafel halen. Werk samen op dezelfde locatie tijdens het implementatietraject. De ene keer bij jou, de andere keer bij hen. Dit klinkt als een duurdere oplossing, maar uiteindelijk werk je efficiënter en dat is goedkoper.

Operatie

Frustraties omdat de dienstverlener de patch nog steeds niet heeft uitgevoerd of een te groot aantal SOC-meldingen waar vervolgens niets meegedaan wordt. Acties die te lang op zich laten wachten in een dreigende situatie, of waar niets meegedaan wordt, brengen een groot risico met zich mee.

Als er geen ruimte voor feedback is, dit niet bij de juiste persoon terecht komt of hier te weinig mee gedaan wordt, stapelen de frustraties en teleurstellingen zich snel op. Met als resultaat dat het vertrouwen afneemt. De optie om de samenwerking te beëindigen wordt steeds reëler. Zonde. Bepaal wanneer de samenwerking succesvol is en hoe dit continu geëvalueerd wordt. Maar bovendien bepaal hoe feedback verwerkt wordt en conflicten snel opgelost worden.

Crisis

Dan gebeurt hetgeen waarvan je had gehoopt dat nooit zou gebeuren. De organisatie wordt slachtoffer van een cyberaanval. Van het niet kunnen bereiken van de IT-dienstverlener tot aan discussies over wie er verantwoordelijk was voor de back-ups. De verwijten vliegen om je oren tijdens een cyberincident. Onder grote druk komt naar voren hoe goed de samenwerking echt is.

Gelukkig is het mogelijk om hier vóór een cyberaanval al te werken aan de samenwerking. Maak afspraken over bijvoorbeeld bereikbaarheid, beschikbaarheid, verantwoordelijkheden en ook de locatie waar je samenwerkt tijdens een crisis. Tijdens een cybercrisis heb je al genoeg aan je hoofd, dan wil je je niet bezighouden met conflicten in de samenwerking.

1 + 1 = 3

We moeten er met elkaar voor zorgen dat 1 + 1 uitkomt op 3. Samenwerken hoort een beter resultaat op te leveren. Een hoger beveiligingsniveau. Een lagere kans op, en impact van, cyberaanvallen. Er zijn zoveel manieren om de samenwerking te verbeteren. Het gaat niet om of je het een dienstverlening, samenwerking of partnership noemt. Het gaat om wat je doet en hoe je dat doet. Dit bepaal je samen. Om er even een metafoor in te gooien: een samenwerking in IT of security is niet heel veel anders dan samen een plant verzorgen. Je hebt hiervoor nodig:

- Een gemeenschappelijk doel
- Inzicht in behoeftes
- Duidelijk afspraken en communicatie
- Het vermogen om problemen te constateren
- Creativiteit om oplossingen te bedenken en door te voeren
- Geduld en tijd

Tijd voor actie

We zijn op de goede weg, maar we zijn er nog niet. We dragen allemaal bij aan fantastische initiatieven op security-vlak. Communities, publiek-private samenwerkingen, kennisdelingsessies en ga zo maar door. Een zeer goede ontwikkeling, maar vergeet de bijdrage aan de samenwerking met jouw IT- en security-dienstverleners niet.

Het is tijd om aan de slag te gaan en je samenwerkingen onder de loep te nemen.

- Welke samenwerkingen zijn er?
- Welke hebben meer aandacht nodig, en hoe?
- Waar is meerwaarde te behalen, en hoe?
- Welke frustraties moeten opgelost worden, en hoe?

Belangrijk hierbij is dat de afspraken tussen jouw organisatie en de dienstverlener goed en duidelijk vastgelegd zijn. Om het gesprek hierover aan te gaan heeft het Digital Trust Center een 'Praatplaat Digitale Veiligheid' (1) ontwikkeld.

Referentie:

- (1) <https://www.digitaltrustcenter.nl/nieuws/praatplaat-digitale-veiligheid-samenwerken-aan-preventie-en-incidentrespons>



COLUMN PRIVACY

Mr. Rachel Marbus

Mis- of gebruik van recht?

Pietje Weetgraag schrijft zich bij Organisatie XYZ in voor hun nieuwsbrief. Vlak daarna doet Pietje een verzoek tot inzage in zijn persoonsgegevens. De organisatie reageert, allicht wat laat en met wat weinig te melden. Pietje is het er niet mee eens en dient direct een schadeclaim in omdat hij vindt dat de AVG geschonden is. Als Organisatie XYZ online speurwerk verricht, ziet ze dat Pietje Weetgraag dit bij allerlei andere organisaties exact eender heeft gedaan. Vol vertrouwen gaat Organisatie XYZ naar de rechtszaak die volgt. Dit zal toch vast en zeker misbruik van recht zijn?

De Duitse rechter weet het niet zeker en stelt daarom prejudiciële vragen aan het Hof van Justitie van de EU (HvJ). De Advocaat-Generaal (AG) is in diens advies aan het HvJ duidelijk: dit is geen misbruik van recht. De lat voor misbruik van recht bij verzoeken op grond van de AVG is namelijk behoorlijk hoog. Met andere woorden, je moet het wel flink bont maken of je moet wel heel duidelijk een verzoek indienen dat niets meer met jouw privacy van doen heeft.

In deze van origine Duitse zaak schreef de AG in september 2025 in diens advies aan de rechter van het HvJ: "als 'buitensporig' kan worden aangemerkt wanneer (...) er sprake is van opzettelijk misbruik door de betrokkene, dat kan worden vastgesteld wanneer deze betrokkene met de verwerking van zijn persoonsgegevens heeft ingestemd om dit verzoek tot inzage te kunnen indienen en vervolgens een vordering tot schadevergoeding te kunnen instellen". De AG vervolgt: "het feit dat uit openbaar toegankelijke informatie blijkt dat de betrokkene in een groot aantal gevallen (...) vorderingen tot schadevergoeding jegens verwerkingsverantwoordelijken heeft ingesteld, op zich niet volstaat om een dergelijk verzoek als 'buitensporig' aan te merken."

En hoewel ik de AG zeer goed kan volgen, de lat voor misbruik moet ook hoog gelegd worden om de uitoefening van rechten niet te frustreren, voelt dit advies aan de rechter toch niet helemaal rechtvaardig. Je zou je dan ook kunnen afvragen of het wel deugt dat deze Pietje dit telkens maar weer blijft doen, moreel stinkt het zaakje een beetje. Er is een duidelijk aantoonbaar patroon waarin Pietje telkens hetzelfde gedrag vertoont. De angel zit hem er dan natuurlijk wel in of je kunt aantonen dat Pietje in deze specifieke zaak een intentie tot misleiden heeft, er moet sprake zijn van opzettelijk misbruik. En daar wordt het wel lastig. Toch zie ik wel degelijk ruimte om die intentie af te leiden uit het voorgaande gedrag. Of de rechter van het Hof van Justitie van de EU dat ook zo zal zien, is afwachten. En eigenlijk hoop ik toch dat de rechter tenminste zal benadrukken dat dit herhaalde gedrag wel behoorlijk in de richting begint te komen van dat misbruik van recht en daarmee een afschrikkende werking in gang zet bij - in ieder geval - Pietje Weetgraag.

Rachel

Op zoek naar verbinding

Het IB Magazine van PvIB zoekt nieuwe redactieleden. Heb je passie voor informatiebeveiliging en wil je meebouwen aan hét magazine dat vakgenoten verbindt? Schrijf je graag of denk je mee over onderwerpen? Dan pas je perfect in ons team!

Ervaring is mooi meegenomen, maar vooral jouw motivatie telt. Samen zorgen we voor een sterk en relevant magazine, dóór en vóór professionals.

Nieuwsgierig?

Mail ons via ibmagazine@pvib.nl – we maken graag kennis!



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

Alex Dingemanse
Marcel Feenstra
Maarten Hartsuijker
Fook Hwa Tan
Lilian Knippenberg
Leo van Koppen
Rachel Marbus
Chris de Vries

BLADMANAGEMENT

Congres- en Organisatiebureau Interactie BV
Zeynep Turkan
ibmagazine@pvib.nl

VORMGEVING

Neverseen Art & Design
Dimitri van den Berg

DRUK

Veldhuis Media, Meppel

UITGEVER

Platform voor InformatieBeveiliging (PvIB)
Horapark 9
6717LZ Ede
+31 85 799 0233
secretariaat@pvib.nl
www.pvib.nl

*Heb je vragen, opmerkingen of
suggesties, mail dan naar
ibmagazine@pvib.nl*

ABONNEMENTEN

De abonnementsprijs in 2025 bedraagt
€ 118,50 (exclusief btw), prijswijzigingen
voorbehouden.

ABONNEMENTENADMINISTRATIE

Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
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



Is uw organisatie klaar voor de uitdagingen van morgen?

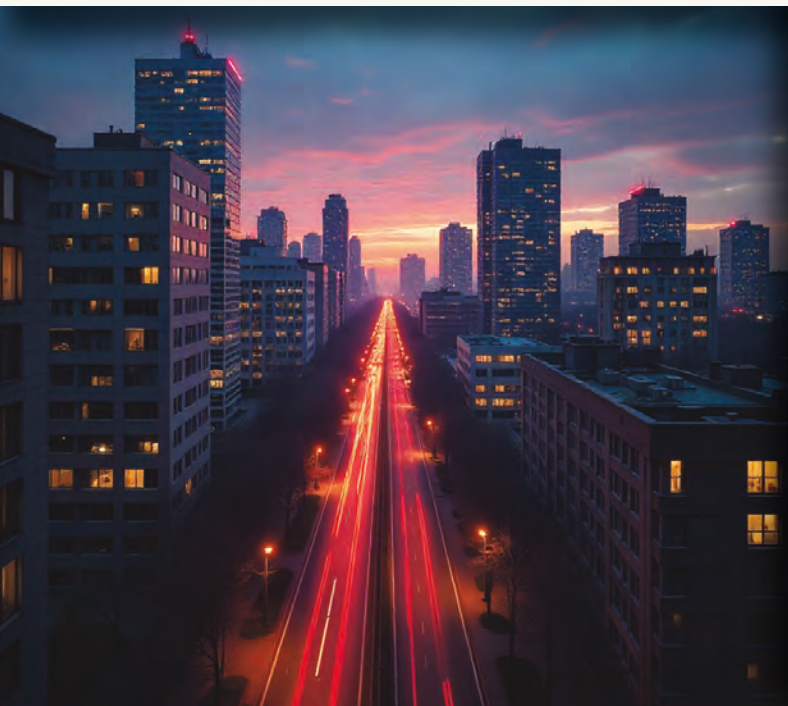
De Security Academy biedt toekomstgerichte cursussen voor organisaties en individuele professionals die voorbereid willen zijn op wat komen gaat.



NIS2-richtlijn



**Quantumveilige
cryptografie**



Artificial-intelligence



Security leadership

Meer informatie

securityacademy.nl

